On Kummer characters arising from Galois actions on the pro-p fundamental groups of once-punctured CM elliptic curves

Shun Ishii
ishii.shun@keio.jp

Department of Mathematics, Keio University, 3-14-1 Hiyoshi, Kouhoku-ku, Yokohama 223-8522, Japan.

Abstract

In this paper, we study certain Kummer characters arising from the pro-p geometric fundamental groups of CM elliptic curves minus their origins (*once-punctured CM elliptic curves*). They may be regarded as analogues of the Soulé characters. We study sufficient conditions under which such characters are nontrivial or even surjective.

Contents

1 Introduction

In this paper, we study certain characters arising from Galois actions on the pro-p geometric fundamental groups (i.e. the maximal pro-p quotients of the geometric étale fundamental groups) of once-punctured CM elliptic curves.

These characters may be regarded as elliptic analogues of *the Soulé characters*, which arise from Galois actions on the pro-p geometric fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\})^{(p)}$ of the thrice-punctured projective line.

In the following, we briefly recall backgrounds. Please refer to Notations for some symbols appearing this section without further explanation.

Let $(\zeta_n)_{n\geq 1}$ be a sequence primitive p^n-th root of unity in $\bar{\mathbb{Q}}$ satisfying $\zeta_{n+1}^p = \zeta_n$ for every n, i.e. a basis of $\mathbb{Z}_p(1)$. For every odd integer $m \geq 3$, *the m-th Soulé character* is a $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$-equivariant character

$$\kappa_m \colon G^{\mathrm{ab}}_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$$

whose reduction modulo p^n is, via Kummer theory, corresponds to the p^n-th root of

$$\prod_{1\leq a\leq p^n,(a,p)=1} (1-\zeta_n^a)^{a^{m-1}}$$

for every $n \geq 1$. This definition depends on the choice of $(\zeta_n)_{n\geq 1}$, but the resulting character is unique up to multiplication by elements of $\mathbb{Z}_p^\times$.

Theorem 1.1 (Fundamental properties of the Soulé characters)**.**

1. *κ_m is nontrivial for every odd $m \geq 3$.*
2. *κ_m is surjective for every odd $m equiv 1 \bmod p-1$.*
3. *κ_m are surjective for all $m \geq 3$ if and only if Vandiver's conjecture holds for p, i.e. the class number of the maximal real subfield of $\mathbb{Q}(\mu_p)$ is not divisible by p.*

For proofs, see Ichimura-Sakaguchi [IS87]. There the nontriviality of the Soulé characters are mainly resorted to the two ingredients : the one is the finiteness of $H^2_{\text{ét}}(\mathrm{Spec}(\mathbb{Z}[\frac{1}{p}]), \mathbb{Z}_p(m))$ for $m \geq 2$ proved by Soulé [Sou79, page 287, Corollaire], and the other is Iwasawa main conjecture proved by Mazur-Wiles [MW84]. As for the surjectivity, a key ingredient is a relation between the class number of $\mathbb{Q}(\mu_p)$ and the group of cyclotomic units.

Let us briefly mention a relationship between the Soulé characters and the Galois action on the fundamental group $\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0,1,\infty\})^{(p)}$. In his pioneering work [Iha86], Ihara constructed and studied a homomorphism

$$\alpha_{0,3} \colon G^{\mathrm{ab}}_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p[[T_1, T_2]]$$

called *the universal power series for Jacobi sums* in a group-theoretical way from the maximal meta-abelian quotient of $\pi_1^{\text{ét}}(\mathbb{P}^1_{\bar{\mathbb{Q}}} \setminus \{0,1,\infty\})^{(p)}$. Ihara-Kaneko-Yukinari proved that the Soulé characters appear as its coefficients.

Theorem 1.2 (Ihara-Kaneko-Yukinari [IKY87])**.**

$$\alpha_{0,3}(\sigma) = \sum_{m\geq 3\colon \mathit{odd}} \frac{\kappa_m(\sigma)}{1-p^{m-1}} \sum_{i+j=m} \frac{U_1^{m_1} U_2^{m_2}}{m_1! m_2!}.$$

holds for every $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$. Here, we regard $\mathbb{Z}_p[[T_1,T_2]]$ as a subring of $\mathbb{Q}_p[[U_1,U_2]]$ where $U_i := \log(1+T_i)$ for $i = 1,2$.

For more discussions about Galois action on the pro-p geometric fundamental group of $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$, see e.g. Ihara [Iha02].

In [Nak95], Nakamura studied Galois actions on the pro-p geometric fundamental groups $\pi_1^{\text{ét}}(E_{\bar{K}} \setminus O)^{(p)}$ of a once-punctured elliptic curve $E \setminus O$ over a number field K by constructing an analogue of Ihara's power series

$$\alpha_{1,1} \colon G^{\mathrm{ab}}_{K(E[p^\infty])} \to \mathbb{Z}_p[[T_p(E)]](1)$$

which is denoted by α in the original paper. Moreover, he found explicit Kummer characterizations of characters arising as coefficients of his power series.

To state the theorem, we fix a basis $\omega_1 = (\omega_{1,n})_{n\geq 1}$ and $\omega_2 = (\omega_{2,n})_{n\geq 1}$ of $T_p(E) = \varprojlim_n E[p^n](\bar{\mathbb{Q}})$ and identify $\mathbb{Z}_p[[T_p(E)]]$ with $\mathbb{Z}_p[[T_1, T_2]]$ via $T_i \coloneqq \omega_i - 1$ for $i = 1, 2$. Note that we use the convention $0^0 \coloneqq 1$ in the following formula.

Theorem 1.3 (Nakamura [Nak95, Theorem (A)])**.**

$$\alpha_{1,1}(\sigma) = \sum_{m\geq 2\colon \text{ even}}^{\infty} \frac{1}{1-p^m} \sum_{\substack{(m_1,m_2)\in\mathbb{Z}^2_{\geq 0}\\ m_1+m_2=m}} \kappa_{(m_1+1,m_2+1)}(\sigma) \frac{U_1^{m_1} U_2^{m_2}}{m_1! m_2!}$$

holds for every $\sigma \in G_{K(E[p^\infty])}$. Here, $\kappa_{(m_1,m_2)} \colon G^{\mathrm{ab}}_{K(E[p^\infty])} \to \mathbb{Z}_p$ is a Kummer character whose reduction modulo p^n is associated to the p^n-th root of

$$\epsilon_{(m_1,m_2),n} \coloneqq \prod_{\substack{0\leq a,b<p^n\\ p\nmid \gcd(a,b)}} \left(\prod_{k=0}^{\infty} \theta_p(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})^{-p^{2k}} \right)^{a^{m_1-1}b^{m_2-1}}$$

for every $n \geq 1$, where θ_p is a rational function on E defined in Section 2.1.

Definition 1.1 (Elliptic Soulé characters)**.** We call the character

$$\kappa_{\boldsymbol{m}} \colon G^{\mathrm{ab}}_{K(E[p^\infty])} \to \mathbb{Z}_p$$

appearing in Theorem 1.3 *the (m_1, m_2)-th elliptic Soulé character.*

As in the case of Soulé characters, these characters depend on the choice of a basis of $T_p(E)$. However, for each $m \geq 1$, the degree m-part of $\alpha_{1,1}$ defines a homomorphism from the Galois group $G_{K(E[p^\infty])}$ with value in $\mathrm{Sym}^m T_p(E)(1)$ which can be shown to be independent of the choice of the basis. Since we work with the fixed basis $\{\omega_1, \omega_2\}$, we do not mention this dependence hereafter.

Note that Theorem 1.3 is originally stated via a certain basis of $T_p(E)$ which comes from a topological one and simplify the Kummer characterization given in the theorem by using the fundamental theta function $\theta(z, \mathcal{L})$ associated to a lattice $\mathcal{L}$ for $E(\mathbb{C})$ (for more details, see the original paper [Nak95, §2]). However, the proof given in [Nak95] works for every basis.

While properties of the Soulé characters are well understood, the fundamental properties of the elliptic Soulé characters, such as the surjectivity or even

the nontriviality, are not much known. As a partial result, Nakamura [Nak95, (3.12)] observed that certain linear combinations of them are nontrivial.

In this paper, we consider the elliptic Soulé characters arising from once-punctured CM elliptic curves over imaginary quadratic fields, and study the nontriviality or the surjectivity of them.

In the rest of this paper, assume that K is an imaginary quadratic field of class number one and let (E, O) be an elliptic curve over K which has complex multiplication by the ring of integers O_K.

Let $p \geq 5$ be a prime number such that E has potentially good ordinary reduction at primes above p. Then the ideal (p) splits into a product of two primes $\mathfrak{p} = (\pi)$ and its complex conjugate $\bar{\mathfrak{p}} = (\bar{\pi})$ for some $\pi \in O_K$. The Tate module $T_p(E)$ also splits into the direct sum of $T_{\mathfrak{p}}(E) \coloneqq \varprojlim_n E[\mathfrak{p}^n](\bar{\mathbb{Q}})$ and $T_{\bar{\mathfrak{p}}}(E) \coloneqq \varprojlim_n E[\bar{\mathfrak{p}}^n](\bar{\mathbb{Q}})$, both of which are free $\mathbb{Z}_p$-modules of rank one. We have the corresponding characters

$$\chi_1 \colon G_K \to \mathrm{Aut}(T_{\mathfrak{p}}(E)) \cong \mathbb{Z}_p^\times \quad \text{and} \quad \chi_2 \colon G_K \to \mathrm{Aut}(T_{\bar{\mathfrak{p}}}(E)) \cong \mathbb{Z}_p^\times.$$

We choose a basis $\omega_1 = (\omega_{1,n})_{n \geq 1}$ and $\omega_2 = (\omega_{2,n})_{n \geq 1}$ of $T_p(E)$ so that ω_1 (resp. ω_2) generates $T_{\mathfrak{p}}(E)$ (resp. $T_{\bar{\mathfrak{p}}}(E)$). With respect to this basis, the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}}$ is a $\mathrm{Gal}(K(E[p^\infty])/K)$-equivariant homomorphism

$$\kappa_{\boldsymbol{m}} \colon G^{\mathrm{ab}}_{K(E[p^\infty])} \to \mathbb{Z}_p(\boldsymbol{m}) \coloneqq \mathbb{Z}_p(\chi_1^{m_1}\chi_2^{m_2}).$$

The following main result of this paper gives an analogue of Theorem 1.1. Note that the ray class field of K modulo p (resp. $\mathfrak{p}$, $\bar{\mathfrak{p}}$) is denoted by $K(p)$ (resp. $K(\mathfrak{p})$, $K(\bar{\mathfrak{p}})$) cf. Notations.

Theorem 1.4 (Theorem 4.4 and Section 5.1- Section 5.4)**.**
Let $I \coloneqq \{\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{(1,1)\} \mid m_1 \equiv m_2 \bmod |O_K^\times|\}$.

1. *For* $\boldsymbol{m} \in I$, $\kappa_{\boldsymbol{m}}$ *is nontrivial if* $H^2_{\text{ét}}(\mathrm{Spec}(O_K[\frac{1}{p}]), \mathbb{Z}_p(\boldsymbol{m}))$ *is finite.*
2. $\kappa_{\boldsymbol{m}}$ *is not surjective for every* $\boldsymbol{m} \in I$ *such that* $\boldsymbol{m} \geq (2,2)$ *and* $\boldsymbol{m} \equiv (1,1) \bmod p-1$.
3. *If the class number of* $K(p)$ *is not divisible by* p *and there exists a unique prime of* $K(p)$ *above* $\mathfrak{p}$*, then* $\kappa_{\boldsymbol{m}}$ *is surjective for every* $\boldsymbol{m} \in I$ *such that* $\boldsymbol{m} \not\equiv (1,1) \bmod p-1$.
4. $\kappa_{(m,1)}$ *(resp.* $\kappa_{(1,m)}$*) is surjective for every* $m > 1$ *such that* $m \equiv 1 \bmod p-1$.
5. $\kappa_{(m,1)}$ *(resp.* $\kappa_{(1,m)}$*) are surjective for all* $(m,1) \in I$ *(resp.* $(1,m) \in I$*) if and only if the class number of* $K(\mathfrak{p})$ *(resp.* $K(\bar{\mathfrak{p}})$*) is not divisible by* p.

Remark 1.5. *(1) The finiteness of* $H^2_{\text{ét}}$ *in Theorem 1.4 (1) is a special case of a conjecture of Jannsen [Jan89, Conjecture 1]. We will discuss some assumptions under which this finiteness holds in Section 4.2.*

(2) It is known by Kucuksakalli [Kuc11, Theorem 2] that the class number of $K(\mathfrak{p})$ is divisible by p when $K = \mathbb{Q}(\sqrt{-163})$ and $\mathfrak{p}$ is a prime above $p = 307$. In particular, some elliptic Soulé characters of the form $\kappa_{(m,1)}$ are not surjective.

(3) We cannot prove the converse of Theorem 1.4 (3) at the moment, cf. Remark 5.7.

Theorem 1.4 is used in a subsequent work of the author to determine the kernels of the pro-p outer Galois representations associated to once-punctured CM elliptic curves. Such a result may be regarded as a theorem of Sharifi [Sha02] which states that the kernel of the pro-p outer Galois action on $\mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ corresponds to the maximal pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p when $p > 2$ is regular.

This paper is organized as follows: In Section 2, we briefly discuss properties of elliptic units used in the following sections. In Section 3, we slightly modify elliptic Soulé characters to obtain certain cocycles coming from a norm compatible system of elliptic units in Section 4. Such a construction originates from Soulé [Sou81] [Sou87] and is also studied by Kings [Kin01, 2.2.1] in a similar situation. In Section 4.1, we prove Theorem 1.4 (1) by adopting an argument of Kings [Kin01, Proposition 5.2.5]. In Section 4.2, we discuss conditions which imply the finiteness of $H^2_{\text{ét}}$. In Section 5, using a relation between the class numbers of ray class fields of imaginary quadratic fields and elliptic units, we prove (2)-(5) of Theorem 1.4.

Acknowledgements. This paper is based on a part of the author's doctoral thesis submitted to Kyoto University. He would like to thank Professor Akio Tamagawa for helpful advices. He also would like to thank Benjamin Collas for carefully reading a draft version of the thesis and giving the author a lot of advice. This work is supported by JSPS KAKENHI Grand Number 23KJ1882.

Notations

The following notations are used throughout the paper.

Indexes. For a pair of integers $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2$ and an integer n, we write $\boldsymbol{m} \equiv 0 \bmod n$ if $\boldsymbol{m} \in n\mathbb{Z}^2$. For any two pairs of integers $\boldsymbol{m} = (m_1, m_2)$ and $\boldsymbol{n} = (n_1, n_2)$, we write $\boldsymbol{m} \geq \boldsymbol{n}$ if $m_i \geq n_i$ for $i = 1, 2$. Similarly, we write $\boldsymbol{m} > \boldsymbol{n}$ if $\boldsymbol{m} \geq \boldsymbol{n}$ and $\boldsymbol{m} \neq \boldsymbol{n}$. In the following, we denote $(1, 1)$ by $\mathbf{1}$.

Profinite Groups. For a profinite group G, we denote the maximal abelian quotient of G by G^{ab}. Moreover, for a prime number p, we denote the maximal pro-p quotient of G by $G^{(p)}$.

Number Fields. We fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and every number field is considered to be a subfield of $\bar{\mathbb{Q}}$. For a number field F, we denote the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ of F by G_F, the ring of integers by O_F and the group of roots of unity in F by $\mu(F)$. For an integer $m \geq 1$, we denote the group of m-th roots of unity in $\bar{\mathbb{Q}}$ by μ_m.

For a set S of nonarchimedean places of F, we denote the ring of S-integers of F by $O_{F,S}$. For a nonarchimedean place v of F, we denote the v-adic completions of K (resp. O_F) by F_v (resp. O_{F_v}).

For a subfield F of $\bar{\mathbb{Q}}$, the set of primes of F above p (resp. $\mathfrak{p}$, $\bar{\mathfrak{p}}$, if F is an extension of K) is denoted by $S_p(F)$ (resp. $S_{\mathfrak{p}}(F)$, $S_{\bar{\mathfrak{p}}}(F)$). Moreover, we denote the maximal pro-p extension of F unramified outside $S_p(F)$ (resp. $S_{\mathfrak{p}}(F)$, $S_{\bar{\mathfrak{p}}}(F)$) by $F_{S_p}(p)$ (resp. $F_{S_{\mathfrak{p}}}(p)$, $F_{S_{\bar{\mathfrak{p}}}}(p)$). We drop F from e.g. $S_p(F)$ if the field is clear from the context.

Imaginary Quadratic Fields. We denote the cardinality $|O_K^\times|$ of the unit group of K by w. For a nonzero ideal $\mathfrak{m}$ of O_K, we denote the cardinality $|O_k/\mathfrak{m}|$ by $N\mathfrak{m}$ and the ray class field of K modulo $\mathfrak{m}$ by $K(\mathfrak{m})$. We write $K(\mathfrak{m}^\infty) \coloneqq \cup_{n\geq 1} K(\mathfrak{m}^n)$. Moreover, for a nonzero ideal $\mathfrak{a}$ of O_K relatively prime to $\mathfrak{m}$, we denote the Artin symbol $(\mathfrak{a}, K(\mathfrak{m})/K) \in \mathrm{Gal}(K(\mathfrak{m})/K)$ by $\sigma_{\mathfrak{a}}$.

Note that the natural inclusions $\mathbb{Z}_p \hookrightarrow O_{K_{\mathfrak{p}}}$ and $\mathbb{Z}_p \hookrightarrow O_{K_{\bar{\mathfrak{p}}}}$ are isomorphisms since p splits in K. Hence we have two homomorphisms

$$i_1 \colon O_K \hookrightarrow O_{K_{\mathfrak{p}}} \xrightarrow{\sim} \mathbb{Z}_p \quad \text{and} \quad i_2 \colon O_K \hookrightarrow O_{K_{\bar{\mathfrak{p}}}} \xrightarrow{\sim} \mathbb{Z}_p.$$

For a pair of nonnegative integers $\boldsymbol{m} = (m_1, m_2)$, we denote $i_1^{m_1} i_2^{m_2} \colon O_K \to \mathbb{Z}_p$ by $i^{\boldsymbol{m}}$.

CM Elliptic Curves. For $\alpha \in O_K$, we shall write the corresponding endomorphism of E by $[\alpha]$. For an ideal $\mathfrak{m}$ of O_K, the set of $\bar{\mathbb{Q}}$-points of the $\mathfrak{m}$-torsion subgroup scheme $E[\mathfrak{m}]$ determines an injective homomorphism

$$\mathrm{Gal}(K(E[\mathfrak{m}])/K) \hookrightarrow \mathrm{Aut}(E[\mathfrak{m}](\bar{\mathbb{Q}})) \cong (O_K/\mathfrak{m})^\times.$$

Moreover, this injection induces an isomorphism

$$\mathrm{Gal}(K(\mathfrak{m})/K) \xrightarrow{\sim} (O_K/\mathfrak{m})^\times / \mathrm{im}(O_K^\times)$$

which does not depend on the choice of E.

Since p splits in K, the G_K-action on $T_{\mathfrak{p}}(E) = \varprojlim_n E[\mathfrak{p}^n](\bar{\mathbb{Q}})$ (resp. $T_{\bar{\mathfrak{p}}}(E) = \varprojlim_n E[\bar{\mathfrak{p}}^n](\bar{\mathbb{Q}})$) determines a character

$$\chi_1 \colon G_K \to \mathrm{Aut}(T_{\mathfrak{p}}(E)) \cong \mathbb{Z}_p^\times \quad \text{resp.} \quad \chi_2 \colon G_K \to \mathrm{Aut}(T_{\bar{\mathfrak{p}}}(E)) \cong \mathbb{Z}_p^\times.$$

For $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2$, we write $\chi^{\boldsymbol{m}} \coloneqq \chi_1^{m_1} \chi_2^{m_2} \colon G_K \to \mathbb{Z}_p^\times$. Note that, if $m_1 \equiv m_2 \bmod |O_K|$, then the character $\chi^{\boldsymbol{m}}$ factors through $\mathrm{Gal}(K(E[p^\infty])/K) \to \mathrm{Gal}(K(p^\infty)/K)$.

Moreover, for a $\mathbb{Z}_p$-module M on which G_K acts, we denote the $\chi^{\boldsymbol{m}}$-twist of M by $M(\boldsymbol{m})$. With this notation, we can write $T_{\mathfrak{p}}(E) = \mathbb{Z}_p(1,0)$, $T_{\bar{\mathfrak{p}}}(E) = \mathbb{Z}_p(0,1)$ and $\mathbb{Z}_p(m,m)$ is the m-th Tate twist $\mathbb{Z}_p(m)$ for $m \in \mathbb{Z}$.

2 Preliminaries on elliptic units

In this section, we define a certain rational function $\theta_{\mathfrak{a}}$ on E associated to every nontrivial ideal $\mathfrak{a}$ of O_K and study arithmetic properties of its special values

evaluated at torsion points of E. The function $\theta_{\mathfrak{a}}$ is also a quotient of the so-called fundamental theta function, cf. de Shalit [dS87, Chapter II]. Our main references in this section are de Shalit [dS87] and Rubin [Rub99] [Rub91].

2.1 The function $\theta_{\mathfrak{a}}$

Definition 2.1 ([dS87, Chapter II §2, 2.3])**.** Let $\mathfrak{a}$ be a nontrivial ideal of O_K. We define a rational function $\theta_{\mathfrak{a}}$ on E by

$$\theta_{\mathfrak{a}} = \alpha^{-12}\Delta(E)^{N\mathfrak{a}-1} \prod_{\nu \in E[\mathfrak{a}]\setminus O} (x - x(\nu))^{-6}.$$

Here, α is a generator of $\mathfrak{a}$ and $\Delta(E)$ is the discriminant of the chosen Weierstrass model of E. Moreover, $x\colon E \to \mathbb{P}^1$ is a finite morphism of degree two corresponding to the x-coordinate of E.

The function $\mathfrak{a}$ is defined over K with $\operatorname{div}(\theta_{\mathfrak{a}}) = 12(N\mathfrak{a}[O] - \sum_{P\in E[\mathfrak{a}]}[P])$. Moreover, $\theta_{\mathfrak{a}}$ is invariant under the action of $\operatorname{Aut}(E)$.

The following two propositions are often used in this section:

Proposition 2.1 (The distribution relation [dS87, Chapter II §2, 2.3 Proposition])**.** *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nontrivial ideals of O_K relatively prime to each other and β a generator of $\mathfrak{b}$. Then we have*

$$\prod_{\nu \in E[\mathfrak{b}]} \theta_{\mathfrak{a}}(\tau + \nu) = \theta_{\mathfrak{a}}(\beta\tau).$$

Proposition 2.2 ([dS87, Chapter II §2, 2.4 Proposition])**.** *Let $\mathfrak{m}$ and $\mathfrak{a}$ be nontrivial ideals of O_K relatively prime to each other, and τ a primitive $\mathfrak{m}$-torsion point of E. Then, the following assertions hold:*

1. *$\theta_{\mathfrak{a}}(\tau) \in K(\mathfrak{m})$.*
2. *For every ideal $\mathfrak{c} = (c)$ of O_K relatively prime to $\mathfrak{m}$, we have*

$$\theta_{\mathfrak{a}}(\tau)^{\sigma_{\mathfrak{c}}} = \theta_{\mathfrak{a}}(c\tau) = \theta_{\mathfrak{a}\mathfrak{c}}(\tau)\theta_{\mathfrak{c}}(\tau)^{-N\mathfrak{a}}.$$

3. *$\theta_{\mathfrak{a}}(\tau)$ is a unit unless $\mathfrak{m}$ is a power of a maximal ideal. If $\mathfrak{m}$ is a power of a maximal ideal $\mathfrak{l}$, then $\theta_{\mathfrak{a}}(\tau)$ is an $\mathfrak{l}$-unit.*

Lemma 2.3. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be nontrivial ideals of O_K relatively prime to each other and take generators of $a, b \in O_K$ of $\mathfrak{a}$ and $\mathfrak{b}$, respectively. Then, as a rational function on E, we have*

$$\frac{\theta_{\mathfrak{b}}^{N\mathfrak{a}}}{\theta_{\mathfrak{b}} \circ [a]} = \frac{\theta_{\mathfrak{a}}^{N\mathfrak{b}}}{\theta_{\mathfrak{a}} \circ [b]}.$$

Proof. Since the divisors associated to both sides coincide, the two functions are equal up to a multiple of $K^\times$. Moreover, for an arbitrary primitive $\mathfrak{m}$-torsion point τ of E where $\mathfrak{m}$ is prime to $\mathfrak{ab}$,

$$\theta_{\mathfrak{a}}(b\tau)\theta_{\mathfrak{b}}(\tau)^{N\mathfrak{a}} = \theta_{\mathfrak{b}}(a\tau)\theta_{\mathfrak{a}}(\tau)^{N\mathfrak{b}}$$

holds by Lemma 2.2. This concludes the proof. □

By using Proposition 2.1 and Proposition 2.2, one can compute the norm of special values of $\theta_{\mathfrak{a}}$ as follows.

Proposition 2.4 ([dS87, Chapter II §2, 2.5 Proposition (i)])**.** *Let $\mathfrak{f}$ be a nontrivial ideal of O_K, $\mathfrak{l} = (l)$ a maximal ideal of O_K, $\mathfrak{a}$ a nontrivial ideal of O_K relatively prime to $\mathfrak{g} \coloneqq \mathfrak{f}\mathfrak{l}$ and τ a primitive $\mathfrak{g}$-torsion point of E. If we denote the number of roots of unity in K congruent to $1 \bmod \mathfrak{f}$ (resp. $\mathfrak{g}$) by $w_{\mathfrak{f}}$ (resp. $w_{\mathfrak{g}}$) and set $e \coloneqq \frac{w_{\mathfrak{f}}}{w_{\mathfrak{g}}}$, then we have*

$$N_{K(\mathfrak{g})/K(\mathfrak{f})}(\theta_{\mathfrak{a}}(\tau)^e) = \begin{cases} \theta_{\mathfrak{a}}(l\tau)^{1-\sigma_{\mathfrak{l}}^{-1}} & (\textit{if } \mathfrak{l} \nmid \mathfrak{f}) \\ \theta_{\mathfrak{a}}(l\tau) & (\textit{if } \mathfrak{l} \mid \mathfrak{f}) \end{cases}.$$

2.2 The group of elliptic units

In this subsection, we briefly recall Rubin's group of elliptic units. A useful reference is given by Schmitt [Sch15], which carefully compares the three different kinds of elliptic units (defined by Rubin, de Shalit and Yager, respectively).

Definition 2.2 ([Sch15, Definition 2.1], see also [Rub91, §1])**.** Let F be a finite abelian extension of K.

1. We define a subgroup C_F of $O_F^\times$ to be a subgroup generated by

$$N_{FK(\mathfrak{m})/F}(\theta_{\mathfrak{a}}(\tau))^{\sigma-1},$$

where $\mathfrak{m}$ ranges over the ideals of O_K such that $O_K^\times \to O_K/\mathfrak{m}$ is injective, τ over the primitive $\mathfrak{m}$-torsion points of E, $\mathfrak{a}$ over the ideals of O_K with $(\mathfrak{a}, 6\mathfrak{m}) = 1$ and σ over $\mathrm{Gal}(F/K)$. Note that C_F is a $\mathrm{Gal}(F/K)$-submodule of $O_F^\times$.

2. We define a subgroup $C(F)$ of $O_F^\times$, *the group of elliptic units of* F, to be

$$C(F) \coloneqq \mu(F)C_F.$$

3. We define a group $\mathcal{C}$ to be

$$\mathcal{C} \coloneqq \varprojlim_n (C(K(p^n)) \otimes \mathbb{Z}_p),$$

where the transition map $C(K(p^{n+1})) \otimes \mathbb{Z}_p \to C(K(p^n)) \otimes \mathbb{Z}_p$ is induced by the norm map associated to $K(p^{n+1})/K(p^n)$ for every n.

Remark 2.5. *In fact, the definition appearing in [Sch15] [Rub91] are slightly different from the definitions given above since they consider suitable* 12*-th roots of elliptic units. However, since we assume* $p \geq 5$*, the resulting groups are the same once taking tensor products with* $\mathbb{Z}_p$*.*

The following theorem relates the group of elliptic units $C(F)$ with the p-part of the class number of F.

Theorem 2.6 ([Rub91, Theorem 1.3])**.** *Let* F *be an abelian extension of* K *and assume that* $[F\colon K]$ *is prime to* p*. Then the* p*-part of the index* $[O_F^\times\colon C(F)]$ *is equal to the* p*-part of the class number of* F*.*

First, we prove that one can impose more conditions on $\mathfrak{m}$ appearing in the definition of the group of elliptic units:

Lemma 2.7. *Let* $n \geq 1$ *be an integer. Then, the group* $C_{K(p^n)}$ *is generated by*

$$\theta_{\mathfrak{a}}(\tau)^{\sigma-1},$$

where $\mathfrak{m}$ *ranges over ideals of the form* $\mathfrak{p}^{m_1}\bar{\mathfrak{p}}^{m_2}$ *for some* $(m_1, m_2) \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\}$ *such that* $m_i \leq n$ *for* $i = 1, 2$*,* τ *over the primitive* $\mathfrak{m}$*-torsion points of* E *and* $\mathfrak{a}$ *over the ideals of* O_K *with* $(\mathfrak{a}, 6\mathfrak{m}) = 1$ *and* σ *over* $\mathrm{Gal}(K(p^n)/K)$*.*

Proof. Let $\mathfrak{n}$ be an arbitrary ideal of O_K such that $O_K^\times \to O_K/\mathfrak{n}$ is injective. Write $\mathfrak{n} = \mathfrak{p}^{m_1}\bar{\mathfrak{p}}^{m_2}\mathfrak{m}$ for an ideal $\mathfrak{m}$ with $(\mathfrak{m}, p) = 1$. Let τ be a primitive $\mathfrak{n}$-torsion point of E and $\mathfrak{a}$ an arbitrary ideal with $(\mathfrak{a}, 6\mathfrak{n}) = 1$.

First, since

$$K(p^n) \cap K(\mathfrak{n}) = K(\mathfrak{p}^{\min(n,m_1)}\bar{\mathfrak{p}}^{\min(n,m_2)}),$$

there is a natural isomorphism

$$\mathrm{Gal}(K(p^n)K(\mathfrak{n})/K(p^n)) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{n})/K(\mathfrak{p}^{\min(n,m_1)}\bar{\mathfrak{p}}^{\min(n,m_2)})).$$

Since $\theta_{\mathfrak{a}}(\tau) \in K(\mathfrak{n})$, we have

$$N_{K(p^n)K(\mathfrak{n})/K(p^n)}\theta_{\mathfrak{a}}(\tau) = N_{K(\mathfrak{n})/K(\mathfrak{p}^{\min(n,m_1)}\bar{\mathfrak{p}}^{\min(n,m_2)})}\theta_{\mathfrak{a}}(\tau).$$

If $(m_1, m_2) = (0, 0)$, then this norm is contained in K and taking the action of $\sigma - 1$ for $\sigma \in \mathrm{Gal}(K(p^n)/K)$ yields 1. Hence we may assume $(m_1, m_2) \neq (0, 0)$.

By Proposition 2.4, this norm is contained in a Galois submodule generated by $\theta_{\mathfrak{a}}(\pi^{m_1-\min(n,m_1)}\bar{\pi}^{m_2-\min(n,m_2)}\alpha\tau)$ where α is a generator of $\mathfrak{m}$. The claim follows since $\pi^{m_1-\min(n,m_1)}\bar{\pi}^{m_2-\min(n,m_2)}\alpha\tau$ is a primitive $\mathfrak{p}^{\min(n,m_1)}\bar{\mathfrak{p}}^{\min(n,m_2)}$-torsion point. □

Proposition 2.8. *Let* $n \geq 1$ *be an integer. Then, the group* $C_{K(p^n)}$ *is generated by*

$$\theta_{\mathfrak{a}}(\omega_{1,n} + \omega_{2,n})^{\sigma-1}, \theta_{\mathfrak{a}}(\omega_{1,n})^{\sigma-1} \quad \text{and} \quad \theta_{\mathfrak{a}}(\omega_{2,n})^{\sigma-1}$$

where σ *ranges over* $\mathrm{Gal}(K(p^n)/K)$ *and* $\mathfrak{a}$ *ranges over the ideals of* O_K *with* $(\mathfrak{a}, 6p) = 1$*,* $(\mathfrak{a}, 6\mathfrak{p}) = 1$ *and* $(\mathfrak{a}, 6\bar{\mathfrak{p}}) = 1$*, respectively.*

Proof. We consider an arbitrary element of the form $\theta_{\mathfrak{b}}(\tau)$, where $\mathfrak{b}$ is an ideal of O_K with $(\mathfrak{b}, 6\mathfrak{m}) = 1$ and τ is a primitive $\mathfrak{p}^{m_1}\bar{\mathfrak{p}}^{m_2}$-torsion points of E for a pair of nonnegative integers (m_1, m_2) such that $m_i \leq n$ for $i = 1, 2$.

First, if $m_1 = 0$ and, then Proposition 2.2 (2) and Proposition 2.4 implies that $\theta_{\mathfrak{b}}(\tau)$ is contained in the Galois module generated by $\theta_{\mathfrak{b}}(\omega_{2,n})$. The same argument shows that we may assume that $m_1, m_2 \geq 1$. Iin this case, again Proposition 2.2 (2) and Proposition 2.4 implies that $\theta_{\mathfrak{b}}(\tau)$ is contained in the Galois module generated by $\theta_{\mathfrak{b}}(\omega_{1,n} + \omega_{2,n})$. By Lemma 2.7, This concludes the proof. □

Remark 2.9. *By a similar argument, the group $C_{K(\mathfrak{p}^n)}$ (resp. $C_{K(\bar{\mathfrak{p}}^n)}$) is generated by $\theta_{\mathfrak{a}}(\omega_{1,n})^{\sigma-1}$ (resp. $\theta_{\mathfrak{a}}(\omega_{2,n})^{\sigma-1}$), where $\mathfrak{a}$ runs through ideals of O_K with $(\mathfrak{a}, 6\mathfrak{p}) = 1$ (resp. $(\mathfrak{a}, 6\bar{\mathfrak{p}}) = 1$) and σ through $\mathrm{Gal}(K(\mathfrak{p}^n)/K)$ (resp. $\mathrm{Gal}(K(\bar{\mathfrak{p}}^n)/K)$) for every $n \geq 1$.*

We separate the group of elliptic unit into three subgroups C', D_1 and D_2 according to generators as follows:

Definition 2.3. Let $n \geq 1$ be an integer.

1. Let $C'(K(p^n))$ be the subgroup of $C(K(p^n))$ generated by $\mu(K(p^n))$ and
$$\theta_{\mathfrak{a}}(\omega_{1,n} + \omega_{2,n})^{\sigma-1}$$
where $\mathfrak{a}$ ranges over the ideals of O_K with $(\mathfrak{a}, 6p) = 1$ and σ over $\mathrm{Gal}(K(p^n)/K)$.
2. Let $D_1(K(p^n))$ be the subgroup of $C(K(p^n))$ generated by
$$\theta_{\mathfrak{a}}(\omega_{1,n})^{\sigma-1}$$
where $\mathfrak{a}$ ranges over the ideals of O_K with $(\mathfrak{a}, 6\mathfrak{p}) = 1$ and σ over $\mathrm{Gal}(K(\mathfrak{p}^n)/K)$. Similarly, let $D_2(K(p^n))$ be the subgroup of $C(K(p^n))$ generated by
$$\theta_{\mathfrak{a}}(\omega_{2,n})^{\sigma-1}$$
where $\mathfrak{a}$ ranges over the ideals of O_K with $(\mathfrak{a}, 6\bar{\mathfrak{p}}) = 1$ and σ over $\mathrm{Gal}(K(\bar{\mathfrak{p}}^n)/K)$.
3. We define three subgroups $\mathcal{C}'$, $\mathcal{D}_1$ and $\mathcal{D}_2$ of $\mathcal{C}$ by
$$\mathcal{C}' \coloneqq \varprojlim_n C'(K(p^n)) \otimes \mathbb{Z}_p,$$
$$\mathcal{D}_1 \coloneqq \varprojlim_n D_1(K(p^n)) \otimes \mathbb{Z}_p \quad \text{and} \quad \mathcal{D}_2 \coloneqq \varprojlim_n D_2(K(p^n)) \otimes \mathbb{Z}_p,$$
respectively. Note that the group $\mathcal{C}$ is generated by $\mathcal{D}_1$, $\mathcal{D}_2$ and $\mathcal{C}'$ by Proposition 2.8.

Proposition 2.10. *We have*
$$\mathcal{D}_1 = \mathcal{D}_2 = 1 \quad \textit{and} \quad \mathcal{C} = \mathcal{C}'.$$

Proof. To prove the first equality, let $(x_n)_{n\geq 1} \in \mathcal{D}_1$ and fix an arbitrary integer $n_0 \geq 1$. For every $N \geq 1$, since x_{n_0+N} is contained in $K(\mathfrak{p}^{n_0+N}) \subset K(p^{n_0}\mathfrak{p}^N)$, it holds that

$$\begin{aligned} x_{n_0} &= N_{K(p^{n_0+N})/K(p^{n_0})}(x_{n_0+N}) \\ &= N_{K(p^{n_0}\mathfrak{p}^N)/K(p^{n_0})}(N_{K(p^{n_0+N})/K(p^{n_0}\mathfrak{p}^N)}(x_{n_0+N})) \\ &= N_{K(p^{n_0}\mathfrak{p}^N)/K(p^{n_0})}(x_{n_0+N}^{[K(p^{n_0+N})\colon K(p^{n_0}\mathfrak{p}^N)]}) \in (D_1(K(p^{n_0})) \otimes \mathbb{Z}_p)^{p^N} \end{aligned}$$

Since N is arbitrary, we conclude $x_{n_0} = 1$. This proves that $\mathcal{D}_1$ is trivial, and the same proof yields that $\mathcal{D}_2 = 0$. Finally, the second equality follows from the first one. □

3 Rewriting elliptic Soulé characters

First, one can easily observe the following lemma.

Lemma 3.1. *Let $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 1} \setminus \{\mathbf{1}\}$ such that $m_1 \equiv m_2 \bmod 2$.*

1. *If $\boldsymbol{m} \notin I$, then $\kappa_{\boldsymbol{m}}$ is trivial.*
2. *$\kappa_{\boldsymbol{m}}$ factors through the natural surjection $G^{\mathrm{ab}}_{K(E[p^\infty])} \to G^{\mathrm{ab}}_{K(p^\infty)}$.*

Proof. For every $\zeta \in O_K^\times$, it follows that $\kappa_{\boldsymbol{m}} = \zeta^{m_1-m_2}\kappa_{\boldsymbol{m}}$ by observing the action of $O_K^\times$ on E. This proves (1). The second assertion immediately follows from the Kummer characterization of $\kappa_{\boldsymbol{m}}$. □

Our first task to prove the nontriviality of the elliptic Soulé characters is to modify $\epsilon_{\boldsymbol{m},n}$ into a product of elliptic units in $K(p^n)$. This can be done by multiplying $\epsilon_{\boldsymbol{m},n}$ by a suitable nonzero multiple of $\mathbb{Z}_p$.

In the following of this section, let $\boldsymbol{m} = (m_1, m_2) \in I$, $\mathfrak{a}$ a nontrivial ideal of O_K prime to p and $\alpha \in O_K$ a generator of $\mathfrak{a}$. Since the Artin symbol corresponding to $\mathfrak{a}$ acts on p-power torsion points of E by multiplication by α up to multiplication by an element of $O_K^\times = \mathrm{Aut}(E)$ which leaves θ_p invariant, it follows that

$$\sigma_{\mathfrak{a}}\left(\theta_p(\tau)\right) = \theta_p(\alpha\tau)$$

for every nontrivial p-power torsion point τ of E.

Lemma 3.2. *Let $n \geq 1$ be an integer. Then, as an element of $K(p^\infty)^\times/(K(p^\infty)^\times)^{p^n}$,*

$$\epsilon_{\boldsymbol{m},n}^{N\mathfrak{a}-\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}})} = \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \theta_{\mathfrak{a}}(a\omega_{1,n} + b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}.$$

Proof. First, by the above discussion it holds that

$$\begin{aligned} \theta_p(a\omega_{1,n+1+k} + b\omega_{2,n+1+k}) &= \theta_p\left(\sigma_{\mathfrak{a}}(\sigma_{\mathfrak{a}}^{-1}(a\omega_{1,n+1+k} + b\omega_{2,n+1+k}))\right) \\ &= (\theta_p \circ [\alpha])(a\chi_1(\sigma_{\mathfrak{a}}^{-1})\omega_{1,n+1+k} + b\chi_2(\sigma_{\mathfrak{a}}^{-1})\omega_{2,n+1+k}) \end{aligned}$$

for every $k \geq 0$. Hence it follows that

$$\epsilon_{\boldsymbol{m},n}^{\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}})} = \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \left(\prod_{k=0}^{\infty} (\theta_p \circ [\alpha])(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})^{-p^{2k}} \right)^{a^{m_1-1}b^{m_2-1}},$$

and we obtain

$$\epsilon_{\boldsymbol{m},n}^{-N\mathfrak{a}+\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}})} = \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \left(\prod_{k=0}^{\infty} \left(\frac{(\theta_p \circ [\alpha])(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})}{\theta_p(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})^{N\mathfrak{a}}}\right)^{-p^{2k}} \right)^{a^{m_1-1}b^{m_2-1}}.$$

By Lemma 2.3, we simplify the right hand side as follows.

$$\begin{aligned}
&= \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \left(\prod_{k=0}^{\infty} \left(\frac{(\theta_{\mathfrak{a}} \circ [p])(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})}{\theta_{\mathfrak{a}}(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})^{p^2}} \right)^{-p^{2k}} \right)^{a^{m_1-1}b^{m_2-1}} \\
&= \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \left(\prod_{k=0}^{\infty} \left(\frac{\theta_{\mathfrak{a}}(a\omega_{1,n+k} + b\omega_{2,n+k})}{\theta_{\mathfrak{a}}(a\omega_{1,n+1+k} + b\omega_{2,n+1+k})^{p^2}} \right)^{-p^{2k}} \right)^{a^{m_1-1}b^{m_2-1}} \\
&= \prod_{\substack{0\leq a,b<p^n \\ p\nmid \gcd(a,b)}} \theta_{\mathfrak{a}}(a\omega_{1,n} + b\omega_{2,n})^{-a^{m_1-1}b^{m_2-1}}.
\end{aligned}$$

This concludes the proof. □

Recall that the Soulé characters modulo p^n correspond to products of cyclotomic p-units of $\mathbb{Q}(\mu_{p^n})$, which are special values of certain rational functions evaluated over *primitive* p^n-torsion points of $\mathbb{G}_m[p^n]$ in Section 1.

Now we modify $\epsilon_{\boldsymbol{m},n}$ into such a form that it only involves $\theta_{\mathfrak{a}}$ evaluated over primitive p^n-torsion points of E. If $m_1 = 1$ or $m_2 = 1$, we transform $\epsilon_{\boldsymbol{m},n}$ into a product of $\theta_{\mathfrak{a}}$ evaluated over primitive $\bar{\mathfrak{p}}^n$ (resp. $\mathfrak{p}^n$)-torsion points of E.

3.1 The case $\boldsymbol{m} = (m_1, m_2) \geq (2, 2)$

In this subsection, we assume that $\boldsymbol{m} = (m_1, m_2) \geq (2, 2)$.

Lemma 3.3. *Let $n \geq 1$ be an integer. Then, as an element of $K(p^n)^\times/(K(p^n)^\times)^{p^n}$,*

$$\prod_{\substack{a,b\in\mathbb{Z}/p^n\mathbb{Z} \\ p\nmid \gcd(a,b)}} \theta_{\mathfrak{a}}(a\omega_{1,n} + b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}$$

is equal to the $\left(\frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\pi)} + \frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi})} - 1\right)$-th power of

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}} \coloneqq \prod_{a,b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n} + b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}.$$

Proof. First, note that

$$\begin{aligned}\epsilon_{\boldsymbol{m},n,\mathfrak{a}}^{p^{m_1-1}} &= \prod_{a,b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{(pa)^{m_1-1}b^{m_2-1}} \\ &= \prod_{\substack{\bar{a}\in p(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}} \left(\prod_{\substack{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times \\ pa\equiv\bar{a} \bmod p^n}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})\right)^{\bar{a}^{m_1-1}b^{m_2-1}}.\end{aligned}$$

On the other hand, the distribution relation (Proposition 2.1) implies

$$\begin{aligned}\prod_{\substack{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times \\ pa\equiv\bar{a} \bmod p^n}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n}) &= \prod_{\tau\in E[\mathfrak{p}]} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n}+\tau) = \theta_{\mathfrak{a}}(\pi(a\omega_{1,n}+b\omega_{2,n})) \\ &= \theta_{\mathfrak{a}}(\bar{\pi}^{-1}\bar{a}\omega_{1,n}+\pi b\omega_{2,n}).\end{aligned}$$

Hence we conclude

$$\begin{aligned}\epsilon_{\boldsymbol{m},n,\mathfrak{a}}^{p^{m_1-1}} &= \prod_{a,b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{(pa)^{m_1-1}b^{m_2-1}} \\ &= \prod_{\substack{\bar{a}\in p(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}} \theta_{\mathfrak{a}}(\bar{\pi}^{-1}\bar{a}\omega_{1,n}+\pi b\omega_{2,n})^{\bar{a}^{m_1-1}b^{m_2-1}} \\ &= \left(\prod_{\substack{\bar{a}\in p(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}} \theta_{\mathfrak{a}}(\bar{a}\omega_{1,n}+b\omega_{2,n})^{\bar{a}^{m_1-1}b^{m_2-1}}\right)^{i_{\mathfrak{p}}^{m_1-1}(\bar{\pi})i_{\bar{\mathfrak{p}}}^{m_2-1}(\pi^{-1})}\end{aligned}$$

Since $p^{m_1-1} = i_{\mathfrak{p}}^{m_1-1}(p) = i_{\mathfrak{p}}^{m_1-1}(\pi)i_{\mathfrak{p}}^{m_1-1}(\bar{\pi})$, we have

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}}^{i^{\boldsymbol{m}-\mathbf{1}}(\pi)} = \prod_{\substack{a\in p(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}.$$

For every $1 \le i < n$, the same argument as above shows

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}}^{i^{\boldsymbol{m}-\mathbf{1}}(\pi)^i} = \prod_{\substack{a\in p^i(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}$$

and

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}}^{i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi})^i} = \prod_{\substack{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times \\ b\in p^i(\mathbb{Z}/p^n\mathbb{Z})^\times}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}b^{m_2-1}}$$

The assertion follows from these equalities. □

3.2 The case where $m_1 = 1$ or $m_2 = 1$

In this subsection, we assume that $m_1 = 1$ or $m_2 = 1$. We only treat the case when $m_2 = 1$ since the remaining case can be treated in the same manner. The main difference from the previous subsection is that we can reduce to a one-variable situation by considering the primitive $\mathfrak{p}^n$-torsion points in place of the primitive p^n-torsion points.

Lemma 3.4. *Let $n \geq 1$ be an integer. Then, as an element of $K(p^n)^\times/(K(p^n)^\times)^{p^n}$,*

$$\prod_{\substack{a,b\in\mathbb{Z}/p^n\mathbb{Z}\\ p\nmid\gcd(a,b)}} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}}$$

is the $\left(\frac{1-i^{\boldsymbol{m-1}}(\bar{\pi})}{1-i^{\boldsymbol{m-1}}(\pi)}+i^{\boldsymbol{m-1}}(\bar{\pi})\right)$-th power of

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}} \coloneqq \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}^n\omega_{1,n})^{a^{m_1-1}}.$$

Proof. First, we divide the set $\{(a,b) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid p \nmid \gcd(a,b)\}$ into the following two subsets

$$S_1 \coloneqq \{(a,b) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid b \in (\mathbb{Z}/p^n\mathbb{Z})^\times\}$$

and

$$S_2 \coloneqq \{(a,b) \in (\mathbb{Z}/p^n\mathbb{Z})^2 \mid a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \text{ and } b \equiv 0 \bmod p\}.$$

Then, the same argument as in the proof of Lemma 3.3 shows the equality

$$\prod_{(a,b)\in S_1} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}} = \left(\prod_{a,b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}}\right)^{\sum_{i=0}^{n-1} i^{\boldsymbol{m-1}}(\pi)^i}$$

To compute the right hand side, note that

$$\begin{aligned}
\prod_{a,b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}} &= \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\prod_{b\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}}\\
&= \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} N_{K(p^n)/K(\mathfrak{p}^n)}(\theta_{\mathfrak{a}}(a\omega_{1,n}+\omega_{2,n}))^{a^{m_1-1}}\\
&= \left(\prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}^n\omega_{1,n})^{a^{m_1-1}}\right)^{1-\sigma_{\bar{\mathfrak{p}}}^{-1}}
\end{aligned}$$

Here, we use Lemma 2.4 to deduce the last equality. Since the inverse of the Artin symbol $\sigma_{\bar{\mathfrak{p}}}^{-1}$ sends $\theta_{\mathfrak{a}}(a\bar{\pi}^n\omega_{1,n})$ to $\theta_{\mathfrak{a}}(a\bar{\pi}^{n-1}\omega_{1,n})$, it follows that

$$\left(\prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}^n\omega_{1,n})^{a^{m_1-1}}\right)^{1-\sigma_{\bar{\mathfrak{p}}}^{-1}} = \left(\prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}^n\omega_{1,n})^{a^{m_1-1}}\right)^{1-i^{\boldsymbol{m-1}}(\bar{\pi})}.$$

Next, we compute the product $\prod_{(a,b)\in S_2}\theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}}$ by using Proposition 2.1 as follows:

$$\begin{aligned}\prod_{(a,b)\in S_2}\theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}} &= \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left(\prod_{b\in p\mathbb{Z}/p^n\mathbb{Z}}\theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})\right)^{a^{m_1-1}}\\ &= \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\left(\prod_{\tau\in E[\bar{\mathfrak{p}}^{n-1}]}\theta_{\mathfrak{a}}(a\omega_{1,n}+\tau)\right)^{a^{m_1-1}}\\ &= \prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\theta_{\mathfrak{a}}(a\bar{\pi}^{n-1}\omega_{1,n})^{a^{m_1-1}}\\ &= \left(\prod_{a\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\theta_{\mathfrak{a}}(a\bar{\pi}^{n}\omega_{1,n})^{a^{m_1-1}}\right)^{i^{\boldsymbol{m-1}}(\bar{\pi})}.\end{aligned}$$

Combining these computations yields that $\prod_{\substack{a,b\in\mathbb{Z}/p^n\mathbb{Z}\\ p\nmid\gcd(a,b)}}\theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{a^{m_1-1}}$ multiplied by

$$(1-i^{\boldsymbol{m-1}}(\bar{\pi}))\sum_{i=0}^{\infty}i^{\boldsymbol{m-1}}(\pi)^i+i^{\boldsymbol{m-1}}(\bar{\pi})=\frac{1-i^{\boldsymbol{m-1}}(\bar{\pi})}{1-i^{\boldsymbol{m-1}}(\pi)}+i^{\boldsymbol{m-1}}(\bar{\pi})$$

is equal to $\epsilon_{\boldsymbol{m},n,\mathfrak{a}}$ as desired. □

The same computation yields the following:

Lemma 3.5. *Let $n\geq 1$ be an integer. Then, as an element of $K(p^n)^\times/(K(p^n)^\times)^{p^n}$,*

$$\prod_{\substack{a,b\in\mathbb{Z}/p^n\mathbb{Z}\\ p\nmid\gcd(a,b)}}\theta_{\mathfrak{a}}(a\omega_{1,n}+b\omega_{2,n})^{b^{m_2-1}}$$

is equal to the $\left(\frac{1-i^{\boldsymbol{m-1}}(\pi)}{1-i^{\boldsymbol{m-1}}(\bar{\pi})}+i^{\boldsymbol{m-1}}(\pi)\right)$-th power of

$$\epsilon_{\boldsymbol{m},n,\mathfrak{a}}:=\prod_{b\in(\mathbb{Z}/p^n\mathbb{Z})^\times}\theta_{\mathfrak{a}}(b\pi^n\omega_{2,n})^{b^{m_2-1}}.$$

4 Nontriviality of elliptic Soulé characters

In this section, we prove Theorem 1.4 (1) (=Theorem 4.4). We adopt some techniques used by Kings in [Kin01] to study the Tamagawa number conjecture for CM elliptic curves. There he uses the étale (or Galois) cohomology groups with coefficient in the Tate twist of the p-adic Tate module $T_p(E)(k+1)=\mathbb{Z}_p(k+2,k+1)\oplus\mathbb{Z}_p(k+1,k+2)$ for an integer $k\geq 0$. Moreover, in Section

4.2, we study certain assumptions under which the assumption on Theorem 4.4 holds.

In the following, for $\boldsymbol{m} = (m_1, m_2) \in \mathbb{Z}^2_{\geq 0}$ we abbreviate the group of units $O^\times_{K(\mathfrak{p}^{m_1}\bar{\mathfrak{p}}^{m_2})}$ as $E_{\boldsymbol{m}}$. If $m_1 = m_2 = m$, it is even abbreviated as E_m.

Definition 4.1. We define a $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K)]]$-module $\mathcal{E}$ to be

$$\mathcal{E} \coloneqq \varprojlim_n E_n \otimes \mathbb{Z}_p,$$

where transition maps are taken to be norms. Note that this is equivalent to defining $\mathcal{E} \coloneqq \varprojlim E_n/E_n^{p^n}$.

4.1 Conditional nontriviality of elliptic Soulé characters

First, we review the construction of the Soulé elliptic elements given in Kings [Kin01, 2.2.1], which originates from Soulé [Sou81] [Sou87].

First, we fix $\boldsymbol{m} = (m_1, m_2) \in I$ and a basis $\omega^{\boldsymbol{m-1}} \coloneqq \omega_1^{\otimes(m_1-1)} \otimes \omega_2^{\otimes(m_2-1)}$ of $\mathbb{Z}_p(\boldsymbol{m}-\boldsymbol{1})$ and let $e = (e_n)_{n\geq 1} \in \mathcal{E}$ be a norm compatible system of units.

For every $n \geq 1$, the element $e_n \otimes \omega_n^{\boldsymbol{m-1}}$ can be regarded as an element of $H^1_{\text{ét}}(O_{K(p^n),S_p}, \mathbb{Z}/p^n(\boldsymbol{m}))$ via the following inclusion from Kummer theory:

$$E_n/E_n^{p^n}(\boldsymbol{m}-\boldsymbol{1}) \subset H^1_{\text{ét}}(O_{K(p^n),S_p}, \mathbb{Z}/p^n(\boldsymbol{m})).$$

Moreover, by composing this inclusion with the corestriction map with respect to $\mathrm{Spec}(O_{K(p^n),S_p}) \to \mathrm{Spec}(O_{K,S_p})$, we obtain an element of $H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}/p^n(\boldsymbol{m}))$. Then it holds by direct computation that such a system of elements of $H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}/p^n(\boldsymbol{m}))$ forms a projective system with respect to the reduction map, hence defines an element of $H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$.

This construction gives a map

$$\mathcal{E}(\boldsymbol{m}-\boldsymbol{1}) = (\varprojlim E_n/E_n^{p^n})(\boldsymbol{m}-\boldsymbol{1}) \to H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})),$$

and one can easily observe that this map is a homomorphism which factors through the $\mathrm{Gal}(K(p^\infty)/K)$-coinvariant of $\mathcal{E}(\boldsymbol{m}-\boldsymbol{1})$. We write the corresponding homomorphism as

$$e_{\boldsymbol{m}} \colon \mathcal{E}(\boldsymbol{m}-\boldsymbol{1})_{\mathrm{Gal}(K(p^\infty)/K)} \to H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})).$$

Moreover, by composing the homomorphism $e_{\boldsymbol{m}}$ with the restriction map

$$H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})) \to H^1_{\text{ét}}(O_{K(p^\infty),S_p}, \mathbb{Z}_p(\boldsymbol{m}))^{\mathrm{Gal}(K(p^\infty)/K)},$$

which is also denoted by the same letter $e_{\boldsymbol{m}}$, we obtain a $\mathrm{Gal}(K(p^\infty)/K)$-equivariant homomorphism from $G^{\mathrm{ab}}_{K(p^\infty)}$ to $\mathbb{Z}_p(\boldsymbol{m})$ for every norm compatible system of units.

Note that the kernel and the cokernel of the restriction map $H^1_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})) \to H^1_{\text{ét}}(O_{K(p^\infty),S_p}, \mathbb{Z}_p(\boldsymbol{m}))^{\mathrm{Gal}(K(p^\infty)/K)}$ are finite. This follows from the four-term

exact sequence and the fact that $H^i(\mathrm{Gal}(K(p^\infty)/K), \mathbb{Z}_p(\boldsymbol{m}))$ are finite for $i = 1, 2$.

The next proposition allows us to relate the homomorphism $e_{\boldsymbol{m}}$ with the elliptic Soulé characters.

Lemma 4.1. *For $u = (u_n)_{n\geq 1} \in \mathcal{E}$, the character $e_{\boldsymbol{m}}(u)\colon G^{\mathrm{ab}}_{K(p^\infty)} \to \mathbb{Z}_p(\boldsymbol{m})$ modulo p^n coincides with the Kummer character associated to the p^n-th root of*

$$\prod_{\sigma\in\mathrm{Gal}(K(p^n)/K)} \sigma(u_n)^{\chi^{\boldsymbol{m-1}}(\sigma)}.$$

Proof. The assertion directly follows from the construction of $e_{\boldsymbol{m}}$. □

Note that the system of elliptic units $(\theta_{\mathfrak{a}}(\omega_{1,n} + \omega_{2,n}))_{n\geq 1}$ is contained in $\mathcal{E}$ for every nontrivial ideal $\mathfrak{a}$ of O_K relatively prime to p by Lemma 2.4. Hence we can make the following definition:

Definition 4.2. Let $\boldsymbol{m} \in I$ and $\mathfrak{a}$ a nontrivial ideal of O_K relatively prime to p. We define a character $\kappa_{\boldsymbol{m},\mathfrak{a}}\colon G^{\mathrm{ab}}_{K(p^\infty)} \to \mathbb{Z}_p(\boldsymbol{m})$ to be the image of the system $(\theta_{\mathfrak{a}}(\omega_{1,n} + \omega_{2,n}))_{n\geq 1}$ under the homomorphism $e_{\boldsymbol{m}}$.

Then, computations in the previous section shows the following explicit formula between $\kappa_{\boldsymbol{m},\mathfrak{a}}$ and $\kappa_{\boldsymbol{m}}$:

Proposition 4.2. *Let $\boldsymbol{m} = (m_1, m_2) \in I$ and $\mathfrak{a}$ a nontrivial ideal of O_K relatively prime to p. Then the following relation holds between $\kappa_{\boldsymbol{m},\mathfrak{a}}$ and $\kappa_{\boldsymbol{m}}$:*

$$w\left(\frac{1}{1 - i^{\boldsymbol{m-1}}(\pi)} + \frac{1}{1 - i^{\boldsymbol{m-1}}(\bar{\pi})} - 1\right)\kappa_{\boldsymbol{m},\mathfrak{a}} = (N\mathfrak{a} - \chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}))\kappa_{\boldsymbol{m}}.$$

Proof. If $\boldsymbol{m} \geq (2, 2)$, the assertion follows from Lemma 3.2, Lemma 3.3 and the fact that we count the same value w times.

If $m_2 = 1$, the character $\chi^{\boldsymbol{m-1}} (= \chi_1^{m_1-1})$ factors through $\mathrm{Gal}(K(\mathfrak{p}^\infty)/K)$. Hence $\kappa_{\boldsymbol{m},\mathfrak{a}}$ modulo p^n corresponds to

$$\prod_{\sigma\in\mathrm{Gal}(K(p^n)/K)} \sigma\left(\theta_a(\omega_{1,n} + \omega_{2,n})\right)^{\chi^{\boldsymbol{m-1}}(\sigma)} = \prod_{\sigma\in\mathrm{Gal}(K(\mathfrak{p}^n)/K)} \sigma\left(N_{K(p^n)/K(\mathfrak{p}^n)}(\theta_{\mathfrak{a}}(\omega_{1,n} + \omega_{2,n}))\right)^{\chi^{\boldsymbol{m-1}}(\sigma)}.$$

for every $n \geq 1$. By Lemma 2.4, the right hand side can be simplified as

$$\left(\prod_{\sigma\in\mathrm{Gal}(K(\mathfrak{p}^n)/K)} \sigma(\theta_{\mathfrak{a}}(\bar{\pi}^n\omega_{1,n}))^{\chi_1^{m_1-1}(\sigma)}\right)^{1-\sigma_{\bar{\mathfrak{p}}}^{-1}}.$$

Hence the right hand side is equal to $w^{-1}(1 - i^{\boldsymbol{m-1}}(\bar{\pi}))$-th power of $\epsilon_{\boldsymbol{m},n,\mathfrak{a}}$. By Lemma 3.2 and Lemma 3.4, we conclude that

$$(N\mathfrak{a} - \chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}))\kappa_{\boldsymbol{m}} = \left(\frac{1 - i^{\boldsymbol{m-1}}(\bar{\pi})}{1 - i^{\boldsymbol{m-1}}(\pi)} + i^{\boldsymbol{m-1}}(\bar{\pi})\right)\frac{w}{1 - i^{\boldsymbol{m-1}}(\bar{\pi})}\kappa_{\boldsymbol{m},\mathfrak{a}}$$

as desired. □

Before proving a conditional nontriviality of the elliptic Soulé characters, we make the following observation.

Lemma 4.3. *The submodule $e_{\boldsymbol{m}}(\mathcal{C}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)})$ inside $H^1_{\text{ét}}(O_{K(p^\infty),S_p},\mathbb{Z}_p(\boldsymbol{m}))^{\mathrm{Gal}(K(p^\infty)/K)}$ is contained in a $\mathbb{Z}_p$-submodule generated by the character $\kappa_{\boldsymbol{m}}$.*

Proof. Note that we have $\mathcal{C}=\mathcal{C}'$ by Proposition 2.10. Moreover, by [Sch15, Lemma 3.6], it holds that $\varprojlim_n \mu(K(p^n))\subset\mathcal{C}'$ is trivial. Hence, to conclude the assertion, it suffices to prove that every image of an element of the form $\theta_{\mathfrak{a}}(\omega_{1,n}+\omega_{2,n})^{\sigma-1}$ (cf. Definition 2.3) in $H^1_{\text{ét}}(O_{K(p^\infty),S_p},\mathbb{Z}/p^n(\boldsymbol{m}))$ can be written as a scalar multiple of $\kappa_{\boldsymbol{m}}$ mod p^n for every $n\geq 1$. This immediately follows from the definition of $e_{\boldsymbol{m}}$ and Proposition 4.2. □

We now prove one of main results of this section:

Theorem 4.4. *Let $\boldsymbol{m}\in I$ and suppose that the cohomology $H^2_{\text{ét}}(O_{K,S_p},\mathbb{Z}_p(\boldsymbol{m}))$ is finite. Then, the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}}\colon G^{\mathrm{ab}}_{K(p^\infty)}\to\mathbb{Z}_p(\boldsymbol{m})$ is nontrivial.*

Proof. The proof of this theorem is similar to that of [Kin01, Proposition 5.2.5]: We divide the proof into several steps.

First, let $M\subset K(p)$ (resp. $L\subset K(p^\infty)$) be the subfield of $K(p)$ (resp. $K(p^\infty)$) which corresponds to the kernel of $\chi^{\boldsymbol{m}-\mathbf{1}}$ modulo p (resp. the kernel of $\chi^{\boldsymbol{m}-\mathbf{1}}$). Then L/M is a $\mathbb{Z}_p$-extension. Let L_n/M denote the subextension of L/M such that $[L_n:M]=p^n$ for every $n\geq 1$ and $\mathcal{E}_L:=\varprojlim_n O_{L_n}^\times/(O_{L_n}^\times)^{p^n}$. Similar to the construction of $e_{\boldsymbol{m}}$, one can construct a homomorphism:

$$e_{\boldsymbol{m},L}:\mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}\to H^1_{\text{ét}}(O_{K,S_p},\mathbb{Z}_p(\boldsymbol{m}))$$

so that the following diagram commutes:

$$\begin{array}{ccc}\mathcal{E}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)} & \xrightarrow{e_{\boldsymbol{m}}} & H^1_{\text{ét}}(O_{K,S_p},\mathbb{Z}_p(\boldsymbol{m}))\\ \downarrow & & \|\\ \mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} & \xrightarrow{e_{\boldsymbol{m},L}} & H^1_{\text{ét}}(O_{K,S_p},\mathbb{Z}_p(\boldsymbol{m})).\end{array}$$

Here, the left vertical arrow is induced by norm maps $Nr_{K(p^n)/L_n}$ for every $n\geq 1$.

Now let $\mathcal{A}_L$ be projective limit of the p-part of the ideal class group of L_n for $n\geq 1$, where transition maps are induced by norms. By a similar argument as in [Kin01, Proposition 5.2.5], it holds that $\mathcal{A}_L(\boldsymbol{m}-1)_{\mathrm{Gal}(L/K)}$ and the kernel of $e_{\boldsymbol{m},L}$ are finite under the assumption that the cohomology $H^2_{\text{ét}}(O_{K,S_p},\mathbb{Z}_p(\boldsymbol{m}))$ is finite.

Let $\mathcal{C}_L:=\varprojlim_n C(L_n)\otimes\mathbb{Z}_p\subset\mathcal{E}_L$. Then the Iwasawa main conjecture for imaginary quadratic fields [Rub91, Theorem 4.1 (i)] implies that the finiteness of $\mathcal{A}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$ is equivalent to that of $(\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$. Since

$(\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$ is finite and $(\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})$ is a torsion $\mathbb{Z}_p[[\mathrm{Gal}(L/K)]]$-module by [Rub91, Corollary 7.8], $(\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})^{\mathrm{Gal}(L/K)}$ is also finite. By the exact sequence

$$(\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})^{\mathrm{Gal}(L/K)} \to \mathcal{C}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} \to \mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} \to (\mathcal{E}_L/\mathcal{C}_L)(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} \to 0$$

(see [Rub91, Lemma 6.1]), it follows that the kernel and the cokernel of the natural homomorphism $\mathcal{C}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} \to \mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$ are both finite.

Note that norm maps induce a homomorphism $p_L \colon \mathcal{C}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)} \to \mathcal{C}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$. We claim that $\ker(p_L)$ and $\mathrm{coker}(p_L)$ of p_L are both finite. In fact, by [Rub91, Theorem 7.7 (ii)], it follows that the kernel and cokernel of the natural homomorphism between $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K)]]$-modules:

$$\mathcal{C}_{\mathrm{Gal}(K(p^\infty)/L)} \to \mathcal{C}_L$$

are annihilated by the product of $\mathrm{ann}(\mathbb{Z}_p(1)) \subset \mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K)]]$ and $\mathcal{I}_{\mathfrak{p}}\mathcal{I}_{\bar{\mathfrak{p}}}$. Here, $\mathcal{I}_{\mathfrak{p}}$ (resp. $\mathcal{I}_{\bar{\mathfrak{p}}}$) is an ideal of $\mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty)/K)]]$ generated by elements of the form $\sigma - 1$, where σ ranges over the decomposition group at $\mathfrak{p}$ (resp. $\bar{\mathfrak{p}}$). Hence both $\ker(p_L)$ and $\mathrm{coker}(p_L)$ are annihilated by every element of $\mathbb{Z}_p$ of the following form

$$(1-\chi^{\boldsymbol{m}}(\sigma))(1-\chi^{\boldsymbol{m}-\mathbf{1}}(\tau_1))(1-\chi^{\boldsymbol{m}-\mathbf{1}}(\tau_2)) \qquad (\star)$$

where τ_1 (resp. τ_2) is an element of the decomposition group of $\mathrm{Gal}(K(p^\infty)/K)$ at $\mathfrak{p}$ (resp. at $\bar{\mathfrak{p}}$) and $\sigma \in \mathrm{Gal}(K(p^\infty)/K)$. Since the decomposition groups at $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are open in $\mathrm{Gal}(K(p^\infty)/K)$, we can choose σ, τ_1 and τ_2 so that $(\star)$ is nonzero. Therefore $\ker(p_L)$ and $\mathrm{coker}(p_L)$ are finite, as desired.

We have shown that both the kernel and the cokernel of $\mathcal{C}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)} \to \mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)}$ are finite. Since $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{E}_L(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(L/K)} \geq 1$ by [Rub91, Corollary 7.8], we also have $\mathrm{rank}_{\mathbb{Z}_p}\mathcal{C}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)} \geq 1$.

Since the kernel of $\ker(e_{\boldsymbol{m},L})$ is finite, it holds that the image $e_{\boldsymbol{m}}(\mathcal{C}(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(K(p^\infty)/K)}) \subset H^1_{\text{ét}}(O_{K(p^\infty),S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ is nontrivial. By Lemma 4.3, we obtain the desired assertion. □

4.2 On the finiteness of $H^2_{\text{ét}}(\mathrm{Spec}(O_K[\frac{1}{p}]), \mathbb{Z}_p(\boldsymbol{m}))$

In this subsection, we prove the finiteness of $H^2_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ under various assumptions. First, we make some observations. Let F be a subfield of $K(p)$ containing K,

$$I_F \coloneqq \{\boldsymbol{m} \in I \mid \text{the Galois group } G_F \text{ acts trivially on } \mathbb{F}_p(\boldsymbol{m})\}$$

and let $\boldsymbol{m} \in I_F$.

Note that $H^2_{\text{ét}}(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ is isomorphic to $H^2(G_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$, where the latter is a Galois cohomology group of $G_{F,S_p} \coloneqq \pi_1^{\text{ét}}(\mathrm{Spec}(O_{F,S_p}))$, the maximal Galois group of F unramified outside S_p by [Mil06, II, Proposition 2.9]. Moreover, by [NSW08, Corollary 10.4.8], there is a natural isomorphism

$$H^2(G^{(p)}_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m})) \xrightarrow{\sim} H^2(G_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$$

since $\boldsymbol{m} \in I_F$.

Lemma 4.5. *Let F be a subfield of $K(p)$ containing K and $\boldsymbol{m} \in I$. Then there is an isomorphism*

$$H^2_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})) \xrightarrow{\sim} H^2_{\text{ét}}(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))^{\mathrm{Gal}(F/K)}$$

Proof. Since $\mathrm{Spec}(O_{F,S_p}) \to \mathrm{Spec}(O_{K,S_p})$ is an étale $\mathrm{Gal}(F/K)$-covering, there is a spectral sequence

$$E_2^{p,q} = H^p(\mathrm{Gal}(F/K), H^q(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))) \Rightarrow H^{p+q}_{\text{ét}}(O_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m})).$$

Since $\mathrm{Gal}(F/K)$ is a finite prime-to-p group, $E_2^{1,1}$, $E_2^{1,2}$ and $E_2^{2,0}$ vanish. Hence we obtain a desired isomorphism. □

By the above observation and Lemma 4.5, we are reduced to considering the cohomology group $H^2(G^{(p)}_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$. In the rest of this section, we derive the desired finiteness of this cohomology in the following three situations : (1) $\boldsymbol{m} \in (p-1)\mathbb{Z}^2$, (2) $\boldsymbol{m} = (m, m)$ for $m \geq 2$ and (3) every $\boldsymbol{m} \in I_F$ when p is a "purely local" prime.

First, we consider the case $\boldsymbol{m} \in (p-1)\mathbb{Z}^2$. First, we show

Lemma 4.6. *The Galois group $G^{(p)}_{K,S_p}$ is a free pro-p group of rank two. In particular, the group $H^2(G^{(p)}_{K,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ is trivial for every $\boldsymbol{m} \in I_K$.*

Proof. By [NSW08, Theorem 10.7.13], it holds that $\dim H^1(G^{(p)}_{K,S_p}, \mathbb{F}_p) = 2 + \dim V_{S_p}(K)$ and $\dim H^2(G^{(p)}_{K,S_p}, \mathbb{F}_p) = \dim V_{S_p}(K)$, where

$$V_{S_p}(K) \coloneqq \{a \in K^\times \mid a \in (K_v^\times)^p \text{ if } v \in \{\mathfrak{p}, \bar{\mathfrak{p}}\} \text{ and } a \in U_v(K_v^\times)^p \text{ otherwise}\}/(K^\times)^p.$$

Since O_K is PID, one can easily observe that $V_{S_p}(K)$ is trivial. □

This implies the following corollary:

Corollary 4.7. *The elliptic Soulé character $\kappa_{\boldsymbol{m}} \colon G_{K(p^\infty)} \to \mathbb{Z}_p(\boldsymbol{m})$ is nontrivial for every $\boldsymbol{m} \in I_K = (p-1)\mathbb{Z}^2_{\geq 1}$.*

As for the next case, we have the following unconditional result due to Soulé.

Theorem 4.8 (Soulé [Sou79, page 287, Corollaire])**.**

$$H^2_{\text{ét}}(O_{K(\mu_p),S_p}, \mathbb{Z}_p(m))$$

is finite for every $m \geq 2$.

Hence we have:

Corollary 4.9. *The elliptic Soulé character $\kappa_{(m,m)} \colon G_{K(p^\infty)} \to \mathbb{Z}_p(m)$ is nontrivial for every $m \geq 2$.*

Remark 4.10. *If $m \geq 3$ is odd, one may relate $\kappa_{(m,m)}$ with the m-th Soulé character κ_m by computing norms of elliptic units in terms of cyclotomic units.*

For the last case, we prove the finiteness of $H^2_{\text{ét}}(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ for every $\boldsymbol{m} \in I_F$ when p satisfies a certain condition which is analogous to the regularity of prime numbers.

Definition 4.3. Let F be a subfield of $K(E[p])$ containing K, v a prime of F above p and $F_v(p)$ the maximal pro-p extension of F_v. We say that v is *purely local* if the natural map

$$\mathrm{Gal}(F_v(p)/F_v) \to \mathrm{Gal}(F_{S_p}(p)/F)$$

is an isomorphism.

The pure locality is a strong condition as the following lemma suggests.

Lemma 4.11. *Let F be a subfield of $K(E[p])$ containing K and assume that $v \in S_{\mathfrak{p}}(F)$ is purely local. Then the following assertions hold.*

1. *There exists a unique prime of F above $\mathfrak{p}$, i.e. $S_{\mathfrak{p}}(F) = \{v\}$. Moreover, if F contains μ_p, then there exists a unique prime of F above $\bar{\mathfrak{p}}$.*
2. *If F contains μ_p, then the class number of F is not divisible by p.*

Proof. (1) We compare the dimensions of H^1 with coefficients in $\mathbb{F}_p$ of $\mathrm{Gal}(F_v(p)/F_v)$ and $\mathrm{Gal}(F_{S_p}(p)/F)$. For the former group, we have

$$\dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(F_v(p)/F_v), \mathbb{F}_p) = 1 + \delta_v + [F_v : \mathbb{Q}_p]$$

by the local class field theory. Here, δ_v is 1 if F_v contains μ_p and otherwise 0. For the latter, by [NSW08, Theorem 10.7.13], it holds that

$$\dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{F}_p) \geq 1 - \delta + [F : K] + \sum_{w \in S_p(F)} \delta_w.$$

Here, δ is 1 if F contains μ_p and otherwise 0. The definition of δ_w is similar to that of δ_v. Now since v is purely local, it holds that

$$\delta_v + [F_v : \mathbb{Q}_p] \geq -\delta + [F : K] + \sum_{w \in S_p(F)} \delta_w,$$

which is equivalent to saying that

$$([F_v : \mathbb{Q}_p] - [F : K]) + \sum_{w \in S_p(F) \setminus \{v\}} \delta_w \leq \delta.$$

If F does not contain μ_p, then this inequality implies that $[F_v : \mathbb{Q}_p] = [F : K]$. If F contains μ_p, then it holds that $[F_v : \mathbb{Q}_p] = [F : K]$ and $S_p(F) \setminus \{v\}$ is a singleton. Hence the assertion follows.

(2) Since F contains μ_p, by [NSW08, Theorem 10.7.13] and (1), it holds that

$$\dim_{\mathbb{F}_p} H^1(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{F}_p) = 2 + [F : K] + \dim Cl_{S_p}(F)/p$$

where $Cl_{S_p}(F)$ is a quotient of the usual ideal class group $Cl(F)$ divided by a subgroup generated by $S_p(F)$. By comparing again, it holds that $Cl_{S_p}(F)/p = 0$. Since primes of F above $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are unique by (1) and $[F : K]$ is prime to p, the orders of such two primes in $Cl(F)$ are not divisible by p. Therefore the class number of F is not divisible by p. □

For a prime number p, one can observe that p is regular if and only if there exists a unique prime of $F_{S_p}(p)$ above p where $F = \mathbb{Q}(\mu_p)$. This fact, together with the following proposition, explains a certain similarity between regular primes and purely local primes.

Proposition 4.12. *Let F be a subfield of $K(E[p])$ containing K and v a prime of F above $\mathfrak{p}$. The following assertions are equivalent.*

1. *v is purely local.*
2. *The natural map $\mathrm{Gal}(F_v(p)/F_v) \to \mathrm{Gal}(F_{S_p}(p)/F)$ is surjective.*
3. *There exists a unique prime of $F_{S_p}(p)$ above $\mathfrak{p}$.*

Proof. (1) $\Rightarrow$ (2) and (3) $\Rightarrow$ (2) : clear. (2) $\Rightarrow$ (3) : The same argument as the proof of Lemma 4.11 (1) shows that (2) implies that there exists a unique prime of F above $\mathfrak{p}$. Hence a prime of $F_{S_p}(p)$ above $\mathfrak{p}$ is also unique. (2) $\Rightarrow$ (1) : Let H be the kernel of the concerned surjection. By the Hochschild-Serre spectral sequence,

$$0 \to H^1(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathrm{Gal}(F_v(p)/F_v), \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(H, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(F_{S_p}(p)/F)} \to 0$$

is exact since $H^2(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{Q}_p/\mathbb{Z}_p) = 0$ by Leopoldt's conjecture for F.

We claim that the right term $H^1(H, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(F_{S_p}(p)/F)}$ is trivial, which in turn implies $H \subset [H : \mathrm{Gal}(F_v(p)/F_v)]$ and hence $H = 0$ as desired. To prove this claim, first we have

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(\mathrm{Gal}(F_v(p)/F_v), \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{corank}_{\mathbb{Z}_p} H^1(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{Q}_p/\mathbb{Z}_p) = [F : K]+1$$

since Leopoldt's conjecture holds for F and (2) $\Rightarrow$ (3). Moreover, we also have

$$\dim H^1(\mathrm{Gal}(F_{S_p}(p)/F), \mathbb{F}_p) = [F : K] + 1 + \delta \geq \dim H^1(\mathrm{Gal}(F_v(p)/F_v), \mathbb{Q}_p/\mathbb{Z}_p)$$

by [NSW08, Theorem 10.7.13] and the local class field theory. From these two (in)equalities, the claim follows as desired. □

Proposition 4.13. *Let F be a subfield of $K(p)$ containing K and $\boldsymbol{m} \in I_F$. If one of $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ is purely local for F, then $H^2_{\text{ét}}(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ is finite. In particular, the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}}$ is nontrivial.*

Proof. First, recall that $H^2(O_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ is isomorphic to $H^2(G^{(p)}_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$. If one of $\mathfrak{p}$ or $\bar{\mathfrak{p}}$ is purely local for F, $G^{(p)}_{F,S_p}$ is a free pro-p group if $\mu_p \not\subset F$ or a pro-p Demushkin group (cf. [NSW08, Definition 3.9.9] for the definition) otherwise by [NSW08, Theorem 7.5.11]. For the former case, the cohomology $H^2(G^{(p)}_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m}))$ clearly vanishes. For the latter, by the Tate duality, it holds that

$$\begin{aligned} H^2(G^{(p)}_{F,S_p}, \mathbb{Z}_p(\boldsymbol{m})) &= H^0(G^{(p)}_{F,S_p}, \mathbb{Q}_p/\mathbb{Z}_p(\mathbf{1}-\boldsymbol{m}))^* \\ &= \mathbb{Z}_p(\boldsymbol{m}-\mathbf{1})_{\mathrm{Gal}(F_\infty/F)} \end{aligned}$$

where F_∞ is a unique $\mathbb{Z}_p^2$-extension of F inside $K(p^\infty)$. The last coinvariant is finite since $\boldsymbol{m} \neq \mathbf{1}$. □

In the rest of this subsection, we briefly discuss a work of Wingberg which relates pure locality of primes to a work of Yager [Yag82] on a "regular" primes for (extensions of) imaginary quadratic fields K, and give examples of purely local primes of $K(p)$.

Definition 4.4. Let F be a subfield of $K(E[p])$ containing K. We say $\mathfrak{p}$ (resp. $\bar{\mathfrak{p}}$) is *regular for* F if the field $F_{S_\mathfrak{p}}(p)$ (resp. $F_{S_{\bar{\mathfrak{p}}}}(p)$) is a $\mathbb{Z}_p$-extension of F. We say p is regular for F if $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are both regular for F.

We then have the following lemma.

Lemma 4.14. *The following assertions hold.*

1. *p is always regular for K.*
2. *Let $K \subset F \subset L \subset K(E[p])$ be subfields of $K(E[p])$ containing K. If $\mathfrak{p}$ is regular for L, then $\mathfrak{p}$ is so for F.*

Proof. (1) Note that the maximal abelian quotient of $\mathrm{Gal}(K_{S_\mathfrak{p}}(p)/K)$ is equal to the maximal pro-p quotient of $\mathrm{Gal}(K(\mathfrak{p}^\infty)/K)$ which is isomorphic to $\mathbb{Z}_p$. Hence $\mathrm{Gal}(K_{S_\mathfrak{p}}(p)/K)$ itself is isomorphic to $\mathbb{Z}_p$. The same argument shows that $\bar{\mathfrak{p}}$ is also regular for K as desired.

(2) The claim follows since the natural homomorphism $\mathrm{Gal}(L_{S_\mathfrak{p}}(p)/L) \to \mathrm{Gal}(F_{S_\mathfrak{p}}(p)/F)$ is surjective and $F_{S_\mathfrak{p}}(p)$ contains a $\mathbb{Z}_p$-extension $K_{S_\mathfrak{p}}(p) \cdot F$ of F. □

Theorem 4.15 (Wingberg [Win90, Theorem])**.** *Let $K \subset F \subset K(E[p])$ be a subfield of $K(E[p])$ containing K. Then $\mathfrak{p}$ is regular for F of Yager if and only if a prime of F above $\bar{\mathfrak{p}}$ is purely local. A similar statement also holds when replacing $\mathfrak{p}$ by $\bar{\mathfrak{p}}$.*

If this theorem is true, then $\mathfrak{p}$ would be always purely local for K. However, as we see in the following example, this does not hold. Note that, if $F = K$, then both $G^{(p)}_{K_\mathfrak{p}}$ and $\mathrm{Gal}(K_{S_p}(p)/K)$ are free pro-p groups of rank two, hence are isomorphic as abstract profinite groups.

Example 4.1. Let $F = K = \mathbb{Q}(\sqrt{-1})$ and $p = 29789$. We claim that the natural map $G_{K_{\mathfrak{p}}}^{(p)} \to \mathrm{Gal}(K_{S_p}(p)/K)$ is not surjective. To prove this claim, it suffices to show that the map

$$G_{K_{\mathfrak{p}}}^{(p)} \to \mathrm{Gal}(K_{S_{\bar{\mathfrak{p}}}}(p)/K)$$

is not surjective, i.e. the Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ does not generate $\mathrm{Gal}(K_{S_{\bar{\mathfrak{p}}}}(p)/K)$.

Note that the group $\mathrm{Gal}(K_{S_{\bar{\mathfrak{p}}}}(p)/K) \cong \mathbb{Z}_p$ is nothing but the group of principal units in $\mathrm{Gal}(K(\bar{\mathfrak{p}}^\infty)/K) \cong O_{K_{\bar{\mathfrak{p}}}}^\times/O_K^\times$. We can choose $\mathfrak{p} = (\pi)$ where $\pi := 110 + 133\sqrt{-1}$. Then $\mathrm{Frob}_{\mathfrak{p}}$ is equal to $\pi \bmod \mu(K)$ and one can observe that $\pi^{p-1} \in 1 + \bar{\mathfrak{p}}^2 O_{K_{\bar{\mathfrak{p}}}}$. Therefore the image of $\mathrm{Frob}_{\mathfrak{p}}$, so the image of the decomposition subgroup at $\mathfrak{p}$, does not generate $\mathrm{Gal}(K_{S_{\bar{\mathfrak{p}}}}(p)/K)$ as desired.

In fact, the proof of [Win90, Theorem] essentially shows the following slightly weaker statement than the original one:

Theorem 4.16 (A modified version of Theorem 4.15)**.** *Let F be a subfield of $K(E[p])$ containing K. Then $\mathfrak{p}$ is regular for F and there exists a unique prime of $F_{S_{\mathfrak{p}}}(p)$ above $\bar{\mathfrak{p}}$ if and only if a unique prime of F above $\bar{\mathfrak{p}}$ is purely local. A similar statement also holds when replacing $\mathfrak{p}$ by $\bar{\mathfrak{p}}$.*

Remark 4.17. *If $\mathfrak{p}$ is regular for F, then $F_{S_{\mathfrak{p}}}(p) = F \cdot K_{S_{\mathfrak{p}}}(p)$. Hence there exists a unique prime of $F_{S_{\mathfrak{p}}}(p)$ above $\bar{\mathfrak{p}}$ if and only if there exists a unique prime of F and $K_{S_{\mathfrak{p}}}$ above $\bar{\mathfrak{p}}$. Moreover, the latter condition is equivalent to saying $\mathrm{Frob}_{\bar{\mathfrak{p}}}$ generates the group of principal units in $\mathrm{Gal}(K(\mathfrak{p}^\infty)/K) \cong O_{K_{\mathfrak{p}}}^\times/O_K^\times$ (which does not hold in general as Example 4.1 shows).*

Example 4.2. In [Yag82, page 33], Yager provided a Kummer-type criterion which relates the regularity of $\mathfrak{p}$ to $\mathfrak{p}$-adic properties of special values of Hecke L-functions.

By using his criterion, Yager gives examples of regular primes when $K = \mathbb{Q}(\sqrt{-1})$. For example, $p = 5$ is regular for the mod-5 ray class field $K(5)$. As an another example, $p = 29$ is regular for the mod-$\mathfrak{p}$ ray class field $K(\mathfrak{p})$ although it is not regular for $K(29)$. Moreover in this case, one can show that a prime over $\mathfrak{p}$ is purely local for $K(\mathfrak{p})$. Hence we can apply Proposition 4.13 to conclude the nontriviality of the corresponding elliptic Soulé characters.

5 Surjectivity of elliptic Soulé characters

In this section, we consider the reduction of the $\boldsymbol{m}$-th elliptic Soulé characters $\kappa_{\boldsymbol{m}}$ modulo p. First we note that the character $\kappa_{\boldsymbol{m}}$ is congruent to $\kappa_{\boldsymbol{n}}$ modulo p for every $\boldsymbol{m}, \boldsymbol{n} \geq (2,2)$ such that $\boldsymbol{m} \equiv \boldsymbol{n} \bmod p-1$. Similarly, $\kappa_{(m,1)}$ is congruent to $\kappa_{(n,1)}$ modulo p and $\kappa_{(1,m)}$ is congruent to $\kappa_{(1,n)}$ modulo p for every $m, n \geq 2$ such that $m \equiv n \bmod p-1$.

In the following we show that $\kappa_{\boldsymbol{m}} \bmod p$ is nontrivial if the p-part of the class number of $K(p)$ is trivial. To prove such a result, we need to treat $\kappa_{\boldsymbol{m}}$ separately according to $\boldsymbol{m} \in I$ as follows:

Case 1: $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv \mathbf{1} \bmod p-1$.
Case 2: $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \not\equiv \mathbf{1} \bmod p-1$.
Case 3: either $m_1 = 1$ or $m_2 = 1$ and $\boldsymbol{m} \equiv \mathbf{1} \bmod p-1$.
Case 4: either $m_1 = 1$ or $m_2 = 1$ and $\boldsymbol{m} \not\equiv \mathbf{1} \bmod p-1$.

In Case 1, we show that $\kappa_{\boldsymbol{m}}$ is not surjective and, in Case 3, we show that $\kappa_{\boldsymbol{m}}$ is surjective. In the remaining two cases, we prove the surjectivity $\kappa_{\boldsymbol{m}}$ under assumptions on the class number on the mod-p and mod-$\mathfrak{p}$ class fields of K and the number of primes of $K(p)$ above $\mathfrak{p}$.

Note that, if $\boldsymbol{m} \geq (2,2)$, the surjectivity of the character $\kappa_{\boldsymbol{m},\mathfrak{a}}$ (cf. Definition 4.2) for a suitable ideal $\mathfrak{a}$ implies that of $\kappa_{\boldsymbol{m}}$. In fact, Proposition 4.2:

$$w\left(\frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\pi)}+\frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi})}-1\right)\kappa_{\boldsymbol{m},\mathfrak{a}} = (N\mathfrak{a}-\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}}))\kappa_{\boldsymbol{m}}$$

implies that $\kappa_{\boldsymbol{m}}$ is also surjective if $\frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\pi)}+\frac{1}{1-i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi})}-1$ is a unit of $\mathbb{Z}_p$ (w is prime to p since we assume $p \geq 5$). If $\boldsymbol{m} \geq (2,2)$, then this term is congruent to 1 modulo p. If $m_1 = 1$ or $m_2 = 1$, then we use Lemma 3.2 and Lemma 3.4 instead of Proposition 4.2 to prove the desired surjectivity of $\kappa_{\boldsymbol{m}}$.

Recall that the group of units $O_{K(p)}^{\times}$ (resp. $O_{K(\mathfrak{p})}^{\times}$, $O_{K(\bar{\mathfrak{p}})}^{\times}$) is abbreviated as E_1 (resp. $E_{(1,0)}$, $E_{(0,1)}$) cf. the beginning of Section 4.

5.1 First case

We assume that $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv (1,1) \bmod p-1$. By the above discussion, we may assume that $\boldsymbol{m} = (p,p)$.

The character $\kappa_{(p,p),\mathfrak{a}} \bmod p$ corresponds to $N_{K(p)/K}(\theta_{\mathfrak{a}}(\omega_{1,1}+\omega_{2,1}))$, which is a unit in a finite prime-to-p group $O_K^{\times}$, via Kummer theory. Hence it holds that $\kappa_{(p,p),\mathfrak{a}}$ modulo p is trivial.

Proposition 5.1. *Let $\boldsymbol{m} = (m_1, m_2) \in I$ such that $\boldsymbol{m} \geq (2,2)$ and $\boldsymbol{m} \equiv \mathbf{1} \bmod p-1$. Then, the $\boldsymbol{m}$-th elliptic Soulé character $\kappa_{\boldsymbol{m}}$ is not surjective.*

5.2 Second case

Proposition 5.2. *Let $\boldsymbol{m} = (m_1, m_2) \in I$ such that $\boldsymbol{m} \geq (2,2)$, $m_1, m_2 \not\equiv 1 \bmod p-1$. If the class number of $K(p)$ is not divisible by p, then $\kappa_{\boldsymbol{m}}$ is surjective (in particular, nontrivial).*

Proof. First, we prove the assertion assuming that $\boldsymbol{m} \not\equiv (0,0) \bmod p-1$. Since the class number of $K(p)$ is not divisible by p, the equality

$$C(K(p))/C(K(p)) \cap E_1^p = E_1/E_1^p$$

holds by Theorem 2.6. The left hand side is generated by the image of $C'(K(p))$, $D_1(K(p))$ and $D_2(K(p))$, cf. Definition 2.3.

The image of $D_1(K(p))$ in E_1/E_1^p is contained in the $\mathrm{Gal}(K(p)/K(\mathfrak{p}))$-invariant subspace $(E_1/E_1^p)^{\mathrm{Gal}(K(p)/K(\mathfrak{p}))}$. Hence its $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component is trivial since $\mathrm{Gal}(K(p)/K(\mathfrak{p})) \not\subset \ker(\chi^{\mathbf{1}-\boldsymbol{m}})$. A similar argument shows that the image of $D_2(K(p))$ has the trivial $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component.

Recall the definition of $C'(K(p))$: if we write $\omega \coloneqq \omega_{1,1}+\omega_{2,1}$, then $C'(K(p))$ is generated by $\mu(K(p))$ and $\theta_{\mathfrak{a}}(\omega)^{\sigma-1}$ where $\mathfrak{a}$ ranges over the ideals relatively prime to $6p$ and σ over $\mathrm{Gal}(K(p)/K)$.

If we consider the action of

$$\phi_{\boldsymbol{m}} \coloneqq \sum_{\sigma\in\mathrm{Gal}(K(p)/K)} \chi^{\boldsymbol{m}-\mathbf{1}}(\sigma)\sigma \in \mathbb{F}_p[\mathrm{Gal}(K(p)/K)]$$

on E_1/E_1^p, which maps E_1/E_1^p onto its $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component, the above argument implies that the $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component of E_1/E_1^p is generated by $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$, where $\mathfrak{a}$ ranges over the ideals relatively prime to $6p$. Note that $\mu(K(p))$ does not affect the $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component since we assume $\boldsymbol{m} \not\equiv (0,0) \bmod p-1$.

Take an arbitrary ideal $\mathfrak{a}$ prime to $6p$ such that $\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}}) - N\mathfrak{a} \not\equiv 0 \bmod p$. Then, for an arbitrary ideal $\mathfrak{c}$ prime to $6p$, we have

$$\theta_{\mathfrak{a}}(\omega)^{\sigma_{\mathfrak{c}}-N\mathfrak{c}} = \theta_{\mathfrak{c}}(\omega)^{\sigma_{\mathfrak{a}}-N\mathfrak{a}}$$

by Lemma 2.3. Hence it follows that

$$(\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{c}}) - N\mathfrak{c})\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega)) = (\chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}}) - N\mathfrak{a})\phi_{\boldsymbol{m}}(\theta_{\mathfrak{c}}(\omega)).$$

This shows that the $\chi^{\mathbf{1}-\boldsymbol{m}}$-component of E_1/E_1^p is generated by a single element $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$. On the other hand, the $\chi^{\mathbf{1}-\boldsymbol{m}}$-component of E_1/E_1^p is observed to be one-dimensional by Dirichlet's unit theorem [NSW08, Proposition 8.7.2]. Hence it follows that $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega)) \neq 0$, which is equivalent to saying that $\kappa_{\boldsymbol{m},\mathfrak{a}}$ is surjective. Hence the assertion follows from Proposition 4.2.

If $\boldsymbol{m}$ is congruent to $(0,0) \bmod p-1$, then the above argument shows that the $\chi^{\mathbf{1}}$-component of E_1/E_1^p is generated by a single element $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$ and μ_p. Since the $\chi^{\mathbf{1}}$-component of E_1/E_1^p is two-dimensional by [NSW08, Proposition 8.7.2], $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$ is also nonzero in this case as desired. □

If m_1 is congruent to $1 \bmod p-1$, then the above proof of Proposition 5.2 does not work since $\chi^{\mathbf{1}-\boldsymbol{m}}$-isotypic component of the image of $D_2(K(p))$ in E_1/E_1^p can be nontrivial. However, we have the following result:

Proposition 5.3. *Let $\boldsymbol{m} = (m_1, m_2) \in I$ such that $\boldsymbol{m} \geq (2,2)$.*

1. *Assume that $m_1 \equiv 1 \bmod p-1$ and $m_2 \not\equiv 1 \bmod p-1$. If the class number of $K(p)$ is not divisible by p and there exists a unique prime of $K(p)$ above $\mathfrak{p}$, then $\kappa_{\boldsymbol{m}}$ is surjective.*

2. *Assume that $m_1 \not\equiv 1 \bmod p-1$ and $m_2 \equiv 1 \bmod p-1$. If the class number of $K(p)$ is not divisible by p and there exists a unique prime of $K(p)$ above $\mathfrak{p}$[1] , then $\kappa_{\boldsymbol{m}}$ is surjective.*

[1]Note that the number of primes of $K(p)$ above $\mathfrak{p}$ is equal to that of $K(\bar{\mathfrak{p}})$ above $\mathfrak{p}$, hence is also equal to that of $K(\mathfrak{p})$ above $\bar{\mathfrak{p}}$ (by considering the conjugate).

Proof. We only prove (1) since the proof of (2) is similar. Let

$$\phi_{\boldsymbol{m}} \coloneqq \sum_{\sigma \in \mathrm{Gal}(K(p)/K)} \chi^{\boldsymbol{m-1}}(\sigma)\sigma \in \mathbb{F}_p[\mathrm{Gal}(K(p)/K)].$$

We shall consider the action of $\phi_{\boldsymbol{m}}$ on E_1/E_1^p. Since the class number of $K(p)$ is not divisible by p, the same argument as in the proof of Proposition 5.2 shows that the $\chi^{\boldsymbol{1-m}}$-isotypic component of E_1/E_1^p is generated by the images of $C'(K(p))$ and $D_2(K(p))$ under $\phi_{\boldsymbol{m}}$.

Take an arbitrary ideal $\mathfrak{a}$ prime to $6p$ such that $\chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}) - N\mathfrak{a} \not\equiv 0 \bmod p$ and set $\omega \coloneqq \omega_{1,1} + \omega_{2,1}$. Then $\phi_{\boldsymbol{m}}(C'(K(p)))$ is generated by $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$. Similar argument as in the proof of Proposition 5.2 shows that $\phi_{\boldsymbol{m}}(D_2(K(p)))$ is generated by $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\pi\omega))$.

Since $N_{K(p)/K(\bar{\mathfrak{p}})}(\theta_{\mathfrak{a}}(\omega)) = \theta_{\mathfrak{a}}(\pi\omega)^{1-\sigma_{\mathfrak{p}}^{-1}}$ by Proposition 2.4, it follows that

$$\begin{aligned}\phi_{\boldsymbol{m}}\left(N_{K(p)/K(\bar{\mathfrak{p}})}(\theta_{\mathfrak{a}}(\omega))\right) &= \phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))^{[K(p):K(\mathfrak{p})]} \\ &= \phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\pi\omega)^{1-\sigma_{\mathfrak{p}}^{-1}}) = \phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\pi\omega))^{1-\chi^{\boldsymbol{m-1}}(\sigma_{\mathfrak{p}})}.\end{aligned}$$

This computation shows that $\phi_{\boldsymbol{m}}(C'(K(p)))$ is contained in $\phi_{\boldsymbol{m}}(D_2(K(p)))$ and that the two groups are equal to each other if and only if $1 - \chi^{\boldsymbol{m-1}}(\sigma_{\mathfrak{p}}) = 1 - \pi^{m_2-1} \not\equiv 0 \bmod \bar{\mathfrak{p}}$.

Since we assume that there exists a unique prime of $K(\bar{\mathfrak{p}})$ above $\mathfrak{p}$, it follows by considering the Frobenius element at $\mathfrak{p}$ that the order of $\pi^w \bmod \bar{\mathfrak{p}}$ is equal to $\frac{p-1}{w}$. Therefore we have $1 - \pi^{m_2-1} \not\equiv 0 \bmod \bar{\mathfrak{p}}$, so $\phi_{\boldsymbol{m}}(\theta_{\mathfrak{a}}(\omega))$ generates the $\chi^{\boldsymbol{1-m}}$-isotypic component of E_1/E_1^p. This concludes the proof. □

5.3 Third case

We assume that either $m_1 = 1$ or $m_2 = 1$ and $\boldsymbol{m} \equiv (1,1) \bmod p-1$. We then may assume that $\boldsymbol{m} = (p,1)$ since the case of $(1,p)$ can be treated in the same manner.

By Lemma 3.2 and Lemma 3.4, it holds that $\kappa_{\boldsymbol{m}} \bmod p$ is a Kummer character corresponding to the p-th root of

$$\epsilon_{\boldsymbol{m},1,\mathfrak{a}} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}\omega_{1,1}) = N_{K(\mathfrak{p})/K}(\theta_{\mathfrak{a}}(\bar{\pi}\omega_{1,1}))^w$$

up to

$$N\mathfrak{a} - \chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}) \quad \text{and} \quad \frac{1 - i^{\boldsymbol{m-1}}(\bar{\pi})}{1 - i^{\boldsymbol{m-1}}(\pi)} + i^{\boldsymbol{m-1}}(\bar{\pi}).$$

Since $N\mathfrak{a} - \chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}) \equiv N\mathfrak{a} - 1 \bmod p$, we can choose a ideal $\mathfrak{a}$ such that $N\mathfrak{a} - \chi^{\boldsymbol{1-m}}(\sigma_{\mathfrak{a}}) \not\equiv 0 \bmod p$. Moreover, the third term is easily shown to be congruent to 1 modulo p.

Therefore, the nontriviality of $\kappa_{\boldsymbol{m}} \bmod p$ is equivalent to that of $\epsilon_{\boldsymbol{m},1,\mathfrak{a}} \in E_1/E_1^p$, which is equivalent to that of $\epsilon_{\boldsymbol{m},1,\mathfrak{a}} \in E_{(1,0)}/E_{(1,0)}^p$ since $E_{(1,0)}/E_{(1,0)}^p$ is the $\mathrm{Gal}(K(p)/K(\mathfrak{p}))$-invariant subspace of E_1/E_1^p.

Now $\epsilon_{\boldsymbol{m},1,\mathfrak{a}}$ is congruent to $\pi^{12w(N\mathfrak{a}-1)}$ modulo the image of $\mu(K)$ by [dS87, Chapter II §2, 2.2 Proposition and 2.5 Proposition (ii)]. Since $[K(\mathfrak{p})\colon K]$ is prime to p, the field $K(\mathfrak{p})$ does not contain any p-th roots of π. Hence we have proved the following:

Proposition 5.4. *Let $m > 1$ be an integer such that $m \equiv 1 \bmod p-1$. Then, the $(m,1)$-th (resp. the $(1,m)$-th) elliptic Soulé characters $\kappa_{(m,1)}$ (rest. $\kappa_{(1,m)}$) is surjective (in particular, nontrivial).*

5.4 Fourth case

Suppose that $\boldsymbol{m} = (m_1, m_2) \in I$ satisfies $m_2 = 1$ and $m_1 \not\equiv 1 \bmod p-1$. By Lemma 3.2 and Lemma 3.4, it holds that $\kappa_{\boldsymbol{m}} \bmod p$ is a Kummer character corresponding to the p-th root of

$$\epsilon_{\boldsymbol{m},1,\mathfrak{a}} = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \theta_{\mathfrak{a}}(a\bar{\pi}\omega_1)^{a^{m_1-1}}$$

up to

$$N\mathfrak{a} - \chi^{\mathbf{1}-\boldsymbol{m}}(\sigma_{\mathfrak{a}}) \quad \text{and} \quad \frac{1 - i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi})}{1 - i^{\boldsymbol{m}-\mathbf{1}}(\pi)} + i^{\boldsymbol{m}-\mathbf{1}}(\bar{\pi}).$$

We can choose a ideal $\mathfrak{a}$ relatively prime to $6p$ such that we have $N\mathfrak{a} - \chi_1^{1-m_1}(\sigma_{\mathfrak{a}}) \not\equiv 0 \bmod p$. Hence, as in the previous case, the nontriviality of $\kappa_{\boldsymbol{m}} \bmod p$ is equivalent to that of $\epsilon_{\boldsymbol{m},1,\mathfrak{a}} \in E_{(1,0)}/E_{(1,0)}^p$.

Proposition 5.5. *Let $\boldsymbol{m} = (m_1, m_2) \in I$.*

1. *Suppose that $m_2 = 1$. If the class number of $K(\mathfrak{p})$ is not divisible by p, then $\kappa_{\boldsymbol{m}}$ is surjective (in particular, nontrivial).*
2. *Suppose that $m_1 = 1$. If the class number of $K(\bar{\mathfrak{p}})$ is not divisible by p, then $\kappa_{\boldsymbol{m}}$ is surjective (in particular, nontrivial).*

Proof. We prove the first assertion. As in Remark 2.9, $C(K(\mathfrak{p}))$ is generated by $\theta_{\mathfrak{a}}(\bar{\pi}\omega_{1,1})^{\sigma-1}$, where $\mathfrak{a}$ runs through the ideals of O_K with $(\mathfrak{a}, 6\mathfrak{p}) = 1$ and σ through $\mathrm{Gal}(K(\mathfrak{p})/K)$. The same argument as the proof of Proposition 5.2 shows that $\chi^{\mathbf{1}-(m_1,1)} = \chi_1^{1-m_1}$-isotypic component of the image of $C(K(\mathfrak{p}))$ in $E_{(1,0)}/E_{(1,0)}^p$ is generated by $\epsilon_{\boldsymbol{m},1,\mathfrak{a}}$ for an ideal $\mathfrak{a}$ which is prime to $6\mathfrak{p}$ and $N\mathfrak{a} - \chi_1^{1-m_1}(\sigma_{\mathfrak{a}}) \not\equiv 0 \bmod p$. Thus the result follows from Theorem 2.6. □

Now we finally prove the following two theorems, which are analogues of Theorem 1.1 (3).

Theorem 5.6. *The following two assertions are equivalent.*

1. *The elliptic Soulé characters $\kappa_{(m,1)}$ are surjective for all $(m,1) \in I$.*
2. *The class number of the mod-$\mathfrak{p}$ ray class field $K(\mathfrak{p})$ is not divisible by p.*

A similar equivalence also holds for $K(\bar{\mathfrak{p}})$.

Proof. We have that (2) implies (1) by Proposition 5.4 and 5.5. Moreover, if (1) holds, then the argument in Section 5.4 shows that image of $C(K(\mathfrak{p}))$ generates $E_{(1,0)}/E_{(1,0)}^p$. Hence (2) also holds by Theorem 2.6. □

Remark 5.7. *The elliptic Soulé characters $\kappa_{\boldsymbol{m}}$ are surjective for all $\boldsymbol{m} \in I$ such that $\boldsymbol{m} \not\equiv \mathbf{1} \bmod p-1$ if the class number of $K(p)$ is not divisible by p and there exists a unique prime of $K(p)$ above $\mathfrak{p}$ by Proposition 5.2-5.5. We cannot prove the converse at the writing of this paper. The problem is that the $\chi^{\mathbf{1}}$-component of E_1/E_1^p may be bigger than that of $C(K(p))/C(K(p)) \cap E_1^p$ even if $\kappa_{(p-1,p-1)}$ is surjective. This can happen only if the latter group coincides with μ_p.*

References

[dS87] Ehud de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol. 3, Academic Press, Inc., Boston, MA, 1987, p-adic L functions.

[Iha86] Yasutaka Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. of Math. (2) **123** (1986), no. 1, 43–106.

[Iha02] ———, *Some arithmetic aspects of Galois actions in the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 247–273.

[IKY87] Yasutaka Ihara, Masanobu Kaneko, and Atsushi Yukinari, *On some properties of the universal power series for Jacobi sums*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 65–86.

[IS87] H. Ichimura and K. Sakaguchi, *The nonvanishing of a certain Kummer character χ_m (after C. Soulé), and some related topics*, Galois representations and arithmetic algebraic geometry (Kyoto, 1985/Tokyo, 1986), Adv. Stud. Pure Math., vol. 12, North-Holland, Amsterdam, 1987, pp. 53–64.

[Jan89] Uwe Jannsen, *On the l-adic cohomology of varieties over number fields and its Galois cohomology*, Galois groups over $\mathbf{Q}$ (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 315–360.

[Kin01] Guido Kings, *The Tamagawa number conjecture for CM elliptic curves*, Invent. Math. **143** (2001), no. 3, 571–627.

[Kuc11] Omer Kucuksakalli, *Class numbers of ray class fields of imaginary quadratic fields*, Math. Comp. **80** (2011), no. 274, 1099–1122.

[Mil06] J. S. Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006. MR 2261462

[MW84] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.

[Nak95] Hiroaki Nakamura, *On exterior Galois representations associated with open elliptic curves*, J. Math. Sci. Univ. Tokyo **2** (1995), no. 1, 197–231.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[Rub91] Karl Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[Rub99] ———, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 167–234.

[Sch15] Ulrich Schmitt, *A comparison of elliptic units in certain prime power conductor cases*, Acta Arith. **171** (2015), no. 1, 39–65.

[Sha02] Romyar T. Sharifi, *Relationships between conjectures on the structure of pro-p Galois groups unramified outside p*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 275–284.

[Sou79] C. Soulé, *K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979), no. 3, 251–295.

[Sou81] Christophe Soulé, *On higher p-adic regulators*, Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980), Lecture Notes in Math., vol. 854, Springer, Berlin-New York, 1981, pp. 372–401.

[Sou87] ———, *p-adic K-theory of elliptic curves*, Duke Math. J. **54** (1987), no. 1, 249–269.

[Win90] Kay Wingberg, *On the étale K-theory of an elliptic curve with complex multiplication for regular primes*, Canad. Math. Bull. **33** (1990), no. 2, 145–150.

[Yag82] Rodney I. Yager, *A Kummer criterion for imaginary quadratic fields*, Compositio Math. **47** (1982), no. 1, 31–42.