Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

March 26, 2024

Contents

Introduction

Notation

We use the following notation for characters:

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

1 Birch and Swinnerton-Dyer Conjecture

2 Algebraic number theory and representation theory background

2.1 Representation theory of finite groups

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

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

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

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

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

Induction, Restriction...

Theorem 2.1 (Mackey Decomposition)**.**

2.1.1 Permutation representations and the Burnside ring

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

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

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

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

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

2.2 Decompositions of primes in field extensions

2.3 Class field theory

2.3.1 Genus field

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

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

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

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

Theorem 2.2 (Janusz 3. Extended Class group)**.** *Let r be the number of real primes of K. Let U_K, U_K^+ the group of units and totally positive units of K respectively, Then*

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

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

Corollary 2.3. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free positive integer. Let ϵ be a fundamental unit of K. Then $[H^+\colon H] = 1$ or 2, according as $N_{K/\mathbb{Q}}(\epsilon) = -1$ or 1.*

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

Definition 2.4. For any abelian extension $K/\mathbb{Q}$, the **genus field** of K over $\mathbb{Q}$ is the largest abelian extension E of $\mathbb{Q}$ contained in H. The **extended genus field** is the largest abelian extension E^+ of $\mathbb{Q}$ contained in H^+.

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

Theorem 2.5 (Janusz 3.3)**.**

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

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

Theorem 2.6. *Let p be a prime in $\mathbb{Q}$. If the inertial degree of p in $E/\mathbb{Q}$ is 1, then p is the norm of a principal ideal in K.*

Proof. It's clear by inspection that $\mathrm{Gal}(E/K) = \mathrm{Cl}_K/\left(\mathrm{Cl}_K\right)^2$ is the maximal quotient of exponent 2. Let $\mathfrak{p}$ be a prime of K lying over p. Then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and $\mathfrak{p}$ splits in E, so that $[\mathfrak{p}] \in (\mathrm{Cl}_K)^2$. Thus by theorem 2.5 there is a fractional ideal $\mathfrak{U}$ of I_K such that $[\mathfrak{p}] = [\sigma(\mathfrak{U})\mathfrak{U}^{-1}]$. Observe that $N_{K/\mathbb{Q}}(\sigma(\mathfrak{U})\mathfrak{U}^{-1}) = 1$. It follows that $[\mathfrak{p}]^n$ is represented by a fractional ideal of norm p for all n. Since Cl_K is finite, this implies there is a principal fractional ideal in K of norm p. $\square$

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

Theorem 2.7. *Suppose the discriminant of $K/\mathbb{Q}$ has t prime divisors. Then $C_K/(C_K)^2$ has order 2^{t-1} if $d < 0$ or if $d > 0$ and a unit of K has norm -1. Otherwise, if $d > 0$ and all units of K have norm 1, it has order 2^{t-2}.*

Theorem 2.8. *Let the discriminant of K be Δ and suppose $|\Delta| = p_1 p_2 \cdots p_t$ where $p_2, \ldots p_t$ are odd primes, and p_1 is either odd or a power of 2. Then the extended genus field of K is*

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

where

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

Corollary 2.9. *Let q be a prime in $\mathbb{Q}$, $K = \mathbb{Q}(\sqrt{d})$ with discriminant Δ such that $|\Delta| = p_1 p_2 \cdots p_t$ as above. If $q \equiv 1 \pmod{|\Delta|}$, then q is the norm of a principal ideal in K.*

Proof. Any prime above q in K splits in E^+, hence also in E. □

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

Theorem 2.10. *Let $K = \mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\zeta_m)$ with m odd. Suppose that K is real. Then -1 is the norm of an element from K.*

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

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

Proposition 2.11. $\mathbb{Q}(\sqrt{p^*})$ *has odd narrow class number.*

Corollary 2.12. *The prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

3 Norm relations

Recall that in Section 2.1, we associated to $\rho \in R_{\mathbb{C}}(G)$ the character

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

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

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

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

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

Remark 3.1. If $\rho = 0$ then we call functions $\psi \sim_{\rho} 1$ **representation theoretic**. These have been studied in cite.

Example 3.2. Take $\rho = 0$, and V a representation of G. The function $\psi(H) = \dim V^H$ satisfies $\psi \sim_{\rho} 1$ as $\dim V^H = \langle \mathrm{Res}_H V, \mathbb{1}_H \rangle = \langle V, \mathrm{Ind}_H^G \mathbb{1} \rangle$ by Frobenius reciprocity.

Example 3.3. Let $G = C_p$ for p a prime. Let ρ be a character of degree p. There is a unique ρ-relation given by $\Theta = C_1 - C_p$. Let $\psi(H) = [G \colon H]$. Then $\psi(\Theta) = p$, which is a norm from $\mathbb{Q}(\sqrt{p^*}) \subset \mathbb{Q}(\zeta_p)$ by Corollary 2.12.

Example 3.4. Let $G = C_n$. For each $d \mid n$, let $\chi_d = \widetilde{\varphi_d}$, where φ_d is an irreducible complex character of G with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d. Then $\{\chi_d \colon d \mid n\}$ form a basis for the irreducible rational-valued representations of G. Note that $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1}$ is the direct sum of irreducible complex representations of G contain $C_{n/d}$ in their kernel. Thus, $\mathrm{Ind}_{C_{n/d}}^G \mathbb{1} \simeq \sum_{d' \mid d} \chi_{d'}$. Applying Möbius inversion, we obtain the unqiue φ_d-relation for each $d \mid n$:

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

Example 3.5. Let $E/\mathbb{Q}$ be an elliptic curve, $G = \mathrm{Gal}(F/\mathbb{Q})$ for $F/\mathbb{Q}$ a Galois extension. For $H \leq G$, the function $\psi \colon H \mapsto C(E/F^H)$ extends to a multiplicative function on the Burnside ring. Given a representation ρ of G, one can ask when $\psi \sim_{\rho} 1$.

3.1 D-local functions

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

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

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

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

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

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

Definition 3.6. Suppose $I \lhd D < G$ with D/I cyclic, and $\psi(e, f)$ is a function of $e, f \in \mathbb{N}$. Define

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

Then, this is a function on the Burnside ring.

Example 3.7. For semi-stable reduction, we're considering $\psi(e, f) = e$ (the Tamagawa number). For the d_v terms in the case of additive potentially good reduction at p (p not equal to 2 or 3), we consider $\psi(e, f) = p^{f \lfloor en/12 \rfloor}$, where $n \in \{2, 3, 4, 6, 9, 10\}$.

4 Forcing points of infinite order

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

Theorem 4.1. *Let $E/\mathbb{Q}$ be an elliptic curve, $F/\mathbb{Q}$ a Galois extension with Galois group G, ρ an irreducible representation of G and*

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

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

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

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

As discussed in section 3.1, the function on $B(G)$ sending $H\mapsto C(E/F^H)$ is the product of local functions depending on the decomposition group D_p at a prime p. We denote each of these as (D_p, I_p, ψ_p), as in definition 3.6. Then the product of Tamagawa numbers in 4.1 is the evaluation of $\prod_p(D_p, I_p, \psi_p)$ on $\sum_i H_i - \sum_j H'_j$.

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

Lemma 4.2. *In an odd degree unramified extension, Tamagawa numbers change only up to squares. In particular, if $[D_p\colon I_p]$ is odd, then $(D_p, I_p, \psi_p)\sim_\rho(D_p, D_p, \psi_p)$ for any ρ with $\mathbb{Q}(\rho)$ even.*

Proof. Yadada ☐

4.1 Compatibility in odd order extensions

In this section we prove the following:

Theorem 4.3. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $F/\mathbb{Q}$ be an extension of* **odd order** *with Galois group G. Suppose that the primes of additive reduction of E are at worst tamely ramified in $F/\mathbb{Q}$ (and ≥ 5).*

Then for any representation ρ of G and any expression as in 1, the corresponding ratio of Tamagawa numbers is a norm from any quadratic subfield of $\mathbb{Q}(\rho)$.

If $\mathbb{Q}(\rho)=\mathbb{Q}$ there is nothing to prove. If $[\mathbb{Q}(\rho)\colon\mathbb{Q}]>1$ then this index is even. Indeed, since G has odd order, there is an element $\sigma\in\mathrm{Aut}(\mathbb{Q}(\rho)/\mathbb{Q})$ that acts by conjugation (i.e. is of order 2). Therefore there is a quadratic subfield $\mathbb{Q}(\sqrt{d})\subset\mathbb{Q}(\rho)$. Choose any such quadratic subfield. Replacing ρ by the sum of its conjugates by elements of $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}(\sqrt{d}))$, we may assume that $\mathbb{Q}(\rho)=\mathbb{Q}(\sqrt{d})$. Let τ be the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Let m be the smallest integer such that $\mathbb{Q}(\sqrt{d})\subset\mathbb{Q}(\zeta_m)$. Then m divides the exponent of G, hence is odd.

We prove that each (D_p,I_p,ψ_p) satisfies $(D_p,I_p,\psi_p)\sim_\rho 1$. Since we deal with each local factor individually, we may assume that $D_p=I_p$ by theorem 4.2.

Good reduction

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

Multiplicative reduction

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

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

Lemma 4.4. *Let G, ρ be as above. If (D_p,I_p,ψ_p) is such that ψ_p is constant, then $(D_p,I_p,\psi_p)\sim_\rho 1$.*

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

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

$\square$

Now suppose that p has split multiplicative reduction. Then $\psi_p(e,f)=e$. We have $I_p=P_p\ltimes C_l$, 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 $l\mid p^f-1=p-1$ (recalling we can take $D_p=I_p$).

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

$$\Theta=\sum_i n_i\mathrm{Ind}_{H_i}^G\mathbb{1}\simeq\rho\oplus\tau(\rho), \tag{2}$$

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

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

We understand Res_D best when D is cyclic. Let $D = C_n$ with $m \mid n$. Applying Res_D to (2), we get

$$\sum_i n_i \sum_{x \in H_i \backslash G/D} \mathrm{Ind}_{D \cap x^{-1} H_i x}^{D} \mathbb{1} \simeq \mathrm{Res}_D \rho \oplus \tau(\mathrm{Res}_D \rho). \tag{3}$$

Since both sides are now rationally valued, we can write this as $\sum_{d|n} a_d \cdot \chi_d$ where $a_d \in \mathbb{Z}$ and χ_d are defined in example 3.4. Writing each χ_d in terms of permutation representations as in the example, one obtains an expression for the LHS of (2) (since cyclic groups have no Brauer relations, this is on the nose). Therefore, if $\psi(\Theta) = \prod_p \psi(\mathrm{Res}_{D_p} \Theta)$, we have $\psi(\mathrm{Res}_{D_p} \Theta) = \prod_{d|n} \psi(\chi_d)^{a_d}$ whenever $D_p = C_n$.

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

Semistable reduction

In this subsection we work towards proving the following:

Theorem 4.5. *Let $F/\mathbb{Q}$ be a Galois extension of odd degree, with $G = \mathrm{Gal}(F/\mathbb{Q})$. Consider a semistable elliptic curve $E/\mathbb{Q}$ with good reduction at primes that are wildly ramified in $F/\mathbb{Q}$.*

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

dv terms in additive reduction

Tamagawa numbers in additive reduction

We use the following description of Tamagawa numbers.

Lemma 4.6. *Let $K'/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let E/K be an elliptic curve with addtive reduction;*

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

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

If E has potentially good reduction, then

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

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

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

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

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

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

assuming $d > 1$.

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

Type II and II^* reduction:

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

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

Type IV and IV^* reduction:

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

In summary,

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

Remark 4.7. There's no reason why we can't get 3; see elliptic curve 441b1 with additive reduction at 7 of type IV and Tamagawa number equal to 3)

However, it turns out we will only get 3 occuring oddly when $d = 3$. Indeed, one has that $\langle \mathrm{Ind}_{D_{d'}}^{D} \mathbb{1}, \psi_3 \rangle = 1$ if $3 \mid d'$, and 0 if $3 \nmid d'$, where ψ_3 is an irreducible character of D of order 3. Therefore one sees that the number of places with ramification degree divisible by 3 cancels unless $d = 3$. Indeed, $\langle \chi_d, \psi_3 \rangle = 0$ unless $d = 3$, in which case it is 1. Therefore (4) can only be non-square when $d = 3$.

References

[BH06] C. J. Bushnell and G. Henniart, *The Local Langlands Conjecture for GL(2)*, Grundlehren der mathematischen Wissenschaften, Springer Berlin, 2006.