A Study of the Arithmetic Consequences of Artin Formalism for Predicting Positive Rank

Edwina Aylward, Albert Lopez Bruch

June 27, 2024

Abstract

In this report we explore the arithmetic applications of Norm Relations tests; a new test introduced in [DEW21] that can force families of elliptic curves over $\mathbb{Q}$ to have positive rank over Galois extensions, based solely on local data. In particular, we prove that one cannot use this test to force positive rank when the extension is cyclic or has odd degree. We also include a survey of relevant topics associated to this test, as well as examples where we use this test to predict rank growth.

Contents

1 Introduction

The Birch–Swinnerton-Dyer conjecture is one the most important and celebrated statements in classical algebraic number theory, and has been driving large amounts of current research in the area. The statement conjecturally provides a bridge between the arithmetic of elliptic curves, or abelian varieties more generally, and the properties of their associated L-functions, a (conjecturally) meromorphic function in the complex plane, and therefore an analytic object in nature. This connection between arithmetic and analytic objects is ubiquitous throughout pure mathematics, and it has remarkable and surprising consequences, many of which are deep and non-trivial. The BSD conjecture for elliptic curves establishes the following connection.

Conjecture 1.1 (BSD Conjecture)**.** Let E be an elliptic curve over a number field F, and let $L(E/F,s)$ be the associated L-function. Then

$$\operatorname{ord}_{s=1} L(E/F,s) = \operatorname{rk} E/F, \tag{BSD1}$$

and the leading term of the Taylor series at $s=1$ of $L(E/F,s)$ is given by

$$\lim_{s\to 1} \frac{L(E/F,s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_F|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}} = \frac{\operatorname{Reg}_{E/F}|Ш_{E/F}|C_{E/F}}{|E(F)_{\mathrm{tors}}|^2}, \tag{BSD2}$$

where r is the order of the zero of $L(E/F,s)$ at $s=1$, (r_1,r_2) is the signature of F, $\Omega_\pm$ are the periods of E, $\operatorname{Reg}_{E/F}$ is the regulator, $Ш_{E/F}$ is the Tate-Shafarevich group and $C_{E/F}$ is a product of local terms depending on the primes in F of bad reduction over E (see Section 4).

In this document, we investigate the arithmetic consequences of the factorization of L-functions of elliptic curves over number fields, commonly known as Artin formalism. Dokchitser, Evans and Wiersema in [DEW21] have already studied some of these and, in particular, they constructed a test that predicts positive rank for families of elliptic curves, which is only dependent on certain local arithmetic data associated to the primes of bad reduction of the elliptic curve. The existence of such tests, which we call 'Norm Relations tests', is encoded in the following statement.

Conjecture 1.2. [DEW21, Theorem 33] Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a finite Galois extension with Galois group G, ρ an Artin representation over $\mathbb{Q}$ that factors through G and

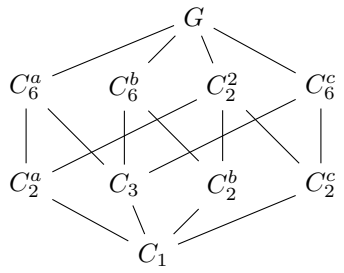
$$\left(\bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}\right)^{\oplus m} = \bigoplus_i \operatorname{Ind}_{F_i/\mathbb{Q}} \mathbb{1} \ominus \bigoplus_j \operatorname{Ind}_{F'_j/\mathbb{Q}} \mathbb{1} \tag{†}$$

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.

In the above conjecture, $\mathbb{Q}(\rho)$ is the field obtained by attaching $\{\mathrm{Tr}(\rho(\mathfrak{g})) : \mathfrak{g} \in \mathrm{Gal}(K/\mathbb{Q})\}$, which is a Galois abelian extension of $\mathbb{Q}$, and $\rho^{\mathfrak{g}}$ is the representation with character given by $\mathrm{Tr}\circ\rho^{\mathfrak{g}} = (\mathrm{Tr}\circ\rho)^{\mathfrak{g}}$ for $\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$, denoted as the twist of ρ by $\mathfrak{g}$.

Let us briefly describe an example where Conjecture 1.2 indeed predicts positive rank. We revisit this example in detail in Section 5.3.

Example 1.3 (Example 5.14)**.** Let $F/\mathbb{Q}$ be a finite Galois extension such that $\mathrm{Gal}(F/\mathbb{Q}) = C_2 \times C_6$, which has the following subfield diagram.



Let $E/\mathbb{Q}$ be an elliptic curve such that it has multiplicative reduction at a prime p with decomposition group G and inertia group C_6^b and such that every other prime of bad reduction is unramified in $F/\mathbb{Q}$. If ρ is an order 6 character of G with kernel C_2^a, then $\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Following Conjecture 1.2, we aim to compute

$$\left(\frac{C_{E/F^{C_2^a}} C_{E/\mathbb{Q}}}{C_{E/F^{C_6^a}} C_{E/F^{C_2^2}}}\right) \cdot \left(\frac{C_{E/F^{C_3}} C_{E/\mathbb{Q}}^2}{C_{E/F^{C_6^a}} C_{E/F^{C_6^b}} C_{E/F^{C_6^c}}}\right).$$

We remark that the underlying fields do satisfy the condition (†) from Conjecture 1.2. This evaluates to $2 \cdot \square$, and since 2 is not a norm of an element from $\mathbb{Q}(\sqrt{-3})$, Conjecture 1.2 forces $\mathrm{rk}\, E/F > 0$.

This test of predicting positive rank for families of elliptic curves should be reminiscent of using root number computations to predict positive rank based on local data. One takes the product of local roots numbers to obtain a global root number $w(E/K) \in \pm 1$, and this arises in the (conjectural) functional equation of $L(E/K, s)$ (see Conjecture 5.2). Hence, it describes the parity of the vanishing of the L-function at $s = 1$. Assuming BSD, one expects the following to hold.

Conjecture 1.4 (Parity Conjecture)**.** Let E be an elliptic curve over a number field K. Then $(-1)^{\mathrm{rk}\, E/K} = w(E/K)$.

Using the Parity Conjecture to test for rank growth is known as a 'parity test'. The Parity Conjecture has been extensively studied in the literature, see for example [Dok13] It is known to hold in certain conditions under the assumption of finiteness of $Ш_{E/F}$. One can observe that the rank growth in the above example can also be explained by the Parity Conjecture, and we expect this phenomenon to happen in general.

Conjecture 1.5. Consider an elliptic curve $E/\mathbb{Q}$, $F/\mathbb{Q}$ a finite Galois extension, and relation

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

as in (†). If the product $\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F_j'}}$ 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 there exists a subfield $K \subseteq F$ such that $w(E/K)w(E/\mathbb{Q}) = -1$.

In Section 5.2 we describe a refined version of this conjecture, where it is phrased in terms of Artin twists of root numbers.

Parity tests cannot predict rank growth of elliptic curves in odd degree extensions. This is a direct consequence of the fact that odd degree groups have no non-trivial self dual representations (see Lemma 5.11). Accordingly, Norm Relations tests cannot make such a prediction either.

Theorem 1.6 (Theorem 9.1)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let $F/\mathbb{Q}$ be a Galois extension of odd order with Galois group G. Assume that E has semistable reduction at 2 and 3 and take any representation ρ of G. Suppose $m \geq 1$ and $F_i, F_j' \subseteq F$ satisfy*

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

Then, for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, we have that

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

The other setting in which Norm Relation tests cannot predict rank growth is when $F/\mathbb{Q}$ is a Galois cyclic extension. When $G = \mathrm{Gal}(F/\mathbb{Q})$ is even and cyclic, parity tests can predict rank growth through the sign representation, which is a self-dual representation. However, for Norm Relation tests, the following holds.

Theorem 1.7 (Theorem 8.2)**.** *Let $d \geq 2$ be a positive integer and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_d$. Take any representation ρ of C_d and any semistable elliptic curve $E/\mathbb{Q}$ at 2 and 3.*

Let F_i, F_j' be the intermediate fields of F/K (which exist and are unique up to permutation) such that

$$\bigoplus_{\mathfrak{g}\in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} = \bigoplus_i \mathrm{Ind}_{F_i/K} \mathbb{1} \ominus \bigoplus_j \mathrm{Ind}_{F_j'/K} \mathbb{1}$$

Then, for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, we have that

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F_j'}} \in N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\mathbb{Q}(\sqrt{D})^\times).$$

The strategy to prove these results is to break down the product

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F_j'}} = \prod_{\mathfrak{p}} \left(\frac{\prod_i C_{\mathfrak{P}|\mathfrak{p}}(E/F_i)}{\prod_j C_{\mathfrak{P}|\mathfrak{p}}(E/F_j')}\right)$$

into the local contributions of each prime $\mathfrak{p}$ in the base field (see Notation 5.9). Each one of these local factors depends on the decomposition group $D_\mathfrak{p} \leq G$ and inertia group $I_\mathfrak{p} \triangleleft D_\mathfrak{p}$. Consequently, the following corollary also holds.

Corollary 1.8 (Corollary 9.15)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G. Assume that E has good or multiplicative reduction at 2 and 3.*

Let ρ be a representation of G, and let $m \geq 1$ and $F_i, F_j' \subseteq F$ be as in (†). Let p be a rational prime and suppose that $D_p \leq G$ is either cyclic or a group of odd order. Then, for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, one has

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

Therefore, when trying to use Norm Relations tests to force positive rank, interesting cases can only occur when $E/\mathbb{Q}$ has bad reduction at primes that ramify in $F/\mathbb{Q}$ and such that D_p is non-cyclic and has even order.

Layout of the Report

The purpose of this project is two-fold: firstly, it aims to serve as an introduction to the topics related to the Birch–Swinnerton-Dyer conjecture and, secondly, it studies the arithmetic consequences of Conjecture 1.2 for elliptic curves.

Sections 2 to 4 serve the first purpose. In Section 2, we give a brief and rather informal discussion on the theory of elliptic curves, where we dedicate most of our attention in describing their local behaviour. In Section 3, we introduce the notion of an Artin representation and ℓ-adic representation, and we also give a detailed description on the construction of the L-functions $L(E/F, s)$ associated to an elliptic curve over a number field F and of its twist by an Artin representation ρ. Finally, in Section 4 we discuss the BSD conjecture in more detail and we explain the arithmetic terms appearing in the statement of the conjecture. We also discuss an important conjectural analogue of BSD for Artin twists which naturally leads to the statement of Conjecture 4.6, which motivates the latter half of the discussion.

The remaining sections serve the second purpose of studying the arithmetic of elliptic curves through Conjecture 4.6. In Section 5 we describe how to derive Conjecture 1.2 from the statement of Conjecture 4.6, and we provide detailed examples on how Norm Relations test predict positive rank. The statement and proofs of Theorems 1.6 and 1.7 are more naturally phrased in representation theoretic terms. Therefore, in Section 6, we introduce the necessary notation and results required for the later sections.

The last three sections of the report are devoted to proving Theorems 1.6 and 1.7. In Section 7, we prove some preliminary results that describe the local behaviour of some families of elliptic curves. Sections 8 and 9 contain the main proofs of the report on the cyclic and odd cases, respectively. At the end of the report, the reader can find the Appendix with some global class field theory that are used throughout the latter sections.

Acknowledgements

We would like to thank our supervisor Vladimir Dokchitser for his generosity with his time, his many helpful suggestions, and for introducing us to this interesting topic.

2 Elliptic Curves

In this preliminary section, we introduce elliptic curves, our main object of study throughout this document. Our discussion will be rather informal and brief, and will avoid most proofs. Therefore, even though we introduce most notions that will be relevant to us, we assume significant familiarity with the topic. For the unfamiliar reader, there is great material available for elliptic curves, such as [Sil86], where a complete discussion is given. Whenever material is readily available, we give the references. Nevertheless, we will spend some time discussing reduction types of elliptic curves and some relevant results that are less well-known and harder to find in the literature.

2.1 Elliptic Curves over Local Fields and Reduction Types

Recall that 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**

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in K, \tag{*}$$

together with the specified K-rational point $[0 : 1 : 0]$ at infinity. Associated to this equation is the j-invariant j, as well as the discriminant Δ (see [Sil86, §III.1] for more details).

Now assume that K is a local field of characteristic 0 with a discrete valuation ν, ring of integers R, maximal ideal $\mathfrak{m}$ and residue field $\kappa = R/\mathfrak{m}$. We denote by $a \mapsto \tilde{a}$ for the natural quotient map $K \to \kappa$. We say that (*) is a **minimal Weierstrass equation** if $a_1, a_2, a_3, a_4, a_6 \in R$ 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 $y^2 + \tilde{a_1}xy + \tilde{a_3}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$ and the associated **reduction map**

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

obtained by reducing the coordinates of a point $P \in E(K)$ modulo $\mathfrak{m}$. One needs to have some care defining the reduction map. For a detailed construction, see [Sil86, §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 2.1. Let E/K and $\tilde{E}/\kappa$ be as above. Then we say that

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

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

(c) E/K has **additive** 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.

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 2.2 ([Sil86, §VII Proposition 5.4])**.** *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 specifically 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 split multiplicative over F.

Item (ii) of the above lemma motivates the following definition that we will use later on.

Definition 2.3. Given an elliptic curve E with additive reduction over K, we say that it has **potentially good** (resp. **potentially multiplicative**) reduction if it has good (resp. multiplicative) reduction over a finite field extension of K.

This behaviour is characterized by the value of the j-invariant.

Proposition 2.4. *Let E be an elliptic curve of characteristic 0. Then*

- *If $\nu(j) \geq 0$, then E has good or potentially good reduction.*
- *If $\nu(j) < 0$, then E has multiplicative or potentially multiplicative reduction.*

One can use Tate's algorithm ([Sil94, §IV.9]) to determine the reduction type of E. The reduction types are encoded by Kodaira symbols. These are described in the following table, assuming that the characteristic of κ is not equal to 2 or 3 when E/K has additive reduction.

I_0 :	E/K has good reduction,
I_n :	E/K has multiplicative reduction, $\nu(\Delta) = n$,
I_n^* :	E/K has potentially multiplicative reduction, $\nu(\Delta) = 6 + n$,
I_0^* :	E/K has potentially good reduction, $\nu(\Delta) = 6$,
II, III, IV :	E/K has potentially good reduction, $\nu(\Delta) = 2$, 3, 4, respectively,
IV^*, III^*, II^* :	E/K has potentially good reduction, $\nu(\Delta) = 8$, 9, 10 respectively.

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

$$c(E/K) := |E(K)/E_0(K)|.$$

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 multiplicative reduction, Tamagawa numbers have a simple explicit description.

Lemma 2.6. *Let E/K have multiplicative reduction, and let $n = \nu(\Delta)$ be the valuation of the minimal discriminant. Then*

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

In the case of additive reduction, if we assume that the residue characteristic is ≥ 5, then one can determine the Tamagawa number from the shortened Weierstrass equation of E. The following result is a consequence of Tate's algorithm.

Lemma 2.7. *[DD09, Lemma 3.22] Let $F/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let*

$$E\colon y^2 = x^3 + Ax + B, \qquad A, B \in K$$

be an elliptic curve over K with additive reduction. One has $\Delta = -16(4A^3 + 27B^2)$. Let $\delta = v_K(\Delta)$ be the valuation of the minimal discriminant, and e the ramification index of F/K. If E has potentially good reduction, then

$$\begin{array}{lll}
\gcd(\delta e, 12) = 2 \implies c(E/F) = 1, & & (\mathrm{II}, \mathrm{II}^*) \\
\gcd(\delta e, 12) = 3 \implies c(E/F) = 2, & & (\mathrm{III}, \mathrm{III}^*) \\
\gcd(\delta e, 12) = 4 \implies c(E/F) = \begin{cases} 1, & \sqrt{B} \notin F \\ 3, & \sqrt{B} \in F \end{cases}, & (\mathrm{IV}, \mathrm{IV}^*) \\
\gcd(\delta e, 12) = 6 \implies c(E/F) = \begin{cases} 2, & \sqrt{\Delta} \notin F \\ 1 \text{ or } 4, & \sqrt{\Delta} \in F \end{cases}, & (\mathrm{I}_0^*)
\end{array}$$

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

$$\begin{array}{lll}
2 \nmid e, 2 \nmid n \implies c(E/F) = \begin{cases} 2, & \sqrt{B} \notin F, \\ 4, & \sqrt{B} \in F. \end{cases} & (\mathrm{I}_{en}^*) \\
2 \nmid e, 2 \mid n \implies c(E/F) = \begin{cases} 2 & \sqrt{\Delta} \notin F, \\ 4 & \sqrt{\Delta} \in F \end{cases} & (\mathrm{I}_{en}^*) \\
2 \mid e, \sqrt{-6B} \notin F \implies c(E/F) = 2 & & (\mathrm{I}_{en},\ \textit{non-split}) \\
2 \mid e, \sqrt{-6B} \in F \implies c(E/F) = en & & (\mathrm{I}_{en},\ \textit{split})
\end{array}$$

2.3 Elliptic Curves over Number 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 elliptic curves over number fields. Hence, let E be 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

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

Definition 2.8. Given a set S of primes in K, we say that an elliptic curve E/K is **semistable at** S if the reduction at any prime of S is good or multiplicative. In addition, if E has nowhere additive reduction, we say that E is **semistable**.

Finally, we say that a Weierstrass equation (*) 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 general number fields K, it does hold for $\mathbb{Q}$.

Proposition 2.9. *[Sil86, §VIII, Corollary 8.3] 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 preliminary 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. The results in this section are self-contained, and the discussion is inspired by a course on elliptic curves by Vladimir Dokchitser.

Throughout this section we fix a field K, which will either be a number field or a non-Archimedean local field of characteristic 0. For convenience, whenever we say local field from now on we refer to a non-Archimedean 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. 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 continuous 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 $\mathrm{GL}_n(\mathbb{C})$. Hence, Artin representations are simply continuous 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. A **continuous ℓ-adic representation** ρ over K is a continuous 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, continuity 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 continuous 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** in the natural way.

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.

Notation 3.5. We 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 representations. These objects are usually described for local fields. Then, one constructs global objects attached to number fields by completing them at their finite places, obtaining the local information and then combining it appropriately.

To begin, let K be a local field 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 result 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 inertia-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 3.6. Let K be a local field and let p the characteristic of its residue 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 associated L-function.

Definition 3.7. 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 3.8. 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 3.9. 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 **$\ell$-adic Tate module** of the elliptic curve E. By the uniformization theorem, we know that

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

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

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

commutes. Therefore, 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 typically constructed using the later ones.

Remark 3.10. 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 3.11. *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,*

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

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 3.12. 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.

Fix some number field K, an elliptic curve E over K and an Artin representation ρ over K. Then, similarly 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. The following important result is known as **Artin Formalism**.

Theorem 3.13 (Artin Formalism)**.** *Let E be an elliptic curve over a number field K.*

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

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

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

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

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

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

then

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

4 Birch–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 minimal Weierstrass equation. Since we will be mainly interested in elliptic curves over $\mathbb{Q}$, and in view of Proposition 2.9, 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 $\omega = dx/(2y + a_1x + a_3)$ be the associated **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 F. Then

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

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

BSD2. The group $Ш_{E/F}$ has finite order and the leading term of the Taylor series at $s = 1$ of the L-function is

$$\lim_{s\to 1} \frac{L(E/F, s)}{(s-1)^r} \cdot \frac{\sqrt{|\Delta_F|}}{\Omega_+(E)^{r_1+r_2}|\Omega_-(E)|^{r_2}} = \frac{\operatorname{Reg}_{E/F}\,|Ш_{E/F}|C_{E/F}}{|E(F)_{\text{tors}}|^2}. \tag{BSD2}$$

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 F. These are the discriminant Δ_F of F and the numbers r_1 and r_2, corresponding to the number of real and complex embeddings of F. A basic formula states that if $n = [F : \mathbb{Q}]$, 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. **Regulator:** To properly define the regulator one needs to carefully construct the canonical height $\hat{h} : E(\bar{F}) \to \mathbb{R}^+$, which roughly evaluates the 'arithmetic complexity' of a given point $P \in E(\bar{F})$. We refer the reader to [Sil86, Chapter VIII: §4, §5, §6 and §9] for a complete discussion of this topic. This map satisfies many important properties (as listed in [Sil86, Chapter VIII, Theorem 9.3]), among which is the fact that $\hat{h}$ is a quadratic form; in particular, the pairing
$$\langle \cdot, \cdot \rangle : E(\bar{F}) \times E(\bar{F}) \longmapsto \mathbb{R}$$
$$\langle P, Q \rangle = \hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q)$$
is bilinear. Then the regulator is the volume of $E(F)/E(F)_{\text{tors}}$ computed using the quadratic form $\hat{h}$. In other words, let $P_1, \ldots, P_r$ be generators of the group $E(F)/E(F)_{\text{tors}}$. Then
$$\operatorname{Reg}_{E/F} = \det(\langle P_i, P_j \rangle)_{1\le i,j\le r}$$
if $r \ge 1$ and $\operatorname{Reg}_{E/F} = 1$ if $r = 0$.

3. **Tate-Shafarevich group:** This is the most mysterious group and it is commonly defined using Galois cohomology as
$$Ш_{E/F} = \ker\left[H^1(F,E) \to \prod_{\mathfrak{p}} H^1(F_{\mathfrak{p}},E)\right],$$
where the product ranges over all places, finite and infinite, of F. One has $H^1(F,E) := H^1(G_F, E(\bar{F}))$ and the implicit map is induced by the inclusions $G_{F_{\mathfrak{p}}} \hookrightarrow G_F$. One can interpret $H^1(F,E)$ as 'homogeneous spaces' of E over F up to equivalence. A homogeneous space over F is trivial if and only if it has a F-rational point, so a non-trivial element of $Ш_{E/F}$ is a homogeneous space that has points locally in every $F_{\mathfrak{p}}$ but has no F-rational point.
4. **Local data:** The term $C_{E/F}$ is defined in terms of local data as
$$C_{E/F} = \prod_{\mathfrak{p}} c_{\mathfrak{p}}(E/F)\left|\frac{\omega}{\omega_{\mathfrak{p}}^{\min}}\right|_{\mathfrak{p}}.$$
Here the product ranges over the finite places of F. The term $c_{\mathfrak{p}}(E/F)$ is the Tamagawa number of E/F at $\mathfrak{p}$, as defined in §2.2. Here ω is the global minimal differential for $E/\mathbb{Q}$, and $\omega_{\mathfrak{p}}^{\min}$ is the minimal differential at $\mathfrak{p}$. By $\omega/\omega_{\mathfrak{p}}^{\min}$ one means any scalar $\lambda \in F^\times$ with $\omega = \lambda\omega_{\mathfrak{p}}^{\min}$. In terms of minimal discriminants, one has
$$\left|\frac{\omega}{\omega_{\mathfrak{p}}^{\min}}\right|_{\mathfrak{p}}^{-12} = \left|\frac{\Delta_E}{\Delta_{E,\mathfrak{p}}^{\min}}\right|_{\mathfrak{p}},$$
where $\Delta_{E,\mathfrak{p}}^{\min}$ is the minimal discriminant at $\mathfrak{p}$.

The following result will be helpful to compute these local terms arising from the minimal differential in explicit examples.

Lemma 4.2. *Let E be an elliptic curve over a number field K, F/K a finite extension. Let $\mathfrak{p}$ be a prime in K and $\mathfrak{P}$ a prime in F above $\mathfrak{p}$. Let q be the size of the residue field of K at $\mathfrak{p}$.*

Let $\Delta_{\mathfrak{p}}$, $\omega_{\mathfrak{p}}$ and $\Delta_{\mathfrak{P}}$, $\omega_{\mathfrak{P}}$ be the minimal discriminants and differentials for $E/K_{\mathfrak{p}}$ and $E/F_{\mathfrak{P}}$, respectively. Then the following holds.

(i) If $\mathfrak{p}$ is unramified at F/K or if E has good or multiplicative reduction at $\mathfrak{p}$, then the minimal model of $E/K_{\mathfrak{p}}$ and $E/F_{\mathfrak{P}}$ coincide so $|\omega_{\mathfrak{p}}/\omega_{\mathfrak{P}}|_{\mathfrak{P}} = 1$.

(ii) If the residual characteristic is distinct from 2 or 3, and E has potentially good reduction over K, then $v_{\mathfrak{p}}(\Delta_{\mathfrak{p}}) < 12$ and the same holds for $\mathfrak{P}$. In particular,
$$\left|\frac{\omega_{\mathfrak{p}}}{\omega_{\mathfrak{P}}}\right|_{\mathfrak{P}} = q^{f_{\mathfrak{P}|\mathfrak{p}}\cdot\lfloor\frac{e_{\mathfrak{P}|\mathfrak{p}}\nu_{\mathfrak{p}}(\Delta_{\mathfrak{p}})}{12}\rfloor}.$$

(iii) If the residual characteristic is distinct from 2 or 3, and $E/K_{\mathfrak{p}}$ has potentially multiplicative reduction over K then
$$\left|\frac{\omega_{\mathfrak{p}}}{\omega_{\mathfrak{P}}}\right|_{\mathfrak{P}} = q^{f_{\mathfrak{P}|\mathfrak{p}}\cdot\lfloor\frac{e_{\mathfrak{P}|\mathfrak{p}}}{2}\rfloor}.$$

Proof Sketch. Let $e = e_{\mathfrak{P}|\mathfrak{p}}$, $f = f_{\mathfrak{P}|\mathfrak{p}}$, $\delta = v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})$ and $\delta_{\mathfrak{P}} = v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$. Then $v_{\mathfrak{P}}(\Delta_{\mathfrak{p}}) = en$. Thus $|\Delta_{\mathfrak{p}}/\Delta_{\mathfrak{P}}|_{\mathfrak{P}} = q^{f\cdot(\delta\cdot e-\delta_{\mathfrak{P}})}$, whence
$$\left|\frac{\omega_{\mathfrak{p}}}{\omega_{\mathfrak{P}}}\right|_{\mathfrak{P}} = q^{f\cdot\lfloor\frac{\delta\cdot e-\delta_{\mathfrak{P}}}{12}\rfloor}.$$

(ii) If $E/K_{\mathfrak{p}}$ has potentially good reduction then $\delta \in \{2,3,4,6,8,9,10\}$ and $\delta_{\mathfrak{P}} \le 12$. By reducing to minimal Weierstrass equation for $E/F_{\mathfrak{P}}$ it follows that $\delta_{\mathfrak{P}} = \delta\cdot e - 12\cdot\lfloor\delta\cdot e/12\rfloor$.

(iii) Let E/K_p have Kodaira type I_n^*, so $\delta = 6+n$. If e is even then $E/F_{\mathfrak{P}}$ has Kodaira type I_{en}, so $\delta_{\mathfrak{P}} = en$ and $\delta\cdot e - \delta_{\mathfrak{P}} = 6e$. Else if e is odd, $E/F_{\mathfrak{P}}$ has Kodaira type I_{en}^* so $\delta_{\mathfrak{P}} = 6+en$ and $\delta\cdot e - \delta_{\mathfrak{P}} = 6e-6$. But then $\lfloor(6e-6)/12\rfloor = \lfloor(e-1)/2\rfloor = \lfloor e/2\rfloor$ since e is odd.

□

We remark that the way we have organised the terms in (BSD2) 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 F a number field. We define

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

and

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

4.2 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 4.4 (BSD1 for Twists)**.** Let $E/\mathbb{Q}$ be an elliptic curve, ρ an Artin representation and F any Galois extension over $\mathbb{Q}$ such that ρ factors through $G = \mathrm{Gal}(F/\mathbb{Q})$. Then

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

where $E(F)_{\mathbb{C}} = E(F) \otimes_{\mathbb{Z}} \mathbb{C}$ is viewed as a G-representation, and $\langle \cdot,\cdot \rangle$ is the usual inner product of characters of 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 4.5. [DEW21, Definition 12] Let $E/\mathbb{Q}$ be an elliptic curve and ρ an Artin representation over $\mathbb{Q}$. We define

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

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

For an elliptic curve $E/\mathbb{Q}$ and Galois extension $F/\mathbb{Q}$, Artin formalism allows one to factor $L(E/F,s)$ as a product of L-functions twisted by Artin representations. One would like to similarly factorize the leading term $\mathrm{BSD}(E/F)$ according to Artin representations. Specifically, one would like the following to hold:

Conjecture 4.6. [DEW21, Conjecture 4] Let $E/\mathbb{Q}$ be an elliptic curve. For every Artin representation ρ over $\mathbb{Q}$ there exists an invariant $\mathrm{BSD}(E,\rho) \in \mathbb{C}^\times$ with the following properties. Let ρ and τ be Artin representations over $\mathbb{Q}$ that factor through $G = \mathrm{Gal}(F/\mathbb{Q})$ for some finite Galois extension $F/\mathbb{Q}$. Then

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

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

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

C3. $\mathrm{BSD}(E,\rho) \in \mathbb{Q}(\rho)^\times$ and $\mathrm{BSD}(E,\rho^{\mathfrak{g}}) = \mathrm{BSD}(E,\rho)^{\mathfrak{g}}$ for all $\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$.

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. The authors of [DEW21] justify posing this conjecture by studying $\mathscr{L}(E,\rho)$, and proving the following.

Theorem 4.7. *[DEW21, Corollary 25] Let $E/\mathbb{Q}$ be an elliptic curve, ρ, τ Artin representations over $\mathbb{Q}$. Suppose that for any Artin representations ψ over $\mathbb{Q}$, the L-function $L(E,\psi,s)$ has analytic continuation to $\mathbb{C}$ and satisfies Deligne's period conjecture ([Del79]). Further assume that* BSD *holds for elliptic curves over number fields. Then Conjecture 4.6 holds if one takes* $\mathrm{BSD}(E,\rho) = \mathscr{L}(E,\rho)$.

5 Predicting Positive Rank

In this section, we study arithmetic applications of Conjecture 4.6, focusing on when we can use this conjecture to force positive rank for families of elliptic curves. In particular we describe a result introduced in [DEW21] that provides a test for forcing rank growth. We call this a Norm Relations test. As we will observe, this test depends only on local arithmetic data associated to the elliptic curve.

We also compare this new test to a well-studied method of forcing rank growth, namely by using the Parity Conjecture. As such, we first introduce root numbers and the Parity conjecture, before going on to describe the Norm Relations test and presenting some examples of its use.

5.1 Root Numbers and The Parity Conjecture

Root numbers (conjecturally) govern the parity of the rank of an elliptic curve. In this subsection, we briefly discuss root numbers and the parity conjecture. We omit the notation, but descriptions of the completed L-functions for $L(E/F, s)$ and $L(E/F, \rho, s)$ can be found in [DEW21, §2.5].

Let F be a number field and E/F an elliptic curve. The parity conjecture states that the rank of E/F is determined by the global root number $w(E/F) \in \{\pm 1\}$, that is

Conjecture 5.1 (Parity conjecture)**.** $(-1)^{\operatorname{rk} E/F} = w(E/F)$.

In particular if $w(E/F) = -1$, one has that $\operatorname{rk} E/F$ is odd, and so $\operatorname{rk} E/F > 0$. Therefore the computation of root numbers provides a test for forcing positive rank. We note that parity conjecture follows from assuming BSD and the Hasse–Weil conjecture:

Conjecture 5.2 (Hasse–Weil conjecture)**.** $L(E/F, s)$ has a completed L-function $\hat{L}(E/F, s)$ that can be analytically continued to $\mathbb{C}$ and satisfies the following functional equation:

$$\hat{L}(E/F, s) = w(E/F)\hat{L}(E/F, 2 - s).$$

This is known when $F = \mathbb{Q}$ due to modularity of elliptic curves. Assuming the Hasse–Weil conjecture, one has that if $w(E/F) = 1$, then $\hat{L}(E/F, s)$ is symmetric under $s \leftrightarrow 2 - s$, and so the order of vanishing at $s = 1$ of $\hat{L}(E/F, s)$ is even. Then $\operatorname{ord}_{s=1} L(E/F, s) = \operatorname{ord}_{s=1} \hat{L}(E/F, s)$ and assuming BSD one has that $\operatorname{rk} E/F$ is even. The parity conjecture for elliptic curves is known to be true over number fields F, assuming finiteness of $|Ш_{E/F}|$, as proven in [DD11].

The global root number is a product of local root numbers.

$$w(E/F) = \prod_v w(E/F_v),$$

taking the product over all places (including infinite ones) of F. The following proposition details how to compute these root numbers.

Proposition 5.3. *[DD10, Theorem 3.1] Let F be a number field, F_v the completion of F with respect to a place v. When v is finite, let κ be the residue field of F_v. Then the local root number $w(E/F_v)$ is given by*

(i) $w(E/F_v) = -1$ *if v is infinite, or if E/F_v has split multiplicative reduction,*

(ii) $w(E/F_v) = 1$ *if E/F_v has good reduction, or if E/F_v has non-split multiplicative reduction,*

(iii) $w(E/F_v) = \left(\frac{-1}{\kappa}\right)$ *if E/F_v has potentially multiplicative reduction and κ has characteristic ≥ 3, where $\left(\frac{*}{\kappa}\right)$ is the quadratic residue symbol on $\kappa^\times$,*

(iv) $w(E/F_v) = (-1)^{\lfloor \frac{v(\Delta_E)|\kappa|}{12} \rfloor}$, *if E/F_v has potentially good reduction and κ has characteristic ≥ 5, where Δ_E is the minimal discriminant of E.*

Example 5.4 (Modular curve $X_1(11)$)**.** The elliptic curve $E\colon y^2+y = x^3-x^2$ over $\mathbb{Q}$ has good reduction at $p \neq 11$, and split multiplicative reduction at $p = 11$. Hence by Proposition 5.3, $w(E/\mathbb{Q}) = (-1)(-1) = 1$ and so the parity conjecture implies that $\operatorname{rk} E/\mathbb{Q}$ is even (actually, it is zero).

There is also a global root number for the twist of E by an Artin representation ρ, denoted $w(E/F,\rho)\in\{\pm 1\}$. This appears in a functional equation relating the completed twisted L functions $\hat{L}(E/F,\rho,s)$ and $\hat{L}(E/F,\rho^*,2-s)$, where ρ^* is the dual representation of ρ. Then one has a parity conjecture for twists by self-dual representations:

Conjecture 5.5 (Parity conjecture for twists)**.** Let ρ be a self-dual Artin representation that factors through $\mathrm{Gal}(F/\mathbb{Q})$. Then

$$w(E/\mathbb{Q},\rho)=(-1)^{\langle\rho,E(F)_{\mathbb{C}}\rangle}.$$

Again this is the product of local root numbers; $w(E/\mathbb{Q},\rho)=\prod_v w(E/\mathbb{Q}_v,\rho)$, where $w(E/\mathbb{Q}_v,\rho)\in\{\pm 1\}$. The twisted root numbers satisfy the following properties:

Proposition 5.6. *[DD09, Lemma A.1, Proposition A.2] Let E/F be an elliptic curve, L/F a finite Galois extension with Galois group G. Let ρ, τ be Artin representations over F that factor through G and let $\mathbb{1}$ denote the trivial Artin representation over F. Then*

(i) $w(E/F,\rho\oplus\tau)=w(E/F,\rho)w(E/F,\tau)$,
(ii) $w(E/F,\mathbb{1})=w(E/F)$,
(iii) If $H\leq G$ *then* $w(E/L^H)=w(E/F,\mathrm{Ind}_H^G\,\mathbb{1})$,
(iv) $w(E/F,\rho\oplus\rho^*)=1$.

Therefore, similarly to the L-function of E/F, one can factor the root number $w(E/F)$ into twisted root numbers.

5.2 Norm Relations Tests

We are concerned with the case of predicting positive rank for families of elliptic curves over certain number fields. We illustrate the proof of the main result that predicts positive rank conditional on Conjecture 4.6. 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 a 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[1] there is some $m\geq 1$ and subfields $F_i,F_j'\subseteq F$ such that

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

Assume that $\mathrm{rk}\,E/F=0$ so that in particular $\langle\rho,E(F)_{\mathbb{C}}\rangle_G=0$. Therefore Conjecture 4.6 implies that

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

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 (†) involves 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 Cassels proved the following.

[1] see Remark 6.3

Theorem 5.7. *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 of $\mathbb{Q}(\rho)$, then the RHS of (†) 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 $|E(F)_{\text{tors}}|^2$ are rational squares and therefore norms from $\mathbb{Q}(\sqrt{D})$. The only remaining terms on the LHS of (†) are the product of local factors C_{E/F_i} and $C_{E/F_j'}$. We have therefore proven the following.

Theorem 5.8. *[DEW21, Theorem 33] Suppose Conjecture 4.6 holds. Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a finite Galois extension with Galois group G, ρ an Artin representation over $\mathbb{Q}$ that factors through G and*

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

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 for general families of elliptic curves based solely on local data. Let us call applying this theorem a **norm relations test**. Following this result, we introduce some notation that will be very useful to compute the local factors $C_{E/F}$.

Notation 5.9. 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 the **local contribution of $\mathfrak{p}$** as

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

and $C_{\mathfrak{P}|\mathfrak{p}}(E/F) = T_{\mathfrak{P}|\mathfrak{p}}(E/F)D_{\mathfrak{P}|\mathfrak{p}}(E/F)$, where the product ranges over primes $\mathfrak{P}$ of F over $\mathfrak{p}$. The local Tamagawa number is defined in §2.2, Δ_E is the global minimal discriminant of $E/\mathbb{Q}$, and $\Delta_{E,\mathfrak{P}}^{\min}$ is the minimal discriminant of E at $\mathfrak{P}$.

Thus given F/K, one can obtain the global contributions from the terms above by taking the product over all primes $\mathfrak{p}$ of K. We denote the **global contribution over** F of the Tamagawa numbers and the discriminant terms as

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

An immediate consequence of this notation is the fact that $C_{E/F} = T(E/F)D(E/F)$.

We have now seen that both Theorem 5.8 and Conjecture 5.1 can force the rank of an elliptic curve to be positive. One can observe that for the examples in the next subsection, whenever our norm relations test forces rank growth, a root number computation for the subfields appearing in our relation also implies positive rank. It would be a lot more interesting if we could find an example where the norm relations test forces positive rank and root numbers do not. We suspect however that such an example does not exist.

Consider $G = \mathrm{Gal}(F/K)$. Then changes in parity between subfields of F/K correspond to twisted root numbers being equal to -1. Indeed by Proposition 5.6, for $H \leq G$,

$$\mathrm{Ind}_H^G \mathbb{1} \simeq \mathbb{1} \oplus \bigoplus_i \rho_i \implies w(E/F^H) = w(E/K)\prod_i w(E/K, \rho_i)$$

for some representations ρ_i of G. Hence a change in parity from $w(E/K)$ to $w(E/F^H)$ is determined by $\prod_i w(E/K, \rho_i)$. On the premise that a failure of our Norm Relations test is always explained by root numbers, we conjecture the following:

Conjecture 5.10. Consider an elliptic curve $E/\mathbb{Q}$, $F/\mathbb{Q}$ a finite Galois extension, and relation

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

as in Theorem 5.8. If the product $\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}}$ 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 there exists a self-dual Artin representation τ of G such that $w(E/\mathbb{Q}, \tau) = -1$.

The case of odd order Galois groups inspires some confidence in this conjecture. Let $F/\mathbb{Q}$ be a Galois extension of odd order. In §9, we prove that one cannot use Theorem 5.8 to conclude that $\mathrm{rk}\, E/F > 0$, i.e. that our Norm Relations test never "fails". The reason one would expect that our Norm Relations test never forces rank growth in this case is because root number computations do not, as we now show.

Lemma 5.11. *Let $F/\mathbb{Q}$ be an odd Galois extension with $G = \mathrm{Gal}(F/\mathbb{Q})$. Then $w(E/\mathbb{Q}) = w(E/F^H)$ for all $H \leq G$.*

Proof. Consider $H \leq G$ and intermediate field F^H. Then $\mathrm{Ind}_H^G \mathbb{1} \simeq \mathbb{1} \oplus \rho \oplus \rho^*$ for some non self-dual representation ρ of G, since the only self-dual representation of an odd-order group is the trivial representation. Therefore by Proposition 5.6, $w(E/F^H) = w(E/F)w(E, \rho \oplus \rho^*)$ and $w(E, \rho \oplus \rho^*) = 1$. Hence $w(E/\mathbb{Q}) = w(E/F^H)$ for all $H \leq G$. □

Therefore once we assume that $\mathrm{rk}\, E/\mathbb{Q} = 0$, the parity conjecture tells us that $\mathrm{rk}\, E/F^H$ is even for all $H \leq G$, which does not force it to be non-zero.

5.3 Examples

We now present some examples where we use Theorem 5.8 to force positive rank. Throughout we will consider an elliptic curve E defined over $\mathbb{Q}$, and a finite Galois extension $F/\mathbb{Q}$ with Galois group $G = \mathrm{Gal}(F/\mathbb{Q})$. We let Δ_E denote the global minimal differential of $E/\mathbb{Q}$. We start with a small observation:

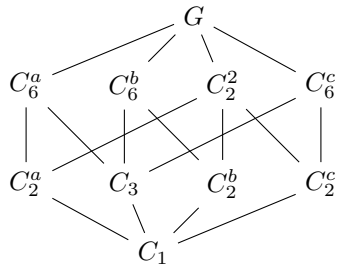
Remark 5.12 (Taking quotients)**.** Let E, F, G be as above. Consider $H \leq G$, and $N \triangleleft G$ such that $N \leq H$. Let $L = F^N$. Then C_{E/F^H} is equal to $C_{E/L^{H/N}}$ as the fields F^H and $L^{H/N}$ are isomorphic.

When computing Tamagawa numbers, we will need to be able to count primes and compute ramification degrees in intermediate extensions of $F/\mathbb{Q}$, which is described by the following.

Exercise 5.13 (Counting primes and ramification degrees)**.** Consider a prime $p \in \mathbb{Q}$ and decomposition and inertia groups D_p, $I_p \leq G$. Let $H \leq G$.

1. The number of primes above p in F^H is given by the number of orbits of D_p on $H\backslash G$, where D_p acts by $d(Hg) = Hgd^{-1}$ for $d \in D_p$. Equivalently it is $|H\backslash G/D_p|$.
2. Let a prime $\mathfrak{P}$ above p in F^H correspond to an orbit Y of D_p acting on $H\backslash G$. Then the ramification degree of $\mathfrak{P}$ over $\mathbb{Q}$ is the size of the I_p sub-orbits on Y.

Example 5.14 (Brauer relation forces growth)**.** Let $G = C_2 \times C_6$, with subgroup diagram



Consider an order 6 character ρ_a of G with C_2^a in its kernel. This has $\mathbb{Q}(\rho_a) = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$. Let τ generate $\mathrm{Gal}(\mathbb{Q}(\rho_a)/\mathbb{Q})$. One has

$$\mathrm{Ind}_{C_2^a}^G \mathbb{1} \ominus \mathrm{Ind}_{C_6^a}^G \mathbb{1} \ominus \mathrm{Ind}_{C_2^2}^G \mathbb{1} \oplus \mathrm{Ind}_G^G \mathbb{1} \simeq \rho_a \oplus \rho_a^\tau. \tag{†}$$

Let $E/\mathbb{Q}$ be a semistable elliptic curve. To apply Theorem 5.8, we need to compute

$$\frac{C_{E/F^{C_2^a}} C_{E/\mathbb{Q}}}{C_{E/F^{C_6^a}} C_{E/F^{C_2^2}}} = \frac{C_{E/L} C_{E/\mathbb{Q}}}{C_{E/L^{C_3}} C_{E/L^{C_2}}} \tag{*}$$

where $L = F^{C_2^a}$ has $\mathrm{Gal}(L/\mathbb{Q}) = C_6$, and check whether it is a norm from $\mathbb{Q}(\sqrt{-3})$. This is a product of local Tamagawa numbers, as the minimal differential terms are 1 when $E/\mathbb{Q}$ is semistable (Lemma 4.2(i)).

One needs to compute these locally for each $p \in \mathbb{Q}$. If $E/\mathbb{Q}_p$ has good reduction, then the Tamagawa numbers at all places above p in the subfields of L are 1. Suppose that $E/\mathbb{Q}_p$ has split multiplicative reduction at p. Let $n = v_p(\Delta_E)$. For $H \leq G$, the Tamagawa number at a prime $\mathfrak{P}$ above p in L^H is given by $c_{\mathfrak{p}}(E/L^H) = e_{\mathfrak{P}|p} n$, where $e_{\mathfrak{P}|p}$ is the ramification degree. Thus the computation of Tamagawa numbers depends on the choice of decomposition group $D_p \leq C_6$ (to count the number of primes above p in a given subfield) and the choice of inertia group $I_p \leq C_6$ (to compute the ramification indices).

The following table describes the product of Tamagawa numbers at places above p in our expression, for varying D_p and I_p. We let $T_{\mathfrak{P}|p}(E/L^H) = \prod_{\mathfrak{P}|p} c_{\mathfrak{P}}(E/L^H)$ for $H \leq \mathrm{Gal}(L/\mathbb{Q})$ as defined in Notation 5.9. Let $C_p = c_p(E/\mathbb{Q}) T_{\mathfrak{P}|p}(E/L) / T_{\mathfrak{P}|p}(E/L^{C_3}) T_{\mathfrak{P}|p}(E/L^{C_2})$.

D_p	I_p	$c_p(E/\mathbb{Q})$	$T_{\mathfrak{P}\|p}(E/L^{C_3})$	$T_{\mathfrak{P}\|p}(E/L^{C_2})$	$T_{\mathfrak{P}\|p}(E/L)$	C_p
C_1	C_1	n	n^2	n^3	n^6	$\square$
C_2	C_1	n	n	n^3	n^3	$\square$
C_3	C_1	n	n^2	n	n^2	$\square$
C_6	C_1	n	n	n	n	$\square$
C_2	C_2	n	$2n$	n^3	$(2n)^3$	$\square$
C_6	C_2	n	$2n$	n	$2n$	$\square$
C_3	C_3	n	n^2	$3n$	$(3n)^2$	$3 \cdot \square$
C_6	C_3	n	n	$3n$	$3n$	$\square$
C_6	C_6	n	$2n$	$3n$	$6n$	$\square$

In all cases we see that C_p, the contribution of Tamagawa numbers above p, is a norm form $\mathbb{Q}(\sqrt{-3})$. It is not too hard to check that this is also the case when $E/\mathbb{Q}_p$ has non-split multiplicative reduction. Therefore the expression in (*) is always a norm from $\mathbb{Q}(\rho_a)$. This is an example of a more general phenomenon; for cyclic groups we always get a norm. This follows from Theorem 8.2, which is proven in §8.

But! Observe that[2]

$$\mathrm{Ind}_{C_3}^G \mathbb{1} \ominus \mathrm{Ind}_{C_6^a}^G \mathbb{1} \ominus \mathrm{Ind}_{C_6^b}^G \mathbb{1} \ominus \mathrm{Ind}_{C_6^c}^G \mathbb{1} \oplus (\mathrm{Ind}_G^G \mathbb{1})^{\oplus 2} = 0$$

[2]this is called a Brauer relation, see Definition 6.8

as a virtual permutation representation. Append this to the left hand side of (†). Then Theorem 5.8 asks us to compute

$$\left(\frac{C_{E/F^{C_2^a}}C_{E/\mathbb{Q}}}{C_{E/F^{C_6^a}}C_{E/F^{C_2^2}}}\right)\cdot\left(\frac{C_{E/F^{C_3}}C_{E/\mathbb{Q}}^2}{C_{E/F^{C_6^a}}C_{E/F^{C_6^b}}C_{E/F^{C_6^c}}}\right). \tag{**}$$

We can find instances where the second factor is not a norm from $\mathbb{Q}(\sqrt{-3})$. Indeed suppose $E/\mathbb{Q}$ has split multiplicative reduction at a prime p with $D_p = G$, $I_p = C_6^b$. Let $v_p(\Delta_E) = n$. Then there is only one prime above p in each subfield. Suppose E has good reduction at all other primes (or multiplicative reduction at primes that are totally split in $F/\mathbb{Q}$ would also be fine). Then our expression (**) is equal to

$$\frac{(6n)(n)}{(2n)(3n)}\cdot\frac{(2n)(n)^2}{(2n)(n)(2n)}\cdot\square = \frac{1}{2}\cdot\square,$$

which is not a norm from $\mathbb{Q}(\sqrt{-3})$. Hence one must have $\operatorname{rk} E/F > 0$.

Example 5.15 (Dihedral)**.** Let q_1, q_2 be odd primes. Consider $G = D_{2q_1q_2}$ the dihedral group of order $2q_1q_2$. Let ρ, τ_1, τ_2 be two-dimensional irreducible representations of G corresponding to rotating a (q_1q_2)-gon by $2\pi/q_1q_2$, $2\pi/q_1$, $2\pi/q_2$ respectively. These are all self-dual. The Galois conjugates of these representations, as well as the trivial $\mathbb{1}$ and sign ϵ, yield all the irreducible representations of G. Let

$$\sigma_\rho = \bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})}\rho^{\mathfrak{g}}, \qquad \sigma_1 = \bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\tau_1)/\mathbb{Q})}\tau_1^{\mathfrak{g}}, \qquad \sigma_2 = \bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\tau_2)/\mathbb{Q})}\tau_2^{\mathfrak{g}}.$$

Then $\{\mathbb{1}, \epsilon, \sigma_\rho, \sigma_1, \sigma_2\}$ are a basis for the irreducible representations of G over $\mathbb{Q}$. One has

$$\mathrm{Ind}_{C_2}^G \mathbb{1} \simeq \mathbb{1}\oplus\sigma_1\oplus\sigma_2\oplus\sigma_\rho, \quad \mathrm{Ind}_{D_{2q_1}}^G \mathbb{1} \simeq \mathbb{1}\oplus\sigma_2, \quad \mathrm{Ind}_{D_{2q_2}}^G \mathbb{1} \simeq \mathbb{1}\oplus\sigma_1,$$

and so

$$\mathrm{Ind}_{C_2}^G \mathbb{1} \ominus \mathrm{Ind}_{D_{2q_1}}^G \mathbb{1} \ominus \mathrm{Ind}_{D_{2q_2}}^G \mathbb{1} \oplus \mathrm{Ind}_G^G \mathbb{1} \simeq \bigoplus_{\mathfrak{g}\in\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})}\rho^{\mathfrak{g}}.$$

Assume $E/\mathbb{Q}$ is semistable. Suppose that $E/\mathbb{Q}_p$ has split multiplicative reduction, with $n = v_p(\Delta_E)$. We compute Tamagawa numbers above p as in the previous example, using the same notation. Corollary 9.15 implies that we always get a norm from the contribution above p whenever the decomposition group is a group of odd-order. In fact we only get a non-square contribution when the decomposition group is D_{2q_1} or D_{2q_2} (and I_p is non-trivial).

For example, let p have decomposition group D_{2q_1} and inertia group C_{q_1}. This time, counting primes and computing ramification degrees is a little more awkward, we use Exercise 5.13.

- The action of D_{2q_1} on $C_2\backslash G$ yields 1 orbit of size C_{q_1} (the orbit of the identity) and $\frac{q_2-1}{2}$ orbits of size $2q_1$ (coming from C_2 acting faithfully on C_{q_2}). The size of the inertia sub-orbits is q_1. Hence $T_{\mathfrak{P}|p}(E/F^{C_2}) = (q_1n)^{1+\frac{q_2-1}{2}}$.
- The action of D_{2q_1} on $D_{2q_1}\backslash G$ yields the same number of orbits as above, but now the action of $C_{q_1} \le D_{2q_1}$ is trivial, so that $T_{\mathfrak{P}|p}(E/F^{D_{2q_1}}) = n^{1+\frac{q_2-1}{2}}$.
- The action of D_{2q_1} on $D_{2q_2}\backslash G$ yields one orbit of size q_1, with the inertia sub-orbit also of size q_1, hence $T_{\mathfrak{P}|p}(E/F^{D_{2q_2}}) = q_1n$.

In total,

$$\frac{T_{\mathfrak{P}|p}(E/F_2^C)\cdot c_{\mathfrak{p}}(E/\mathbb{Q})}{T_{\mathfrak{P}|p}(E/F^{D_{2q_1}})\cdot T_{\mathfrak{P}|p}(E/F^{D_{2q_2}})} = \frac{(q_1n)^{1+\frac{q_2-1}{2}}(n)}{(n)^{1+\frac{q_2-1}{2}}(q_1n)} = q_1^{\frac{q_2-1}{2}}.$$

So let $E/\mathbb{Q}$ have split multiplicative reduction at p with decomposition group D_{2q_1} and inertia group $I_p = C_{q_1}$, and good reduction at all other primes. Further suppose that $q_1, q_2 \equiv 3 \pmod 4$ and that $\left(\frac{q_1}{q_2}\right) = -1$. Then $\mathbb{Q}(\sqrt{q_1q_2}) \subset \mathbb{Q}(\rho)$ but

$$\frac{C_{E/F_2^C}C_{E/\mathbb{Q}}}{C_{E/F^{D_{2q_1}}}C_{E/F^{D_{2q_2}}}} = q_1\cdot\square$$

is not a norm from $\mathbb{Q}(\sqrt{q_1q_2})$. Indeed, q_1 is not the norm of an element of $\mathbb{Q}(\sqrt{q_1q_2})$, since $z^2q_1 = x^2 - q_1q_2y^2$ for $x, y, z \in \mathbb{Z}$ implies $q_1 = \square \pmod{q_2}$, a contradiction. Thus $\operatorname{rk} E/F > 0$.

This rank growth is predicted by root number computations also, however. Assume that $F/\mathbb{Q}$ is totally real. Then $w(E/F^H) = (-1)^{[F^H:\mathbb{Q}]+|H\backslash G/D_p|}$ by Proposition 5.3. Thus

$$\begin{aligned} w(E/\mathbb{Q}) &= (-1)^2 = 1, & w(E/F^{C_2}) &= (-1)^{q_1q_2}(-1)^{1+\frac{q_2-1}{2}} = (-1)^{\frac{q_2-1}{2}}, \\ w(E/F^{D_{2q_2}}) &= (-1)^{q_1}(-1) = 1, & w(E/F^{D_{2q_1}}) &= (-1)^{q_2}(-1)^{1+\frac{q_2-1}{2}} = (-1)^{\frac{q_2-1}{2}}. \end{aligned}$$

Therefore we must have $\operatorname{rk} E/F^{C_2}$, $\operatorname{rk} E/F^{D_{2q_1}} > 0$, so $\operatorname{rk} E/F > 0$. Using the properties in Proposition 5.6, the computations of the root numbers for the subfields implies that

$$w(E/\mathbb{Q}, \sigma_1) = 1, \quad w(E/\mathbb{Q}, \sigma_2) = -1, \quad w(E/\mathbb{Q}, \sigma_\rho) = 1,$$

and in particular $w(E/\mathbb{Q}, \tau_1^{\mathfrak{g}}) = -1$ for some $\mathfrak{g} \in \operatorname{Gal}(\mathbb{Q}(\tau_1)/\mathbb{Q})$.

Example 5.16 (Additive reduction example)**.** Let $G = C_{65} \rtimes C_4$, where C_4 acts faithfully on C_{65}, as well as the subgroups C_{13} and C_5. By inducing a faithful character of order 65 from C_{65}, one obtains a faithful irreducible representation ρ of G of dimension 4 and with $\mathbb{Q}(\rho) = \mathbb{Q}(\zeta_{65})^{C_4}$. In particular one has $\mathbb{Q}(\sqrt{65}) \subset \mathbb{Q}(\rho)$. Then

$$\operatorname{Ind}_{C_4}^G \mathbb{1} \ominus \operatorname{Ind}_{C_{13}\rtimes C_4}^G \mathbb{1} \ominus \operatorname{Ind}_{C_5\rtimes C_4}^G \mathbb{1} \oplus \operatorname{Ind}_G^G \mathbb{1} \simeq \bigoplus_{\mathfrak{g}\in\operatorname{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}.$$

Therefore by Theorem 5.8, either

$$\frac{C_{E/F^{C_4}} C_{E/\mathbb{Q}}}{C_{E/F^{C_{13}\rtimes C_4}} C_{E/F^{C_5\rtimes C_4}}} \tag{***}$$

is a norm from $\mathbb{Q}(\sqrt{65})$, or $\operatorname{rk} E/F > 0$.

Suppose $p = 5$ and $E/\mathbb{Q}_p$ has additive, potentially good reduction. Further suppose that $F/\mathbb{Q}$ is an extension such that $D_5 = I_5 = C_5 \rtimes C_4$ (this is wildly ramified). Let $n = v_p(\Delta_E) < 12$. Then

- In F^{C_4} there is one prime above p with ramification degree 5 and 3 primes above p with ramification degree 20,
- In $F^{C_{13}\rtimes C_4}$ there is one prime above p with ramification degree degree 5,
- In $F^{C_5\rtimes C_4}$ there is one prime above p with ramification degree 1 and 3 primes above p with ramification degree 4.

Therefore, by Lemma 4.2(iii), the product of the minimal differential term is

$$\frac{D_{\mathfrak{P}|p}(E/F^{C_4}) D_{\mathfrak{P}|p}(E/\mathbb{Q})}{D_{\mathfrak{P}|p}(E/F^{C_{13}\rtimes C_4}) D_{\mathfrak{P}|p}(E/F^{C_5\rtimes C_4})} = \frac{5^{\lfloor 5n/12\rfloor} \cdot \left(5^{\lfloor 20n/12\rfloor}\right)^3}{5^{\lfloor 5n/12\rfloor} \left(5^{\lfloor 4n/12\rfloor}\right)^3}.$$

If $n = 2$, then this is equal to $5 \mod (\mathbb{Q}^\times)^2$. By Lemma 2.7 the Tamagawa number product is

$$\frac{T_{\mathfrak{P}|p}(E/F^{C_4}) T_{\mathfrak{P}|p}(E/\mathbb{Q})}{T_{\mathfrak{P}|p}(E/F^{C_{13}\rtimes C_4}) T_{\mathfrak{P}|p}(E/F^{C_5\rtimes C_4})} = \frac{1^2 \cdot 3^3}{1^2 \cdot 3^3} = 1 \quad \text{or} \quad \frac{1^5}{1^5} = 1.$$

We claim that 5 is not a norm from $\mathbb{Q}(\sqrt{65})$. Indeed, $5z^2 = x^2 - 65y^2$ for $x, y, z \in \mathbb{Z}$ implies that $5 = \square \pmod 1 3$, a contradiction since $\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$. Therefore the local contribution of (***) above 5 is not a norm from $\mathbb{Q}(\sqrt{65})$.

What are the local root numbers above p? By Proposition 5.3, one has

- $w(E/\mathbb{Q}_5) = (-1)^{\lfloor 10/12\rfloor} = 1$,
- $\prod_{\mathfrak{p}|p} w(E/F_{\mathfrak{p}}^{C_4}) = (-1)^{\lfloor 50/12\rfloor} \left((-1)^{\lfloor 200/12\rfloor}\right)^3 = 1$,
- $\prod_{\mathfrak{p}|p} w(E/F_{\mathfrak{p}}^{C_{13}\times C_4}) = (-1)^{\lfloor 50/12\rfloor} = 1$,
- $\prod_{\mathfrak{p}|p} w(E/F_{\mathfrak{p}}^{C_5\times C_4}) = (-1)^{\lfloor 10/12\rfloor} \left((-1)^{\lfloor 40/12\rfloor}\right)^3 = -1$.

Hence we see a change in the contributions of local root numbers above p in the intermediate subfields.

6 Norm Relations

Hopefully the last section will have convinced the reader that knowledge of representation theory of finite groups G, in particular relations between permutation representations of G, has useful applications to the study of elliptic curves. Specifically, in this section we introduce some theory and notation that will help us prove general results about when we obtain norms from expressions in Theorem 5.8.

The first two subsections discuss rational representations of G, and writing these as a sum of virtual permutation representations. In the third subsection, we consider functions defined on subgroups of G, corresponding to subfields of $F/\mathbb{Q}$. Our main example of interest is the function sending $H \mapsto C_{E/F^H}$ for $H \leq G$ (when $E/\mathbb{Q}$ is an elliptic curve). We also describe *D-local functions*, which are functions that depend on a decomposition group, borrowing definitions that appear in [DD09, Section 2.iii].

We have attempted to make this section mainly representation-theoretic, in case the results within can be applied in other contexts. We assume familiarity with representations of finite groups. If necessary one can consult [Ser77].

6.1 Rational Characters and Permutation Representations

Let G be a finite group, K a number field. Denote by $\mathrm{R}_K(G)$ the group generated by characters of the representations of G over K. A representation of G is then defined over K if and only if its character is in $\mathrm{R}_K(G)$ ([Ser77, Proposition 33]). $\mathrm{R}_K(G)$ is a subring of $\mathrm{R}_{\mathbb{C}}(G)$, where $\mathrm{R}_{\mathbb{C}}(G)$ is finitely generated by the irreducible characters of G over $\mathbb{C}$. 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 $\mathrm{R}_K(G)$ with respect to the usual inner product of characters of G ([Ser77, Proposition 32]). Let m be the exponent of G. If K contains the m-th roots of unity, then $\mathrm{R}_K(G) = \mathrm{R}_{\mathbb{C}}(G)$ ([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 $\mathbb{C}[G/H] = \mathrm{Ind}_H^G \mathbb{1}$ for $H \leq G$). Let $\mathrm{Char}_{\mathbb{Q}}(G)$ be the ring of rationally valued characters of G. Then we have inclusions

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

Each of these groups have equal $\mathbb{Z}$-rank, equal to the number of conjugacy classes of cyclic subgroups of G ([Ser77, Chapter 13, §13.1]). Moreover the cokernels of these maps are finite.

Definition 6.1. Let ρ be a representation of G. We define the norm of ρ, denoted $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$, by

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) := \bigoplus_{\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}} \quad ,$$

where $\mathbb{Q}(\rho)$ is the abelian extension of $\mathbb{Q}$ generated by $\{\mathrm{Tr}\,\rho(g) \colon g \in G\}$, and $\rho^{\mathfrak{g}}$ is the representation of G such that $\mathrm{Tr}\,\rho^{\mathfrak{g}}(g) = \mathfrak{g}(\mathrm{Tr}\,\rho(g))$ for $g \in G$.

It's clear that $\mathrm{Char}_{\mathbb{Q}}(G)$ is generated by the characters of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ as ρ ranges over the complex irreducible representations of G. Indeed, if a representation has a rationally valued character, then any complex irreducible constituent must occur along with all its Galois conjugates with equal multiplicity.

Example 6.2 (The norm is not additive)**.** Let $G = C_p$ and ψ_p a character of order p. Then $\mathbb{Q}(\psi_p) = \mathbb{Q}(\zeta_p)$ and $\mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p)$ is the sum over the $p-1$ non-trivial characters of G. But $\mathfrak{N}_{\mathbb{Q}(\psi_p+\mathbb{1})/\mathbb{Q}}(\psi_p + \mathbb{1}) = \mathbb{1}^{\oplus(p-1)} + \mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p) \neq \mathfrak{N}_{\mathbb{Q}(\mathbb{1})/\mathbb{Q}}(\mathbb{1}) + \mathfrak{N}_{\mathbb{Q}(\psi_p)/\mathbb{Q}}(\psi_p)$.

Remark 6.3. The group

$$\hat{C}(G) := \frac{\mathrm{Char}_{\mathbb{Q}}(G)}{\mathrm{Perm}(G)}$$

is a finite abelian group, of exponent dividing $|G|$ (this follows from Artin's induction theorem, [Ser77, Theorem 17]). The study of this group is quite subtle. For us, it's enough to know that given a representation ρ of G, there exists a minimum integer m, depending on ρ and dividing $|G|$, such that

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m} = \bigoplus_i \operatorname{Ind}_{H_i}^G \mathbb{1} \ominus \bigoplus_j \operatorname{Ind}_{H'_j}^G \mathbb{1}$$

for some subgroups H_i, $H'_j \leq G$, i.e. that the character of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$ is in $\operatorname{Perm}(G)$. This minimum integer m is the order of the character of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$.

Example 6.4. If $G = C_n$ then $\hat{C}(G)$ is trivial (see Example 6.14).

Example 6.5. $G = Q_8$, the quaternion group, has $\hat{C}(G) = \mathbb{Z}/2\mathbb{Z}$. Let ρ be the faithful irreducible representation of G of dimension 2. Its character χ is rational and one has $\rho^{\oplus 2} = \operatorname{Ind}_{C_1}^G \mathbb{1} \ominus \operatorname{Ind}_{C_2}^G \mathbb{1}$, but one cannot write ρ as a virtual permutation representation (χ has Schur index 2 so $\chi \notin \mathrm{R}_{\mathbb{Q}}(G)$).

6.2 The Burnside Ring and Relations for Permutation Representations

Let G be a finite group. Recall that there is a bijection

$$\{\text{transitive finite } G\text{-sets } X \text{ up to isomorphism}\} \leftrightarrow \{\text{subgroups } H \leq G \text{ up to conjugacy}\}$$

given by sending a transitive finite G-set X to $H = \operatorname{Stab}_G(x)$ for some $x \in X$. The action of G on X is equivalent to the action of G on G/H.

Definition 6.6. Let $[X]$ denote the isomorphism class of a G-set X. The **Burnside ring** $\mathrm{B}(G)$ is the free abelian group on isomorphism classes of finite G-sets, modulo the relations $[S] + [T] = [S \sqcup T]$ for S, T finite G-sets. This is a ring; multiplication is given by $[S] \cdot [T] = [S \times T]$.

We only need that $\mathrm{B}(G)$ is a group, and do not use its multiplicative structure. $\mathrm{B}(G)$ is generated by $\{[X] \colon X \text{ finite transitive } G\text{-set}\}$. Using the identification of finite transitive G-sets with subgroups of G, we write elements of $\mathrm{B}(G)$ as $\sum_i n_i H_i$ for $n_i \in \mathbb{Z}$, $H_i \leq G$.

Definition 6.7. Given a G-set X, one obtains a representation of G by considering its permutation representation $\mathbb{C}[X]$. We extend this to $\mathrm{B}(G)$; given $\Theta = \sum_i n_i H_i \in \mathrm{B}(G)$, define

$$\mathbb{C}[G/\Theta] = \sum_i n_i \operatorname{Ind}_{H_i}^G \mathbb{1}.$$

Let $\chi_{\mathbb{C}[G/\Theta]}$ be the character of $\mathbb{C}[G/\Theta]$. Then $\Theta \mapsto \chi_{\mathbb{C}[G/\Theta]}$ defines a homomorphism $\mathrm{B}(G) \to \operatorname{Perm}(G)$.

Definition 6.8. If $\mathbb{C}[G/\Theta] = 0$ as a virtual permutation representation (i.e. $\chi_{\mathbb{C}[G/\Theta]} = 0$), then Θ is called a **Brauer relation**. Non-trivial Brauer relations are instances of non-isomorphic G-sets giving rise to isomorphic permutation representations.

Examples 6.9.

1. The irreducible representations of $G = S_3$ are the trivial representation $\mathbb{1}$, the sign representation ϵ and the 2-dimensional representation ρ. We have

$$\begin{aligned} \mathbb{C}[G/C_1] &= \mathbb{1} \oplus \epsilon \oplus \rho^{\oplus 2}, & \mathbb{C}[G/C_2] &= \mathbb{1} \oplus \rho, \\ \mathbb{C}[G/C_3] &= \mathbb{1} \oplus \epsilon, & \mathbb{C}[G/G] &= \mathbb{1}. \end{aligned}$$

   Then $\Psi = C_1 - 2C_2 - C_3 + 2S_3$ is the unique Brauer relation for G.

2. In Example 5.14, we observed that $\Psi = C_3 - C_6^a - C_6^b - C_6^c - 2G$ is a Brauer relation for $G = C_2 \times C_6$. This relation can be lifted from the $C_2 \times C_2$ quotient of G.

Example 6.10. Cyclic groups have no Brauer relations. Indeed, if $G = C_n$, the $\mathbb{Z}$-rank of $\mathrm{Perm}(G)$ is the number of cyclic subgroups of C_n, i.e the number of subgroups of C_n, which is the $\mathbb{Z}$-rank of $\mathrm{B}(G)$. Hence the rank of the kernel of the map $\mathrm{B}(G) \to \mathrm{Perm}(G)$ is zero.

Definition 6.11. Let ρ be a representation of G. We call $\Theta = \sum_i n_i H_i \in \mathrm{B}(G)$ a **ρ-relation** if $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, for some $m \geq 1$.

If $D \leq G$, then one can pass from virtual permutation representations of G to virtual permutation representations of D via restriction, and in the other direction via induction. We define analogous maps for the Burnside ring.

Definition 6.12. For $D \leq G$, define maps $\mathrm{Res}_D \colon \mathrm{B}(G) \to \mathrm{B}(D)$ and $\mathrm{Ind}_D \colon \mathrm{B}(D) \to \mathrm{B}(G)$ by

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

These correspond to the representation theory side, where $\mathrm{Res}_D \mathrm{Ind}_H^G \mathbb{1} = \sum_{x \in H\backslash G/D} \mathrm{Ind}_{D\cap H^{x^{-1}}}^D \mathbb{1}$ (Mackey's decomposition, cf. [Ser77, Chapter 7, §7.3], $H^{x^{-1}} = x^{-1}Hx$), and $\mathrm{Ind}_D^G \mathrm{Ind}_H^D \mathbb{1} = \mathrm{Ind}_H^G \mathbb{1}$.

The following are some elementary properties of ρ-relations:

Proposition 6.13. *Let ρ be a representation of G, $\Theta = \sum_i n_i H_i \in \mathrm{B}(G)$ a ρ-relation. Then,*

(i) $n\Theta$ is a ρ-relation for all $n \geq 1$.

(ii) $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$ where m is a multiple of the order of the character of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$.

(iii) If $\Psi \in B(G)$ is a Brauer relation, then $\Theta + \Psi$ is also a ρ-relation.

(iv) (Projection) If $N \trianglelefteq G$ then $(N \cdot \Theta)/N = \sum_i n_i N H_i/N$ is a ρ^N-relation, viewing this relation as an isomorphism of representations of G/N.

(v) (Restriction) For $D \leq G$, $\mathrm{Res}_D \Theta$ is a $\mathrm{Res}_D \rho$-relation.

Proof. All but (iv) are clear. For (iv), observe that for $H \leq G$, $\mathbb{C}[G/H]^N \simeq \mathbb{C}[G/NH]$ as G-representations for N normal (see proof of [DD09, Theorem 2.8]). We also need to show that $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^N \simeq \mathfrak{N}_{\mathbb{Q}(\rho^N)/\mathbb{Q}}(\rho^N)^{\oplus k}$ for some $k \geq 1$. This is the case;

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^N \simeq \bigoplus_{\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} (\rho^{\mathfrak{g}})^N \simeq \bigoplus_{\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} (\rho^N)^{\mathfrak{g}} = \mathfrak{N}_{\mathbb{Q}(\rho^N)/\mathbb{Q}}(\rho^N)^{\oplus k},$$

where $k = [\mathbb{Q}(\rho) : \mathbb{Q}(\rho^N)]$. □

Example 6.14. [[Ser77, Exercise 13.1]] Let $G = C_n$. For each $d \mid n$, let $\chi_d = \mathfrak{N}_{\mathbb{Q}(\psi_d)/\mathbb{Q}}(\psi_d)$, where ψ_d is a 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. Since $C_{n/d} \trianglelefteq G$, $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G containing $C_{n/d}$ in their kernel. Thus, $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain a ψ_d-relation for each $d \mid n$:

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

Note that this is the only way of writing χ_d as a sum of permutation representations, since cyclic groups have no Brauer relations (Example 6.10). Similarly, there is a unique $\Theta \in B(G)$ such that $\mathbb{C}[G/\Theta] \simeq \chi_d^m$ for all $m \geq 1$.

6.3 Functions on the Burnside Ring and Norm Relations

In this subsection we explore functions on the Burnside ring. Consider $f\colon \mathrm{B}(G) \to A$ a multiplicative function with $f(\sum_i n_i H_i) = \prod_i f(H_i)^{n_i}$ where A is an abelian group. As in [DD09], we say that f is **representation theoretic** if f is trivial on Brauer relations. This implies that for a G-set X, f only depends on the representation $\mathbb{C}[X]$.

Example 6.15. Let $\lambda \in \mathbb{R}^\times$ and consider the function $H \mapsto \lambda^{[G:H]}$. This is trivial on Brauer relations; if $\sum_i n_i H_i$ is a Brauer relation then $\lambda^{\sum_i n_i [G:H]} = \lambda^{\dim(\oplus_i \mathbb{C}[G/H_i]^{\oplus n_i})} = 1$.

Let ρ be a representation of G. Let $\Theta \in \mathrm{B}(G)$ be a ρ-relation, with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. Let $f : \mathrm{B}(G) \to \mathbb{Q}^\times$. Since $\rho \mapsto \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ is a process analogous to taking the norm of an element of $\mathbb{Q}(\rho)$, one may then expect that $f(\Theta)$ is a norm from $\mathbb{Q}(\rho)$.

Definition 6.16. Let ρ be a representation of G, Θ a ρ-relation, and $f\colon \mathrm{B}(G) \to \mathbb{Q}^\times$. If $f(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, then we call Θ a **norm relation** for f. If $f(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every ρ-relation in $\mathrm{B}(G)$, then we say f is **trivial on ρ-relations**.

Example 6.17. Let $G = C_p$ for p an odd prime. Let ψ_p be a character of degree p, so $\mathbb{Q}(\psi_p) = \mathbb{Q}(\zeta_p)$. There is a unique ψ_p-relation given by $\Theta = C_1 - C_p$. Let $\alpha\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ be given by $\alpha(H) = [G\colon H]$. Then $\alpha(\Theta)$ is a norm relation, as $\alpha(\Theta) = p$ is the norm of $1 - \zeta_p$.

In general, showing that a ρ-relation Θ is a norm relation for f does not imply that this is the case for all possible ρ-relations. Under certain circumstances however, we can conclude as such:

Proposition 6.18. *Let ρ be a representation of G and $f\colon \mathrm{B}(G) \to \mathbb{Q}^\times$. Suppose that $f(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every Brauer relation $\Psi \in \mathrm{B}(G)$. Let $\Theta \in \mathrm{B}(G)$ be a ρ-relation, with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, where m is the order of the character of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. If Θ is a norm relation for f, then f is trivial on ρ-relations.*

Proof. Consider an arbitrary ρ-relation Θ' such that $\mathbb{C}[G/\Theta'] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus l}$ for some $l \geq 1$. Then $m \mid l$ and $\Psi = \Theta' - \frac{l}{m}\Theta$ is a Brauer relation. Thus

$$f(\Theta') = f(\Psi) \cdot f(\Theta)^{\frac{l}{m}} \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$$

and so f is trivial on all ρ-relations. □

Example 6.19. Let $G = C_n$. Then any function $f\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ is trivial on Brauer relations since G does not have any. Let ψ_d be an irreducible complex character of G of order $d \mid n$. Thus to conclude that f is trivial on ψ_d-relations, it is enough to show that the ψ_d-relation constructed in Example 6.14 is a norm relation for f.

Example 6.20. Let $E/\mathbb{Q}$ be an elliptic curve, $G = \mathrm{Gal}(F/\mathbb{Q})$ for $F/\mathbb{Q}$ a Galois extension. If H, $H' \leq G$ are conjugate subgroups, then F^H, $F^{H'}$ are isomorphic fields and so $C_{E/F^H} = C_{E/F^{H'}}$. Thus the function $C\colon H \mapsto C_{E/F^H}$ for $H \leq G$ is well-defined and extends to a multiplicative function on the Burnside ring. In later sections we will investigate when this is trivial on ρ-relations, in particular when ρ is a representation of G with $\mathbb{Q}(\rho)$ quadratic.

It appears quite difficult in general to describe the set of ρ-relations for some finite group G and representation ρ. Thus determining functions that are trivial on ρ-relations is even more difficult. As seen in Example 6.14, we at least have a better understanding of the relations when G is cyclic, and can prove the following result.

Proposition 6.21. *Let $G = C_n$. Let ρ be a representation of G with $[\mathbb{Q}(\rho)\colon \mathbb{Q}] = 2$. Consider the function $g\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ given by $H \mapsto [G : H]$. Then g is trivial on ρ-relations.*

Proof. Let $\mathfrak{f}$ be the minimum positive integer such that $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_\mathfrak{f})$. As $\mathbb{Q}(\rho)$ is quadratic, $\mathfrak{f}$ is described in Remark A.14 (it is the absolute value of the discriminant Δ of $\mathbb{Q}(\rho)$). Observe that $\mathfrak{f} \mid n$ since all characters of G are realized over $\mathbb{Q}(\zeta_n)$. Since $\hat{C}(G) = 1$ and G has no Brauer relations, by Proposition 6.18 it suffices to show that $g(\Theta)$ is a norm from $\mathbb{Q}(\rho)$ for $\Theta \in \mathrm{B}(G)$ such that $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$.

Let $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) = \sum_{d|n} a_d \chi_d$ where $a_d \in \mathbb{Z}$ and χ_d are the basis of irreducible rational representations of C_n defined in Example 6.14. Let $\Theta_d = \sum_{d'|d} \mu(d/d') \cdot C_{n/d'}$ so that $\mathbb{C}[\Theta_d] = \chi_d$, as observed in the example. Then $\mathbb{C}[G/\Theta] \simeq \mathbb{C}[\sum_{d|n} a_d \Theta_d]$ which implies that $\Theta = \sum_{d|n} a_d \Theta_d$.

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

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

On the other hand,

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

The irreducible representations of C_n over $\mathbb{Q}(\rho)$ are given by the orbits of the complex irreducible characters of C_n acted upon by $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\rho))$. Consider $d \mid n$ with $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_d)$. Recall that $\chi_d = \mathfrak{N}_{\mathbb{Q}(\psi_d)/\mathbb{Q}}(\psi_d)$, where $\mathbb{Q}(\psi_d) = \mathbb{Q}(\zeta_d)$. Let $B = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_d))$. Then $\mathbb{Q}(\rho) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$, so $BH = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The orbit of ψ_d under H is fixed by BH, hence is rational. It follows that $\langle \rho, \psi_d \rangle = \langle \rho^\sigma, \psi_d \rangle$ for σ the generator of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$. Thus $2 = [\mathbb{Q}(\rho) : \mathbb{Q}]$ divides a_d, and so $g(a_d \Theta_d) = g(\Theta_d)^{a_d} \in (\mathbb{Q}^\times)^2 \subset N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.

Thus a_d can only be odd when $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_d)$, i.e $\mathfrak{f} \mid d$. Therefore for $g(\Theta)$ to be non-square we require $\mathfrak{f} = p$ for some prime p. Then p must be odd ($|\Delta|$ cannot be 2) and $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{p^*})$. But p is a norm in $\mathbb{Q}(\sqrt{p^*})$ by Corollary A.11. □

6.3.1 D-local Functions

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*.

Example 6.22. Let F/K be a finite Galois extension of number fields and let $G = \mathrm{Gal}(F/K)$. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{q}$ a prime of F above $\mathfrak{p}$. Let $D_\mathfrak{q} \leq G$ be the corresponding decomposition group. For $H \leq G$, the number of primes in $L = F^H$ above $\mathfrak{p}$ are in one-to-one correspondence with the double cosets $H\backslash G/D_\mathfrak{q}$. This correspondence is given by sending a prime $\mathfrak{s}$ in L above $\mathfrak{p}$ to the elements of G that send $\mathfrak{q}$ to some prime above $\mathfrak{s}$.

We can use the function $f\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ given by $H \mapsto \lambda^{|H\backslash G/D_\mathfrak{q}|}$ (for $\lambda \neq \pm 1$) to describe the number of places above $\mathfrak{p}$ in any intermediate extension of F/K. But if we let $g\colon \mathrm{B}(D_\mathfrak{q}) \to \mathbb{Q}^\times$ be defined by $H \mapsto \lambda$, then

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

Therefore the value of f on any G-set X only depends on the structure of X as a $D_\mathfrak{q}$-set.

Such functions motivate the following definition:

Definition 6.23. ([DD09, Definition 2.33]) If $D \leq G$, we say a function f on $\mathrm{B}(G)$ is **D-local** if there is a function f_D on $\mathrm{B}(D)$ 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 6.24. For $G = \mathrm{Gal}(F/K)$, $\mathfrak{p}$ a place of K with decomposition group D, the function

$$H \mapsto \prod_{\mathfrak{P}|\mathfrak{p}} c_\mathfrak{P}(E/F^H)$$

is D-local, where E is an elliptic curve over K and $c_\mathfrak{P}$ is the local Tamagawa number.

Again assume that $G = \mathrm{Gal}(F/K)$ and let I, D be the inertia group and decomposition group respectively of a place v of K. Then 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 $f_w = \frac{[D:I]}{[H\cap D^x : H \cap I^x]}$. We will consider functions that depend on e and f, and so introduce the following:

Definition 6.25. [DD09, Definition 2.35] Suppose $I \lhd D < G$ with D/I cyclic, and $\psi(e, f)$ is a function of $e, f \in \mathbb{N}$. Define a function on $\mathrm{B}(G)$ by

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

This is a D-local function on $\mathrm{B}(G)$ with

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

(since $(U \cap D)/(U \cap I) \simeq UI/I$ for $U \leq D$).

Example 6.26. Let E/K have split multiplicative reduction at $\mathfrak{p}$ with $c_\mathfrak{p}(E/K) = n$. Then $c_\mathfrak{P}(E/F^H) = e_\mathfrak{P} n$ for a place $\mathfrak{P}$ of F^H above $\mathfrak{p}$. In this case the function in Example 6.24 is (D, I, en).

Proposition 6.27. *Let $D \leq G$, $N \trianglelefteq G$. Let ρ be a representation of G.*

1. *(Restriction) Suppose that $\mathbb{Q}(\rho) = \mathbb{Q}(\mathrm{Res}_D \rho)$. If $f = (D, f_D)$ and f_D is trivial on $(\mathrm{Res}_D \rho)$-relations, then f is trivial on ρ-relations.*
2. *(Projection) Suppose that $\mathbb{Q}(\rho) = \mathbb{Q}(\rho^N)$ (view ρ^N as a representation of G/N). Consider f a function on $\mathrm{B}(G)$ such that $f(H) = f_{G/N}(NH/N)$ for some function $f_{G/N}$ on $\mathrm{B}(G/N)$. If $f_{G/N}$ is trivial on ρ^N-relations, then f is trivial on ρ-relations.*

One would like to be able to say that if $f = (D, f_D)$ and f_D is trivial on $(\mathrm{Res}_D \rho)$-relations, then f is trivial on ρ-relations. But as defined, one cannot conclude this when $[\mathbb{Q}(\rho) : \mathbb{Q}(\mathrm{Res}_D \rho)] > 1$. Under some conditions however, when $\mathbb{Q}(\mathrm{Res}_D \rho) = \mathbb{Q}$, one can automatically conclude that f is trivial on ρ-relations, as in the following.

Proposition 6.28. *Let $D \leq G$. Consider a representation ρ with $[\mathbb{Q}(\rho) : \mathbb{Q}] = n$, where multiplication by n is injective on $\hat{C}(D)$. Consider $f = (D, f_D)$ a D-local function on $\mathrm{B}(G)$. Suppose that $f_D(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ for every Brauer relation $\Psi \in \mathrm{B}(D)$. Then, if $\mathbb{Q}(\mathrm{Res}_D \rho) = \mathbb{Q}$, f is trivial on ρ-relations.*

Proof. Let Θ be a ρ-relation, with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. Then

$$\mathbb{C}[D/\operatorname{Res}_D \Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\mathrm{Res}_D \rho)/\mathbb{Q}}(\mathrm{Res}_D \rho)^{\oplus mn}$$

so that the character of $\mathfrak{N}_{\mathbb{Q}(\mathrm{Res}_D \rho)/\mathbb{Q}}(\mathrm{Res}_D \rho)^{\oplus mn}$ is in $\mathrm{Perm}(D)$. The condition on n ensures that the character of $\mathfrak{N}_{\mathbb{Q}(\mathrm{Res}_D \rho)/\mathbb{Q}}(\mathrm{Res}_D \rho)^{\oplus m}$ is in $\mathrm{Perm}(D)$, i.e. that there exists $\Theta' \in \mathrm{B}(D)$ with $\mathbb{C}[D/\Theta'] \simeq \mathfrak{N}_{\mathbb{Q}(\mathrm{Res}_D \rho)/\mathbb{Q}}(\mathrm{Res}_D \rho)^{\oplus m}$. Then $\Psi = \mathrm{Res}_D \Theta - n\Theta'$ is a Brauer relation for D. Thus

$$f(\Theta) = f_D(\mathrm{Res}_D \Theta) = f_D(\Psi) f_D(n\Theta') = f_D(\Psi) f_D(\Theta')^n \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times),$$

since $f_D(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$ and $(\mathbb{Q}^\times)^n \subset N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. □

Sometimes we don't need our functions to be trivial on ρ-relations, but require that they give norms from quadratic subfields of $\mathbb{Q}(\rho)$ when evaluated on ρ-relations. The following proposition shows when this holds for certain D-local functions.

Proposition 6.29. *Let G be a group and ρ a representation of G. Consider $f = (D, f_D)\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ for $D \leq G$. Suppose that $f_D(\Theta) \in (\mathbb{Q}^\times)^2$ for all Brauer relations $\Theta \in \mathrm{B}(D)$, and $\hat{C}(D)$ has odd order.*

Then, if $f_D(\Psi')$ is a norm from every quadratic subfield of $\mathbb{Q}(\mathrm{Res}_D \rho)$ for every $(\mathrm{Res}_D \rho)$-relation $\Psi' \in \mathrm{B}(D)$, it follows that $f(\Psi)$ is a norm from every quadratic subfield of $\mathbb{Q}(\rho)$ for every ρ-relation Ψ.

Proof. If $\mathbb{Q}(\rho)$ has no quadratic subfields, there is nothing to prove, so assume it has least one.

First suppose that there is a quadratic subfield $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\rho)$ such that $\mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\mathrm{Res}_D \rho) = \mathbb{Q}$. Then $[\mathbb{Q}(\rho) : \mathbb{Q}(\mathrm{Res}_D \rho)]$ is even since $\mathbb{Q}(\mathrm{Res}_D \rho)(\sqrt{d}) \subset \mathbb{Q}(\rho)$. Then, if $\Psi \in \mathrm{B}(G)$ is a ρ-relation, one has that $\mathbb{C}[D/\mathrm{Res}_D \Psi] \simeq \mathfrak{N}_{\mathbb{Q}(\mathrm{Res}_D \rho)/\mathbb{Q}}(\mathrm{Res}_D \rho)^{\oplus \alpha}$ where α is even. Applying the same computation as in Proposition 6.28, one has $f(\Psi) = f_D(\mathrm{Res}_D \Psi) \in (\mathbb{Q}^\times)^2$, hence is the norm of an element of every quadratic subfield of $\mathbb{Q}(\rho)$.

On the other hand, if $\mathbb{Q}(\mathrm{Res}_D \rho)$ contains all the quadratic subfields of $\mathbb{Q}(\rho)$ then $f(\Psi) = f_D(\mathrm{Res}_D \Psi)$ is a norm from every quadratic subfield of $\mathbb{Q}(\rho)$ by assumption. □

The following is an example of when constant D-local functions are squares when evaluated on ρ-relations.

Proposition 6.30. *Let $D \leq G$ with D of odd order, and $f = (D, \alpha)$ a D-local function on $\mathrm{B}(G)$, where $\alpha \in \mathbb{Q}^\times$ is constant. Let ρ be a representation of G with $[\mathbb{Q}(\rho) : \mathbb{Q}]$ even. Then for a ρ-relation Θ, $f(\Theta) \in (\mathbb{Q}^\times)^2$.*

Proof. The function (D, α) on $\mathrm{B}(G)$ sends $H \leq G$ to $\alpha^{|H\backslash G/D|}$. Let $\Theta = \sum_i n_i H_i$ be a ρ-relation with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$ for some $m \geq 1$. Then

$$(D, \alpha)(\Theta) = \alpha^{\sum_i n_i \cdot |H_i\backslash G/D|}.$$

We show that $\sum_i n_i \cdot |H_i\backslash G/D|$ is even.

One has $\mathrm{Res}_D \Theta = \sum_i n_i \sum_{x \in H_i\backslash G/D} D \cap H_i^{x^{-1}}$, and $\mathbb{C}[D/\mathrm{Res}_D \Theta]$ has even dimension, since it is isomorphic to $\sum_{\mathfrak{g} \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \mathrm{Res}_D \rho^{\mathfrak{g}}$, which has dimension $[\mathbb{Q}(\rho) \colon \mathbb{Q}] \cdot \dim(\mathrm{Res}_D \rho)$. The dimension is

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

Since each $[D : D \cap H_i^{x^{-1}}]$ is odd, this implies there are an even number of terms in the summation, i.e. that $\sum_i n_i \cdot |H_i\backslash G/D|$ is even.

□

7 Preliminary Results

As we discussed in Section 5, our motivation is to use Theorem 5.8 to predict points of infinite order for families of elliptic curves. However, in Sections 8 and 9 we prove that in the theorem will never make such a prediction with the group is either cyclic or has odd order. In other words, in such cases, and after fixing some representation ρ of the Galois group, the product

$$\frac{\prod_i C_{E/F_i}}{\prod_j C_{E/F'_j}} \tag{1}$$

arising from a ρ-relation is always a norm from every subfield $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$. The aim of this section is to introduce some more useful notation and important results that will be used throughout in the next sections, where the main results of the document are proven. The results are number theoretic in nature, and we exhibit two technical consequences of these results on elliptic curves.

7.1 Expressing Local Data as Functions on the Burnside Ring

We extend the notation introduced in Notation 5.9 by defining functions on $\mathrm{B}(G)$.

Notation 7.1. If $G = \mathrm{Gal}(F/K)$ then for $\mathfrak{p} \in K$ we define functions $T_{\mathfrak{P}|\mathfrak{p}}$, $D_{\mathfrak{P}|\mathfrak{p}}$ and $C_{\mathfrak{P}|\mathfrak{p}}$ on $\mathrm{B}(G)$ by

$$T_{\mathfrak{P}|\mathfrak{p}}(H) = T_{\mathfrak{P}|\mathfrak{p}}(E/F^H), \quad D_{\mathfrak{P}|\mathfrak{p}}(H) = D_{\mathfrak{P}|\mathfrak{p}}(E/F^H), \quad C_{\mathfrak{P}|\mathfrak{p}}(H) = C_{\mathfrak{P}|\mathfrak{p}}(E/F^H),$$

as defined in Notation 5.9. Note that if H, H' are conjugate then F^H, $F^{H'}$ are isomorphic, and so the values of these functions are constant on conjugate subgroups, hence they are well-defined. When $K = \mathbb{Q}$ we write p instead of $\mathfrak{p}$.

Define the global contributions $C\colon \mathrm{B}(G) \to \mathbb{Q}^\times$, $T\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ and $D\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ by

$$C(H) = C_{E/F^H}, \quad T(H) = T(E/F^H), \quad D(H) = D(E/F^H).$$

Of course one then has $C = T \cdot D = \prod_{\mathfrak{p}} C_{\mathfrak{P}|\mathfrak{p}}$, ranging over the primes $\mathfrak{p}$ of K.

Remark 7.2. Note that $C_{\mathfrak{P}|p}$ is a D_p-local function. Indeed, suppose $D_p = \mathrm{Gal}(F_w/\mathbb{Q}_p)$, where F_w denotes the completion of F with respect to a place w lying above p. For a number field K and place v, define

$$C_v(E/K) = c_v(E/K) \cdot \left|\omega/\omega_v^{\min}\right|_v.$$

We use the same notation if K is a local field (then the v subscript holds no meaning). One has

$$C_{\mathfrak{P}|p} = (D_p, C_v)$$

where C_v is a function on $\mathrm{B}(D_p)$ sending $H \mapsto C_v(E/F_w^H)$.

The following proposition describes these functions in the language introduced in Section 6.3 for each reduction type of $E/\mathbb{Q}$. We do not attempt to write a formula for $T_{\mathfrak{P}|p}$ in the case of additive reduction, computing this involves using Lemma 2.7.

Proposition 7.3. *Let $E/\mathbb{Q}$ be an elliptic curve, $G = \mathrm{Gal}(F/\mathbb{Q})$ and p a prime of $\mathbb{Q}$. Let $n = v_p(\Delta_E)$. Consider the functions $C_{\mathfrak{P}|p}$, $T_{\mathfrak{P}|p}$, and $D_{\mathfrak{P}|p}$ on $\mathrm{B}(G)$ defined above. Then,*

(i) If $E/\mathbb{Q}_p$ has good reduction, $C_{\mathfrak{P}|p} = 1$,

(ii) If $E/\mathbb{Q}_p$ has split multiplicative reduction then $C_{\mathfrak{P}|p} = T_{\mathfrak{P}|p} = (D_p, I_p, en)$,

(iii) If $E/\mathbb{Q}_p$ has non-split multiplicative reduction, $C_{\mathfrak{P}|p} = T_{\mathfrak{P}|p} = \left(D_p, I_p, \begin{cases} 2 & 2|en, 2\nmid f, \\ en & 2|f, \\ 1 & else \end{cases}\right)$,

(iv) If $E/\mathbb{Q}_p$ has potentially good reduction and $p \neq 2, 3$, $D_{\mathfrak{P}|p} = (D_p, I_p, p^{f\lfloor en/12 \rfloor})$,

(v) If $E/\mathbb{Q}_p$ has potentially multiplicative reduction and $p \neq 2, 3$, $D_{\mathfrak{P}|p} = (D_p, I_p, p^{f\lfloor e/2 \rfloor})$.

Proof.

(i) Clear.

(ii) Lemma 4.2(i) implies $D_{\mathfrak{P}|p} = 1$. If $K'/\mathbb{Q}_p$ is a finite extension of ramification degree e, then E/K' has split multiplicative reduction of type I_{en}, which has Tamagawa number en by Lemma 2.6.

(iii) As for split, $D_{\mathfrak{P}|p} = 1$. The description follows from applying Proposition 2.2 (iii) (non-split becomes split when the residue degree is even), and Lemma 2.6.

(iv) Follows from Lemma 4.2(ii),

(v) Follows from Lemma 4.2(iii).

□

Remark 7.4. We rephrase Theorem 5.8 in the language introduced in §6.3. 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 the order of ρ in $\hat{C}(G)$, nor the set of ρ-relations (since $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ is unchanged).

Let Θ be a ρ-relation with $\mathbb{C}[G/\Theta] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. Let $C\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ be the function sending $H \mapsto C_{E/F^H}$. The theorem then states that, if Θ is not a norm relation for C when m is odd, or if $C(\Theta) \notin (\mathbb{Q}^\times)^2$ for m even, then $\operatorname{rk} E/F > 0$.

7.2 Number Theoretic Results

In Sections 8 and Sections 9, we will require some number theoretic results, and in this subsection we discuss some of them. The remaining ones can be found in the Appendix, and we encourage the reader to visit them when they are needed later on. Here we describe the quadratic subfields of certain cyclotomic extensions and prove a couple of results that are naturally phrased in terms of local fields and that have direct consequences on Type II and II* elliptic curves.

Lemma 7.5. *Let q be an odd rational prime, n, m a positive integers and let $q^* = (-1)^{(q-1)/2}q$. Then the following holds.*

Cyclotomic field	Conditions	Quadratic subfields
$\mathbb{Q}(\zeta_{q^n})$	any n	$\mathbb{Q}(\sqrt{q^*})$
$\mathbb{Q}(\zeta_{2^m})$	$m = 1$	none
	$m = 2$	$\mathbb{Q}(i)$
	$m \geq 3$	$\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})$
$\mathbb{Q}(\zeta_{2^m q^n})$	$m = 1$, any n	$\mathbb{Q}(\sqrt{q^*})$
	$m = 2$, any n	$\mathbb{Q}(i), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{-q})$
	$m \geq 3$, any n	$\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{q}), \mathbb{Q}(\sqrt{-q}), \mathbb{Q}(\sqrt{2q}), \mathbb{Q}(\sqrt{-2q})$

Proof. Firstly, we remark that the discriminant of the field $\mathbb{Q}(\sqrt{D})$, with D squarefree is

$$\Delta(\mathbb{Q}(\sqrt{D})) = \begin{cases} D & \text{if } D \equiv 1 \pmod 4, \\ 4D & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

In addition, we also recall that $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^*$ and that a rational prime r ramifies in $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ if and only if $r \mid N$. The result follows by combining these two properties with the Galois correspondence, as we show now.

If q is odd, then $\mathrm{Gal}(\mathbb{Q}(\zeta_{q^n})/\mathbb{Q}) = (\mathbb{Z}/q^n\mathbb{Z})^* = C_{q^{n-1}(q-1)}$ is a cyclic group of even order, and therefore $\mathbb{Q}(\zeta_{q^n})$ has one unique quadratic subfield, which can only ramify at q. If $q \equiv 1 \pmod 4$, then the only such field is $\mathbb{Q}(\sqrt{q})$ and if $q \equiv 3 \pmod 4$ the only such field is $\mathbb{Q}(\sqrt{-q})$. This proves the first row.

Since $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, the second and third row are immediate. For $m \geq 3$, $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}) = (\mathbb{Z}/2^m\mathbb{Z})^* = C_2 \times C_2^{m-2}$ and therefore $\mathbb{Q}(\zeta_{2^m})$ has three quadratic subfields that can only ramify at 2. Again, it is easy to check that the only such fields are $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, as desired. Alternatively, one can also show that $\zeta_8 = (1+i)/\sqrt{2}$, which also implies the result. This proves the third row.

The remaining rows are essentially a combination of the results we have already shown. We note that $\mathrm{Gal}(\mathbb{Q}(\zeta_{2q^n})/\mathbb{Q}) = (\mathbb{Z}/2q^n\mathbb{Z})^*$ is cyclic while

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^m q^n})/\mathbb{Q}) = (\mathbb{Z}/2^m q^n\mathbb{Z})^* = (\mathbb{Z}/2^m\mathbb{Z})^* \times (\mathbb{Z}/q^n\mathbb{Z})^* = C_2 \times C_{2^{m-2}} \times C_{p^{n-1}(p-1)}.$$

Hence, $\mathbb{Q}(\zeta_{2^m p^n})$ has one unique quadratic subfield if $m = 1$ which must be $\mathbb{Q}(\sqrt{p^*})$, three quadratic subfields if $m = 2$, which must be $\mathbb{Q}(i), \mathbb{Q}(\sqrt{p}), \mathbb{Q}(\sqrt{-p})$, and seven quadratic subfields if $m \geq 3$. Since $\mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_q) \subseteq \mathbb{Q}(\zeta_{2^m q^n})$, it follows that $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_{2^m q^n})$ for $D \in \{-1, \pm 2, \pm q, \pm 2q\}$. These are seven distinct quadratic fields, so we are done. □

We now state and prove the local field theory results. The first gives a necessary divisibility condition on primes ramifying in finite extensions of number fields.

Proposition 7.6. *Let $F/\mathbb{Q}_p$ be a finite extension with residue field κ. Then there exists a tame, totally ramified Galois cyclic extension F_n of degree n over F if and only if $n \mid |\kappa^*|$.*

Proof. Assume first that $n \mid |\kappa^*|$. Then $x^n - 1$ splits in κ, and so by Hensel's lemma, since $p \nmid n$, $Q_p(\zeta_n) \subseteq F$. Therefore, if $\pi \in F$ is a uniformizer, the extension $F_n = F(\pi^{1/n})$ is the splitting field of $x^n - \pi$. Hence F_n/F is Galois, and totally tamely ramified. By Kummer theory, this is a cyclic extension.

Conversely, any tamely totally ramified extension of F of degree n is of the form $F(\pi^{1/n})$ ([Sun16, Theorem 11.9]). Such an extension is Galois if and only if $\mathbb{Q}(\zeta_n) \subseteq F$, which, together with the condition that $p \nmid n$, is equivalent to $n \mid |\kappa^*|$. □

The second result gives an explicit description of C_4 with equal ramification index and residual degree.

Lemma 7.7. *Let F/K be a finite Galois extension of local fields of characteristic 0 with residual characteristic distinct from 2 or 3 and such that $\mathrm{Gal}(F/K) = C_4$. If the ramification index and residual degree are both 2, then $F = K(\sqrt{u}, \sqrt{v\pi})$ where π is a uniformizer of K, u is a non-square unit of K and v is a non-square unit of $K(\sqrt{u})$. In particular, if ϖ is a uniformizer of F, then ϖ^2/π is a non-square unit of F.*

Proof. Let $L = F^{C_2}$ be the unique intermediate field of F/K. Since F is also the fixed field by inertia, then F/L is ramified while L/K is unramified. We recall that K has a unique unramified extension of any degree, and the unramified quadratic extension is generated by any $\sqrt{u}$ of any non-square unit of K. Hence $L = K(\sqrt{u})$ for some non-square unit, and note that π is a uniformizer of L too. Since F/L is ramified, F is either generated by $\sqrt{\pi}$ or $\sqrt{v\pi}$ for some non-square unit v of L. If $F = L(\sqrt{\pi})$, then F contains all three quadratic extensions of K, in which case $\mathrm{Gal}(F/K) = C_2 \times C_2$, a contradiction. Hence, necessarily, $F = L(\sqrt{v\pi}) = K(\sqrt{u}, \sqrt{v\pi})$ for some non-square unit v of L.

To prove the last statement, note that $\sqrt{v\pi}$ is a uniformizer of F and $(\sqrt{v\pi})^2/\pi = v$ is a non-square unit of F. Since any two uniformizers are equal up to multiplication by units, the result follows. □

7.3 Type II and II* Elliptic Curves

As mentioned earlier, we now prove two technical consequences of these results about the behaviour of Type II or II* elliptic curves over local fields K. We advise the reader to skip the proofs by now and revisit them when these results are used later.

Lemma 7.8. *Let $p \geq 5$ be a rational prime and $F_{\mathfrak{P}}/K_{\mathfrak{p}}/\mathbb{Q}_p$ be finite extensions with $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ Galois, ramified and $\mathrm{Gal}(F_{\mathfrak{P}}/K_{\mathfrak{p}}) = C_3$. Let*

$$E/\mathbb{Q}_p : y^2 = x^3 + Ax + B$$

be a minimal Weierstrass equation at $\mathfrak{p}$ with potentially good reduction. Let $n = \nu_{\mathfrak{p}}(\Delta)$ be the valuation of the minimal discriminant. If $\gcd(n, 12) = 2$, then $\sqrt{\Delta} \in K_{\mathfrak{p}}$.

Proof. The condition that E has additive reduction is equivalent to $A, B \in \mathfrak{p}$, and the condition on ramification implies that $3 \mid N(\mathfrak{p}) - 1$ by Proposition 7.6. In addition, by Lemma 4.2(b), we know that $\nu_{\mathfrak{p}}(\Delta) < 12$, so we need to consider two cases: $n = 2$ and $n = 10$, and we consider them separately. By Hensel's Lemma, $\sqrt{\Delta} \in K_{\mathfrak{p}}$ is equivalent to $\sqrt{\Delta} \in \kappa_{\mathfrak{p}}$ where $\kappa_{\mathfrak{p}}$ is the residue field of $K_{\mathfrak{p}}$. Recall that when E has this simple expression, $\Delta = -16(4A^3 + 27B^2)$.

Case $n = 2$:

In this case, $\nu_{\mathfrak{p}}(-4A^3 - 27B^2) = 2$ and this implies that $\nu_{\mathfrak{p}}(B) = 1$. Note that we also have that $A, B \in p\mathbb{Z}_p$ and therefore $\nu_p(B) = 1$ and $\nu_p(-4A^3 - 27B^2) = 2$. Let $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$ be the residue field of $\mathbb{Q}_p$. Then

$$\frac{-4A^3 - 27B^2}{p^2} \equiv -3\left(\frac{3B}{p}\right)^2 \pmod{p},$$

and hence $\sqrt{\Delta} \in \mathbb{F}_p$ if and only if $\sqrt{-3} \in K_{\mathfrak{p}}$. If $p \equiv 1 \pmod 3$, then

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = 1,$$

and hence $\sqrt{\Delta} \in \mathbb{F}_p \subseteq \kappa_{\mathfrak{p}}$. If $p \equiv 2 \pmod 3$, then from the condition that $3 \mid N(\mathfrak{p}) - 1$, it follows that the extension $\kappa_{\mathfrak{p}}/\mathbb{F}_p$ has even degree. By the uniqueness of extensions of finite fields, it follows that $\sqrt{\Delta} \pmod{\mathfrak{p}} \in \kappa_{\mathfrak{p}}$ as desired.

Case $n = 10$:

In this case, $\nu_{\mathfrak{p}}(-4A^3 - 27B^2) = 10$. When E is defined by this simple expression, then $c_4 = -48A$ and since E is assumed to have potentially good reduction, $\nu_{\mathfrak{p}}(j) = \nu_{\mathfrak{p}}(A^3/\Delta) = 3\nu_{\mathfrak{p}}(A) - 10 \geq 0$. Hence, $\nu_{\mathfrak{p}}(A^3) \geq 12$ which implies that $\nu_{\mathfrak{p}}(-27B^2) = 10$ or, equivalently, that $\nu_{\mathfrak{p}}(B) = 5$. This means that $\nu_p(B) = 5$ if $K_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified or $\nu_p(B) = 1$ if $K_{\mathfrak{p}}/\mathbb{Q}_p$ has ramification index 2. In the latter case, we have that $v_p(4A^3 + 27B^2) = 2$ and we are back to the case $n = 2$. So assume that $K_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified. Then

$$\frac{-4A^3 - 27B^2}{p^{10}} \equiv -3\left(\frac{3B}{p^5}\right)^2 \pmod{p},$$

and therefore $\sqrt{\Delta} \in \mathbb{F}_p$ if and only if $\sqrt{-3} \in K_{\mathfrak{p}}$. The remaining of the proof is identical to the case $n = 2$. □

Lemma 7.9. *Let $p \geq 5$ be a rational prime and $F_{\mathfrak{P}}/K_{\mathfrak{p}}/\mathbb{Q}_p$ be finite extensions with $F_{\mathfrak{P}}/K_{\mathfrak{p}}$ Galois, $\mathrm{Gal}(F_{\mathfrak{P}}/K_{\mathfrak{p}}) = C_4$ and ramification index and residual degree equal to 2. Let*

$$E/\mathbb{Q}_p : y^2 = x^3 + Ax + B$$

be a minimal Weierstrass equation at $\mathfrak{p}$ with potentially good reduction. Let $n = \nu_{\mathfrak{p}}(\Delta)$ be the valuation of the minimal discriminant. If $\gcd(n, 12) = 2$, then $\sqrt{B} \notin F_{\mathfrak{P}}$.

Proof. By Lemma 7.7, we know that $F_{\mathfrak{P}} = K_{\mathfrak{p}}(\sqrt{u}, \sqrt{v\pi})$ where π is a uniformizer of K, u is a non-square unit of K and v is a non-square unit of $K(\sqrt{u})$. We also note that π is a uniformizer of $K(\sqrt{u})$. Similarly to the previous proof, we need to consider the case $n = 2$ and $n = 10$.

Case $n = 2$:

In this case, $\nu_{\mathfrak{p}}(B) = 1$ and therefore $B = \mu\pi$ for some unit μ of K. Since the extension $K(\sqrt{u})/K$ is unramified of degree 2, $\mu = \lambda^2$ for some unit λ of $K(\sqrt{u})$. Therefore, if ϖ is a uniformizer of $F_{\mathfrak{P}}$, then $B/\varpi^2 = \lambda^2\pi/\varpi^2$ is a non-square unit by Lemma 7.7. In particular, $\sqrt{B} \notin F_{\mathfrak{P}}$.

Case $n = 10$: This case is solved similarly. Following the same argument as in Lemma 7.8, it follows that $\nu_{\mathfrak{p}}(B) = 5$ and hence $B = \mu\pi^5$ where μ is a unit in K and $\mu = \lambda^2$ for some unit λ in $K(\sqrt{u})$. Hence,

$$\frac{B}{\varpi^{10}} = \frac{\lambda^2\pi^5}{\varpi^{10}} = \left(\frac{\lambda\pi^2}{\varpi^4}\right)^2 \frac{\pi}{\varpi^2}$$

is a non-square unit of $F_{\mathfrak{P}}$, which implies that $\sqrt{B} \notin F_{\mathfrak{P}}$. □

8 Cyclic Extensions and Consistency with BSD

The aim of this section is to give a complete analysis of the case when F/K is a cyclic extension of number fields. We show that for any $d \geq 2$ and representation ρ of C_d, the product (1) of local factors arising from a ρ-relation is the norm of any quadratic subfield of $\mathbb{Q}(\rho)$. Firstly, we recall the following result, whose proof was covered in Example 6.14.

Lemma 8.1. *Let ρ be a representation of the cyclic group C_d. Then there is one unique relation $\Theta_\rho \in \mathrm{B}(C_d)$ such that*

$$\mathbb{C}[C_d/\Theta_\rho] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) = \bigoplus_{\mathfrak{g}\in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})} \rho^{\mathfrak{g}}.$$

In particular, if $\rho = \psi_d$ is a faithful character of C_d, then

$$\Theta_{\psi_d} = \sum_{k|d} \mu(k) C_k.$$

The main result of this section is therefore the following.

Theorem 8.2. *Let $d \geq 2$ be a positive integer and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_d$. Let ρ be a representation of C_d and let $\Theta_\rho \in \mathrm{B}(C_d)$ be such that*

$$\mathbb{C}[G/\Theta_\rho] = \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho).$$

If $E/\mathbb{Q}$ is a semistable elliptic curve at 2 and 3, then for any $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$,

$$C(\Theta_\rho) \in N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\mathbb{Q}(\sqrt{D})^\times).$$

The semistability condition on 2 and 3 is due to the lack of explicit description of Tamagawa numbers of elliptic curves over local fields of residual characteristic equal to 2 or 3. We certainly conjecture that Theorem 8.2 holds without this assumption, but we will not attempt this. The first step towards proving this result is to show that if the theorem holds for faithful characters, then it holds for arbitrary representations.

Lemma 8.3. *Suppose that Theorem 8.2 holds for faithful characters ψ_d. Then it also holds for any representation ρ of C_d.*

Proof. Firstly, we show that the theorem also holds for arbitrary characters of C_d. Let $\psi_{d'}$ be a character of C_d of order d' for some $d' \mid d$, and recall that

$$\Theta_{\psi_{d'}} = \sum_{k|d'} \mu(k) C_{dk/d'}.$$

Since $\ker \psi_{d'} = C_{d/d'}$, we can view $\psi_{d'}$ as a faithful character of $C_{d'}$. Then the result follows immediately from the theorem applied to d' and the $C_{d'}$-extension $F/F^{C_{d'}}$. Now assume that ρ is any representation of C_d. Then $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ is a rational valued representation, and the representations

$$\chi_k := \mathfrak{N}_{\mathbb{Q}(\psi_k)/\mathbb{Q}}(\psi_k)$$

for each $k \mid d$ are a basis of the rational representations. Hence, there is a unique decomposition

$$\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho) = \sum_{k|d} a_k \chi_k, \ a_k \in \mathbb{Z},$$

where which in particular implies that

$$C(\Theta_\rho) = \prod_{k|d} C(\Theta_{\psi_k})^{a_k} \equiv \prod_{\substack{k|d \\ a_k \text{ odd}}} C(\Theta_{\psi_k})^{a_k} \pmod{(\mathbb{Q}^\times)^2}.$$

Fix $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\rho)$. As in the argument of Proposition 6.21 it follows that if $\mathbb{Q}(\sqrt{D}) \nsubseteq \mathbb{Q}(\zeta_k) = \mathbb{Q}(\psi_k)$, then a_k is even. Hence if a_k is odd, then $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta_k)$. Therefore $C(\Theta_{\psi_k})$ is a norm from $\mathbb{Q}(\sqrt{D})$ whenever a_k is odd. This implies that $C(\Theta_\rho)$ is a norm from $\mathbb{Q}(\sqrt{D})$ too. This holds for all quadratic subfields of $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\rho)$, and thus Theorem 8.2 holds. □

This lemma has the advantage that it allows us to restrict our attention to faithful characters of C_d.

Notation 8.4. Given $d \geq 2$, we denote

$$\Theta_d = \sum_{k|d} \mu(k) C_k \in \mathrm{B}(C_d)$$

as the ψ_d-relation, where ψ_d is a faithful character of C_d.

Remark 8.5. Lemma 8.1 has an important consequence. Given an integer $d \geq 2$, note that a subgroup C_k appears in Θ_d if and only if $C_k \leq C_{\mathrm{rad}(d)}$. Consequently, in terms of fields, if $L_k = F^{C_{d/k}}$ is the unique intermediate field with $[L_k : \mathbb{Q}] = k$ for each $k \mid d$, then $C(\Theta_d)$ contains the local factors of L_k if and only if $L_{d/\mathrm{rad}(d)} \subseteq L_k \subseteq F$.

Following this observation, we will compute $T(\Theta_d)$ and $D(\Theta_d)$ by computing locally $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ and $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ for each prime $\mathfrak{p}$ of some conveniently chosen subfield $L_k \subseteq L_{d/\mathrm{rad}(d)}$, and then combining this local information via the formula

$$T(\Theta_d) = \prod_{\mathfrak{p}} T_{\mathfrak{P}|\mathfrak{p}}(\Theta_d) = \prod_{\mathfrak{p}} \left(\prod_{k|d} T_{\mathfrak{P}|\mathfrak{p}}(C_k)^{\mu(k)} \right), \tag{8.5}$$

and where the same equation holds for $D(\Theta_d)$.

To compute $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ for multiplicative reduction, the following notation will also be useful.

Notation 8.6. Let n be a positive integer. Let

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

Therefore, if E is an elliptic curve with multiplicative reduction at some prime $\mathfrak{p}$ of K and $n = \nu_{\mathfrak{p}}(\Delta_{E,\mathfrak{p}}^{\min})$, then $c_{\mathfrak{p}}(E/K) = n$ if the reduction is split and $c_{\mathfrak{p}}(E/K) = \tilde{n}$ if non-split.

We divide the proof of Theorem 8.2 for faithful characters into two separate 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 $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ for each finite place $\mathfrak{p}$ of K.

8.1 Odd Cyclic Extensions

For the first case, we assume that d is odd. Following the observation in Remark 8.5, we will calculate $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ for each finite place $\mathfrak{p}$ of some subfield of $F^{C_{\mathrm{rad}(d)}}$. However, before we calculate these terms explicitly for distinct cases, we prove a technical result that considerably simplifies the calculations of $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$.

Lemma 8.7. *Let q be an odd prime and L/K a Galois extension of number fields such that $\mathrm{Gal}(L/K) = C_q$, and let $\mathfrak{p}$ be a prime in K. Let $E/\mathbb{Q}$ be an elliptic curve and $\Theta_q = C_1 - C_q \in \mathrm{B}(C_q)$. Then by changing the model of E over K, and therefore by rescaling the discriminant of E, $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ does not change up to squares.*

Proof. Let Δ_E, Δ'_E be the discriminants of two models of E over K, and let $\lambda = (\Delta'_E/\Delta_E)^{1/12} \in K$. Write $D'_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ and $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ for the value usual terms using Δ_E and Δ'_E as discriminants, respectively. Then a simple calculation shows that

$$D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = \frac{\prod_{\mathfrak{P}|\mathfrak{p}} |\lambda|_{\mathfrak{P}}}{|\lambda|_{\mathfrak{p}}} D'_{\mathfrak{P}|\mathfrak{p}}(\Theta_q).$$

Hence, the result will follow by showing that $\prod_{\mathfrak{P}|\mathfrak{p}} |\lambda|_{\mathfrak{P}}/|\lambda|_{\mathfrak{p}} \in (\mathbb{Q}^\times)^2$.

There are three cases, depending on the splitting behaviour of $\mathfrak{p}$ in F.

- If $\mathfrak{p}$ splits, then there are q primes above $\mathfrak{p}$ with the same residue field and normalized valuation. Hence $\prod_{\mathfrak{P}|\mathfrak{p}} |\lambda|_{\mathfrak{P}} = |\lambda|_{\mathfrak{p}}^q$.
- If $\mathfrak{p}$ is inert, then there is one prime $\mathfrak{P}$ above $\mathfrak{p}$ whose residue field is a degree q extension and with the same normalized valuation. Hence $|\lambda|_{\mathfrak{P}} = |\lambda|_{\mathfrak{p}}^q$.
- If $\mathfrak{p}$ ramifies, then there is one prime $\mathfrak{P}$ above $\mathfrak{p}$, with equal residue field but with normalized valuation satisfying $\nu_{\mathfrak{P}}(\lambda) = q\mu_{\mathfrak{p}}(\lambda)$. Hence $|\lambda|_{\mathfrak{P}} = |\lambda|_{\mathfrak{p}}^q$ too.

Hence, we always have that $\prod_{\mathfrak{P}|\mathfrak{p}} |\lambda|_{\mathfrak{P}}/|\lambda|_{\mathfrak{p}} = |\lambda|_{\mathfrak{p}}^{q-1} \in (\mathbb{Q}^\times)^2$ □

The great advantage of this result is that once a prime $\mathfrak{p}$ has been chosen in some subfield of $F^{C_{\mathrm{rad}(d)}}$, we will be able to assume that $\Delta_E = \Delta_{E,\mathfrak{p}}^{\min}$.

To prove Theorem 8.2 for odd d, we first calculate $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ for simple cases, and then we use them to prove the general case. The following lemmas build on this idea.

Lemma 8.8. *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. If $\Theta_q = C_1 - C_q$, then*

$$C(\Theta_q) = \frac{C_{E/F}}{C_{E/K}}$$

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

Proof. Fix some prime $\mathfrak{p}$ in K, and assume that $\Delta_E = \Delta_{E,\mathfrak{p}}^{\min}$. We calculate $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ depending on the reduction type of $\mathfrak{p}$. Primes $\mathfrak{p}$ of good reduction yield no non-trivial factors since $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = 1$. Hence, we may only consider from now on primes of bad reduction. We also note 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 $f_{\mathfrak{p}}$.

If $\mathfrak{p}$ has multiplicative reduction, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = 1$ and Table 1 records $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ depending on $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$, where 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 2.2 and Lemmas 2.6 and 2.7. We also use Notation 8.6.

$e_{\mathfrak{p}}$	$f_{\mathfrak{p}}$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_q)$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_1)$	$T_{\mathfrak{P}\|\mathfrak{p}}(\Theta_q)$
1	1	$n;\tilde{n}$	$n^q;\tilde{n}^q$	□
q	1	$n;\tilde{n}$	$qn;\tilde{n}$	q□;□
1	q	$n;\tilde{n}$	$n;\tilde{n}$	□

Table 1: Contribution of semistable reduction primes in a C_q extension.

Since q is indeed a norm from $\mathbb{Q}(\sqrt{q^*})$ by Lemma A.11, it follows that $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ 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, $p \neq 2, 3$. We note that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = 1$ 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, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) \in (\mathbb{Q}^\times)^2$, 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 Proposition 7.6, it follows that $q \mid p^s - 1$ and therefore

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

Therefore, p splits in $\mathbb{Q}(\sqrt{q^*})$ and by Corollary A.12, it follows that p is a norm from $\mathbb{Q}(\sqrt{q^*})$.

Finally, we compute $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$. Note that since q is odd, any residue degree is odd and therefore if $\mathfrak{P}$ is any prime in F above $\mathfrak{p}$, $\sqrt{D} \in K_\mathfrak{p}$ if and only if $\sqrt{D} \in L_\mathfrak{P}$ for any $D \in \mathbb{Q}$. Moreover, if $q \neq 3$, then $\gcd(e_{\mathfrak{P}|\mathfrak{p}}, 12) = 1$ and by Lemma 2.7, $c_\mathfrak{p}(E/K) = c_\mathfrak{P}(E/F)$. This implies that

$$T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = c_\mathfrak{p}(E/K)^{\#\{\mathfrak{P}|\mathfrak{p}\}-1} \in (\mathbb{Q}^\times)^2$$

since the number of primes $\mathfrak{P}$ in L above $\mathfrak{p}$ is odd. If $q = 3$ and $\mathfrak{p}$ is unramified in L/K, then $e_{\mathfrak{P}|\mathfrak{p}} = 1$ and the same reasoning shows that $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q) = 1$. Hence, assume $L_\mathfrak{P}/K_\mathfrak{p}$ is ramified and let $n = \nu_\mathfrak{p}(\Delta_{E,\mathfrak{p}}^{\min})$ be the valuation of the minimal discriminant of E at $\mathfrak{p}$. By Lemma 2.7, we can obtain factors of 2 and 3. Since 3 is a norm from $\mathbb{Q}(\sqrt{-3})$, we only need to take care of the factors of 2, which can only arise if $F_\mathfrak{P}/K_\mathfrak{p}$ is ramified, $\gcd(n, 12) = 2$ and $\sqrt{\Delta} \notin K_\mathfrak{p}$. However, Lemma 7.8 shows that these conditions cannot arise, and therefore $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_q)$ is a norm from $\mathbb{Q}(\sqrt{-3})$ as desired. □

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

Lemma 8.9. *Let q, r be distinct, odd rational primes and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{qr}$ and let $L_k = F^{C_{qr/k}}$ be the intermediate subfields such that $[L_k : K] = k$. Let $E/\mathbb{Q}$ be an elliptic curve with semistable reduction at 2 and 3 and let $\Theta_{qr} = C_{qr} - C_q - C_r + C_1 \in \mathrm{B}(C_{qr})$. Then*

$$C(\Theta_{qr}) = \frac{C_{E/F}C_{E/K}}{C_{E/L_q}C_{E/L_r}} \in (\mathbb{Q}^\times)^2.$$

Proof. The idea of the proof is identical to Lemma 8.8 since in a C_{qr} 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 $f_\mathfrak{p}$. Fix some prime $\mathfrak{p}$ in K and assume that $\Delta_E = \Delta_{E,\mathfrak{p}}^{\min}$. If $\mathfrak{p}$ has multiplicative reduction, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr}) = 1$, and Table 2 records the Tamagawa numbers depending on $e_\mathfrak{p}$ and $f_\mathfrak{p}$, and again the entries for split and non-split multiplicative reduction of type I_n are separated by ";".

$e_\mathfrak{p}$	$f_\mathfrak{p}$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_{qr})$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_r)$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_q)$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_1)$	$T_{\mathfrak{P}\|\mathfrak{p}}(\Theta_{qr})$
1	1	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$n^r;\tilde{n}^r$	$n^{qr};\tilde{n}^{qr}$	□
1	q	$n;\tilde{n}$	$n;\tilde{n}$	$n^r;\tilde{n}^r$	$n^r;\tilde{n}^r$	□
1	r	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$n;\tilde{n}$	$n^q;\tilde{n}^q$	□
1	qr	$n;\tilde{n}$	$n;\tilde{n}$	$n;\tilde{n}$	$n;\tilde{n}$	□
q	1	$n;\tilde{n}$	$qn;\tilde{n}$	$n^r;\tilde{n}^r$	$q^r n^r;\tilde{n}^r$	□
q	r	$n;\tilde{n}$	$qn;\tilde{n}$	$n;\tilde{n}$	$qn;\tilde{n}$	□
r	1	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$rn;\tilde{n}$	$r^q n^q;\tilde{n}^q$	□
r	q	$n;\tilde{n}$	$n;\tilde{n}$	$rn;\tilde{n}$	$rn;\tilde{n}$	□
qr	1	$n;\tilde{n}$	$qn;\tilde{n}$	$rn;\tilde{n}$	$qrn;\tilde{n}$	□

Table 2: Contribution of multiplicative reduction primes in a C_{qr} extension.

Assume instead that $\mathfrak{p}$ has additive reduction. It is straightforward to check that $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr})$ is a rational square. Indeed, since q and r are distinct odd primes, we may assume that $q \neq 3$. In that case, both L_q/K and F/L_r are C_q extensions, and from the proof of Lemma 8.8, $T_{\mathfrak{P}|\mathfrak{p}}(C_{qr} - C_r), T_{\mathfrak{P}|\mathfrak{p}}(C_q - C_1) \in (\mathbb{Q}^\times)^2$.

To compute $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr})$, we let $n = \nu_\mathfrak{p}(\Delta_{E,\mathfrak{p}}^{\min})$, and we note that if $\mathfrak{p}$ is unramified in F/K, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr}) = 1$, so we assume that $\mathfrak{p}$ does indeed ramify. Suppose first that $e_\mathfrak{p} = q$, so $\mathfrak{p}$ is unramified in L_r/K. A simple calculation shows that

$$D_{\mathfrak{P}|\mathfrak{p}}(C_q) = D_{\mathfrak{P}|\mathfrak{p}}(C_{qr}) = 1, \quad D_{\mathfrak{P}|\mathfrak{p}}(C_r) = N(\mathfrak{p})^{\lfloor \frac{qn}{12} \rfloor} \quad \text{and} \quad D_{\mathfrak{P}|\mathfrak{p}}(C_1) = N(\mathfrak{p})^{r\lfloor \frac{qn}{12} \rfloor},$$

and therefore $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr}) = N(\mathfrak{p})^{(r-1)\lfloor \frac{qn}{12} \rfloor} \in (\mathbb{Q}^\times)^2$. The case $e_\mathfrak{p} = r$ is analogous. Finally, if $\mathfrak{p}$ ramifies everywhere, then a similar calculation shows that

$$D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr}) = N(\mathfrak{p})^{\lfloor \frac{pqn}{12} \rfloor - \lfloor \frac{pn}{12} \rfloor - \lfloor \frac{qn}{12} \rfloor}.$$

This may seem promising; but nevertheless the parity of the exponent only depends on q, r, n modulo 12, and for $q, r \in \{1, 5, 7, 11\}$ (they are odd primes) and $n \in \{2, 3, 4, 6, 8, 9, 10\}$ (the valuation of the minimal discriminant must be relatively prime to 12) the exponent is always even. Hence, $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{qr}) \in (\mathbb{Q}^\times)^2$, and we are done.

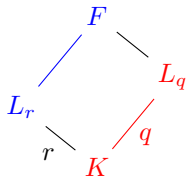


Figure 1: Subfields of a C_{pq}-extension

Again, the result follows immediately from the table and (8.5).

□

We are finally ready to prove the main result of this section, from which Theorem 8.2 will follow.

Lemma 8.10. *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 with semistable reduction at 2 and 3 and let L_k be the intermediate fields such that $\mathrm{Gal}(F/L_k) = C_{d/k}$. If*

$$\Theta_d = \sum_{k|d} \mu(k) C_k \in \mathrm{B}(C_d),$$

then $C(\Theta_d) \in (\mathbb{Q}^\times)^2$.

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 8.9. Assume that the result holds for squarefree cyclic Galois extensions with $n-1$ prime factors and consider the two sets of subgroups

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

which are clearly a partition of subgroups of C_d. Furthermore, the fields $\{F^{C_k} : C_k \in \mathscr{A}\}$ are precisely the intermediate fields of $L_{d/p_n}/K$, while the fields $\{F^{C_k} : C_k \in \mathscr{B}\}$ are the intermediate fields of F/L_{p_n}. Let

$$\Theta_{\mathscr{A}} = \sum_{H \in \mathscr{A}} \mu(|H|/p_n) H \quad \text{and} \quad \Theta_{\mathscr{B}} = \sum_{H \in \mathscr{B}} \mu(|H|) H$$

and we note that

$$\Theta_d = \sum_{k|d} \mu(k) C_k = \sum_{p_n \nmid k | d} \mu(|C_k|) C_k - \sum_{p_n | k | d} \mu(|C_k|/p_n) C_k = \Theta_{\mathscr{B}} - \Theta_{\mathscr{A}}. \tag{8.10}$$

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} that $C(\Theta_{\mathscr{A}}), C(\Theta_{\mathscr{B}}) \in (\mathbb{Q}^\times)^2$, and therefore

$$C(\Theta_d) = \frac{C(\Theta_{\mathscr{B}})}{C(\Theta_{\mathscr{A}})} \in (\mathbb{Q}^\times)^2,$$

as desired. □

The proof of Theorem 8.2 for odd d is now straightforward.

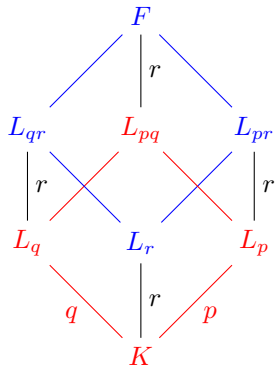


Figure 2: Partition of $n = 3$ into $n = 2$. Red fields are in $\mathscr{A}$ while blue fields are in $\mathscr{B}$.

Proof of Theorem 8.2 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 $\operatorname{rad}(d)$ is a squarefree **composite** number. Then $\Theta_d = \sum_{k|d} \mu(k) C_k \in \mathrm{B}(C_d)$ is the ψ_d-relation of a faithful character of C_d. The subgroups appearing on Θ_d are the subgroups of $C_{\operatorname{rad}(d)}$ and therefore by Lemma 8.10 applied to the $C_{\operatorname{rad}(d)}$ extension $F/F^{C_{\operatorname{rad}(d)}}$, it follows that $C(\Theta_d) \in (\mathbb{Q}^\times)^2$, and hence it is the norm of an element for any quadratic extension of $\mathbb{Q}$.

If $d = q^n$ for some odd prime q and $n \geq 1$, then Lemma 8.1 shows that $\Theta_d = C_1 - C_q$ is the ψ_d-relation of a faithful character of C_d. Lemma 8.8 applied to the C_q extension F/F^{C_q} proves that

$$C(\Theta_d) = \frac{C(C_1)}{C(C_q)} \in N_{\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}}(\mathbb{Q}(\sqrt{q^*})^\times).$$

By Lemma 7.5 this is the only quadratic subfield of $\mathbb{Q}(\zeta_{q^n})$, so the result follows. □

8.2 Even Cyclic Extensions

More care is required to prove Theorem 8.2 for even d. This difficulty mainly lies in the case when d is only divisible by one odd prime q. Consequently, we break down the proof into three distinct cases according to the number of odd prime divisors of d. If d has more than one odd prime divisor, then the result follows without much work from Lemma 8.10, so we prove this first.

Proof of Theorem 8.2 for even d with more than one odd prime divisor. By Remark 8.5, recall that the subgroups present in Θ_d are precisely those such that $C_k \leq C_{\operatorname{rad}(d)}$, and so following a similar idea to Lemma 8.10, we define

$$\mathscr{A} = \{C_k : 2 \mid k \mid \operatorname{rad}(d)\} \quad \text{and} \quad \mathscr{B} = \{C_k : 2 \nmid k \mid \operatorname{rad}(d)\},$$

together with

$$\Theta_{\mathscr{A}} = \sum_{H \in \mathscr{A}} \mu(|H|/2) H \quad \text{and} \quad \Theta_{\mathscr{B}} = \sum_{H \in \mathscr{B}} \mu(|H|) H.$$

For each $k \mid d$, let $L_k = F^{C_{d/k}}$ be the unique subfield of degree k over K. The fields $\{F^{C_k} : C_k \in \mathscr{A}\}$ are the intermediate fields of $L_{d/2}/L_{d/\operatorname{rad}(d)}$ and the fields $\{F^{C_k} : C_k \in \mathscr{A}\}$ are the intermediate fields of $F/L_{2d/\operatorname{rad}(d)}$. However, note that

$$\operatorname{Gal}(L_{d/2}/L_{d/\operatorname{rad}(d)}) = \operatorname{Gal}(F/L_{2d/\operatorname{rad}(d)}) = C_{\operatorname{rad}(d)/2},$$

and by assumption $\operatorname{rad}(d)/2$ is an odd number with more than one prime factor. Then Lemma 7.5 applied to $L_{d/2}/L_{d/\operatorname{rad}(d)}$ and $F/L_{2d/\operatorname{rad}(d)}$ gives $\Theta_{\mathscr{A}}, \Theta_{\mathscr{B}} \in (\mathbb{Q}^\times)^2$. The calculation in (8.10) shows that $\Theta_d = \Theta_{\mathscr{B}} - \Theta_{\mathscr{A}}$ and therefore

$$C(\Theta_d) = \frac{C(\Theta_{\mathscr{B}})}{C(\Theta_{\mathscr{A}})} \in (\mathbb{Q}^\times)^2$$

is the norm of any quadratic extension. □

If d has no odd primes factors, then $d = 2^m$ for some $m \geq 1$. With the results we have proven in Sections 7.3 and 8.1, the proof of Theorem 8.2 for this case is also fairly straightforward.

Proof of Theorem 8.2 for $d = 2^m$. If $d = 2^m$, then $\Theta_d = C_1 - C_2$ and therefore if $L = F^{C_2}$, then

$$C(\Theta_d) = \frac{C_{E/F}}{C_{E/L}}.$$

If $m = 1$, then $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ and there is nothing to prove, so assume that $m \geq 2$. As usual, we fix a prime $\mathfrak{p}$ of K of bad reduction and we compute $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$. Let $\bar{\mathfrak{p}}$ be a prime in L above $\mathfrak{p}$. If $\bar{\mathfrak{p}}$ has multiplicative reduction, then we remark that Table 1 also applies for $q = 2$, and therefore $C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_d)$ is a rational square up to factors of 2. Lemma 7.5 shows that the only subfields of $\mathbb{Q}(\zeta_{2^m})$ are $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, and since

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

it follows that $C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_d)$ is a norm from every quadratic subfield of $\mathbb{Q}(\zeta_{2^m})$.

Assume now that $\bar{\mathfrak{p}}$ has additive reduction, let $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$ be the ramification and residue degree of $\mathfrak{p}$ over L, and note that $e_{\mathfrak{p}} f_{\mathfrak{p}} \mid 2^{m-1}$. If $e_{\mathfrak{p}} f_{\mathfrak{p}} \neq 2^{m-1}$ then $g_{\mathfrak{p}} = 2^{m-1}/(e_{\mathfrak{p}} f_{\mathfrak{p}})$, the number of primes in L above $\mathfrak{p}$, is even. Since they all have the same local behaviour, it follows that $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_d) = C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_d)^{g_{\mathfrak{p}}} \in (\mathbb{Q}^\times)^2$. Hence, we might assume that $e_{\mathfrak{p}} f_{\mathfrak{p}} = 2^{m-1}$. To compute $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$, we note that if $f_{\mathfrak{p}} \neq 1$, then it is even and hence $N(\bar{\mathfrak{p}}) = N(\mathfrak{p})^{f_{\mathfrak{p}}} \in (\mathbb{Q}^\times)^2$. If $f_{\mathfrak{p}} = 1$, then $e_{\mathfrak{p}} = 2^{m-1}$ and $\mathfrak{p}$ is totally ramified in L/K, which is equivalent to being totally ramified in F/K. In this case, $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$ is a power of $N(\mathfrak{p}) = p^s$ for some rational prime p and $s \geq 1$ and by Proposition 7.6, it follows that $p^s \equiv 1 \pmod{2^m}$. If s is even, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_d) \in (\mathbb{Q}^\times)^2$ so assume it is odd. If $m = 2$, then $p \equiv 1 \pmod 4$ is a norm from $\mathbb{Q}(i)$ as desired. If $m \geq 3$, then it also follows that $p \equiv 1 \pmod 8$ since $(\mathbb{Z}/8\mathbb{Z})^* = C_2 \times C_2$. Then

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-2}{p}\right) = 1,$$

so p splits in $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Since they all have class number 1, p is a norm from all of them, as desired.

Finally, we compute $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_d)$. Since 2 is a norm of $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$, we only need to control the contribution of 3. Under the assumption that $e_{\mathfrak{p}} f_{\mathfrak{p}} = 2^{m-1}$, $\bar{\mathfrak{p}}$ is either inert or ramifies in F/L, but it can never split. If $n = \nu_{\bar{\mathfrak{p}}}(\Delta^{\min}_{E,\bar{\mathfrak{p}}})$, we can see from Lemma 2.7 that a factor of 3 can only arise if E has potentially good reduction at $\bar{\mathfrak{p}}$, $\gcd(n, 12) = 2$ and $\bar{\mathfrak{p}}$ ramifies in L/K, so assume this is the case. Then let $L' = F^{C_4}$ and $\mathfrak{p}' = \bar{\mathfrak{p}} \cap L'$, and note that E has additive reduction at $\mathfrak{p}'$. If $e_{\mathfrak{p}} \geq 2$, then $\mathfrak{p}'$ ramifies in L/L' and the valuation of the minimal discriminant at $\mathfrak{p}'$ is either $n/2$ or $(n+12)/2$. In either case, $\gcd(\nu_{\mathfrak{p}'}(\Delta^{\min}_{E,\mathfrak{p}'}), 12) = 1$, a contradiction. Hence, $e_{\mathfrak{p}} = 1$ and therefore $\mathfrak{p}'$ is inert in L/L'. But then we are precisely under the conditions of Lemma 7.9, which implies that $\sqrt{B} \notin F_{\mathfrak{P}}$, where $\mathfrak{P}$ is the unique prime in F above $\bar{\mathfrak{p}}$. Hence, $c_{\mathfrak{P}}(E/F) = 1$ and hence $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_d) \in (\mathbb{Q}^\times)^2$. We have covered all cases, and the result follows. □

The remaining of this section is therefore devoted to the case when d is divisible by one odd prime q, so $d = 2^m q^n$. Recall that the quadratic subfields of $\mathbb{Q}(\zeta_{2^m q^n})$ depend on whether $m = 1$, $m = 2$ or $m \geq 3$. Consequently, we prove three results that will be essential to prove the general version of each different case. The first covers the case $m = 1$.

Lemma 8.11. *Let q be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{2q}$ and let $L_k = F^{C_{2q/k}}$ be the intermediate fields such that $[L_k : K] = k$. Let $E/\mathbb{Q}$ be an elliptic curve and let $\Theta_{2q} = C_{2q} - C_q - C_2 + C_1 \in \mathrm{B}(C_{2q})$. Then*

$$C(\Theta_{2q}) = \frac{C_{E/F} C_{E/K}}{C_{E/L_2} C_{E/L_q}}$$

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

$e_\mathfrak{p}$	$f_\mathfrak{p}$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_{2q})$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_2)$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_q)$	$T_{\mathfrak{P}\|\mathfrak{p}}(C_1)$	$T_{\mathfrak{P}\|\mathfrak{p}}(\Theta_{2q})$
1	1	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$n^2;\tilde{n}^2$	$n^{2q};\tilde{n}^{2q}$	$\square$
1	q	$n;\tilde{n}$	$n;\tilde{n}$	$n^2;\tilde{n}^2$	$n^2;\tilde{n}^2$	$\square$
1	2	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$n;n$	$n^q;n^q$	$\square$
1	$2q$	$n;\tilde{n}$	$n;\tilde{n}$	$n;n$	$n;n$	$\square$
q	1	$n;\tilde{n}$	$qn;\tilde{n}$	$n^2;\tilde{n}^2$	$q^2n^2;\tilde{n}^2$	$q\square;\square$
q	2	$n;\tilde{n}$	$qn;\tilde{n}$	$n;n$	$qn;n$	$\square$
2	1	$n;\tilde{n}$	$n^q;\tilde{n}^q$	$2n;1$	$2^qn^q;1^q$	$\square$
2	q	$n;\tilde{n}$	$n;\tilde{n}$	$2n;1$	$2n;1$	$\square$
$2q$	1	$n;\tilde{n}$	$qn;\tilde{n}$	$2n;1$	$2qn;1$	$\square$

Table 3: Contribution of multiplicative reduction primes in a C_{2q} extension.

Proof. Similarly to the proofs of Lemma 8.8 and 8.9, let $\mathfrak{p}$ be a prime in K and assume that $\Delta_E = \Delta^{\min}_{E,\mathfrak{p}}$. The splitting behaviour of a prime $\mathfrak{p}$ in K is again determined by $e_\mathfrak{p}$ and $f_\mathfrak{p}$ and therefore if $\mathfrak{p}$ has multiplicative reduction $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q}) = 1$ and the following table records $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q})$.

Since q is a norm from $\mathbb{Q}(\sqrt{q^*})$, then $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q})$ is also a norm. Now assume that $\mathfrak{p}$ has additive reduction and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. We first consider the contribution of the Tamagawa numbers. Note that L_q/K and F/L_2 are C_q extensions and therefore $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q}) \in (\mathbb{Q}^\times)^2$ if $q \neq 3$ and a square up to factors of 3 if $q = 3$. In either case, $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q})$ is a norm from $\mathbb{Q}(\sqrt{q^*})$.

Finally, to compute $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q})$, let $n = \nu_\mathfrak{p}(\Delta^{\min}_{E,\mathfrak{p}})$ and note that all terms cancel unless $\mathfrak{p}$ ramifies in F. If $e_\mathfrak{p} = 2$, then

$$D_{\mathfrak{P}|\mathfrak{p}}(C_{2q}) = D_{\mathfrak{P}|\mathfrak{p}}(C_2) = 1, \quad D_{\mathfrak{P}|\mathfrak{p}}(C_q) = N(\mathfrak{p})^{\lfloor \frac{2n}{12} \rfloor} \quad \text{and} \quad D_{\mathfrak{P}|\mathfrak{p}}(C_1) = N(\mathfrak{p})^{q\lfloor \frac{2n}{12} \rfloor}, \tag{$\dagger$}$$

and therefore $D(\Theta_{2q}) = N(\mathfrak{p})^{(q-1)\lfloor n/6 \rfloor} \in (\mathbb{Q}^\times)^2$, a rational square. If $q \mid e_\mathfrak{p}$, then $q \mid N(\mathfrak{p}) - 1$ by Proposition 7.6, and the reasoning is now identical to Lemma 8.8. Write $N(\mathfrak{p}) = p^s$ for some $s \geq 1$ and note that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q}) \in (\mathbb{Q}^\times)^2$ if s is even. Hence, we assume that s is odd. In this case, $p = q$ if $(L_q)_\mathfrak{P}/K_\mathfrak{p}$ is wildly ramified and p splits in $\mathbb{Q}(q^*)$ if $(L_q)_\mathfrak{P}/K_\mathfrak{p}$ is tamely ramified. In either case, by Corollaries A.11 and A.12, p is a norm from $\mathbb{Q}(\sqrt{q^*})$, and hence so is $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{2q})$. The result follows again from (8.5). $\square$

Following this, we state and prove the analogous result for $m = 2$.

Lemma 8.12. *Let q be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{4q}$ and let $L_k = F^{C_{4q/k}}$ be the intermediate fields such that $[L_k : K] = k$. Let $E/\mathbb{Q}$ be an elliptic curve with semistable reduction at 2 and 3 and let $\Theta_{4q} = C_1 - C_2 - C_q + C_{2q}$. Then*

$$C(\Theta_{4q}) = \frac{C_{E/F}C_{E/L_2}}{C_{E/L_4}C_{E/L_{2q}}}$$

is a norm from $\mathbb{Q}(i), \mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. Moreover, $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ for any prime $\mathfrak{p}$ in K, and $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ unless E has additive reduction at $\mathfrak{p}$ and $\mathfrak{p}$ is totally ramified in F/K.

Proof. All fields appearing in the product are intermediate fields of F/L_2, and $\mathrm{Gal}(F/L_2) = C_{2q}$. Let $\mathfrak{p}$ be a prime in K, let $\bar{\mathfrak{p}} \mid \mathfrak{p}$ be a prime above $\mathfrak{p}$ in L_2 and let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Q}$. Assume also that $\Delta_E = \Delta^{\min}_{E,\mathfrak{p}}$. Lemma 8.11 shows that if E has multiplicative reduction over $\bar{\mathfrak{p}}$, $C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ unless $e_{\bar{\mathfrak{p}}} = q$ and $f_{\bar{\mathfrak{p}}} = 1$ over F. When this holds, $\bar{\mathfrak{p}}$ ramifies in L_{2q}/L_2 and is split in L_4/L_2, and this forces $\mathfrak{p}$ to split in L_2/K too. Hence, $\mathfrak{p} = \bar{\mathfrak{p}}\bar{\mathfrak{p}}'$ for two **distinct** primes in K that have the same local behaviour and therefore $C_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) = C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{4q})C_{\mathfrak{P}|\bar{\mathfrak{p}}'}(\Theta_{4q}) = C_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{4q})^2 \in (\mathbb{Q}^\times)^2$, as desired.

Assume now that E has additive reduction over $\bar{\mathfrak{p}}$. When $q = 3$, controlling the Tamagawa numbers is lengthy, so we leave it for the end. We calculate first $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q})$, which is 1 unless $\bar{\mathfrak{p}}$ ramifies in L/F_2 (equivalently, $\mathfrak{p}$ ramifies in L/K). If $\mathfrak{p}$ is inert in L_2/K, then $N(\bar{\mathfrak{p}}) \in (\mathbb{Q}^\times)^2$ and hence the size of all residues fields above $\mathfrak{p}$ are also squares and consequently $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ using Lemma 4.2. If $\mathfrak{p} = \bar{\mathfrak{p}}\bar{\mathfrak{p}}'$

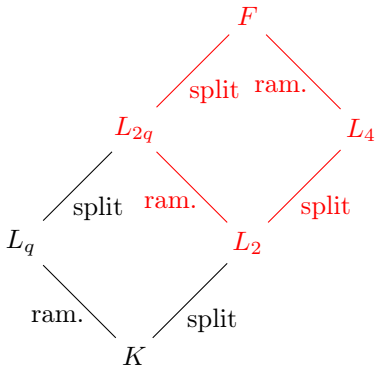


Figure 3: Field diagram for a C_{4q} extension, together with the splitting behaviour of a prime $\mathfrak{p}$ in L_2 with $e_{\mathfrak{p}} = q$ and $f_{\mathfrak{p}} = 1$ over F.

splits, then $D_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{4q}) = D_{\mathfrak{P}|\bar{\mathfrak{p}}'}(\Theta_{4q})$, and therefore $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4_q}) \in (\mathbb{Q}^\times)^2$ too. Finally, assume that $\mathfrak{p} = \bar{\mathfrak{p}}^2$ ramifies in L_2/K, which implies that $\bar{\mathfrak{p}}$ also ramifies in L_4/L_2. On the other hand, if $\bar{\mathfrak{p}}$ is unramified at L_{2q}/L_2, equation (†) during the proof of Lemma 8.11 shows that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ too.

We are therefore left with the case where $\mathfrak{p}$ is totally ramified in F/K, and Proposition 7.6 implies that $4q \mid N(\mathfrak{p}) - 1$. If we let $n = \nu_{\mathfrak{p}}(\Delta^{\min}_{E,\mathfrak{p}})$, Lemma 4.2 implies that

$$D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) = N(\mathfrak{p})^{\lfloor \frac{n}{6} \rfloor - \lfloor \frac{n}{3} \rfloor - \lfloor \frac{qn}{6} \rfloor + \lfloor \frac{qn}{3} \rfloor}.$$

Again, the parity of the expression only depends on $q, n \pmod{12}$. One can easily check that for $n \in \{2, 3, 4, 6, 8, 9, 10\}$ and $q \in \{1, 5, 7, 11\}$, the above expression is a square unless $q \equiv 3 \pmod 4$ and n is odd, so we assume this is the case. Write $N(\mathfrak{p}) = p^s$ for some $s \geq 1$, which satisfies $p^s \equiv 1 \pmod{4q}$. If s is even, then $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$, so assume that s is odd. Since $p^s \equiv 1 \pmod 4$, this implies that $p \equiv 1 \pmod 4$ and hence p is a norm from $\mathbb{Q}(i)$, which implies that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q})$ is a norm from $\mathbb{Q}(i)$ too. Furthermore, the fact that $p^s \equiv 1 \pmod{4q}$ implies that

$$\left(\frac{-q}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{p^s}{q}\right) = 1,$$

and therefore p splits both in $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. Since $q \equiv 3 \pmod 4$, both fields have odd class number (Theorem A.13), and hence p and $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q})$ are norms from $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$ as desired.

Finally, we discuss Tamagawa numbers. Note that L_{2q}/L_2 and F/L_4 are C_q extensions and therefore by Lemma 8.8 it follows that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$ if $q \neq 3$. If $q = 3$, it is also the case that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{4q}) \in (\mathbb{Q}^\times)^2$, but more work is required. We prove this as a separate lemma, from which the result follows. □

Lemma 8.13. *Let L/K be a Galois extension of number fields with $\mathrm{Gal}(L/K) = C_{12}$ and let $L_k = F^{C_{12/k}}$ be the intermediate fields such that $[L_k : K] = k$. Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathfrak{p}$ be a prime in K not dividing 2 or 3 such that E has potentially good reduction at $\mathfrak{p}$. If $\Theta_{12} = C_1 - C_2 - C_3 + C_6 \in \mathrm{B}(C_{12})$, then*

$$T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{12}) = \frac{T_{\mathfrak{P}|\mathfrak{p}}(E/F)T_{\mathfrak{P}|\mathfrak{p}}(E/L_2)}{T_{\mathfrak{P}|\mathfrak{p}}(E/L_6)T_{\mathfrak{P}|\mathfrak{p}}(E/L_4)} \in (\mathbb{Q}^\times)^2.$$

Proof. Let $\bar{\mathfrak{p}}$ be a prime in L_2 above $\mathfrak{p}$ and let $n = \nu_{\bar{\mathfrak{p}}}(\Delta^{\min}_{E,\bar{\mathfrak{p}}})$ be the minimal discriminant of E at $\bar{\mathfrak{p}}$. If $\mathfrak{p}$ is unramified in L_3/K, then so is $\bar{\mathfrak{p}}$ in L_6/L_2 and the primes above them in F/L_4. From Lemma 8.8, we know that that the product of Tamagawa numbers in unramified C_3 extensions is a square, so assume that $\mathfrak{p}$ ramifies in L_3/K.

The proof is now divided in three cases, depending on the splitting behaviour of $\mathfrak{p}$ in L_2. If $\mathfrak{p}$ splits in L_2/K, then $\mathfrak{p} = \bar{\mathfrak{p}}\bar{\mathfrak{p}}'$ where $\bar{\mathfrak{p}}$ and $\bar{\mathfrak{p}}'$ have the same local behaviour. Therefore, $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{12}) = T_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{12})T_{\mathfrak{P}|\bar{\mathfrak{p}}'}(\Theta_{12}) \in (\mathbb{Q}^\times)^2$.

Next, suppose that $\mathfrak{p}$ is inert in L_2/K, which implies that $\bar{\mathfrak{p}}$ is either inert or ramified in L_4/L_2. Let $\mathfrak{P}$ be the prime in L_4 above $\bar{\mathfrak{p}}$. If $\bar{\mathfrak{p}}$ is inert in L_4/L_2, then the valuation of the minimal discriminant of E at $\mathfrak{P}$ is also n and the splitting behaviour of $\bar{\mathfrak{p}}$ in L_6/L_2 coincides with the splitting behaviour of $\mathfrak{P}$ in F/L_4. Hence,

$$\frac{T_{\mathfrak{P}|\mathfrak{p}}(E/F)}{T_{\mathfrak{P}|\mathfrak{p}}(E/L_4)} = \frac{T_{\mathfrak{P}|\mathfrak{p}}(E/L_6)}{T_{\mathfrak{P}|\mathfrak{p}}(E/L_2)},$$

and therefore $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{12}) = 1$. The case where $\bar{\mathfrak{p}}$ is ramified in L_4/L_2 is more subtle. We have already seen that in ramified C_3 extensions we cannot obtain factors of 2. Upon inspection of Lemma 2.7, one can easily show that the Tamagawa numbers cancel out if $\gcd(n, 12) \in \{3, 4, 6, 12\}$, so we only need to consider the case $\gcd(n, 12) = 2$. Since $\mathrm{Gal}((L_4)_{\mathfrak{P}}/K_{\mathfrak{p}}) = C_4$ and $e_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{p}} = 2$, Lemma 7.9 shows that $\sqrt{B} \notin F_{\mathfrak{P}}$ and therefore $c_{\mathfrak{P}}(E/F) = 1$, which implies that $D_{\mathfrak{P}|\mathfrak{p}}(\Theta_{12}) \in (\mathbb{Q}^\times)^2$.

Finally, assume that $\mathfrak{p}$ ramifies in L_2/K so that $\mathfrak{p} = \bar{\mathfrak{p}}^2$. This immediately implies that $\bar{\mathfrak{p}}$ also ramifies in L_4/L_2, and therefore $\mathfrak{p}$ is totally ramified in F/K. As mentioned above, the Tamagawa numbers cancel unless $\gcd(n, 12) = 2$. However, recall that E has potentially good reduction at $\mathfrak{p}$, and since $\mathfrak{p} = \bar{\mathfrak{p}}^2$ ramifies, then the valuation of the minimal discriminant at $\mathfrak{p}$ is $n/2$ or $(n + 12)/2$. But then $\gcd(\nu_{\mathfrak{p}}(\Delta^{\min}_{E,\mathfrak{p}}), 12) = \gcd(n/2, 12) = 1$, a contradiction. Hence, $T_{\mathfrak{P}|\mathfrak{p}}(\Theta_{12}) \in (\mathbb{Q}^\times)^2$ as desired. □

Finally, we state and prove the last result, from which the case $m \geq 3$ follows easily. One needs to check that the product of local factors is the norm of many quadratic subfields; thankfully, Lemma 8.12 has done most of work required.

Lemma 8.14. *Let q be an odd prime and let F/K be a Galois extension of number fields such that $\mathrm{Gal}(F/K) = C_{8q}$ and let $L_k = F^{C_{8q/k}}$ be the intermediate fields such that $[L_k : K] = k$. Let $E/\mathbb{Q}$ be an elliptic curve with semistable reduction at 2 and 3 and let $\Theta_{8q} = C_1 - C_2 - C_q + C_{2q}$. Then*

$$C(\Theta_{8q}) = \frac{C_{E/F}C_{E/L_4}}{C_{E/L_8}C_{E/L_{4q}}} \in (\mathbb{Q}^\times)^2.$$

Proof. We prove the result locally for all primes in L_2, and note $\mathrm{Gal}(F/L_2) = 4q$. Let $\bar{\mathfrak{p}}$ and assume that $\Delta_E = \Delta^{\min}_{E,\bar{\mathfrak{p}}}$. Since the relation $\Theta_{4q} = C_1 - C_2 - C_q + C_{2q} \in \mathrm{B}(C_{4q})$ has the same fixed fields as Θ_{8q}, by Lemma 8.12, we know that $T_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{8q}) \in (\mathbb{Q}^\times)^2$ for any $\bar{\mathfrak{p}}$ and $D_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{8q}) \in (\mathbb{Q}^\times)^2$ too unless $\bar{\mathfrak{p}}$ is totally ramified in F/L_2 and E has potentially good reduction at $\bar{\mathfrak{p}}$, so assume this is the case. If $\mathfrak{p} = \bar{\mathfrak{p}} \cap K$, then it also follows that $\mathfrak{p}$ is totally ramified in F/K and E has potentially good reduction at $\mathfrak{p}$. If $n = \nu_{\bar{\mathfrak{p}}}(\Delta^{\min}_{E,\bar{\mathfrak{p}}})$, then recall from Lemma 8.12 that

$$D_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{8q}) = N(\bar{\mathfrak{p}})^{\lfloor \frac{n}{6} \rfloor - \lfloor \frac{n}{3} \rfloor - \lfloor \frac{qn}{6} \rfloor + \lfloor \frac{qn}{3} \rfloor},$$

and that the exponent is even unless n is odd and $q \equiv 3 \pmod 4$. However, $\mathfrak{p} = \bar{\mathfrak{p}}^2$ is ramified in L_2/K and therefore $n \equiv 2\nu_{\mathfrak{p}}(\Delta^{\min}_{E,\mathfrak{p}}) \pmod{12}$. That is, n is even and therefore $D_{\mathfrak{P}|\bar{\mathfrak{p}}}(\Theta_{8q}) \in (\mathbb{Q}^\times)^2$ as desired. □

We are now ready to prove the remaining case of Theorem 8.2.

Proof of Theorem 8.2 for d even and with one odd prime factor. In this case, write $d = 2^m q^n$ for $n, m \geq 1$ and note that $\Theta_d = C_1 - C_2 - C_q + C_{2q}$ is the ψ_d-relation of a faithful character of C_d. If $m = 1$, Lemma 8.11 applied to the C_{2q} extension $F/F^{C_{2q}}$ shows that $C(\Theta_d)$ is a norm from $\mathbb{Q}(\sqrt{q^*})$, which is the only subfield of $\mathbb{Q}(\zeta_{2q^n})$ by Lemma 7.5. If $m = 2$, then Lemma 8.12 applied to the C_{4q} extension $F/F^{C_{4q}}$ shows that $C(\Theta_d)$ is a norm from $\mathbb{Q}(i), \mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$, which are all quadratic subfields of $\mathbb{Q}(\zeta_{4q^n})$. Finally, if $m \geq 3$, Lemma 8.14 applied to $F/F^{C_{8q}}$ shows that $C(\Theta_{8q}) \in (\mathbb{Q}^\times)^2$, which is the norm from any quadratic subfield. The result follows. □

9 Odd Extensions and Consistency with BSD

In this section we prove the analogous result to the previous section when $F/\mathbb{Q}$ is any Galois extension of odd order. As discussed in §5.2, we expect our Norm Relations test to be "uninteresting" because root number computations don't predict positive rank.

Theorem 9.1. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ be an extension of odd order with Galois group G.*

Assume that E has good or multiplicative reduction at 2 and 3. Take any representation ρ of G with quadratic subfield $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\rho)$ and relation

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

as in Theorem 5.8. 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 5.8 to conclude that E/F must have positive rank.

As in Remark 7.4, replacing ρ by the sum of its conjugates by elements of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{D}))$, we may assume that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{D})$. We take $D \in \mathbb{Z}\backslash\{0,1\}$ to be squarefree.

The product of terms we are computing is $C(\Theta)$, where $C\colon \mathrm{B}(G) \to \mathbb{Q}^\times$ is given by $C\colon H \mapsto C_{E/F^H}$, and Θ is any ρ-relation. We break up the function C into $C = \prod_p C_{\mathfrak{P}|p} = \prod_p T_{\mathfrak{P}|p} \cdot D_{\mathfrak{P}|p}$, ranging over primes $p \in \mathbb{Q}$, as defined in Notation 7.1. In Remark 7.2 we showed that

$$C_{\mathfrak{P}|p} = (D_p, C_v)$$

where C_v is a function on $\mathrm{B}(D_p)$ sending $H \mapsto C_v(E/F_w^H)$, for $D_p = \mathrm{Gal}(F_w/\mathbb{Q}_p)$. The following result will allow us to apply some results from §6.3.

Theorem 9.2. *When D_p has odd order, $C_v(\Psi) \in (\mathbb{Q}^\times)^2$ for any Brauer relation $\Psi \in \mathrm{B}(D_p)$.*

Proof. This follows from [DD09, Theorem 2.47] and [DD09, Theorem 3.2 (Tam)]. □

Corollary 9.3. *It is enough to prove Theorem 9.1 when m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. Thus we need to prove that, given any $\Theta \in \mathrm{B}(G)$ such that $\mathbb{C}[\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, Θ is a norm relation for the function C.*

Proof. Since $\mathbb{Q}(\rho)$ is quadratic, we have that rational squares are norms from $\mathbb{Q}(\rho)$. As G is odd, any choice of D_p is odd. It follows from Theorem 9.2 that $C(\Psi) \in (\mathbb{Q}^\times)^2$ for all Brauer relations $\Psi \in \mathrm{B}(G)$. Therefore by Proposition 6.18, it is enough to prove Theorem 9.1 when m is the order of $\mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)$ in $\hat{C}(G)$. Then m divides $|G|$, hence is odd. □

Let τ be the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q})$. Let $\mathfrak{f}$ be the smallest integer such that $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\zeta_\mathfrak{f})$. Then $\mathfrak{f} \mid |G|$, hence is odd. By Remark A.14, $\mathfrak{f} = |D|$ and $D \equiv 1 \pmod 4$. The following shows that it is only of interest to consider decomposition groups of exponent divisible by $\mathfrak{f}$.

Corollary 9.4. *Let the exponent of D_p be b. If $\mathfrak{f} \nmid b$, then $C_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.*

Proof. One has $\mathbb{Q}(\rho) \subset \mathbb{Q}(\zeta_b) \implies \mathfrak{f} \mid b$ by minimality of $\mathfrak{f}$. Since $\mathfrak{f} \nmid b$, we have $\mathbb{Q}(\rho) \not\subset \mathbb{Q}(\zeta_b)$, so $\mathbb{Q}(\mathrm{Res}_{D_p} \rho) = \mathbb{Q}$. The corollary then follows from Proposition 6.28 and Theorem 9.2, noting that since $\hat{C}(D_p)$ is odd, multiplication by 2 is injective. □

Fix $\Theta = \sum_i n_i H_i \in \mathrm{B}(G)$ with $\mathbb{C}[\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$. We prove that at each prime p, $C_{\mathfrak{P}|p}(\Theta)$ is the norm of an element of $\mathbb{Q}(\rho)$. As observed, this depends on D_p and I_p. As we deal with each local factor individually, we argue that one can take $D_p = I_p$.

Lemma 9.5. *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 9.6. *At a prime p, we may assume that $D_p = I_p$ when computing $C_{\mathfrak{P}|p}(\Theta)$.*

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 $\mathrm{Gal}(FL/L) = G' \simeq G$. 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 9.5 $C_v(E/F_i) \equiv C_w(E/L_i) \mod (\mathbb{Q}^\times)^2$. Letting $C'_{\mathfrak{P}|p}$ be the function on $\mathrm{B}(G)$ defined as in Notation 7.1 but with $\mathbb{Q}$, F replaced by L, FL, we see that $C'_{\mathfrak{P}|p}(\Theta) \equiv C_{\mathfrak{P}|p}(\Theta) \mod (\mathbb{Q}^\times)^2$. Thus it is equivalent to do our computation in FL/L, but here p has residue degree 1. □

To prove Theorem 9.1, we proceed by computing $C_{\mathfrak{P}|p}(\Theta)$ for each reduction type.

Good reduction

If $E/\mathbb{Q}$ has good reduction at p, then by Proposition 7.3(i), $C_{\mathfrak{P}|p} = 1$.

Multiplicative reduction

Lemma 9.7. *Let $E/\mathbb{Q}_p$ have non-split multiplicative reduction. Then $C_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.*

Proof. Since $D_p = I_p$, all primes above p have residue degree 1. Moreover, the ramification degrees are always odd. Thus by Proposition 7.3(iii), $C_{\mathfrak{P}|p} = (D_p, \alpha)$ where α is the constant function on $\mathrm{B}(D_p)$ with $\alpha \in \{1, 2\}$, depending on $v_p(\Delta)$ being even or odd. By Proposition 6.30, it follows that $C_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$. □

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 $v_p(\Delta) = n$. Then by Proposition 7.3(ii),

$$C_{\mathfrak{P}|p} = (D_p, D_p, en).$$

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 Proposition 6.30 .

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 Corollary 9.4, we may consider such D_p with exponent $p^u l$ for some $u \geq 0$ such that $\mathfrak{f} \mid p^u l$. To compute $C_{\mathfrak{P}|p}(\Theta)$, we reduce to the tame quotient.

Lemma 9.8. *Let $g\colon \mathrm{B}(C_l) \to \mathbb{Q}^\times$ be defined by $H \mapsto [C_l \colon H] = \dim \mathbb{C}[C_l/H]$. Let $\Psi = P_p \cdot \mathrm{Res}_{D_p} \Theta / P_p \in \mathrm{B}(C_l)$ Then $(D_p, D_p, e)(\Theta)$ and $g(\Psi)$ differ by a (possible) factor of p.*

Proof. 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 the following isomorphism of D_p-representations

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

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

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

and we can consider these as representations of $D_p/P_p = C_l$. It follows that $(D_p, D_p, e)(\Theta)$ differs from $g(\Psi)$ up to a (possible) factor of p. □

Now we show that this factor of p is a norm from $N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. Note that if $p = 2$ then $P_p = 1$ since $|P_p| \mid |G|$ which is odd. So we only need to consider this factor of p for p odd.

Lemma 9.9. *Let $K = \mathbb{Q}(\sqrt{D})$, with $\mathfrak{f}$ the smallest positive integer such that $K \subset \mathbb{Q}(\zeta_\mathfrak{f})$. Suppose that $\mathfrak{f}$ is odd. Let $\mathfrak{f} \mid p^u l$, for some odd prime p, $u \geq 0$ and l such that $p \equiv 1 \pmod{l}$. Then p is the norm of an element from $K^\times$.*

Proof. Since $\mathfrak{f}$ is odd, one has $D = \prod_{q\mid\mathfrak{f}} q^*$, the product being taken over primes dividing $\mathfrak{f}$. 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 Corollary A.7, p is the norm of a principal fractional ideal of K, and by Theorem A.9 or Theorem A.10, it is the norm of an element of K. □

Corollary 9.10. *Let $E/\mathbb{Q}_p$ have split multiplicative reduction. Then $C_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.*

Proof. By the previous two results, it is sufficient to show that $g(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. Let $\phi = (\mathrm{Res}_{D_p}\,\rho)^{P_p}$, viewed as a representation on $D_p/P_p = C_l$. Then Ψ is a ϕ-relation. If $\mathfrak{f} \nmid l$ then $\mathbb{Q}(\phi) = \mathbb{Q}$. Therefore $\mathbb{C}[C_l/\Psi] \simeq \phi^{\oplus 2}$, implying that $\Psi = 2\Psi'$ for some $\Psi' \in \mathrm{B}(C_l)$ with $\mathbb{C}[C_l/\Psi'] = \phi$. Then $g(\Psi) = g(\Psi')^2 \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. Otherwise, suppose that $\mathbb{Q}(\phi) = \mathbb{Q}(\rho)$. It follows from Proposition 6.21 that $g(\Psi) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. □

Additive reduction

Now suppose that $E/\mathbb{Q}_p$ has additive reduction. In this case, assume that $p \geq 5$ Write $D_p = \mathrm{Gal}(F_w/\mathbb{Q}_p)$ for $w \mid p$ a place of F.

Again we have $D_p = P_p \rtimes C_l$ with $l \mid p-1$ (this follows from Proposition 7.6) , and may assume that $\mathfrak{f} \mid p^u l$ where $p^u l$ is the exponent of D_p by Corollary 9.4. Let $n = v_p(\Delta_E)$.

We will compute $D_{\mathfrak{P}|p}(\Theta)$ and $T_{\mathfrak{P}|p}(\Theta)$ separately. By Proposition 7.3(iv), (v)

$$D_{\mathfrak{P}|p} = \begin{cases} (D_p, D_p,\ p^{\lfloor e/2 \rfloor}) & \text{if } E/\mathbb{Q}_p \text{ has potentially multiplicative reduction,} \\ (D_p, D_p,\ p^{\lfloor en/12 \rfloor}) & \text{if } E/\mathbb{Q}_p \text{ has potentially good reduction.} \end{cases}$$

In either case, $D_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. Indeed, this takes values 1 or p in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. But p is a norm from $\mathbb{Q}(\rho)$ by Lemma 9.9.

To compute $T_{\mathfrak{P}|p}(\Theta)$, since $p \geq 5$ we may write $E/\mathbb{Q}_p$ as $E\colon y^2 = x^3 + Ax + B$ and use the description from [DD09] for computing Tamagawa numbers, as detailed in Lemma 2.7. The discriminant of $E/\mathbb{Q}_p$ is $\Delta = -16(4A^3 + 27B^2)$. The case of potentially multiplicative reduction is almost immediate:

Lemma 9.11 (Potentially multiplicative reduction)**.** *If $E/\mathbb{Q}_p$ has reduction type I_n^* then $T_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.*

Proof. Since we assume $D_p = I_p$, i.e. the residue degree is one, it follows that any subextension L' of $F_w/\mathbb{Q}_p$ satisfies $\sqrt{B} \in L' \iff \sqrt{B} \in \mathbb{Q}_p$ and $\sqrt{\Delta} \in L' \iff \sqrt{B} \in \mathbb{Q}_p$. Therefore $T_{\mathfrak{P}|p} = (D_p, \alpha)$ where $\alpha \in \{2, 4\}$ by Lemma 2.7. But then $(D_p, \alpha)(\Theta) \in (\mathbb{Q}^\times)^2$ by Proposition 6.30. □

Now suppose that $E/\mathbb{Q}_p$ has potentially good reduction. Recall from Lemma 2.7 that if $L'/\mathbb{Q}_p$ has ramification degree e, then the Kodaira type of E/L' depends on $\gcd(en, 12)$. Thus in a ramified extension of degree coprime to 12, the Kodaira type is unchanged, and further if this extension is totally ramified

(so the residue degree is 1), the Tamagawa number is unchanged also. Thus when $3 \nmid |D_p|$, $T_{\mathfrak{P}|p} = (D_p, \alpha)$ for some constant α. If we have type III or III* or I_0^* then the Tamagawa number is still unchanged in any totally ramified extension of odd degree extension, even when the degree is divisible by 3. Then the Proposition 6.30 implies the following lemma:

Lemma 9.12.

(i) If $E/\mathbb{Q}_p$ has potentially good reduction and $3 \nmid |D_p|$, then $T_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.
(ii) If $E/\mathbb{Q}_p$ has potentially good reduction of type III, III*, *or* I_0^*, *then $T_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.*

Thus we assume that $3 \mid |D_p|$. Since we assumed $p \geq 5$, we have $D_p = I_p = P_p \ltimes C_l$ with $3 \mid l$ and $p \equiv 1 \pmod{l}$.

Lemma 9.13. *If $E/\mathbb{Q}_p$ has Type* II *or Type* II* *additive reduction and $3 \mid |D_p|$, then $T_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$.*

Proof. If $3 \mid |D_p|$ then there is a subextension F' of $F_w/\mathbb{Q}_p$ with $\mathrm{Gal}(F_w/F') = C_3$. Then Lemma 7.8 implies that $\sqrt{\Delta} \in F'$. But $F'/\mathbb{Q}_p$ has residue degree 1, hence $\sqrt{\Delta} \in \mathbb{Q}_p$.

If $L'/\mathbb{Q}_p$ is an odd degree extension that is divisible by 3, then E/L' has reduction type I_0^*. By Lemma 2.7 the Tamagawa number of E/L' is 2 if $\sqrt{\Delta} \notin \mathbb{Q}_p$ and 1 or 4 if $\sqrt{\Delta} \in \mathbb{Q}_p$. Therefore the Tamagawa number will be 1 or 4, which is a square. On the other hand if $L'/\mathbb{Q}_p$ is an extension of odd degree then the reduction type over L' is II or II* and the Tamagawa number is 1. It follows that $T_{\mathfrak{P}|p}(\Theta)$ is a product of square terms, so is itself square. □

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 $T_{\mathfrak{P}|p}(\Theta)$, when $\sqrt{B} \notin \mathbb{Q}_p$.

Recall from the proof of Proposition 6.30 that $\mathrm{Res}_{D_p}\Theta = \sum_i n_i \sum_{x \in H_i \backslash G / D_p} D_p \cap H^{x^{-1}}$, with $\sum_i n_i |H_i \backslash G / D_p|$ even. If $D_p = \mathrm{Gal}(F_w/\mathbb{Q}_p)$, then the number of subextensions divisible by 3 (i.e. the number of subextensions where we obtain good reduction) corresponds to the number of subgroups with index divisible by 3 in $\mathrm{Res}_{D_p}\Theta$. We compute this number to determine $\mathrm{ord}_3(T_{\mathfrak{P}|p}(\Theta))$ modulo squares.

Similarly to the split multiplicative case, we may pass to the tame quotient $C_p/P_p = C_l$. Indeed

$$3 \mid [D_p : D_p \cap H^{x^{-1}}] = \dim \mathbb{C}[D_p/D_p \cap H^{x^{-1}}] \iff 3 \mid \dim \mathbb{C}[D_p/D_p \cap H^{x^{-1}}]^{P_p},$$

since $3 \nmid |P_p|$. Therefore we may compute the number of subgroups divisible by 3 in $\Psi = P_p \cdot \mathrm{Res}_{D_p}\Theta / P_p \in \mathrm{B}(C_l)$. Let $h\colon \mathrm{B}(C_l) \to \mathbb{Q}^\times$ be the function given by $H \mapsto \begin{cases} 3 & 3 \mid [C_l : H], \\ 1 & 3 \nmid [C_l : H]. \end{cases}$

Proposition 9.14. *Suppose that $E/\mathbb{Q}_p$ has additive reduction of Type* IV *or* IV*, *with $c_v(E/\mathbb{Q}_p) = 3$. Then $T_{\mathfrak{P}|p}(\Theta) \equiv h(\Psi) \pmod{(\mathbb{Q}^\times)^2}$ and $T_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$.*

Proof. The fact that $T_{\mathfrak{P}|p}(\Theta) \equiv h(\Psi) \pmod{(\mathbb{Q}^\times)^2}$ has been observed above. Let ψ_3 be an irreducible character of D_p of order 3. One has that $\langle \mathrm{Ind}_{C_{l/l'}}^{C_l} \mathbb{1}, \psi_3 \rangle = 1$ when $3 \mid l'$ and is zero when $3 \nmid l'$. Thus

$$h(\Psi) = 3^{\langle \mathbb{C}[C_l/\Psi], \psi_3 \rangle}.$$

As in the proof of Proposition 6.21, write $\mathbb{C}[C_l/\Psi] = \sum_{l' \mid l} a_{l'} \chi_{l'}$, where $\chi_{l'}$ is an irreducible rational character, of C_l with kernel of index l'. Observe that $\langle \chi_{l'}, \psi_3 \rangle = 0$ unless $l' = 3$, in which case it is 1. Therefore $h(\Psi) \equiv 3^{a_3} \pmod{(\mathbb{Q}^\times)^2}$. In the proof of Proposition 6.21, we showed that a_3 is even unless $\mathfrak{f} \mid 3$, i.e. that $\mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$. But then 3 is a norm in $\mathbb{Q}(\rho)$. Thus we see that in all cases $T_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$. □

We have observed that for all reduction types of $E/\mathbb{Q}_p$, one has $C_{\mathfrak{P}|p}(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, and so $C(\Theta) \in N_{\mathbb{Q}(\rho)/\mathbb{Q}}(\mathbb{Q}(\rho)^\times)$, completing the proof of Theorem 9.1.

□

Finally, we show how Theorem 8.2 and Theorem 9.1 yield an interesting corollary for computing $C_{\mathfrak{P}|p}$ for arbitrary groups G when the decomposition group is cyclic or of odd order.

Corollary 9.15. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G. Assume that E has good or multiplicative reduction at 2 and 3.*

Consider ρ a representation of G. Let Θ be a ρ-relation, with $\mathbb{C}[G/\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho)^{\oplus m}$, $m \geq 1$. Let $D_p \leq G$ be a cyclic group, or a group of odd order. If m is even, $C_{\mathfrak{P}|p}(\Theta) \in (\mathbb{Q}^\times)^2$. Else, $C_{\mathfrak{P}|p}(\Theta)$ is the norm of an element of every quadratic subfield of $\mathbb{Q}(\rho)$.

Proof. This result essentially follows from Proposition 6.29. Recall that $C_{\mathfrak{P}|p} = (D_p, C_v)$ by Remark 7.2. If D_p is cyclic, there are no Brauer relations in $\mathrm{B}(D_p)$ and $\hat{C}(D_p) = 1$. If D_p is odd, then $C_v(\Psi) \in (\mathbb{Q}^\times)^2$ for all Brauer relations $\Psi \in \mathrm{B}(D_p)$ by Theorem 9.2 and $\hat{C}(D_p)$ is of odd order.

Taking restriction, one has $\mathbb{C}[D_p/\operatorname{Res}_{D_p}\Theta] \simeq \mathfrak{N}_{\mathbb{Q}(\operatorname{Res}_{D_p}\rho)/\mathbb{Q}}(\operatorname{Res}_{D_p}\rho)^{\oplus m\cdot[\mathbb{Q}(\rho):\,\mathbb{Q}(\operatorname{Res}_{D_p}\rho)]}$. If m is even then $C_{\mathfrak{P}|p}(\Theta) = C_v(\operatorname{Res}_{D_p}\Theta) \in (\mathbb{Q}^\times)^2$, since there exists some $(\operatorname{Res}_{D_p}\rho)$-relation $\Theta' \in \mathrm{B}(D_p)$ with $\mathbb{C}[D_p/2\Theta'] \simeq \mathbb{C}[D_p/\operatorname{Res}_{D_p}\Theta]$.

Else, by Theorem 8.2 or Theorem 9.1, $C_v(\Theta')$ is a norm from every quadratic subfield of $\operatorname{Res}_{D_p}\rho$ for every $\big(\operatorname{Res}_{D_p}\rho\big)$-relation Θ'. The result follows by the statement of Proposition 6.29. □

Appendix A Algebraic Number Theory Background

In this section we give some results relating to the genus field of quadratic number fields, as well as other 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 modulo principal fractional 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 fractional 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 $H \subset H^+$. If K has no real places, $H^+ = H$. For quadratic fields, the index depends on the norm of a fundamental unit:

Theorem A.1. *[Jan96, Chapter VI, Theorem 3.2] Let $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}_{>0}$ square-free. 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.*

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 useful to consider the maximal subfield of H that is abelian over $\mathbb{Q}$.

Definition A.2. For any abelian extension $K/\mathbb{Q}$, the **genus field** of $K/\mathbb{Q}$ is the largest abelian extension $L/\mathbb{Q}$ contained in H. The **extended genus field** is the largest abelian extension $L^+/\mathbb{Q}$ contained in H^+.

Theorem A.3. *[Jan96, Ch. VI, §3, Theorem 3.3] Let $K = \mathbb{Q}(\sqrt{D})$. Let $\sigma \in \mathrm{Gal}(H^+/\mathbb{Q})$ be such that $\sigma|_K$ generates $\mathrm{Gal}(K/\mathbb{Q})$.*

1. *$\mathrm{Gal}(H/L)$ 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. *$\mathrm{Gal}(H/L) \simeq (C_K)^2$.*

Proof sketch of 1. Let $G = \mathrm{Gal}(H/\mathbb{Q})$. Then $L = H^{[G,G]}$ is the fixed field of the commutator subgroup of G. The Artin map induces an isomorphism $\varphi\colon C_K \to C \subset G$ with $\varphi(C_K) \simeq C = \mathrm{Gal}(H/K)$. One shows that $\varphi([\sigma(\mathfrak{U})\mathfrak{U}^{-1}]) \in [G, C]$ and conversely that every commutator element in $[G, G]$ can be expressed as $\varphi([\sigma(\mathfrak{U})\mathfrak{U}^{-1}])$ for some $\mathfrak{U} \in I_K$. □

Observe that $C_K/(C_K)^2$ is an abelian group of exponent 2. The previous theorem allows us to deduce the following:

Theorem A.4. *Let p be a prime in $\mathbb{Q}$. If the residue degree of p in $L/\mathbb{Q}$ is 1, then p is the norm of a principal fractional ideal in $K = \mathbb{Q}(\sqrt{D})$.*

Proof. Let $\varphi\colon C_K \to \mathrm{Gal}(H/K)$ be the isomorphism induced by the Artin map. By Theorem A.3, $\mathrm{Gal}(L/K) = \mathrm{Cl}_K \,/\, (\mathrm{Cl}_K)^2$ is abelian. Let $\mathfrak{p}$ be a prime of K lying over p. Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and $\mathfrak{p}$ has residue degree 1 in L. It follows that $\varphi([\mathfrak{p}])|_L = \mathrm{Id}$ so that $\varphi([\mathfrak{p}]) \in \mathrm{Gal}(H/L)$. Thus by Theorem A.3 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 we can represent $[\mathfrak{p}]^n$ by a fractional ideal of norm p for all $n \geq 1$. Since Cl_K is finite, this implies there is a principal fractional ideal in K of norm p. □

Theorem A.5. *[Jan96, Ch VI, §3, Theorem 3.9] 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}.*

Our introduction of the extended genus field L^+ is because it is easier to describe than L.

Theorem A.6. *[Jan96, Ch VI, §3, Theorem 3.10] Let the discriminant of $K = \mathbb{Q}(\sqrt{D})$ be Δ and suppose $|\Delta| = p_1 p_2 \cdots p_t$ where $p_2, \ldots p_t$ are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is*

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

where

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

Corollary A.7. *Let p be an odd prime in $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{D})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$, as in Theorem A.6. If $p \equiv 1 \mod |\Delta|$, then p is the norm of a principal fractional ideal in K. It is also the norm of a principal fractional ideal in $K' = \mathbb{Q}(\sqrt{p^* D})$.*

Proof. Let $L^+ = \mathbb{Q}(\sqrt{D}, \sqrt{p_2^*}, \ldots \sqrt{p_t^*})$ be the extended genus field of K, and L the genus field. If p has residue degree 1 in $L^+/\mathbb{Q}$, then it has residue degree 1 in $L/\mathbb{Q}$, and the first result follows by Theorem A.4.

Note that p splits in the quadratic subfields $\mathbb{Q}(\sqrt{p_i^*})$ for $i = 2, \ldots t$, since $\left(\frac{p_i^*}{p}\right) = \left(\frac{p}{p_i}\right) = 1$, as $p \equiv 1 \pmod \Delta \implies p \equiv 1 \pmod{p_i}$ for $i = 2, \ldots t$. To show that p splits in L^+ we just need to show that it also splits in K.

First suppose $D \equiv 1 \pmod 4$. Write $D = \prod_{i=1}^t p_i^*$. Then

$$\left(\frac{D}{p}\right) = \prod_{i=1}^t \left(\frac{p_i^*}{p}\right) = \prod_{i=1}^t \left(\frac{p}{p_i}\right) = 1.$$

Thus p splits in K.

Now consider that $D \not\equiv 1 \pmod 4$. First assume $D \equiv 3 \pmod 4$. Write $D = -\prod_{i=2}^t p_i^*$. Then

$$\left(\frac{D}{p}\right) = \left(\frac{-1}{p}\right) \prod_{i=2}^t \left(\frac{p_i^*}{p}\right) = \left(\frac{-1}{p}\right) = 1,$$

since $p \equiv 1 \pmod{|\Delta|}$ and $4 \mid |\Delta| \implies p \equiv 1 \pmod 4$.

Now assume that $2 \mid D$ so that $8 \mid |\Delta|$ and $p \equiv 1 \pmod 8$. Then $D = \pm 2 \prod_{i=2}^t p_i^*$. Thus

$$\left(\frac{D}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right) \prod_{i=2}^t \left(\frac{p_i^*}{p}\right) = 1.$$

Let L'^+ be the extended genus field of K'. Now p ramifies in K', $\mathbb{Q}(\sqrt{p^*})$. Using the calculations above, it is either split or ramified in all quadratic subfields of L'^+, and so has residue degree 1 in L'^+, and the result follows. □

We want to understand when $p \in N_{K/\mathbb{Q}}(K^\times)$. If p is the norm of a principal fractional ideal in K, then $\pm p \in N_{K/\mathbb{Q}}(K^\times)$. If K is imaginary, one must have $p \in N_{K/\mathbb{Q}}(K^\times)$. We can also arrive to the same conclusion when K is real and $-1 \in N_{K/\mathbb{Q}}(K^\times)$.

Theorem A.8. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ squarefree and suppose that all odd primes dividing D are congruent to 1 (mod 4). Then -1 is the norm of an element of $K^\times$.*

Proof. The condition on D ensures that there exists $x, y \in \mathbb{Q}$ such that $D = x^2 + y^2$. Therefore $-1 = (x/y)^2 - D(1/y)^2$ so that -1 is the norm of the element $\frac{x}{y} + \frac{1}{y}\sqrt{D}$. □

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 $\frac{5}{3} + \frac{1}{3}\sqrt{34}$ has norm -1, but there is no unit with norm -1.

Theorem A.9. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. If p is an odd prime such that $p \equiv 1 \pmod{|\Delta|}$, then p is the norm of an element of K.*

Proof. We know that p is the norm of a principal fractional ideal of K by Corollary A.7. Therefore there exists integers x, y, z such that $\pm pz^2 = x^2 - Dy^2$. If K is imaginary this automatically implies p is the norm of an element of K, so we assume K is real.

Suppose firstly that all odd primes dividing D are congruent to 1 (mod 4). Then there is an element of $K^\times$ of norm -1 by Theorem A.8. 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 of $K^\times$. □

Theorem A.10. *Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field. Let p be an odd prime such that $p \mid D$ and $p \equiv 1 \pmod{|\Delta|/p}$. Then p is the norm of an element of K.*

Proof. By Corollary A.7, 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. □

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

Corollary A.12. *Let q be an odd prime and let p be a prime that splits in $K = \mathbb{Q}(\sqrt{q^*})$. Then p is the norm of an element of K.*

Proof. By Theorem A.6, one has $L^+ = K$, and so the genus field of K is itself. Since p splits in K, by Theorem A.11, p is the norm of a principal fractional ideal of K. Thus there is $\alpha \in K^\times$ such that $N_{K/\mathbb{Q}}(\alpha) = \pm p$. If K is imaginary then one must have $N_{K/\mathbb{Q}}(\alpha) = p$. Else, K is real and $q \equiv 1 \pmod 4$. Then by Theorem A.8, -1 is a norm from $\mathbb{Q}(\sqrt{q})$, and the result follows. □

Theorem A.13. *Let $h(D)$ be the class number of $\mathbb{Q}(\sqrt{D})$ and let p be a rational prime. Then the following holds.*

- *If $p \equiv 1 \pmod 4$, then $h(p)$ is odd and $h(-p)$ is even.*
- *If $p \equiv 3 \pmod 4$, then $h(p)$ and $h(-p)$ are both odd.*

Proof. By Theorem A.5, it follows that $C_K/(C_K)^2$ is trivial for $\mathbb{Q}(\sqrt{p})$ when $p \equiv 1 \pmod 4$, and $\mathbb{Q}(\sqrt{\pm p})$ when $p \equiv 3 \pmod 4$. Hence C_K is odd in each of these cases.

When $p \equiv 1 \pmod 4$, then $\mathbb{Q}(i, \sqrt{-p})$ is a quadratic unramified extension of $\mathbb{Q}(\sqrt{-p})$, hence $h(-p)$ is even. □

Finally, the following remark is an important fact that we use throughout the report:

Remark A.14 (Conductor-Discriminant)**.** Let $K = \mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}_{>0}$ squarefree. The conductor of $K/\mathbb{Q}$ is a particular modulus for $K/\mathbb{Q}$ ([Neu99, Ch VI, Definition 6.4]). We denote the finite part of it by $\mathfrak{f} \in \mathbb{Z}_{>0}$. Then $\mathfrak{f}$ is the smallest positive integer such that $K \subset \mathbb{Q}(\zeta_\mathfrak{f})$. For quadratic fields, one has that $\mathfrak{f} = |\Delta|$ where Δ is the discriminant of K (this follows from the conductor-discriminant formula [Neu99, Ch VII, (11.9)]). Thus

$$\mathfrak{f} = |\Delta| = \begin{cases} |D| & D \equiv 1 \pmod 4, \\ 4|D| & D \not\equiv 1 \pmod 4. \end{cases}$$

References

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

[DD10] ———, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596. MR 2680426

[DD11] ———, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64. MR 2831512

[Del79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., vol. XXXIII, Amer. Math. Soc., Providence, RI, 1979, With an appendix by N. Koblitz and A. Ogus, pp. 313–346. MR 546622

[DEW21] Vladimir Dokchitser, Robert Evans, and Hanneke Wiersema, *On a BSD-type formula for L-values of Artin twists of elliptic curves*, J. Reine Angew. Math. **773** (2021), 199–230. MR 4237970

[Dok13] Tim Dokchitser, *Notes on the parity conjecture*, Elliptic curves, Hilbert modular forms and Galois deformations, Adv. Courses Math. CRM Barcelona, Birkhäuser/Springer, Basel, 2013, pp. 201–249. MR 3184338

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

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[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

[Sil86] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR 817210

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Sun16] Andrew V. Sunderland, *Number theory i: Lecture 11. totally ramified extensions and krasner's lemma*, Fall 2016.