Arithmetic Applications of Artin Twist and BSD

Edwina Aylward, Albert Lopez Bruch

March 22, 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:

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

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

2.2 Decompositions of primes in field extensions

2.3 Class field theory

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

Proposition 2.2. *$\mathbb{Q}(\sqrt{p^*})$ has odd narrow class number.*

Corollary 2.3. *The prime $p \in \mathbb{Q}$ is the norm of an element in $\mathbb{Q}(\sqrt{p^*})^\times$.*

3 Proving things...

3.1 Norm relations

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

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

We call $\sum_i n_i H_i \in B(G)$ a ρ-**relation** if

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

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.

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 $\psi \sim_\rho 0$ 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. Then the unique ρ-relation is given by $\Theta = C_1 - C_p$. Let $\psi(H) = [G\colon H]$. Then $\psi(\Theta) = p$, which is a norm from $\mathbb{Q}(\zeta_p)$ by Corollary 2.3.

Example 3.4. 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 $\psi \sim_\rho 1$.

3.1.1 D-local functions

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

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

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

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

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

Definition 3.5. Suppose $I \triangleleft D < G$ with D/I cyclic, and $\psi(e,f)$ is a function of $e, f \in \mathbb{N}$. Define

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

Then, this is a function on the Burnside ring.

For example, 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 $n \in \{2,3,4,6,9,10\}$.

3.2 Compatibility in odd order extensions

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

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

where ρ is a character of G with $\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) = \langle\tau\rangle$ of size 2. In particular we 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 $H_i \subseteq G$.

If I consider $\mathrm{Res}_D(\rho)$ where D is a decomposition group of exponent k, then for $\mathrm{Res}_D(\rho)$ to be non-rationally valued, one needs $m \mid k$. Note that in the context of norm relations, if $\mathrm{Res}_D(\rho) = \mathrm{Res}_D(\tau(\rho))$, then we always get squares.

So now suppose that $D = I = C_n$ with $m \mid n$. Applying Res_D to (1), we get

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

Since both sides are now rationally valued, we can write this as $\sum_{d|n} a_d \cdot \chi_d$ where $a_d \in \mathbb{Z}$ and $\{\chi_d\colon d \mid n\}$ form a basis for the irreducible rational-valued representations of D. Explicitly, χ_d is the sum of the Galois conjugates of an irreducible complex character of D with field of values $\mathbb{Q}(\zeta_d)$ and kernel of index d (which we'll write as D_d).

We can write each χ_d in terms of permutation modules:

$$\chi_d = \sum_{d'|d} \mu(d'/d) \mathrm{Ind}_{D_{d'}}^D \mathbb{1}. \tag{3}$$

Substituting this into $\sum_{d|n} a_d \cdot \chi_d$ gives an expression for the LHS of (1) (since cyclic groups have no Brauer relations, this is on the nose). In particular, if we have a D-local function, we can evaluate it on each χ_d-relation as in (3). Then the total expression is the product of these, raised to a_d.

Since we understand represntation theory of cyclic groups (wow!), we'd like to be able to reduce to cyclic decomposotion groups. Note that since we only assume bad reduction at tamely ramified primes in $F/\mathbb{Q}$, one has that I is cyclic. It turns out that we may assume that $D = I$ when $[D\colon I]$ is odd.

Lemma 3.6. *In an odd degree unramified extension, Tamagawa numbers change only up to squares. In particular, if $[D\colon I]$ is odd, then $(D, I, \psi) \sim_\rho (I, I, \psi)$ for any ρ with $\mathbb{Q}(\rho)$ even, where $\psi(e, f)$ is the Tamagawa number.*

Proof. Yadada □

3.2.1 Semistable reduction

In this subsection we work towards proving the following:

Theorem 3.7. *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 $f \sim_\rho 1$.

3.2.2 dv terms in additive reduction

3.2.3 Tamagawa numbers in additive reduction

We use the following description of Tamagawa numbers.

Lemma 3.8. *Let $K'/K/\mathbb{Q}_p$ be finite extensions and $p \geq 5$. Let E/K be an elliptic curve with addtive reduction;*

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

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

If E has potentially good reduction, then

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

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

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

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

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

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

assuming $d > 1$.

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

Type II and II^* reduction:

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

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

Type IV and IV^* reduction:

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

In summary,

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

(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.