

# Special values of L-functions modulo $p$

Vinayak Vatsal

**Abstract.** This article surveys the various known results on non-vanishing of special values of L-functions in  $p$ -adic families, with an emphasis on the rigidity theorems that underlie the proof in each case.

**Mathematics Subject Classification (2000).** Primary 14G10; Secondary 37A45.

**Keywords.** L-functions, ergodic theory.

## 1. Introduction

The original intent of this article was to survey the results of the author on the nonvanishing of  $p$ -adic families of anticyclotomic twists of modular L-functions of  $GL_2$ , and in particular, the introduction of Ratner's theorems in ergodic theory to this domain. However, in preparing the article, it soon became evident that the use of Ratner's theorem is an instance of an apparently general phenomenon – namely, that every result thus far known (to the author, at least) about non-vanishing modulo  $p$  of L-functions in  $p$ -adic families seems to ultimately rely on some kind of ergodic principle about the closure of certain group action orbits, of which Ratner's theorem is a sophisticated example. Since the particular subject of anticyclotomic twists has been amply described elsewhere (notably in the introduction to [7]), the present article will focus instead on surveying the general issue of nonvanishing of  $p$ -adic families of twists in variety of different settings, with the goal of exposing the common theme of rigidity which seems to underpin the whole subject. This approach may perhaps be interesting to a wider audience, and in any case may have historical legitimacy since it is the observation that orbit closures of group actions played a key role in the classical theorems of Ferrero and Washington that led the author to introduce ergodic theory in the more general setting.

**1.1. Non-vanishing of twists in general.** Let  $\zeta(s) = \sum_{n \geq 1} n^{-s}$  denote the Riemann zeta function. This series is convergent when the real part of  $s$  is greater than 1, and admits a meromorphic continuation to  $s \in \mathbb{C}$ , with a simple pole at  $s = 1$ . Furthermore,  $\zeta(s)$  satisfies the functional equation

$$\pi^{-s/2} \Gamma(s/2) \zeta(s) = \pi^{-(1-s)/2} \Gamma((1-s)/2) \zeta(1-s), \quad (1)$$

It follows trivially from this functional equation that  $\zeta(k) = 0$  whenever  $k$  is a negative even integer. On the other hand, it was known to Euler that the value of  $\zeta(k)$  is rational when  $k$  is negative and odd. For instance, the well-known formulae  $\zeta(2) = \sum_n 1/n^2 = \pi^2/6$  and  $\zeta(4) = \sum 1/n^4 = \pi^4/90$ , together with the functional equation, show that

$$\zeta(-1) = -1/12 \quad \text{and} \quad \zeta(-3) = 1/60.$$

More generally, it can be shown that if  $k$  is a positive integer, then

$$\zeta(1 - 2k) = -B_k/k$$

where  $B_k$  is the Bernoulli number defined by the Taylor expansion

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

The Bernoulli numbers  $B_k$  are closely related to the arithmetic of the cyclotomic fields  $\mathbb{Q}(\zeta_p)$ , where  $\zeta_p = e^{2\pi i/p}$ . In fact, one has the following

**Theorem 1.1** (Kummer). *Let  $p$  denote an odd prime number. Then the class number of the cyclotomic field  $\mathbb{Q}(\zeta_p)$  is divisible by  $p$  if and only if  $p$  divides the numerator of some  $B_k$ , for  $k = 2, 4, 6, \dots, p - 3$ .*

More generally, let  $N > 2$  denote an integer, and let  $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$  denote a primitive Dirichlet character modulo  $N$ . Then it can be shown that if  $n \geq 1$  is an integer, then

$$L(1 - n, \chi) = -B_{n, \chi}/n \tag{2}$$

where the twisted Bernoulli number  $B_{n, \chi}$  is the algebraic number defined by the formula

$$\sum_{a=1}^N \frac{\chi(a) t e^{at}}{e^{Nt} - 1} = \sum B_{n, \chi} \frac{t^n}{n!}. \tag{3}$$

Furthermore, the class number formula, due to Dirichlet, relates the quantities  $B_{1, \chi}$  with the class number of certain cyclotomic fields. For instance, suppose that  $\chi = \chi_p$  is the quadratic residue character associated to the imaginary quadratic field  $\mathbb{Q}(\sqrt{-p})$ , where  $p > 3$  is a prime. Then one can show that the class number  $h(\mathbb{Q}(\sqrt{-p}))$  is given by

$$h(\mathbb{Q}(\sqrt{-p})) = \frac{\sqrt{p}}{\pi} \cdot L(1, \chi).$$

In this article, we will consider the general issue of determining whether some fixed prime  $p$  divides the special values of L-functions as above. In view of the class number formulae, this gives information on whether or not certain class numbers are divisible by  $p$ . For any given character, this is of course a hopeless problem, so one is naturally led to pose the following question: Suppose that  $S$  is a family of Dirichlet characters, and that  $n$  is a positive integer. Then how often is the number  $L(1 - n, \chi)$  divisible by a fixed prime  $p$  of  $\overline{\mathbb{Q}}$ ?

**Example 1.2.** Suppose that  $S = S_{\text{quad}}$  is the family of quadratic characters associated to imaginary quadratic fields. Then Gauss showed that the 2-primary subgroup of the class group of  $\mathbb{Q}(\sqrt{-D})$  has order  $2^{g-1}$ , where  $g$  is the number of distinct primes dividing the discriminant of  $\mathbb{Q}(\sqrt{-D})$ . In particular,  $h(\mathbb{Q}(\sqrt{-D}))$  is even unless  $D$  is a prime congruent to 1 mod 4.

What about other primes? If  $p = 3$ , Davenport and Heilbronn showed that  $h(\mathbb{Q}(\sqrt{-D}))$  is prime to 3 for a positive proportion of  $D$ . For  $p > 3$  it is known that there are infinitely many  $D$  with  $(h(\sqrt{-D}), p) = 1$ , and also infinitely many  $D$  with  $(h(\sqrt{-D}), p) = p$ .

**Example 1.3.** Recent work of Bhargava shows that at least 75% of totally real cubic fields and 50% of complex cubic fields have odd class number. For more in this direction, we refer to [2].

The examples cited above give information on the  $p$ -divisibility of various class numbers, and in view of the class number formulae, may be translated into statements about L-functions. However, it is to be noted that the *proofs* of these results are based essentially on the study of homogeneous forms of various degree, and make no reference to the L-functions as such. In the rest of this paper, we will restrict our attention to examples where one can study the L-functions directly. Specifically, we will consider the divisibility by a prime  $\ell$  of L-functions varying in certain  $p$ -adic families. Here  $\ell$  may or may not be the same as  $p$ .

## 2. $p$ -adic families

### 2.1. Cyclotomic Dirichlet characters and the work of Ferrero–Washington

**Example 2.1.** Thus, for a different kind of example, we now take  $S = S_{p\text{-cyc}}$  to denote the set of Dirichlet characters of conductor  $p^n$ , for  $n \geq 0$ . Such characters are in bijective correspondence with characters of the group  $\text{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ , where  $\mathbb{Q}(\mu_{p^\infty})$  is the field obtained by adjoining to  $\mathbb{Q}$  all  $p$ -power roots of unity. Thus  $\mathbb{Q}(\mu_{p^\infty})$  is the union of the fields  $K_n = \mathbb{Q}(\zeta_{p^n})$ , where  $\zeta_{p^n}$  is a primitive  $p^n$ -th root of unity. Let  $h(K_n)$  denote the class number of  $K_n$ . Then one can ask how often  $h(K_n)$  is divisible by a fixed prime  $\ell$ . It turns out that the behavior depends basically on whether or not  $\ell = p$ .

We consider first the case that  $\ell = p$ . In this case, it was shown by Iwasawa that if  $p^{e_n}$  denotes the exact power of  $\ell = p$  dividing the class number  $h(K_n)$ , then there exist integers  $\lambda$ ,  $\mu$ , and  $\nu$ , such that

$$e_n = \lambda n + \mu p^n + \nu.$$

for all  $n$  sufficiently large. Iwasawa conjectured further that in fact  $\mu = 0$ , so that  $e_n$  is a linear function of  $n$ , which is constant if and only if  $\lambda = 0$ . On the other hand, experimental evidence suggests that  $\text{ord}_\ell(h(K_n))$  is bounded if  $\ell \neq p$ . Both these phenomena were confirmed by Ferrero and Washington.

**Theorem 2.2** (Ferrero–Washington). *Suppose that  $p$  is a prime number. Then the invariant  $\mu$  vanishes, so we have  $e_n = \lambda n + v$ , for sufficiently large  $n$ . If  $\ell \neq p$  is a fixed prime, then  $\text{ord}_\ell(h(K_n))$  is bounded as  $n$  tends towards infinity.*

We now want to make some remarks about the proof of the Ferrero–Washington theorems, since this will be the first appearance in the subject of ideas from ergodic theory.

As we have remarked above, the first step in Ferrero–Washington is to express the class numbers in terms of L-values. In view of the formula (2), the problem becomes one of determining the divisibility properties of the numbers  $B_{n,\chi}$  defined in (3). In the original papers [11] and [36], the authors use an ingenious formula (apparently due to Iwasawa) which expresses the numbers  $B_{n,\chi}$  in terms of the  $p$ -adic digits of certain  $p$ -adic numbers related to the  $p - 1$ -st roots of unity. The calculation is somewhat involved, and we will not reproduce it here. But the central point may be succinctly described: to obtain the properties stated in Theorem 2.2, one needs to show that the digits of certain  $r$ -tuples of  $p$ -adic numbers behave like independent random variables.

To state this precisely, recall that  $\beta \in \mathbb{Z}_p$  is called *normal* if the digits in the  $p$ -adic expansion of  $\beta$  contain every random string of length  $k$  with asymptotic frequency  $p^{-k}$ . It is not hard to see that  $\beta$  is normal in this sense if and only if the sequence of numbers  $x_n(\beta) = p^{-n}s_n(\beta)$  is uniformly distributed mod 1, where  $s_n(\beta)$  denotes the unique integer in the range  $[0, p^n - 1]$  such that  $s_n(\beta) \equiv \beta \pmod{p^n}$ .

Now the main lemma in Ferrero–Washington may be stated as follows:

**Lemma 2.2.1** ([11]). *Suppose that  $\gamma_1, \gamma_2, \dots, \gamma_r \in \mathbb{Z}_p$  are linearly independent over  $\mathbb{Q}$ . Then for almost all  $\beta \in \mathbb{Z}_p$  the sequence of vectors*

$$X_n(\beta) = (x_n(\beta\gamma_1), \dots, x_n(\beta\gamma_r)) \in [0, 1]^r$$

*is uniformly distributed mod 1.*

In practice, the numbers  $\gamma_1, \dots, \gamma_r$  are taken to be a maximal set of linearly independent  $p - 1$ -st roots of unity. The connection with ergodic theory comes by analogy with the classical result of Kronecker:

**Theorem 2.3** (Kronecker). *Suppose that  $\gamma_1, \dots, \gamma_r$  are real numbers, linearly independent over  $\mathbb{Q}$ . Then the image of the 1-parameter group  $(t\gamma_1, \dots, t\gamma_r)$  for  $t \in \mathbb{R}$  is dense in the torus  $\mathbb{R}^r / \mathbb{Z}^r$ . More generally, for arbitrary  $\gamma_i$ , the closure of the group  $(t\gamma_1, \dots, t\gamma_r)$  is a subtorus of rank equal to the  $\mathbb{Q}$ -rank of the vector space spanned by the  $\gamma_i$  over  $\mathbb{Q}$ .*

Another view of the Ferrero–Washington theorems was given by Sinnott in [31] and [32], where it was observed that one can relate the Bernoulli numbers to the derivatives of certain rational functions. (This was already known to Euler.) Letting  $\mathbb{F}_p$  denote the finite field with  $p$  elements, and letting  $\mathbb{F}((T - 1))$  denote the field of Laurent expansions in the variable  $T - 1$ , the key lemma takes the following form:

**Lemma 2.3.1** (Sinnott). *Suppose that  $\gamma_1, \gamma_2, \dots, \gamma_r \in \mathbb{Z}_p$  are linearly independent over  $\mathbb{Q}$ . Then the power series  $T^{\gamma_1}, T^{\gamma_2}, \dots, T^{\gamma_r}$  are algebraically independent in  $\mathbb{F}_p((T - 1))$ .*

Here we understand that  $T^a = \sum_{n=0}^{\infty} \binom{a}{n} (T - 1)^n$  for any  $a \in \mathbb{Z}_p$ , where  $\binom{a}{n} = a \cdot (a - 1) \dots (a - n + 1)$ .

**Remark 2.4.** We would like to point out here that the main ingredient in the proof of Sinnott’s lemma is quite elementary and amounts to an application of Artin’s theorem on the linear independence of characters. In particular, the use of explicit ergodic theory is completely absent. However, the statement that the  $T^{\gamma_i}$  are algebraically independent may be rephrased as stating that the ring  $\mathbb{F}_p[T^{\gamma_1}, \dots, T^{\gamma_r}] \subset \mathbb{F}_p[[T - 1]]$  is isomorphic to a polynomial ring in  $r$  variables. Since  $\mathbb{F}_p[[T - 1]]$  is complete along the ideal  $(T - 1)$ , and  $\text{Specf}(\mathbb{F}_p[[T - 1]])$  is a formal torus, this statement is formally analogous to Kronecker’s theorem above in the sense that the image of the 1-parameter formal torus is Zariski dense in the  $r$ -dimensional variety  $\text{Spec}(\mathbb{F}_p[T^{\gamma_1}, \dots, T^{\gamma_r}])$ .

**2.2. CM L-functions.** In this section we discuss the case of Hecke L-series associated to imaginary quadratic and more general CM fields. Thus let  $F$  denote a totally real field, and let  $M/F$  denote a totally imaginary quadratic extension of  $F$ . Let  $\lambda: M^\times \backslash \mathcal{A}_M^\times \rightarrow \mathbb{C}$  denote an arithmetic idele class character of  $M$ . Let  $\lambda_\infty$  denote the restriction of  $\lambda$  to  $(M \otimes \mathbb{R})^\times$  and write

$$\lambda_\infty(x) = \prod_{\sigma} \sigma(x)^{\kappa_\sigma}$$

where the product is taken over all embeddings  $\sigma: M \rightarrow \mathbb{C}$ . The formal sum  $\kappa = \sum \kappa_\sigma \cdot \sigma$  is called the infinity type of  $\lambda$ . Let  $\mathfrak{f}$  denote the conductor of  $\lambda$ , so that  $\mathfrak{f}$  is the largest ideal of the ring of integers  $\mathcal{O}_M$  with the property that  $\lambda(x) = 1$  for all  $x \in \mathcal{O}_M \otimes \hat{\mathbb{Z}}$  such that  $x \equiv 1 \pmod{\mathfrak{f}}$ .

Now let  $L(s, \lambda)$  denote the L-function associated to the idele class character  $\lambda$ . It is well-known that the values  $L(0, \lambda)$  are critical in the sense of Deligne [9], under some suitable condition on the infinity type of  $\lambda$  (see [8] for the case  $F = \mathbb{Q}$ , or [30] in general). In other words, there exists a period  $\Omega_\lambda$  associated to  $\lambda$  such that the number

$$L^{\text{alg}}(0, \lambda) = \frac{L(0, \lambda)}{\Omega_\lambda}$$

is an algebraic number. If we fix embeddings  $i_\infty$  and  $i_p$  of  $\overline{\mathbb{Q}}$  in to  $\mathbb{C}$  and  $\mathbb{C}_p$  respectively, we may regard the complex number  $L^{\text{alg}}(0, \lambda)$  as being an element of  $\mathbb{C}_p$ , via the map  $i_p \circ i_\infty^{-1}$ . Furthermore, if one normalizes the period  $\Omega_\lambda$  in some canonical way, one can even show that the number  $L^{\text{alg}}$  is  $p$ -adically integral in  $\mathbb{C}_p$ , and one can then ask whether these numbers are  $p$ -adic units, as  $\lambda$  varies over the members of some family. This problem was first studied by Gillard [13], [14], and Schneps [29], in the case of  $F = \mathbb{Q}$  using a generalization of Sinnott’s method, and the connection

between the L-values and explicit elliptic units. Further results in the case  $F = \mathbb{Q}$  were given by Finis in [12]. Recently the subject was taken up by Hida in a series of deep papers (see [19], [20], for example) which treat the subject in great generality. For a sample of Hida's results, we restrict ourselves to a (relatively) simple statement. But to state even this, we need to introduce some notation. Here we follow [20].

Let  $X$  denote a finite set of embeddings  $M \rightarrow \mathbb{C}$  of cardinality  $[F : \mathbb{Q}]$ , such that  $X \cap cX = \emptyset$ , where  $cX$  denotes the set  $\{c\sigma, \sigma \in X\}$ , and  $c$  denotes complex conjugation. We say that  $X$  is a  $p$ -ordinary CM-type of  $M$  if the set  $\{i_p \circ i_\infty^{-1} \circ \sigma\}_{\sigma \in X}$  consists of  $[F : \mathbb{Q}]$  distinct  $p$ -adic places of  $M$ . Then we consider a character  $\lambda$  as above whose infinity type is given by

$$k \sum_{\sigma \in X} \sigma + \kappa(1 - c)$$

where  $\kappa = \sum_{\sigma \in X} \kappa_\sigma \sigma$  with  $\kappa_\sigma \geq 0$  for  $\sigma \in X$ , and  $0 < k \in \mathbb{Z}$ . Then to define the transcendental factor  $\Omega_\lambda$ , we can proceed as follows. Pick an abelian variety  $A$  of CM type such that  $A(\mathbb{C}) \cong \mathbb{C}^{[F:\mathbb{Q}]} / \mathfrak{a}$ , where the product is indexed by the  $[F : \mathbb{Q}]$  places in  $X$ , and the fractional ideal  $\mathfrak{a} \subset \mathcal{O}_M$  is embedded diagonally via the corresponding places of  $X$ . Let  $R \subset \overline{\mathbb{Q}}$  denote the Witt ring of  $\mathcal{O}_M$ , with respect to the place induced by  $i_p$ . Then  $A$  can be defined over  $R$ , and we can pick a Néron differential  $\omega$  on  $A$  such that  $\omega$  generates  $\Omega_{A/W}$  over  $R$ . Picking an isomorphism  $\phi: A(\mathbb{C}) \cong \mathbb{C}^{[F:\mathbb{Q}]} / \mathfrak{a}$ , we define a vector  $\Omega_\infty \in \mathbb{C}^{[F:\mathbb{Q}]}$  via  $\phi^*(\prod (du_\sigma)) = \Omega_\infty \omega$ . Here  $u_\sigma$  is the standard complex variable on the copy of  $\mathbb{C}$  indexed by  $\sigma$ . Writing the components of  $\Omega_\infty$  as  $\Omega_\sigma$  for  $\sigma \in X$ , we have that  $\Omega_\sigma \neq 0$ , and

$$L^{\text{alg}}(0, \lambda) = \frac{\prod_{\sigma \in X} \pi^{\kappa_\sigma} \Gamma(k + \kappa_\sigma) L(0, \lambda)}{\prod_{\sigma \in X} \Omega_\sigma^{k+2\kappa_\sigma}} \in R \quad (4)$$

Then the problem is to study  $p$ -divisibility properties of the numbers  $L^{\text{alg}}(0, \lambda)$  as defined above, as  $\lambda$  varies over some prescribed set. Recall therefore that the character  $\chi: \mathbf{A}_M^\times \rightarrow \mathbb{C}^\times$  is called anticyclotomic if  $\chi \circ \tau = \chi^{-1}$ , where  $\tau$  is the nontrivial automorphism of  $M/F$ . Then we let  $\lambda$  denote a fixed Hecke character, and consider the values  $L^{\text{alg}}(0, \lambda\chi)$ , as  $\chi$  varies over the set of anticyclotomic characters of  $M$  of conductor  $\mathfrak{l}^n$ , for some fixed prime  $\mathfrak{l}$  of  $K$  with residue characteristic  $\ell \neq p$ , and an integer  $n$ . The principal result in this direction is due to Hida. To state the theorem, let us write  $L_{\mathfrak{l}}^{\text{alg}}(0, \lambda\chi) = L^{\text{alg}}(0, \lambda\chi) \cdot (1 - \lambda\chi(\mathfrak{l}))$  for the algebraic part of the  $\mathfrak{l}$ -imprimitive L-function.

**Theorem 2.5** ([20], Theorem 1.1). *Suppose that  $p > 2$  is an unramified prime in  $M/\mathbb{Q}$  and that  $(M, X)$  is a  $p$ -ordinary CM type. Fix a character  $\lambda$  of conductor 1 with infinity type  $k \sum_{\sigma \in X} \sigma + \kappa(1 - c)$  as above. Then we have*

$$|L^{\text{alg}}(0, \lambda\chi)|_p = 1$$

*for almost all anticyclotomic characters of  $\mathfrak{l}$ -power conductor, unless the following three conditions are satisfied simultaneously:*

1.  $M/F$  is unramified at all finite places,
2. the Artin symbol  $\left(\frac{M/F}{\mathfrak{c}}\right)$  has the value  $-1$ , for the polarization ideal  $\mathfrak{c}$  of  $A$ , and
3. for all ideals  $\mathfrak{a}$  prime to  $p$ , we have  $\lambda N(\mathfrak{a}) \equiv \left(\frac{M/F}{\mathfrak{c}}\right) \pmod{\mathfrak{m}}$ .

If all these conditions are satisfied simultaneously, then  $|L^{\text{alg}}(0, \lambda\chi)|_p < 1$  for all  $\chi$ .

Here we understand that ‘almost all’ means ‘a Zariski dense subset’ in general, and ‘all but finitely many’ if  $F_1$  has dimension 1 over  $\mathbb{Q}_p$ .

The proof of this theorem is long and intricate, and we will not discuss it here, except to remark that the proof is a generalization of Sinnott’s method mentioned above. Essentially, one has to relate the values of the L-function to the values of certain Hilbert modular Eisenstein series at CM points, and prove a basic result on the linear independence of certain of these series in characteristic  $p$ . For our purposes, it will suffice to observe that key ingredient is a rigidity theorem of C.-L. Chai, which enables one to prove that under some condition, schemes fixed by torus actions tend to be rather big. For comparison with the results from ergodic theory that were cited above, we state a precise theorem, as follows.

Suppose that  $k$  is an algebraically closed field of characteristic  $p > 0$  and let  $X$  be a finite dimensional smooth formal  $p$ -divisible group over  $k$ . Let  $E_{\mathbb{Z}_p} = \text{End}(X)$  and set  $E = E_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ . Then  $E$  is a finite dimensional vector space over  $\mathbb{Q}_p$ . We let  $\mathbf{E}$  denote the linear algebraic group over  $\mathbb{Q}_p$  such that  $\mathbf{E}(R) = (E \otimes_{\mathbb{Q}_p} R)^\times$  for any commutative  $\mathbb{Q}_p$ -algebra  $R$ .

If  $G$  is any connected algebraic group over  $\mathbb{Q}_p$ , and  $\rho: G \rightarrow \mathbf{E}$  is a homomorphism of algebraic groups, then we may regard  $\rho$  as a linear representation of  $G$  on the vector space  $E$  via the canonical map  $\mathbf{E} \subset \text{Aut}(E)$ . Then Chai has proven the following striking result. (The notation is as above.)

**Theorem 2.6** (Chai). *Suppose that the trivial representation is not a subquotient of the representation  $\rho$  of  $G$  on  $E$ . Suppose also that  $Z$  is a reduced and irreducible closed formal subscheme of  $X$  which is closed under the action of an open subgroup of  $G(\mathbb{Z}_p)$ . Then  $Z$  is closed under the group law of  $X$  and is a  $p$ -divisible subgroup scheme of  $X$ .*

**2.3. Anticyclotomic L-functions.** Finally, we treat the applications of ergodic theory to anticyclotomic L-functions associated to Hilbert modular forms over totally real fields.

To describe the results, let  $F$  denote a totally real field, and let  $K/F$  denote an imaginary quadratic extension. Let  $\pi$  denote a cuspidal automorphic representation of  $\text{GL}_2(F)$ . We assume throughout that the data of  $\pi$  and  $K$  are *non-exceptional*, meaning that the representations  $\pi$  and  $\pi \otimes \eta$  are distinct, where  $\eta$  denotes the quadratic character associated to the extension  $K/F$ .

Let  $\chi: A_K^\times/K^\times \rightarrow \mathbb{C}$  be a quasi-character of  $K$ , and write  $L(\pi, \chi, s)$  for the Rankin–Selberg  $L$ -function associated to  $\pi$  and  $\pi(\chi)$ . Here  $\pi(\chi)$  denotes the automorphic representation of  $GL_2$  attached to  $\chi$ . (For the definitions, we refer the reader to [22] and [21].) Then this  $L$ -function, which is first defined as a product of Euler factors over all places of  $F$ , may be shown to have a meromorphic extension to  $\mathbb{C}$  with functional equation

$$L(\pi, \chi, s) = \varepsilon(\pi, \chi, s)L(\tilde{\pi}, \chi^{-1}, 1-s)$$

where  $\tilde{\pi}$  is the contragredient of  $\pi$  and  $\varepsilon(\pi, \chi, s)$  is the  $\varepsilon$ -factor.

Let  $\omega: A_F^\times/F^\times \rightarrow \mathbb{C}^\times$  be the central quasi-character of  $\pi$ . We will make the following assumption on the quasi-characters  $\omega$  and  $\chi$ :

$$\chi \cdot \omega = 1 \quad \text{on } A_F^\times \subset A_K^\times. \quad (5)$$

This assumption implies that  $L(\pi, \chi, s)$  is entire and equal to  $L(\tilde{\pi}, \chi^{-1}, s)$ . Thus the functional equation of  $L(\pi, \chi, s)$  may be restated as

$$L(\pi, \chi, s) = \varepsilon(\pi, \chi, s)L(\pi, \chi, 1-s)$$

and the parity of the order of vanishing of  $L(\pi, \chi, s)$  at  $s = 1/2$  is determined by the value of

$$\varepsilon(\pi, \chi) \stackrel{\text{def}}{=} \varepsilon(\pi, \chi, 1/2) \in \{\pm 1\}.$$

Following [6] and [7], we say that the pair  $(\pi, \chi)$  is *even* or *odd*, depending upon whether  $\varepsilon(\pi, \chi)$  is  $+1$  or  $-1$ . According to the conjectures introduced by Mazur in [24], it is expected that the order of vanishing of  $L(\pi, \chi, s)$  at  $s = 1/2$  should ‘usually’ be minimal, meaning that either  $L(\pi, \chi, 1/2)$  or  $L'(\pi, \chi, 1/2)$  should be nonzero, depending upon whether  $(\pi, \chi)$  is even or odd.

Results of this kind were first proven by Rohrlich [28], for the case where  $F = \mathbb{Q}$ , and  $\pi$  and  $K$  are *exceptional* in the sense that  $\pi \cong \pi \otimes \eta$ , using results from transcendence theory, notably  $p$ -adic cases of Roth’s theorems. However, nothing was known for non-exceptional  $\pi$  and  $K$  until the introduction of ergodic theory in [33] and [34], which treated the case of  $F = \mathbb{Q}$ . The ideas from ergodic theory were quickly assimilated and extended in [5], and the generalization to the case of general  $F$  was given in [6] and [7].

To proceed, we need to introduce some notation. Thus let  $n$  denote the conductor of the representation  $\pi$ . Let  $\mathfrak{p}$  denote a fixed prime of  $F$ , and let  $\chi$  denote a ring class character of  $\mathfrak{p}$ -power conductor. Here we recall that the quasi-character  $\chi$  of  $K$  is called a ring class character, or an anticyclotomic character, if the restriction of  $\chi$  to  $A_F^\times$  is everywhere unramified. Then we propose to study the order of vanishing of  $L(\pi, \chi, s)$  at  $s = 1/2$  as  $\chi$  varies over the set  $S = S_{\mathfrak{p}}^{\text{anticyc}}$  of ring class characters of  $\mathfrak{p}$ -power conductor.

In view of equation (5), it makes sense to require that the central character  $\omega$  of  $\pi$  is everywhere unramified. We assume also that  $\pi$  corresponds to a Hilbert modular

form of parallel weight  $(2, \dots, 2)$  and that the discriminant  $\mathfrak{D}$  of  $K/F$  is relatively prime to the prime-to- $p$  part  $n'$  of  $n$ . Under these conditions, it may be shown that for all  $n \gg 0$ , and all  $\chi$  of conductor  $p^n$ , the root number  $\varepsilon(\pi, \chi)$  is given by the formula

$$\varepsilon(\pi, \chi) = (-1)^{\#S} \tag{6}$$

where  $S$  denotes the set of real places of  $F$ , together with those finite primes of  $F$  which do not divide  $p$ , are inert in  $K$ , and divide  $n$  to an odd power. In particular, the root number  $\varepsilon = \varepsilon(\pi, \chi) = \pm 1$  depends only on  $\pi$  and  $K$  and  $p$ , once the conductor of  $\chi$  is sufficiently divisible. Thus one expects the order of vanishing of  $L(\pi, \chi, 1/2)$  to be equal to either 0 or 1, for ‘generic’  $\chi$ , depending only on the sign of  $\varepsilon$ . That this is indeed the case was confirmed by the main results in [6] and [7], and we refer the reader to the introduction of [6] for a very detailed discussion.

In the present paper, we will focus on the non-vanishing of  $L(\pi, \chi, 1/2)$  modulo a prime of  $\overline{\mathbb{Q}}$ . The basic results in this direction were given in [34], for the case  $F = \mathbb{Q}$ , and we now proceed to state them.

Thus, let us assume that  $F = \mathbb{Q}$ . Let  $N = n$  denote the level of  $\pi$ , let  $D = \mathfrak{D}$  denote the discriminant of the imaginary quadratic field  $K = \mathbb{Q}(\sqrt{D})$ , and let  $p = \mathfrak{p}$  denote a rational prime. We assume further that the numbers  $N, D, p$  are pairwise co-prime. We let  $f$  denote the primitive form of level  $N$  associated to  $\pi$ ; since the central character  $\omega$  of  $\pi$  is unramified and  $\mathbb{Q}$  has class number 1, we see that  $f$  is a primitive form on the group  $\Gamma_0(N)$ . We assume further that we are in the even case, so that there are an even number of places in  $S$ . We let  $\Omega_\pi = \Omega_f$  denote the canonical integral period for  $f$ , as defined by Hida in [18]. Then the number

$$L^{\text{alg}}(\pi, \chi) = \frac{L(\pi, \chi, 1/2)}{\Omega_\pi} \cdot C_\chi$$

is an algebraic integer. Here  $C_\chi = Dp^{2n}$ , where  $p^n$  denotes the conductor of  $\chi$ . Let  $\lambda$  denote a fixed prime of  $\overline{\mathbb{Q}}$ , and consider the  $\lambda$ -adic absolute value  $|L^{\text{alg}}(\pi, \chi)|_\lambda$ . We want to study the general question of how  $|L^{\text{alg}}(\pi, \chi)|_\lambda$  varies as a function of  $\chi$ , and the result depends on whether or not  $\lambda$  has residue characteristic  $p$ . In either case, let us define two constants  $C_{\text{csp}}$  and  $C_{\text{Eis}}$  associated to  $\pi$ , as in [34], Section 2.4.<sup>1</sup>

Then one has the following result:

**Theorem 2.7** ([34]). *Suppose that  $\lambda$  has residue characteristic  $\ell \neq p$ . Then we have*

$$|L^{\text{alg}}(\pi, \chi)|_\lambda = |C_{\text{csp}}^2 C_{\text{Eis}}|_\lambda$$

for all but finitely many  $\lambda$  of conductor  $p^n$ .

Actually, the theorem above was stated in [34] under some mild assumptions on  $\ell$ , but these restrictions are easily removed, for example with the improved formalism

---

<sup>1</sup>The definition of these constants is rather technical, and we prefer not to reproduce it. The significance of these numbers, in particular the relationship to congruences, is elucidated in the paper [25].

introduced in [7], or by a slightly more detailed analysis of the original proof. We remark here that the numbers  $C_{\text{csp}}$  and  $C_{\text{Eis}}$  are *not* necessarily  $\lambda$ -adic units.

As for the case where  $\lambda$  has residue characteristic  $p$ , the result is in the same vein, provided one assumes that the local component  $\pi_p$  is ordinary at  $\lambda$ , in the sense that the Hecke eigenvalue  $a_p(\pi)$  is a  $\lambda$ -adic unit.

**Theorem 2.8** ([34]). *Suppose that  $\lambda$  has residue characteristic  $\ell = p$  and that  $\pi_p$  is ordinary at  $\lambda$ . Then we have*

$$\lim_{\chi} |L^{\text{alg}}(\pi, \chi)|_{\lambda} = |C_{\text{csp}}^2 C_{\text{Eis}}|_{\lambda},$$

where the limit is taken over characters  $\chi$  of conductor  $p^n$ , as  $n \rightarrow \infty$ .

**Remark 2.9.** In view of recent results in the Iwasawa theory of elliptic curves, our results on L-functions may be formulated in terms of the growths of certain Selmer groups, which are generalizations of the Iwasawa ideal class groups occurring in our discussion of the Ferrero–Washington theorem above. For more details, we refer the reader to [1] and [25]. We remark also that our results above have not yet been extended to general  $F$ , but it seems likely that such generalizations would follow without difficulty from the techniques of [7].

**Remark 2.10.** We point out also that there are results analogous to those above in the case that the sign in the functional equation is  $-1$ . However, in these cases, one is dealing with derivatives of L-functions, and there is no general notion of what it means for a derivative of an L-function to be nonzero modulo  $p$ . In the case at hand one has an *ad hoc* definition in terms of  $p$ -divisibility of certain Heegner points arising from the Gross–Zagier formula for derivatives, and it is this kind of result that is proven. For details we refer the reader to [34] and [5].

In keeping with the general theme of this article, we wish now to elaborate on the role of ergodic theorems in the proofs of our results. A detailed description of the strategy may be found in the introductions to [33] and [7], and we will not cut and paste from those articles here. For the present, we simply note that the starting point comes from the formulae of Gross, Zagier, and Zhang, which relate the values of the L-functions in question to the heights of certain special points on quaternion algebras. (See [17], [15], and [37] for the theorems, which were then reframed in the article [16]. A more elementary perspective may be found in [35].) In view of these special value formulae, the essential point in proving that the L-values are non-zero modulo  $p$  boils down to showing that certain vectors whose components are formed by the special points and their conjugates, are uniformly distributed in the appropriate sense on certain Shimura varieties. The necessary uniform distribution is then deduced by applying deep theorems in ergodic theory due to M. Ratner [27].<sup>2</sup>

<sup>2</sup>In [6] and [7], appeals were made to results of Margulis and Tomanov [23], since these results were formulated in a manner convenient for our applications there. The author has since been informed by Ratner that the results we quoted from [23] can in fact be deduced from those given earlier in [26].

The reduction of our number theoretic results to Ratner's theorem has been amply documented elsewhere, so we will just state some of Ratner's key results, in a manner that we hope will make clear the analogy with the results of Ferrero–Washington, Sinnott, and Chai. It is perhaps germane to remark here that the introduction of Ratner's theorem in [33] was inspired by direct analogy with the use of Kronecker's theorem by Ferrero and Washington.

Thus let  $G$  denote the  $p$ -adic Lie group  $\mathrm{SL}_2(\mathbb{Q}_p)$ , and let  $\Gamma_i \subset G$ ,  $i = 1, 2$  denote discrete and cocompact subgroups. We say that  $\Gamma_1$  and  $\Gamma_2$  are commensurable if  $\Gamma_1 \cap \Gamma_2$  has finite index in  $\Gamma_1$  and  $\Gamma_2$ . Then the following remarkable result is a very simple consequence of the main results in [27]:

**Theorem 2.11** (Ratner). *The set  $\Gamma_1 \cdot \Gamma_2 = \{\gamma_1 \cdot \gamma_2, \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$  is dense in  $G$  if and only if the subgroups  $\Gamma_1$  and  $\Gamma_2$  are not commensurable.*

**Remark 2.12.** Note that it is obvious that the product  $\Gamma_1 \cdot \Gamma_2$  cannot be dense if  $\Gamma_1$  and  $\Gamma_2$  are commensurable. But the reverse implication is extremely deep, and seems to admit no elementary proof.

**Remark 2.13.** For an analogy, let  $G$  denote the additive group  $\mathbb{R}$  of real numbers, and let  $X_i$ ,  $i = 1, 2$  denote discrete subgroups of  $G$ . Then each  $X_i$  is abstractly isomorphic to the additive group of  $\mathbb{Z}$ . If  $x_i$  is a generator of  $X_i$ , then the groups  $X_i$  are commensurable if and only if the  $x_i$  are linearly dependent over  $\mathbb{Q}$ . In this case the product  $X_1 \cdot X_2$  is discrete in  $G$ . On the other hand, Kronecker's theorem implies that the product  $X_1 \cdot X_2$  is dense if the  $x_i$  are independent over  $\mathbb{Q}$ , which is to say, if the groups  $X_i$  fail to be commensurable. Thus Ratner's theorem above is a  $p$ -adic and non-abelian analogue of Kronecker's theorem.

Actually, one requires a slightly more refined theorem for the applications to number theory. As above, write  $G$  for the  $p$ -adic Lie group  $\mathrm{SL}_2(\mathbb{Q}_p)$ . Let  $r$  denote a positive integer, and for each  $i$  with  $1 \leq i \leq r$ , we let  $\Gamma_i$  denote a discrete and cocompact subgroup of  $G$ . Then

$$\Gamma = \prod_{i=1}^r \Gamma_i \subset \prod_{i=1}^r G$$

is a discrete and cocompact subgroup of the product  $G^r$  of  $r$  copies of  $G$ . We may then formulate the following result:

**Theorem 2.14** (Ratner). *Suppose that the groups  $\Gamma_i$  are pairwise non-commensurable. Then the image of the diagonal  $\Delta(G) = \{(g, \dots, g), g \in G\} \subset G^r$  has dense image in the quotient  $\Gamma \backslash G^r$ .*

Finally, we give a rigidity result which implies the two above as special cases.

**Theorem 2.15** (Ratner). *Let  $G$  denote a  $p$ -adic Lie group, and let  $\Gamma \subset G$  be such that  $\Gamma \backslash G$  has finite volume with respect to the unique  $G$ -invariant measure. Let  $U \subset G$*

denote any subgroup generated by 1-parameter subgroups, namely, by the image of (additive) homomorphisms  $u_i: \mathbb{Q}_p \rightarrow G$ . Then the closure  $\bar{U}$  of the orbit of  $U$  in  $\Gamma \backslash G$  is homogeneous, in the sense that there exists a subgroup  $H$  of  $G$  such that the orbit of  $H$  is closed in  $\Gamma \backslash G$  and  $\bar{U}$  coincides with the orbit of  $H$ .

**Remark 2.16.** We would like to point out here that for the purposes of the results in [5] and some of the results in [7] (namely, the indefinite case), one can get by with yet another kind of rigidity principle, namely certain cases of the André–Oort conjecture. For more on this subject, we refer the reader to [5]. For the relationship with Chai’s theorem, see [3]. Further discussion of this and related topics may be found in [10] and [4].

To conclude, we would hope that the analogy between the theorems of Kronecker, Sinnott, Chai, and Ratner is now evident. Namely, in every case, we are asserting that the closure of rather small group orbits, (the diagonal, in Ratner’s case, or a 1-parameter group in Kronecker’s theorem) is forced, by rigidity, to be rather big. In the Ferrero–Washington and anticyclotomic cases, the orbit of a small group inside an  $r$ -dimensional object turns out to be dense, and in every case, including the theorem of Chai, the key statement is a rigidity principle of the form that the closures of the relevant orbits coincide with the orbits of subgroups. Is there a general ergodic or rigidity principle that accounts for all of these results? We hope that the answer is affirmative, but at present we seem to be far from finding it.

## References

- [1] Bertolini, Massimo, and Darmon, Henri, Iwasawa’s main conjecture for elliptic curves over anticyclotomic extensions. *Ann. of Math.*, to appear.
- [2] Bhargava, Manjul, The density of discriminants of quartic rings and fields. *Ann. of Math.* (2) **162** (2) (2005), 1031–1063.
- [3] Chai, C.-L., Families of ordinary abelian varieties: canonical coordinates,  $p$ -adic monodromy, tate-linear subvarieties and hecke orbits. Preprint, 2003.
- [4] Clozel, Laurent, Oh, Hee, and Ullmo, Emmanuel, Hecke operators and equidistribution of Hecke points. *Invent. Math.* **144** (2) (2001), 327–351.
- [5] Cornut, C., Mazur’s conjecture on higher Heegner points. *Invent. Math.* **148** (3) (2002), 495–523.
- [6] Cornut, C., and Vatsal, V., Nontriviality of Rankin–Selberg L-functions and CM points. Preprint, 2004.
- [7] Cornut, C., and Vatsal, V., CM points and quaternion algebras. *Doc. Math.* **10** (2005), 263–309 (electronic).
- [8] de Shalit, E., *Iwasawa theory of elliptic curves with complex multiplication*. *Perspect. Math.* 3, Academic Press, Boston, MA, 1987.
- [9] Deligne, P., Valeurs de fonctions L et périodes d’intégrales. In *Automorphic forms, representations and L-functions*, Proc. Sympos. Pure Math. 33, Part 2, Amer. Math. Soc., Providence, RI, 1979, 313–346.

- [10] Edixhoven, B., and Yafaev, A., Subvarieties of Shimura varieties. *Ann. of Math. (2)* **157** (2) (2003), 621–645.
- [11] Ferrero, B., and Washington, L., The Iwasawa invariant  $\mu_p$  vanishes for abelian number fields. *Ann. of Math. (2)* **109** (2) (1979), 377–395.
- [12] Finis, T., Divisibility of anticyclotomic L-functions and theta functions with complex multiplication. Preprint, 2002.
- [13] Gillard, Roland, Fonctions  $L$   $p$ -adiques des corps quadratiques imaginaires et de leurs extensions abéliennes. *J. Reine Angew. Math.* **358** (1985), 76–91.
- [14] Gillard, Roland, Croissance du nombre de classes dans des  $\mathbf{Z}_l$ -extensions liées aux corps quadratiques imaginaires. *Math. Ann.* **279** (3) (1988), 349–372.
- [15] Gross, B., Heights and the special values of L-series. In *Number Theory* (ed. by H. Kisilevsky and J. Labute.), CMS Conference Proceedings 7, Amer. Math. Soc., Providence, RI, 1987, 115–189.
- [16] Gross, B., Heegner points and representation theory. In *Heegner points and Rankin L-series*, Math. Sci. Res. Inst. Publ. 49, Cambridge University Press, Cambridge 2004, 37–66.
- [17] Gross, B., and Zagier, D., Heegner points and derivatives of L-series. *Invent. Math.* **84** (1986), 225–320.
- [18] Hida, H., Modules of congruence of Hecke algebras and  $L$ -functions associated with cusp forms. *Amer. J. Math.* **110** (2) (1988), 323–382.
- [19] Hida, H., The Iwasawa  $\mu$ -invariant of  $p$ -adic Hecke  $L$ -functions. Preprint, 2006.
- [20] Hida, H., Non-vanishing modulo  $p$  of Hecke  $L$ -values. In *Geometric Aspects of Dwork Theory* (ed. by A. Adolphson, F. Baldassarri, P. Berthelot, N. Katz and F. Loeser), Volume II, Walter de Gruyter, Berlin 2004, 731–780.
- [21] Jacquet, H., *Automorphic forms on  $GL(2)$ . Part II*, Lecture Notes in Math. 278, Springer-Verlag, Berlin 1972.
- [22] Jacquet, H., and Langlands, R. P., *Automorphic forms on  $GL(2)$* . Lecture Notes in Math. 114, Springer-Verlag, Berlin 1970.
- [23] Margulis, G. A., and Tomanov, G. M., Invariant measures for actions of unipotent groups over local fields on homogeneous spaces. *Invent. Math.* 116(1-3) (1994), 347–392.
- [24] Mazur, B., Modular curves and arithmetic. In *Proceedings of the International Congress of Mathematicians* (Warszawa, 1983), Vol. 1, PWN, Warsaw 1984, 185–211.
- [25] Pollack, R., and Weston, T., On  $\mu$ -invariants of anticyclotomic  $p$ -adic L-functions of elliptic curves. Preprint, 2005.
- [26] Ratner, M., Raghunathan’s Conjectures for  $p$ -adic Lie groups. *Internat Math. Res Notices* **5** (1993), 141–146.
- [27] Ratner, M., Raghunathan’s conjectures for Cartesian products of real and  $p$ -adic Lie groups. *Duke Math. J.* **77** (2) (1995), 275–382.
- [28] Rohrlich, D. E., On  $L$ -functions of elliptic curves and cyclotomic towers. *Invent. Math.* **75** (3) (1984), 409–423.
- [29] Schneps, Leila, On the  $\mu$ -invariant of  $p$ -adic  $L$ -functions attached to elliptic curves with complex multiplication. *J. Number Theory* **25** (1) (1987), 20–33.
- [30] Shimura, Goro, On some arithmetic properties of modular forms of one and several variables. *Ann. of Math. (2)* **102** (3) (1975), 491–515.

- [31] Sinnott, W., On the  $\mu$ -invariant of the  $\Gamma$ -transform of a rational function. *Invent. Math.* **75** (2) (1984), 273–282.
- [32] Sinnott, W.,  $\Gamma$ -transforms of rational function measures on  $\mathbf{Z}_S$ . *Invent. Math.* **89** (1) (1987), 139–157.
- [33] Vatsal, V., Uniform distribution of Heegner points. *Invent. Math.* **148** (2002), 1–46.
- [34] Vatsal, V., Special values of anticyclotomic L-functions. *Duke Math J.* **116** (2) (2003), 219–261.
- [35] Vatsal, Vinayak, Special value formulae for Rankin  $L$ -functions. In *Heegner points and Rankin  $L$ -series*, Math. Sci. Res. Inst. Publ. 49, Cambridge University Press, Cambridge 2004, 165–190.
- [36] Washington, L., The non- $p$ -part of the class number in a cyclotomic  $\mathbb{Z}_p$ -extension. *Invent. Math.* **49** (1) (1978), 87–97.
- [37] S. Zhang, S., Gross-Zagier formula for  $GL_2$ . II. In *Heegner points and Rankin  $L$ -series*, Math. Sci. Res. Inst. Publ. 49, Cambridge University Press, Cambridge 2004, 191–242.

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2,  
Canada  
E-mail: vatsal@math.ubc.ca