Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

April 8, 2024

Contents

Introduction

In this report we study a method proposed in [DEW21] for forcing points of infinite order on elliptic curves over finite extensions $F/\mathbb{Q}$.

Notation

We use the following notation for characters:

$B(G)$	the Burnside ring of G,
$R(G)$	the representation ring of G,
$R_{\mathbb{Q}}(G)$	the rational representation ring of G,
$\mathrm{Perm}(G)$	the ring of virtual permutations of G,
$\mathrm{Char}_{\mathbb{Q}}(G)$	the ring of rationally-valued characters of G,
$\mathrm{Irr}(G)$	the set of characters of complex irreducible representations of G,
$\mathbb{Q}(\rho)$	the field of character values of a complex character ρ of G,
$C(G)$	the finite abelian group $\mathrm{Char}_{\mathbb{Q}}(G)/\mathrm{Perm}(G)$,
H^x	$= xHx^{-1}$ for $H \leq G$ a subgroup of a group G and $x \in G$,
p^*	defined for an odd prime p. If $p \equiv 1 \pmod 4$, $p^* = p$. If $p \equiv 3 \pmod 4$, $p^* = -p$

Given an elliptic curve $E/\mathbb{Q}$ and a number field F, we define

$$C_{E/F} = \prod_v c_v(E/F) \left| \frac{\omega}{\omega_v^{\min}} \right|_v .$$

The product is taken over the finite places of F, ω is a global minimal differential for $E/\mathbb{Q}$, and $\omega_v^{\min}$ is a minimal differential at v. In terms of minimal discriminants, if E is of the form

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

with minimal discriminant Δ_E and $\omega = \frac{dx}{2y+a_1x+a_3}$, then

$$\left| \frac{\omega}{\omega_v^{\min}} \right|_v^{-12} = \left| \frac{\Delta_E}{\Delta_{E,v}^{\min}} \right|_v .$$

1 Norm relations

1.1 Representations 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 representations, 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 $\chi_1, \dots \chi_h$ be the distinct characters of the complex irreducible representations of G. Then the **representation ring** of G is

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

Since we take differences of characters in $R(G)$, we sometimes call elements of $R(G)$ **virtual representations**.

Let K be a number field. Denote by $R_K(G)$ the group generated by characters of the representations of G over K. This is a subring of $R(G)$. When $K = \mathbb{Q}$ this is called the **rational representation ring**. The characters of the distinct irreducible representations of G over K form an orthogonal basis of $R_K(G)$ ([Ser77, Proposition 32]). Let m be the exponent of G. If K contains the m-th roots of unity, then $R_K(G) = R(G)$ ([Ser77, Theorem 24]). This implies every representation of G can be realized over such K.

Let $\mathrm{Perm}(G)$ be the ring of virtual permutation representations of G (i.e. the ring generated by the characters of $\mathbb{C}[G/H]$ for $H \leq G$). Let $\mathrm{Char}_{\mathbb{Q}}(G)$ be the ring of rationally valued characters of G. Then we have inclusions

$$\mathrm{Perm}(G) \to R_{\mathbb{Q}}(G) \to \mathrm{Char}_{\mathbb{Q}}(G).$$

Each of these groups have equal $\mathbb{Z}$-rank, equal to the number of conjugacy classes of cyclic subgroups of G ref. Moreover the cokerenels of these maps are finite.

It is of interest to obtain characters of $\mathrm{Perm}(G)$ from characters of $R(G)$. For $\rho \in R(G)$ one obtains an element of $\mathrm{Char}_{\mathbb{Q}}(G)$ by taking

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

Here $\mathbb{Q}(\rho)$ means the smallest Galois field extension that contains the values of $\rho(g)$ for all $g \in G$, and ρ^σ is the character such that $\rho^\sigma(g) = \sigma(\rho(g))$. Conversely, if a representation has a rationally valued character, then any complex irreducible constituent must occur along with all its Galois conjugates with equal multiplicity. Therefore our map $R(G) \to \mathrm{Char}_{\mathbb{Q}}(G)$ is surjective.

Such a character may not be in $R_{\mathbb{Q}}(G)$, however. That is, it has rational character, but the corresponding representation cannot be realized over $\mathbb{Q}$. The quotient $\mathrm{Char}_{\mathbb{Q}}(G)/R_{\mathbb{Q}}(G)$ is the study of Schur indices. If $\rho \in R(G)$ is an irreducible representation, the **Schur index** is the smallest integer $m(\rho)$ such that

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

We are more interested in the group

$$C(G) = \mathrm{Char}_{\mathbb{Q}}(G)/\,\mathrm{Perm}(G).$$

This is a finite abelian group. It has exponent dividing $|G|$ by Artin's induction theorem ref. The study of this group is quite subtle, see for example [BD16]. For us, it's enough to know that there exists an integer m dividing $|G|$ such that $\widetilde{\rho}^{\,\oplus m} \in \mathrm{Perm}(G)$, where m is the order of $\widetilde{\rho}$ in $C(G)$. Thus, we have a map $\mathrm{Irr}(G) \to \mathrm{Perm}(G)$. We extend this additively to a map $R(G) \to \mathrm{Perm}(G)$.

could add some examples of when $C(G)$ is trivial

1.2 The Burnside ring and permutation 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 1.2. 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 1.3. 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:

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

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

Example 1.4. S_3 example

Example 1.5. Cyclic groups have no Brauer relations. reference/explain?

In the last section, we constructed a character in $\mathrm{Perm}(G)$ for $\rho \in R(G)$. We are interested in when this is an image of an element from the Burnside ring.

Definition 1.6. We call $\Theta = \sum_i n_i H_i \in B(G)$ a **ρ-relation** if $\mathbb{C}[\Theta] \simeq \widetilde{\rho}^{\,\oplus m}$, for some $m \geq 1$.

Of course, when $\rho = 0$ these are Brauer relations.

Example 1.7. 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 $\mathrm{Ind}_{C_{n/d}}^{G} \mathbb{1}$ is the direct sum of irreducible complex representations of G

contain $C_{n/d}$ in their kernel. Thus, $\operatorname{Ind}_{C_{n/d}}^{G} \mathbb{1} \simeq \sum_{d'|d} \chi_{d'}$. Applying Möbius inversion, we a φ_d-relation for each $d \mid n$:

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

Note that this is the only way of writing χ_d as a sum of permutation representations, since cyclic groups have no Brauer relations. Similarly, there is a unique $\Theta \in B(G)$ such that $\mathbb{C}[\Theta] \simeq \chi_d^m$ for all $m \geq 1$.

Notation 1.8. 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 representation 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 a multiplicative function $f \colon B(G) \to A$, where A is an abelian group. As in [DD09], say that f is **representation theoretic** if f is trivial on Brauer relations. This means that for a G-set X, f only depends on the representation $\mathbb{C}[X]$.

Example 1.9. Let V be a representation of G. The function $\psi(H) = \dim V^H$ is trivial on Brauer relations, 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.

We want to extend this notion and consider functions that are trivial on ρ-relations. Take a multiplicative function on the Burnside ring of the form $\psi \colon B(G) \to \mathbb{Q}^\times$. Given $\rho \in R_{\mathbb{C}}(G)$ we can extend such functions from the Burnside ring to $\overline{\psi} \colon B(G) \to \mathbb{Q}^\times / N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. try motivate this a bit better, e.g. why do we expect functions to give norms... try relate this back to introduction

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.

If a function f satisfies $f \sim_\rho 1$, we say f is trivial on ρ-relations.

Example 1.12. 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.13.

Example 1.13. Let $\mathbb{Q}(\rho)$ be a quadratic field. Then if $f \colon B(G) \to \mathbb{Q}^\times$ satisfies $f(\Theta) \in \mathbb{Q}^{\times 2}$ for all ρ-relations Θ, one has $f \sim_\rho 1$.

Example 1.14. 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

For our application of functions on the Burnside ring to reference something in intro, we introduce some of the concepts and notation introduced in [DD09, Section 2.iii].

We are interested in functions on the Burnside ring that are number-theoretic in nature, where we take G to be a Galois group. Often, these functions are *local*. For example, let $G = \mathrm{Gal}(F/K)$ and D the decomposition group at the place v. For $H \leq G$, the number of primes in $L = F^H$ above v are in one-to-one correspondence with the double cosets $D \backslash H/G$. We can use the function $f\colon B(G) \to \mathbb{Q}[x]^\times$ given by $H \mapsto x^{|H\backslash G/D|}$ to describe the number of places above v in any intermediate extension of F/K. But if we let $g\colon B(D) \to \mathbb{Q}[x]^\times$ be defined by $H \mapsto x$, then

$$f(H) = g\left(\mathrm{Res}_D H\right) = \prod_{x \in H\backslash G/D} g(D \cap H^{x^{-1}}).$$

Therefore the value of f on any G-set X only depends on the structure of X as a D-set.

Such functions motivate the following definition:

Definition 1.15. ([DD09, Definition 2.33]) If $D \leq G$, we say a function f on $B(G)$ is D**-local** if there is a function f_D on $B(D)$ such that $f(H) = f_D(\mathrm{Res}_D H)$ for $H \leq G$. If this is the case, we write

$$f = (D, f_D).$$

Example 1.16. For $G = \mathrm{Gal}(F/K)$, v a place of K with decomposition group D, the function

$$H \mapsto \prod_{w|v} c_w(E/F^H)$$

is D-local, where E is an elliptic curve over K and c_w is the local Tamagawa number.

Let $I \triangleleft D$ be the inertia subgroup of the place v, so D/I is cyclic. If a prime w in F^H corresponds 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. The ramification degree and residue degree of w over K are given by $e_w = \frac{|I|}{|H \cap I^x|}$ and $f_w = \frac{[D\colon I]}{[H\cap D^x\colon H \cap I^x]}$. We will consider functions that depend on e and f, and so introduce the following:

Definition 1.17. [DD09, Definition 2.35] Suppose $I \triangleleft D < G$ with D/I cyclic, and $\psi(e, f)$ is a function of $e, f \in \mathbb{N}$. Define a function on $B(G)$ by

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

This is a D-local function on $B(G)$ with

$$(D, I, \psi) = \left(D, U \mapsto \psi\left(\frac{|I|}{|U \cap I}, \frac{|D|}{|UI|}\right)\right).$$

Example 1.18. If E/K has split multiplicative reduction at v with $c_v(E/K) = n$, then $c_w(E/F^H) = e_w n$ for a place w of F^H above v. In this case the function in example 1.16 is (D, I, e).

Example 1.19. 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

Question: do i need to be worried about m when i restrict a representation? do i need to adjust my definition of rho relations?

Proposition 1.20. *Let $I \triangleleft D \leq G$ with D/I cyclic. Let $\rho \in R(G)$ Then*

1. *If $f = (D, f_D)$ and f_D is trivial on $(\mathrm{Res}_D \rho)$-relations, then f is trivial on ρ-relations.*
2. *maybe more things to say here. See e.g. [DD09, Theorem 2.36]*

2 Elliptic Curves

Having discussed the relevant aspects of representation theory that we will require, we now introduce elliptic curves, our main object to study. Our discussion will be rather informal and brief, and will avoid most proofs. We will spend some time discussing the reduction type of elliptic curves and how this can change over finite extensions. Nevertheless, we assume good familiarity with elliptic curves. There is great material available for elliptic curves, and [Sil09] gives a complete discussion.

An elliptic curve E over a field K is a genus one smooth projective curve with a specified K-rational point. Any such curve can be written as the locus on $\mathbb{P}^2$ of a **Weierstrass equation**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_2, a_4, a_6 \in K, \tag{1}$$

together with the specified K-rational point $[0 : 1 : 0]$ at infinity.

Associated to this equation, there are constants

$$c_4 = \phi(a_1, a_2, a_3, a_4, a_6) \quad \text{and} \quad \Delta = \psi(a_1, a_2, a_3, a_4, a_6)$$

and differential

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

where ϕ and ψ are explicit polynomials with coefficients over K. The explicit description is lenghty and we omit it. The relevant proposition is the following one.

Proposition 2.1. *The curve given by a Weierstrass equation satisfies:*

1. *It is nonsingular if and only if $\Delta \neq 0$.*
2. *It has a node (singular point with two tangent directions) if and only if $\Delta = 0$ and $c_4 \neq 0$.*
3. *It has a cusp (singular point with one tangent direction) if and only if $\Delta = c_4 = 0$.*

For a complete discussion and proof of the above proposition, see [Sil09, §III.1].

When $\Delta \neq 0$, the equation defines an elliptic curve. A fundamental property is that the set of K-rational points of an elliptic curve forms an abelian group, denoted by $(E(K), \oplus)$ ([Sil09, §III.2]). When K is a number field, the Mordell-Weil theorem shows that this group is also finitely generated, and therefore

$$E(K) = E(K)_{\text{tors}} \times \mathbb{Z}^r,$$

where $E(K)_{\text{tors}}$ is a finite abelian group and r is denoted the rank of E.

2.1 Elliptic Curves over Local Fields and Reduction Types

Now assume that K is a local field of characteristic 0 with a discrete valuation ν, ring of integers R and residue field κ. We denote by $a \mapsto \tilde{a}$ for the natural quotient map $K \to \kappa$. We say that (1) is a **minimal Weierstrass equation** if $a_2, a_4, a_6 \in R$ and $\nu(\Delta)$ is minimal among all such equations. When this is the case, we have a well-defined associated curve $\tilde{E}$ over κ defined by the equation $y^2 = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$ and the associated **reduction map**

$$\widetilde{(\cdot)} : E(K) \longrightarrow \tilde{E}(\kappa), \tag{2}$$

obtained by reducing the coordinates of a point $P \in E(K)$ modulo κ. One needs to have some care defining the reduction map. For a detailed construction, see [Sil09, §1 VII.2]. We remark that $\tilde{E}$ may be a singular curve, and the **reduction type** of E over K describes the behaviour of $\tilde{E}$ as a curve over κ.

Definition 2.2. Let E/K and $\tilde{E}/\kappa$ be as above. Then we say that

(a) E/K has good (or stable) reduction if $\tilde{E}$ is non-singular.

(b) E/K has multiplicative (or semistable) reduction if $\tilde{E}$ has a node.

(c) E/K has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

In cases (b) and (c) we say that E/K has bad reduction. Moreover, if E/K has multiplicative reduction, we say that the reduction is split if the slopes of the tangent lines at the node are in K, and non-split otherwise.

By Proposition 2.1 we immediately see that E/K has good reduction if $\nu(\Delta) = 0$ and bad otherwise. In that case, E/K has multiplicative reduction if $\nu(c_4) = 0$ and additive otherwise.

An important question which will be of interest for us is to understand how the reduction type of an elliptic curve E changes over a finite field extension F/K. The following proposition gathers this information.

Proposition 2.3 (Semistable Reduction Theorem)**.** *Let E be an elliptic curve over a local field K of characteristic* 0.

(i) Let F/K be an unramified extension. Then the reduction type of E over K (good multiplicative or additive) is the same as the reduction type of E over F.

(ii) Let F/K be a finite extension. If E has good or multiplicative reduction over K, then it has the same reduction type over F. This also applies specfically to split multiplicative reduction.

(iii) If E has non-split multiplicative reduction over K and F/K is a finite extension with even residual degree, then E has split multiplicative reduction over F.

(iv) There exists a finite extension F/K such that E has either good or spit multiplicative over F.

Proof. [Sil09, §VII Proposition 5.4] □

Given an unstable elliptic curve E over K, we say that it has potentially good (resp. multiplicative) reduction if it has good (resp. multiplicative) reduction over a finite field extension of K.

2.2 Tamagawa Numbers

Recall from the previous section that if E/K has bad reduction, then $\tilde{E}$ is not a smooth curve and therefore its κ-rational points may not form a group. However, the set $\tilde{E}_{ns}(\kappa)$ of non-singular points of $\tilde{E}(\kappa)$ does indeed form a group. The reduction map (2) is in general not surjective, but it does surject onto $\tilde{E}_{ns}(\kappa)$. It is natural therefore to define $E_0(K) = \{P \in E(K) : \widetilde{P} \in \tilde{E}_{ns}(\kappa)\}$, which is also a subgroup of $E(K)$. Importantly, the resulting reduction map

$$\widetilde{(\cdot)} : E_0(K) \longrightarrow \tilde{E}_{ns}(\kappa)$$

is a surjective homomorphism of abelian groups.

Definition 2.4. The **Tamagawa number** of E/K is defined as

$$c(E/K) := |E(K)/E_0(K)|. \tag{3}$$

In later sections we will be concerned in computing Tamagawa numbers. Note that if E/K has good reduction, then $E_0(K) = E(K)$ and therefore $c(E/K) = 1$. However, when E/K has bad reduction, this is a hard question to answer in general. Fortunately, this question can always be resolved using Tate's Algorithm (see [Sil94, §IV.9]), and for semistable reduction, Tamagawa numbers have a simple explicit description.

Lemma 2.5. *Let E/K have multiplicative reduction, and let $n = \nu(\Delta)$ be the valuation of the minimal discriminant. Then*

$$c(E/K) = \begin{cases} n & \text{if } E/K \text{ has split reduction,} \\ 1 & \text{if } n \text{ is odd and } E/K \text{ is non-split,} \\ 2 & \text{if } n \text{ is even and } E/K \text{ is non-split.} \end{cases}$$

Elliptic curves with multiplicative reduction and $n = \nu(\Delta)$ are said to be of type I_n. The following notation is motivated by the above result and will be useful later on.

Notation 2.6. Let n be a positive integer. Let

$$\tilde{n} = \begin{cases} 1 \text{ if } n \text{ is odd,} \\ 2 \text{ if } n \text{ is even.} \end{cases}$$

The unstable case is harder, but there exists an explicit description for elliptic curves with equation $y^2 = x^3 + Ax + B$ and residual characteristic is at least 5.

Lemma 2.7. *Let $F/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let*

$$E : y^2 = x^3 + Ax + B$$

be an elliptic curve over K with additive reduction. Let $n = v_K(\Delta)$ be the valuation of the minimal discriminant, and e the ramification index of F/K.

If E has potentially good reduction, then

$$\begin{aligned}
\gcd(ne,12)=2 &\implies c(E/F)=1, && (II, II^*)\\
\gcd(ne,12)=3 &\implies c(E/F)=2, && (III, III^*)\\
\gcd(ne,12)=4 &\implies c(E/F)=\begin{cases}1, & \sqrt{B}\notin F\\ 3, & \sqrt{B}\in F\end{cases}, && (IV, IV^*)\\
\gcd(ne,12)=6 &\implies c(E/F)=\begin{cases}2, & \sqrt{\Delta}\notin F\\ 1 \text{ or } 4, & \sqrt{\Delta}\in F\end{cases}, && (I_0^*)\\
\gcd(ne,12)=12 &\implies c(E/F)=1. && (I_0)
\end{aligned}$$

Moreover, the extensions $F\left(\sqrt{B}\right)/F$ and $F\left(\sqrt{\Delta}\right)/F$ are unramified.

If E has potentially multiplicative reduction of type I_n^* over K, and e is odd, then it has Kodaira type I_{en}^* over F. Moreover,

$$\begin{aligned}
2\nmid n &\implies c(E/F)=\begin{cases}2, & \sqrt{B}\notin F,\\ 4, & \sqrt{B}\in F.\end{cases} && (I_{ne^*})\\
2\mid n &\implies c(E/F)=\begin{cases}2 & \sqrt{\Delta}\notin F,\\ 4 & \sqrt{\Delta}\in F\end{cases} && (I_{ne}^*)
\end{aligned}$$

Proof. [DD09, Lemma 3.22] □

2.3 Elliptic Curves over Global Fields

The topics we have discussed so far, such as the reduction type of an elliptic curve and the Tamagawa number, are intrinsically local objects. We now briefly discuss how we can associate these objects to global fields. For simplicity, assume that E is an elliptic curve over a number field K, let $\mathfrak{p}$ be a finite place of K and denote $K_{\mathfrak{p}}$ by the completion of K at $\mathfrak{p}$ with residue field $\kappa_{\mathfrak{p}}$. Clearly, we have that $E(K)\subseteq E(K_{\mathfrak{p}})$ and therefore we can apply the previous description to the curve $E/K_{\mathfrak{p}}$.

In particular, the reduction type of E/K at $\mathfrak{p}$ is the reduction type of $E/K_{\mathfrak{p}}$ and the Tamagawa number of E/K at $\mathfrak{p}$ is defined as

$$c_{\mathfrak{p}}(E/K) := c(E/K_{\mathfrak{p}}),$$

and we also define

$$c(E/K) := \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/K).$$

Finally, we say that a Weierstrass equation (1) is a **global minimal equation** if it is a minimal equation for all finite places $\mathfrak{p}$ of K. Even though such an equation does not always exists for any K, it does hold for $\mathbb{Q}$.

Proposition 2.8. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E has a global minimal Weierstrass equation.*

Throughout the document, we will work with elliptic curves over $\mathbb{Q}$, so unless stated otherwise we will assume the defining equation is global minimal.

3 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 $\bar{K}$ 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.

3.1 Artin Representations and ℓ-adic Representations

We begin by recalling the notion of an Artin representation.

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

Remark 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 $\rho : G_K \to \mathrm{GL}_n(\bar{\mathbb{Q}})$ 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 $L = L_1L_2$, then the natural maps $\rho_1 \oplus \rho_2 : G_K \to \mathrm{GL}_{n_1+n_2}(L)$ and $\rho_1 \otimes \rho_2 : G_K \to \mathrm{GL}_{n_1n_2}(L)$ 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.

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 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 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

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

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 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 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 3.7. 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 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

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

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

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

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

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

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

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

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

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 $F_n := K(E[\ell^n])$ 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,*

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

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 $\operatorname{Ind}_{L/K}\rho$ 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 3.4, 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 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. Some arithmetic terms present in the conjecture are easier to describe if the elliptic curve has a global minimial Weierstrass equation. Since we will be mainly interested in elliptic curves over $\mathbb{Q}$, and in view of Propostion 2.8, we will assume throughout that E is an elliptic curve over $\mathbb{Q}$ with **global minimal Weierstrass equation**

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

for some $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$, and let

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

be the associalted **global minimal differential**.

4.1 BSD and the Arithmetic Terms

The Birch-Swinnerton-Dyer conjecture states the following.

Conjecture 4.1 (BSD)**.** Let E be an elliptic curve defined 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

$$\lim_{s\to 1} \frac{L(E/K, s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_K|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}} = \frac{\operatorname{Reg}_{E/K} |Ш_{E/K}| C_{E/K}}{|E(K)_{\text{tors}}|^2}. \tag{4}$$

We briefly explore the arithmetic invariants that appear as part of the statement of BSD2. 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. Importantly, here we assume that E has rational coefficients.

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

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

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

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

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

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

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

where $c_{\mathfrak{p}}(E/K)$ are the Tamagawa numbers of E/K at a prime $\mathfrak{p}$ of K, as discussed in §2.2. To discuss the second term, 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 $\mathfrak{p}$ if $K_{\mathfrak{p}}/\mathbb{Q}_p$ is ramified, and we denote $\Delta_{E,\mathfrak{p}}^{\min}$ as the minimal discriminat of E/K at $\mathfrak{p}$.

   We remark that 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.

We will spend some time computing the local terms for families of elliptic curves, so we introduce some more notation that will be used throughout.

Notation 4.2. 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

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

and we also write

$$C_{\mathfrak{P}|\mathfrak{p}}(F/K) = T_{\mathfrak{P}|\mathfrak{p}}(F/K) D_{\mathfrak{P}|\mathfrak{p}}(F/K)$$

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 immediate consequence of this notation is the fact that

$$C_{E/F} = \prod_{\mathfrak{p}} C_{\mathfrak{P}|\mathfrak{p}}(F/K);$$

that is, we can calculate $C_{E/F}$ by calculating the contribution locally at each prime of K. Another 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 (4) is not arbitrary, and in fact we give specific notation to both sides of the equation.

Notation 4.3. Let $E/\mathbb{Q}$ be an elliptic curve and K a number field. We define

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

and

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

4.2 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 4.4. *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. *For $P, Q \in E(K)$, their Néron-Tate height pairings over K and F are related by $\langle P, Q \rangle_F = \langle P, Q \rangle_K$.*

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

3. *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 $n = \mathrm{ord}_{\mathfrak{p}} \Delta_{E,\mathfrak{p}}^{\min}$ 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).*

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

5. *If $E/K_{\mathfrak{P}}$ has potentially good reduction and the residue characteristic is not 2 or 3, then*

$$\left|\frac{\omega_{\mathfrak{p}}}{\omega_{\mathfrak{P}}}\right|_{\mathfrak{P}} = q^{\lfloor \frac{e_{F/K} \operatorname{ord}_{\mathfrak{p}} \Delta^{\min}_{E,\mathfrak{p}}}{12} \rfloor},$$

where q is the size of the residue field at $\mathfrak{P}$.

6. *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.*

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

4.3 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 4.5 (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

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

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 4.6. 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 4.7. [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 $\text{Ш}_{E/F}$ 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 $\mathrm{BSD}(E,\rho) = \text{sign } \omega_\rho$.

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 4.7 holds.

Theorem 4.8. *[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* $L(E,\rho,s)$*.*

5 Predicting Positive Rank

At this point, we aim to study the arithmetic applications of Conjecture 4.7. 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 4.7. 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 4.7 imply that

$$\frac{\prod_i \mathrm{BSD}(E/F_i)}{\prod_j \mathrm{BSD}(E/F'_j)} = \frac{\prod_i \mathrm{BSD}(E, \mathrm{Ind}_{F_i/\mathbb{Q}} \mathbb{1})}{\prod_j \mathrm{BSD}(E, \mathrm{Ind}_{F'_j/\mathbb{Q}} \mathbb{1})} = \left(\prod_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \mathrm{BSD}(E,\rho)^{\mathfrak{g}}\right)^m \tag{5}$$

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 (5) 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 5.1. *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 (5) 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 (5) are the product of local factors C_{E/F_i} and C_{E/F'_j}. We have therefore proven the following.

Theorem 5.2. *[DEW21, Theorem 33] Suppose Conjecture 4.7 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 4.2 will be useful.

Notation 5.3. Let F, ρ, m and the fields F_i, F'_j be as in Theorem 5.2. Let K be a subfield of F and $\mathfrak{p}$ a prime of K. Then we define

$$\mathrm{contr}_\rho(\mathfrak{p}) = \frac{\prod'_i C_{\mathfrak{p}|p}(F_i)}{\prod'_j C_{\mathfrak{p}|p}(F'_j)},$$

where the restricted product is taken over all F_i and F'_j containing K. 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.

I think at this point it would be nice to give some examples about when this test forces positive rank. In later sections we talk about when it's useless, so it's probably good to stress that there are plenty of times when it's not. On the other hand, in any examples we know the forced positive rank is also always described by root numbers. I don't know if we need to explain much about root numbers (or want to) but it might be worth mentioning that we haven't found an example where our norm relations force positive rank and root numbers don't explain it (and we don't know whether one exists).

Is there an example where root numbers force pos rank but our norm relations don't?

6 Consistency cases with BSD

As we discussed in the previous section, our motivation is to use Theorem 5.2 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 $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$.

6.1 Cyclic Extensions

In this subsection we prove the following.

Theorem 6.1. *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 6.1 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 6.2. *Let $E/\mathbb{Q}$, F and χ be as in Theorem 6.1. Writing characters of C_d additively, we have that*

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

Furthermore, such an expression is unique.

Add reference here from the exact result in the Rep Theory section.

Remark 6.3. 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 6.4. Let $E/\mathbb{Q}$, F and χ be as in Theorem 6.1, and let L_k and K be as in Remark 6.3. 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 4.2.

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 6.1 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. During the proof, we will also need the following result about quadratic subfields of cyclotomic extensions.

Lemma 6.5. *Let p be a rational prime, n a positive integer and let $p^* = (-1)^{(p-1)/2}p$. Then the quadratic subfields of $\mathbb{Q}(\zeta_{p^n})$ are*

- $\mathbb{Q}(\sqrt{p^*})$ *if p is odd,*
- $\mathbb{Q}(i)$ *if $p = n = 2$,*
- $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ *and* $\mathbb{Q}(\sqrt{-2})$ *if $p = 2$ and $n \geq 3$.*

Proof. If p is odd, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n\mathbb{Z})^* = C_{p^{n-1}(p-1)}$ is a cyclic group of even order, and therefore $\mathbb{Q}(\zeta_{p^n})$ has one unique quadratic subfield. Hence, it suffices to find the unique quadratic subfield of $\mathbb{Q}(\zeta_p)$. Two proofs:

1. 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 $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$ as desired.

2. Let $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_{p^n})$ be a quadratic subfield. The extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ only ramifies at p and therefore $\mathbb{Q}(\sqrt{D})$ can only (in fact, it must) ramify at p. If $p \equiv 1 \pmod 4$, then the only such field is $\mathbb{Q}(\sqrt{p})$ and if $p \equiv 3 \pmod 4$, then the field is $\mathbb{Q}(\sqrt{-p})$.

If $p = n = 2$, then $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ so there is nothing to prove. If $p = 2$ and $n \geq 3$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}) = (\mathbb{Z}/2^n\mathbb{Z})^* = C_2 \times C_2^{n-2}$ and therefore $\mathbb{Q}(\zeta_{2^n})$ has three quadratic subfields, and therefore it is enough to find the quadratic subfields of $\mathbb{Q}(\zeta_8)$. Since $\zeta_8 = (1+i)/\sqrt{2}$, it is clear that the quadratic subfields are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ as desired.

□

Odd Cyclic Extensions

For the first case, we assume that d is odd. Following the observation in Remark 6.3, 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 6.6. *Let q be an odd rational prime, F/K a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_q$ and $E/\mathbb{Q}$ an elliptic curve with semistable reduction at 2 and 3. Then*

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

is a norm from $\mathbb{Q}(\sqrt{q^*})$.

Proof. Fix some prime $\mathfrak{p}$ in K and note that since the extension L/K is cyclic, the splitting behaviour of $\mathfrak{p}$ in L is determined by the ramification index $e_\mathfrak{p}$ and the residual degree $f_\mathfrak{p}$. Since $\mathrm{contr}_\chi(\mathfrak{p}) = 1$ if E has good reduction at $\mathfrak{p}$, we assume that E bad reduction at $\mathfrak{p}$. If $\mathfrak{p}$ has multiplicative reduction, then $D_{\mathfrak{P}|\mathfrak{p}}(F/K) = 1$ and the following table records the contribution of the Tamagawa numbers of $\mathfrak{p}$ depending 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 ";". To complete these calculations, we use repeatedly Proposition 2.3 and Lemmas 2.5 and 2.7. We also use Notation 2.6.

$e_\mathfrak{p}$	$f_\mathfrak{p}$	$T_{\mathfrak{P}\vert\mathfrak{p}}(K/K)$	$T_{\mathfrak{P}\vert\mathfrak{p}}(F/K)$	$\mathrm{contr}_\chi(\mathfrak{p})$
1	1	$n; \tilde{n}$	$n^q; \tilde{n}^q$	$\square$
q	1	$n; \tilde{n}$	$qn; \tilde{n}$	$q\square; \square$
1	q	$n; \tilde{n}$	$n; \tilde{n}$	$\square$

Since q is indeed a norm from $\mathbb{Q}(\sqrt{q^*})$ by Lemma A.13, it follows that $\mathrm{contr}_\chi(\mathfrak{p})$ is a norm from $\mathbb{Q}(\sqrt{q^*})$ as well.

Now assume $\mathfrak{p}$ has additive reduction, and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. By assumption, $p \neq 2, 3$. Firstly, we note that $D_{\mathfrak{P}|\mathfrak{p}}(F/K) = 1$ unless $\mathfrak{p}$ ramifies in F/K, and in that case it is a power of $N_{K/\mathbb{Q}}(\mathfrak{p}) = p^s$. If s is even, we are immediately done, so assume instead that s is odd. If $L_\mathfrak{P}/K_\mathfrak{p}$ is wildly ramified, then $p = q$ is a norm from $\mathbb{Q}(\sqrt{q^*})$. If $L_\mathfrak{P}/K_\mathfrak{p}$ is tamely ramified, then by Lemma **Add here reference of Lemma for tame totally ramified extensions**, it follows that $q \mid p^r - 1$ and therefore

$$\left(\frac{q^*}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{p^s}{q}\right) = 1 \tag{8}$$

Therefore, p splits in $\mathbb{Q}(\sqrt{q^*})$ and by Lemma **insert relevant thm here**, it follows that p is a norm from $\mathbb{Q}(\sqrt{q^*})$.

The proof follows immediately from (7). $\square$

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

Lemma 6.7. *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 with semistable reduction at 2 and 3 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 6.6 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	$n;\tilde{n}$	$pn;\tilde{n}$	$n^q;\tilde{n}^q$	$p^qn^q;\tilde{n}^q$	$\square$
p	q	$n;\tilde{n}$	$pn;\tilde{n}$	$n;\tilde{n}$	$pn;\tilde{n}$	$\square$
q	1	$n;\tilde{n}$	$n^p;\tilde{n}^p$	$qn;\tilde{n}$	$q^pn^p;\tilde{n}^p$	$\square$
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 6.1 will follow.

Lemma 6.8. *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*

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

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 6.7. Assume that the result holds for squarefree cyclic Galois extensions 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 $L_{d/p_n}/K$, while the fields in $\mathscr{B}$ are the intermediate fields of F/L_{p_n}. 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 $L_{d/p_n}/K$ and F/L_{p_n} respectively that

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

are both rational squares. By the natural decomposition

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

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

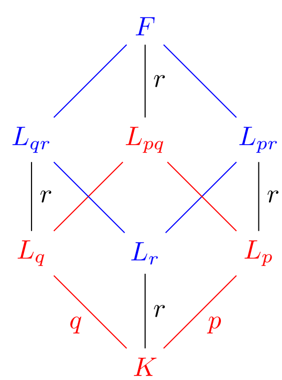

Figure 2: Partition of $n = 3$ into $n = 2$. Red fields are in $\mathscr{A}$ while blue fields are in $\mathscr{B}$.

We are now ready to prove Theorem 6.1 for odd d.

Theorem 6.1 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 6.3

and Lemma 6.8 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 6.2 and Lemma 6.6 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.13, and so the Theorem follows. □

Even Cyclic Extensions

A bit more care is required to prove Theorem 6.1 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 6.9. *Let p be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{2p}$ 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 6.6 and 6.7 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.

The result follows again from (7).

□

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 6.10. *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.

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

Proof. All fields appearing in the product are intermediate fields of L_2 and F, and $\mathrm{Gal}(F/L_2) = C_{2p}$. Lemma 6.9 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.

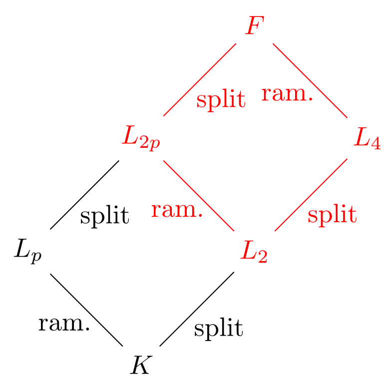

Figure 3: Field diagram for a C_{4p} extension, together with the splitting behaviour of a prime $\mathfrak{p}$ in L_2 with $e_{\mathfrak{p}} = p$ and $f_{\mathfrak{p}} = 1$ over F.

$\square$

We are now ready to prove Theorem 6.1 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 6.6, 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^l})/\mathbb{Q}) = (\mathbb{Z}/2^l\mathbb{Z})^* = C_{2^{l-2}} \times C_2$

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 6.3 such that $\mathrm{Gal}(F/K) = C_{\mathrm{rad}(d)}$ and all fields appearing in the product of local factors contain K. Then using the same idea as in Lemma 6.8, 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 fields in $\mathscr{A}$ and $\mathscr{B}$ are the intermediate fields of (distinct!) $C_{\mathrm{rad}(d)/2}$ extensions. These are odd cyclic extensions, and therefore by Lemma 6.8 the contribution is a rational square and therefore a norm from any quadratic extension.

Case 3: d is divisible by one odd prime

In this case, write $d = 2^l p^n$ and let L_k be the fields as above. In this case, we note that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} = \frac{C_{E/F} C_{E/L_{d/2p}}}{C_{E/L_{d/2}} C_{E/L_{d/p}}}.$$

By Lemma 6.6, we know that this product is a square up to multiples of p. If $l = 1$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{2p^n})/\mathbb{Q}) = (\mathbb{Z}/2p^n\mathbb{Z})^* = (\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic, and therefore the unique quadratic subfield is $\mathbb{Q}(\sqrt{p^*})$, and we already know that p is a norm of this field.

From Lemma 6.9 that the contribution of p comes from those primes $\mathfrak{p}$ in $L_{d/2p}$ such that they ramify in $L_{d/2}$ and they split in $L_{d/p}$. However, as in the proof of Lemma 6.10, the prime $\bar{\mathfrak{p}} = \mathfrak{p} \cap L_{d/4p}$ must also split in $L_{d/2p}$ so $\bar{\mathfrak{p}} = \mathfrak{p}\mathfrak{p}'$ for $\mathfrak{p}' \neq \mathfrak{p}$ in $L_{d/2p}$. Since $\mathfrak{p}$ and $\mathfrak{p}'$ have the same splitting behaviour, they give the same contribution. Hence, the product of local terms is in fact a rational square and therefore the norm of any quadratic extension.

This concludes the proof of Theorem 6.1, and we have in addition shown that the contribution is always a square except when $d = 2^n, p^n$ or $2p^n$, where p is an odd rational prime. $\square$

6.2 Abelian Extensions

6.3 Odd-Degree Extensions

6.4 Norm relations in odd order extensions

add some motivation (justification) for why I'm proving this result. The point is that the test for positive rank provided by root number computations never says anything in odd order extensions. If we expect the norm relations test to be weaker than root numbers, then nor should this test.

Theorem 6.11. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ 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). Take any representation $\rho \in R(G)$ with quadratic subfield $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\rho)$ and relation

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

as in theorem 5.2. Then

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} \in \begin{cases} N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\mathbb{Q}(\sqrt{D})^\times) & m \text{ odd,} \\ \mathbb{Q}^{\times 2} & m \text{ even.} \end{cases}$$

In other words, one cannot use theorem 5.2 to conclude that E/F must have positive rank.

Let us break up the function $C\colon H \mapsto C_{E/F^H}$ into $C = \prod_p \mathfrak{c}_p \cdot d_p$ where

$$\mathfrak{c}_p(H) = \prod_{v|p} c_v(E/F^H), \qquad d_p(H) = \prod_{v|p} \left|\frac{\omega}{\omega_v^{\min}}\right|_v, \tag{9}$$

the product ranging over all finite places of F^H dividing p. Observe that $\mathfrak{c}_p$ and d_p are D_p-local functions. Recall the notation that for a number field K and place v, $C_v(E/K) = c_v(E/K) \cdot \left|\omega/\omega_v^{\min}\right|_v$. Then

$$\mathfrak{c}_p \cdot d_p = (D_p, f_p) \tag{10}$$

where f_p is a function on $B(D_p)$ with $D_p \cap H^{x^{-1}} \mapsto C_v(E/F^H)$ when HxD_p is a double coset representative corresponding to the place v of F^H. say this better. write D_p as a local Galois group and say more generally how this fn is defined

We first argue that it is enough to prove this theorem when m is the order of $\widetilde{\rho}$ in $C(G)$.

Lemma 6.12. *Consider the set-up as in theorem 6.11. If the statement of the theorem holds when m is the order of $\widetilde{\rho}$ in $C(G)$, then it holds for all possible m. really, this is saying that if f is trivial on Brauer relations, then showing it is trivial on rho-relations for minimum m is enough (maybe I could add that in rep theory section)*

Proof. By definition, if m is the order of $\widetilde{\rho}$ in $C(G)$ then there exists $\Theta \in B(G)$ such that $\mathbb{C}[\Theta] \simeq \widetilde{\rho}^{\oplus m}$. Now consider n and $\Psi \in B(G)$ such that $\mathbb{C}[\Psi] \simeq \widetilde{\rho}^{\oplus n}$. Clearly $m \mid n$. Then $\Phi = \Psi - \frac{n}{m}\Theta$ is a Brauer relation.

At this point, we use that the function C on $B(G)$, viewed as a function to $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, is trivial on Brauer relations. For odd order groups this follows from [DD09, Theorem 2.47] and [DD09, Theorem 3.2 (Tam)], looking locally at each C_p. Then $C(\Psi) = C(\Theta)^{n/m} \cdot C(\Phi)$ so $C(\Psi) \equiv C(\Theta)^{n/m} \mod \mathbb{Q}^{\times 2}$. It follows that if $C(\Theta)$ satisfies the conditions of theorem 6.11, then so does $C(\Psi)$. ∎

Taking m to be the order of $\widetilde{\rho}$ in $C(G)$, we have that m divides $|G|$, hence is odd. Therefore we need to prove that, given any $\Theta \in B(G)$ such that $\mathbb{C}[\Theta] \simeq \widetilde{\rho}^{\oplus m}$, the expression $C(\Theta)$ is the norm of an element from $\mathbb{Q}(\sqrt{D})^\times$. Replacing ρ by the sum of its conjugates by elements of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{D}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{D})$. Note that this does not affect m.

We record

τ the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$,

k the smallest integer such that $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_k)$. Then $k \mid |G|$, hence is odd.

Fix $\Theta = \sum_i n_i H_i \in B(G)$ with $\mathbb{C}[\Theta] \simeq \widetilde{\rho}^{\oplus m}$. We prove that at each prime p, $\mathfrak{c}_p(\Theta)$ and $d_p(\Theta)$ are the norms of elements from $\mathbb{Q}(\rho)^\times$. These depends on D_p and I_p ; the decomposition and inertia group respectively at p. As we deal with each local factor individually, we argue that one can take $D_p = I_p$.

Lemma 6.13. *Let E/K be an elliptic curve. Let K'/K be an extension of number fields odd degree, unramified at the place v of K. Then $C_w(E/K') \equiv C_v(E/K) \mod \mathbb{Q}^{\times 2}$ for any place w of K' with $w \mid v$.*

Proof. This is automatic for good reduction and split multiplicative reduction. It is also clear for non-split multiplicative reduction since the residue degree cannot be even (so the reduction type remains non-split at w). For additive reduction, see [DD09, Lemma 3.12]. □

Lemma 6.14. *At a prime p, we may assume that $D_p = I_p$ when computing $(\mathfrak{c}_p \cdot d_p)(\Theta)$.*

Proof. Let p have residue degree f_p. Let $L/\mathbb{Q}$ be a Galois extension of degree f_p with cyclic Galois group, such that p is inert in L. Further ensure that $F \cap L = \mathbb{Q}$. Then $\mathrm{Gal}(FL/L) = G$. Let $F_i = F^{H_i}$ and $L_i = F_i L$.

Let v be a place over p in F_i. The extension L_i/F_i is Galois, so v is either split or inert in L_i. We claim that $C_v(E/F_i) \equiv \prod_{w|v} C_w(E/L_i) \mod \mathbb{Q}^{\times 2}$. Indeed, the number of terms in the product on the right is odd, and by lemma 6.13 $C_v(E/F_i) \equiv C_w(E/L_i) \mod \mathbb{Q}^{\times 2}$. Letting $\mathfrak{c}'_p$ and d'_p be functions on $B(G)$ defined as in (9) but with $\mathbb{Q}$, F replaced by L, FL, we see that $(\mathfrak{c}_p \cdot d_p)(\Theta) \equiv (\mathfrak{c}'_p \cdot d'_p)(\Theta) \mod \mathbb{Q}^{\times 2}$. Thus it is equivalent to do our computation in FL/L, but here p has residue degree 1. □

We also show that if $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) = \mathbb{Q}$, then $(\mathfrak{c}_p \cdot d_p)(\Theta) \in \mathbb{Q}^\times$.

Lemma 6.15. *Let the exponent of D_p be b. If $k \nmid b$, then $(\mathfrak{c}_p \cdot d_p)(\Theta) \in \mathbb{Q}^\times$.*

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 $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b) \implies k \mid b$ by minimality of k. Since $k \nmid b$, we have $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_b)$, so $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) = \mathbb{Q}$ and $\mathrm{Res}_{D_p} \rho = \tau(\mathrm{Res}_{D_p} \rho)$.

Now $\mathbb{C}[\mathrm{Res}_{D_p} \Theta] \simeq (\mathrm{Res}_{D_p} \rho)^{\oplus 2m} \in \mathrm{Perm}(D_p)$. Since $C(D_p) = \mathrm{Char}_{\mathbb{Q}}(D_p)/\mathrm{Perm}(D_p)$ has odd order, it follows that $(\mathrm{Res}_{D_p} \rho)^{\oplus m} \in \mathrm{Perm}(D_p)$. Therefore there is $\Theta' \in B(D_p)$ such that $\mathbb{C}[\Theta'] \simeq (\mathrm{Res}_{D_p} \rho)^{\oplus m}$. Then $\Psi = (\mathrm{Res}_{D_p} \Theta) - 2\Theta'$ is a Brauer relation for D_p. Then

$$(\mathfrak{c}_p \cdot d_p)(\Theta) \overset{(10)}{=} f_p(\mathrm{Res}_{D_p} \Theta) = f_p(\Psi) \cdot f_p(\Theta')^2 \in \mathbb{Q}^{\times 2}.$$

Again we are using [DD09, Theorem 2.47] and [DD09, Theorem 3.2] which imply that $f_p(\Psi) \in \mathbb{Q}^{\times 2}$ when Ψ is a Brauer relation for D_p (since D_p is odd). □

To prove theorem 6.11, we proceed by considering separately each reduction type.

Good reduction

If $E/\mathbb{Q}$ has good reduction at p,it has good reduction at all primes lying above p in subfields of F. Hence the Tamagawa number is always one, as well as $\left|\omega/\omega_v^{\min}\right|_v$ for any place $v \mid p$ in an intermediate field. Therefore $\mathfrak{c}_p$, $d_p = 1$ as functions on $B(G)$.

Multiplicative reduction

If $E/\mathbb{Q}_p$ has multiplicative reduction, then as in the good reduction case one has $\left|\omega/\omega_v^{\min}\right|_v = 1$ for any place $v \mid p$ in an intermediate field. Thus $d_p = 1$. For $\mathfrak{c}_p$, we consider non-split/split reduction separately.

Non-split multiplicative reduction

Let $E/\mathbb{Q}_p$ have non-split multiplicative reduction. Since $D_p = I_p$, all primes above p have residue degree 1. Then the reduction at places above p remains non-split in all intermediate subfields. It follows that

$$\mathfrak{c}_p = (D_p, \alpha)$$

where α is the constant function on $B(D_p)$ with $\alpha \in \{1, 2\}$, depending on $\mathrm{ord}_p(\Delta)$ being even or odd. We prove a more general lemma that D_p-local constant functions are trivial on ρ-relations.

Lemma 6.16. *Let G, ρ be as above. The function (D_p, α) for $\alpha \in \mathbb{Q}^\times$ satisfies $(D_p, \alpha)(\Theta) \in \mathbb{Q}^\times$.*

Proof. The function (D_p, α) on $B(G)$ sends $H \leq G$ to $\alpha^{|H\backslash G/D_p|}$. Thus if $\Theta = \sum_i n_i H_i$ is a ρ-relation, $(D_p, \alpha)(\Theta) = \alpha^{\sum_i n_i \cdot |H_i\backslash G/D_p|}$. We show that $\sum_i n_i \cdot |H_i\backslash G/D_p|$ is even.

One has $\mathrm{Res}_{D_p} \Theta = \sum_i n_i \sum_{x \in H_i\backslash G/D_p} D_p \cap H^{x^{-1}}$ and the permutation representation $\mathbb{C}[\mathrm{Res}_{D_p} \Theta]$ of D_p is isomorphic to $\mathrm{Res}_{D_p}(\rho^{\oplus m} \oplus \tau(\rho^{\oplus m}))$. In particular the dimension is even. The dimension is

$$\sum_i n_i \sum_{x \in H_i\backslash G/D_p} [D_p \colon D_p \cap H^{x^{-1}}].$$

Since each $[D_p \colon D_p \cap H^{x^{-1}}]$ 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 $E/\mathbb{Q}_p$ has split multiplicative reduction. The reduction type remains split at all places above p within sub-extensions of $F/\mathbb{Q}$. Let $\mathrm{ord}_p(\Delta) = n$. Then

$$\mathfrak{c}_p = (D_p, D_p, en).$$

Since the n factor is constant, $(D_p, D_p, en)(\Theta) \equiv (D_p, D_p, e)(\Theta) \mod \mathbb{Q}^{\times 2}$ by lemma 6.16 .

We have $D_p = I_p = P_p \ltimes C_l$, where $P_p \triangleleft I_p$ 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 lemma 6.15, it is only of interest to consider such D_p with exponent $p^u l$ for some $u \geq 0$ such that $k \mid p^u l$.

Now, $(D_p, I_p, e)(\Theta)$ is the product of ramification indices at primes above p. We separate 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 $e_w = \frac{|I_p|}{|H_i \cap I_p^x|} = \frac{|I_p|}{|I_p \cap H^{x^{-1}}|}$. This is the dimension of the permutation representation $\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]$. Let $D_p \cap H^{x^{-1}} = P' \ltimes C_a$ where $P' \leq P$ and $a|l$. Then the ramification index is $\frac{|P|}{|P'|} \cdot \frac{l}{a}$.

Taking fixed points under wild inertia, one has

$$\mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p} \simeq \mathbb{C}[D_p/P_p(D_p \cap H^{x^{-1}})] \simeq \mathbb{C}[D_p/P_p \ltimes C_a].$$

This permutation representation has dimension $\frac{l}{a}$, so we've killed off the p-part. Then

$$\mathbb{C}[\operatorname{Res}_{D_p} \Theta]^{P_p} \simeq \left(\operatorname{Res}_{D_p} \rho^{\oplus m} \oplus \tau\left(\operatorname{Res}_{D_p} \rho^{\oplus m}\right)\right)^{P_p},$$

and we can consider these as representations of $D_p/I_p = C_l$.

Consider the function g on $B(C_l)$ with $H \mapsto [C_l \colon H] = \dim \mathbb{C}[C_l/H]$. It follows that $(D_p, D_p, e)(\Theta)$ differs from $g(P_p \cdot \operatorname{Res}_{D_p} \Theta/P_p)$ up to a factor of p.

Crucially, this factor of p doesn't matter:

Lemma 6.17. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field, contained in the minimal cyclotomic field $\mathbb{Q}(\zeta_k)$ with k odd. Let $k \mid p^u l$, 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 k is odd, it is clear that $D = \prod_{q|k} q^*$, the product being taken over primes dividing k. Note that if $q \neq p$, then since $q \mid l$, we have $p \equiv 1 \pmod{l} \implies p \equiv 1 \pmod{q}$. By theorem A.8, p is the norm of a principal fractional ideal of K. If K is imaginary, then p is the norm of an element of K. Else, we invoke theorem A.10 or theorem A.11. □

Thus, we only need to worry about the tame part of our ramification indices. If $k \nmid l$, then $\phi = (\operatorname{Res}_{D_p} \rho)^{P_p}$ (viewed as a representation on D_p/P_p) has rational character. Therefore, arguing as in lemma 6.15, $g(P_p \cdot \operatorname{Res}_{D_p} \Theta/P_p) \in \mathbb{Q}^{\times 2}$ say more?. Therefore we may assume that $k \mid l$ and that $\mathbb{Q}(\phi) = \mathbb{Q}(\rho) = K$.

Proposition 6.18. *Let $k \mid l$. Then $g(P_p \cdot \operatorname{Res}_{D_p} \Theta/P_p) \in N_{K/\mathbb{Q}}(K^\times)$.*

Proof. Let $\Psi = P_p \cdot \operatorname{Res}_{D_p} \Theta/P_p$, so that $\phi^{\oplus m} \oplus \tau(\phi^{\oplus m}) = \mathbb{C}[\Psi] = \sum_{l'|l} a_{l'} \chi_{l'}$ where $a_{l'} \in \mathbb{Z}$ and $\chi_{l'}$ are defined in example 1.7. Let $\Psi_{l'} = \sum_{l''|l'} \mu(l'/l'') \cdot C_{l/l''}$ so that $\mathbb{C}[\Psi_{l'}] = \chi_{l'}$, as observed in the example. Then $\mathbb{C}[\Psi] \simeq \mathbb{C}[\sum_{l'|l} a_{l'} \Psi_{l'}]$ which implies that $\Psi = \sum_{l'|l} a_{l'} \Psi_{l'}$ since cyclic groups have no Brauer relations.

Evaluating g on $\Psi_{l'}$ is trivial unless $l' = q^a$ for some q prime, $a \geq 1$. Indeed, if $l' = p_1^{e_1} \cdots p_r^{e_r}$, with $r \geq 2$ and $e_i \geq 1$, then

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

On the other hand,

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

We claim that $k \nmid l'$ implies $a_{l'}$ 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 $\chi_{l'} = \widetilde{\varphi_{l'}}$ where $\mathbb{Q}(\varphi_{l'}) = \mathbb{Q}(\zeta_{l'})$. If $k \nmid l'$ then $\mathbb{Q}(\phi) \not\subset \mathbb{Q}(\zeta_{l'})$, so that $B = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q}(\zeta_{l'})) \not\leq H$. Then $\mathbb{Q}(\phi) \cap \mathbb{Q}(\zeta_{l'}) = \mathbb{Q}$ so $BH = \mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q})$. The orbit of $\varphi_{l'}$ under H is fixed by BH, hence is rational. It follows that $\langle \phi, \varphi_{l'} \rangle = \langle \tau(\phi), \varphi_{l'} \rangle$ so that $a_{l'}$ is even.

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

Additive reduction

Now suppose that $E/\mathbb{Q}_p$ has additive reduction. 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 $l \mid p-1$. Once again we may assume that $k \mid l$ by lemma 6.15.

Let $\delta = \mathrm{ord}_p(\Delta_E)$. Consider a place w of F^H over p with ramification degree $e_w$over $\mathbb{Q}$. Then Δ_E has valuation ne_w with respect to w. Then $\left|\Delta_E/\Delta_{E,w}^{\min}\right|_w = p^{-(\delta \cdot e_w - \delta_H)}$, where $\delta_H = \mathrm{ord}_w(\Delta_{E,w}^{\min})$. Recall that

$$\left|\frac{\omega}{\omega_w^{\min}}\right|_w^{-12} = \left|\frac{\Delta_E}{\Delta_{E,w}^{\min}}\right|_w.$$

Therefore $\left|\omega/\omega_w^{\min}\right|_w = p^{\lfloor \frac{\delta \cdot e_w - \delta_H}{12} \rfloor}$.

Suppose that $E/\mathbb{Q}_p$ has Kodaira type I_n^*, so $\delta = 6+n$. For a finite extension $K'/\mathbb{Q}_p$ with ramification degree e, E/K' has Kodaira type I_{en}^* if e is odd, and type I_{en} if n is even. Thus in odd degree extensions the reduction type will stay potentially multiplicative. Then $\delta \cdot e_w - \delta_H = 6e_w$.

If $E/\mathbb{Q}_p$ has potentially good reduction then $\delta \in \{2, 3, 4, 6, 8, 9, 10\}$. E also has potentially good reduction at the place w in F^H. It follows that $\delta_H = \delta \cdot e_w - 12 \cdot \lfloor \delta \cdot e_w / 12 \rfloor$.

In conclusion,

$$d_p = \begin{cases} (D_p, D_p,\ p^{\lfloor e_w/2 \rfloor}) & \text{if } E \text{ has potentially multiplicative reduction,} \\ (D_p, D_p,\ p^{\lfloor \delta \cdot e_w/12 \rfloor}) & \text{if } E \text{ has potentially good reduction.} \end{cases}$$

In either case, $d_p(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. Indeed, this takes values 1 or p in $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. But $p \equiv 1 \pmod{l}$ implies $p \equiv 1 \pmod{k}$ so 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.10.

For the Tamagawa number computations we use the following description

Lemma 6.19. *Let $K'/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let E/K be an elliptic curve with additive 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

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

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

If E has potentially multiplicative reduction of type I_n^* over K, and e is odd, then it has Kodaira type I_{en}^* over K'. Moreover,

$$\begin{aligned}
&2 \nmid n && \Longrightarrow && c_v(E/K') = \begin{cases} 2, & \sqrt{B} \notin K', \\ 4, & \sqrt{B} \in K'. \end{cases} && (I_{ne^*}) \\
&2 \mid n && \Longrightarrow && c_v(E/K') = \begin{cases} 2 & \sqrt{\Delta} \notin K', \\ 4 & \sqrt{\Delta} \in K' \end{cases} && (I_{ne}^*)
\end{aligned}$$

Potentially multiplicative reduction

TO DO

Potentially good reduction

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

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')}. \tag{11}$$

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 constant across 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 separately:

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 (11).

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,

$$\prod_{d' \mid d} C(E/F_{\mathfrak{p}}^{D_{d'}})^{\mu(d/d')} = \begin{cases} 1 & 3 \nmid d, \\ 1 & 3 \mid d, \delta \in \{0,3,6,9\}, \\ 1 \cdot \square & 3 \mid d, \delta \in \{2,10\}, \\ 3^a \cdot \square, a \in \{0,1\} & 3 \mid d, \delta \in \{4,8\}. \end{cases} \tag{12}$$

Remark 6.20. 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 occurring 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 (11) can only be non-square when $d = 3$. then conclude why this is fine

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 properties that will be useful for us.

Let K be a number field. The **ideal class group** $\mathrm{Cl}_K = I_K/P_K$ is the group of fractional ideals quotiened? 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 $\mathrm{Cl}_K^+ = I_K/P_K^+$, 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 unramified 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. *[Jan96, Chapter VI, Section 3, Theorem 3.1] 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 $[H^+ \colon H] = 1$ 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. *[Jan96, Chapter VI, Section 3, Theorem 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. □

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 $p_2, \dots p_t$ are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is*

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

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 p be a prime in $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{D})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$, where all p_i are odd primes. If $p \equiv 1 \mod |\Delta|$, then p is the norm of a fractional principal ideal in K. It is also the norm of a fractional principal ideal in $K' = \mathbb{Q}(\sqrt{pD})$.*

Proof. Any prime above p in K splits in E^+, hence also in E (in particular it has residue degree 1). Similarly for K', the residue degree of p in its extended genus field is 1, and so in its genus field also. □

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 $K = \mathbb{Q}(\sqrt{D})$ and suppose that all odd primes dividing D are congruent to $1 \pmod 4$. Then -1 is the norm of an element of $K^\times$.*

Proof. write. □

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.

The following two results are needed in the body of this report.

Theorem A.10. *Let $K = \mathbb{Q}(\sqrt{D})$ and let k be the minimal cyclotomic field such that $K \subset \mathbb{Q}(\zeta_k)$. Suppose that k is odd and K is real. If p is a prime such that $p \equiv 1 \pmod{|\Delta|}$, then p is the norm of an element from K.*

Proof. Note that k being odd implies D is odd. We know that p is the norm of a principal fractional ideal of K by corollary A.8. Therefore there exists integers x, y, z such that $\pm pz^2 = x^2 - Dy^2$. Suppose firstly that all primes dividing D are congruent to $1 \pmod 4$. Then there is an element of $K^\times$ of norm -1 by theorem A.9. Hence we can find an element of norm p.

Otherwise, there exists a prime $q \mid D$ such that $q \equiv 3 \pmod 4$. Reducing mod q, we have $\pm p = \square$. Since $p \equiv 1 \pmod q$, it is a square $\pmod q$. But -1 is not a square mod q, hence our sign must have been $+$ and so p is the norm of an element from $K^\times$. $\square$

Theorem A.11. *Let $K = \mathbb{Q}(\sqrt{D})$ and let k be the minimal cyclotomic field such that $K \subset \mathbb{Q}(\zeta_k)$. Suppose that k is odd and K is real. Let p be a prime such that $p \mid D$ and $p \equiv 1 \pmod q$ for all other primes $q \mid D$. Then p is the norm of an element from K.*

Proof. By corollary A.8, we know that p is the norm of a principal fractional ideal of K. The rest of the argument is analogous to the previous proof. $\square$

Proposition A.12. *$\mathbb{Q}(\sqrt{p^*})$ has odd narrow class number.*

Corollary A.13. *The prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

References

[BD16] Alex Bartel and Tim Dokchitser, *Rational representations and permutation representations of finite groups*, Math. Ann. **364** (2016), no. 1-2, 539–558. MR 3451397

[DD09] Tim Dokchitser and Vladimir Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71. MR 2534092

[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.

[Jan96] Gerald J. Janusz, *Algebraic number fields*, second ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR 1362545

[Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, french ed., Graduate Texts in Mathematics, vol. Vol. 42, Springer-Verlag, New York-Heidelberg, 1977. MR 450380

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Springer, 1994.

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