Werk

Titel: On the Birch and Swinnerton-Dyer Conjecture.

Autor: Greenberg, Ralph

Jahr: 1983

PURL: https://resolver.sub.uni-goettingen.de/purl?356556735_0072|log16

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Invent. math. 72, 241-265 (1983)

Inventiones mathematicae
© Springer-Verlag 1983

On the Birch and Swinnerton-Dyer Conjecture

Ralph Greenberg*

Department of Mathematics, University of Washington, Seattle, Washington 98195/USA

Introduction

Let F be a finite extension of the rational field $\mathbb{Q}$. If E is an elliptic curve defined over F, then the Mordell-Weil group $E(F)$ of points on E with coordinates in F is a finitely generated abelian group. Let $L(E/F, s)$ be the Hasse-Weil zeta function of E over F which, at least in the case where E has complex multiplication, is known to be an analytic function on the entire complex plane. Birch and Swinnerton-Dyer have conjectured that $L(E/F, s)$ has a zero at $s=1$ of order precisely equal to the rank of $E(F)$ over $\mathbb{Z}$. The strongest result known in support of this conjecture is the following theorem of Coates and Wiles [4].

Theorem. *Assume E has complex multiplication by the ring of integers of an imaginary quadratic field K and that $F=\mathbb{Q}$ or K. If $E(F)$ has rank $\geqq 1$, then $L(E/F, s)$ vanishes at $s=1$.*

Generalizations of this theorem have been proved by Arthaud [1] and by Rubin [20].

In this paper, we will prove the following partial converse to the Coates-Wiles theorem.

Theorem 1. *Assume that E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by the ring of integers of an imaginary quadratic field K. If $L(E/\mathbb{Q}, s)$ has an odd order zero at $s=1$, then either $E(\mathbb{Q})$ has* rank $\geqq 1$ *or the p-primary subgroup of the Tate-Shafarevich group $Ш(E, \mathbb{Q})$ is infinite for all primes p where E has good, ordinary reduction (except possibly $p=2$ or 3).*

The function $L(E/\mathbb{Q}, s)$ can be identified with a Hecke L-series $L(\Psi, s)$, where Ψ is a certain grossencharacter of K associated with the elliptic curve E, which we define in Sect. 1. From this, one can obtain the analytic continuation and also the following functional equation:

$$\Lambda(E/\mathbb{Q}, 2-s) = w\Lambda(E/\mathbb{Q}, s),$$

* Supported in part by a National Science Foundation grant

where $\Lambda(E/\mathbb{Q}, s)=(2\pi/\sqrt{N})^{-s}\Gamma(s)\,L(E/\mathbb{Q}, s)$. Here N denotes the conductor of the elliptic curve E over $\mathbb{Q}$ and the "root number" w is ± 1. Obviously, $w=-1$ precisely when $L(E/\mathbb{Q}, s)$ has an odd order zero and so our theorem could be stated as follows: If $w=-1$, then the p^∞-Selmer group $S_{p^\infty}(E, \mathbb{Q})$ is infinite for all p where E has good, ordinary reduction ($p\neq 2, 3$). We will define the Selmer groups later, but will just mention here the fundamental exact sequence:

$$0\to E(F)\otimes_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p)\to S_{p^\infty}(E, F)\to Ш(E, F)_{p\text{-primary}}\to 0.$$

(Here E is any elliptic curve defined over a number field F. Also $\mathbb{Q}_p$ is the field of p-adic numbers, $\mathbb{Z}_p$ the p-adic integers.)

The main reason we are able to prove a result of this kind is that the odd order zero reveals itself in a rather dramatic way. To explain what we mean, let K_∞^- denote the so-called anti-cyclotomic $\mathbb{Z}_p$-extension of K. Thus, $K_\infty^- = \bigcup_{n\geq 0} K_n^-$ where K_n^- is a cyclic extension of K of degree p^n and is Galois over $\mathbb{Q}$ with a dihedral Galois group. We assume (as we almost always will throughout this paper) that E is again defined over $\mathbb{Q}$, has complex multiplication by the ring of integers $\mathcal{O}$ of the imaginary quadratic field K, and that E has good, ordinary reduction at p ($p\neq 2, 3$). Then p must split in K, $p\mathcal{O}=\mathfrak{p}\mathfrak{p}^*$. Let $\mathfrak{p}=(\pi)$, $\pi\in\mathcal{O}$. (Under our assumptions, K must have class number one.) We will prove the following theorem.

Theorem 2. *If* $w=-1$, *then* $S_{\pi^\infty}(E, K_n^-)$ *contains a subgroup isomorphic to* $(\mathbb{Q}_p/\mathbb{Z}_p)^{p^n}$ *for* $n=0, 1, 2, \ldots$.

In particular, $S_{\pi^\infty}(E, K)$ is infinite. As we will explain in section 5, this implies that $S_{p^\infty}(E, \mathbb{Q})$ is also infinite and hence theorem 1 is a consequence of theorem 2. The π^∞-Selmer groups that occur here are contained in the exact sequences:

$$0\to E(K_n^-)\otimes_{\mathcal{O}}(K_\mathfrak{p}/\mathcal{O}_\mathfrak{p})\to S_{\pi^\infty}(E, K_n^-)\to Ш(E, K_n^-)_{\pi\text{-primary}}\to 0,$$

where $K_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ denote the completions of K and $\mathcal{O}$ at $\mathfrak{p}$ (so that $K_\mathfrak{p}/\mathcal{O}_\mathfrak{p}\cong\mathbb{Q}_p/\mathbb{Z}_p$, but is also an $\mathcal{O}$-module). We have that $E(K_n^-)\otimes_{\mathcal{O}}(K_\mathfrak{p}/\mathcal{O}_\mathfrak{p})\cong(\mathbb{Q}_p/\mathbb{Z}_p)^{r_n}$, where r_n is the rank of $E(K_n^-)$ as a module over $\mathcal{O}$ (or equivalently, $r_n=\frac{1}{2}\operatorname{rank}_{\mathbb{Z}}(E(K_n^-))$). Now assume that $Ш(E, F)$ is finite (or at least its π-primary subgroup) for $F=K_n^-$, $n\geq 0$. It would then follow from Mazur's results in [17] that $r_n=ap^n+O(1)$ as $n\to\infty$ for some integer a, which from Theorem 2 must clearly be positive. We can actually prove however that $a=1$, if we make this assumption about $Ш$ for a somewhat larger collection of fields F (e.g. all subfields of $K(E_p)K_\infty^-$, where $K(E_p)$ is the field generated by points of order p on E).

The assertion that $a\geq 1$ is predicted by the Birch and Swinnerton-Dyer conjecture. The zeta function for E over K_n^- is given by $L(E/K_n^-, s)=\prod_\rho L(\Psi\rho, s)^2$, where ρ varies over all characters of $\operatorname{Gal}(K_n^-/K)$, considered (by class field theory) as Dirichlet characters for K. Now the functional equation for $L(\Psi\rho, s)$ will relate it to $L(\Psi(\bar{\rho}\circ c), s)$, where c is complex conjugation (in $\operatorname{Gal}(K/\mathbb{Q})$). But, since $\operatorname{Gal}(K_n^-/\mathbb{Q})$ is dihedral, we can see that $\bar{\rho}\circ c=\rho$. Thus the root number $w(\Psi\rho)$ will be ± 1, depending on the parity of

$\mathrm{ord}_{s=1}(L(\Psi\rho, s))$. However, as we explain in Sect. 1, $w(\Psi\rho)=w(\Psi)=w$ for all such ρ. Hence, if $w=-1$, $L(E/K_n^-, s)$ must have a zero of order at least $2p^n$ at $s=1$. Furthermore, if in fact $a=1$, then the Birch and Swinnerton-Dyer conjecture would imply that $L(\Psi\rho, s)$ has just a simple zero at $s=1$ for all but possibly finitely many complex characters ρ of $\mathrm{Gal}(K_\infty^-/K)$.

If $w=+1$, we will actually be able to prove that $L(\Psi\rho, 1)\neq 0$ for all but finitely many such ρ's. Using a theorem of K. Rubin, we can then immediately prove the following result (with the assumptions stated before Theorem 2).

Theorem 3. *If* $w=+1$, *then* $\mathrm{rank}_{\mathcal{O}}(E(K_n^-))$ *is bounded as* $n\to\infty$.

This result together with some similar but easier results concerning certain other $\mathbb{Z}_p$-extensions of K will be proved in Sect. 6. We also show that $E(K_\infty^-)$ is finitely generated as a consequence of the above result.

To prove our theorems, we consider the functions $L(\Psi^{2k+1}, s)$ for $k=0, 1, 2, \ldots$. These satisfy the functional equations:

$$\Lambda(\Psi^{2k+1}, 2k+2-s)=w_k\Lambda(\Psi^{2k+1}, s),$$

where

$$\Lambda(\Psi^{2k+1}, s)=(2\pi/\sqrt{N_k})^{-s}\Gamma(s)\,L(\Psi^{2k+1}, s).$$

Here

$$N_k=|\mathrm{disc}(K)|\,\mathcal{N}_{K/\mathbb{Q}}(f_{\Psi^{2k+1}}),$$

where $f_{\Psi^{2k+1}}$ is the conductor of the grossencharacter Ψ^{2k+1} of K. Let m denote the number of roots of unity in K. We will show that the root numbers w_k, which clearly must be ± 1, have the following properties: (i) w_k depends only on the residue class of k modulo m, and (ii) if $k_1+k_2\equiv -1 \pmod m$, then $w_{k_1}w_{k_2}=-1$. Since w_k determines the parity of the order of vanishing of $L(\Psi^{2k+1}, s)$ at $s=k+1$, we find that $L(\Psi^{2k+1}, k+1)=0$ for half of the integers $k\geqq 0$ simply because of the sign in the functional equation. Our next theorem concerns the other k's.

Theorem 4. *There are only finitely many values of* k *with* $w_k=+1$ *such that* $L(\Psi^{2k+1}, k+1)$ *vanishes.*

This result was suggested to us by some calculations of Gross and Zagier [10]. They consider the above L-values where Ψ is the grossencharacter attached to several elliptic curves with complex multiplication by the ring of integers of $K=\mathbb{Q}(\sqrt{-7})$ and for a number of values of k. They find just one zero (when $w_k=+1$), namely $L(\Psi, 1)$ for a certain elliptic curve E such that $E(\mathbb{Q})$ has rank 2. In addition, among some unpublished calculations of Swinnerton-Dyer, Nelson Stephens found two cases where $L(\Psi^3, 2)$ vanishes with $+1$ as the corresponding root number. The elliptic curves were defined by $y^2=x^3-Dx$ for $D=2\cdot 73^2$ and 79^3, which have complex multiplication by $\mathbb{Z}[i]$. It would be very interesting to understand the meaning of such zeros, even conjecturally.

A crucial role in the proof of Theorem 4 is played by the two-variable p-adic L-functions constructed by Katz in [13] and by Manin and Vishik in [15]. The L-values being considered are essentially the values of the one-variable p-adic L-functions obtained by specializing Katz's functions to a

certain "critical line". Theorem 4 is equivalent to the non-triviality of one of these specializations and this in turn implies that only finitely many of the $L(\Psi\rho, 1)$'s mentioned above can vanish when $w(\Psi)=+1$. As for the proof of Theorem 2, we will just say here that it involves a more subtle use of Theorem 4 together with a recent theorem of Yager [28] which gives an interpretation of the two-variable p-adic L-functions in terms of a certain Iwasawa module constructed from elliptic units.

The conclusion of Theorem 1 is undoubtedly true even when $L(E/\mathbb{Q}, s)$ has an even order zero at $s=1$. Although our approach here hasn't provided a proof, we will have some remarks to make about this case later. One can go further in other directions though. We can prove a more general nonvanishing result by the method used in proving Theorem 4. As a consequence, we can show that $\text{rank}_{\mathbb{Z}}(E(K_n^-))$ will be bounded as $n\to\infty$, if E is any elliptic curve defined over K (and with complex multiplication by $\mathcal{O}$) but not isomorphic over K to an elliptic curve defined over $\mathbb{Q}$. We also want to remark that our results are valid for elliptic curves defined over $\mathbb{Q}$ with complex multiplication by a non-maximal order in K, because such elliptic curves are known to be $\mathbb{Q}$-isogenous to ones with $\mathcal{O}$ as an endomorphism ring.

In a subsequent paper [9], we will study a certain new type of root number, defined purely algebraically, and its relationship to the root number of complex L-functions. This topic is closely related and in fact led us to the results in this paper. The algebraic root number, although defined as the sign in a certain functional equation for a characteristic power series, turns out to be $(-1)^e$ where e is the power to which the critical divisor Θ defined in Sect. 2 divides this characteristic power series.

In conclusion, we want to thank Barry Mazur and Dick Gross for some very helpful discussions concerning the topics in this paper.

1. *L*-functions and Root Numbers

Let E be an elliptic curve defined over $\mathbb{Q}$. If E has good reduction at a prime l, the reduced elliptic curve has a zeta function of the form

$$\frac{P_l(t)}{(1-t)(1-lt)},$$

where $P_l(t)=(1-\alpha_l t)(1-\bar{\alpha}_l t)$ has integral coefficients and complex conjugate roots such that $\alpha_l\bar{\alpha}_l=l$. The zeta function of E over $\mathbb{Q}$ is defined by an Euler product $L(E/\mathbb{Q}, s)=\prod_l P_l(l^{-s})^{-1}$ for $\text{Re}(s)>\frac{3}{2}$, where the polynomials $P_l(t)$ are defined as in Tate [25'] when E has bad reduction at l. Assume that E has complex multiplication by the ring of integers $\mathcal{O}$ of the imaginary quadratic field K. If E has good, ordinary reduction at l, then l splits in K. In this case, α_l and $\bar{\alpha}_l$ are in $\mathcal{O}$ and generate the prime ideals of $\mathcal{O}$ dividing l: $\mathfrak{l}=(\alpha_l)$, $\bar{\mathfrak{l}}=(\bar{\alpha}_l)$, $\mathfrak{l}\bar{\mathfrak{l}}=l\mathcal{O}$. We define $\Psi(\mathfrak{l})=\alpha_l$ and $\Psi(\bar{\mathfrak{l}})=\bar{\alpha}_l$. If E has good, supersingular reduction at l, then l remains prime in K, and $P_l(t)=1+lt^2$. We define $\Psi(\mathfrak{l})=-l$ for $\mathfrak{l}=l\mathcal{O}$. If E has bad reduction at l, then it must be of additive type (integrality of

the j-invariant of E) and so $P_{\mathfrak{l}}(t)=1$. Define $\Psi(\mathfrak{l})=0$ for any prime ideal $\mathfrak{l}$ dividing such l. We can then define $\Psi(\mathfrak{a})$ for any ideal $\mathfrak{a}$ of $\mathcal{O}$ so that Ψ is multiplicative. Clearly, with these definitions,

$$L(E/\mathbb{Q}, s)=\prod_{\mathfrak{l}}(1-\Psi(\mathfrak{l})\,\mathcal{N}(\mathfrak{l})^{-s})^{-1}=\sum_{\mathfrak{a}}\Psi(\mathfrak{a})\,\mathcal{N}(\mathfrak{a})^{-s}=L(\Psi, s)$$

for $\mathrm{Re}(s)>\frac{3}{2}$.

It is known that Ψ is a grossencharacter of type A_0 for K (Deuring [6]) of infinity type $(1,0)$. In general, a multiplicative complex-valued function $\mathscr{C}$ on the ideals of K is a grossencharacter of type A_0 with infinity type (a,b) if there is an ideal $f_{\mathscr{C}}$, the conductor of $\mathscr{C}$, such that $\mathscr{C}(\alpha\mathcal{O})=\alpha^a\bar{\alpha}^b$ for all $\alpha\in\mathcal{O}$ such that $\alpha\equiv 1\,(\mathrm{mod}\, f_{\mathscr{C}})$, where $a, b\in\mathbb{Z}$. There is a standard way (which is described in Weil [26] and which we will take for granted in what follows) to associate with such $\mathscr{C}$ a continuous character $\mathscr{C}\colon I_K\to\mathbb{C}$, where I_K denotes the idele group for K, such that $\mathscr{C}$ is trivial on the principal ideles $K^x\subseteq I_K$. No confusion should result from using the same letter $\mathscr{C}$. In fact, it is for such continuous idele class group characters $\mathscr{C}$ that one can attach an L-function $L(\mathscr{C}, s)$ which can be analytically continued and satisfies a functional equation (see Tate [25], for example). If $\mathscr{C}$ is of type A_0 and has infinity type (a,b), then the functional equation will relate $L(\mathscr{C}, s)$ to $L(\bar{\mathscr{C}}, d-s)$, where $d=a+b+1$. However, since complex conjugation c simply permutes the ideals of $\mathcal{O}$, $L(\bar{\mathscr{C}}, s)$ is identical to $L(\bar{\mathscr{C}}\circ c, s)$ and, if $\bar{\mathscr{C}}\circ c=\mathscr{C}$, the functional equation relates the function $L(\mathscr{C}, s)$ to itself and the root number $w(\mathscr{C})$ that occurs in this functional equation must be ± 1. Our definition of Ψ makes it clear that $\bar{\Psi}(\bar{\mathfrak{a}})=\Psi(\mathfrak{a})$ for all ideals $\mathfrak{a}$ of $\mathcal{O}$ and so Ψ and its powers have the property just mentioned. As in the introduction, let $w_k=w(\Psi^{2k+1})$ for $k=0, 1, 2, \ldots$. We should say here that we will only consider primitive grossencharacters. Thus, for example, Ψ^t is the primitive grossencharacter of K such that $\Psi^t(\mathfrak{a})=\Psi(\mathfrak{a})^t$ for all $\mathfrak{a}$ prime to f_Ψ, where $t\in\mathbb{Z}$.

The proof of the following proposition was essentially shown to us by B. Gross. A special case is mentioned in [10].

Proposition 1. *Let m denote the number of roots of unity of K. Then w_k depends only on the residue class of k modulo m. Also, if $k_1+k_2\equiv -1\,(\mathrm{mod}\, m)$, then $w_{k_1}w_{k_2}=-1$.*

Proof. The crucial observation is that, since $\Psi(\mathfrak{a})$ is in K for all ideals, Ψ^m is precisely the grossencharacter of K defined by $\mathfrak{a}=\alpha\mathcal{O}\to\alpha^m$ for any $\alpha\in\mathcal{O}$, which has trivial conductor. If $\mathscr{C}$ is a continuous idele class character, let $\mathscr{C}_{v_\infty}$ be its component at the infinite prime v_∞, a character of $\mathbb{C}^x$ of the form $z\to z^n|z|^{s_0}$ for some $n=n(\mathscr{C})\in\mathbb{Z}$, $s_0\in\mathbb{C}$. We will also need the following useful fact (which can be found in Weil [27], page 161): Assume $\mathscr{C}$ and $\mathscr{C}'$ are idele class characters of absolute value 1 and relatively prime conductors such that $n(\mathscr{C})\,n(\mathscr{C}')\geqq 0$. Then

$$w(\mathscr{C}\mathscr{C}')=w(\mathscr{C})\,w(\mathscr{C}')\,\mathscr{C}(f_{\mathscr{C}'})\,\mathscr{C}'(f_{\mathscr{C}}). \tag{1}$$

If $j\equiv k\,(\mathrm{mod}\, m)$, $j\geqq k\geqq 0$, then $\Psi^{2j+1}=\Psi^{2k+1}\Psi^{tm}$ for some even integer $t\geqq 0$. Let $\mathscr{C}=\Psi^{2k+1}/|\Psi^{2k+1}|$ and $\mathscr{C}'=\Psi^{tm}/|\Psi^{tm}|$, where $|\Psi^v|(\mathfrak{a})=\mathcal{N}(\mathfrak{a})^{v/2}$ on ideals.

Then $w(\mathscr{C})=w(\Psi^{2k+1})=w_k$ and $\mathscr{C}(f_{\mathscr{C}'})=\mathscr{C}(\mathcal{O})=1$. To compute $w(\mathscr{C}')$, we write $\mathscr{C}'=\prod_v \mathscr{C}'_v$ as a product of local characters so that, as in Tate [25], $w(\mathscr{C}')$ equals the product of local root numbers $\prod_v w(\mathscr{C}'_v)$, the product running over all primes of K, finite and infinite. The formulas for these local root numbers are given in [25]. We have $w(\mathscr{C}'_{v_\infty})=(-i)^{tm}$ since $|n(\mathscr{C}')|=tm$. Also, let v_0 be the unique ramified prime in $K/\mathbb{Q}$. (Recall that K has class number 1.) Then $w(\mathscr{C}'_{v_0})=\mathscr{C}'_{v_0}(\delta_{v_0})$, where δ_{v_0} is a generator of the local different. If δ_K is the global different (an ideal), then $\mathscr{C}'(\delta_K)=\mathscr{C}'_{v_0}(\delta_{v_0})$. In all cases, δ_K has a generator δ such that $\delta/|\delta|=i$ and hence $\mathscr{C}'(\delta_K)=i^{tm}$. If v is a prime of K, $v\neq v_\infty$ or v_0, then $w(\mathscr{C}'_v)=1$. It follows that $w(\mathscr{C}')=1$ for any integer t. In order to compute $\mathscr{C}'(f_{\mathscr{C}})$, we observe that $\bar{f}_{\mathscr{C}}=f_{\mathscr{C}}$ since $\bar{\mathscr{C}}\circ c=\mathscr{C}$ and so $f_{\mathscr{C}}=\pi_{v_0}^e a\mathcal{O}$, where π_{v_0} is a generator of the ramified prime of K, $e\geqq 0$, and a is a rational integer prime to disc (K). We have $\mathscr{C}'(a\mathcal{O})=1$ obviously and so $\mathscr{C}'(f_{\mathscr{C}})=\mathscr{C}'(\pi_{v_0}\mathcal{O})=(\pi_{v_0}/|\pi_{v_0}|)^{tme}$. If $K\neq\mathbb{Q}(i)$, then π_{v_0} can be chosen so that $\pi_{v_0}/|\pi_{v_0}|=i$. If $K=\mathbb{Q}(i)$, we can take $\pi_{v_0}=1+i$ and we have $\pi_{v_0}/|\pi_{v_0}|=\eta$, where η is an 8-th root of unity. Now since $n(\mathscr{C})\,n(\mathscr{C}')\geqq 0$, we can apply (1) and we clearly get that $w(\Psi^{2j+1})=w(\Psi^{2k+1})$.

One can prove the remaining part of Proposition 1 in the cases where $m=2$ from the above discussion. The only additional result one needs is that e is odd in these cases. In fact, it is not too difficult to show that $e=1$ except when $K=\mathbb{Q}(\sqrt{-2})$ in which case $e=5$. It follows that $w_k=w_0(-1)^k$, which is the content of Proposition 1 when $m=2$. If $m>2$, e can be even or odd.

We could settle the general case by using a slightly stronger version of (1). However, we prefer to proceed as follows. Let $\mathscr{C}_1=\Psi^{2k_1+1}/|\Psi^{2k_1+1}|$ and $\mathscr{C}_2=\Psi^{2k_2+1}/|\Psi^{2k_2+1}|$ so that $\mathscr{C}=\mathscr{C}_1\mathscr{C}_2=\Psi^{2mt}/|\Psi^{2mt}|$ for some t. Then $w(\mathscr{C}_{1,v_\infty})=(-i)^{2k_1+1}$, $w(\mathscr{C}_{2,v_\infty})=(-i)^{2k_2+1}$ and the product of these local root numbers is $+1$. Now let v be any finite prime. For brevity, let $\theta_1=\mathscr{C}_{1,v}$, $\theta_2=\mathscr{C}_{2,v}$, and $\theta=\theta_1\theta_2=\mathscr{C}_v$, an unramified character of the completion $K_v^\times$. Proposition 2.2 of [16] states that $w(\theta_1)\,w(\theta_1^{-1})=\theta_1(-1)$, essentially just the well-known fact about the product of Gaussian sums for θ_1 and θ_1^{-1}. Furthermore, $w(\theta_1^{-1})=w(\theta_2\theta^{-1})=w(\theta_2)\,\theta^{-1}(c_v)$, where c_v is a generator of $\delta_{K_v}f(\theta_2)$, δ_{K_v} is the local different, and $f(\theta_2)$ is the conductor of θ_2. This follows easily from the definition of local root numbers in [16], pages 29, 32 and the fact that θ^{-1} is unramified. (This is essentially the local version of (1) and can be used to prove it. See also [25″].) Thus $w(\theta_1)\,w(\theta_2)=\theta_1(-1)\,\theta(c_v)$. Now $\theta=\mathscr{C}_v$ and $\prod_{\substack{\text{finite}\\ v}}\mathscr{C}_v(c_v)=\mathscr{C}(\delta_K f_{\mathscr{C}_2})$ which is easily verified to be $+1$ because $\delta_K f_{\mathscr{C}_2}=\pi_{v_0}^b a\mathcal{O}$ for some $b, a\in\mathbb{Z}$ and one can argue as before. Also, $\theta_1=\mathscr{C}_{1,v}$ and, viewing $\mathscr{C}_1$ as a character of the idele group I_K,

$$\mathscr{C}_1(-1)=+1=\mathscr{C}_{1,v_\infty}(-1)\prod_{\substack{\text{finite}\\ v}}\mathscr{C}_{1,v}(-1).$$

From all of this we get that

$$w_{k_1}w_{k_2}=\prod_{\substack{\text{finite}\\ v}} w(\mathscr{C}_{1,v})\,w(\mathscr{C}_{2,v})=\mathscr{C}_{1,v_\infty}(-1)^{-1}=(-1)^{2k_1+1}=-1,$$

proving Proposition 1.

It will be useful to know how the N_k's vary. If v is any finite prime, let β_v denote the restriction of Ψ_v to the units in K_v. For any integer t, the conductor of Ψ^t is determined in a well-known way by the kernels of the β_v^t's. (See [16].) Since Ψ^m is unramified, β_v has order dividing m. If $m=2$ or 4, this shows that $f_{\Psi^{2k+1}}$ is independent of k and hence $N_k=N$ for all k. Therefore, in this case $\Psi^{2k+1}(\mathfrak{a})=\Psi(\mathfrak{a})^{2k+1}$ for all ideals $\mathfrak{a}$ of $\mathcal{O}$. If $K=\mathbb{Q}(\sqrt{-3})$, N_k can vary (which will cause some difficulty in our proof of Theorem 4), but clearly N_k depends only on k modulo m (allowing us to overcome the difficulty). We will also need the fact that $f_{\Psi^{2k+1}}$ is always divisible by the ramified prime of K. It is enough to show that $\Psi_{v_0}(-1)=-1$. Then $\beta_{v_0}^{2k+1}$ will be nontrivial. Let $\alpha=(\alpha_v)\in I_K$ be such that $\alpha_v=-1$ for all $v\neq v_0, v_\infty$ and $\alpha_{v_0}=\alpha_{v_\infty}=1$. It is easy to verify that there exists a $\gamma=(\gamma_v)\in I_K$ such that $\gamma c(\gamma)=\alpha$. We can assume γ_v is a unit for all finite v and $\gamma_{v_\infty}=1$. Now, as a character of I_K, Ψ still has the properties $\overline{\Psi}=\Psi\circ c$, $\Psi\overline{\Psi}=\mathcal{N}$ and so $\Psi(\alpha)=\Psi(\gamma)\,\overline{\Psi}(\gamma)=\mathcal{N}(\gamma)=1$. This implies that $\Psi_{v_\infty}(-1)\,\Psi_{v_0}(-1)=1$. Since $\Psi_{v_\infty}(-1)=-1$, we're done.

We want to now explain the remarks we made in the introduction about $w(\Psi\rho)$, where ρ is a Dirichlet character for K which corresponds by class field theory to a character of $\mathrm{Gal}(K_n^-/K)$. Here K_n^- is the n-th layer of the anticyclotomic $\mathbb{Z}_p$-extension of K for any prime p at which E has good, ordinary reduction. The conductor of ρ involves only the primes dividing p and so is certainly relatively prime to f_Ψ. We can use formula (1). First we observe that $L(\rho,s)=L(\rho^*,s)$, where ρ^* is the two-dimensional Artin character of $\mathrm{Gal}(K_n^-/\mathbb{Q})$ obtained by induction. Since this Galois group is dihedral, it is well-known that $w(\rho^*)=w(\rho)$ must be $+1$ (see [7]). Next since $\rho\circ c=\rho^{-1}$, we have $f_\rho=\bar{f}_\rho$ and so $f_\rho=(\mathfrak{p}\bar{\mathfrak{p}})^e$, where $\mathfrak{p}$, $\bar{\mathfrak{p}}$ are the two primes of K dividing p and $e\geqq 0$. Hence $\Psi(f_\rho)=(\Psi(\mathfrak{p})\,\Psi(\bar{\mathfrak{p}}))^e=(\Psi(\mathfrak{p})\,\overline{\Psi}(\mathfrak{p}))^e=p^e=|\Psi(f_\rho)|$. Finally, $\bar{f}_\Psi=f_\Psi$ and therefore $\rho(f_\Psi)=\rho(\bar{f}_\Psi)=\rho^{-1}(f_\Psi)$. But since ρ has p-power roots of unity as values, $\rho(f_\Psi)=1$ if p is odd. For $p=2$, a slightly more careful argument would show this. Hence (1) implies that $w(\Psi\rho)=w(\Psi)$ for such ρ.

It is interesting to notice what happens if E has good, supersingular reduction at p instead. Assume ρ has order p^n with $n\geqq 1$, p odd. One can verify that $f_\rho=p^{n+1}\mathcal{O}$. We then have $\Psi(f_\rho)=(-1)^{n+1}p^{n+1}=(-1)^{n+1}|\Psi(f_\rho)|$ and hence we get $w(\Psi\rho)=(-1)^{n+1}w(\Psi)$. The Birch and Swinnerton-Dyer conjecture implies that new points of infinite order appear in every other layer of the anticylotomic $\mathbb{Z}_p$-extension of K!

As a final remark in this section, we want to point out a similarity between the $L(\Psi\rho,1)$'s and the values $L(\Psi^{2k+1},k+1)$ discussed earlier. Namely, we can write $L(\Psi^{2k+1},k+1)$ as $L(\Psi^{2k+1}\mathcal{N}^{-k},1)$, where $\mathcal{N}$ is the norm grossencharacter of K. Since $\mathcal{N}=\Psi\overline{\Psi}$, we have $\Psi^{2k+1}\mathcal{N}^{-k}=\Psi\Phi^k$, where $\Phi=\Psi/\overline{\Psi}$. Note that $\Phi\circ c=\Phi^{-1}$ and similarly for all powers of Φ. Of course, the characters ρ of $\mathrm{Gal}(K_\infty^-/K)$ have the same property, as we've mentioned before.

2. Various Galois Groups and Modules

Let $\mathcal{F}_\infty=K(E_{p^\infty})$, the field generated by all p-power division points on E. Here E is defined over $\mathbb{Q}$ and $\mathrm{End}_K(E)=\mathcal{O}$, as before. Clearly, $\mathcal{F}_\infty$ is Galois over $\mathbb{Q}$.

The action of $G=\mathrm{Gal}(\mathcal{F}_\infty/K)$ on the Tate module for E gives an isomorphism $\imath$ of G into $(\mathcal{O}\otimes_{\mathbf{Z}}\mathbf{Z}_p)^\times=\mathcal{O}_p^\times$, say. Hence G is abelian. Therefore, complex conjugation c (in $\mathrm{Gal}(K/\mathbf{Q})$) induces a natural involution on G: $g\to c(g)$. There is also a natural action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathcal{O}_p$ and it is easy to verify that $\imath$ is a $\mathrm{Gal}(K/\mathbf{Q})$-homomorphism. It is also not difficult to see that the image of $\imath$ is of finite index in $\mathcal{O}_p^\times$. Hence $\mathcal{F}_\infty$ has a subfield $\mathcal{K}_\infty$ such that $\Gamma=\mathrm{Gal}(\mathcal{K}_\infty/K)\cong\mathbf{Z}_p^2$. In fact, $\mathcal{K}_\infty$ is just the composite of all $\mathbf{Z}_p$-extensions of K. Moreover, taking into account the action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathcal{O}_p^\times$, we find that, for odd p, $\Gamma=\Gamma^+\times\Gamma^-$, where $\Gamma^+\cong\Gamma^-\cong\mathbf{Z}_p$ and c acts on Γ^+ and Γ^- by $+1$ and -1 respectively. Corresponding to this decomposition of Γ, we have $\mathcal{K}_\infty=K_\infty^+K_\infty^-$, where K_∞^+ is the cyclotomic $\mathbf{Z}_p$-extension of K, K_∞^- the anti-cyclotomic $\mathbf{Z}_p$-extension mentioned in the introduction. Fix a choice of topological generators σ (for Γ^+) and τ (for Γ^-).

Now assume from here on that p is odd, that $p\nmid N$, and that p splits in K: $p\mathcal{O}=\mathfrak{p}\mathfrak{p}^*$. The fields $K(E_\mathfrak{p})$, $K(E_{\mathfrak{p}^*})$ generated by the $\mathfrak{p}$ and $\mathfrak{p}^*$ division points on E are subfields of $\mathcal{F}_\infty$. As explained in [4], $\mathrm{Gal}(K(E_\mathfrak{p})/K)\cong(\mathbf{Z}/(p))^\times$ and also $\mathfrak{p}$ is totally ramified in this extension. Since E has good reduction at p, we also have that $\mathfrak{p}^*$ is unramified in $K(E_\mathfrak{p})/K$. Similar remarks apply to $K(E_{\mathfrak{p}^*})/K$. Thus $K(E_\mathfrak{p})\cap K(E_{\mathfrak{p}^*})=K$, $K(E_\mathfrak{p})K(E_{\mathfrak{p}^*})=K(E_p)$, and $\Delta=\mathrm{Gal}(K(E_p)/K)\cong(\mathbf{Z}/(p))^\times\times(\mathbf{Z}/(p))^\times$. Since $|\Delta|=(p-1)^2=|\mathrm{tors}(\mathcal{O}_p^\times)|$, we see that $G\cong\Delta\times\Gamma$, where Δ is identified with $\mathrm{Gal}(\mathcal{F}_\infty/\mathcal{K}_\infty)$ and Γ with $\mathrm{Gal}(\mathcal{F}_\infty/K(E_p))$. It should also be clear that the involution c acts on Δ by simply interchanging two copies of $(\mathbf{Z}/(p))^\times$, i.e. $\Delta\cong\mathbf{Z}/(p-1)[\mathrm{Gal}(K/\mathbf{Q})]$.

There are two other subfields of $K(E_p)$ which we want to mention. One is $K(\mu_p)$, generated by the p-th roots of unity. We have $\mathrm{Gal}(K(\mu_p)/K)\cong(\mathbf{Z}/(p))^\times$. Note that $K(\mu_{p^\infty})=K(\mu_p)K_\infty^+$ which has its Galois group over K isomorphic to $\mathbf{Z}_p^\times$. Also, let F_0^- denote the subfield of $K(E_p)$ fixed by Δ^{1+c} so that $\Delta^-=\mathrm{Gal}(F_0^-/K)\cong\Delta/\Delta^{1+c}\cong(\mathbf{Z}/(p))^\times$ too. Later, we will consider the field $F_\infty^-=F_0^-K_\infty^-$. Note that $\mathrm{Gal}(F_\infty^-/K)\cong\mathbf{Z}_p^\times$.

Let ψ and ψ^* denote the characters of Δ with values in $\mathbf{Z}_p^\times$ which give the action of Δ on $E_\mathfrak{p}$ and $E_{\mathfrak{p}^*}$ respectively. Because E is defined over $\mathbf{Q}$ and complex conjugation maps $E_\mathfrak{p}$ to $E_{\mathfrak{p}^*}$, one can verify that $\psi^*=\psi\circ c$. Our remarks about Δ show that all the characters of Δ with values in $\mathbf{Z}_p^\times$ are of the form $\psi^a(\psi^*)^b$, $0\leqq a,b\leqq p-2$. Among these are $\omega=\psi\psi^*$, the determinant of the action of Δ on E_p (which of course is exactly the character giving the action of Δ on μ_p), and also $\phi=\psi/\psi^*$. This last character ϕ gives an isomorphism of $\mathrm{Gal}(F_0^-/K)$ to the $(p-1)st$ roots of unity in $\mathbf{Z}_p^\times$. We will be especially interested in the characters χ of Δ with the property that $\chi(\chi\circ c)=\omega$; they are all of the form $\psi\phi^k$, $0\leqq k\leqq p-2$.

Weil describes in [26] a way of forming a continuous Ω_p-valued character of $\mathrm{Gal}(\bar{K}/K)$ from any grossencharacter of type A_0 for K, given a fixed embedding of $\bar{\mathbf{Q}}$ into Ω_p. Here Ω_p denotes the completion of an algebraic closure of the p-adic numbers $\mathbf{Q}_p$. Fix such an embedding $\sigma_\mathfrak{p}$ so that it induces the $\mathfrak{p}$-adic valuation on K. In what follows, we will take for granted Weil's procedure and usually use the same notation for the grossencharacter and the Galois character. The simplest case is the norm grossencharacter $\mathcal{N}$ of K which, as a Galois character, gives the action on μ_{p^∞}. It factors through

$\mathrm{Gal}(K(\mu_{p^\infty})/K)$, giving a canonical isomorphism of this Galois group to $\mathbb{Z}_p^\times$. Since $\mu_{p^\infty} \subset \mathcal{F}_\infty$, we can regard $\mathcal{N}$ as a character of G.

If $\mathfrak{l}$ is any prime ideal of K not dividing N or p, then $\mathfrak{l}$ is unramified in $\mathcal{F}_\infty/K$ (by [23]) and Frob $(\mathfrak{l})$ (in G) acts on the $\mathfrak{p}$-power division points simply as multiplication by $\Psi(\mathfrak{l}) \in \mathcal{O}$, where Ψ is the grossencharacter attached to E. Furthermore, the action of $\mathcal{O}$ on $E_{\mathfrak{p}^\infty}$ obviously gives the isomorphism $\sigma_\mathfrak{p}: \mathcal{O} \to \mathbb{Z}_p$. Thus, the character of $\mathrm{Gal}(\bar{K}/K)$ obtained from Ψ (via $\sigma_\mathfrak{p}$) is just the character giving the Galois action on $E_{\mathfrak{p}^\infty}$ and so clearly factors through G. Hopefully, no confusion will result from letting Ψ denote this character of G also. Let Ψ^* denote the character of G giving the action on $E_{(\mathfrak{p}^*)^\infty}$. Then $\Psi\Psi^*$ is the determinant of the action of G on E_{p^∞} and hence must be $\mathcal{N}$. As grossencharacters of K, $\Psi\bar{\Psi} = \mathcal{N}$ and therefore Ψ^* is just the character of G obtained (via $\sigma_\mathfrak{p}$) from $\bar{\Psi}$. Also, since E is defined over $\mathbb{Q}$, we have $\Psi^* = \Psi \circ c$. The grossencharacter Φ defined at the end of Sect. 1 gives us a character $\Phi = \Psi/\Psi^*$ of G which induces an isomorphism of $\mathrm{Gal}(F_\infty^-/K)$ to $\mathbb{Z}_p^\times$.

Corresponding to the decomposition $G = \Delta \times \Gamma$, any character $\mathscr{C}$ of G can be written as a product $\mathscr{C} = \mathscr{C}_\Delta \mathscr{C}_\Gamma$ of characters of Δ and Γ. For the characters described above, we have $\Psi_\Delta = \psi$, $\Psi_\Delta^* = \psi^*$, $\mathcal{N}_\Delta = \omega$, and $\Phi_\Delta = \phi$. Also, the completed group ring $\Lambda_G = \mathbb{Z}_p[[G]]$ over $\mathbb{Z}_p$ is just $\Lambda_\Gamma[\Delta]$. Here $\Lambda_\Gamma = \mathbb{Z}_p[[\Gamma]]$ can be identified in the usual way with the power series ring $\mathbb{Z}_p[[S, T]]$, where $S = \sigma - \mathrm{id}_\Gamma$ and $T = \tau - \mathrm{id}_\Gamma$. If $\mathfrak{B}$ is any $\mathbb{Z}_p$-module on which G (or Λ_G) acts, then one can think of $\mathfrak{B}$ as a Γ (or Λ_Γ) module with a commuting action of Δ. If χ is any Ω_p-valued and therefore $\mathbb{Z}_p$-valued character of Δ, we can define a Γ (or Λ_Γ) submodule

$$\mathfrak{B}_\chi = \{b \in \mathfrak{B} \mid \delta(b) = \chi(\delta)\, b \text{ for all } \delta \in \Delta\},$$

the χ-component of $\mathfrak{B}$.

Let $\mathcal{M}_\infty$ denote the maximal abelian pro-p extension of $\mathcal{F}_\infty$ which is unramified outside the primes of $\mathcal{F}_\infty$ lying over $\mathfrak{p}$. Let $\mathfrak{X}_\infty = \mathrm{Gal}(\mathcal{M}_\infty/\mathcal{F}_\infty)$. Then $\mathfrak{X}_\infty$ is a $\mathbb{Z}_p$-module on which G acts by inner automorphisms (since $\mathcal{M}_\infty$ is clearly Galois over K). The action is $x \to gx = \bar{g}\, x\, \bar{g}^{-1}$ for $x \in \mathfrak{X}_\infty$, $g \in G$, where $\bar{g}$ is any extension of g to an automorphism of $\mathcal{M}_\infty$. Then $\mathfrak{X}_\infty$ can be considered as a Λ_G-module and turns out to be Noetherian and torsion as a Λ_Γ-module (see Coates [3]). We will denote a characteristic power series for the χ-component $(\mathfrak{X}_\infty)_\chi$, for any character χ of Δ, by $F_\chi(S, T)$, uniquely determined only up to an invertible factor in Λ_Γ.

We will also need to consider the maximal abelian pro-p-extension $\mathcal{L}_\infty$ of $\mathcal{F}_\infty$ which is unramified at all primes of $\mathcal{F}_\infty$. Then $\mathcal{L}_\infty \subseteq \mathcal{M}_\infty$ and the Λ_G-module $\mathfrak{H}_\infty = \mathrm{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty)$ is a quotient module of $\mathfrak{X}_\infty$. But $\mathcal{L}_\infty$ is actually Galois over $\mathbb{Q}$ and so we have an action of $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$ on $\mathfrak{H}_\infty$. This additional structure will be quite useful to us.

Let $\mathfrak{B}$ denote any $\mathbb{Z}_p$-module on which $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$ acts. Once and for all, choose some fixed extension of c (in $\mathrm{Gal}(K/\mathbb{Q})$) to an automorphism of $\bar{\mathbb{Q}}$ of order 2, which we also denote by c. We can regard c as an element of $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$ and so we have an involution $c: \mathfrak{B} \to \mathfrak{B}$, $b \to c(b) = cb$. If $g \in G$, $b \in \mathfrak{B}$, we have $c(gb) = c(g)\, c(b)$ as the following calculation shows: $c(gb) = cgb = cgc^{-1}cb = c(g)\, c(b)$. Let $\mathfrak{B}^c$ denote the G-module which is the same $\mathbb{Z}_p$-

module as $\mathfrak{B}$ but has a new action of G:

$$\text{new } g\,b = \text{old } c(g)\,b.$$

The mapping c then becomes a G-isomorphism $c\colon \mathfrak{B} \to \mathfrak{B}^c$. If χ is a character of Δ, we get a Γ-isomorphism $c\colon \mathfrak{B}_\chi \to (\mathfrak{B}^c)_\chi = (\mathfrak{B}_{\chi\circ c})^c$. Now assume that $\mathfrak{B}$ is a Noetherian, torsion Λ_Γ-module, and let $B_\chi(S, T)$ denote a characteristic power series for $\mathfrak{B}_\chi$. Then we have that

$$B_\chi(S, T) = B_{\chi\circ c}\left(S, -\frac{T}{1+T}\right)$$

up to an invertible factor in Λ_Γ. The reason is simply that $c(\sigma)=\sigma$, $c(\tau)=\tau^{-1}$ and so the involution c of Γ induces an involution of Λ_Γ which sends an arbitrary power series $P(S, T)$ to $P^c(S, T) = P\left(S, -\frac{T}{1+T}\right)$. These remarks apply to the characteristic power series $H_\chi(S, T)$ of the Λ_Γ-module $(\mathfrak{H}_\infty)_\chi$.

We want to define here a certain element of Λ_Γ which will play a crucial role in our later arguments. Let $\kappa = \mathcal{N}_\Gamma$, a $\mathbb{Z}_p^\times$-valued character of Γ with kernel Γ^-. Then $u = \kappa(\sigma)$ is a principal unit in $\mathbb{Z}_p$. We define

$$\Theta = \sigma - u\sigma^{-1},$$

which we will refer to as the "critical divisor". For odd p, it clearly differs by just an invertible factor in Λ_Γ from $\sigma - \sqrt{u} = S - (\sqrt{u} - 1)$, where $\sqrt{u}$ is the principal unit square root of u. Also note that $\Theta^c(S, T) = \Theta(S, T)$.

If Θ divides $H_\chi(S, T)$, then it would also divide $H_{\chi\circ c}(S, T)$. Since $H_\chi(S, T)$ divides $F_\chi(S, T)$, Θ would then divide both $F_\chi(S, T)$ and $F_{\chi\circ c}(S, T)$. For reasons that will be apparent later, we believe this cannot happen.

We now describe the kernel of the homomorphism $\mathfrak{X}_\infty \to \mathfrak{H}_\infty$. Let $\mathcal{U}_n = \prod_{v|\mathfrak{p}} U_{n,v}$, where $U_{n,v}$ is the group of principal units in the v-adic completion of $\mathcal{F}_n = K(E_{p^{n+1}})$ for $n \geqq 0$. Let E'_n be the group of global units of $\mathcal{F}_n$ which are $\equiv 1 \pmod{v}$ for all $v|\mathfrak{p}$. We can embed E'_n into $\mathcal{U}_n$ by the diagonal map. By class field theory, $\mathcal{U}_n/\bar{E}'_n$ is canonically isomorphic to the composite of inertia groups for all $v|\mathfrak{p}$ in $\mathrm{Gal}(\mathcal{M}_n/\mathcal{F}_n)$. Here $\mathcal{M}_n$ is the maximal abelian pro-p extension of $\mathcal{F}_n$ unramified outside of these v's and so $\mathcal{U}_n/\bar{E}'_n \cong \mathrm{Gal}(\mathcal{M}_n/\mathcal{L}_n)$, where $\mathcal{L}_n$ denotes the p-Hilbert class field of $\mathcal{F}_n$. Here $\bar{E}'_n$ is the closure of E'_n in $\mathcal{U}_n$. If E_n denotes the units of $\mathcal{F}_n \equiv 1 \pmod{v}$ for all v dividing p, then E_n is of prime to p index in E'_n and hence $\bar{E}_n = \bar{E}'_n$. Now we have the following commutative diagram for $m \geqq n \geqq 0$:

$$\begin{array}{ccc} \mathcal{U}_m/\bar{E}_m & \xrightarrow{\text{norm}} & \mathcal{U}_n/\bar{E}_n \\ \downarrow & & \downarrow \\ \mathrm{Gal}(\mathcal{M}_m/\mathcal{L}_m) & \xrightarrow{\text{rest.}} & \mathrm{Gal}(\mathcal{M}_n/\mathcal{L}_n). \end{array}$$

Since $\mathcal{M}_\infty = \bigcup \mathcal{M}_n$, $\mathcal{L}_\infty = \bigcup \mathcal{L}_n$ (as shown in a similar situation in [22]), we find that $\mathfrak{R}_\infty = \mathrm{Gal}(\mathcal{M}_\infty/\mathcal{L}_\infty)$ is isomorphic to $\varprojlim (\mathcal{U}_n/\bar{E}_n)$, the inverse limit defined by the norm maps. The isomorphism is compatible with the action of G and so is an isomorphism of Λ_G-modules. We have the exact sequence:

$$0 \to \mathfrak{R}_\infty \to \mathfrak{X}_\infty \to \mathfrak{H}_\infty \to 0. \tag{2}$$

The module $\mathfrak{R}_\infty$ is also related to a module considered by R. Yager in [28]. Namely, let $\mathcal{E}_n$ denote the group of elliptic units of $\mathcal{F}_n$ contained in E_n. Then $E_n/\mathcal{E}_n$ is finite. (We will say more about the definition of $\mathcal{E}_n$ in Sect. 3.) We let $\mathfrak{Y}_\infty = \varprojlim (\mathcal{U}_n/\bar{\mathcal{E}}_n)$, again defined by the norm maps. This time we have the exact sequence of Λ_G-modules

$$0 \to \mathfrak{J}_\infty \to \mathfrak{Y}_\infty \to \mathfrak{R}_\infty \to 0 \tag{3}$$

where $\mathfrak{J}_\infty = \varprojlim \bar{E}_n/\bar{\mathcal{E}}_n$. But, as we will explain, $\mathfrak{J}_\infty$ admits an action of $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$. Clearly, E_n is invariant under the action of $\mathrm{Gal}(\mathcal{F}_n/\mathbb{Q})$. So is $\mathcal{E}_n$, as we can see from the definition given in chapter 3 of [28], using the fact that the lattice L can be assumed to be invariant under complex conjugation in our case. Now, as Brumer has shown in [2],

$$\bar{E}_n \cong E_n \otimes_{\mathbb{Z}} \mathbb{Z}_p, \qquad \bar{\mathcal{E}}_n \cong \mathcal{E}_n \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

(The p-adic Leopoldt conjecture is valid for $\mathcal{F}_n$, since this field is abelian over the imaginary quadratic field K.) Hence $\bar{E}_n/\bar{\mathcal{E}}_n \cong (E_n/\mathcal{E}_n)_{p\text{-primary}}$, where the isomorphism is compatible with the action of $\mathrm{Gal}(\mathcal{F}_n/K)$. Therefore, $\mathfrak{J}_\infty$ is isomorphic to $\varprojlim (E_n/\mathcal{E}_n)_{p\text{-primary}}$ as G-modules. But the norm map $\mathcal{N}_{\mathcal{F}_m/\mathcal{F}_n}$ is compatible with the $\mathrm{Gal}(\mathcal{F}_m/\mathbb{Q})$ action on $E_m/\mathcal{E}_m$ since c simply permutes the elements of $\mathrm{Gal}(\mathcal{F}_m/\mathcal{F}_n)$ when it acts as an inner automorphism. This allows us to put a $\mathrm{Gal}(\mathcal{F}_\infty/\mathbb{Q})$ action on $\mathfrak{J}_\infty$.

For each character χ of Δ, let $G_\chi(S, T)$ denote a characteristic power series for $(\mathfrak{Y}_\infty)_\chi$, $J_\chi(S, T)$ one for $(\mathfrak{J}_\infty)_\chi$. The same considerations as before show that $J_{\chi \circ c}(S, T) = J_\chi^c(S, T)$, up to a factor in $\Lambda_\Gamma^\times$. Also $J_\chi(S, T)$ divides $G_\chi(S, T)$. We can summarize some of our observations in the following proposition.

Proposition 2. *Let Θ be the critical divisor. If Θ divides $H_\chi(S, T)$, then Θ divides both $F_\chi(S, T)$ and $F_{\chi \circ c}(S, T)$. If Θ divides $J_\chi(S, T)$ then Θ divides both $G_\chi(S, T)$ and $G_{\chi \circ c}(S, T)$.*

We will prove later (Proposition 6) that for χ of the form $\psi\phi^k$, Θ divides exactly one of the two power series $G_\chi(S, T)$ and $G_{\chi \circ c}(S, T)$, and therefore Θ cannot divide $J_\chi(S, T)$ for such χ. Note that, if $\chi = \psi\phi^{k_1}$, then $\chi \circ c = \psi^* \phi^{-k_1} = \psi\phi^{-1-k_1} = \psi\phi^{k_2}$ where $k_1 + k_2 \equiv -1 \pmod{p-1}$. If χ is not of the form $\psi\phi^k$, we can prove that Θ doesn't divide $G_\chi(S, T)$, but we will not go into this here.

3. *p*-Adic *L*-Functions and a Theorem of Yager

For primes p which split in the imaginary quadratic field K, Katz [13] has constructed a p-adic L-function $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$ defined for all continuous characters

$\mathscr{C}: G \to \Omega_p^\times$ and which takes values in Ω_p. It is constructed as an integral of $\mathscr{C}$ against a certain $\mathscr{A}$-valued measure on G, where $\mathscr{A}$ is the ring of integers in the completion of the maximal unramified extension of $\mathbb{Q}_p$. This implies that, for each (Ω_p-valued) character χ of Δ, there exists a power series $\mathscr{G}_\chi(S,T) \in \mathscr{A}[[S,T]]$ with the property that $\mathfrak{L}_\mathfrak{p}(\mathscr{C}) = \mathscr{C}_\Gamma(\mathscr{G}_\chi(S,T)) = \mathscr{G}_\chi(\mathscr{C}_\Gamma(\sigma)-1, \mathscr{C}_\Gamma(\tau)-1)$ for all $\mathscr{C}$ such that $\mathscr{C}_\Delta = \chi$. (Convergence is easily verified.) Thus $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$ is an analytic function of two p-adic variables, because if κ_1, κ_2 are two independent characters of Γ with values in $1+p\mathbb{Z}_p$, then $\mathfrak{L}_\mathfrak{p}(\kappa_1^{s_1}\kappa_2^{s_2})$ will have a power series expansion in s_1 and s_2 convergent for $|s_1|, |s_2| \leqq 1$. The power series $\mathscr{G}_\chi(S,T)$ are uniquely determined by the interpolation property satisfied by $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$, which we will now describe.

If $\mathscr{C}$ is a grossencharacter of type A_0 for K, then its values on ideals of K are in $\overline{\mathbb{Q}}$. We assume that we have chosen embeddings $\sigma_\mathfrak{p}: \overline{\mathbb{Q}} \to \Omega_p$ (which is $\mathfrak{p}$-adically continuous on K) and $\sigma_\infty: \overline{\mathbb{Q}} \to \mathbb{C}$. Then we obtain from $\mathscr{C}$ both a continuous Ω_p-valued character of $\mathrm{Gal}(\bar{K}/K)$, as we have already mentioned in Sect. 2, and a complex-valued grossencharacter. We denote both by $\mathscr{C}$. The defining property of $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$ is:

$$\sigma_\mathfrak{p}^{-1}(A_\mathfrak{p}(\mathscr{C})\,\mathfrak{L}_\mathfrak{p}(\mathscr{C})) = \sigma_\infty^{-1}(A_\infty(\mathscr{C})\,L(\mathscr{C},1))$$

for characters $\mathscr{C}$ such that $\mathscr{C}$ is of type A_0, factors through G, and has infinity type (a,b) with $a \geqq 1$, $b \leqq 0$. Here $A_\mathfrak{p}(\mathscr{C})$, $A_\infty(\mathscr{C})$ are explicitly describable quantities (in Ω_p and $\mathbb{C}$ respectively) involving p-adic and complex periods, factorials, Euler factors, etc., which make the above expressions algebraic. We only need the fact that they are non-zero. For more details, see the explicit formulas in [13], page 546. Note however that we have applied the complex functional equation to his values. Also, $L(\mathscr{C},1)$ is the complex L-function for $\mathscr{C}$ evaluated at 1 (by analytic continuation if necessary). The properties of these functions are also described in [28] and [29]. In [29], Yager gives a new construction of the power series $\mathscr{G}_\chi(S,T)$.

In particular, if $\mathscr{C} = \Psi^a(\Psi^*)^b$ with integral a, b such that $a \geqq 1$, $b \leqq 0$, then $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$ is "essentially" equal to $L(\Psi^a\overline{\Psi}^b, 1) = L(\Psi^{a-b}\mathscr{N}^b, 1) = L(\Psi^r, s)$ where $r = a-b$, $s = 1-b$ satisfy the inequalities $r \geqq 1$, $1 \leqq s \leqq r$. Damarell's theorem states that, up to a certain transcendental factor (which is part of $A_\infty(\mathscr{C})$), these L-values are algebraic [5]. For $k \geqq 0$, $L(\Psi^{2k+1}, k+1) = 0$ if and only if $\mathfrak{L}_\mathfrak{p}(\Psi\Phi^k) = 0$. This will allow us to prove the following result. We assume p is odd.

Proposition 3. *Let $0 \leqq k_0 \leqq p-2$. Then either all of the values $L(\Psi^{2k+1}, k+1)$ for $k \geqq 0$, $k \equiv k_0 \pmod{p-1}$ are zero, or only finitely many of them are zero. All will be zero if and only if the critical divisor Θ divides the power series $\mathscr{G}_{\psi\phi^{k_0}}(S,T)$.*

Proof. Up to an invertible factor in Λ_Γ, Θ is of the form $S-\alpha$ with α of absolute value <1. We can therefore write $\mathscr{G}_{\psi\phi^{k_0}}(S,T) = \mathscr{G}_{k_0}(T) + \Theta\mathscr{R}(S,T)$, where $\mathscr{G}_{k_0}(T) \in \mathscr{A}[[T]]$, $\mathscr{R}(S,T) \in \mathscr{A}[[S,T]]$. Now $\Psi^2(\sigma) = \Psi(\sigma)\Psi^*(\sigma) = \mathscr{N}(\sigma) = u$ and so $\Psi(\sigma) = \sqrt{u}$. Also, $\Phi(\sigma) = \Psi(\sigma)/\Psi^*(\sigma) = 1$. Hence $(\Psi\Phi^k)_\Gamma(\Theta) = \Psi\Phi^k(\Theta) = 0$ for all integers k. If $k \equiv k_0 \pmod{p-1}$, $(\Psi\Phi^k)_\Delta = \psi\phi^{k_0}$. It follows that

$$\mathfrak{L}_\mathfrak{p}(\Psi\Phi^k) = (\Psi\Phi^k)(\mathscr{G}_{k_0}(T)) = \mathscr{G}_{k_0}(v^{2k+1}-1)$$

where $v=\Psi(\tau)=(\Psi^*(\tau))^{-1}$. Note that v is a principal unit in $\mathbb{Z}_p$ and cannot be 1 since this would imply that τ is in the kernel of the two independent characters Ψ_Γ and Ψ_Γ^* of Γ, which is impossible. Now, by the Weierstrass Preparation Theorem (Bourbaki, Comm. Alg., Chapter 7) and the fact that p is a prime element in $\mathscr{A}$, either $\mathscr{G}_{k_0}(T)$ is the zero power series or we can write $\mathscr{G}_{k_0}(T)=p^e u(T)\mathscr{P}_{k_0}(T)$, where $e\geqq 0$, $u(T)$ is an invertible power series over $\mathscr{A}$, and $\mathscr{P}_{k_0}(T)$ is a so-called distinguished polynomial. Since a polynomial can have only finitely many zeros, we see that if $\mathfrak{L}_\mathfrak{p}(\Psi\Phi^k)=0$ for infinitely many $k\equiv k_0 \pmod{p-1}$, then $\mathscr{G}_{k_0}(T)$ is the zero power series. Proposition 3 follows.

Now if k_0 is such that $w_{k_0}=-1$, then we will have $w_k=-1$ for all $k\equiv k_0 \pmod{p-1}$, since m clearly divides $p-1$. (Recall that p is odd and splits in K.) Thus $L(\Psi^{2k+1}, k+1)$ vanishes trivially for such k, and hence we have the following result.

Corollary. *Let $0\leqq k_0\leqq p-2$. Assume $w_{k_0}=-1$. Then Θ divides $\mathscr{G}_{\psi\phi^{k_0}}(S,T)$.*

We also state the following very similar proposition. Here ϕ, which was defined as a certain character of Δ with values in the $(p-1)$st roots of unity in $\mathbb{Z}_p$, will also be regarded as a complex-valued Dirichlet character for K via $\sigma_\infty\sigma_\mathfrak{p}^{-1}$.

Proposition 4. *Let $0\leqq k_0\leqq p-2$. Then either all of the values $L(\Psi\phi^{k_0}\rho,1)$ are zero or only finitely many are zero, where ρ varies over all complex-valued characters of $\mathrm{Gal}(K_\infty^-/K)$ regarded as Dirichlet characters of K. All will be zero if and only if Θ divides $\mathscr{G}_{\psi\phi^{k_0}}(S,T)$.*

Proof. The proof is virtually identical to that of the previous proposition. Considering Ψ, ϕ, and ρ as Ω_p-valued via $\sigma_\mathfrak{p}\sigma_\infty^{-1}$, we have

$$\mathfrak{L}_\mathfrak{p}(\Psi\phi^{k_0}\rho)=(\Psi\phi^{k_0}\rho)_\Gamma(\mathscr{G}_{\psi\phi^{k_0}}(S,T))=\Psi_\Gamma\rho(\mathscr{G}_{k_0}(T))=\mathscr{G}_{k_0}(\rho(\tau)v-1),$$

since $\rho(\sigma)=1$ and so, as before, $\Psi_\Gamma\rho(\Theta)=0$. Since as ρ varies, $\rho(\tau)$ takes on all p-power roots of unity as values, the proof can be finished as before.

Yager's theorem relates the module $\mathfrak{Y}_\infty$ defined in Sect. 2 to Katz's function $\mathfrak{L}_\mathfrak{p}(\mathscr{C})$. Recall that, for each character χ of Δ, $G_\chi(S,T)$ is a characteristic power series of the Λ_Γ-module $(\mathfrak{Y}_\infty)_\chi$. We assume now, as Yager does, that $p\neq 2$ or 3.

Theorem (Yager). *For each character χ of Δ, $\mathscr{G}_\chi(S,T)=u_\chi(S,T)\,G_\chi(S,T)$ where $u_\chi(S,T)$ is invertible in $\mathscr{A}[[S,T]]$. Furthermore, there is an injective Λ_Γ-homomorphism of $(\mathfrak{Y}_\infty)_\chi$ to $\Lambda_\Gamma/(G_\chi(S,T))$ such that the cokernel is a finitely generated $\mathbb{Z}_p$-module.*

Thus $(\mathfrak{Y}_\infty)_\chi$ is pseudo-isomorphic to a cyclic Λ_Γ-module. Actually, for most χ, the Λ_Γ-isomorphism in Yager's theorem is surjective. (See Chap. 10 of [28] for more details.) We also remark that the critical divisor Θ divides $\mathscr{G}_\chi(S,T)$ (over $\mathscr{A}$) if and only if Θ divides $G_\chi(S,T)$ in Λ_Γ, as is easy to show. Hence our Propositions 3 and 4 could be stated in terms of the G's, if $p\neq 3$.

Actually, the above result is exactly what is proved in [28] only when the prime-to-p part of the conductor of χ is f_Ψ, which is sufficient for proving the results described in the introduction. Yager considers the powers of Ψ and $\overline{\Psi}$

as characters defined modulo f_Ψ and so his L-values may be non-primitive. As a result, the power series constructed in [28] may be only a multiple of $\mathscr{G}_\chi(S,T)$; the quotient will be a product of Iwasawa functions constructed from the missing Euler factors. Correspondingly, the elliptic units considered in [28] are defined by evaluating certain elliptic functions (of Robert) at division points whose annihilator is divisible by f_Ψ. By including the elliptic units constructed from "non-primitive" division points also, one gets a larger group of units $\mathscr{E}_n$. This group will be of finite index in E_n and will make the above theorem valid. We are grateful to J. Coates for pointing this difference out to us and to R. Yager for explaining how to modify his arguments to prove the result stated above.

Finally, we want to mention the so-called "two-variable main conjecture".

Conjecture. *For each character χ of Δ, $F_\chi(S,T)=G_\chi(S,T)$, up to an invertible factor in Λ_Γ.*

The exact sequences (2) and (3) show that this conjecture is equivalent to the statement that $H_\chi(S,T)$ and $J_\chi(S,T)$ differ just by a factor in $\Lambda_\Gamma^\times$. For a discussion of the above conjecture and the related one-variable conjectures, see [8].

4. The Non-Vanishing Theorem

Our approach to proving Theorem 4 is to show that, for $0\leqq k_0<m$, the numbers $L_k=L(\Psi^{2k+1},k+1)$ for $k\equiv k_0 \pmod m$ have Abel mean value equal to $(1+w_{k_0})\,L(\xi,1)$, where ξ is a certain non-principal Dirichlet character. Since this is nonzero for $w_{k_0}=+1$, we will then have that $L_k\neq 0$ for infinitely many $k\equiv k_0 \pmod m$. From this, we can prove that only finitely many of these L-values will be zero by a rather novel argument using p-adic L-functions for two different primes p.

First, we need an expression for L_k by a convergent series. Now $L(\Psi^{2k+1},s)=\sum_{n=1}^{\infty} a_n n^{-s}$, where the a_n's depend on k. Let $f(z)=\sum_{n=1}^{\infty} a_n q^n$ with $q=e^{2\pi i z}$ and let $g(t)=f(it/\sqrt{N_k})=\sum_{n=1}^{\infty} a_n e^{-Ant}$, where $A=A_k=2\pi/\sqrt{N_k}$. It is known that $f(z)$ is a cusp form for $\Gamma_0(N_k)$. (See Shimura [24] and Ogg [18].) As in Ogg, we obtain:

$$\Lambda(\Psi^{2k+1},s)=\int_1^\infty (t^{s-1}\,g(t)+w_k t^{d-s-1}\,g(t)\,dt.$$

Here $d=2k+2$. For $s=k+1$, this becomes

$$A^{-(k+1)}k!\,L_k=(1+w_k)\int_1^\infty t^k g(t)\,dt=(1+w_k)\sum_{n=1}^{\infty} a_n \int_1^\infty t^k e^{-Ant}\,dt.$$

Now $\int_1^\infty t^k e^{-Ant}\,dt=(An)^{-(k+1)}\int_{An}^\infty t^k e^{-t}\,dt$ and it is easy to show that

$$\int_x^\infty t^k e^{-t}\,dt=k!\,e^{-x}\sum_{j=0}^{k}\frac{x^j}{j!}.$$

This gives us the convergent series

$$\begin{aligned} L_k &= (1+w_k)\sum_{n=1}^{\infty} a_n n^{-(k+1)} e^{-An} \sum_{j=0}^{k} \frac{(An)^j}{j!} \\ &= (1+w_k)\sum_{\mathfrak{a}} \Psi^{2k+1}(\mathfrak{a})\, \mathcal{N}(\mathfrak{a})^{-(k+1)} e^{-A\mathcal{N}(\mathfrak{a})} \sum_{j=0}^{k} \frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!} \\ &= (1+w_k)\, G_k, \end{aligned}$$

with G_k denoting the sum over all ideals $\mathfrak{a}$ of $\mathcal{O}$.

We will assume throughout most of this section that $\Psi^{2k+1}(\mathfrak{a}) = \Psi(\mathfrak{a})^{2k+1}$ for all $k \geqq 0$, which is true except possibly if $K = \mathbb{Q}(\sqrt{-3})$. We will describe later how to handle this slightly awkward case. Assume $(\mathfrak{a}, f_\Psi) = 1$. Then $\Psi^{2k+1}(\mathfrak{a})\,\mathcal{N}(\mathfrak{a})^{-(k+1)} = \overline{\Psi}(\mathfrak{a})^{-1}\,\Phi(\mathfrak{a})^k$, where $\Phi = \Psi/\overline{\Psi}$ as before. If $\mathfrak{a} = \bar{\mathfrak{a}}$, then $\mathfrak{a} = n\mathcal{O}$ for some integer $n \geqq 1$ (since, as we explained in Section 1, f_Ψ is divisible by the ramified prime in $K/\mathbb{Q}$) and we have $\Phi(\mathfrak{a}) = 1$, $\Psi(\mathfrak{a}) = \xi(n)\, n$, where ξ is the Dirichlet character with defining modulus N such that, for primes l not dividing N, $\xi(l) = +1$ if l splits in K and $\xi(l) = -1$ if l remains prime in K. Thus ξ is a (usually non-primitive) Dirichlet character for $\mathbb{Q}$ equivalent to the character associated with the extension $K/\mathbb{Q}$. If $\mathfrak{a} \neq \bar{\mathfrak{a}}$, $\Phi(\mathfrak{a})$ has absolute value 1, but cannot be equal to 1 (or even a root of unity). We can write $G_k = G_k' + G_k''$ where

$$G_k' = \sum_{n=1}^{\infty} \frac{\xi(n)}{n} e^{-An^2} \sum_{j=0}^{k} \frac{(An^2)^j}{j!} \tag{4}$$

$$G_k'' = \sum_{\mathfrak{a} \neq \bar{\mathfrak{a}}} \overline{\Psi}(\mathfrak{a})^{-1}\, \Phi(\mathfrak{a})^k\, e^{-A\mathcal{N}(\mathfrak{a})} \sum_{j=0}^{k} \frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!} \tag{5}$$

The sum for G_k'' is over ideals $\mathfrak{a}$ of $\mathcal{O}$ prime to an integer $M (= N$ in the above case).

We will study the sums G_k', G_k'' in greater generality. We let A be any positive constant, ξ any non-principal Dirichlet character for $\mathbb{Q}$, and Ψ any function defined and nonzero for all ideals $\mathfrak{a} \neq \bar{\mathfrak{a}}$ relatively prime to some fixed integer $M \geqq 1$ and having the property that $\Psi(\mathfrak{a})$ is a generator of the ideal $\mathfrak{a}$. Consider the generating functions $F'(x) = \sum_{k=0}^{\infty} G_k' x^k$ and $F''(x) = \sum_{k=0}^{\infty} G_k'' x^k$. The calculation

$$\begin{aligned} \sum_{k=0}^{\infty} \left(\sum_{\mathfrak{a}} e^{-A\mathcal{N}(\mathfrak{a})} \sum_{j=0}^{k} \frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!} \right) |x|^k &= \sum_{\mathfrak{a}} e^{-A\mathcal{N}(\mathfrak{a})} \sum_{j=0}^{\infty} \left(\frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!} \sum_{k=j}^{\infty} |x|^k \right) \\ &= \frac{1}{1-|x|} \sum_{\mathfrak{a}} e^{-A\mathcal{N}(\mathfrak{a})} \sum_{j=0}^{\infty} \frac{(A\mathcal{N}(\mathfrak{a})\,|x|)^j}{j!} \\ &= \frac{1}{1-|x|} \sum_{\mathfrak{a}} e^{-(1-|x|)\,A\mathcal{N}(\mathfrak{a})} \end{aligned}$$

shows that the series defining $F'(x)$, $F''(x)$ are absolutely convergent for $|x| < 1$ and also justifies various changes in order of summation in similar sums in the rest of our argument.

The following lemma is the heart of our proof.

Lemma. *Let ζ be an m-th root of unity. Then*

(i) $\lim_{x\to 1}(1-x)F'(x)=L(\xi,1)$

(ii) $\lim_{x\to 1}(1-x)F'(\zeta x)=0$ *if* $\zeta\neq 1$

(iii) $\lim_{x\to 1}(1-x)F''(\zeta x)=0$ *for all* ζ

Proof. The series for $L(\xi,1)$ is convergent, since ξ is non-principal. If $\sum_{n=1}^{\infty} c_n$ is any convergent series, consider

$$C(x)=\sum_{k=0}^{\infty}\left(\sum_{n=1}^{\infty} c_n e^{-An}\sum_{j=0}^{k}\frac{(An)^j}{j!}\right)x^k=\frac{1}{1-x}\sum_{n=1}^{\infty} c_n u^n$$

where $u=u(x)=e^{-A(1-x)}$. As $x\to 1$ from below, so will $u(x)$, and a well-known theorem of Abel implies that $\lim_{x\to 1}(1-x)C(x)=\sum_{n=1}^{\infty} c_n$. If ζ is a root of unity, $\zeta\neq 1$, then $|u(\zeta x)|<1$ and is bounded away from 1 as $x\to 1$ from below (through real values). This makes it clear that $\lim_{x\to 1}(1-x)C(\zeta x)=0$ for such ζ. We obtain (i) and (ii) by letting $c_n=\xi(r)r^{-1}$ if $n=r^2$, $c_n=0$ otherwise.

To prove (iii), we have for $0\leqq x<1$,

$$\begin{aligned}
F''(\zeta x)&=\sum_{k=0}^{\infty}\left(\sum_{\mathfrak{a}\neq\bar{\mathfrak{a}}}\overline{\Psi}(\mathfrak{a})^{-1}\Phi(\mathfrak{a})^k e^{-A\mathcal{N}(\mathfrak{a})}\sum_{j=0}^{k}\frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!}\right)(\zeta x)^k\\
&=\sum_{\mathfrak{a}\neq\bar{\mathfrak{a}}}\overline{\Psi}(\mathfrak{a})^{-1}e^{-A\mathcal{N}(\mathfrak{a})}\sum_{j=0}^{\infty}\frac{(A\mathcal{N}(\mathfrak{a}))^j}{j!}\sum_{k=j}^{\infty}(\Phi(\mathfrak{a})\zeta x)^k\\
&=\sum_{\mathfrak{a}\neq\bar{\mathfrak{a}}}\overline{\Psi}(\mathfrak{a})^{-1}e^{-A\mathcal{N}(\mathfrak{a})}\frac{e^{A\mathcal{N}(\mathfrak{a})\Phi(\mathfrak{a})\zeta x}}{1-\Phi(\mathfrak{a})\zeta x}\\
&=\sum_{\mathfrak{a}\neq\bar{\mathfrak{a}}}\frac{e^{-(1-\Phi(\mathfrak{a})\zeta x)A\mathcal{N}(\mathfrak{a})}}{\delta(\mathfrak{a},\zeta,x)},
\end{aligned}$$

where $\delta(\mathfrak{a},\zeta,x)=\overline{\Psi}(\mathfrak{a})-\Psi(\mathfrak{a})\zeta x$. We can write $\zeta=\eta/\bar{\eta}$ for some $\eta\in\mathcal{O}$ (by Hilbert's Theorem 90), and then

$$\delta(\mathfrak{a},\zeta,x)=\bar{\eta}^{-1}(\bar{\eta}\overline{\Psi}(\mathfrak{a})-\eta\Psi(\mathfrak{a})x)=\bar{\eta}^{-1}(\bar{\alpha}-\alpha x),$$

where $\alpha\in\mathcal{O}$, $\alpha\neq\bar{\alpha}$ (since they generate different ideals of $\mathcal{O}$). Since $|\mathrm{Im}(\bar{\alpha})|$ is bounded below for such α, we see that $|\delta(\mathfrak{a},\zeta,x)|>\delta>0$ for some fixed δ, independent of $\mathfrak{a}$ ($\neq\bar{\mathfrak{a}}$) and x ($0\leqq x<1$). As for the exponent, we have

$$\mathrm{Re}((1-\Phi(\mathfrak{a})\zeta x)A\mathcal{N}(\mathfrak{a}))=\mathrm{Re}\left(1-\frac{\alpha}{\bar{\alpha}}x\right)B\alpha\bar{\alpha}=B\,\mathrm{Re}(\alpha\bar{\alpha}-\alpha^2 x),$$

where $B=A/\eta\bar{\eta}>0$. We may write $\alpha(\in\mathcal{O})$ as $\alpha=sa+tbi$, where $s,t\in\mathbb{Z}$, and a,b are fixed nonzero real constants depending only on $\mathcal{O}$. Then

$$\mathrm{Re}(\alpha\bar{\alpha}-\alpha^2 x)=s^2a^2(1-x)+t^2b^2(1+x).$$

Thus the final series we obtained for $F''(\zeta x)$ is dominated in absolute value by

$$\frac{1}{\delta}\sum_{s=-\infty}^{+\infty}\sum_{t=-\infty}^{+\infty} e^{-Bs^2a^2(1-x)}e^{-Bt^2b^2(1+x)}$$

$$<(\text{constant})\sum_{s=0}^{+\infty} e^{-Bs^2a^2(1-x)}$$

$$<(\text{constant})\int_0^{\infty} e^{-Bs^2a^2(1-x)}\,ds=0\left(\frac{1}{\sqrt{1-x}}\right)$$

as $x\to 1$. The final statement in our lemma follows immediately.

As a consequence of the above lemma, we see that for $0\leqq k_0<m$,

$$\lim_{x\to 1}(1-x)\sum_{\substack{k=0\\ k\equiv k_0 (\mathrm{mod}\, m)}}^{\infty} G_k x^k=\frac{1}{m}L(\xi,1),$$

where $G_k=G_k'+G_k''$. Since $L(\xi,1)\neq 0$, $G_k\neq 0$ for infinitely many $k\equiv k_0 \pmod m$. This will allow us to prove the following.

Proposition 5. *Let* $0\leqq k_0<m$. *Assume* $w_{k_0}=+1$. *Then* $L(\Psi^{2k+1},k+1)\neq 0$ *for infinitely many* k's, $k\geqq 0$, $k\equiv k_0 \pmod m$.

Proof. We must just show that for an appropriate choice of A, ξ, Ψ, and M, we have $L_k=(1+w_k)G_k$. This is clear from what we said earlier if $K\neq \mathbb{Q}(\sqrt{-3})$, since N_k is independent of k. Assume $K=\mathbb{Q}(\sqrt{-3})$. If $k\not\equiv 1 \pmod 3$ (so that $2k+1,m)=1$), then we have $N_k=N$. We also have $\Psi^{2k+1}(\mathfrak{a})=\Psi(\mathfrak{a})^{2k+1}$ for all ideals $\mathfrak{a}$, where Ψ is the grossencharacter for E. If we take $M=N$ and ξ the Dirichlet character described earlier, then again $L_k=(1+w_k)G_k$ at least for $k\not\equiv 1 \pmod 3$. This leaves just $k_0=1$ and 4 to consider. We have $N_k=N_{k_0}$ if $k\equiv k_0 \pmod m$ and so we will choose $M=N_{k_0}$, $A=2\pi/\sqrt{N_{k_0}}$. For $n\in\mathbb{Z}$, we define $\xi(n)=\Psi^{2k_0+1}(n)/n^{2k_0+1}$, which must clearly be a Dirichlet character for $\mathbb{Q}$. (It is essentially the character described before but with N_{k_0} as defining modulus.) If N_{k_0} and N have the same prime factors we can choose Ψ exactly as above and will have $L_k=(1+w_k)G_k$ for $k\equiv k_0 \pmod m$. The other G_k's would not seem to be related to the L_k's necessarily. Finally, if there are primes l dividing N, but not N_{k_0}, let $\mathfrak{l}$ be a prime ideal factor of such l. Assume $\mathfrak{l}=(\beta)$. Let $\alpha\in\mathcal{O}$ be such that $(\alpha,N)=1$, $\alpha\beta\equiv 1 \pmod{f_{\Psi^{2k_0+1}}}$. Then

$$\Psi^{2k_0+1}(\alpha\beta\mathcal{O})=(\alpha\beta)^{2k_0+1}=\Psi^{2k_0+1}(\alpha\mathcal{O})\,\Psi^{2k_0+1}(\mathfrak{l}),$$

and since $\Psi^{2k_0+1}(\alpha\mathcal{O})=(\Psi(\alpha\mathcal{O}))^{2k_0+1}$, we have $\Psi^{2k_0+1}(\mathfrak{l})=\beta_0^{2k_0+1}$ for some $\beta_0\in\mathcal{O}$ generating $\mathfrak{l}$. Define $\Psi_0(\mathfrak{l})=\beta_0$ for such $\mathfrak{l}$ and, for all prime ideals $\mathfrak{l}$ dividing N_{k_0} or prime to N, define $\Psi_0(\mathfrak{l})=\Psi(\mathfrak{l})$. Define $\Psi_0(\mathfrak{a})$ for all ideals of $\mathcal{O}$ by making Ψ_0 multiplicative. Then $\Psi^{2k+1}(\mathfrak{a})=\Psi_0(\mathfrak{a})^{2k+1}$ for all $k\equiv k_0 \pmod m$. We then take Ψ equal to the function Ψ_0 (and $\Phi=\Psi_0/\overline{\Psi}_0$) in (5) for all $k\geqq 0$. For $k\equiv k_0 \pmod m$, we will have $L_k=(1+w_k)G_k$, completing the proof of Proposition 5.

Remark. It follows from what we have proved that

$$\lim_{x\to 1}(1-x)\sum_{k=0}^{\infty} L(\Psi^{2k+1},k+1)\,x^k=L(\xi,1)$$

for some Dirichlet character ξ (except possibly if $K=\mathbb{Q}(\sqrt{-3})$ in which case the limit exists but might be slightly different). Now it is undoubtedly true that $L(\Psi^{2k+1}, k+1)\geqq 0$ for all k. This would follow from the Riemann Hypothesis for $L(\Psi^{2k+1}, s)$ for example, but is probably much more approachable. A similar result is proved by Zagier and Kohnen in [14] for Dirichlet series attached to modular forms for $SL(2,\mathbb{Z})$. If this could be proved, then a standard result in summability theory (Theorem 96 in Hardy [11]) would imply that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} L(\Psi^{2k+1}, k+1)$$

exists and is the same as the above Abelian limit. One consequence would be that $L(\Psi^{2k+1}, k+1)=o(k)$ as $k\to\infty$. It would be interesting to have a more precise result. Are these L-values bounded?

Now let $0\leqq k_0<m$ be such that $w_{k_0}=+1$. By the results proved above, there exists some $k_1\equiv k_0 \pmod m$ such that $L(\Psi^{2k_1+1}, k_1+1)\neq 0$. Let p be an odd prime for which E has good reduction and which splits in K (so that $m|p-1$). Then, by Proposition 3, $L(\Psi^{2k+1}, k+1)\neq 0$ for all but possibly finitely many $k\equiv k_1 \pmod{p-1}$. Choose an odd prime q such that $q\nmid N$, q splits in K, and $(p-1, q-1)=m$. The existence of such a prime q can be proved without too much difficulty using Dirichlet's theorem on primes in arithmetic progressions. Let k_2 be any integer such that $k_2\equiv k_0 \pmod m$. By the Chinese Remainder theorem, there are infinitely many k's such that $k\equiv k_1 \pmod{p-1}$ and $k\equiv k_2 \pmod{q-1}$. Therefore, again by Proposition 3, we see that $L(\Psi^{2k+1}, k+1)\neq 0$ for all but finitely many $k\equiv k_2 \pmod{q-1}$. It clearly follows that these L-values can vanish for at most finitely many $k\equiv k_0 \pmod m$. We have proved Theorem 4 and also the following result (using Yager's theorem).

Proposition 6. *Let $0\leqq k_0\leqq p-2$, where p is a prime $(\neq 2, 3)$ for which E has good, ordinary reduction. Then Θ divides $G_{\psi\phi^{k_0}}(S, T)$ if and only if $w_{k_0}=-1$.*

5. The Selmer Group

We assume in this section that p is an odd prime for which E has good, ordinary reduction. Let F be any algebraic extension of K, not necessarily of finite degree. The Tate-Shafarevich group $Ш(E, F)$ is the subgroup of $H^1(\mathrm{Gal}(\bar{F}/F), E(\bar{F}))$ (or more briefly $H^1(F, E)$) defined by

$$Ш(E, F)=\bigcap_v \mathrm{Ker}(H^1(F, E)\to H^1(F_v, E)),$$

where the intersection is over all primes v of F and the maps between the cohomology groups are the natural restriction maps. We also define the modified Tate-Shafarevich group $Ш'(E, F)$ as above, but taking the intersection over all v not lying over p. If $\mathcal{A}$ is any $\mathcal{O}$-module and $n\geqq 1$, $\mathcal{A}_{\pi^n}$ denotes the kernel of π^n and $\mathcal{A}_{\pi^\infty}$ the π-primary submodule of $\mathcal{A}$. Then, for each $n\geqq 1$, the exact sequence of $\mathrm{Gal}(\bar{F}/F)$-modules

$$0\to E_{\pi^n}\to E(\bar{F}) \xrightarrow{\pi^n} E(\bar{F})\to 0$$

will give us an exact cohomology sequence

$$0 \to E(F)/\pi^n E(F) \to H^1(F, E_{\pi^n}) \to H^1(F, E)_{\pi^n} \to 0.$$

By taking the direct limits as $n \to \infty$, we obtain

$$0 \to E(F) \otimes_{\mathcal{O}} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to H^1(F, E_{\pi^\infty}) \to H^1(F, E)_{\pi^\infty} \to 0$$

The π^∞-Selmer group $S_{\pi^\infty}(E, F)$ is the subgroup of $H^1(F, E_{\pi^\infty})$ defined by the exact sequence

$$0 \to E(F) \otimes_{\mathcal{O}} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to S_{\pi^\infty}(E, F) \to Ш(E, F)_{\pi^\infty} \to 0.$$

We similarly define the modified Selmer group $S'_{\pi^\infty}(E, F)$ by using $Ш'$ in place of $Ш$ in this exact sequence.

We will need a number of results from Perrin-Riou [19], which we now briefly recall without proof. The references are to [19]. First of all, $S'_{\pi^\infty}(E, F) = S_{\pi^\infty}(E, F)$. If F is any subfield of $\mathcal{F}_\infty$ in which $\mathfrak{p}$ is "infinitely ramified". This condition is equivalent to saying that F contains a $\mathbb{Z}_p$-extension of K different than the unique one in which $\mathfrak{p}$ is unramified, denoted by N_∞^* in [19]. (Lemma 1.1) if F is a finite extension of K, then $S_{\pi^\infty}(E, F)$ is of finite index in $S'_{\pi^\infty}(E, F)$ (Proposition 3.1). Furthermore, the modified Selmer group behaves well Galois theoretically. Let F be a subfield of $\mathcal{F}_\infty$ and let $H = \mathrm{Gal}(\mathcal{F}_\infty/F)$. If F either contains $\mathcal{K}_\infty$ or at least a $\mathbb{Z}_p$-extension of K different than the one in which $\mathfrak{p}^*$ is unramified (denoted by N_∞ in [19]), then $S'_{\pi^\infty}(E, F) = S'_{\pi^\infty}(E, \mathcal{F}_\infty)^H$. Here the H indicates the subgroup of H-invariant elements. The isomorphism is the natural restriction map. (Proposition 1.3 together with the fact that the "prime to p" subgroup of H obviously acts well Galois theoretically.) If F is a finite extension of K, then the map $S'_{\pi^\infty}(E, F) \to S'_{\pi^\infty}(E, \mathcal{F}_\infty)^H$ has finite kernel and cokernel (Lemma 3.4).

We will also need the following result of Coates, which is derived from the Kummer theory for E corresponding to the π^∞-division points E_{π^∞}. (See [3′]. The proof is similar to the one variable version in [3].) The result is that there exists a perfect pairing of the compact G-module $\mathfrak{X}_\infty$ (defined in Sect. 2) and the discrete G-module $\mathcal{S}_\infty = S_{\pi^\infty}(E, \mathcal{F}_\infty)$

$$\mathfrak{X}_\infty \times \mathcal{S}_\infty \to E_{\pi^\infty}$$

such that

$$g(x, s) = (gx, gs) \tag{6}$$

for all $g \in G$, $x \in \mathfrak{X}_\infty$, and $s \in \mathcal{S}_\infty$. From this one gets a perfect pairing of Γ-modules

$$(\mathfrak{X}_\infty)_\chi \times (\mathcal{S}_\infty)_{\psi\chi^{-1}} \to E_{\pi^\infty}$$

for each character χ of Δ, where we recall that ψ is the character giving the action of Δ on E_π (and also on E_{π^∞} when Δ is regarded as a subgroup of G).

Before going further, we introduce the following terminology, taken from Mazur [17]. If $\mathcal{A}$ is a discrete $\mathbb{Z}_p$-module, we say $\mathcal{A}$ has $\mathbb{Z}_p$-corank r if its dual $\hat{\mathcal{A}}$ is a finitely generated $\mathbb{Z}_p$-module of rank r. This means $\mathcal{A}$ has a subgroup

of finite index isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$. If $\mathscr{A}$ is a discrete Λ_Γ-module, such that $\hat{\mathscr{A}}$ is a torsion Λ_Γ-module, we say $\mathscr{A}$ is Λ_Γ-cotorsion. If $\hat{\mathscr{A}}$ is a finitely generated Λ_Γ-module of rank r, then we refer to r as the Λ_Γ-corank of $\mathscr{A}$. We use the same terminology for Λ_1--modules.

We will consider the π^∞-Selmer group for the field $F_\infty^- = \mathscr{F}_\infty^H$, where $H = \{gc(g) | g \in G\}$, described in Sect. 2. Recall that $\mathrm{Gal}(F_\infty^-/K) \cong \Delta^- \times \Gamma^-$ and that Φ gives an isomorphism of this Galois group to $\mathbb{Z}_p^\times$. It is interesting to note that, for $m=2$, F_∞^- as well as the isomorphism Φ does not depend on the elliptic curve $E/\mathbb{Q}$. One might consider F_∞^- as an "anticyclotomic" analogue of the field $K(\mu_{p^\infty})$.

Now the Galois group $(\mathfrak{X}_\infty)_\chi$ is a Noetherian, torsion Λ_Γ-module [3]. If the critical divisor Θ divides the characteristic power series $F_\chi(S,T)$ for this module, then $(\mathfrak{X}_\infty)_\chi$ will have a quotient pseudo-isomorphic to $\bigoplus_{j=1}^{a} \Lambda_\Gamma/(\Theta^{e_j})$ with the e_j's $\geqq 1$ for some positive integer $a = a_\chi$. We would then have that $(\mathfrak{X}_\infty)_\chi/\Theta(\mathfrak{X}_\infty)_\chi$ is pseudo-isomorphic to $(\Lambda_\Gamma/(\Theta))^a$. But by (6), $(\mathfrak{X}_\infty)_\chi/\Theta(\mathfrak{X}_\infty)_\chi$ is isomorphic to $\mathrm{Hom}((\mathscr{S}_\infty)^{\Gamma^+}_{\psi\chi^{-1}}, \mathbb{Q}_p/\mathbb{Z}_p)$ as a group and so this last module is pseudo-isomorphic to $(\Lambda_\Gamma/(S))^a$. If $\chi = \psi\phi^k$, we see that $\mathrm{Hom}(S_{\pi^\infty}(E, F_\infty^-)_{\phi^{-k}}, \mathbb{Q}_p/\mathbb{Z}_p)$ is pseudo-isomorphic as a Λ_Γ--module to $\Lambda_\Gamma^a \oplus M$, where M is a torsion Λ_Γ--module and $a = a_\chi$. This clearly implies that $S_{\pi^\infty}(E, F_\infty^-)_{\phi^{-k}}$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{ap^n}$ for $n = 0, 1, 2, \ldots$, where F_n^- is the cyclic extension of K of degree $(p-1)p^n$ in F_∞^-. These arguments are reversible. We summarize in the following proposition.

Proposition 7. *Let $0 \leqq k \leqq p-2$ and let $\chi = \psi\phi^k$. Then Θ divides $F_\chi(S,T)$ if and only if $S_{\pi^\infty}(E, F_\infty^-)_{\phi^{-k}}$ has positive Λ_Γ--corank. The corank is $a = a_\chi$, as defined above. Also, $S_{\pi^\infty}(E, F_n^-)_{\phi^{-k}}$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{ap^n}$ for $n \geqq 0$.*

In particular, let $k=0$. If Θ divides $F_\psi(S,T)$, we see that $S_{\pi^\infty}(E,K)$ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^a$, $a \geqq 1$. We want to prove the same statement about $S_{p^\infty}(E,\mathbb{Q})$. Since $E_{p^\infty} = E_{\pi^\infty} \times E_{(\pi^*)^\infty}$, it is clear that

$$S_{p^\infty}(E,K) \cong S_{\pi^\infty}(E,K) \times S_{(\pi^*)^\infty}(E,K) \cong B \times B^*,$$

say. Also, since E is defined over $\mathbb{Q}$, there is a natural action of c on $H^1(K, E_{p^\infty})$ (which is defined by sending a cocycle f to f^c, where $f^c(g) = c(f(c^{-1}gc))$ for $g \in G$). Since c acting on E_{p^∞} maps E_{π^∞} isomorphically to $E_{(\pi^*)^\infty}$, it is easy to see that $f \to f^c$ gives us an isomorphism of $H^1(K, E_{\pi^\infty})$ to $H^1(K, E_{(\pi^*)^\infty})$ and also of B to B^*, $b \to c(b)$. Therefore $S_{p^\infty}(E,K)$ contains a subgroup $\{(b, c(b)) | b \in B\}$ isomorphic to B and invariant under $\mathrm{Gal}(K/\mathbb{Q})$. But, because p is odd, $S_{p^\infty}(E,\mathbb{Q}) = S_{p^\infty}(E,K)^{\mathrm{Gal}(K/\mathbb{Q})}$, and the result we want follows.

It is also worth making the following remark. Assume that $\chi = \psi\phi^k$ and that $\Psi_\Gamma(F_\chi(S,T)) = 0$. Without too much difficulty, this can be seen to imply that $(\mathfrak{X}_\infty)_\chi$ has a quotient isomorphic to $\mathbb{Z}_p$ on which Γ acts by Ψ_Γ. Then $(\mathscr{S}_\infty)_{\phi^{-k}}$ will have a subgroup isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ on which Γ acts trivially, by (6). It follows that $S_{\pi^\infty}(E, F_0^-)_{\phi^{-k}}$ is infinite. For $k=0$, we would get that $S_{p^\infty}(E,\mathbb{Q})$ is infinite.

We end this section with some remarks which would be of interest only if it turns out to be possible for an elliptic curve to have an infinite Tate-Shafarevich group. Let E be an elliptic curve defined over any number field F. It is known that $Ш(E,F)$ has only finitely many elements of order p, for any prime p, and hence the p-primary subgroup of $Ш(E,F)$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{t_p}\times$(a finite group) for some $t_p \geqq 0$. Let $r=\mathrm{rank}_{\mathbb{Z}}(E(F))$. It follows that $S_{p^\infty}(E,F)$ contains a subgroup of finite index isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{d_p}$, where $d_p=r+t_p$. It is tempting to state a variant on the conjecture of Birch and Swinnerton-Dyer (suggested by Coates): The order of vanishing of $L(E/F,s)$ at $s=1$ should be d_p. Obviously, this statement implies that d_p is independent of p, a fact which would be trivial if $Ш(E,F)$ is finite. We can give a conditional but rather convincing proof of the following result. If E is an elliptic curve defined over $F=\mathbb{Q}$ with complex multiplication and if w is the sign in the functional equation for $L(E/\mathbb{Q},s)$, then $w=(-1)^{d_p}$ for all odd primes p where E has good, ordinary reduction. Thus at least the parity of d_p (and therefore t_p) would be independent of p for these primes. We will discuss this in [9].

6. The Proof of Theorem 3

We will prove a somewhat more general result. First we recall the following theorem of Rubin [20], for an elliptic curve defined over K and with complex multiplication by $\mathcal{O}$.

Theorem. *Let M be a finite, abelian extension of K and let χ be a complex valued character of* $\mathrm{Gal}(M/K)$. *If χ occurs in the representation space $E(M)\otimes_{\mathcal{O}}\mathbb{C}$ of* $\mathrm{Gal}(M/K)$, *then $L(\overline{\Psi}\chi,1)=0$.*

We remark that, by the functional equation, $L(\overline{\Psi}\chi,1)=0$ if and only if $L(\Psi\chi^{-1},1)=0$.

In what follows, we will regard the character ϕ as either complex-valued or Ω_p-valued (via σ_∞ or $\sigma_\mathfrak{p}$). We assume that E is an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}$, and that p is an odd prime for which E has good, ordinary reduction. Let $0\leqq k_0\leqq p-2$. Denote by $T_K(\phi^{-k_0})$ the character of the irreducible representation of $\mathrm{Gal}(F_0^-/K)$ over K which has ϕ^{-k_0} as a constituent. The other constituents are ϕ^{-tk_0} where $(t,p-1)=1$ and $t\equiv 1\,(\mathrm{mod}\,m)$. (We note in passing that $w_{k_0}=w_{tk_0}$ for such t.) We have the following result which includes Theorem 3.

Proposition 8. *Assume $w_{k_0}=+1$. Considering $E(F_n^-)\otimes_{\mathcal{O}}K$ as a representation space for $\Delta^-\cong\mathrm{Gal}(F_0^-/K)$ over K, the dimension of the $T_K(\phi^{-k_0})$-component is bounded as $n\to\infty$.*

Proof. If this were false, then there would exist infinitely many n's and complex-valued characters ρ of $\mathrm{Gal}(F_n^-/K)$ of order p^n such that $\phi^{-k_0}\rho$ occurs in $E(F_n^-)\otimes_{\mathcal{O}}\mathbb{C}$. Thus, by Rubin's theorem, $L(\Psi\phi^{k_0}\rho^{-1},1)$ must vanish for infinitely many characters ρ^{-1} of $\mathrm{Gal}(K_\infty^-/K)$. By Proposition 4, this implies that Θ divides $\mathcal{G}_{\psi\phi^{k_0}}(S,T)$, now regarding ϕ as Ω_p-valued. By Proposition 6 (or at least its proof if $p=3$) this contradicts our assumption that $w_{k_0}=+1$.

One can also apply Rubin's theorem to certain other $\mathbb{Z}_p$-extensions, where the necessary non-vanishing result is more trivial. To describe what we mean let $\mathscr{E}$ denote the set of all $\mathbb{Z}_p$-extensions of K. We can identify $\mathscr{E}$ with the projective line $\mathbb{P}_1(\mathbb{Q}_p)$ in the following way. Let $\lambda=\Psi_\Gamma$, $\kappa=\mathcal{N}_\Gamma$. If $\gamma\in\mathbb{P}_1(\mathbb{Q}_p)$ is represented by (a,b) with $a,b\in\mathbb{Z}_p$, not both zero, then $\kappa^{-a}\lambda^b\colon \Gamma\to 1+p\mathbb{Z}_p$ factors through a $\mathbb{Z}_p$-extension $K_\infty^{(\gamma)}$ of K, depending just on γ. If γ is the point at ∞, $K_\infty^{(\gamma)}$ is the cyclotomic $\mathbb{Z}_p$-extension K_∞^+. Otherwise (if $b\neq 0$) we can identify γ with $a/b\in\mathbb{Q}_p$. The anti-cyclotomic $\mathbb{Z}_p$-extension corresponds to $\gamma=\frac{1}{2}$. The extensions N_∞ and N_∞^* mentioned in Sect. 5 correspond to $\gamma=0$ and 1 respectively. We have a natural topology on $\mathscr{E}$ from the identification with $\mathbb{P}_1(\mathbb{Q}_p)$. The following result concerns a certain dense subset.

Proposition 9. *Let $K_n^{(\gamma)}$ denote the n-th layer in the $\mathbb{Z}_p$-extension $K_\infty^{(\gamma)}$. Assume γ is rational, $0\leqq\gamma\leqq 1$, and $\gamma\neq\frac{1}{2}$. Then $\operatorname{rank}_{\mathcal{O}}(E(K_n^{(\gamma)}))$ is bounded as $n\to\infty$.*

Proof. If $\operatorname{rank}_{\mathcal{O}}(E(K_n^{(\gamma)}))$ were unbounded, then we would have infinitely many complex-valued characters ρ of $\operatorname{Gal}(K_\infty^{(\gamma)}/K)$ such that $L(\Psi\rho,1)=0$. Viewing these characters as Ω_p-valued (via $\sigma_{\mathfrak{p}}\sigma_\infty^{-1}$), it would follow that $\mathfrak{L}_{\mathfrak{p}}(\Psi\rho)=0$ also. Therefore $\mathfrak{L}_{\mathfrak{p}}(\Psi\mathscr{C})$ must vanish for all Ω_p-valued characters $\mathscr{C}$ of $\operatorname{Gal}(K_\infty^{(\gamma)}/K)$. If $\gamma=a/b$ with a, b nonnegative integers, put $r=1+(p-1)bt$, $s=1+(p-1)at$ for integral $t\geqq 1$. We have $\mathfrak{L}_{\mathfrak{p}}(\Psi\Psi^{(p-1)bt}\mathcal{N}^{-(p-1)at})=0$ and, since $1\leqq s\leqq r$, it follows that $L(\Psi^r,s)=0$ also. But, because $\gamma\neq\frac{1}{2}$, either r and s or r and $r+1-s$ are in the region where the Euler products for these L-functions converge. Clearly, none of these L-values are zero.

It is shown in [19] that there are only finitely many $\mathbb{Z}_p$-extensions of K in which E has unbounded rank. We would tend to believe that in fact only the anti-cyclotomic $\mathbb{Z}_p$-extensions could have this property. For the cyclotomic $\mathbb{Z}_p$-extension, Rubin and Wiles [21] have proved that the rank must be bounded for a large class of elliptic curves defined over $\mathbb{Q}$ with complex multiplication by K.

It is not difficult to deduce from the results of this section a "Mordell-Weil theorem" for certain $\mathbb{Z}_p$-extensions. For example, we can prove that if K_∞ is any $\mathbb{Z}_p$-extension of K such that $\operatorname{rank}_{\mathcal{O}}(E(K_n))$ is bounded, then $E(K_\infty)$ is finitely generated. It is enough to prove that the torsion subgroup of $E(K_\infty)$ is finite, as the following argument (taken from [17]) shows. Assume $t=|\operatorname{tors}(E(K_\infty))|$ is finite. Let n be such that E achieves its maximal rank over K_n. Thus, if $m\geqq n$, $E(K_m)/E(K_n)$ is finite. Let g be a generator of $\operatorname{Gal}(K_\infty/K_n)$. If $P\in E(K_m)$, then dP is invariant under g for some $d\geqq 1$. Thus, $d(P^g-P)=0_E$. We must have $t(P^g-P)=0_E$. This implies that $[E(K_m)\colon E(K_n)]$ is bounded as $m\to\infty$. Obviously it follows that $E(K_m)=E(K_\infty)$ if m is large enough.

We first show that the prime-to-p torsion subgroup of $E(\mathscr{F}_\infty)$ is finite. Let l be a prime, $l\neq p$. The field $K(E_{l^\infty})$ is the composite of a finite extension of K and the extension of K with Galois group $\mathbb{Z}_l^2$, in which only primes over l can ramify (see [12]). It follows easily that any infinite subgroup of E_{l^∞} generates an extension of K in which at least one prime of K dividing l must be infinitely ramified. Since l is at most finitely ramified in F_∞, we get that the l-primary subgroup of $E(\mathscr{F}_\infty)$ is finite. If $l\nmid 2N$, the l-torsion must be trivial. To see this, note that such l either split or remain prime in K (since $\operatorname{disc}(K)$

divides N). Also $E(\mathscr{F}_\infty)_l$ is an $\mathcal{O}$-submodule of E_l. If l splits as II*, then the nontrivial $\mathcal{O}$-submodules of E_l are E_{I}, E_{I^*}, and E_l itself. As mentioned earlier, $K(E_{\mathrm{I}})$ has degree $l-1$ over K and I is totally ramified. Since only primes where E has bad reduction and p can ramify in $\mathscr{F}_\infty$, it is clear that $E(\mathscr{F}_\infty)$ has no I (or I*) torsion and hence no l-torsion. If l remains prime, then E_l has no proper $\mathcal{O}$-submodules. Since $K(E_l)$ contains $K(\mu_l)$ and l is certainly ramified nontrivially in $K(\mu_l)$ for $l \nmid 2\,\mathrm{disc}(K)$, we again see that $E(\mathscr{F}_\infty)$ has no l-torsion. All of these remarks obviously justify the statement made at the beginning of this paragraph.

Finally, it is simple to show that $E(K_\infty)$ has no p-torsion. The only nontrivial $\mathcal{O}$-submodules of E_p are $E_{\mathfrak{p}}$, $E_{\mathfrak{p}^*}$, and E_p. But $K(E_{\mathfrak{p}})$ has degree $p-1$ over K and therefore cannot be contained in K_∞. Similarly for $K(E_{\mathfrak{p}^*})$. Since $E(K_\infty)$ is an $\mathcal{O}$-module, $E(K_\infty)_p$ must be trivial. Combining our observations, it should be clear that $\mathrm{tors}(E(K_\infty))$ is in fact finite.

7. Concluding Arguments

Now we can give the final steps of the proofs of Theorems 1 and 2. By Proposition 7 and the discussion after it, it will be enough to prove the following result. We must assume $p \neq 2$ or 3, as well as the other usual assumptions.

Proposition 10. *If* $w_{k_0} = -1$, *then* Θ *divides* $F_{\psi\phi^{k_0}}(S, T)$.

Proof. Let $\chi_0 = \psi\phi^{k_0}$. Choose $k_1 \geqq 0$ so that $k_0 + k_1 \equiv -1 \pmod{p-1}$. By Proposition 1, $w_{k_0} w_{k_1} = -1$ and so $w_{k_1} = +1$. If $\chi_1 = \psi\phi^{k_1}$, then Proposition 6 implies that Θ divides $G_{\chi_0}(S, T)$, but not $G_{\chi_1}(S, T)$. Since $\chi_1 = \chi_0 \circ c$, it follows from Proposition 2 that Θ cannot divide $J_{\chi_0}(S, T)$. Now the exact sequence

$$0 \to (\mathfrak{J}_\infty)_{\chi_0} \to (\mathfrak{Y}_\infty)_{\chi_0} \to (\mathfrak{R}_\infty)_{\chi_0} \to 0$$

shows that Θ must divide the characteristic power series for $(\mathfrak{R}_\infty)_{\chi_0}$. Finally, the exact sequence

$$0 \to (\mathfrak{R}_\infty)_{\chi_0} \to (\mathfrak{X}_\infty)_{\chi_0} \to (\mathfrak{H}_\infty)_{\chi_0} \to 0$$

proves that Θ divides $F_{\chi_0}(S, T)$.

Of course, it seems almost certain that Θ divides $F_{\psi\phi^k}(S, T)$ if and only if $w_k = -1$. Obviously this would be a consequence of the two-variable main conjecture stated at the end of Sect. 3. It would also be a consequence of the following hypothesis: the π-primary subgroup of $Ш(E, F_n^-)$ is finite or at least of bounded $\mathbb{Z}_p$-corank for all $n \geqq 0$. For this hypothesis together with Proposition 8 implies $S_{\pi^\infty}(E, F_n^-)_{\phi^{-k}}$ has bounded $\mathbb{Z}_p$-rank as $n \to \infty$ (or, what amounts to the same $S_{\pi^\infty}(E, F_\infty^-)_{\phi^{-k}}$ is cotorsion as a Λ_Γ-module) when $w_k = +1$. By Proposition 7, this in turn is equivalent to the assertion that, if $w_k = +1$, then $F_{\psi\phi^k}(S, T)$ is not divisible by Θ. Finally, another equivalent statement is that Θ does not divide $H_{\psi\phi^k}(S, T)$ for any k. This follows from the exact sequences (2) and (3), Propositions 2 and 6.

If one assumes any of the statements in the last paragraph, then one could determine the a_χ's referred to in Proposition 7. This is because $(\mathfrak{R}_\infty)_\chi$ is always pseudo-isomorphic to a cyclic Λ_Γ-module. We would have the result that $a_\chi = 0$ or 1 for $\chi = \psi\phi^k$ depending just on the value of w_k. These comments should explain the remarks we made in the introduction about Mazur's invariant. We can also see that, if one assumes the hypothesis about *Ш* stated above, then Mazur's invariant for the tower F_∞^-/F_0^- is exactly $(p-1)/2$.

Can one prove a result similar to Theorem 1 when $L(E/\mathbb{Q}, s)$ has an even order zero at $s=1$? We can only make the following remark. Assume $L(\Psi, 1) = 0$, but $w = +1$. Then $\Omega_\mathfrak{p}(\Psi)$ vanishes and hence the power series $G_\psi(S, T)$ will have at least one irreducible factor $P(S, T)$ in Λ_Γ such that $\Psi_\Gamma(P(S, T)) = 0$. By Proposition 6, $P(S, T)$ is distinct from Θ. It would be enough to show that $P(S, T)$ divides $F_\psi(S, T)$. For then one could use the results from Sect. 5 to prove that $S_{p^\infty}(E, \mathbb{Q})$ is infinite. If $P(S, T)$ divides the characteristic power series for $(\mathfrak{R}_\infty)_\psi$, we would clearly have what we want. If not, then $P(S, T)$ must divide $J_\psi(S, T)$. Therefore $P^c(S, T)$ would divide $J_{\psi^*}(S, T)$ and hence $G_{\psi^*}(S, T)$. Since Θ also divides $G_{\psi^*}(S, T)$, and since both Θ and $P^c(S, T)$ vanish at Ψ_Γ^*, we would find that $\Omega_\mathfrak{p}(\mathscr{C})$ has at least a second order zero at $\mathscr{C} = \Psi^*$ as an analytic function in two variables. That is, its power series expansion about Ψ^* would have to begin with at least quadratic terms. Thus we are led to a question about the behavior of $\Omega_\mathfrak{p}(\mathscr{C})$ at a grossencharacter of type A_0 outside of the range of interpolation.

References

1. Arthaud, N.: On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I. Comp. Math. **37**, 209–232 (1978)
2. Brumer, A.: On the units of algebraic number fields. Mathematika **14**, 121–124 (1967)
3. Coates, J.: Infinite descent on elliptic curves with complex multiplication. To appear in Progress in Mathematics. Boston: Birkhauser
3′. Coates, J.: Elliptic curves with complex multiplication. Hermann Weyl lectures, 1979, Annals of Math. Studies, to appear
4. Coates, J., Wiles, A.: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **39**, 223–251 (1977)
5. Damarell, R.: *L*-functions of elliptic curves with complex multiplication I. Acta Arith. **17**, 287–301 (1970)
6. Deuring, M.: Die Zetafunktionen einer algebraischen Kurve vom Geschlecht Eins I, II, III, IV. Nachr. Akad. Wiss. Göttingen, 85–94 (1953); 13–42 (1955); 37–76 (1956); 53–80 (1957)
7. Frohlich, A., Queyrut, J.: On the functional equation of the Artin *L*-function for characters of real representations. Invent. Math. **14**, 173–183 (1971)
8. Greenberg, R.: On *p*-adic *L*-functions and Iwasawa's theory for imaginary quadratic fields. Proceedings of conference on modern trends in Alg. No. theory related to Fermat's last theorem, pp. 215–286. Boston: Birkhäuser
9. Greenberg, R.: Functional equations, root numbers, and Iwasawa theory. In preparation
10. Gross, B., Zagier, D.: On the critical values of Hecke *L*-series. Soc. Math. de France, Memoire No. **2**, 49–54 (1980)
11. Hardy, G.H.: Divergent Series. Clarendon Press (1949)
12. Iwasawa, K.: On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann. of Math. **98**, 246–326 (1973)
13. Katz, N.: *p*-adic interpolation of real analytic Eisenstein series. Ann. of Math. **104**, 459–571 (1976)

14. Kohnen, W., Zagier, D.: Values of L-series of modular forms at the center of the critical strip. Invent. Math. **64**, 175–198 (1981)
15. Manin, J., Vishik, S.: p-adic Hecke series for imaginary quadratic fields. Math. Sbornik **95** (137) (1974), No. 3
16. Martinet, J.: Character theory and Artin L-functions. Alg. No. fields. (Frohlich, A. ed.). New York: Academic Press (1977)
17. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. **18**, 183–266 (1972)
18. Ogg, A.: Modular forms and dirichlet series. New York: Benjamin 1969
19. Perrin-Riou, B.: Groupe de Selmer d'une courbe elliptique a multiplication complexe. Comp. Math. **43**, 387–417 (1981)
20. Rubin, K.: Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer. Invent. Math. **64**, 455–470 (1981)
21. Rubin, K., Wiles, A.: Mordell-Weil groups of elliptic curves over cyclotomic fields. Proceedings of conference on modern trends in Alg. No. theory related to Fermat's last theorem, pp. 237–254. Boston: Birkhäuser
22. Serre, JP.: Classes de corps cyclotomique. Sem. Bourbaki **174** (1958)
23. Serre, JP., Tate, J.: Good reduction of abelian varieties. Ann. Math. **88**, 492–517 (1968)
24. Shimura, G.: On elliptic curves with complex multiplication as factors of the Jacobian of modular function fields. Nagoya Math. J. **43**, 199–208 (1971)
25. Tate, J.: Fourier analysis in number fields and Hecke's zeta functions. Alg. No. theory. (Cassels, Frohlich, eds.). London: Academic Press 305–347 (1967)
25′. Tate, J.: Arithmetic of elliptic curves. Invent. Math. **23**, 179–206 (1974)
25″. Tate, J.: Local constants. Alg. No. fields, (Frohlich, A., ed.). New York: Academic Press 1977
26. Weil, A.: On a certain type of character of the idele-class groups of an algebraic number field. Proc. Int'l. Symp. Tokyo-Nikko, 1–7 (1955)
27. Weil, A.: Dirichlet series and automorphic forms. Lecture notes in math. Vol. 189. Berlin-Heidelberg-New York: Springer 1971
28. Yager, R.: On two-variable p-adic L-functions. Ann. of Math. **115**, 411–449 (1982)
29. Yager, R.: p-adic measures on Galois groups. Preprint

Oblatum 13-IX-1982