ACTA ARITHMETICA
Online First version

On L-functions of Hecke characters and anticyclotomic towers

by

Haijun Jia

Abstract. We generalize a result of Rohrlich (1984). Let $K/\mathbb{Q}$ be an imaginary quadratic field and ϕ be a Hecke character of K of infinite type $(1,0)$ whose restriction to $\mathbb{Q}$ is the quadratic character corresponding to $K/\mathbb{Q}$. We consider a class of Hecke characters χ, which are anticyclotomic twists of ϕ with ramification in a prescribed finite set of primes. We prove that the central vanishing order of the Hecke L-function $L(s,\chi)$ attached to each χ is 0 or 1 depending on the root number $W(\chi)$ for all but finitely many such χ.

1. Introduction. Let K be an imaginary quadratic field with class number h and $\mathcal{O}$ be the ring of integers of K. Let M be an abelian extension of K which can be infinite. We say M/K is *anticyclotomic* if the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(M/K)$ by inversion. Let P be a fixed finite set of rational primes. Let L be the compositum of all anticyclotomic extensions of K which are unramified outside P. The field L can also be described as the union of all ring class fields of K with conductor divisible only by primes in P. Using class field theory, we know that $\mathrm{Gal}(L/K)$ is isomorphic to the product of a finite group and the group

$$\prod_{p\in P}\mathbb{Z}_p,$$

where $\mathbb{Z}_p$ is the ring of p-adic integers.

Let ϕ be a Hecke character (also called Grössencharacter in the literature) of K with infinite type $(1,0)$, and $\mathfrak{f}(\phi)$ be the conductor of ϕ. We say ϕ is *equivariant with respect to complex conjugation* (or just *equivariant* for

2020 *Mathematics Subject Classification*: Primary 11R42; Secondary 11M11.
Key words and phrases: Hecke character, L-function, anticyclotomic tower.
Received 10 December 2024; revised 31 August 2025.
Published online 25 June 2026.

Haijun Jia passed away on November 6, 2025. The editors gratefully acknowledge the help of Professors Zheng Liu and Xin Wan in the final editing of the paper.

 © Instytut Matematyczny PAN, 2026

simplicity) if for all integral ideals $\mathfrak{a}$ of K, we have

$$\phi(\bar{\mathfrak{a}}) = \overline{\phi(\mathfrak{a})}.$$

In the following, we assume that ϕ is equivariant with respect to complex conjugation.

For a given finite order character $\rho : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$, we view it as an idele class character through

$$\mathbb{A}_K^\times / K^\times \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \to \mathbb{C}^\times,$$

and we let $\phi\rho$ denote the primitive Hecke character given by their product. Let

$$X = \{\chi \mid \chi = \phi\rho \text{ for some finite order character } \rho \text{ of } \mathrm{Gal}(L/K)\}.$$

We note that ρ is equivariant because L/K is anticyclotomic, so χ is also equivariant for all $\chi \in X$. Hence

$$L(s,\chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a}) N\mathfrak{a}^{-s} = \sum_{\mathfrak{a}} \chi(\bar{\mathfrak{a}}) N\mathfrak{a}^{-s} = \sum_{\mathfrak{a}} \overline{\chi}(\mathfrak{a}) N\mathfrak{a}^{-s} = L(s,\bar{\chi}).$$

For any real number s,

$$L(s,\bar{\chi}) = \lim_{t\to\infty} \sum_{N\mathfrak{a}\le t} \bar{\chi}(\mathfrak{a}) N\mathfrak{a}^{-s} = \lim_{t\to\infty} \overline{\sum_{N\mathfrak{a}\le t} \chi(\mathfrak{a}) N\mathfrak{a}^{-s}} = \overline{L(s,\chi)},$$

so $L(s,\chi)$ is real. Therefore, in the functional equation

$$\Lambda(s,\chi) = W(\chi)\Lambda(2-s,\bar{\chi}) = W(\chi)\Lambda(2-s,\chi),$$

the root number $W(\chi)$ is 1 or -1, and $W(\chi)$ determines the parity of the vanishing order of $L(s,\chi)$ at $s=1$. Here Λ is the completed L-function which is defined exactly in (2.10) below. However, $W(\chi)$ in fact almost determines the vanishing order, and we give the main result of this paper:

THEOREM 1.1. *For all but finitely many $\chi \in X$,*

$$\mathrm{ord}_{s=1} L(s,\chi) = \begin{cases} 0 & \text{if } W(\chi) = 1, \\ 1 & \text{if } W(\chi) = -1. \end{cases}$$

Our result is a generalization of that of Rohrlich [Roh84], who actually proved the case when the class number h of K is 1. As there are only nine imaginary quadratic fields with class number 1, it is desirable to remove the class number 1 assumption. We explain this from an arithmetic point of view. We know that there is a cusp form of weight 2, which has trivial central character in our case, associated with χ (see [Hec59, Shi71a, Shi72]). Then there is an abelian variety A associated to this cusp form (see [DDT95, Definition 1.44]). This abelian variety has to be defined over $\mathbb{Q}$ and of GL_2-type, and has complex multiplication over K as well (see [YZZ13, Chapter 3.2] for the definition of GL_2-type, and see [Mil] for the definition of abelian variety with complex multiplication). Every elliptic curve defined over $\mathbb{Q}$ with complex

multiplication by the ring of integers $\mathcal{O}$ of K can be obtained through this approach. This is because for each elliptic curve E of this type, there is a Hecke character ϕ of K associated to E, i.e. satisfying

$$L(s, E/\mathbb{Q}) = L(s, \phi),$$

by Deuring's result (see [Sil94, Chapter II, Theorem 10.5]). This Hecke character is equivariant because it is determined by an elliptic curve over $\mathbb{Q}$ (see [Shi71b, p. 519, (4.6)]), and also has infinite type $(1, 0)$, so we use the same notation ϕ when we state our main result. E is given by this ϕ under the corresponding principle. Note that the class number h of K must be 1 if this kind of elliptic curves exists. Rohrlich [Roh84] proved the same theorem for this kind of Hecke characters given by elliptic curves, and his calculation relies on the assumption that K has class number 1. Our main result does not need this assumption. So it can be viewed as a generalization from elliptic curves to abelian varieties defined over $\mathbb{Q}$ and of GL_2-type with complex multiplication over K. Even earlier, Greenberg proved the case of an elliptic curve E where P consists of a single prime (except 2, 3) of ordinary reduction for E (see [Gre83, Theorem 3 and Proposition 8, and the argument before Theorem 3]). The method of Greenberg is quite different.

The proof of Theorem 1.1 follows the pattern of [Roh84]. A key ingredient of [Roh84] is the following conclusion. Given $\chi \in X$ and a field automorphism σ of $\mathbb{C}$, let $\chi^\sigma : \mathfrak{a} \mapsto \chi(\mathfrak{a})^\sigma$. Then we have

$$\begin{aligned} L(1, \chi) = 0 &\implies L(1, \chi^\sigma) = 0, \\ W(\chi) = -1 \text{ and } L'(s, \chi) = 0 &\implies L'(s, \chi^\sigma) = 0. \end{aligned}$$

The first statement follows from [Shi76, Shi77], and the second from [GZ83]. These results allow us to take a suitable kind of average. Another key ingredient of [Roh84] is Ridout's p-adic version of Roth's theorem [Rid58]. Rohrlich uses it to give an important estimation, which we shall use later.

Our contribution is in the transition to Roth's theorem. The main difficulty is that the Hecke character has no good description on nonprincipal ideals. A novel point of our work is to formulate the restriction given by χ on nonprincipal ideals. More precisely, for each integral ideal $\mathfrak{a}$ which contributes to the average, every generator of $\mathfrak{a}^h$ must satisfy a strict restriction given by χ. Another point is to give a more general version of the Main Lemma of Rohrlich – it is necessary to work with certain hth radicals in each local part so that we can apply Rohrlich's estimation directly to get the right bound for a crucial set.

2. L-functions. We retain the above notations. Define $v = v(\chi) = 0$ or 1 through $W(\chi) = (-1)^{v(\chi)}$. We want to prove that for all but finitely

many $\chi \in X$,

$$L^{(v)}(1,\chi) \neq 0.$$

We recall some basic notations and results about Hecke characters. Let I be the group of nonzero fractional ideals and P be the subgroup of nonzero principal ideals. Given an integral ideal $\mathfrak{b}$ of K, we say that a fractional ideal $\mathfrak{a} \in I$ is *coprime* to $\mathfrak{b}$ if no prime ideal dividing $\mathfrak{b}$ occurs in the factorization of $\mathfrak{a}$ as a product of prime ideals. The multiplicative group consisting of such $\mathfrak{a}$ will be denoted $I_{\mathfrak{b}}$, and the subgroup $P \cap I_{\mathfrak{b}}$ will be denoted $P(\mathfrak{b})$. We say an element $\alpha \in K^\times$ is *coprime* to $\mathfrak{b}$ if $\alpha O \in P(\mathfrak{b})$, and we write $K(\mathfrak{b})$ for the subgroup of $K^\times$ consisting of all such α. Given $\alpha \in K^\times$, we write $\alpha \equiv 1 \bmod \mathfrak{b}$ to mean that for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{b}$, we have $v_{\mathfrak{p}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}\,\mathfrak{b}$, where $v_{\mathfrak{p}}$ is the valuation associated to $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}\,\mathfrak{b}$ is the multiplicity of $\mathfrak{p}$ in $\mathfrak{b}$. The set of such α is a subgroup $K_{\mathfrak{b}}$ of $K(\mathfrak{b})$.

Now ϕ is a character of $I_{\mathfrak{f}(\phi)}$ and we write $\phi(\mathfrak{a}) = 0$ if $\mathfrak{a} \in I$ is not coprime to $\mathfrak{f}(\phi)$. We know that there exists

$$\epsilon_1 : K(\mathfrak{f}(\phi)) \to K(\mathfrak{f}(\phi))/K_{\mathfrak{f}(\phi)} \simeq (\mathcal{O}/\mathfrak{f}(\phi))^\times \to \mathbb{C}^\times \tag{2.1}$$

such that

$$\phi(w\mathcal{O}) = \epsilon_1(w)w, \quad \forall w \in K^\times. \tag{2.2}$$

Here we set $\epsilon_1(w) = 0$ if w is not coprime to the conductor. In particular, let

$$\phi(n\mathcal{O}) = \kappa_1(n)n, \quad \forall n \in \mathbb{Z}. \tag{2.3}$$

Then

$$\kappa_1(n) = \phi(n\mathcal{O})n^{-1} \tag{2.4}$$

is a Dirichlet character. Let κ be the quadratic Dirichlet character corresponding to $K/\mathbb{Q}$. The following proposition is an equivalent description of equivariant Hecke characters with infinite type $(1,0)$. This is used in the argument of Rohrlich [Roh84, Section 1].

PROPOSITION 2.1. *Let ϕ be as above, but we do not assume ϕ is equivariant here. Then the following are equivalent:*

(1) $\phi(\bar{\mathfrak{a}}) = \bar{\phi}(\mathfrak{a})$ *for every integral ideal* $\mathfrak{a}$.
(2) κ_1 *is a quadratic Dirichlet character, and it coincides with* κ *on rational integers coprime to* $N\mathfrak{f}(\phi)$, *where* N *denotes the absolute norm. Moreover,* $\phi(\mathfrak{a}) = 0$ *for an integral ideal* $\mathfrak{a}$ *implies* $\phi(\bar{\mathfrak{a}}) = 0$.

Proof. (1)⇒(2). If $\phi(\mathfrak{a}) = 0$, then $\phi(\bar{\mathfrak{a}}) = \bar{\phi}(\mathfrak{a}) = 0$, so we may assume $\phi(\mathfrak{a}) \neq 0$. Note

$$\overline{\kappa_1(n)} = \overline{\phi(n\mathcal{O})n^{-1}} = \phi(n\mathcal{O})n^{-1} = \kappa_1(n).$$

This means that κ_1 is a quadratic Dirichlet character. Assume κ_1 is a character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then

$$\kappa_1(-n) = \phi_1(n\mathcal{O})(-n)^{-1} = -\kappa_1(n), \quad \text{so} \quad \kappa_1(-1) = -1.$$

So κ_1 is nontrivial, hence it equals 1 on half of the residue classes of $(\mathbb{Z}/m\mathbb{Z})^\times$, and -1 on the other half.

For each integral ideal $\mathfrak{a}$ of K which is coprime to $\mathfrak{f}(\phi)$,

$$\kappa_1(N\mathfrak{a}) = \phi(N\mathfrak{a}\cdot\mathcal{O})N\mathfrak{a}^{-1} = \phi(\mathfrak{a})\phi(\bar{\mathfrak{a}})N\mathfrak{a}^{-1} = \phi(\mathfrak{a})\bar{\phi}(\mathfrak{a})N\mathfrak{a}^{-1} = 1.$$

Here we use the fact that for the infinite type $(1,0)$ Hecke character ϕ, we have $\phi(\mathfrak{a})\bar{\phi}(\mathfrak{a}) = N\mathfrak{a}$. Therefore, $\kappa_1(p) = 1$ for each prime p which is coprime to $N\mathfrak{f}(\phi)$ and splits in K. These primes take up half of the residue classes of $(\mathbb{Z}/m\mathbb{Z})^\times$, because they have Dirichlet density $1/2$. So the other half of the residue classes of $(\mathbb{Z}/m\mathbb{Z})^\times$ will be taken up by primes which are inert in K, and κ_1 takes value -1 on that half. Recall that $\kappa(p) = 1$ if p splits in K, and $\kappa(p) = -1$ if p is inert in K. So we get the conclusion.

(2)$\Rightarrow$(1). If $\phi(\mathfrak{a}) = \phi(\bar{\mathfrak{a}}) = 0$, then (1) is obvious. Hence we may assume $\phi(\mathfrak{a}) \neq 0$. Since ϕ has infinite type $(1,0)$, we get $\phi(\mathfrak{a})\bar{\phi}(\mathfrak{a}) = N\mathfrak{a}$. Using condition (2) and the definition of κ_1, and noting that $\kappa(N\mathfrak{a}) = 1$ for each integral ideal $\mathfrak{a}$ if $\kappa(N\mathfrak{a}) \neq 0$, we get

$$\phi(\mathfrak{a})\phi(\bar{\mathfrak{a}})N\mathfrak{a}^{-1} = \kappa_1(N\mathfrak{a}) = \kappa(N\mathfrak{a}) = 1,$$

and hence $\phi(\mathfrak{a})\phi(\bar{\mathfrak{a}}) = N\mathfrak{a}$. Therefore

$$\phi(\mathfrak{a})\bar{\phi}(\mathfrak{a}) = \phi(\mathfrak{a})\phi(\bar{\mathfrak{a}})$$

and so $\bar{\phi}(\mathfrak{a}) = \phi(\bar{\mathfrak{a}})$ since $\phi(\mathfrak{a}) \neq 0$. ∎

We also need a technical reduction. Let $R(\chi)$ be the set of rational prime factors of $N\mathfrak{f}(\chi)$. Then $R(\chi)$ is a finite subset of $R(\phi) \cup P$. In particular, there are only finitely many possibilities for $R(\chi)$. Therefore, we fix a subset $R \subseteq R(\phi) \cup P$, and let

$$Y = \{\chi \in X \mid R(\chi) = R\}.$$

It will be sufficient to show that $L^{(v)}(1,\chi) \neq 0$ for all but finitely many $\chi \in Y$.

For $\chi \in Y$, let

$$\epsilon : K(\mathfrak{f}(\chi)) \to K(\mathfrak{f}(\chi))/K_{\mathfrak{f}(\chi)} \simeq (\mathcal{O}/\mathfrak{f}(\chi))^\times \to \mathbb{C}^\times \tag{2.5}$$

be such that

$$\chi(w\mathcal{O}) = \epsilon(w)w, \quad \forall w \in K^\times. \tag{2.6}$$

Here we also set $\epsilon(w) = 0$ if w is not coprime to χ. We have shown that

$$\chi(n\mathcal{O}) = \kappa(n)n, \quad \forall n \in \mathbb{Z} \text{ coprime to } \mathfrak{f}(\chi). \tag{2.7}$$

Now we begin to deal with L-functions. Let

$$A = (2\pi)^{-1}|\text{discriminant of } K|^{1/2}, \tag{2.8}$$

$$f = f(\chi) = (N\mathfrak{f}(\chi))^{1/2}, \tag{2.9}$$

$$\Lambda(s,\chi) = \Gamma(s)(Af)^s L(s,\chi). \tag{2.10}$$

The functional equation is

$$\Lambda(s,\chi) = W(\chi)\Lambda(2-s,\chi). \tag{2.11}$$

Let $K(\chi)$ be the finite extension of K generated by the values of χ. Let σ be a K-automorphism of $\mathbb{C}$. Define the Hecke character χ^σ by

$$\chi^\sigma(\mathfrak{a}) = (\chi(\mathfrak{a}))^\sigma \tag{2.12}$$

for all integral ideals $\mathfrak{a}$. Then χ^σ has infinite type $(1,0)$.

We consider

$$L^{(v)}(1,\chi)_{\text{av}} = [K(\chi):K]^{-1}\sum_\sigma L^{(v)}(1,\chi^\sigma), \tag{2.13}$$

where σ runs through the set of automorphisms of $\mathbb{C}$ which restrict to the distinct embeddings of $K(\chi)$ over K. The reason that this average can simplify the problem is the following. Suppose $L^{(v)}(1,\chi) = 0$. Then by the implications

$$L(1,\chi) = 0 \implies L(1,\chi^\sigma) = 0,$$
$$W(\chi) = -1 \text{ and } L'(s,\chi) = 0 \implies L'(s,\chi^\sigma) = 0,$$

which we have mentioned in the introduction, we know that every $L^{(v)}(1,\chi^\sigma)$ is zero. In particular, $L^{(v)}(1,\chi)_{\text{av}} = 0$. On the other hand, we shall prove that $L^{(v)}(1,\chi)_{\text{av}} \neq 0$ when $f(\chi)$ is sufficiently large. This will prove the theorem, because there are only finitely many $\chi \in Y$ such that $f(\chi)$ lies below a given bound. We define

$$\chi_{\text{av}}(\mathfrak{a}) = [K(\chi):K]^{-1}\sum_\sigma \chi(\mathfrak{a})^\sigma = [K(\chi):K]^{-1}\,\text{Tr}_{K(\chi)/K}(\chi(\mathfrak{a})). \tag{2.14}$$

For $\chi \in Y$, let $\mathcal{N}(\chi,t)$ denote the set of integral ideals $\mathfrak{a}$ of K satisfying the following conditions:

(1) $\chi_{\text{av}}(\mathfrak{a}) \neq 0$;
(2) $\mathfrak{a} \neq \bar{\mathfrak{a}}$;
(3) $N\mathfrak{a} \leq t$.

Let $N(\chi,t)$ be the cardinality of $\mathcal{N}(\chi,t)$.

The following two propositions about $N(\chi,t)$ will be proved in the next section:

PROPOSITION 2.2. *Fix $a < 1$. If $f = f(\chi)$ is sufficiently large, then*

$$N(\chi, f^a) = 0.$$

PROPOSITION 2.3. *There exist numbers $b > 1$ and $r < 1/2$ such that if $f = f(\chi)$ is sufficiently large, then*

$$N(\chi, f^b) < f^r.$$

Now assuming Propositions 2.2 and 2.3, we can follow the discussion in Rohrlich [Roh84] to obtain the asymptotic property of $L(1,\chi)_{\mathrm{av}}$ when f goes to infinity:

$$\begin{cases} L(1,\chi)_{\mathrm{av}} \to 2L(1,\kappa) & \text{if } W(\chi) = 1, \\ L'(1,\chi)_{\mathrm{av}} \sim 2L(1,\kappa)\log(Af) & \text{if } W(\chi) = -1. \end{cases}$$

We refer to Rohrlich [Roh84, Section 1], or to the arXiv version of the present paper 2412.05867v1, for the detailed proof. We say a few words about $\mathcal{N}(\chi,t)$ here. In the proof, the functional equation is involved and $L(s,\chi)_{\mathrm{av}}$ can be written as a sum in terms of $\chi_{\mathrm{av}}(\mathfrak{a})$, where $\mathfrak{a}$ is an integral ideal. Only $\mathfrak{a}$ such that $\chi_{\mathrm{av}}(\mathfrak{a}) \neq 0$ contribute to the sum, so condition (1) in the definition of $\mathcal{N}(\chi,t)$ should appear. If one checks the proof, it will be found that the sum of $\mathfrak{a} = \bar{\mathfrak{a}}$ terms forms the main term, and the sum of $\mathfrak{a} \neq \bar{\mathfrak{a}}$ terms forms the error term. So condition (2) in the definition of $\mathcal{N}(\chi,t)$ should appear as well. Hence $\mathcal{N}(\chi,t)$ should be considered.

There are two points which should be additionally verified when applying Rohrlich's method. The first point is that we know χ^σ is still an equivariant Hecke character because of Proposition 2.1 although it may not be in Y. Note that χ^σ is in Y in the class number 1 case. The second point is that the formula [Roh84, (16)]

$$W(\chi^\sigma) = W(\chi) \tag{2.15}$$

should be verified in the general case rather than in the class number 1 case. We write it as a proposition.

PROPOSITION 2.4. *Let χ be an equivariant Hecke character of infinite type $(1,0)$. Let σ be a K-automorphism of $\mathbb{C}$. Then*

$$W(\chi^\sigma) = W(\chi).$$

Proof. There is an explicit formula for $W(\chi)$ (see [Miy89, p. 93, Theorem 3.3.1]). Let $\mathcal{D}$ be the different ideal of K, i.e. the integral ideal of K such that

$$\mathcal{D}^{-1} = \{a \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(ab) \in \mathbb{Z},\ \forall b \in \mathcal{O}\}. \tag{2.16}$$

For a quadratic field $K = \mathbb{Q}(\sqrt{D})$, we have

$$\mathcal{D} = \begin{cases} (2\sqrt{D})\mathcal{O} & \text{if } D \equiv 2,3 \bmod 4, \\ \sqrt{D}\mathcal{O} & \text{if } D \equiv 1 \bmod 4. \end{cases} \tag{2.17}$$

Take an integral ideal $\mathfrak{c}$ such that $\mathfrak{f}(\chi)\mathfrak{c} = b\mathcal{O}$, $b \in \mathcal{O}$, and $\mathfrak{f}(\chi)$ is coprime to $\mathfrak{c}$. Let δ be a generator of $\mathcal{D}$. Then by [Miy89, Theorem 3.3.1, p. 93], we have

$$W(\chi) = (-i) \cdot f^{-1} \cdot \frac{\delta}{|\delta|} \cdot \frac{b}{|b|} \cdot \frac{N(\mathfrak{c})^{1/2}}{\chi(\mathfrak{c})} \cdot \sum_w \epsilon(w) e^{2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\frac{w}{\delta b})}, \tag{2.18}$$

where w runs through the representatives of $\mathfrak{c}/\mathfrak{f}(\chi)\mathfrak{c}$. We may assume that $\delta/|\delta| = i$. Then we substitute $f = N(\mathfrak{f}(\chi))^{1/2}$, $|b| = N(\mathfrak{f}(\chi)\mathfrak{c})^{1/2}$, and let $c(\chi) = \frac{b}{N(\mathfrak{f}(\chi))}\chi(\mathfrak{c})^{-1}$. Then

$$W(\chi) = \frac{b}{N(\mathfrak{f}(\chi))}\chi(\mathfrak{c})^{-1} \sum_w \epsilon(w) e^{2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\frac{w}{\delta b})} = c(\chi) \sum_w \epsilon(w) e^{2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\frac{w}{\delta b})}. \tag{2.19}$$

Let ξ be a root of unity such that $\mathbb{Q}(\xi)$ includes K and all roots of unity $e^{2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\frac{w}{\delta b})}$. Let $\sigma(\xi) = \xi^m$, where m is a positive integer. We apply σ to $W(\chi)$ (recall that $W(\chi) = 1$ or -1) to get

$$W(\chi) = c(\chi^\sigma) \sum_w \epsilon(w)^\sigma e^{2\pi i \operatorname{Tr}_{K/\mathbb{Q}}(\frac{mw}{\delta b})}. \tag{2.20}$$

Taking $n \in \mathbb{Z}$ such that $nm \equiv 1 \bmod \mathfrak{f}(\chi)$ and replacing w by nw in the above equation, we have

$$W(\chi) = \kappa(n) W(\chi^\sigma), \tag{2.21}$$

where we use $\epsilon(nw) = \kappa(n)\epsilon(w)$. Note that $\kappa(n) = \kappa(m) = 1$, because a description of κ is $\mathrm{Gal}(\mathbb{Q}(\xi')/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \simeq \{\pm 1\}$, for a suitable root of unity ξ', and we have assumed σ fixes K. ∎

By the two points described pior to (2.15), we can show that the statement before formula (17) in [Roh84], '...whence formula (14) remains true (with the same v and f) if χ is replaced by χ^σ', holds true in our case.

Now we can use the asymptotic property of $L(1,\chi)_{\mathrm{av}}$ when f goes to infinity and the well-known result $L(1,\kappa) \neq 0$ to obtain $L(1,\chi)_{\mathrm{av}} \neq 0$ when f is sufficiently large, and thus finish the proof of the theorem under the assumption of Propositions 2.2 and 2.3. Hence, it remains to prove the propositions.

3. The proof of Propositions 2.2 and 2.3. We shall convert Propositions 2.2 and 2.3 into statements about pairs of rational integers. The final form is exactly the estimation given by Rohrlich, which will finish the proof. We begin with a lemma about the trace of a root of unity.

LEMMA 3.1. *Let F be a number field, and ξ be a root of unity of order N. Then there is a positive integer μ only depending on F such that if there exists a prime p satisfying $p^\mu \mid N$, then* $\operatorname{Tr}_{F(\xi)/F}(\xi) = 0$.

Proof. We prove that for a fixed prime p, there is a positive integer μ_p, depending on F and p, such that if $p^{\mu_p} \mid N$, then $\mathrm{Tr}_{F(\xi)/F}(\xi) = 0$, and we can take $\mu_p = 2$ for all but finitely many p.

Let $\xi = \zeta\eta$, where ζ is a root of unity of order p^k, and η is a root of unity of order coprime to p. Let F^p and $\mathbb{Q}^p$ denote the fields generated by all roots of unity of p-power order over F and $\mathbb{Q}$ respectively. View $\mathrm{Gal}(F^p/F)$ as a subgroup of $\mathrm{Gal}(\mathbb{Q}^p/\mathbb{Q}) \simeq \mathbb{Z}_p^\times$ through $\mathrm{Gal}(F^p/F) \simeq \mathrm{Gal}(\mathbb{Q}^p/\mathbb{Q}^p \cap F)$. Take $\mu_p \geq 2$ such that the inertia subgroup at some prime of F over p contains $1 + p^{\mu_p - 1}\mathbb{Z}_p$. Then the ramification index of $F(\zeta)/F(\zeta^p)$ over this prime is p when $k \geq \mu_p$. Since $F(\xi)/F(\zeta)$ and $F(\xi^p)/F(\zeta^p)$ are unramified at every prime over p, the ramification index of $F(\xi)/F(\xi^p)$ at some prime over p is p when $p^{\mu_p} \mid N$. In particular, $[F(\xi) : F(\xi^p)] = p$, thus $\mathrm{Tr}_{F(\xi)/F}(\xi) = 0$.

Note that we can take $\mu_p = 2$ if $\mathbb{Q}^p \cap F = \mathbb{Q}$, and this is true for all but finitely many p. So the constant

$$\mu = \max_{p \mid [F:\mathbb{Q}]} \mu_p$$

satisfies our demand. ∎

We define some notations before applying Lemma 3.1. Fix an ideal class of K. Let $\mathfrak{a}_0$ be a fractional ideal in this class such that $\mathfrak{a}_0$ is coprime to $\mathfrak{f}(\chi)$ and every integral ideal in this class can be written as $w\mathfrak{a}_0$ ($w \in \mathcal{O}$). Let $\mathcal{N}_0(\chi, t)$ be the set of all integral ideals $\mathfrak{a}$ satisfying the following conditions:

(1) $\chi_{\mathrm{av}}(\mathfrak{a}) \neq 0$;
(2) $\mathfrak{a} \neq \bar{\mathfrak{a}}$;
(3) $N\mathfrak{a} \leq t$;
(4) $\mathfrak{a}$ is in the ideal class of $\mathfrak{a}_0$.

Thus $\mathcal{N}_0(\chi, t)$ is a subset of $\mathcal{N}(\chi, t)$. Let $N_0(\chi, t)$ be the cardinality of $\mathcal{N}_0(\chi, t)$. It suffices to prove $N_0(\chi, t)$ satisfies the same bound as in Propositions 2.2 and 2.3 since the class number is finite.

Let $\mathfrak{a}_0^h = w_0\mathcal{O}$ and fix $p \in R$. Consider the natural embedding

$$\mathcal{O} \to \mathcal{O} \otimes \mathbb{Z}_p.$$

Then

$$w_0 \in (\mathcal{O} \otimes \mathbb{Z}_p)^\times \simeq \prod_{v \mid p} \mathcal{O}_v^\times,$$

where $\mathcal{O}_v$ is the completion of $\mathcal{O}$ with respect to v. This is because we have assumed that $\mathfrak{a}_0$ is coprime to $\mathfrak{f}(\chi)$ and $p \in R$, so $w_0 \in \mathcal{O}_v^\times$ for all $v \mid p$. Recall

$$\mathcal{O}_v^\times \simeq \mu_{q-1} \oplus \mu_{p^a} \oplus \mathbb{Z}_p^{[k_v : \mathbb{Q}_p]}, \tag{3.1}$$

where q is the cardinality of the residue field, μ with a subscript denotes the group of roots of unity of a certain order, and a is a positive integer. Hence

$$(\mathcal{O} \otimes \mathbb{Z}_p)^\times \simeq \text{finite group} \oplus \mathbb{Z}_p^2. \tag{3.2}$$

We know there exists a character ϵ_p of $(\mathcal{O}\otimes\mathbb{Z}_p)^\times$ for each $p\in R$ such that

$$\epsilon(w)=\prod_{p\in R}\epsilon_p(w),\qquad \forall w\in\mathcal{O}. \tag{3.3}$$

Here ϵ_p is extended to $\mathcal{O}\otimes\mathbb{Z}_p$ by setting it to be 0 on nonunits. This decomposition can be found in [Roh, Lecture 2].

Now we apply Lemma 3.1 to get the following lemma.

LEMMA 3.2. *There exists a positive integer μ such that if $\chi_{\mathrm{av}}(\mathfrak{a})\neq 0$, then the order of $\epsilon_p(w^h w_0)$ is not divisible by p^μ for any $p\in R$.*

Proof. Let $\mathfrak{a}=w\mathfrak{a}_0$. Note that

$$\chi(\mathfrak{a})^h=\chi(\mathfrak{a}^h)=\chi(w^hw_0\mathcal{O})=\epsilon(w^hw_0)w^hw_0,$$

thus $\chi(\mathfrak{a})$ has the form $\zeta w\sqrt[h]{w_0}$, where $\sqrt[h]{w_0}$ is a fixed hth radical of w_0 in $\mathbb{C}$ (we do not care which one), and ζ is a root of unity. Hence

$$\begin{aligned}\chi_{\mathrm{av}}(\mathfrak{a})&=\mathrm{Tr}_{K(\chi)/K}(\zeta w\sqrt[h]{w_0})\\&=\frac{1}{n}\,\mathrm{Tr}_{K(\chi,\sqrt[h]{w_0})/K}(\zeta w\sqrt[h]{w_0})\\&=\frac{1}{n}\,\mathrm{Tr}_{K(\sqrt[h]{w_0})/K}(\mathrm{Tr}_{K(\chi,\sqrt[h]{w_0})/K(\sqrt[h]{w_0})}(\zeta w\sqrt[h]{w_0}))\\&=\frac{1}{n}\,\mathrm{Tr}_{K(\sqrt[h]{w_0})/K}(w\sqrt[h]{w_0}\,\mathrm{Tr}_{K(\chi,\sqrt[h]{w_0})/K(\sqrt[h]{w_0})}(\zeta)),\end{aligned} \tag{3.4}$$

where $n=[K(\chi,\sqrt[h]{w_0}):K(\chi)]$. Therefore,

$$\chi_{\mathrm{av}}(\mathfrak{a})\neq 0\implies \mathrm{Tr}_{K(\chi,\sqrt[h]{w_0})/K(\sqrt[h]{w_0})}(\zeta)\neq 0.$$

Applying Lemma 3.1 to $K(\sqrt[h]{w_0})$, we find that

- *there exists a positive integer μ_1 such that if $\chi_{\mathrm{av}}(\mathfrak{a})\neq 0$ then the order of ζ is not divisible by p^{μ_1} for any prime p.*

Thus

- *there exists a positive integer μ_2 such that if $\chi_{\mathrm{av}}(\mathfrak{a})\neq 0$ then the order of $\epsilon(w^hw_0)=\zeta^h$ is not divisible by p^{μ_2} for any prime p.*

Therefore

- *there exists a positive integer μ such that if $\chi_{\mathrm{av}}(\mathfrak{a})\neq 0$ then the order of $\epsilon_p(w^hw_0)$ is not divisible by p^μ for any $p\in R$.*

This is because for every $w\in\mathcal{O}$,

$$\epsilon(w)=\epsilon_p(w)\prod_{l\in R,\,l\neq p}\epsilon_l(w),$$

and the power of p in the order of $\epsilon_l(w)$ is controlled by a constant because $(\mathcal{O}\otimes\mathbb{Z}_l)^\times$ is the product of a finite group and a pro-l group. Thus the

statement that the order of $\epsilon(w)$ is divisible by p^μ is equivalent to the order of $\epsilon_p(w)$ being divisible by p^μ when μ is sufficiently large. ∎

We view $\mathbb{Z}_p^\times \simeq (\mathbb{Z}\otimes\mathbb{Z}_p)^\times$ as a subgroup of $(\mathcal{O}\otimes\mathbb{Z}_p)^\times$, and define

$$H_p = \{a \in (\mathcal{O}\otimes\mathbb{Z}_p)^\times \mid a^m \in \mathbb{Z}_p^\times \text{ for some positive integer } m\}.$$

Then $\mathbb{Z}_p^\times$ is of finite index in H_p. For every $p \in P$, fix a set Ω_p of representatives of $H_p/\mathbb{Z}_p^\times$. Define

$$S_p = \{a \in (\mathcal{O}\otimes\mathbb{Z}_p)^\times \mid a^h \in H_p w_0^{-1}\}.$$

The set S_p may be empty. When it is not empty, for all $x_1, x_2 \in S_p$ we have $x_1^h x_2^{-h} \in H_p$, and thus $x_1 x_2^{-1} \in H_p$. We fix $x_p \in S_p$ if S_p is not empty; then every element in S_p can be written as $\eta_p\omega_p x_p$, where $\eta_p \in \mathbb{Z}_p^\times$ and $\omega_p \in \Omega_p$. Let

$$P' = \{p \in P \mid S_p \text{ is not empty}\}.$$

Lemma 3.3 (Main Lemma). *For every $\chi \in Y$, there exists a positive integer*

$$q(\chi) = \prod_{p\in P\cap R} p^{n_p(\chi)}$$

satisfying the following conditions:

(1) *Assume $\chi_{\mathrm{av}}(\mathfrak{a}) \neq 0$ for some $\mathfrak{a} = w\mathfrak{a}_0$. Then for every $p \mid q(\chi)$, we have $p \in P'$, and there exist $\eta_p \in \mathbb{Z}_p^\times$ and $\omega_p \in \Omega_p$ such that*

$$w \equiv \eta_p\omega_p x_p \bmod q(\chi)\mathcal{O}\otimes\mathbb{Z}_p.$$

(2) *$f(\chi) \le k_0 q(\chi)$ and $q(\chi) \le k_1 f(\chi)$, where k_0 and k_1 are positive integers independent of χ.*

Proof. Let μ be the constant of Lemma 3.2. We may assume μ is so large that p^μ annihilates the Sylow p-subgroup of $(\mathcal{O}\otimes\mathbb{Z}_p)^\times/(1+p^3\mathcal{O}\otimes\mathbb{Z}_p)$. For every $\chi \in Y$, define $m_p(\chi)$, $p \in R$, through

$$N\mathfrak{f}(\chi) = \prod_{p\in R} p^{m_p(\chi)}. \tag{3.5}$$

Let

$$\text{order of } \epsilon_p|_{1+p^3\mathcal{O}\otimes\mathbb{Z}_p} = p^{o_p(\chi)}. \tag{3.6}$$

For every $p \in P\cap R$, define

$$n_p(\chi) = \begin{cases} 0 & \text{if } o_p(\chi) \le \mu + h, \\ o_p(\chi) - \mu - h & \text{if } o_p(\chi) > \mu + h. \end{cases} \tag{3.7}$$

Now we analyse the kernel of $\epsilon_p|_{1+p^3\mathcal{O}\otimes\mathbb{Z}_p}$. The restriction of ϵ_p to $\mathbb{Z}_p^\times$ is κ_p, which is the p-component of κ, hence a quadratic character. In particular, ϵ_p is trivial on $1+p^3\mathbb{Z}_p$, because every element in $1+p^3\mathbb{Z}_p$ is a square.

On the other hand, ϵ_p is also trivial on $1+p^{3+o_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p$, because we have (3.6) and every element in $1+p^{3+o_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p$ is a $p^{o_p(\chi)}$th power. Since

$$(1+p^3\mathcal{O}\otimes\mathbb{Z}_p)/(1+p^3\mathbb{Z}_p)(1+p^{3+o_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p)$$

is a cyclic group of order $p^{o_p(\chi)}$, we obtain

$$\ker\epsilon_p|_{1+p^3\mathcal{O}\otimes\mathbb{Z}_p}=(1+p^3\mathbb{Z}_p)(1+p^{3+o_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p). \tag{3.8}$$

We begin to verify (1). The condition $p\,|\,q(\chi)$ means $o_p(\chi)>\mu+h$. Since $\chi_{\mathrm{av}}(\mathfrak{a})\neq 0$, we have $p^\mu\nmid$ order of $\epsilon_p(w^hw_0)$. Since p^μ annihilates the Sylow p-subgroup of $(\mathcal{O}\otimes\mathbb{Z}_p)^\times/(1+p^3\mathcal{O}\otimes\mathbb{Z}_p)$ as we have assumed, we have

$$w^{mh}w_0^m\in 1+p^3\mathcal{O}\otimes\mathbb{Z}_p, \tag{3.9}$$

where $m=jp^\mu$ with j a positive integer coprime to p.

The order of $\epsilon_p(w^hw_0)$ is not divisible by p^μ, so the order of $\epsilon_p(w^{mh}w_0^m)$ is coprime to p. Then $\epsilon_p(w^{mh}w_0^m)$ has to be 1 as its order is a power of p. Because of (3.8), we can assume

$$zw^{mh}w_0^m\in 1+p^3\mathbb{Z}_p,\quad z\in 1+p^{3+o_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p. \tag{3.10}$$

Write

$$z=z_1^m,\quad z_1\in 1+p^{n_p(\chi)+h}\mathcal{O}\otimes\mathbb{Z}_p. \tag{3.11}$$

So

$$(z_1w^hw_0)^m\in 1+p^3\mathbb{Z}_p. \tag{3.12}$$

In particular,

$$z_1w^hw_0=\eta_p'\omega_p',\quad \eta_p'\in\mathbb{Z}_p^\times,\ \omega_p'\in\Omega_p. \tag{3.13}$$

Write

$$z_1=z_2^h,\quad z_2\in 1+p^{n_p(\chi)}\mathcal{O}\otimes\mathbb{Z}_p. \tag{3.14}$$

Then

$$(z_2w)^h=\eta_p'\omega_p'w_0^{-1}. \tag{3.15}$$

So S_p is not empty, i.e. $p\in P'$, and we can suppose

$$z_2w=\eta_p\omega_px_p,\quad \eta_p\in\mathbb{Z}_p^\times,\ \omega_p\in\Omega_p. \tag{3.16}$$

Hence we obtain the congruence equation

$$w\equiv\eta_p\omega_px_p \bmod q\mathcal{O}\otimes\mathbb{Z}_p. \tag{3.17}$$

Now we verify (2). For every $p\in P\cap R$, let $\mathfrak{f}(\epsilon_p)$ be the conductor of ϵ_p, i.e. the maximal integral ideal of k such that

$$\epsilon_p|_{1+\mathfrak{f}(\epsilon_p)\otimes\mathbb{Z}_p}=1. \tag{3.18}$$

Then $N\mathfrak{f}(\epsilon_p)=p^{m_p(\chi)}$.

If $o_p(\chi) \leq \mu + h$, then $n_p(\chi) = 0$ and ϵ_p is trivial on $1 + p^{3+\mu+h}\mathcal{O} \otimes \mathbb{Z}_p$. Hence

$$\left| \frac{m_p(\chi)}{2} - n_p(\chi) \right| \leq 3 + \mu + h. \tag{3.19}$$

If $o_p(\chi) > \mu + h$, then $n_p(\chi) = o_p(\chi) - \mu - h$, ϵ_p is trivial on $1 + p^{3+o_p(\chi)}\mathcal{O} \otimes \mathbb{Z}_p$, but is nontrivial on $1 + p^{2+o_p(\chi)}\mathcal{O} \otimes \mathbb{Z}_p$. So we also have

$$\left| \frac{m_p(\chi)}{2} - n_p(\chi) \right| \leq 3 + \mu + h. \tag{3.20}$$

Let

$$k = \prod_{p \in R,\, p \notin P} p^{\frac{m_p(\chi)}{2}}, \tag{3.21}$$

$$k' = \prod_{p \in P \cap R} p^{3+\mu+h}. \tag{3.22}$$

Let $k_0 = kk', k_1 = k'/k$. Note that

$$f(\chi) = \prod_{p \in R,\, p \notin P} p^{\frac{m_p(\chi)}{2}} \cdot \prod_{p \in P \cap R} p^{\frac{m_p(\chi)}{2}}, \tag{3.23}$$

$$q(\chi) = \prod_{p \in P \cap R} p^{n_p(\chi)}. \tag{3.24}$$

Along with (3.19), (3.20), we obtain (2). ∎

If every integral ideal $\mathfrak{a}$ in the ideal class of $\mathfrak{a}_0$ satisfies $\chi_{\mathrm{av}}(\mathfrak{a}) = 0$, then the conclusions of Propositions 2.2 and 2.3 obviously hold. We can always assume that there exists $\mathfrak{a}$ such that $\chi_{\mathrm{av}}(\mathfrak{a}) \neq 0$, thus (1) of the Main Lemma implies that $q(\chi)$ is only divisible by primes in P'.

Now we begin to apply the Main Lemma. Let

$$\Omega = \prod_{p \in P'} \Omega_p,$$

which is a finite set. For $\omega \in \Omega$ and $p \in P'$, let ω_p be the p-component of ω. Take $\omega \in \Omega$, a positive real number t, and a positive integer q which is only divisible by primes in P'. Define $\mathcal{N}_\omega(q, t)$ to be the set of $w \in \mathcal{O}$ satisfying the following conditions:

(1) for every $p \in P'$, there exists $\eta_p \in \mathbb{Z}_p^\times$ such that

$$w \equiv \eta_p \omega_p x_p \bmod q\mathcal{O} \otimes \mathbb{Z}_p;$$

(2) $w^h w_0 \mathcal{O} \neq \overline{w^h w_0}\mathcal{O}$;
(3) $|w| \leq t$.

Let $N_\omega(q, t)$ be the cardinality of $\mathcal{N}_\omega(q, t)$.

In view of the Main Lemma, there exists a map

$$\mathcal{N}_0(\chi,t)\to\bigcup_{\omega\in\Omega}\mathcal{N}_\omega(q(\chi),lt^{1/2}).$$

The map assigns to each $\mathfrak{a}=w\mathfrak{a}_0$ an arbitrarily chosen generator $w\in\mathcal{O}$ for the integral ideal $\mathfrak{a}\mathfrak{a}_0^{-1}$, and the constant l equals $|w_0|^{-1/h}$. The map is injective since these ideals are uniquely determined by their generators. So

$$N_0(\chi,t)\le\sum_{\omega\in\Omega}N_\omega(q(\chi),lt^{1/2}).$$

Therefore it suffices to show the following form of Propositions 2.2 and 2.3.

PROPOSITION 3.4 (Second form of Propositions 2.2 and 2.3). *Fix $c<1/2$. If q is sufficiently large, then*

$$N_\omega(q,q^c)=0.$$

Moreover, there exist absolute constants $d>1/2$ and $s<1/2$ such that if q is sufficiently large, then

$$N_\omega(q,q^d)<q^s.$$

Let us see how to deduce the first form of Propositions 2.2 and 2.3 from the second form. Fix $a<1$ and choose c such that $a/2<c<1/2$. From (2) of the Main Lemma, when $q(\chi)$ is sufficiently large,

$$f(\chi)^{a/2}\le(k_0q(\chi))^{a/2}\le l^{-1}q(\chi)^c. \tag{3.25}$$

Hence when $q(\chi)$ is sufficiently large,

$$N_0(\chi,f(\chi)^a)\le\sum_{\omega\in\Omega}N_\omega(q(\chi),q(\chi)^c), \tag{3.26}$$

and the right side is 0. Thus we obtain the first form of Proposition 2.2.

Next, take $d>1/2$ and $s<1/2$ as in the second form of Proposition 2.3, and choose b,r such that $2d>b>1$ and $s<r<1/2$. Then, if $f(\chi)$ is sufficiently large,

$$N_0(\chi,f(\chi)^b)\le\sum_{\omega\in\Omega}N_\omega(q(\chi),q(\chi)^d)<\sum_{\omega\in\Omega}q(\chi)^s<f(\chi)^r, \tag{3.27}$$

i.e. the first form of Proposition 2.3 holds true.

Fix $\omega\in\Omega$ and let τ be an element of $\mathcal{O}$ such that $\{1,\tau\}$ is a basis for $\mathcal{O}$ over $\mathbb{Z}$. Then for each $p\in P'$, $\{1,\tau\otimes1\}$ is a basis for $\mathcal{O}\otimes\mathbb{Z}_p$ over $\mathbb{Z}_p$. In particular, for every $p\in P'$, there exist unique $\alpha_p,\beta_p\in\mathbb{Z}_p$ such that

$$\omega_px_p=\alpha_p+\beta_p\tau\otimes1. \tag{3.28}$$

Let $\mathcal{M}(q,t)$ be the set of all pairs (u,v) of rational integers satisfying

(1) for every $p\in P'$, $u\beta_p-v\alpha_p\equiv0 \bmod q\mathbb{Z}_p$;
(2) for every $p\in P'$, $u\beta_p-v\alpha_p\neq0$;
(3) $|u|,|v|\le t$.

Let $M(q,t)$ be the cardinality of $\mathcal{M}(q,t)$. Our purpose is to convert Propositions 2.2 and 2.3 into a description of $M(q,t)$.

Since all norms on a Euclidean space are equivalent, there exists a constant k such that

$$\max(|x|,|y|) \le k|x+\tau y|, \qquad x,\, y \in \mathbb{R}. \tag{3.29}$$

Now we verify that

$$w = u + v\tau \mapsto (u,v)$$

is a map from $\mathcal{N}_\omega(q,t)$ to $\mathcal{M}(q,kt)$. From

$$w \equiv \eta_p \omega_p x_p \bmod q\mathcal{O}\otimes\mathbb{Z}_p,$$

we see that for each $p \in P'$,

$$u \equiv \eta_p \alpha_p \bmod q\mathbb{Z}_p, \tag{3.30}$$

$$v \equiv \eta_p \beta_p \bmod q\mathbb{Z}_p. \tag{3.31}$$

Multiplying the first congruence by β_p and the second by α_p, and subtracting, we obtain

$$u\beta_p - v\alpha_p \equiv 0 \bmod q\mathbb{Z}_p, \tag{3.32}$$

i.e. (u,v) satisfies (1) of the definition $\mathcal{M}(q,kt)$.

Suppose $u\beta_p - v\alpha_p = 0$. Since α_p, β_p are not both 0, we can write

$$(u,v) = \eta(\alpha_p,\beta_p), \qquad \eta \in \mathbb{Q}_p. \tag{3.33}$$

Then $w = \eta\omega_p x_p$ in $K\otimes\mathbb{Q}_p$. From $x_p \in S_p$, we have

$$w^h = \eta^h \omega_p^h x_p^h = \eta'\omega' w_0^{-1} \in K\otimes\mathbb{Q}_p, \qquad \eta' \in \mathbb{Q}_p,\ \omega' \in H_p. \tag{3.34}$$

Take a positive integer m such that $(\omega')^m \in \mathbb{Z}_p^\times$. Then

$$w^{mh} w_0^m = (\eta'\omega')^m \in \mathbb{Q}_p \cap \mathcal{O} = \mathbb{Z}, \tag{3.35}$$

contradicting $w^h w_0 \mathcal{O} \ne \overline{w^h w_0}\mathcal{O}$. So $u\beta_p - v\alpha_p \ne 0$, i.e. (u,v) satisfies (2) of the definition of $\mathcal{M}(q,kt)$.

Finally, if $|w| \le t$, then $|u|, |v| \le kt$ (by (3.29)), i.e. (u,v) satisfies (3) of the definition of $\mathcal{M}(q,kt)$. So $w = u + v\tau \mapsto (u,v)$ indeed defines a map from $\mathcal{N}_\omega(q,t)$ to $\mathcal{M}(q,kt)$, and the map is obviously injective. Therefore,

$$N_\omega(q,t) \le M(q,kt). \tag{3.36}$$

So it is sufficient to show the following form of Propositions 2.2 and 2.3.

Proposition 3.5 (Third form of Propositions 2.2 and 2.3). *Fix $c < 1/2$. If q is sufficiently large, then*

$$M(q,q^c) = 0.$$

Moreover, there exist absolute constants $d > 1/2$ and $s < 1/2$ such that if q is sufficiently large, then

$$M(q,q^d) < q^s.$$

Since $N_\omega(q,t) \le M(q,kt)$, we can easily deduce the second form from the third. Fix $c < 1/2$ and choose c' such that $c < c' < 1/2$. Then if q is sufficiently large, we have

$$N_\omega(q,q^c) \le M(q,kq^c) \le M(q,q^{c'}) = 0, \tag{3.37}$$

i.e. the second form of Proposition 2.2. The argument for Proposition 2.3 is similar.

We now show that we may assume that α_p, β_p are algebraic over $\mathbb{Q}$.

LEMMA 3.6. *(α_p, β_p) can be written as $(\alpha_p, \beta_p) = \eta_p(\alpha_p', \beta_p')$, where α_p', β_p' are elements in $\mathbb{Z}_p$ which are algebraic over $\mathbb{Q}$, and $\eta_p \in \mathbb{Z}_p^\times$.*

Proof. For each nonnegative integer j, define $a_j, b_j \in \mathbb{Z}$ through $\tau^j = a_j\tau \otimes 1 + b_j$. Take a positive integer m such that

$$(\omega_p x_p)^{mh} \in \mathbb{Z}_p^\times w_0^{-m}. \tag{3.38}$$

Then

$$(\omega_p x_p)^{mh} w_0^m \in \mathbb{Z}_p^\times, \tag{3.39}$$

and

$$(\omega_p x_p)^{mh} = \Big(\sum_{j=0}^{mh} b_j \binom{mh}{j} \alpha_p^{mh-j}\beta_p^j\Big) + \Big(\sum_{j=0}^{mh} a_j \binom{mh}{j} \alpha_p^{mh-j}\beta_p^j\Big)\tau \otimes 1. \tag{3.40}$$

Let

$$w_0^m = u_0 + v_0\tau \otimes 1, \quad u_0, v_0 \in \mathbb{Z}. \tag{3.41}$$

Then

$$\begin{aligned}(\omega_p x_p)^{mh} w_0^m = &\Big(\sum_{j=0}^{mh} (u_0 b_j + v_0 b_2 a_j) \binom{mh}{j} \alpha_p^{mh-j}\beta_p^j\Big) \\ &+ \Big(\sum_{j=0}^{mh} (v_0 b_j + (u_0 + v_0 a_2)a_j) \binom{mh}{j} \alpha_p^{mh-j}\beta_p^j\Big)\tau \otimes 1.\end{aligned} \tag{3.42}$$

Therefore,

$$\sum_{j=0}^{mh} (v_0 b_j + (u_0 + v_0 a_2)a_j) \binom{mh}{j} \alpha_p^{mh-j}\beta_p^j = 0. \tag{3.43}$$

Note that $a_0 = 0, b_0 = 1, a_1 = 1, b_1 = 0$. If $v_0 \ne 0$, we have $v_0 b_0 + (u_0 + v_0 a_2)a_0 = v_0 \ne 0$. If $v_0 = 0$, we have $u_0 \ne 0, v_0 b_1 + (u_0 + v_0 a_2)a_1 = u_0 \ne 0$. Hence (α_p, β_p) always satisfies a nontrivial homogeneous polynomial equation with coefficients in $\mathbb{Z}$. This implies the desired conclusion. ∎

Since the conditions of $\mathcal{M}(q,t)$ are homogeneous, we may assume α_p, β_p are algebraic over $\mathbb{Q}$.

The third form of Propositions 2.2 and 2.3 is already proved in [Roh84, Section 3], by applying Roth's theorem. So the proof of Theorem 1.1 is complete.

Acknowledgements. This paper will be the crucial part of the author's master degree thesis under the supervision of Professor Xin Wan. The author extends his deepest gratitude to Professor Xin Wan for suggesting this interesting project, for his patient and insightful guidance, and for his encouragement throughout the whole process. He is also indebted to Professor David E. Rohrlich for his paper [Roh84] which inspired this work, and for his positive perspective on this problem and helpful communications passed on to the author by Professor Xin Wan. He wants to thank the anonymous reviewer for his/her detailed and helpful revision suggestions. Finally, he is grateful to Haidong Li, Ruichen Xu, and Dr. Luochen Zhao for beneficial conversations.

References

[DDT95] H. Darmon, F. Diamond and R. Taylor, *Fermat's last theorem*, in: Current Developments in Mathematics, Int. Press, 1995, 1–157.

[Gre83] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math. 72 (1983), 241–266.

[GZ83] B. H. Gross et D. Zagier, *Points de Heegner et dérivées de fonctions L*, C. R. Acad. Sci. Paris Sér. I 297 (1983), 85–87.

[Hec59] E. Hecke, *Mathematische Werke*, Vandenhoeck & Ruprecht, 1959.

[Mil] J. S. Milne, *Complex Multiplication*, https://www.jmilne.org/math/CourseNotes/cm.html.

[Miy89] T. Miyake, *Modular Forms*, Springer, 1989.

[Rid58] D. Ridout, *The p-adic generalization of the Thue–Siegel–Roth theorem*, Mathematika 5 (1958), 40–48.

[Roh84] D. E. Rohrlich, *On L-functions of elliptic curves and anticyclotomic towers*, Invent. Math. 75 (1984), 383–408.

[Roh] D. E. Rohrlich, *Root numbers*, http://math.bu.edu/people/rohrlich/pcmi.pdf.

[Shi71a] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. 43 (1971), 199–208.

[Shi71b] G. Shimura, *On the zeta-function of an abelian variety with complex multiplication*, Ann. of Math. 94 (1971), 504–533.

[Shi72] G. Shimura, *Class fields over real quadratic fields and Hecke operators*, Ann. of Math. 95 (1972), 130–190.

[Shi76] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. 29 (1976), 783–804.

[Shi77] G. Shimura, *On the periods of modular forms*, Math. Ann. 229 (1977), 211–221.

[Sil94] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, 1994.

[YZZ13] X. Yuan, S. Zhang and, W. Zhang, *The Gross–Zagier Formula on Shimura Curves*, Princeton Univ. Press, 2013.

Haijun Jia
Academy of Mathematics and Systems Science
Chinese Academy of Sciences
100190, Beijing, P. R. China
E-mail: jiahaijun22@mails.ucas.ac.cn