A MOD-p ARTIN–TATE CONJECTURE, AND GENERALIZING THE HERBRAND–RIBET THEOREM

DIPENDRA PRASAD

A MOD-p ARTIN–TATE CONJECTURE, AND GENERALIZING THE HERBRAND–RIBET THEOREM

DIPENDRA PRASAD

We propose conjectures about the integrality properties of the values at $s = 0$ of certain abelian L-functions of $\mathbb{Q}$ and totally real number fields. We also propose a conjecture which generalizes the theorems of Herbrand and Ribet for values at $s = 0$ of totally odd Artin L-functions of totally real number fields. Various calculations, some of which are familiar to experts, are made to provide examples.

1. Introduction

Following the natural instinct that when a group operates on a number field then every term in the class number formula should factorize "compatibly" according to the representation theory (both complex and modular) of the group, we are led — in the spirit of Herbrand and Ribet's theorem on the p-component of the class number of $\mathbb{Q}(\zeta_p)$ — to some natural questions about the p-part of the class group of any CM Galois extension E of $\mathbb{Q}$ as a module for $\mathrm{Gal}(E/\mathbb{Q})$. The compatible factorization of the class number formula is at the basis of *Stark's conjecture*, where one is mostly interested in factorizing the regulator term — whereas for us in this paper, we put ourselves in a situation where the regulator term can be ignored, and it is the factorization of the class number that we seek. All this is presumably part of various "equivariant" conjectures in arithmetic-geometry, such as the "equivariant Tamagawa number conjecture", but the literature does not seem to address this question in any precise way. In trying to formulate these questions, we are naturally led to consider $L(0, \rho)$, for ρ an Artin representation, in situations where this is known to be nonzero and algebraic, and it is important for us to understand if this is $\mathfrak{p}$-integral for a prime $\mathfrak{p}$ of the ring of algebraic integers $\overline{\mathbb{Z}}$ in $\mathbb{C}$, which we call a *mod-p Artin–Tate conjecture*. As an attentive reader will notice, the most innocuous term in the class number formula, the number of roots of unity, plays an important role for us — it, being the only term in the denominator, is responsible for all the poles!

Let F be a number field contained in $\mathbb{C}$ with $\overline{\mathbb{Q}}$ its algebraic closure in $\mathbb{C}$. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible Galois representation with $L(s, \rho)$ its associated Artin L-function. According to a famous conjecture of Artin, $L(s, \rho)$ has an analytic continuation to an entire function on $\mathbb{C}$ unless ρ is the trivial representation, in which case it has a unique pole at $s = 1$ which is simple.

More generally, let M be an irreducible motive over $\mathbb{Q}$ with $L(s, M)$ its associated L-function. According to Tate, $L(s, M)$ has an analytic continuation to an entire function on $\mathbb{C}$ unless M is a twisted Tate motive $\mathbb{Q}(j)$ with $\mathbb{Q}(1)$ the motive associated to $\mathbb{G}_m$. For the motive $\mathbb{Q} = \mathbb{Q}(0)$, $L(s, \mathbb{Q}) = \zeta_{\mathbb{Q}}(s)$, the usual Riemann zeta function, which has a unique pole at $s = 1$ which is simple.

This paper will deal with certain Artin representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_n(\mathbb{C})$ for which we will know a priori that $L(0, \rho)$ is a nonzero algebraic number (in particular, F will be totally real). It is then an important question to understand the nature of the algebraic number $L(0, \rho)$: to know if it is an algebraic integer, but if not, what are its possible denominators. We think of the possible denominators in $L(0, \rho)$, as existence of poles for $L(0, \rho)$, at the corresponding prime ideals of $\overline{\mathbb{Z}}$. It is thus analogous to the conjectures of Artin and Tate, both in its aim — and as we will see — in its formulation. Since we have chosen to understand L-values at 0 instead of 1, which is where Artin and Tate conjectures are formulated, there is an "ugly" twist by ω_p — the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-th roots of unity — throughout the paper, giving a natural character $\omega_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$, also a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ for L any algebraic extension of $\mathbb{Q}$, as well as a character of $\mathrm{Gal}(L/\mathbb{Q})$ if L is a Galois extension of $\mathbb{Q}$ containing p-th roots of unity; if there are no nontrivial p-th roots of unity in L, we will define ω_p to be the trivial character of $\mathrm{Gal}(L/\mathbb{Q})$.

We now fix some notation. We will fix an isomorphism of $\overline{\mathbb{Q}}_p$ with $\mathbb{C}$ where $\overline{\mathbb{Q}}_p$ is a fixed algebraic closure of $\mathbb{Q}_p$, the field of p-adic numbers. This allows one to define $\mathfrak{p}$, a prime ideal in $\overline{\mathbb{Z}}$, the integral closure of $\mathbb{Z}$ in $\mathbb{C}$, over the prime ideal generated by p in $\mathbb{Z}$. The prime p will always be an odd prime in this paper.

All the finite-dimensional representations of finite groups in this paper will take values in $\mathrm{GL}_n(\overline{\mathbb{Q}}_p)$, and therefore in $\mathrm{GL}_n(\mathbb{C})$, as well as $\mathrm{GL}_n(\overline{\mathbb{Z}}_p)$. It thus makes sense to talk of "reduction modulo $\mathfrak{p}$" of (complex) representations of finite groups. These reduced representations are well defined up to semisimplification on vector spaces over $\overline{\mathbb{F}}_p$ (theorem of Brauer and Nesbitt); we denote the reduction modulo $\mathfrak{p}$ of representations as $\rho \to \bar\rho$.

If F is a finite Galois extension of $\mathbb{Q}$ with Galois group G, then it is well known that the zeta function $\zeta_F(s)$ can be factorized as

$$\zeta_F(s) = \prod_\rho L(s, \rho)^{\dim \rho},$$

where ρ ranges over all the irreducible complex representations of G, and $L(s, \rho)$ denotes the Artin L-function associated to ρ.

According to the class number formula, we have the power series expansion of $\zeta_F(s)$ at $s = 0$ as

$$\zeta_F(s) = -\frac{hR}{w}s^{r_1+r_2-1} + \text{higher-order terms},$$

where r_1, r_2, h, R, w are the standard invariants associated to F: r_1 the number of real embeddings, r_2 the number of pairs of complex conjugate embeddings which are not real, h the class number of F, R the regulator, and w the number of roots of unity in F.

This paper considers ζ_E/ζ_F where E is a CM field with F its totally real subfield, in which case $r_1 + r_2$ is the same for E as for F, and the regulators of E and F too are the same except for a possible power of 2. Therefore, for c the complex conjugation on $\mathbb{C}$,

$$(\zeta_E/\zeta_F)(0) = \prod_{\rho(c)=-1} L(0, \rho)^{\dim \rho} = \frac{h_E/h_F}{w_E/w_F},$$

where each L-value $L(0, \rho)$ in the above expression is a nonzero algebraic number by a theorem of Klingen and Siegel.

In this identity, observe that L-functions are associated to $\mathbb{C}$-representations of $\mathrm{Gal}(E/\mathbb{Q})$, whereas the class groups of E and F are finite Galois modules. Modulo some details, we basically assert that for each odd prime p, each irreducible odd $\mathbb{C}$-representation ρ of $\mathrm{Gal}(E/\mathbb{Q})$ contributes a certain number of copies (depending on $\mathfrak{p}$-adic valuation of $L(0, \rho)$) of $\bar{\rho}$ to the class group of E tensored with $\mathbb{F}_p$ modulo the class group of F tensored with $\mathbb{F}_p$ (up to semisimplification). This is exactly what happens for $E = \mathbb{Q}(\zeta_p)$ by the theorems of Herbrand and Ribet, which is the main motivating example for all that we do here, and this is what we will review next.

2. The Herbrand–Ribet theorem

In this section we recall the Herbrand–Ribet theorem from the point of view of this paper. We refer to the original work of Ribet [1976] and to [Washington 1982] for an exposition on the theorem together with a proof of Herbrand's theorem.

There are actually two a priori important aspects of the Herbrand–Ribet theorem dealing with the p-component of the class group for $\mathbb{Q}(\zeta_p)$. First, as the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p)^\times$ is of order coprime to p, its action on the p-component of the class group is semisimple, and therefore, the p-component of the class group can be written as a direct sum of eigenspaces for the action of $(\mathbb{Z}/p)^\times$ on it. We do not consider this aspect of the Herbrand–Ribet theorem to be important, and simply consider semisimplification of representations of Galois groups on class groups to be a good-enough substitute.

The second — and more serious — aspect of the Herbrand–Ribet theorem is that among the characters of $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p)^\times$, only the odd characters, i.e., characters $\chi : (\mathbb{Z}/p)^\times \to \mathbb{Q}_p^\times$ with $\chi(-1) = -1$, present themselves — as it is only for these that there is any result about the χ-eigencomponent in the class group, and even among these, the Teichmüller character $\omega_p : (\mathbb{Z}/p)^\times \to \mathbb{Q}_p^\times$ plays a role different from other characters of $(\mathbb{Z}/p)^\times$. (Note that earlier we have used ω_p for the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-th roots of unity, giving a natural character $\omega_p : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/p)^\times$, as well as to its restriction to $\text{Gal}(\overline{\mathbb{Q}}/L)$ for L any algebraic extension of $\mathbb{Q}$. Since $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/p)^\times$, the two roles that ω_p will play throughout the paper are actually the same.)

To elaborate on the role of "odd" characters in the Herbrand–Ribet theorem, observe that the class number formula

$$\zeta_F(s) = -\frac{hR}{w} s^{r_1+r_2-1} + \text{higher-order terms}$$

can be considered both for $F = \mathbb{Q}(\zeta_p)$ as well as its maximal real subfield $F^+ = \mathbb{Q}(\zeta_p)^+$. It is known that [Washington 1982, Proposition 4.16],

$$R/R^+ = 2^{(p-3)/2},$$

where R is the regulator for $\mathbb{Q}(\zeta_p)$ and R^+ is the regulator for $\mathbb{Q}(\zeta_p)^+$. We will similarly denote h and h^+ to be the order of the two class groups, with $h^- = h/h^+$, an integer.

Dividing the class number formula of $\mathbb{Q}(\zeta_p)$ by that of $\mathbb{Q}(\zeta_p)^+$, we find

$$(1) \qquad \prod_{\chi \text{ an odd character of } (\mathbb{Z}/p)^\times} L(0, \chi) = \frac{1}{p} \cdot \frac{h}{h^+} \cdot 2^{(p-3)/2},$$

the factor $1/p$ arising because there are $2p$ roots of unity in $\mathbb{Q}(\zeta_p)$ and only 2 in $\mathbb{Q}(\zeta_p)^+$.

It is known that for χ an odd character of $(\mathbb{Z}/p)^\times$, $L(0, \chi)$ is an algebraic number which is given in terms of the generalized Bernoulli number $B_{1,\chi}$ as

$$L(0, \chi) = -B_{1,\chi} = -\frac{1}{p} \sum_{a=1}^{a=p} a\chi(a).$$

It is easy to see that $pB_{1,\omega_p^{p-2}} \equiv (p-1) \bmod p$ since $a\omega_p^{p-2}(a)$ is the trivial character of $(\mathbb{Z}/p)^\times$ whereas for all the other characters of $(\mathbb{Z}/p)^\times$, $L(0, \chi)$ is not only an algebraic number but is p-adic integral (Schur orthogonality!); all this is clear by looking at the expression

$$L(0, \chi) = -B_{1,\chi} = -\frac{1}{p} \sum_{a=1}^{a=p} a\chi(a).$$

Rewrite (1) up to p-adic units as

$$\prod_{\substack{\chi \text{ an odd character of } (\mathbb{Z}/p)^\times \\ \chi \neq \omega_p^{p-2} = \omega_p^{-1}}} L(0, \chi) = \frac{h}{h^+},$$

where we note that both sides of the equality are p-adic integral elements; in fact, since all characters $\chi : (\mathbb{Z}/p)^\times \to \overline{\mathbb{Q}}_p^\times$ take values in $\mathbb{Z}_p$, for $\chi \neq \omega_p^{-1}$, $L(0, \chi) \in \mathbb{Z}_p$. This, when interpreted — just an interpretation in the optics of this paper without any suggestions for proof in either direction! — for each χ component on the two sides of this equality, amounts to the theorem of Herbrand and Ribet which asserts that p divides $L(0, \chi) = -B_{1,\chi}$ for χ an odd character of $(\mathbb{Z}/p)^\times$, which is not ω_p^{p-2}, if and only if the corresponding χ^{-1}-eigencomponent of the class group of $\mathbb{Q}(\zeta_p)$ is nontrivial (note the χ^{-1}, and not χ!). Furthermore, the character ω_p does not appear in the p-class group of $\mathbb{Q}(\zeta_p)$. It can happen that $L(0, \chi)$ is divisible by higher powers of p than 1, and one expects — this is not proven yet! — that in such cases, the corresponding χ^{-1}-eigencomponent of the class group of $\mathbb{Q}(\zeta_p)$ is $\mathbb{Z}/p^{(\mathrm{val}_p\, L(0,\chi))}$, and in particular, it still has p-rank 1. (By [Mazur and Wiles 1984], the χ^{-1}-eigencomponent of the class group of $\mathbb{Q}(\zeta_p)$ is of order $p^{(\mathrm{val}_p\, L(0,\chi))}$.)

The work of Ribet was to prove that if $p \mid B_{1,\chi}$, then the χ^{-1}-eigencomponent of the class group of $\mathbb{Q}(\zeta_p)$ is nontrivial by constructing an unramified extension of $\mathbb{Q}(\zeta_p)$ by using a congruence between a holomorphic cusp form and an Eisenstein series on $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$.

To be able to use the class number formula in other situations, we will need to have the integrality of $L(0, \chi)$ for χ a character associated to the Galois group of a number field, or even of $L(0, \rho)$ for general irreducible representations ρ of the Galois group of a number field, in more situations that we call a mod-p Artin–Tate conjecture.

Let E be a CM number field which we assume is Galois over $\mathbb{Q}$. Assume that E contains p^n-th roots of unity but no p^{n+1}-th root of unity. Let F be the totally real subfield of E with $[E : F] = 2$. Let $G = \mathrm{Gal}(E/Q)$ with $-1 \in G$, the complex conjugation in G.

We have

$$\zeta_E(s) = \prod_\rho L_\mathbb{Q}(s, \rho)^{\dim \rho},$$

$$\zeta_F(s) = \prod_{\rho(-1)=1} L_\mathbb{Q}(s, \rho)^{\dim \rho},$$

$$(\zeta_E/\zeta_F)(s) = \prod_{\rho(-1)=-1} L_\mathbb{Q}(s, \rho)^{\dim \rho},$$

where all the products above are over irreducible representations ρ of $G = \mathrm{Gal}(E/\mathbb{Q})$ with values in $\mathrm{GL}_d(\overline{\mathbb{Q}}_p)$.

By the class number formula,

$$(2) \qquad h^-(E)/p^n = \prod_{\rho(-1)=-1} L_{\mathbb{Q}}(0, \rho)^{\dim \rho}.$$

By Corollary 6 below, there is an $a \in \mathbb{Z}_p^\times$ with

$$(3) \qquad a/p^n = \prod_{\chi(-1)=-1} L_{\mathbb{Q}}(0, \chi),$$

where χ are all the characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n)^\times$ for which $\bar{\chi} = \omega_p^{-1}$.

Dividing (2) by (3), we have up to p-adic units

$$(4) \qquad h^-(E) = \prod_{\substack{\rho(-1)=-1, \\ \rho \neq \chi}} L_{\mathbb{Q}}(0, \rho)^{\dim \rho}$$

where the product on the right is taken over irreducible representations ρ of $G = \mathrm{Gal}(E/\mathbb{Q})$ for which $\rho(-1) = -1$, and which are not cyclotomic characters of the form $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n)^\times \to \mathbb{Q}_p^\times$ with $\bar{\chi} = \omega_p^{-1}$.

It is known that $L(0, \rho) \in \bar{\mathbb{Q}}^\times$ for $\rho(-1) = -1$. This is a simple consequence of a theorem due to Klingen and Siegel that partial zeta functions of a totally real number field take rational values at all nonpositive integers [Tate 1984]. (Note that to prove $L(0, \rho) \in \bar{\mathbb{Q}}^\times$ for $\rho(-1) = -1$, it suffices by Brauer to prove it for abelian CM extensions by a lemma of Serre [Tate 1984, Chapter III, Lemma 1.3].)

The left-hand side of (4) is integral, and we would like to suggest the same for each term on the right-hand side of (4).

The following conjecture about $L(0, \rho)$ extends the known integrality properties of $L(0, \chi) = -B_{1,\chi} = -\frac{1}{p} \sum_{a=1}^{a=p} a \chi(a)$, encountered and used earlier. The formulation of the conjecture also assumes known integrality properties about $L(0, \chi)$ for $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n)^\times \to \mathbb{C}^\times$ discussed in the last section of this paper.

Conjecture 1 (mod-p analogue of the Artin–Tate conjecture). *Let $\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ be an irreducible representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with $\rho(c) = -1$ where c is a complex conjugation in $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then unless ρ is a one-dimensional representation factoring through $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ (for some prime p) with $\bar{\rho}$ the reduction of ρ modulo $\mathfrak{p}$ (the maximal ideal in $\bar{\mathbb{Z}}_p$) being $\bar{\rho} = \omega_p^{-1}$, $L(0, \rho) \in \bar{\mathbb{Q}}$ is integral outside 2, i.e., $L(0, \rho) \in \bar{\mathbb{Z}}\left[\frac{1}{2}\right]$.*

We next recall the following theorem of Deligne and Ribet [1980], which could be considered as a weaker version of Conjecture 1.

Theorem. *Let k be a totally real number field, and let $\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/k) \to \bar{\mathbb{Q}}^\times$ be a character of finite order with $\chi(c) = -1$ where c is a complex conjugation*

in $\text{Gal}(\overline{\mathbb{Q}}/k)$. *Let w be the order of the group of roots of unity in E, the smallest extension of k such that χ is trivial when restricted to $\text{Gal}(\overline{\mathbb{Q}}/E)$. Then*

$$wL(0, \chi) \in \overline{\mathbb{Z}}.$$

In fact Conjecture 1 can be used to make precise the above theorem of Deligne–Ribet as follows; the simple argument using the fact that the Artin L-function is invariant under induction from $\text{Gal}(\overline{\mathbb{Q}}/k)$ to $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ will be left to the reader.

Conjecture 2. *Let k be a totally real number field, and $\chi : \mathbb{A}_k^\times/k^\times \to \overline{\mathbb{Z}}_p^\times$ a finite-order character, with $\chi(c) = -1$ where c is a complex conjugation in $\text{Gal}(\overline{\mathbb{Q}}/k)$. Then if $L(0, \chi) \notin \overline{\mathbb{Z}}_p$,*

(1) *$\chi \mod p$ is ω_p^{-1} and*

(2) *χ is a character of $\mathbb{A}_k^\times/k^\times$ associated to a character of the Galois group $\text{Gal}(k(\zeta_q)/k)$ for some q which is a power of p.*

Remark. In the examples that I know, which are for characters $\chi : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ with $\chi = \omega_p^{-1} \pmod{p}$, if $L(0, \chi)$ has a (mod-p) pole, the pole is of order 1; more precisely, if $L = \mathbb{Q}_p[\chi(\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p))]$ is the subfield of $\overline{\mathbb{Q}}_p$ generated by the image under χ of the decomposition group at p, then $L(0, \chi)$ is the inverse of a uniformizer of this field L. It would be nice to know if this is the case for characters χ of $\text{Gal}(\overline{\mathbb{Q}}/k)$ for k arbitrary. This would be in the spirit of Artin's classical conjecture where the only possible poles of $L(1, \rho)$, for ρ an irreducible representation of $\text{Gal}(\overline{\mathbb{Q}}/k)$, are simple.

3. Proposed generalization of Herbrand–Ribet for CM number fields

The Herbrand–Ribet theorem is about the relationship of L-values $L(0, \chi)$ with the χ^{-1}-eigencomponent of the class group of $\mathbb{Q}(\zeta_p)$. In the last section, we proposed a precise conjecture about integrality properties for the L values $L(0, \rho)$. In this section, we now propose their relationship to class groups.

We begin by introducing some notation involved in constructing in a functorial way an elementary abelian p-group $\overline{A}[p]$ out of a finite abelian group A with

(1) $p \cdot \overline{A}[p] = 0$ and

(2) the cardinality of $\overline{A}[p]$ equals the cardinality of the p-Sylow subgroup of A.

We define $\overline{A}[p]$ to be the direct sum of the p-groups $p^i A/p^{i+1}A$ for $i \geq 0$. If A is a G-module, then naturally, $\overline{A}[p]$ too is a G-module. If A is a G-module, then we let $\overline{A}[p]^{\text{ss}}$ be the semisimplification of the corresponding G-module $\overline{A}[p]$ over $\mathbb{F}_p$.

Since according to the theorem of Klingen and Siegel, the value $L(0, \rho)$ for an odd representation ρ of $\text{Gal}(\overline{\mathbb{Q}}/k)$, where k is a totally real number field, belongs to

the algebraic number field generated by the character values of ρ, and since we are trying to equate powers of p appearing on the two sides of the class number formula, it will be important to consider only those representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ which actually take values in $\mathbb{Q}_p^{\mathrm{unr}}$, the maximal unramified extension of $\mathbb{Q}_p$. Observe that the Brauer group of $\mathbb{Q}_p^{\mathrm{unr}}$ is trivial, and thus, an irreducible representation of a finite group is defined over $\mathbb{Q}_p^{\mathrm{unr}}$ if and only if its character is defined over $\mathbb{Q}_p^{\mathrm{unr}}$. If an irreducible representation π of a finite group is defined over $\overline{\mathbb{Q}}_p$, one can take the sum of the Galois conjugates π^σ of π for $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}})$, to construct canonically an irreducible representation, say $\langle \pi \rangle$ over $\mathbb{Q}_p^{\mathrm{unr}}$. The representation π can be reduced modulo $\mathfrak{p}$ and the representation $\langle \pi \rangle$ modulo p, and the semisimplification of these reductions are related by

$$\overline{\langle \pi \rangle}^{\mathrm{ss}} \cong d\overline{\pi}^{\mathrm{ss}},$$

where d is the number of distinct Galois conjugates of π under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{unr}})$.

Let E be a Galois CM extension of a totally real number field k with F the totally real subfield of E with $[E : F] = 2$, and $G = \mathrm{Gal}(E/k)$. Let c denote the element of order 2 in the Galois group of E over F.

Let H_E and H_F denote the class groups of E and F, respectively. Observe that the kernel of the natural map from H_F to H_E is a 2-group. (This follows from using the norm mapping from H_E to H_F.) Therefore, since we are interested in p-primary components for only odd primes p, H_F can be considered to be a subgroup of H_E, and the quotient H_E/H_F becomes a G-module of order h_E/h_F.

The following conjecture on the structure of the *minus-part* of the class group of E (as a module for the Galois group G) is arrived at by considering the p-adic valuations of the two sides of the class number formula

$$(\zeta_E/\zeta_F)(0) = \prod_{\rho(c)=-1} L(0, \rho)^{\dim \rho} = \prod_{\rho(c)=-1} L(0, \langle \rho \rangle)^{\dim \rho} = \frac{h_E}{h_F} \frac{1}{w_E},$$

with E, F, k as above, and the first product taken over all irreducible representations ρ of $G = \mathrm{Gal}(E/k)$ with values in $\mathrm{GL}_n(\overline{\mathbb{Q}}_p)$, whereas the second one is over all irreducible representations $\langle \rho \rangle$ of $G = \mathrm{Gal}(E/k)$ with values in $\mathrm{GL}_n(\mathbb{Q}_p^{\mathrm{unr}})$. Since we are formulating the conjecture below based on equality of (p-adic valuations of) numbers in the class number formula, it is not sensitive to the subtlety discussed earlier about χ-eigencomponents in the class group of $\mathbb{Q}(\mu_p)$ being cyclic or not; all we care about is their order.

Conjecture 3. *Let E be a CM, Galois extension of a totally real number field k, with F the totally real subfield of E, and $c \in \mathrm{Gal}(E/F)$, the nontrivial element of the Galois group. Let $\langle \rho \rangle : \mathrm{Gal}(E/k) \to \mathrm{GL}_{dn}(\mathbb{Q}_p^{\mathrm{unr}})$ be an irreducible, odd (i.e., $\rho(c) = -1$) representation of $\mathrm{Gal}(E/k)$ associated to an irreducible representation $\rho : \mathrm{Gal}(E/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ as above, with $\overline{\rho}$ the semisimplification of the reduction*

of ρ mod $\mathfrak{p}$ for p an odd prime. Let $\omega_p : \mathrm{Gal}(E/k) \to (\mathbb{Z}/p)^\times$ be the action of $\mathrm{Gal}(E/k)$ *on the p-th roots of unity in E (so $\omega_p = 1$ if $\zeta_p \notin E$). Then*

$$\overline{H_E/H_F}[p]^{\mathrm{ss}} = \sum_{\langle \rho \rangle} v_p(L(0, \langle \rho \rangle))\bar{\rho}^\vee,$$

an equality of representations of $\mathrm{Gal}(E/k)$, except for the ω_p-component ($\bar{\rho}^\vee$ denotes the contragredient of $\bar{\rho}$). If $\omega_p \neq 1$, we make no assertion on the ω_p-component in $\overline{H_E/H_F}[p]^{\mathrm{ss}}$, but if $\omega_p = 1$, there is no ω_p-component inside $\overline{H_E/H_F}[p]^{\mathrm{ss}}$.

Remark. For absolutely abelian fields, i.e., in the notation above, if E is an abelian extension of $\mathbb{Q}$, the conjecture above is known, and amounts to a conjecture of Gras [1977] which, for p not dividing the order of the Galois group, is proved by Mazur and Wiles [1984] as a consequence of their proof of the main conjecture, and for p dividing the order of the Galois group it is due to Solomon [1990].

4. Integrality of abelian *L*-values for $\mathbb{Q}$

The aim of this section is to prove certain results on integrality of $L(0, \chi)$ for χ an odd Dirichlet character of $\mathbb{Q}$ which are first examples of all the integrality conjectures made in this paper. Although these are all well known results, we have decided to give our proofs.

Lemma 4. *For integers $m > 1$ and $n > 1$, with $(m, n) = 1$, let $\chi = \chi_1 \times \chi_2$ be a primitive Dirichlet character on $(\mathbb{Z}/mn\mathbb{Z})^\times = (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ with $\chi(-1) = -1$. Then*

$$L(0, \chi) = -B_{1,\chi} = -\frac{1}{mn} \sum_{a=1}^{mn} a\chi(a)$$

is an algebraic integer, i.e., belongs to $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$.

Proof. Observe that $B_{1,\chi} = \frac{1}{mn} \sum_{a=1}^{mn} a\chi(a)$ has a possible fraction by mn, and that in this sum over $a \in \{1, 2, \ldots, mn\}$, if we instead sum over an arbitrary set A of integers which have these residues mod mn, then $\frac{1}{mn} \sum_{a \in A} a\chi(a)$ will differ from $B_{1,\chi}$ by an integral element (in $\overline{\mathbb{Z}}$). Since our aim is to prove that $B_{1,\chi}$ is integral, it suffices to prove that $\frac{1}{mn} \sum_{a \in A} a\chi(a)$ is integral for some set of representatives $A \subset \mathbb{Z}$ of residues mod mn.

For an integer $a \in \{1, 2, \ldots, m\}$, let $\bar{a}$ be an arbitrary integer whose reduction mod m is a, and whose reduction mod n is 1. Similarly, for an integer $b \in \{1, 2, \ldots, n\}$, let $\bar{b}$ be an arbitrary integer whose reduction mod n is b and whose reduction mod m is 1. Clearly, the set of integers $\bar{a} \cdot \bar{b}$ represents — exactly once — each residue class mod mn, and that $\bar{a} \cdot \bar{b}$ as an element in $\mathbb{Z}$ goes to the pair $(a, b) \in \mathbb{Z}/m \times \mathbb{Z}/n$. (It is important to note that $\bar{a} \cdot \bar{b}$ as an element in $\mathbb{Z}$ is *not* congruent

to *ab* mod *mn*, and therein lies a subtlety in the Chinese remainder theorem: there is no simple inverse to the natural isomorphism: $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n$.)

By definition of the character χ, $\chi(\bar{a} \cdot \bar{b}) = \chi_1(a)\chi_2(b)$. It follows that

$$(5) \qquad \frac{1}{mn} \sum \bar{a}\bar{b}\chi(\bar{a} \cdot \bar{b}) - \left[\frac{1}{m} \sum_{a=1}^{m} a\chi_1(a)\right] \cdot \left[\frac{1}{n} \sum_{b=1}^{n} b\chi_2(b)\right] \in \mathbb{Z}.$$

Since the character χ is odd, one of the characters, say χ_2, is even (and χ_1 is odd).

Observe that

$$B_{1,\chi_2} = \frac{1}{n} \sum_{b=1}^{n} b\chi_2(b) = \frac{1}{n} \sum_{b=1}^{n} (n-b)\chi_2(b).$$

It follows that

$$\frac{2}{n} \sum_{b=1}^{n} b\chi_2(b) = \sum_{b=1}^{n} \chi_2(b) = 0,$$

where the last sum is zero because the character χ_2 is assumed to be nontrivial.

Since

$$\frac{1}{mn} \sum \bar{a}\bar{b}\chi(\bar{a} \cdot \bar{b}) - \frac{1}{mn} \sum_{c=1}^{mn} c\chi(c) \in \mathbb{Z},$$

by (5), it follows that

$$\frac{1}{mn} \sum_{c=1}^{mn} c\chi(c) \in \mathbb{Z},$$

as desired.   □

Lemma 5. *For p a prime, let χ be a primitive Dirichlet character on $(\mathbb{Z}/p^n\mathbb{Z})^{\times}$ with $\chi(-1) = -1$. Write $(\mathbb{Z}/p^n\mathbb{Z})^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times} \times (1 + p\mathbb{Z}/1 + p^n\mathbb{Z})$, and the character χ as $\chi_1 \times \chi_2$ with respect to this decomposition. Then*

$$L(0, \chi) = -B_{1,\chi} = -\frac{1}{p^n} \sum_{a=1}^{p^n} a\chi(a)$$

is an algebraic integer, i.e., belongs to $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$ if and only if $\chi_1 \neq \omega_p^{-1}$. Further, if $\chi_1 = \omega_p^{-1}$,

$$L(0, \chi) = -B_{1,\chi} = -\frac{1}{p^n} \sum_{a=1}^{p^n} a\chi(a)$$

is the inverse of a uniformizer in the local field $\mathbb{Q}_p(B_{1,\chi}) = \mathbb{Q}_p(\chi)$ which is a totally ramified cyclic extension of $\mathbb{Q}_p$ of degree equal to the order of χ_2.

Proof. Assuming that $\chi_1 \neq \omega_p^{-1}$, we prove that $B_{1,\chi}$ belongs to $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$.

By an argument similar to the one used in the previous lemma, it can be checked that

$$\frac{1}{p^n} \sum_{a=1}^{p^n} a\chi(a) - \left[\frac{1}{p}\sum_{a=1}^{p} a\chi_1(a)\right] \cdot \left[\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}}(1+bp)\chi_2(1+bp)\right] \in \overline{\mathbb{Z}}.$$

If $\chi_1 \neq \omega_p^{-1}$, $\frac{1}{p}\sum_{a=1}^{p} a\chi_1(a)$ is easily seen to be integral. To prove the lemma, it then suffices to prove that $\left[\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}}(1+bp)\chi_2(1+bp)\right]$ is integral.

Note the isomorphism of the additive group $\mathbb{Z}_p$ with the multiplicative group $1+p\mathbb{Z}_p$ by the map $n \to (1+p)^n \in 1+p\mathbb{Z}_p$. Let $\chi_2(1+p) = \alpha$ with $\alpha^{p^{n-1}} = 1$.

Then (the first and third equalities below are up to $\overline{\mathbb{Z}}$)

$$\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}}(1+bp)\chi_2(1+bp) = \frac{1}{p^{n-1}}\sum_{c=1}^{p^{n-1}}(1+p)^c\alpha^c$$

$$= \frac{1}{p^{n-1}}\sum_{c=1}^{p^{n-1}}[\alpha(1+p)]^c$$

$$= \frac{1}{p^{n-1}}\frac{1-[\alpha(1+p)]^{p^{n-1}}}{1-\alpha(1+p)}$$

$$= \frac{1}{p^{n-1}}\frac{[1-(1+p)^{p^{n-1}}]}{[1-\alpha(1+p)]}.$$

Note that since $\alpha^{p^{n-1}} = 1$ either $\alpha = 1$, or $1-\alpha$ is a uniformizer in $\mathbb{Q}_p(\zeta_{p^d})$ for some $d \leq n-1$. Therefore, either $-p = [1-\alpha(1+p)]$ if $\alpha = 1$, or $[1-\alpha(1+p)]$ is a uniformizer in $\mathbb{Q}_p(\zeta_{p^d})$. Finally, it suffices to observe that

$$(1+p)^{p^{n-1}} \equiv 1 \bmod p^n;$$

hence, $\frac{1}{p^{n-1}}\sum_{b=1}^{p^{n-1}}(1+bp)\chi_2(1+bp)$ is integral.

If $\chi_1 = \omega_p^{-1}$, the same argument gives nonintegrality, and analyzing the proof gives the last assertion in the statement of the lemma regarding $B_{1,\chi}$ being a uniformizing parameter in the local field $\mathbb{Q}_p(B_{1,\chi}) = \mathbb{Q}_p(\chi)$; we omit the details. $\square$

Corollary 6. *For p a prime, let χ be a Dirichlet character on $(\mathbb{Z}/p^n\mathbb{Z})^{\times}$ with $\chi(-1) = -1$. Write $(\mathbb{Z}/p^n\mathbb{Z})^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times} \times (1+p\mathbb{Z}/1+p^n\mathbb{Z})$, and the character χ as $\chi_1 \times \chi_2$ with respect to this decomposition. Then*

$$\prod_{\substack{\chi=\chi_1\times\chi_2 \\ \chi_1=\omega_p^{-1}}} L(0,\chi)$$

belongs to $\mathbb{Q}_p$, and has valuation $-n$ as an element of $\mathbb{Q}_p$.

The following proposition follows by putting the previous two lemmas together, and making an argument similar to what went into the proof of these two lemmas. We omit the details.

Proposition 7. *Primitive odd Dirichlet characters* $\chi : (\mathbb{Z}/n)^\times \to \overline{\mathbb{Z}}_p^\times$ *for which* $L(0, \chi)$ *does not belong to* $\overline{\mathbb{Z}}_p$ *are exactly those for which*

(1) $n = p^d$ *and*

(2) $\chi = \omega_p^{-1} \mod \mathfrak{p}$.

The following consequence of the proposition suggests that prudence is to be exercised when discussing congruences of L-values for Artin representations which are congruent.

Corollary 8. *Let* p, q *be odd primes with* $p \mid (q - 1)$. *For any character* χ_2 *of* $(\mathbb{Z}/q\mathbb{Z})^\times$ *of order* p, *define the character* $\chi = \omega_p^{-1} \times \chi_2$ *of* $(\mathbb{Z}/pq\mathbb{Z})^\times$. *Then although the characters* ω_p^{-1} *and* χ *have the same reduction modulo* p, $L(0, \omega_p^{-1})$ *is p-adically nonintegral whereas* $L(0, \chi)$ *is integral.*

Question. Let $\chi : (\mathbb{Z}/p^d m)^\times \to \overline{\mathbb{Z}}_p^\times$ with $(p, m) = 1, m > 1$, be a primitive Dirichlet character for which $\chi = \omega_p^{-1} \mod \mathfrak{p}$ so that by Proposition 7, $L(0, \chi)$ is $\mathfrak{p}$-integral. Is it possible to have $L(0, \chi) = 0$ modulo $\mathfrak{p}$, the maximal ideal of $\overline{\mathbb{Z}}_p$? Our proofs in this section are "up to $\overline{\mathbb{Z}}$", so good to detect integrality, but not good for questions modulo $\mathfrak{p}$. The question is relevant to Conjecture 3 to see if the character ω_p appears in the class group H/H^+ for $E = \mathbb{Q}(\zeta_{p^d m})$; such a character is known not to appear in the class group of H/H^+ for $E = \mathbb{Q}(\zeta_{p^d})$.

5. Congruences and their failure for L-values

This paper considers integrality properties of certain Artin L-functions at 0. It may seem most natural that if two such Artin representations $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ have the same semisimplification mod p and do not contain the character ω_p^{-1}, then $L(0, \rho_1)$ and $L(0, \rho_2)$, which are in $\overline{\mathbb{Z}}_p$ by Conjecture 1, have the same reduction mod p. This is not true even in the simplest case of Dirichlet characters for $\mathbb{Q}$. It is possible to fix this problem for abelian characters of $\mathbb{Q}$, and more generally for any totally real number field, which is what this section strives to do; see Proposition 13. The recipe given in Proposition 13 immediately suggests itself in the nonabelian case, but we have not spelled it out.

The problem that we find dealing with abelian characters χ_1, χ_2 is that they may be congruent for some prime, but may have different conductors in which case it is not the L-values $L(0, \chi_1)$ and $L(0, \chi_2)$ which are congruent, but a modified L-value, say $L_f(0, \chi)$, which gives the right congruence; these L-values are products of $\prod_\wp (1 - \chi(\wp))$ with $L(0, \chi)$ where $\wp$ are all primes dividing either the conductor of χ_1 or of χ_2.

We begin with some elementary lemmas which go into congruences of L-values at 0 of Dirichlet characters, and then we consider totally real number fields.

Lemma 9. *Let V be a vector space over $\mathbb{Q}$, and $\chi = \chi_f : \mathbb{Z}/f \to V$ be any function with the property that $\sum_{a=1}^{f} \chi(a) = 0$. Let χ_{df} be the function on $\mathbb{Z}/df$ obtained from χ by composing with the natural map $\mathbb{Z}/df \to \mathbb{Z}/f$. Then:*

(1) $L(0, \chi) := \frac{1}{f} \sum_{a=1}^{f} a\chi(a) = \frac{1}{df} \sum_{a=1}^{df} a\chi_{df}(a) := L(0, \chi_{df})$.

(2) *Let $\chi : (\mathbb{Z}/f)^\times \to \mathbb{C}^\times$ be a primitive character of conductor f with $\chi \neq 1$. Then for any $f \mid f'$,*

$$\frac{1}{f'} \sum_{\substack{a=1 \\ (a,f')=1}}^{f'} a\chi(a) = \prod_{p \mid f'} (1 - \chi(p)) L(0, \chi).$$

Proof. Observe that

$$\sum_{a=1}^{df} a\chi_{df}(a) = \sum_{a=1}^{f} \sum_{i=0}^{d-1} (a+if)\chi_{df}(a+if)$$

$$= \sum_{a=1}^{f} \sum_{i=0}^{d-1} (a+if)\chi(a)$$

$$= \sum_{a=1}^{f} \left[da\chi(a) + \frac{fd(d-1)}{2}\chi(a) \right]$$

$$= d \sum_{a=1}^{f} a\chi(a),$$

where in the last step we have used that $\sum_{a=1}^{f} \chi(a) = 0$. The proof of part (1) of the lemma follows.

The proof of part (2) will proceed in several steps, according to the value of f'. Observe first that if f and f' have the same prime divisors, then $(a, f) = 1$ if and only $(a, f') = 1$. Therefore,

$$\frac{1}{f'} \sum_{\substack{a=1 \\ (a,f')=1}}^{f'} a\chi(a) = \frac{1}{f'} \sum_{a=1}^{f'} a\chi_{f'}(a) = \frac{1}{f} \sum_{a=1}^{f} a\chi_f(a),$$

where the second equality is a consequence of part (1) of the lemma. In this case, i.e., when f and f' have the same prime divisors, for all $p \mid f'$, $\chi(p) = 0$. It follows that $\prod_{p \mid f'} (1 - \chi(p)) = 1$, proving this case of part (2) of the lemma.

Assume next that $f' = fp^m$, $m \geq 1$ and p a prime with $(f, p) = 1$. In this case note that (using the notation of $L(0, \chi_{fp^m})$ introduced in part (1) of the lemma),

$$L(0, \chi_{fp^m}) = \frac{1}{fp^m} \sum_{\substack{a=1 \\ (a, fp^m)=1}}^{fp^m} a\chi(a) + \frac{1}{fp^m} \sum_{i=1}^{fp^{m-1}} (pi)\chi_{fp^{m-1}}(pi)$$

$$= \frac{1}{fp^m} \sum_{\substack{a=1 \\ (a, fp^m)=1}}^{fp^m} a\chi(a) + \chi(p)L(0, \chi_{fp^{m-1}}).$$

Since by part (1) of the lemma, $L(0, \chi_{fp^m}) = L(0, \chi_{fp^{m-1}})$, the proof of part (2) follows in this case.

For general $f' = df''$, with f'' having the same prime divisors as f, and d having prime divisors which are coprime to those of f, let $d = p_1^{m_1} \cdots p_r^{m_r}$. We argue by induction on r, thus assuming the result for $d_{r-1} = p_1^{m_1} \cdots p_{r-1}^{m_{r-1}}$, adding the prime power $p_r^{m_r}$ at the end which proves (2) for $d = p_1^{m_1} \cdots p_r^{m_r}$ using part (1), and part of (2) just proved for prime powers (to be used for $p_r^{m_r}$).   □

Lemma 10. *Let $\chi_1, \chi_2 : (\mathbb{Z}/f)^\times \to \overline{\mathbb{Z}}_p^\times$ be two (not necessarily primitive) odd characters. Consider χ_1, χ_2 as functions on $\mathbb{Z}/f$ by declaring their values outside of $(\mathbb{Z}/f)^\times$ to be zero. Assume that the reductions mod $\wp$, $\overline{\chi}_1, \overline{\chi}_2 : (\mathbb{Z}/f)^\times \to \overline{\mathbb{F}}_p^\times$, are the same. If $p \mid f$, assume that neither of the $\overline{\chi}_1, \overline{\chi}_2 : (\mathbb{Z}/f)^\times \to \overline{\mathbb{F}}_p^\times$ factors through $(\mathbb{Z}/p)^\times \to \overline{\mathbb{F}}_p^\times$ to give ω_p^{-1} where ω_p is the natural map from $(\mathbb{Z}/p)^\times$ to $\mathbb{F}_p^\times$. Then $L_f(0, \chi_1) := \frac{1}{f} \sum_{a=1}^f a\chi_1(a)$ and $L_f(0, \chi_2) := \frac{1}{f} \sum_{a=1}^f a\chi_2(a)$ are in $\overline{\mathbb{Z}}_p$, and have the same reduction to $\overline{\mathbb{F}}_p$.*

Proof. By the hypothesis in the lemma, there is a $b \in (\mathbb{Z}/f)^\times$ such that $[b\chi_1(b)-1] \in \overline{\mathbb{Z}}_p^\times$, and hence also $[b\chi_2(b) - 1] \in \overline{\mathbb{Z}}_p^\times$. Fix such a $b \in (\mathbb{Z}/f)^\times$.

For $a \in \{1, \ldots, f\}$, write

$$ab = [ab] + \lambda_a f,$$

with $[ab] \in \{1, \ldots, f\}$.

From the definition of $L_f(0, \chi_1)$,

$$b\chi_1(b)L_f(0, \chi_1) = \frac{1}{f} \sum_{a=1}^f ab\chi_1(ab).$$

As b is invertible in $\mathbb{Z}/f$, $a \to [ab]$ is a bijection on $\{1, \ldots, f\}$; therefore, the above equation yields

$$(6) \qquad\qquad [b\chi_1(b) - 1]L_f(0, \chi_1) = \sum_{a=1}^f \lambda_a \chi_1(ab).$$

Similarly,

$$(7) \qquad [b\chi_2(b) - 1]L_f(0, \chi_2) = \sum_{a=1}^{a=f} \lambda_a \chi_2(ab).$$

Since χ_1, χ_2 are congruent, the right-hand sides of (6) and (7) are the same in $\bar{\mathbb{F}}_p$, and by the choice of b made in the beginning of the proof of the lemma, $[b\chi_1(b)-1]$ as well as $[b\chi_2(b) - 1]$ are in $\bar{\mathbb{F}}_p^{\times}$, and are the same; thus, it follows that $L_f(0, \chi_1)$ and $L_f(0, \chi_2)$ are in $\bar{\mathbb{Z}}_p$, and are the same in $\bar{\mathbb{F}}_p$. □

Proposition 11. *Let f_1, f_2 be integers, and f any integer divisible by both f_1, f_2. Suppose χ_1 and χ_2 are primitive odd Dirichlet characters of conductors f_1 and f_2 with values in $\bar{\mathbb{Z}}_p^{\times}$, respectively. If $p \mid f$, assume that neither of the $\bar{\chi}_1, \bar{\chi}_2 :$ $(\mathbb{Z}/f)^{\times} \to \bar{\mathbb{F}}_p^{\times}$ factor through $(\mathbb{Z}/p)^{\times} \to \bar{\mathbb{F}}_p^{\times}$ to give ω_p^{-1} where ω_p is the natural map from $(\mathbb{Z}/p)^{\times}$ to $\bar{\mathbb{F}}_p^{\times}$. Then $L_f(0, \chi_1) := \frac{1}{f}\sum_{a=1}^{f} a\chi_1(a)$ (where χ_1 is considered as a function on $\mathbb{Z}/f$ zero outside $(\mathbb{Z}/f)^{\times}$) has the value given by*

$$L_f(0, \chi_1) = \prod_{p\mid f}(1 - \chi_1(p)) \cdot L(0, \chi_1)$$

and similarly for $L_f(0, \chi_2)$. Both $L(0, \chi_1)$ and $L(0, \chi_2)$ are $\bar{\mathbb{Z}}_p$, and if χ_1 and χ_2 are congruent modulo the maximal ideal in $\bar{\mathbb{Z}}_p$, so is the case for $L_f(0, \chi_1)$ and $L_f(0, \chi_2)$.

Proof. $L_f(0, \chi_1) := \frac{1}{f}\sum_{a=1}^{f} a\chi_1(a)$ has the value as asserted in the proposition by part (2) of Lemma 9, and their congruence holds by Lemma 10. □

Corollary 12. *If χ_1 and χ_2 have conductors f_1 and f_2 such that the prime divisors of f_1 and f_2 are the same, then for f which is the least common multiple of f_1 and f_2, $L_f(0, \chi_1) = L(0, \chi_1)$ and $L_f(0, \chi_2) = L(0, \chi_2)$; hence, if χ_1 and χ_2 are congruent, so are $L(0, \chi_1)$ and $L(0, \chi_2)$. On the other hand, suppose $f_1 = p$, $f_2 = pq$, and $\chi_2 = \chi_1 \times \alpha : (\mathbb{Z}/p)^{\times} \times (\mathbb{Z}/q)^{\times} = (\mathbb{Z}/pq)^{\times} \to \bar{\mathbb{Z}}_p^{\times}$ with $\bar{\alpha} = 1$; then*

$$L_{pq}(0, \chi_2) = L(0, \chi_2),$$
$$L_{pq}(0, \chi_1) = (1 - \chi_1(q))L(0, \chi_1).$$

Since $L_{pq}(0, \chi_1)$ and $L_{pq}(0, \chi_2)$ are congruent mod $\wp$, we find that if $L(0, \chi_1)$ and $L(0, \chi_2)$ are not both zero mod $\wp$, they cannot be the same mod $\wp$ since $(1 - \chi_1(q))$ cannot be 1 mod $\wp$.

Remark. The hypothesis that the reduction mod $\wp$ of $\chi : (\mathbb{Z}/f)^{\times} \to \bar{\mathbb{Z}}_p^{\times}$ does not factor through $(\mathbb{Z}/p)^{\times} \to \bar{\mathbb{F}}_p^{\times}$ to give ω_p^{-1} is stronger than what is required for p-integrality of $L(0, \chi)$. For example, by Lemma 4, $L(0, \chi)$ is integral if the conductor of χ has two distinct prime factors, say $f = pq$, with $(\mathbb{Z}/f)^{\times} = (\mathbb{Z}/p)^{\times} \times (\mathbb{Z}/q)^{\times}$, and $\chi = \alpha \times \beta$. In Lemma 10 we would be excluding characters χ for which $\bar{\alpha} = \omega_p^{-1}$, and $\bar{\beta} = 1$.

Here is the more general version of the previous proposition.

Proposition 13. *Let k be a totally real number field with $G = \mathrm{Gal}(\bar{\mathbb{Q}}/k)$ its absolute Galois group. For $\chi : G \to \bar{\mathbb{Z}}_p^\times$, a character of finite order of G, which is also to be considered as a character of the group of ideals coprime to a nonzero ideal $\mathfrak{f}$ in k by class field theory (so $\mathfrak{f}$ is divisible by the conductor of χ, but may not be the conductor of χ), let $L(s, \chi)$ be the "true" L-function associated to the character χ, and define $L_{\mathfrak{f}}(s, \chi)$ by*

$$L_{\mathfrak{f}}(s, \chi) = \sum_{(\mathfrak{a},\mathfrak{f})=1} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s},$$

where $N\mathfrak{a}$ denotes the norm of an integral ideal $\mathfrak{a}$ in k. Then:

(1)
$$L_{\mathfrak{f}}(s, \chi) = \prod_{\wp | \mathfrak{f}} \left(1 - \frac{\chi(\wp)}{(N\wp)^s}\right) \cdot L(s, \chi).$$

(2) *For any integral ideals $\mathfrak{c}$ in k coprime to $p\mathfrak{f}$, integers $k \geq 1$,*

$$\Delta_{\mathfrak{c}}(1 - k, \chi) = (1 - \chi(\mathfrak{c})N\mathfrak{c}^k)L_{\mathfrak{f}}(1 - k, \chi)$$

are in $\bar{\mathbb{Z}}_p$.

(3) *If χ_1 and χ_2 are two characters of G with values in $\bar{\mathbb{Z}}_p^\times$ with conductors dividing $\mathfrak{f}$, such that neither of the two reductions $\bar{\chi}_1, \bar{\chi}_2 : G \to \bar{\mathbb{F}}_p^\times$ is ω_p^{-1}, then $L_{\mathfrak{f}}(0, \chi_1)$ and $L_{\mathfrak{f}}(0, \chi_2)$ are in $\bar{\mathbb{Z}}_p$, and if χ_1 and χ_2 are congruent modulo the maximal ideal in $\bar{\mathbb{Z}}_p$, so is the case for $L_{\mathfrak{f}}(0, \chi_1)$ and $L_{\mathfrak{f}}(0, \chi_2)$.*

Proof. Deligne and Ribet [1980, Theorem 0.4] (see also [Ribet 1979, Theorem 2.1, Proposition 1.4]) prove integrality of $\Delta_{\mathfrak{c}}(1 - k, \chi)$, as well as the congruence between $\Delta_{\mathfrak{c}}(1 - k, \chi_1)$ and $\Delta_{\mathfrak{c}}(1 - k, \chi_2)$.

The final congruence between $L_{\mathfrak{f}}(0, \chi_1)$ and $L_{\mathfrak{f}}(0, \chi_2)$ follows as in Lemma 10 by choosing an integral ideal $\mathfrak{c}$ coprime to $p\mathfrak{f}$ such that $(1 - \chi(\mathfrak{c})N\mathfrak{c})$ is a unit in $\bar{\mathbb{Z}}_p$ which follows just as in Lemma 10 for $\chi = \chi_1$ (hence for $\chi = \chi_2$ too), because $\bar{\chi}_1 : G \to \bar{\mathbb{F}}_p^\times$ is not ω_p^{-1} (see in the beginning of [Ribet 1979, §2] how the "norm map" under the identification of characters on ideals coprime to $\mathfrak{f}$ to characters of G becomes action of G on p-power roots of identity).   □

The discussion in this section leads us to the following conjecture.

Conjecture 14. *Let k be a totally real number field and p an odd prime. Let $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/k) \to \mathrm{GL}_n(\bar{\mathbb{F}}_p)$ be a set of semisimple modular representations of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$ with $\bar{\rho}(c) = -1$, where c is a complex conjugation in $\mathrm{Gal}(\bar{\mathbb{Q}}/k)$. Assume that the set of representations $\bar{\rho}$ considered are unramified outside a fixed finite set of finite places S of k, and that $\omega \otimes \bar{\rho}$ does not contain the*

trivial representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ *where* ω *is the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ *on the* p-th *roots of unity. Then it is possible to define* $\bar{L}_S(0, \bar{\rho}) \in \overline{\mathbb{F}}_p$ *with*

$$\bar{L}_S(0, \bar{\rho}_1 + \bar{\rho}_2) = \bar{L}_S(0, \bar{\rho}_1) \cdot \bar{L}_S(0, \bar{\rho}_2),$$

for any two such representations $\bar{\rho}_1$ *and* $\bar{\rho}_2$*, and such that, if* $\bar{\rho}$ *arises as the semisimplification of reduction mod* p *of a representation* $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ *with* $\rho(c) = -1$*, where* c *is a complex conjugation in* $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$*, then*

$$L_S(0, \rho) = L(0, \rho) / \prod_{v \in S} L(0, \rho_v),$$

which belongs to $\overline{\mathbb{Z}}_p$ *by [Conjecture 1](#), has its reduction mod* p *to be* $\bar{L}_S(0, \bar{\rho})$.

The conjecture above requires that if two representations $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/k) \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ have the same semisimplification mod p, then $L_S(0, \rho_1)$ and $L_S(0, \rho_2)$ are in $\overline{\mathbb{Z}}_p$ and have the same reduction mod p. By a well known theorem of Brauer, a modular representation $\bar{\rho}$ can be lifted to a virtual representation $\sum n_i \rho_i$ in characteristic 0. However, since $L(0, \rho_i)$ may be zero mod p, for some i (for which $n_i < 0$), the theorem of Brauer does not guarantee that $\bar{L}_S(0, \bar{\rho})$ can be defined.

Acknowledgements

References

[Deligne and Ribet 1980] P. Deligne and K. A. Ribet, "Values of abelian L-functions at negative integers over totally real fields", *Invent. Math.* **59**:3 (1980), 227–286. MR Zbl

[Gras 1977] G. Gras, "Étude d'invariants relatifs aux groupes des classes des corps abéliens", pp. 35–53 in *Journées Arithmétiques de Caen* (Caen, 1976), Astérisque **41–42**, Soc. Math. France, Paris, 1977. MR Zbl

[Mazur and Wiles 1984] B. Mazur and A. Wiles, "Class fields of abelian extensions of **Q**", *Invent. Math.* **76**:2 (1984), 179–330. MR Zbl

[Ribet 1976] K. A. Ribet, "A modular construction of unramified p-extensions of $Q(\mu_p)$", *Invent. Math.* **34**:3 (1976), 151–162. MR Zbl

[Ribet 1979] K. A. Ribet, "Report on p-adic L-functions over totally real fields", pp. 177–192 in *Journées Arithmétiques de Luminy* (Luminy, 1978), Astérisque **61**, Soc. Math. France, Paris, 1979. MR Zbl

[Solomon 1990] D. Solomon, "On the classgroups of imaginary abelian fields", *Ann. Inst. Fourier* (*Grenoble*) **40**:3 (1990), 467–492. MR Zbl

[Tate 1984] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Mathematics **47**, Birkhäuser, Boston, 1984. MR Zbl

[Washington 1982] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Springer, 1982. MR Zbl

[Wiles 1990] A. Wiles, "The Iwasawa conjecture for totally real fields", *Ann. of Math.* (2) **131**:3 (1990), 493–540. MR Zbl

DIPENDRA PRASAD
INDIAN INSTITUTE OF TECHNOLOGY BOMBAY
MUMBAI
INDIA

and

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
MUMBAI
INDIA

and

LABORATORY OF MODERN ALGEBRA AND APPLICATIONS
SAINT PETERSBURG STATE UNIVERSITY
SAINT PETERSBURG
RUSSIA

prasad.dipendra@gmail.com

PACIFIC JOURNAL OF MATHEMATICS