



HAL
open science

Numerical evidence toward a 2-adic equivariant "Main Conjecture"

Xavier-François Roblot, Alfred Weiss

► **To cite this version:**

Xavier-François Roblot, Alfred Weiss. Numerical evidence toward a 2-adic equivariant "Main Conjecture". *Experimental Mathematics*, 2011, 20 (2), pp.169-176. hal-00863157

HAL Id: hal-00863157

<https://hal.science/hal-00863157>

Submitted on 19 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

NUMERICAL EVIDENCE TOWARD A 2-ADIC EQUIVARIANT “MAIN CONJECTURE”

XAVIER-FRANÇOIS ROBLOT* AND ALFRED WEISS†

1. THE CONJECTURE

Let K be a totally real finite Galois extension of \mathbb{Q} with Galois group G dihedral of order 8, and suppose that $\sqrt{2}$ is not in K . Fix a finite set S of primes of \mathbb{Q} including $2, \infty$ and all primes that ramify in K . Let C be the cyclic subgroup of G of order 4 and F the fixed field of C acting on K . Fix a 2-adic unit $u \equiv 5 \pmod{8\mathbb{Z}_2}$.

Write $L_F(s, \chi)$ for the 2-adic L -functions, normalized as in [W], of the 2-adic characters χ of C or, equivalently by class field theory, of the corresponding 2-adic primitive ray class characters. We always work with their S -truncated forms

$$L_{F,S}(s, \chi) = L_F(s, \chi) \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})} \langle N(\mathfrak{p}) \rangle^{1-s} \right)$$

where \mathfrak{p} runs through all primes of F above $S \setminus \{2, \infty\}$, and $\langle \cdot \rangle : \mathbb{Z}_2^\times \rightarrow 1 + 4\mathbb{Z}_2$ is the unique function with $\langle x \rangle x^{-1} \in \{-1, 1\}$ for all x . Now our interest is in the 2-adic function

$$f_1(s) = \frac{\rho_{F,S} \log(u)}{8(u^{1-s} - 1)} + \frac{1}{8} (L_{F,S}(s, 1) + L_{F,S}(s, \beta^2) - 2L_{F,S}(s, \beta))$$

where β is a faithful irreducible 2-adic character of C and

$$\rho_{F,S} = \lim_{s \rightarrow 1} (s-1)L_{F,S}(s, 1).$$

It follows from known results that $\frac{1}{2}\rho_{F,S} \in \mathbb{Z}_2$ and that $f_1(s)$ is an *Iwasawa analytic* function of $s \in \mathbb{Z}_2$, in the sense of [R]. This means that there is a unique power series $F_1(T) \in \mathbb{Z}_2[[T]]$ so that

$$F_1(u^n - 1) = f_1(1 - n) \quad \text{for } n = 1, 2, 3, \dots$$

The conjecture we want to test is

Conjecture 1.

$$\frac{1}{2}\rho_{F,S} \in 4\mathbb{Z}_2 \quad \text{and} \quad F_1(T) \in 4\mathbb{Z}_2[[T]].$$

*supported by the *projet AlgoL* (ANR-07-BLAN-0248).

†financial support from the NSERC is gratefully acknowledged.

Testing the conjecture amounts to calculating $\frac{1}{2}\rho_{F,S}$ and (many of) the power series coefficients of

$$F_1(T) = \sum_{j=1}^{\infty} x_j T^{j-1}$$

modulo $4\mathbb{Z}_2$. Were the conjecture false we would expect to find a counterexample in this way.

The idea of the calculation is, roughly, to express the coefficients of the power series $F_1(T)$ as integrals over suitable 2-adic continuous functions with respect to the measures used to construct the 2-adic L -functions.

The conjecture has been tested for 60 fields K determined by the size of their discriminant and the splitting of 2 in the field F . For this purpose, it is convenient to replace the datum K by F together with the ray class characters of F which determine K (cf §5). A description of the results is in §6: they are affirmative.

Where does $f_1(s)$ come from? It is an example which arises by attempting to refine the Main Conjecture of Iwasawa theory. This connection will be discussed next in order to prove that $F_1(T)$ is in $\mathbb{Z}_2[[T]]$.

2. THE MOTIVATION

The Main Conjecture of classical Iwasawa theory was proved by Wiles [W] for odd prime numbers ℓ . More recently [RW2], an equivariant “main conjecture” has been proposed, which would both generalize and refine the classical one for the same ℓ . When a certain μ -invariant vanishes, as is expected for odd ℓ (by a conjecture of Iwasawa), this equivariant “main conjecture”, up to its uniqueness assertion, depends only on properties of ℓ -adic L -functions, by Theorem A of [RW3].

The point is that it is possible to numerically test this Theorem A property of ℓ -adic L -functions, at least in simple special cases when it may be expressed in terms of congruences and the special values of these L -functions can be computed. The conjecture of §1 is perhaps the simplest non-abelian example when this happens, but with the price of taking $\ell = 2$. Although there are some uncertainties about the formulation of the “main conjecture” for $\ell = 2$, partly because [W] applies only in the cyclotomic case, it seems clearer what the 2-adic analogue of the Theorem A properties of L -functions should be, in view of their “extra” 2-power divisibilities [DR].

More precisely, let $L_{k,S} \in \text{Hom}^*(R_\ell(G_\infty), \mathcal{Q}^c(\Gamma_k)^\times)$ be the “power series” valued function of ℓ -adic characters χ of $G_\infty = \text{Gal}(K_\infty/k)$ defined in §4 of [RW2]. This is made from the values of ℓ -adic L -functions by viewing them as a quotient of Iwasawa analytic functions, by the proof of Proposition 11 in [RW2]. When $\ell \neq 2$, the vanishing of the μ -invariant mentioned above means precisely that the coefficients of these power series have no nontrivial common divisor; and the Theorem A property of L -functions is that then $L_{k,S}$ is in $\text{Det}(K_1(\Lambda(G_\infty)_\bullet))$ (see next section for precise definitions).

When $\ell = 2$, we can still form $L_{k,S}$, but now its values at characters χ of degree 1 have numerators divisible by $2^{[k:\mathbb{Q}]}$, because of (4.8), (4.9) of [R]. Define

$$\tilde{L}_{k,S}(\chi) = 2^{-[k:\mathbb{Q}]\chi(1)} L_{k,S}(\chi)$$

for all 2-adic characters χ of G_∞ , so that the deflation and restriction properties of Proposition 12 of [RW2] are maintained. Then the analogous coprimality condition on the coefficients of the “power series” values $\tilde{L}_{k,S}(\chi)$, for all characters χ , will be referred to as vanishing of the $\tilde{\mu}$ -invariant of K_∞/k : the Theorem A property we want to test is therefore

Conjecture 2.

$$\tilde{L}_{k,S} \text{ is in } \text{Det} (K_1(\Lambda(G_\infty)_\bullet)).$$

Remark 2.1. a) When Conjecture 2 holds, then $\tilde{L}_{k,S}(\chi)$ is in $\Lambda^c(\Gamma_k)_\bullet^\times$ for all $\chi \in R_2(G_\infty)$, implying the vanishing of the $\tilde{\mu}$ -invariant of K_∞/k .

b) For $\ell \neq 2$, some cases of the equivariant “main conjecture” have recently been proved ([RW]).

3. INTERPRETING CONJECTURE 2 AS A CONGRUENCE

We now specialize to the situation of §1, so use the notation of its first paragraph, in order to exhibit a congruence equivalent to Conjecture 2 (see Figure 1).

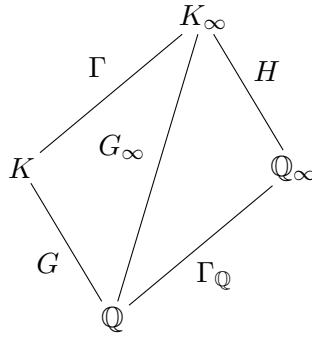


FIGURE 1

Let \mathbb{Q}_∞ be the cyclotomic \mathbb{Z}_2 -extension of \mathbb{Q} , i.e. the maximal totally real subfield of the field obtained from \mathbb{Q} by adjoining all 2-power roots of unity, and set $\Gamma_\mathbb{Q} = \text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_2$. Let $K_\infty = K\mathbb{Q}_\infty$, noting that $K \cap \mathbb{Q}_\infty = \mathbb{Q}$ follows from $\sqrt{2} \notin K$, and set $G_\infty = \text{Gal}(K_\infty/\mathbb{Q})$. Defining $\Gamma = \ker(G_\infty \rightarrow G)$, $H = \ker(G_\infty \rightarrow \Gamma_\mathbb{Q})$, we now have $H \hookrightarrow G_\infty \twoheadrightarrow \Gamma_\mathbb{Q}$ in the notation of [RW2].

Since $G_\infty = \Gamma \times H$ with $\Gamma \simeq \Gamma_\mathbb{Q}$ and $H \simeq G$ dihedral of order 8 we can understand the structure of

$$\Lambda(G_\infty)_\bullet = \Lambda(\Gamma)_\bullet \otimes_{\mathbb{Z}_2} \mathbb{Z}_2[H] = \Lambda(\Gamma)_\bullet[H]$$

where \bullet means “invert all elements of $\Lambda(\Gamma) \setminus 2\Lambda(\Gamma)$.”

Namely, choose σ, τ in G so that $C = \langle \tau \rangle$ with $\sigma^2 = 1$, $\sigma\tau\sigma^{-1} = \tau^{-1}$ and extend them to K_∞ , with trivial action on \mathbb{Q}_∞ , to get s, t respectively. Then the abelianization of H is $H^{ab} = H/\langle t^2 \rangle$ and we get a pullback diagram

$$\begin{array}{ccc} \Lambda(G_\infty)_\bullet = \Lambda(\Gamma)_\bullet[H] & \longrightarrow & (\Lambda(\Gamma)_\bullet(\zeta_4)) * \langle s \rangle \\ \downarrow & & \downarrow \\ \Gamma(G_\infty^{ab})_\bullet = \Lambda(\Gamma)_\bullet[H^{ab}] & \longrightarrow & \Lambda(\Gamma)_\bullet[H^{ab}]/2\Lambda(\Gamma)_\bullet[H^{ab}] \end{array}$$

where the upper right term is the crossed product order with $\Lambda(\Gamma)_\bullet$ -basis $1, \zeta_4, \tilde{s}, \zeta_4\tilde{s}$ with $\zeta_4^2 = -1$, $\tilde{s}^2 = 1$, $\tilde{s}\zeta_4 = \zeta_4^{-1}\tilde{s} = -\zeta_4\tilde{s}$ and the top map takes t, s to ζ_4, \tilde{s} respectively, the right map takes ζ_4, \tilde{s} to t^{ab}, s^{ab} . This diagram originates in the pullback diagram for the cyclic group $\langle t \rangle$ of order 4, then going to the dihedral group ring $\mathbb{Z}_2[H]$ by incorporating the action of s , and finally applying $\Lambda(\Gamma)_\bullet \otimes_{\mathbb{Z}_2} -$.

We now turn to getting the first version of our congruence in terms of the pullback diagram above. This is possible since $R^\times \rightarrow K_1(R)$ is surjective for all the rings considered there. We also simplify notation a little by setting $\mathfrak{A} = (\Lambda(\Gamma)_\bullet(\zeta_4)) * \langle s \rangle$ and writing $\tilde{L}_{k,S}$ as $\tilde{L}_{K_\infty/k}$, because we will now have to vary the fields and S is fixed anyway. The dihedral group G has 4 degree 1 irreducible characters $1, \eta, \nu, \eta\nu$ with $\eta(\tau) = 1$, $\nu(\sigma) = 1$ and a unique degree 2 irreducible α , which we view as characters of G_∞ by inflation.

Proposition 3.1. *Let K_∞^{ab} be the fixed field of $\langle t^2 \rangle$, hence $\text{Gal}(K_\infty^{ab}/\mathbb{Q}) = G_\infty^{ab}$. Then*

- a) $\tilde{L}_{K_\infty^{ab}/\mathbb{Q}} = \text{Det}(\tilde{\Theta}^{ab})$ for some $\tilde{\Theta}^{ab} \in \Lambda(G_\infty^{ab})_\bullet^\times$
- b) $\tilde{L}_{K_\infty^{ab}/\mathbb{Q}} \in \text{Det}(K_1(\Lambda(G_\infty)_\bullet))$ if, and only if, any $y \in \mathfrak{A}$ mapping to $\tilde{\Theta}^{ab} \pmod{2}$ in $\Lambda(G_\infty^{ab})_\bullet/2\Lambda(G_\infty^{ab})_\bullet$ has

$$nr(y) \equiv \tilde{L}_{K_\infty^{ab}/\mathbb{Q}}(\alpha) \pmod{4\Lambda(\Gamma_\mathbb{Q})_\bullet}$$

where nr is the reduced norm of (the total ring of fractions of) \mathfrak{A} to its centre $\Lambda(\Gamma)_\bullet$ and we identify $\Lambda(\Gamma)_\bullet$ with $\Lambda(\Gamma_\mathbb{Q})_\bullet$ via $\Gamma \xrightarrow{\sim} \Gamma_\mathbb{Q}$.

Proof. a) The vanishing of $\tilde{\mu}$ for K_∞/\mathbb{Q} , in the sense of §2, is known by [FW], i.e. $\tilde{L}_{K_\infty^{ab}/\mathbb{Q}}(\chi)$ is a unit in $\Lambda(\Gamma_\mathbb{Q})_\bullet$ for all 2-adic characters χ of G_∞^{ab} . By the proof of Theorem 9 in [RW3] we have $L_{K_\infty^{ab}/\mathbb{Q}} = \text{Det}(\lambda)$ with $\lambda \in \Lambda(G_\infty^{ab})_\bullet$ the pseudomeasure of Serre. The point is then that $\lambda = 2\tilde{\Theta}^{ab}$ with $\tilde{\Theta}^{ab} \in \Lambda(G_\infty^{ab})_\bullet$, which follows from Theorem 3.1b) of [R], because of Theorem 4.1 (loc.cit.) and the relation between λ and μ_c discussed just after it. Then $\tilde{L}_{K_\infty^{ab}/\mathbb{Q}} = \text{Det}(\tilde{\Theta}^{ab})$ and now the proof of the Corollary to Theorem 9 in [RW3] shows that $\tilde{\Theta}^{ab}$ is a unit of $\Lambda(G_\infty^{ab})$.

b) *Claim:* $nr(1 + 2\mathfrak{A}) = 1 + 4\Lambda(\Gamma)_\bullet$.

Proof of the claim. If $x = a1 + b\zeta_4 + c\tilde{s} + d\zeta_4\tilde{s}$ with $a, b, c, d \in \Lambda(\Gamma)_\bullet$, one computes $nr(x) = (a^2 + b^2) - (c^2 + d^2)$ from which $nr(1 + 2\mathfrak{A}) \subseteq 1 + 4\Lambda(\Gamma)_\bullet$; equality follows from $nr((1 + 2a) + 2a\tilde{s}) = (1 + 2a)^2 - (2a)^2 = 1 + 4a$ for $a \in \Lambda(\Gamma)_\bullet$. \square

Suppose first that the congruence for $\tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$ holds. Start with $\tilde{\Theta}^{ab}$ from a) in the lower left corner of the pullback square and map it to $\tilde{\Theta}^{ab} \bmod 2$ in the lower right corner. Choosing any $y_0 \in \mathfrak{A}$ mapping to $\tilde{\Theta}^{ab} \bmod 2$, we note that $y_0 \in \mathfrak{A}^\times$ because the maps in the pullback diagram are ring homomorphisms and the kernel $2\mathfrak{A}$ of the right one is contained in the radical of \mathfrak{A} . Thus $nr(y_0) \in \Lambda(\Gamma)_\bullet^\times$ has $nr(y_0)^{-1}\tilde{L}_{K_\infty/\mathbb{Q}}(\alpha) \in 1 + 4\Lambda(\Gamma_\mathbb{Q})_\bullet$ by the congruence, hence, by the Claim, $nr(y_0)^{-1}\tilde{L}_{K_\infty/\mathbb{Q}}(\alpha) = nr(z)$, $z \in 1 + 2\mathfrak{A}$. So $y_1 = y_0z$ is another lift of $\tilde{\Theta}^{ab} \bmod 2$ and $nr(y_1) = \tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$. By the pullback diagram we get $Y \in \Lambda(G_\infty)_\bullet^\times$ which maps to $\tilde{\Theta}^{ab}$ and y_1 , where $nr(y_1) = \tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$.

It follows that $\text{Det } Y = \tilde{L}_{K_\infty/\mathbb{Q}}$. To see this we check that their values agree at every irreducible character χ of G_∞ ; it even suffices to check it on the characters $1, \eta, \nu, \eta\nu, \alpha$ of G by Theorem 8 and Proposition 11 of [RW2], because every irreducible character of G_∞ is obtained from these by multiplying by a character of type W . It works for the characters $1, \eta, \nu, \eta\nu$ of G_∞^{ab} by Proposition 12, 1b) (loc.cit.) since the deflation of Y equals $\tilde{\Theta}^{ab}$ and $\text{Det } \tilde{\Theta}^{ab} = \tilde{L}_{K_\infty^{ab}/\mathbb{Q}}$ by a). Finally, $(\text{Det } Y)(\alpha) = j_\alpha(nr(Y)) = nr(y_1) = \tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$ by the commutative triangle before Theorem 8 (loc.cit.), the definition of j_α , and $G_\infty = \Gamma \times H$.

The converse depends on related ingredients. More precisely, $\tilde{L}_{K_\infty/\mathbb{Q}} \in \text{Det } K_1((\Lambda G_\infty)_\bullet)$ implies $\tilde{L}_{K_\infty/\mathbb{Q}} = \text{Det } Y$ with $Y \in (\Lambda G_\infty)_\bullet^\times$ by surjectivity of $(\Lambda G_\infty)_\bullet^\times \rightarrow K_1((\Lambda G_\infty)_\bullet)$. Since $(\Lambda G_\infty^{ab})_\bullet^\times \rightarrow K_1((\Lambda G_\infty^{ab})_\bullet)$ is an isomorphism, we get that the deflation of Y equals $\tilde{\Theta}^{ab}$ in $\Lambda(G_\infty^{ab})_\bullet^\times$. Letting $y_1 \in \mathfrak{A}^\times$ be the image of Y in the pullback diagram, it follows that $nr(y_1) = \tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$ and that y_1 maps to $\tilde{\Theta}^{ab} \bmod 2$ in $\Lambda(G_\infty^{ab})_\bullet/2\Lambda(G_\infty^{ab})_\bullet$. Given any y as in b), then $y_1^{-1}y$ maps to 1 hence is in $1 + 2\mathfrak{A}$ and our congruence follows from the Claim on applying nr . \square

4. REWRITING THE CONGRUENCE IN TESTABLE FORM

$$\text{Set } F_0 = \frac{\tilde{L}_{K_\infty/F,S}(1) + \tilde{L}_{K_\infty/F,S}(\beta^2)}{2} - \tilde{L}_{K_\infty/F,S}(\beta).$$

Proposition 4.1. a) F_0 is in $\Lambda(\Gamma_\mathbb{Q})_\bullet$.

b) $\tilde{L}_{K_\infty/\mathbb{Q}} \in \text{Det } K_1(\Lambda(G_\infty)_\bullet)$ if, and only if, $F_0 \in 4\Lambda(\Gamma_\mathbb{Q})_\bullet$.

Proof. Note that $\text{ind}_C^G 1_C = 1_G + \eta$, $\text{ind}_C^G \beta^2 = \nu + \eta\nu$, $\text{ind}_C^G \beta = \alpha$. When we inflate β to a character of $\text{Gal}(K_\infty/F)$ then $\text{ind}_{\text{Gal}(K_\infty/F)}^{G_\infty} \beta = \alpha$ with α inflated to G_∞ , etc.

By Proposition 3.1 of the previous section we can write $\tilde{L}_{K_\infty/\mathbb{Q}} = \text{Det}(\tilde{\Theta}^{ab})$ with

$$\tilde{\Theta}^{ab} = a + bt^{ab} + cs^{ab} + ds^{ab}t^{ab}$$

for some a, b, c, d in $\Lambda(\Gamma)_\bullet$. It follows that

$$\begin{aligned}\tilde{L}_{K_\infty/\mathbb{Q}}(1) &= a + b + c + d \\ \tilde{L}_{K_\infty/\mathbb{Q}}(\eta) &= a + b - c - d \\ \tilde{L}_{K_\infty/\mathbb{Q}}(\nu) &= a - b + c - d \\ \tilde{L}_{K_\infty/\mathbb{Q}}(\eta\nu) &= a - b - c + d.\end{aligned}$$

Form $y = a + b\zeta_4 + c\tilde{s} + d\zeta_4\tilde{s}$ in $(\Lambda(\Gamma)_\bullet(\zeta_4)) * \langle s \rangle$. By the computation in the Claim in the proof of Proposition 3.1, we have

$$\begin{aligned}nr(y) &= (a+c)(a-c) + (b+d)(b-d) \\ &= \frac{\tilde{L}_\mathbb{Q}(1) + \tilde{L}_\mathbb{Q}(\nu)}{2} \frac{\tilde{L}_\mathbb{Q}(\eta) + \tilde{L}_\mathbb{Q}(\eta\nu)}{2} + \frac{\tilde{L}_\mathbb{Q}(1) - \tilde{L}_\mathbb{Q}(\nu)}{2} \frac{\tilde{L}_\mathbb{Q}(\eta) - \tilde{L}_\mathbb{Q}(\eta\nu)}{2} \\ &= \frac{1}{4} (\tilde{L}_\mathbb{Q}(1 + \eta) + \tilde{L}_\mathbb{Q}(1 + \eta\nu) + \tilde{L}_\mathbb{Q}(\nu + \eta) + \tilde{L}_\mathbb{Q}(\nu + \eta\nu)) \\ &\quad + \frac{1}{4} (\tilde{L}_\mathbb{Q}(1 + \eta) - \tilde{L}_\mathbb{Q}(1 + \eta\nu) - \tilde{L}_\mathbb{Q}(\nu + \eta) + \tilde{L}_\mathbb{Q}(\nu + \eta\nu)) \\ &= \frac{\tilde{L}_\mathbb{Q}(1 + \eta) + \tilde{L}_\mathbb{Q}(\nu + \eta\nu)}{2} = \frac{\tilde{L}_F(1) + \tilde{L}_F(\beta^2)}{2},\end{aligned}$$

because

$$\tilde{L}_{K_\infty/\mathbb{Q}}(\text{ind}_{\text{Gal}(K_\infty/F)}^{G_\infty} \chi) = \tilde{L}_{K_\infty/F}(\chi)$$

for all characters χ of $\text{Gal}(K_\infty/F)$. Thus also $\tilde{L}_{K_\infty/\mathbb{Q}}(\alpha) = \tilde{L}_{K_\infty/F}(\beta)$, so we now have shown that

$$F_0 = nr(y) - \tilde{L}_{K_\infty/\mathbb{Q}}(\alpha)$$

proving a), since $\tilde{L}_{K_\infty/F}(\beta) \in (\Lambda\Gamma_F)_\bullet$ by §2, as β has degree 1.

Moreover, the image of y under the right arrow of the pullback diagram of §3 equals $\tilde{\Theta}^{ab} \pmod{2}$, by construction, hence b) follows directly from Proposition 3.1b). \square

Remark 4.2. Considering F_0 in $\Lambda(\Gamma_\mathbb{Q})_\bullet$, instead of its natural home $\Lambda(\Gamma_F)_\bullet$, is done to be consistent with the identification in b) of Proposition 3.1, via the natural isomorphisms $\Gamma \rightarrow \Gamma_F \rightarrow \Gamma_\mathbb{Q}$: this is the sense in which $L_{K_\infty/\mathbb{Q}}(\alpha) = L_{K_\infty/F}(\beta)$.

The congruence $F_0 \equiv 0 \pmod{4\Lambda(\Gamma_\mathbb{Q})_\bullet}$ can now be put in the more testable form of Conjecture 1. Let $\gamma_\mathbb{Q}$ be the generator of $\Gamma_\mathbb{Q}$ which, when extended to $\mathbb{Q}(\sqrt{-1})$ as the identity, acts on all 2-power roots of unity in $\mathbb{Q}_\infty(\sqrt{-1})$ by raising them to the u^{th} power, where $u \equiv 5 \pmod{8\mathbb{Z}_2}$ as fixed before. Then the Iwasawa isomorphism $\Lambda(\Gamma_\mathbb{Q}) \simeq \mathbb{Z}_2[[T]]$, under which $\gamma_\mathbb{Q} - 1$

corresponds to T , makes $F_0 \in \Lambda(\Gamma_{\mathbb{Q}})_{\bullet}$ correspond to some $F_0(T) \in \mathbb{Z}_1[[T]]_{\bullet}$ and the congruence of Proposition 4.1b) to

$$F_0(T) \equiv 0 \pmod{4\mathbb{Z}_2[[T]]_{\bullet}}$$

Since β is an abelian character, we know that $\tilde{L}_{F,S}(\beta^2)$, $\tilde{L}_{F,S}(\beta)$ correspond to elements of $\mathbb{Z}_2[[T]]_{\bullet}$, not just $\mathbb{Z}_2[[T]]_{\bullet}$ (cf. §4 of [RW2]), and $\tilde{L}_F(1)$ to one of $T^{-1}\mathbb{Z}_2[[T]]_{\bullet}$. We thus have

$$F_0(T) = \frac{x_0}{T} + \sum_{j=1}^{\infty} x_j T^{j-1}$$

with $x_j \in \mathbb{Z}_2$ for all $j \geq 0$.

By the interpolation definition of $(\tilde{L}_{F,S}(\beta^i))(T)$ (cf §4 of [R]), it follows that

$$F_0(u^s - 1) = \frac{1}{2} \left(\frac{L_{F,S}(1-s, 1)}{4} + \frac{L_{F,S}(1-s, \beta^2)}{4} - 2 \frac{L_{F,S}(1-s, \beta)}{4} \right).$$

We abbreviate the right hand side of the equality as $f_0(1-s)$. This implies

$$x_0 = - \frac{\rho_{F,S} \log(u)}{8},$$

because the left side is

$$\lim_{T \rightarrow 0} T F_0(T) = \lim_{s \rightarrow 1} \frac{u^{1-s} - 1}{s - 1} (s - 1) f_0(s) = -\log(u) \lim_{s \rightarrow 1} (s - 1) \frac{L_{F,S}(s, 1)}{8}$$

as required. Note that $u \equiv 5 \pmod{8}$ implies that $\frac{\log(u)}{4}$ is a 2-adic unit, hence $\frac{1}{2} \rho_{F,S} \in \mathbb{Z}_2$ is in $4\mathbb{Z}_2$ if, and only if, $x_0 \in 4\mathbb{Z}_2$.

Define $F_1(T) = F_0(T) - x_0 T^{-1} = \sum_{j=1}^{\infty} x_j T^{j-1} \in \mathbb{Z}_2[[T]]_{\bullet}$. It follows that

$$F_1(u^s - 1) = - \frac{x_0}{u^s - 1} + F_0(u^s - 1) = \frac{\rho_{F,S} \log(u)}{8(u^s - 1)} + f_0(1-s)$$

which is $f_1(1-s)$, with f_1 as in §1, hence our present $F_1(T)$ is also the same as in §1. Thus Conjecture 1 of §1 is equivalent to Conjecture 2 of §2 for the special case K_{∞}/\mathbb{Q} of §1.

5. TESTING CONJECTURE 1

Let χ be a 2-adic character of the Galois group C of K/F and let \mathfrak{f} be the conductor of K/F . By class field theory, we view χ as a map on the group of ideals relatively prime to \mathfrak{f} . Fix a prime ideal \mathfrak{c} not dividing \mathfrak{f} . For \mathfrak{a} , a fractional ideal relatively prime to \mathfrak{c} and \mathfrak{f} , let $\mathcal{Z}_{\mathfrak{f}}(\mathfrak{a}, \mathfrak{c}; s)$ denote the associated 2-adic twisted partial zeta function [CN]. Thus, we have

$$L_{F,S}(s, \chi) = \frac{1}{\chi(\mathfrak{c}) \langle N\mathfrak{c} \rangle^{1-s} - 1} \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}} \langle N\mathfrak{p} \rangle^{1-s} \right) \sum_{\sigma \in G} \chi(\sigma)^{-1} \mathcal{Z}_{\mathfrak{f}}(\mathfrak{a}_{\sigma}^{-1}, \mathfrak{c}; s)$$

where \mathfrak{p} runs through the prime ideals of F in S not dividing $2\mathfrak{f}$, \mathfrak{a}_σ is a (fixed) integral ideal coprime with $2\mathfrak{f}\mathfrak{c}$ whose Artin symbol is σ

Denote the ring of integers of F by \mathcal{O}_F and let $\gamma \in \mathcal{O}_F$ be such that $\mathcal{O}_F = \mathbb{Z} + \gamma\mathbb{Z}$. In [Rob] (see also [BBJR] for a slightly different presentation), it is shown that the function $\mathcal{Z}_{\mathfrak{f}}(\mathfrak{a}, \mathfrak{c}; s)$ is defined by the following integral

$$\mathcal{Z}_{\mathfrak{f}}(\mathfrak{a}, \mathfrak{c}; s) = \int \frac{\langle N\mathfrak{a}N(x_1 + x_2\gamma) \rangle^{1-s}}{N\mathfrak{a}N(x_1 + x_2\gamma)} d\mu_{\mathfrak{a}}(x_1, x_2)$$

where the integration domain is \mathbb{Z}_2^2 , $\langle \cdot \rangle$ is extended to \mathbb{Z}_2 by $\langle x \rangle = 0$ if $x \in 2\mathbb{Z}_2$, and the measure $\mu_{\mathfrak{a}}$ is a measure of norm 1 (depending also on γ , \mathfrak{f} and \mathfrak{c}).

Assume now, as we can do without loss of generality, that the ideal \mathfrak{c} is such that $\langle N\mathfrak{c} \rangle \equiv 5 \pmod{8\mathbb{Z}_2}$ and take $u = \langle N\mathfrak{c} \rangle$. For $s \in \mathbb{Z}_2$, we let $t = t(s) = u^s - 1 \in 4\mathbb{Z}_2$, so that $s = \log(1+t)/\log(u)$. For $x \in \mathbb{Z}_2^\times$, one can check readily that

$$\langle x \rangle^s = \left(u^{\mathcal{L}(x)} \right)^s = (1 + u^s - 1)^{\mathcal{L}(x)} = \sum_{n \geq 0} \binom{\mathcal{L}(x)}{n} t^n$$

where $\mathcal{L}(x) = \log \langle x \rangle / \log u \in \mathbb{Z}_2$. For $x \in \mathbb{Z}_2^\times$, we set

$$L(x; T) = \sum_{n \geq 0} \binom{\mathcal{L}(x)}{n} T^n \in \mathbb{Z}_2[[T]]$$

and $L(x; T) = 0$ if $x \in 2\mathbb{Z}_2$. Now, we define

$$R(\mathfrak{a}, \mathfrak{c}; T) = \int \frac{L(N\mathfrak{a}N(x_1 + x_2\gamma); T)}{N\mathfrak{a}N(x_1 + x_2\gamma)} d\mu_{\mathfrak{a}}(x_1, x_2) \in \mathbb{Z}_2[[T]]$$

$$B(\chi; T) = \chi(\mathfrak{c})(T+1) - 1 \in \mathbb{Z}_2[\chi][[T]],$$

$$A(\chi; T) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}} L(N\mathfrak{p}; T) \right) \sum_{\sigma \in G} \chi(\sigma)^{-1} R(\mathfrak{a}_\sigma^{-1}, \mathfrak{c}; T) \in \mathbb{Z}_2[\chi][[[T]]]$$

where \mathfrak{p} runs through the prime ideals of F in S not dividing $2\mathfrak{f}$.

Proposition 5.1. *We have, for all $s \in \mathbb{Z}_2$*

$$L_{F,S}(1-s, \chi) = \frac{A(\chi; u^s - 1)}{B(\chi; u^s - 1)}.$$

We now specialize to our situation. For that, we need to make the additional assumption that $\beta^2(\mathfrak{c}) = -1$, so $\beta(\mathfrak{c})$ is a fourth root of unity in \mathbb{Q}_2^\times that we will denote by i . Thus, we have

$$B(1; T) = T, \quad B(\beta; T) = i(T+1) - 1,$$

$$B(\beta^2; T) = -T - 2, \quad B(\beta^3; T) = -i(T+1) - 1.$$

Let $x \mapsto \bar{x}$ be the \mathbb{Q}_2 -automorphism of $\mathbb{Q}_2(i)$ sending i to $-i$. Then we have $\overline{L_{F,S}(1-s, \beta)} = L_{F,S}(1-s, \beta^3)$ by the expression of $L_{F,S}(s, \chi)$ given at the

beginning of the section since the twisted partial zeta functions have values in \mathbb{Q}_2 and $\bar{\beta} = \beta^3$. And furthermore,

$$L_{F,S}(s, \beta^3) = L_{\mathbb{Q},S}(s, \text{Ind}_C^G(\beta^3)) = L_{\mathbb{Q},S}(s, \text{Ind}_C^G(\beta)) = L_{F,S}(s, \beta).$$

Therefore, by Prop. 5.1, we deduce that

$$\begin{aligned} A(\beta; u^s - 1) + \bar{A}(\beta; u^s - 1) &= (B(\beta; T) + B(\beta^3; T))L_{F,S}(1 - s, \beta) \\ &= -2L_{F,S}(1 - s, \beta). \end{aligned}$$

Since

$$f_1(s) = \frac{\rho_{F,S} \log u}{8(u^{1-s} - 1)} + \frac{1}{8} (L_{F,S}(s, 1) + L_{F,S}(s, \beta^2) - 2L_{F,S}(s, \beta))$$

we find that

$$F_1(T) = \frac{\rho_{F,S} \log u}{8T} + \frac{1}{8} \left(\frac{A(1; T)}{T} - \frac{A(\beta^2; T)}{T+2} + A(\beta; T) + \bar{A}(\beta, T) \right)$$

is such that $F_1(u^n - 1) = f_1(1 - n)$ for $n = 1, 2, 3, \dots$

The conjecture that we wish to check states that

$$\frac{1}{2}\rho_{F,S} \in 4\mathbb{Z}_2 \quad \text{and} \quad F_1(T) \in 4\mathbb{Z}_2[[T]].$$

Now define $D(T) = 8T(T+2)F_1(T)$, so that

$$\begin{aligned} D(T) &= (T+2)(\rho_{F,S} \log u + A(1; T)) \\ &\quad - TA(\beta^2; T) + T(T+2)(A(\beta; T) + \bar{A}(\beta, T)). \end{aligned}$$

We can now give a final reformulation of the conjecture which is the one that we actually tested.

Conjecture 3.

$$\rho_{F,S} \in 8\mathbb{Z}_2 \quad \text{and} \quad D(T) \in 32\mathbb{Z}_2[[T]]$$

The computation of $\rho_{F,S}$ is done using the following formula [Col]

$$\rho_{F,S} = 2h_F R_F d_F^{-1/2} \prod_{\mathfrak{p}} (1 - 1/N(\mathfrak{p}))$$

where h_F , R_F , d_F are respectively the class number, 2-adic regulator and discriminant of F and \mathfrak{p} runs through all primes of F above 2. Note that although R_F and $d_F^{-1/2}$ are only defined up to sign, the quantity $R_F d_F^{-1/2}$ is uniquely determined in the following way: Let ι be the embedding of F into \mathbb{R} for which $\sqrt{d_F}$ is positive and let ε be the fundamental unit of F such that $\iota(\varepsilon) > 1$. Then for any embedding g of F into \mathbb{Q}_2^c , we have

$$R_F d_F^{-1/2} = \frac{\log_2 g(\varepsilon)}{g(\sqrt{d})}.$$

Now, for the computation of $D(T)$, the only difficult part is the computations of the $R(\mathfrak{a}, \mathfrak{c}; T)$. The measures $\mu_{\mathfrak{a}}$ are computed explicitly using

the methods of [Rob] (see also [BBJR]), that is we construct a power series $M_{\mathfrak{a}}(X_1, X_2)$ in $\mathbb{Q}_2[X_1, X_2]$ with integral coefficients, such that

$$\int (1+t_1)^{x_1} (1+t_2)^{x_2} d\mu_{\mathfrak{a}}(x_1, x_2) = M_{\mathfrak{a}}(t_1, t_2) \quad \text{for all } t_1, t_2 \in 2\mathbb{Z}_2.$$

In particular, if f is a continuous function on \mathbb{Z}_2^2 with values in \mathbb{C}_2 and Mahler expansion

$$f(x_1, x_2) = \sum_{n_1, n_2 \geq 0} f_{n_1, n_2} \binom{x_1}{n_1} \binom{x_2}{n_2}$$

then we have

$$\int f(x_1, x_2) d\mu_{\mathfrak{a}}(x_1, x_2) = \sum_{n_1, n_2 \geq 0} f_{n_1, n_2} m_{n_1, n_2}$$

where $M_{\mathfrak{a}}(X_1, X_2) = \sum_{n_1, n_2 \geq 0} m_{n_1, n_2} X_1^{n_1} X_2^{n_2}$.

We compute this way the first few coefficients of the power series $A(\chi; T)$, for $\chi = \beta^j$, $j = 0, 1, 2, 3$, and then deduce the first coefficients of $D(T)$ to see if they do indeed belong to $32\mathbb{Z}_2[[T]]$. We found that this was indeed always the case; see next section for more details.

To conclude this section, we remark that, in fact, we do not need the above formula to compute $\rho_{F,S}$ since the constant coefficient of $A(1; T)$ is $-\rho_{F,S} \log u$. (This can be seen directly from the expression of x_0 given at the end of Section 4 or using the fact that $D(T)$ has zero constant coefficient since $F_1(T) \in \mathbb{Z}_2[[T]]$.) However, we did compute it using this formula since it then provides a neat way to check that (at least one coefficient of) $A(1; T)$ is correct.

6. THE NUMERICAL VERIFICATIONS

We have tested the conjecture in 60 examples. The examples are separated in three subcases of 20 examples according to the way 2 decomposes in the quadratic subfield F : ramified, split or inert. In each subcase, the examples are actually the first 20 extensions K/\mathbb{Q} of the suitable form of the smallest discriminant. These are given in the following three tables of Figure 2 where the entries are: the discriminant d_F of F , the conductor \mathfrak{f} of K/F (which is always a rational integer) and the discriminant d_K of K . In each example, we have computed $\rho_{F,S}$ and the first 30 coefficients of $D(T)$ to a precision of at least 2^8 and checked that they satisfy the conjecture.

We now give an example, namely the smallest example for the discriminant of K . We have $F = \mathbb{Q}(\sqrt{145})$ and K is the Hilbert class field of F . The prime 2 is split in F/\mathbb{Q} and the primes above 2 in F are inert in K/F . We compute $\rho_{F,S}$ and find that

$$\rho_{F,S} \equiv 2^7 \pmod{2^8}$$

2 ramified in F			2 inert in F			2 split in F		
d_F	f	d_K	d_F	f	d_K	d_F	f	d_K
44	3	2 732 361 984	445	1	39 213 900 625	145	1	442 050 625
156	2	9 475 854 336	5	21	53 603 825 625	41	5	44 152 515 625
220	2	37 480 960 000	205	3	143 054 150 625	505	1	65 037 750 625
12	14	39 033 114 624	221	3	193 220 905 761	689	1	225 360 027 841
156	4	151 613 669 376	61	5	216 341 265 625	777	1	364 488 705 441
380	2	333 621 760 000	205	4	452 121 760 000	793	1	395 451 064 801
152	3	389 136 420 864	221	4	610 673 479 936	17	13	403 139 914 489
24	11	587 761 422 336	901	1	659 020 863 601	897	1	647 395 642 881
876	1	588 865 925 376	29	15	895 152 515 625	905	1	670 801 950 625
220	4	599 695 360 000	1 045	1	1 192 518 600 625	305	3	700 945 700 625
444	2	621 801 639 936	5	16	1 911 029 760 000	377	3	1 636 252 863 921
12	28	624 529 833 984	109	5	2 205 596 265 625	1 145	1	1 718 786 550 625
44	12	699 484 667 904	1 221	1	2 222 606 887 281	145	8	1 810 639 360 000
92	6	835 600 748 544	29	20	2 829 124 000 000	305	4	2 215 334 560 000
60	8	849 346 560 000	29	13	3 413 910 296 329	1 313	1	2 972 069 112 961
44	10	937 024 000 000	205	7	4 240 407 600 625	377	4	5 171 367 076 096
12	19	975 543 388 416	149	5	7 701 318 765 625	545	3	7 146 131 900 625
12	26	1 601 419 382 784	1 677	1	7 909 194 404 241	17	21	7 163 272 192 041
44	15	1 707 726 240 000	21	19	9 149 529 982 761	1 705	1	8 450 794 350 625
1 164	1	1 835 743 170 816	341	3	9 857 006 530 569	329	3	8 541 047 165 049

FIGURE 2

Using the method of the previous section, we compute the first 30 coefficients of the power series $A(\cdot; T)$ to a 2-adic precision of 2^8 . We get

$$\begin{aligned}
 A(1; T) \equiv & 2^2(16T + 57T^3 + 44T^4 + 8T^5 + 40T^6 + 21T^7 + 40T^8 + 30T^9 \\
 & + 16T^{10} + 49T^{11} + 56T^{12} + 29T^{13} + 32T^{14} + 50T^{15} \\
 & + 62T^{16} + 47T^{17} + 48T^{18} + 60T^{19} + 32T^{20} + 16T^{21} \\
 & + 8T^{22} + 21T^{23} + 30T^{24} + 26T^{25} + 2T^{26} + 9T^{27} \\
 & + 56T^{28} + 34T^{29}) + O(T^{30}) \pmod{2^8}
 \end{aligned}$$

$$\begin{aligned}
 A(\beta; T) \equiv & 2^2((28 + 1124i) + (36 + 1728i)T + (47 + 45i)T^2 + (56 + 153i)T^3 \\
 & + (46 + 154i)T^4 + (56 + 282i)T^5 + (55 + 433i)T^6 \\
 & + (54 + 435i)T^7 + (40 + 386i)T^8 + (48 + 392i)T^9 \\
 & + (63 + 65i)T^{10} + (48 + 257i)T^{11} + (63 + 161i)T^{12} \\
 & + (20 + 477i)T^{13} + (38 + 182i)T^{14} + (56 + 66i)T^{15} \\
 & + (37 + 35i)T^{16} + (6 + 341i)T^{17} + (20 + 446i)T^{18} \\
 & + (40 + 412i)T^{19} + 368iT^{20} + (56 + 336i)T^{21} \\
 & + (61 + 291i)T^{22} + (40 + 427i)T^{23} + (34 + 38i)T^{24} \\
 & + (48 + 94i)T^{25} + (9 + 47i)T^{26} + (6 + 497i)T^{27} \\
 & + (40 + 42i)T^{28} + (44 + 52i)T^{29}) + O(T^{30}) \pmod{2^8}
 \end{aligned}$$

$$\begin{aligned}
A(\beta^2; T) \equiv & 2^2(32 + 32T + 22T^2 + 39T^3 + 36T^4 + 20T^5 + 62T^6 + 27T^7 \\
& + 16T^8 + 62T^9 + 46T^{10} + 23T^{11} + 30T^{12} + 51T^{13} \\
& + 4T^{14} + 2T^{15} + 56T^{16} + 33T^{17} + 44T^{18} + 12T^{19} \\
& + 40T^{20} + 8T^{21} + 54T^{22} + 11T^{23} + 34T^{24} + 42T^{25} \\
& + 43T^{27} + 56T^{28} + 46T^{29}) + O(T^{30}) \pmod{2^8}
\end{aligned}$$

Therefore

$$\begin{aligned}
D(T) \equiv & 2^5(6T + 7T^2 + 4T^3 + 5T^4 + 4T^7 + 2T^8 + 4T^9 + 2T^{10} + 4T^{11} \\
& + T^{12} + 6T^{13} + 7T^{14} + 3T^{16} + 5T^{17} + 2T^{18} + 3T^{19} \\
& + 7T^{20} + 5T^{21} + 7T^{22} + 4T^{23} + 4T^{24} + T^{25} + 7T^{26} \\
& + 3T^{27} + 7T^{28} + 6T^{29}) + O(T^{30}) \pmod{2^8}
\end{aligned}$$

and the conjecture is satisfied by the first 30 coefficients of the series D associated to the extension.

Note, as a final remark, that we have tested the conjecture in the same way for 30 additional examples where F is real quadratic, K/F is cyclic of order 4 but K is not a dihedral extension of \mathbb{Q} (either K/\mathbb{Q} is not Galois or its Galois group is not the dihedral group of order 8). In all of these examples, we found that the conjecture was not satisfied, that is either $\rho_{F,S}$ did not belong to $8\mathbb{Z}_2$ or one of the first 30 coefficients of the associated power series D did not belong to $32\mathbb{Z}_2$.

REFERENCES

- [BBJR] A. Besser, P. Buckingham, R. de Jeu and X.-F. Roblot, *On the p -adic Beilinson conjecture for number fields*, Pure Appl. Math. Q. **5** (2009), 375-434.
- [CN] P. Cassou-Noguès, *Valeurs aux entiers négatifs des fonctions zêta p -adiques*, Invent. Math. **51** (1979), 29-59.
- [Col] P. Colmez, *Résidu en $s = 1$ des fonctions zêta p -adiques*, Invent. Math. **91** (1988), 371-389.
- [DR] P. Deligne and K.A. Ribet, *Values of abelian L -functions at negative integers over totally real fields*, Invent. Math. **59** (1980), 227-286.
- [FW] B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian fields*, Annals of Math. **109** (1979), 377-395.
- [R] K.A. Ribet, *Report on p -adic L -functions over totally real fields*, Société Mathém. de France, Astérisque **61** (1979), 177-192.
- [Rob] X.-F. Roblot, *Computing p -adic L -functions of totally real number fields*, in preparation
- [RW2] J. Ritter and A. Weiss, *Toward equivariant Iwasawa theorem, II*, Indag. Mathem. N.S. **15** (2004), 549-572.
- [RW3] J. Ritter and A. Weiss, *Toward equivariant Iwasawa theorem, III*, Math. Ann. **336** (2006), 27-49.
- [RW] J. Ritter and A. Weiss, *Equivariant Iwasawa theory: an example*, Documenta Math. **13** (2008), 117-129.

- [W] A. Wiles, *The Iwasawa conjecture for totally real fields*, Annals of Math. **131** (1990), 493-540.

UNIVERSITÉ DE LYON, CNRS, UNIVERSITÉ LYON 1, INSTITUT CAMILLE JORDAN, 43
BLVD DU 11 NOVEMBRE 1918, F-69622 VILLEURBANNE CEDEX, FRANCE

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALBERTA, EDMONTON, AB T6G
2G1, CANADA