ASIAN J. MATH.
Vol. 23, No. 3, pp. 383–400, June 2019

002

ANALOGUES OF IWASAWA'S $\mu = 0$ CONJECTURE AND THE WEAK LEOPOLDT CONJECTURE FOR A NON-CYCLOTOMIC $\mathbb{Z}_2$-EXTENSION*

JUNHWA CHOI†, YUKAKO KEZUKA‡, AND YONGXIONG LI§

Abstract. Let $K = \mathbb{Q}(\sqrt{-q})$, where q is any prime number congruent to 7 modulo 8, and let $\mathcal{O}$ be the ring of integers of K. The prime 2 splits in K, say $2\mathcal{O} = \mathfrak{p}\mathfrak{p}^*$, and there is a unique $\mathbb{Z}_2$-extension K_∞ of K which is unramified outside $\mathfrak{p}$. Let H be the Hilbert class field of K, and write $H_\infty = HK_\infty$. Let $M(H_\infty)$ be the maximal abelian 2-extension of H_∞ which is unramified outside the primes above $\mathfrak{p}$, and put $X(H_\infty) = \mathrm{Gal}(M(H_\infty)/H_\infty)$. We prove that $X(H_\infty)$ is always a finitely generated $\mathbb{Z}_2$-module, by an elliptic analogue of Sinnott's cyclotomic argument. We then use this result to prove for the first time the weak $\mathfrak{p}$-adic Leopoldt conjecture for the compositum J_∞ of K_∞ with arbitrary quadratic extensions J of H. We also prove some new cases of the finite generation of the Mordell-Weil group $E(J_\infty)$ modulo torsion of certain elliptic curves E with complex multiplication by $\mathcal{O}$.

Key words. Iwasawa theory, weak Leopoldt conjecture, Iwasawa μ-invariant, elliptic curves, complex multiplication.

Mathematics Subject Classification. Primary 11R23; Secondary 11G05, 11G15.

1. Introduction. Let $K = \mathbb{Q}(\sqrt{-q})$, where q is any prime number congruent to 7 modulo 8, let $\mathcal{O}$ be the ring of integers of K, and let H be the Hilbert class field of K. We fix once and for all an embedding of K into $\mathbb{C}$. By the theory of complex multiplication, we have $H = K(j(\mathcal{O}))$ where j is the classical modular function; in particular, this fixes an embedding of H into $\mathbb{C}$. We write G for the Galois group of H over K, and h for the class number of K. Then h is odd because K has prime discriminant. The prime $p = 2$ splits in K, and we write

$$2\mathcal{O} = \mathfrak{p}\mathfrak{p}^*.$$

Throughout the remainder of the paper, we fix once and for all an embedding $\iota_\mathfrak{p}$ of $\overline{K}$ into $\mathbb{C}_2$, which induces the prime $\mathfrak{p}$. By global class field theory, K has a unique $\mathbb{Z}_2$-extension which is unramified outside $\mathfrak{p}$, which we denote by K_∞/K. Note that the prime $\mathfrak{p}$ is totally ramified in K_∞ because h is odd. Define

$$H_\infty = HK_\infty,\ \Gamma = \mathrm{Gal}(H_\infty/H).$$

We write $M(H_\infty)$ for the maximal abelian 2-extension of H_∞ which is unramified outside the primes of H_∞ above $\mathfrak{p}$, and put

$$X(H_\infty) = \mathrm{Gal}(M(H_\infty)/H_\infty).$$

Note that $M(H_\infty)$ is clearly Galois over H, and thus Γ acts continuously on $X(H_\infty)$ in the usual fashion via inner automorphisms. This action endows $X(H_\infty)$ with the

*Received November 1, 2017; accepted for publication November 22, 2017.
†School of Mathematics, Korea Institute for Advanced Study, Seoul, Republic of Korea (jhchoi.math@gmail.com).
‡Fakultät für Mathematik, Universität Regensburg, Regensburg, Germany (Yukako.Kezuka@mathematik.uni-regensburg.de).
§Yau Mathematical Sciences Center, Tsinghua University, Beijing, China (liyx_1029@tsinghua.edu.cn).

structure of a module over the Iwasawa algebra $\Lambda(\Gamma)$ of Γ. In fact, it has long been known that $X(H_\infty)$ is a finitely generated torsion module over $\Lambda(\Gamma)$. In the present paper, we prove the following stronger theorem, which is equivalent to saying that the Iwasawa μ-invariant for the $\Lambda(\Gamma)$-module $X(H_\infty)$ vanishes.

THEOREM 1.1. *The Galois group $X(H_\infty)$ is a finitely generated $\mathbb{Z}_2$-module.*

In §5, we give some interesting numerical computations of the group $X(H_\infty)$, which show, somewhat surprisingly, that in fact it is zero for all primes $q < 500$ with $q \equiv 7 \bmod 8$ except $q = 431$. Moreover, by a simple application of Nakayama's lemma, we obtain the following corollary of Theorem 1.1. Let J denote any quadratic extension of the Hilbert class field H, and write $J_\infty = JK_\infty$. Let $M(J_\infty)$ be the maximal abelian 2-extension of J_∞ which is unramified outside the primes above $\mathfrak{p}$, and put $X(J_\infty) = \mathrm{Gal}(M(J_\infty)/J_\infty)$.

COROLLARY 1.2. *For every quadratic extension J of H, the Galois group $X(J_\infty)$ is a finitely generated $\mathbb{Z}_2$-module.*

We point out that this corollary implies in particular (see [4]) that the weak $\mathfrak{p}$-adic Leopoldt conjecture is valid for the $\mathbb{Z}_2$-extension J_∞/J. This is the first example where such a weak $\mathfrak{p}$-adic Leopoldt conjecture has been proven for extensions of K which are not in general abelian over K.

In the proof of Theorem 1.1, we shall make use of what is, in some sense, the simplest elliptic curve with complex multiplication by $\mathcal{O}$, which was introduced by Gross [14]. He has proven that there exists a unique elliptic curve defined over $\mathbb{Q}(j(\mathcal{O}))$, which we shall denote by A, whose j-invariant is equal to $j(\mathcal{O})$, whose ring of H-endomorphisms is equal to $\mathcal{O}$, whose minimal discriminant ideal in H is equal to $(-q^3)$, and which is isogenous to all of its conjugates under the Galois action of G. The Grössencharacter of A is the Hecke character ψ of H with conductor $(\sqrt{-q})$, which, on ideals $\mathfrak{a}$ of H prime to $(\sqrt{-q})$ is defined by the formula

$$\psi(\mathfrak{a}) = \alpha, \text{ where } (\alpha) = N_{H/K}\mathfrak{a} \text{ and } \alpha \text{ is a square modulo } (\sqrt{-q}).$$

We have the identity

$$\psi = \phi \circ N_{H/K} \tag{1.1}$$

where ϕ is the following Grössencharacter of K with conductor $\mathfrak{q} = \sqrt{-q}\mathcal{O}$. Let B denote the abelian variety over K, which is the restriction of scalars from H to K of A. Let $T = \mathrm{End}_K(B) \otimes \mathbb{Q}$. Then T is an extension of degree h of K, and for ideals $\mathfrak{b}$ of K prime to $\mathfrak{q}$ we have $\phi(\mathfrak{b}) = \beta$, where β is the unique element of T such that $\mathfrak{b}^h = (\beta^h)$ and β^h is a square modulo $\mathfrak{q}$. In particular, we remark that B is isomorphic over H to the product of the elliptic curves A^σ, where σ runs over the element of G. It follows that for any integral ideal $\mathfrak{b}$ of K prime to $\mathfrak{q}$, the endomorphism $\phi(\mathfrak{b})$ of B/K defines a unique isogeny defined over H

$$\eta_{A^\sigma}(\mathfrak{b}) : A^\sigma \to A^{\sigma\sigma_{\mathfrak{b}}} \tag{1.2}$$

where $\sigma_{\mathfrak{b}}$ denotes the Artin symbol of $\mathfrak{b}$ in G, whose kernel is $A^\sigma_{\mathfrak{b}}$. For a more detailed discussion on this isogeny, see [14]. Moreover, Gross [15] has proven that A has a global minimal Weierstrass equation over H. Hence we fix once and for all such a global minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.3}$$

with coefficients a_i which are all integers in H. Moreover, there is an interesting new application of Corollary 1.2 to certain quadratic twists of A. Let E denote a twist of A by an arbitrary quadratic extension of H, whose conductor is relatively prime to $2q$. Define

$$F = H(E_{\mathfrak{p}^2}),\ F_\infty = H(E_{\mathfrak{p}^\infty}),\ \mathcal{G} = \mathrm{Gal}(F_\infty/H),\ \Delta = \mathrm{Gal}(F/H). \tag{1.4}$$

The fields F and F_∞ are, of course, abelian extensions of H, but we stress that they are not in general abelian over K. Here Δ is cyclic of order 2, and it can easily be seen that $F_\infty = FK_\infty$. We recall that the $\mathfrak{p}^\infty$-Selmer group of E over F_∞ is defined by

$$S_{\mathfrak{p}^\infty}(E/F_\infty) = \mathrm{Ker}\left(H^1(F_\infty, E_{\mathfrak{p}^\infty}) \to \prod_v H^1(F_{\infty,v}, E)(\mathfrak{p})\right)$$

where v runs over all finite places of F_∞.

THEOREM 1.3. *Let E be a twist of A by any quadratic extension of H of conductor prime to $2q$. Then the Pontrjagin dual of $S_{\mathfrak{p}^\infty}(E/F_\infty)$ is always a finitely generated $\mathbb{Z}_2$-module. In particular, both $E(F_\infty)$ and $E(H_\infty)$ modulo torsion are finitely generated abelian groups.*

We stress that this result was unknown previously, except in the very special case when E is the quadratic twist of A by the compositum with H of a quadratic extension of K. Moreover, none of the analytic results is known for such a curve E, for example, the construction of the $\mathfrak{p}$-adic L-function attached to E.

Our proof of Theorem 1.1 uses an elliptic analogue of Sinnott's beautiful proof of the vanishing of the cyclotomic μ-invariant. Considerable past work in this direction has already been done by Gillard [12], [11] and Schneps [17] for split odd primes p. For the prime $p = 2$ there has recently been independent work by Oukhaba and Viguié [18], which would seemingly include a proof of Theorem 1.1. However, we give the full details of a rather different construction of the $\mathfrak{p}$-adic L-functions and the analogue of Sinnott's proof in our case, rather than the arguments sketched in [18].

2. Construction of the $\mathfrak{p}$-adic L-function. The aim of this section is to construct the $\mathfrak{p}$-adic L-function attached to the curve A/H, by using the method of [9] and [6]. In this section, F and F_∞ will denote the fields defined by (1.4) in the special case in which $E = A$. Thus, we will have

$$F = H(A_{\mathfrak{p}^2}),\ F_\infty = H(A_{\mathfrak{p}^\infty}).$$

Write $\chi_{\mathfrak{p}} : \mathcal{G} \to \mathcal{O}_{\mathfrak{p}}^\times = \mathbb{Z}_2^\times$ for the character giving the action of $\mathcal{G} = \mathrm{Gal}(F_\infty/H)$ on $A_{\mathfrak{p}^\infty}$. It is well-known that A has good reduction everywhere over F (the proof of Lemma 2.1 of [3] generalizes immediately to all of the curves A discussed here). Thus we must have $[F : H] = 2$, whence we see that $\chi_{\mathfrak{p}}$ is an isomorphism. Hence $\mathcal{G} = \Gamma \times \Delta$, where $\Delta = \mathrm{Gal}(F/H)$ is of order 2 and $\Gamma = \mathrm{Gal}(F_\infty/F)$ is isomorphic to $\mathbb{Z}_2$. Note that all the primes of H lying above the $\mathfrak{q}$ must be ramified in the extension F/H, because A/H has bad reduction at the primes of H above $\mathfrak{q}$. As H_∞/H is unramified outside of the primes of H dividing $\mathfrak{p}$, we see that $H_\infty \cap F = H$, whence we can also identify Γ with the Galois group of H_∞/H under restriction.

Recall that G denotes the Galois group of H over K. Let $\mathfrak{a}$ be any non-zero integral ideal of K, which we will always assume is prime to $\mathfrak{pq}$. We write $\sigma_{\mathfrak{a}}$ for the Artin symbol of $\mathfrak{a}$ in G, and $A^{\mathfrak{a}}$ for the image of A under $\sigma_{\mathfrak{a}}$. A global minimal Weierstrass equation for $A^{\mathfrak{a}}/H$, and its associated Néron differential $\omega^{\mathfrak{a}}$, are given respectively by just applying $\sigma_{\mathfrak{a}}$ to the coefficients of the equation (1.3), and to the coefficients of its Néron differential $\omega = dx/(2y+a_1x+a_3)$. We then define an element $\xi(\mathfrak{a})$ of H by the equation

$$\eta_A(\mathfrak{a})^*(\omega^{\mathfrak{a}}) = \xi(\mathfrak{a})\omega, \tag{2.1}$$

where $\eta_A(\mathfrak{a}) : A \to A^{\mathfrak{a}}$ is the isogeny as defined in (1.2). We also write $\mathcal{L}$ and $\mathcal{L}_{\mathfrak{a}}$ for the period lattices of ω and $\omega_{\mathfrak{a}}$. If we write $\mathcal{L} = \Omega_\infty\mathcal{O}$ where $\Omega_\infty \in \mathbb{C}$, then we have $\mathcal{L}_{\mathfrak{a}} = \xi(\mathfrak{a})\Omega_\infty\mathfrak{a}^{-1}$. Note that the Weierstrass isomorphism $\mathfrak{M}(z, \mathcal{L}_{\mathfrak{a}})$ from $\mathbb{C}/\mathcal{L}_{\mathfrak{a}}$ to $A^{\mathfrak{a}}(\mathbb{C})$ is given by

$$\left(\wp(z,\mathcal{L}_{\mathfrak{a}}) - \frac{a_{1,\mathfrak{a}}^2 + 4a_{2,\mathfrak{a}}}{12},\ \frac{1}{2}\left(\wp'(z,\mathcal{L}_{\mathfrak{a}}) - a_{1,\mathfrak{a}}\left(\wp(z,\mathcal{L}_{\mathfrak{a}}) - \frac{a_{1,\mathfrak{a}}^2 + 4a_{2,\mathfrak{a}}}{12}\right) - a_{3,\mathfrak{a}}\right)\right)$$

where we simply write $a_{i,\mathfrak{a}}$ for $\sigma_{\mathfrak{a}}(a_i)$, and where $\wp(z, \mathcal{L}_{\mathfrak{a}})$ denotes the Weierstrass $\wp$-function of the lattice $\mathcal{L}_{\mathfrak{a}}$.

Let $P = (x, y)$ denote a generic point of our global minimal Weierstrass equation for $A^{\mathfrak{a}}/H$. Given any non-zero element λ of $\mathcal{O} = \mathrm{End}_H(A)$ with $\lambda \neq \pm 1$ and $(\lambda, 6\mathfrak{q}) = 1$, we define the rational function $R_{\lambda,\mathfrak{a}}(P)$ on $A^{\mathfrak{a}}$, with coefficients in H, by

$$R_{\lambda,\mathfrak{a}}(P) = c_{\mathfrak{a}}(\lambda) \prod_{M \in V_\lambda} (x(P) - x(M))^{-1}$$

where V_λ denotes any set of representatives of the non-zero λ-division points on $A^{\mathfrak{a}}$ modulo $\{\pm 1\}$, and $c_{\mathfrak{a}}(\lambda)$ is a unique 12-th root in H of $\Delta(\mathcal{L}_{\mathfrak{a}})^{N\lambda}/\Delta(\lambda^{-1}\mathcal{L}_{\mathfrak{a}})$ (see also Proposition 1 of the Appendix of [5]). Here Δ denotes Ramanujan's Δ-function. For each non-zero integral ideal $\mathfrak{b}$ of K with $(\mathfrak{b}, \lambda\mathfrak{q}) = 1$, it is easily seen that we have (see Theorem 4 of the Appendix of [5])

$$R_{\lambda,\mathfrak{ab}}(\eta_{A^{\mathfrak{a}}}(\mathfrak{b})(P)) = \prod_{U \in A^{\mathfrak{a}}_{\mathfrak{b}}} R_{\lambda,\mathfrak{a}}(P \oplus U). \tag{2.2}$$

We introduce the index set $\mathcal{I}$ consisting of all finite sets $\rho = \{(\lambda_i, n_i) \mid i = 1, \cdots, r\}$ where $r \geq 2$, $n_i \in \mathbb{Z}$, $\lambda_i \neq \pm 1$ non-zero elements of $\mathcal{O}$ with $(\lambda_i, 6\mathfrak{q}) = 1$, and satisfying $\sum_{i=1}^r n_i(N\lambda_i - 1) = 0$. Here $N\lambda_i$ denotes the norm from K to $\mathbb{Q}$ of λ_i. Given $\rho \in \mathcal{I}$, we consider the product

$$\mathfrak{R}_{\rho,\mathfrak{a}}(P) = \prod_{i=1}^r R_{\lambda_i,\mathfrak{a}}(P)^{n_i}, \tag{2.3}$$

which is also a rational function on $A^{\mathfrak{a}}/H$. Under the Weierstrass isomorphism, this rational function can be considered as a function on $\mathbb{C}/\mathcal{L}_{\mathfrak{a}}$ with variable z. Taking the derivative logarithm of this function, we have the following result.

Proposition 2.1. *We have*

$$\frac{d}{dz}\log \mathfrak{R}_{\rho,\mathfrak{a}}(P) = \sum_{i=1}^r \sum_{k=2,\ even}^\infty -n_i \frac{\phi^k(\mathfrak{a})}{\xi(\mathfrak{a})^k\Omega_\infty^k}\left(N\lambda_i - \lambda_i^k\right) L(\bar{\phi}^k, \sigma_{\mathfrak{a}}, k) z^{k-1}.$$

In particular, for each even integer $k > 0$, we have

$$\left(\frac{d}{dz}\right)^k \log \mathfrak{R}_{\rho,\mathfrak{a}}(P)\Big|_{z=0} = B_\rho(k)(k-1)!\frac{\phi^k(\mathfrak{a})}{\xi(\mathfrak{a})^k\Omega_\infty^k}L(\bar{\phi}^k, \sigma_\mathfrak{a}, k) \tag{2.4}$$

where $B_\rho(k) = \sum_{i=1}^r -n_i\left(N\lambda_i - \lambda_i^k\right)$.

Proof. We recall the basic properties of Kronecker–Eisenstein series and elliptic functions, which are fully discussed in [13]. Let z and s be complex variables. For any lattice L in $\mathbb{C}$, we define the Kronecker–Eisenstein series by

$$H_k(z, s, L) = \sum_{w \in L} \frac{(\bar{z} + \bar{w})^k}{|z + w|^{2s}}$$

where the sum is taken over all $w \in L$, except $-z$ if $z \in L$. It defines a holomorphic function of s in the half plane $\mathrm{Re}(s) > 1 + k/2$, and has an analytic continuation to the whole s-plane. In particular, for each $k \geq 3$, $G_k(L) = H_k(0, k, L)$ is a classic holomorphic Eisenstein series of weight k. For the convention, we will denote by

$$G_1(L) = 0,\ G_2(L) = \lim_{s \to 0+} \sum_{w \in L\setminus\{0\}} w^{-2}|w|^{-2s}.$$

Let $\sigma(z, L)$ denote the Weierstrass σ-function. We define a non-holomorphic function $\theta(z, L)$ by

$$\theta(z, L) = \exp\left(-G_2(L)\frac{z^2}{2}\right)\sigma(z, L).$$

Then θ possesses a Taylor expansion of the logarithmic derivative of $\theta(z, L)$ as

$$\frac{d}{dz}\log\theta(z, L) = \sum_{k=1}^\infty (-1)^{k-1}G_k(L)z^{k-1} = \sum_{k=2,\ \text{even}}^\infty -G_k(L)z^{k-1},$$

where the second equality follows from $G_k(L) = 0$ for k odd.

Moreover, we have the identity

$$\theta^2(z, L)^{N\lambda}/\theta^2(z, \lambda^{-1}L) = \prod_{0 \neq w \in \lambda^{-1}L/L} (\wp(z, L) - \wp(w, L))^{-1} \tag{2.5}$$

for any non-zero element λ of $\mathcal{O}$. Hence, one gives another expression of the rational function $\mathfrak{R}_{\rho,\mathfrak{a}}(P) = \mathfrak{R}_{\rho,\mathfrak{a}}(\mathfrak{M}(z, \mathcal{L}_\mathfrak{a}))$ as

$$\mathfrak{R}_{\rho,\mathfrak{a}}(\mathfrak{M}(z, \mathcal{L}_\mathfrak{a}))^2 = \prod_{i=1}^r \left(c_\mathfrak{a}(\lambda_i)\frac{\theta^2(z, \mathcal{L}_\mathfrak{a})^{N\lambda_i}}{\theta^2(z, \lambda_i^{-1}\mathcal{L}_\mathfrak{a})}\right)^{n_i}.$$

It follows that

$$\begin{aligned}\frac{d}{dz}\log\mathfrak{R}_{\rho,\mathfrak{a}}(\mathfrak{M}(z, \mathcal{L}_\mathfrak{a})) &= \sum_{i=1}^r n_i\left(N\lambda_i\frac{d}{dz}\log\theta(z, \mathcal{L}_\mathfrak{a}) - \frac{d}{dz}\log\theta(z, \lambda_i^{-1}\mathcal{L}_\mathfrak{a})\right) \\ &= \sum_{i=1}^r \sum_{k=2,\,\text{even}}^\infty -n_i\left(N\lambda_i G_k(\mathcal{L}_\mathfrak{a}) - \lambda_i^k G_k(\mathcal{L}_\mathfrak{a})\right)z^{k-1}.\end{aligned} \tag{2.6}$$

Finally, Proposition 5.5 in [13] shows that the partial Hecke L-function $L(\bar{\phi}^k, \sigma_{\mathfrak{a}}, s)$ decomposes into Kronecker–Eisenstein series $H_k(z, s, \mathcal{L}_{\mathfrak{a}})$. In particular, we have

$$G_k(\mathcal{L}_{\mathfrak{a}}) = \frac{\phi^k(\mathfrak{a})}{\xi(\mathfrak{a})^k \Omega_\infty^k} L(\bar{\phi}^k, \sigma_{\mathfrak{a}}, k).$$

Applying this equality to (2.6), this completes the proof of the proposition. ☐

Now we define the rational function $\mathfrak{I}_{\rho,\mathfrak{a}}(P)$ on A/H by

$$\mathfrak{I}_{\rho,\mathfrak{a}}(P) = \mathfrak{R}_{\rho,\mathfrak{a}}(P)^2 / \mathfrak{R}_{\rho,\mathfrak{a}\mathfrak{p}}(\eta_{A^{\mathfrak{a}}}(\mathfrak{p})(P)).$$

Clearly, it follows from (2.2) that

$$\prod_{V \in A^{\mathfrak{a}}_{\mathfrak{p}}} \mathfrak{I}_{\rho,\mathfrak{a}}(P \oplus V) = 1.$$

Let v be the prime of H lying above $\mathfrak{p}$. Let $\mathfrak{m}_v$ be the maximal ideal of the ring $\mathcal{O}_v$ of integers of the completion H_v. For the elliptic curve $A^{\mathfrak{a}}/H$, we denote by $\widehat{A^{\mathfrak{a},v}}$ the formal group of $A^{\mathfrak{a}}$ at v. We denote by $t = -x/y$ the parameter of this formal group.

LEMMA 2.2. *Let $\mathfrak{D}_{\rho,\mathfrak{a}}(t)$ denote the t-expansion of the rational function $\mathfrak{I}_{\rho,\mathfrak{a}}(P)$. Then $\mathfrak{D}_{\rho,\mathfrak{a}}(t)$ lies in $1+\mathfrak{m}_v[[t]]$. In particular, we can define $m_{\rho,\mathfrak{a}}(t) = \frac{1}{2}\log(\mathfrak{D}_{\rho,\mathfrak{a}}(t))$, which lies in $\mathcal{O}_v[[t]]$.*

Proof. Let $D_{\lambda_i,\mathfrak{a}}(t) = \sum_{n\geq 0} d_n t^n$ denote the t-expansion of the rational function $R_{\lambda_i,\mathfrak{a}}(P)$. We use a classical result (see Lemma 23 of [8]) that $D_{\lambda_i,\mathfrak{a}}(t)$ is a unit in $\mathcal{O}_v[[t]]$. Writing

$$\widehat{\eta_{A^{\mathfrak{a}}}(\mathfrak{p})}(t) : \widehat{A^{\mathfrak{a},v}} \to \widehat{A^{\mathfrak{a}\mathfrak{p},v}}$$

for the formal power series induced by the isogeny $\eta_{A^{\mathfrak{a}}}(\mathfrak{p})$, we have $\widehat{\eta_{A^{\mathfrak{a}}}(\mathfrak{p})}(t) \equiv t^2 \bmod \mathfrak{m}_v$. Since $(\lambda_i, \mathfrak{p}) = 1$, it follows that

$$D_{\lambda_i,\mathfrak{a}\mathfrak{p}}(\widehat{\eta_{A^{\mathfrak{a}}}(\mathfrak{p})}(t)) = \sum_{n\geq 0} d_n^{\sigma_{\mathfrak{p}}} (\widehat{\eta_{A^{\mathfrak{a}}}(\mathfrak{p})}(t))^n \equiv \sum_{n\geq 0} d_n^2 t^{2n} \bmod \mathfrak{m}_v.$$

Hence the lemma follows immediately, since

$$D_{\lambda_i,\mathfrak{a}}(t)^2 = (\sum_{n\geq 0} d_n t^n)^2 \equiv \sum_{n\geq 0} d_n^2 t^{2n} \bmod \mathfrak{m}_v.$$

☐

Let $\mathcal{I}_{\mathfrak{p}}$ denotes the ring of integers of the completion of the maximal unramified extension of $K_{\mathfrak{p}}$. As $\widehat{A^v}$ has height 1 as a formal group, there exists an isomorphism over $\mathcal{I}_{\mathfrak{p}}$

$$\beta_v : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{A^v},$$

where $\widehat{\mathbb{G}}_m$ denotes the formal multiplicative group with parameter w. For each non-zero integral ideal $\mathfrak{a}$ of K with $(\mathfrak{a}, \mathfrak{p}) = 1$, the isogeny $\eta_A(\mathfrak{a}) : A \to A^{\mathfrak{a}}$ induces an isomorphism from $\widehat{A^v}$ onto $\widehat{A^{\mathfrak{a},v}}$, and hence we have an isomorphism over $\mathcal{I}_{\mathfrak{p}}$

$$\beta_v^{\mathfrak{a}} : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{A^{\mathfrak{a},v}}, \ \beta_v^{\mathfrak{a}} = \widehat{\eta_A(\mathfrak{a})} \circ \beta_v.$$

The isomorphism $\beta_v^{\mathfrak{a}}$ is given by a power series $t = \beta_v^{\mathfrak{a}}(w)$ with coefficients in $\mathcal{I}_{\mathfrak{p}}$. We write $\Omega_{\mathfrak{a},v}$ for the coefficient of w in this power series.

LEMMA 2.3. *We have* $\Omega_{\mathfrak{a},v} = \xi(\mathfrak{a})\Omega_v$.

Proof. Viewing z as a parameter of the formal additive group $\widehat{\mathbb{G}}_a$, we have the exponential map $\mathcal{E}(z, \mathcal{L})$ of $\widehat{A^v}$ is given by the formal power series

$$t = \mathcal{E}(z, \mathcal{L}) = -\frac{2\wp(z, \mathcal{L}) - (a_1^2 + 4a_2)/12}{\wp'(z, \mathcal{L}) - a_1\left(\wp(z, \mathcal{L}) - (a_1^2 + 4a_2)/12\right) - a_3}.$$

Similarly, let $\mathcal{E}(z, \mathcal{L}_{\mathfrak{a}})$ be defined analogously for the formal group $\widehat{A^{\mathfrak{a},v}}$ by using the Weierstrass isomorphism $\mathfrak{W}(z, \mathcal{L}_{\mathfrak{a}})$. By the uniqueness of the exponential map for a formal group, we have

$$\beta_v(e^{z/\Omega_v} - 1) = \mathcal{E}(z, \mathcal{L}),\ \beta_v^{\mathfrak{a}}(e^{z/\Omega_{\mathfrak{a},v}} - 1) = \mathcal{E}(z, \mathcal{L}_{\mathfrak{a}}).$$

On the other hand, as $\eta_A(\mathfrak{a})(\mathfrak{W}(z, \mathcal{L})) = \mathfrak{W}(\xi(\mathfrak{a})z, \mathcal{L}_{\mathfrak{a}})$, we have $\widehat{\eta_A(\mathfrak{a})}(\mathcal{E}(z, \mathcal{L})) = \mathcal{E}(\xi(\mathfrak{a})z, \mathcal{L}_{\mathfrak{a}}))$. The lemma then follows by comparing the first coefficients of the last equality on both sides. ◻

We now define the formal power series $\mathfrak{B}_{\rho,\mathfrak{a}}(w)$ in $\mathcal{I}_{\mathfrak{p}}[[w]]$ by

$$\mathfrak{B}_{\rho,\mathfrak{a}}(w) = m_{\rho,\mathfrak{a}}(\beta_v^{\mathfrak{a}}(w)),$$

and let $\nu_{\rho,\mathfrak{a}}$ be the $\mathcal{I}_{\mathfrak{p}}$-valued measure on $\mathbb{Z}_2$ associated to $\mathfrak{B}_{\rho,\mathfrak{a}}(w)$. Indeed, let $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathfrak{G})$ denotes the ring of $\mathcal{I}_{\mathfrak{p}}$-valued measures on a profinite group $\mathfrak{G}$. Then $\nu_{\rho,\mathfrak{a}}$ is determined by Mahler's theorem that there exists the ring isomorphism

$$\mathcal{M} : \Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathbb{Z}_2) \xrightarrow{\sim} \mathcal{I}_{\mathfrak{p}}[[w]],\ \mathcal{M}(\nu) = \sum_{n\geq 0}\left(\int_{\mathbb{Z}_2}\binom{x}{n}d\nu\right)w^n = \int_{\mathbb{Z}_2}(1+w)^x d\nu. \tag{2.7}$$

Now we have the inclusion $i : \Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathbb{Z}_2^\times) \hookrightarrow \Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathbb{Z}_2)$ given by extending a measure on $\mathbb{Z}_2^\times$ to $\mathbb{Z}_2$ by zero. By (2.2) we have

$$\sum_{\zeta\in\{\pm 1\}} \mathfrak{B}_{\rho,\mathfrak{a}}(\zeta(1+w) - 1) = 0,$$

whence the measure $\nu_{\rho,\mathfrak{a}}$ belongs to $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathbb{Z}_2^\times)$. Thus the measure $\nu_{\rho,\mathfrak{a}}$ can be viewed as an element of $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathcal{G})$ via the isomorphism $\chi_{\mathfrak{p}} : \mathcal{G} \xrightarrow{\sim} \mathbb{Z}_2^\times$. For all $k \geq 0$, we have

$$\int_{\mathcal{G}} \chi_{\mathfrak{p}}^k d\nu_{\rho,\mathfrak{a}} = \int_{\mathbb{Z}_2} x^k d\nu_{\rho,\mathfrak{a}} = D^k\mathfrak{B}_{\rho,\mathfrak{a}}(w)\Big|_{w=0} = \left(\frac{d}{dz}\right)^k \mathfrak{B}_{\rho,\mathfrak{a}}(e^z - 1)\Big|_{z=0},$$

where $D = (1+w)\frac{d}{dw}$. It is equal to

$$\Omega_{\mathfrak{a},v}^k\left(\frac{d}{dz}\right)^k \mathfrak{B}_{\rho,\mathfrak{a}}(e^{z/\Omega_{\mathfrak{a},v}} - 1)\Big|_{z=0} = \frac{1}{2}\Omega_{\mathfrak{a},v}^k\left(\frac{d}{dz}\right)^k \log \mathfrak{I}_{\rho,\mathfrak{a}}(\mathfrak{W}(z, \mathcal{L}_{\mathfrak{a}}))\Big|_{z=0}.$$

LEMMA 2.4. *For each even integer* $k > 0$, *we have*

$$\Omega_v^{-k}\int_{\mathcal{G}} \chi_{\mathfrak{p}}^k d\nu_{\rho,\mathfrak{a}} = B_\rho(k)(k-1)!\phi^k(\mathfrak{a})\Omega_\infty^{-k}\left(L(\bar{\phi}^k, \sigma_{\mathfrak{a}}, k) - \frac{\phi^k(\mathfrak{p})}{2}L(\bar{\phi}^k, \sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}}, k)\right).$$

Proof. We have

$$\Omega_{\mathfrak{a},v}^{-k}\int_{\mathcal{G}}\chi_{\mathfrak{p}}^{k}d\nu_{\rho,\mathfrak{a}} = \left(\frac{d}{dz}\right)^{k}\log\mathfrak{R}_{\rho,\mathfrak{a}}(\mathfrak{M}(z,\mathcal{L}_{\mathfrak{a}}))\Big|_{z=0} -\frac{1}{2}\left(\frac{d}{dz}\right)^{k}\log\mathfrak{R}_{\rho,\mathfrak{ap}}(\eta_{A^{\mathfrak{a}}}(\mathfrak{p})(\mathfrak{M}(z,\mathcal{L}_{\mathfrak{a}})))\Big|_{z=0}.$$

Note that $\eta_{A^{\mathfrak{a}}}(\mathfrak{p})(\mathfrak{M}(z,\mathcal{L}_{\mathfrak{a}})) = \mathfrak{M}(\xi(\mathfrak{p})^{\sigma_{\mathfrak{a}}}z,\mathcal{L}_{\mathfrak{ap}})$ and $\xi(\mathfrak{ap}) = \xi(\mathfrak{a})\xi(\mathfrak{p})^{\sigma_{\mathfrak{a}}}$. Then the lemma follows from Proposition 2.1 and Lemma 2.3. □

We now denote by $\mathfrak{C}$ a set of integral ideals $\mathfrak{a}$ of K prime to $\mathfrak{pq}$, whose Artin symbols give precisely the Galois group $G = \mathrm{Gal}(H/K)$. There is the relation

$$L(\bar{\phi}^{k}\chi,s) = \sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})L(\bar{\phi}^{k},\sigma_{\mathfrak{a}},s),\ \forall\chi\in G^{*},$$

where G^{*} denotes the group of characters of G. Hence by Lemma 2.4, for each $\chi\in G^{*}$ we have

$$\Omega_{v}^{-k}\sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})\phi^{-k}(\mathfrak{a})\int_{\mathcal{G}}\chi_{\mathfrak{p}}^{k}d\nu_{\rho,\mathfrak{a}} = B_{\rho}(k)(k-1)!\left(1-\frac{\phi^{k}\chi^{-1}(\mathfrak{p})}{2}\right)\Omega_{\infty}^{-k}L(\bar{\phi}^{k}\chi,k).$$

We can interpret the expression on the left hand side of this formula as follows. Write $\mathscr{G}$ for the Galois group $\mathrm{Gal}(F_{\infty}/K)$. Let B_{H} denote the base extension of B to H, and let $\rho_{\mathfrak{p}}$ be the character of $\mathscr{G}$ which coincides with the character $\chi_{\mathfrak{p}}$ on $\mathcal{G}$ and describes the action of $\mathscr{G}$ on $(B_{H})_{\mathfrak{p}^{\infty}} = \prod_{\mathfrak{a}\in\mathfrak{C}}A^{\mathfrak{a}}_{\mathfrak{p}^{\infty}}$ in the following way. First, we identify $\mathscr{G}$ with $\mathcal{G}\times G$. Then for $\sigma_{\mathfrak{c}}\in G$ with $\mathfrak{c}\in\mathfrak{C}$ and $Q\in A^{\mathfrak{a}}_{\mathfrak{p}^{n}}$, we have

$$\rho_{\mathfrak{p}}(\sigma_{\mathfrak{c}})(Q) = \eta_{A^{\mathfrak{a}}}(\mathfrak{c})(Q)\in A^{\mathfrak{ac}}_{\mathfrak{p}^{n}}.$$

Hence, for $g = h\sigma_{\mathfrak{c}}\in\mathscr{G}$ with $h\in\mathcal{G}$, we have

$$\rho_{\mathfrak{p}}(g) = \chi_{\mathfrak{p}}(h)\phi(\mathfrak{c}).$$

As is shown in §3 of [2], we can fix a prime $\mathfrak{P}$ of T lying above $\mathfrak{p}$ such that $T_{\mathfrak{P}} = K_{\mathfrak{p}}$. Since $\phi(\mathfrak{a})$ is a unit at $\mathfrak{P}$, we note that the value of $\rho_{\mathfrak{p}}$ is in $K_{\mathfrak{p}}^{\times}$.

Now, let $\tau_{\mathfrak{a}}$ denote the Artin symbol of $\mathfrak{a}$ in $\mathscr{G}$ so that $\{\tau_{\mathfrak{a}}|_{H}\}_{\mathfrak{a}\in\mathfrak{C}} = \mathfrak{C}$. We define

$$\nu_{\chi}^{\circ} = \sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})\tau_{\mathfrak{a}}^{-1}\nu_{\rho,\mathfrak{a}}\in\mathcal{I}_{\mathfrak{p}}[[\mathscr{G}]] = \mathcal{I}_{\mathfrak{p}}[G][[\mathcal{G}]].$$

Note that, by Lemma I.3.4 of [10], it is independent of the choice of representatives of G in $\mathscr{G}$. It follows that

$$\Omega_{v}^{-k}\sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})\phi^{-k}(\mathfrak{a})\int_{\mathcal{G}}\chi_{\mathfrak{p}}^{k}d\nu_{\rho,\mathfrak{a}} = \Omega_{v}^{-k}\int_{\mathscr{G}}\rho_{\mathfrak{p}}^{k}d\nu_{\chi}^{\circ}.$$

THEOREM 2.5. *For each $\chi\in G^{*}$, there exists a unique $\mathcal{I}_{\mathfrak{p}}$-valued pseudo-measure ν_{χ} on $\mathscr{G} = \mathrm{Gal}(F_{\infty}/K)$ such that for each even integer $k>0$, we have*

$$\Omega_{v}^{-k}\int_{\mathscr{G}}\rho_{\mathfrak{p}}^{k}d\nu_{\chi} = (k-1)!\left(1-\frac{\phi^{k}\chi^{-1}(\mathfrak{p})}{2}\right)\Omega_{\infty}^{-k}L(\bar{\phi}^{k}\chi,k).$$

This theorem is immediately followed by the next lemma.

LEMMA 2.6. *There exists an $\mathcal{I}_{\mathfrak{p}}$-valued measure θ_ρ on $\mathscr{G}$ such that*

$$\int_{\mathscr{G}} \rho_{\mathfrak{p}}^k d\theta_\rho = B_\rho(k)$$

for all $k \geq 1$, and the restriction θ_ρ to $\Gamma = \mathrm{Gal}(F_\infty/F)$ generates the augmentation ideal of $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\Gamma)$.

Proof. This lemma is essentially the same with Lemma II. 7 of [1]. We can choose an element λ in $\mathcal{O}$ satisfying $(\lambda, 6\mathfrak{q}) = 1$ and

$$\lambda \equiv 1 \bmod \mathfrak{p}^3, \ \bar{\lambda} \equiv 1 + 2^2 \bmod \mathfrak{p}^3. \tag{2.8}$$

We set $\rho = \{(\lambda, 1), (\bar{\lambda}, -1)\} \in \mathcal{I}$ and write τ_λ and $\tau_{\bar{\lambda}}$ for the Artin symbols of the integral ideals (λ) and $(\bar{\lambda})$ of K in $\mathscr{G}$, respectively. Since $B_\rho(k) = \lambda^k - \bar{\lambda}^k$, the measure

$$\theta_\rho = \tau_\lambda - \tau_{\bar{\lambda}}$$

satisfies the first condition of the lemma. For the second condition, we fix a topological generator γ of Γ, and write $\tau_\lambda|_\Gamma = \gamma^a$ and $\tau_{\bar{\lambda}}|_\Gamma = \gamma^b$ with $a, b \in \mathbb{Z}_2$. The congruences (2.8) imply that $a \in 2\mathbb{Z}_2$ and $b \notin 2\mathbb{Z}_2$. Hence we have

$$\tau_\lambda|_\Gamma - \tau_{\bar{\lambda}}|_\Gamma = \gamma^a(1 - \gamma^{b-a})$$

where γ^a is a unit in $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\Gamma)$, and $(1 - \gamma^{b-a}) = (1 - \gamma)u$ with u a unit in $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\Gamma)$. □

3. Vanishing of the μ-invariant for the $\mathfrak{p}$-adic L-function. We have constructed the $\mathfrak{p}$-adic L-function ν_χ in Theorem 2.5 for each $\chi \in G^*$. Since we deal with the Iwasawa module $X(H_\infty)$, not $X(F_\infty)$, we define a related pseudo-measure on $\mathrm{Gal}(H_\infty/K)$ by using the following lemma.

LEMMA 3.1. *Let δ be the generator of $\Delta = \mathrm{Gal}(F_\infty/H_\infty)$. We have $(1 + \delta)\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathscr{G}) = (1 + \delta)\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathrm{Gal}(H_\infty/K))$.*

Proof. Since $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathscr{G}) = \mathcal{I}_{\mathfrak{p}}[\Delta][[\mathrm{Gal}(H_\infty/K)]]$, it suffices to prove that $(1 + \delta)\mathcal{I}_{\mathfrak{p}}[\Delta] = (1 + \delta)\mathcal{I}_{\mathfrak{p}}$. Indeed, if $a + b\delta \in \mathcal{I}_{\mathfrak{p}}[\Delta]$, then $(1 + \delta)(a + b\delta) = (1 + \delta)(a + b) \in (1 + \delta)\mathcal{I}_{\mathfrak{p}}$. □

Hence there exists an $\mathcal{I}_{\mathfrak{p}}$-valued pseudo-measure m_χ on $\mathrm{Gal}(H_\infty/K)$ such that

$$(1 + \delta)\nu_\chi = (1 + \delta)m_\chi. \tag{3.1}$$

We define the $\mathfrak{p}$-adic L-function of χ by

$$L_{\mathfrak{p}}(s, \chi) = \int_{\mathrm{Gal}(H_\infty/K)} \kappa^s dm_\chi, \ s \in \mathbb{Z}_2,$$

where κ is the natural isomorphism of $\mathrm{Gal}(K_\infty/K)$ onto $1 + 2^2\mathbb{Z}_2$ with $\gamma \mapsto u$, and we view such a function on $\mathrm{Gal}(H_\infty/K)$ via the natural surjection from $\mathrm{Gal}(H_\infty/K)$ to $\mathrm{Gal}(K_\infty/K)$. It is well-known that this function is an Iwasawa function, i.e. there exists a formal power series $G_{\mathfrak{p}}(\chi; w) \in \mathcal{I}_{\mathfrak{p}}[[w]]$ such that

$$G_{\mathfrak{p}}(\chi; u^s - 1)/(u^s - 1)^e = L_{\mathfrak{p}}(s, \chi) \tag{3.2}$$

where $e = 0$ or 1, according as $\chi \neq 1$ or $\chi = 1$. The aim of this section is to prove the vanishing of the μ-invariant of m_χ, or equivalently,

THEOREM 3.2. *For each $\chi \in G^*$, the formal power series $G_{\mathfrak{p}}(\chi; w)$ is prime to 2, i.e. the μ-invariant of $G_{\mathfrak{p}}(\chi; w)$ vanishes.*

We remark that this vanishing theorem has recently been proven in [18], but in the present paper we will clarify it for our situation. We will use the idea of Sinnott [19] and Schneps [17]. Let ω be the Teichmüller character on $\mathbb{Z}_2^\times$, and for each $x \in \mathbb{Z}_2^\times$, let $\langle x \rangle = x/\omega(x)$. Given a formal power series $F(w) \in \mathcal{I}_{\mathfrak{p}}[[w]]$, we associate it to a measure m_F via Mahler's theorem (2.7). Then there exists a formal power series $\mathscr{L}(F)(w) \in \mathcal{I}_{\mathfrak{p}}[[w]]$ such that

$$\int_{\mathbb{Z}_2^\times} \langle x \rangle^s dm_F(x) = \mathscr{L}(F)(u^s - 1), \ s \in \mathbb{Z}_2. \tag{3.3}$$

The μ-invariant of a formal power series $F(w)$ and that of m_F are both denoted by $\mu(F)$. Recall that $\beta_v : \widehat{\mathbb{G}}_m \xrightarrow{\sim} \widehat{A^v}$ is the isomorphism of formal groups. Recall also that $\mathcal{O}_v$ is the ring of integers of H_v.

LEMMA 3.3 (Elliptic analogue of Theorem 1 of [19]). *Let $F(w) \in \mathcal{I}_{\mathfrak{p}}[[w]]$ be a formal power series of the form $F(w) = f(\beta_v(w))$, where f is a rational function on A with coefficients in $\mathcal{O}_v$. Then we have*

$$\mu(\mathscr{L}(F)) = \mu(\widetilde{F} + \widetilde{F} \circ (-1)),$$

where

$$\widetilde{F}(w) = F(w) - \frac{1}{2} \sum_{\zeta \in \{\pm 1\}} F(\zeta(1+w) - 1), \ (F \circ (-1))(w) = F((1+w)^{-1} - 1).$$

Proof. Firstly, we may assume that $\widetilde{F} = F$ and $F \circ (-1) = F$. Indeed, we put $F' = \widetilde{F} + \widetilde{F} \circ (-1)$. If the lemma holds for F' then it holds for F, since

$$\mathscr{L}(F') = 2\mathscr{L}(F), \ \widetilde{F'} + \widetilde{F'} \circ (-1) = 2F' = 2(\widetilde{F} + \widetilde{F} \circ (-1)).$$

Moreover, we may also assume that $\mu(F) = 0$. Indeed, replacing f by $\pi^{-t} f$, where π is a uniformizer of H_v, both μ-invariants are decreased by t. Hence we have to show that $\mu(\mathscr{L}(F)) = 1$.

By (3.3), we have

$$\mathscr{L}(F)(u^s - 1) = 2 \int_{1+2^2\mathbb{Z}_2} x^s dm_F(x) = 2G(u^s - 1)$$

where $G(w)$ is the formal power series associated to $m_F|_{1+2^2\mathbb{Z}_2}$. Since the characteristic function of $1 + 2^2\mathbb{Z}_2$ is given by $1_{1+2^2\mathbb{Z}_2}(u) = \frac{1}{4}\sum_{i=1}^4 \zeta_4^{(1-u)i}$ with ζ_4 a primitive 4-th root of unity, we have $G(w) = g(\beta_v(w))$ where g is a rational function on A given by

$$g(t) = \frac{1}{4} \sum_{i=1}^4 \zeta_4^{-i} f(t + t_i), \ t_i = \beta_v(\zeta_4^i - 1),$$

with coefficients in the ring of integers of $H_v(A_4)$. We denote by π' a uniformizer of $H_v(A_4)$.

Assume that $g \equiv 0 \bmod \pi'$, i.e. $\mu(G) > 0$. Clearly, we have $\mu(G \circ (-1)) > 0$. By the first assertion, it is easily seen that $m_F = m_F|_{\mathbb{Z}_2^\times}$ and that $G \circ (-1)$ is associated to $m_F|_{-1+2^2\mathbb{Z}_2}$. But then

$$m_F = m_F|_{\mathbb{Z}_2^\times} = m_F|_{1+2^2\mathbb{Z}_2} + m_F|_{-1+2^2\mathbb{Z}_2}$$

has positive μ-invariant, which contradicts the second assumption that $\mu(F) = 0$. Hence we have $\mu(G) = 0$ and then $\mu(\mathscr{L}(F)) = 1$. □

LEMMA 3.4. *For each $\chi \in G^*$, we have*

$$2G_{\mathfrak{p}}(\chi; w) = \mathscr{L}\left(\sum_{\mathfrak{a}\in\mathfrak{C}} \chi(\sigma_{\mathfrak{a}})(\omega^{-1} * D\mathfrak{B}_{\rho,\mathfrak{a}})\right)(u^{-1}(1+w)-1) \cdot u_\chi(w)$$

where $u_\chi(w)$ is a unit in $\mathcal{I}_{\mathfrak{p}}[[w]]$. Here, ω is the Teichmüller character on $\mathbb{Z}_2^\times$ and $\omega^{-1} * F$ denotes the formal power series associated to the measure $\omega^{-1} \cdot m_F$.

Proof. By (3.1) it is easy to check that

$$\int_{\mathscr{G}} \kappa(\sigma)^s d\nu_\chi(\sigma) = 2L_{\mathfrak{p}}(s, \chi).$$

On the other hand, we recall that $\mathfrak{B}_{\rho,\mathfrak{a}}(w)$ is the formal power series associated to $\nu_{\rho,\mathfrak{a}}$, i.e. $m_{\mathfrak{B}_{\rho,\mathfrak{a}}} = \nu_{\rho,\mathfrak{a}}$. Hence we have

$$\begin{aligned}\int_{\mathscr{G}} \kappa(\sigma)^s d\nu_\chi^\circ(\sigma) &= \sum_{\mathfrak{a}\in\mathfrak{C}} \chi(\sigma_{\mathfrak{a}}) \int_{\mathcal{G}} \kappa(\sigma)^s dm_{\mathfrak{B}_{\rho,\mathfrak{a}}}(\sigma) \\ &= \int_{\mathbb{Z}_2^\times} \langle x\rangle^s dm_{\left(\sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})\mathfrak{B}_{\rho,\mathfrak{a}}\right)}(x) \\ &= \int_{\mathbb{Z}_2^\times} \langle x\rangle^{s-1} dm_{\left(\sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})(\omega^{-1}*D\mathfrak{B}_{\rho,\mathfrak{a}})\right)}(x).\end{aligned}$$

The proof of the lemma is now complete, since the integral on the measure θ_ρ can be written as $u_\chi(w)^{-1}$ or $u_\chi(w)^{-1}w$ according as $\chi \neq 1$ or $\chi = 1$. □

Recall that the formal power series $D\mathfrak{B}_{\rho,\mathfrak{a}}(w)$ is a rational function whose integral power expansion in z is given by

$$\frac{1}{2}\Omega_v \frac{d}{dz} \log \mathfrak{I}_{\rho,\mathfrak{a}}(\eta_A(\mathfrak{a})(\mathfrak{M}(z,\mathcal{L})). \tag{3.4}$$

By our construction, it is clear that $\widetilde{D\mathfrak{B}_{\rho,\mathfrak{a}}} = D\mathfrak{B}_{\rho,\mathfrak{a}}$. Moreover, $D\mathfrak{B}_{\rho,\mathfrak{a}}$ and $D\mathfrak{B}_{\rho,\mathfrak{a}} \circ (-1)$ have the same poles, which implies that $D\mathfrak{B}_{\rho,\mathfrak{a}} = D\mathfrak{B}_{\rho,\mathfrak{a}} \circ (-1)$. We also note that $\mu(F) = \mu(\omega * F)$. Hence by Lemma 3.3 and Lemma 3.4, the proof of Theorem 3.2 is now complete by the following lemma.

LEMMA 3.5. *For each $\chi \in G^*$, we have $\mu\left(\sum_{\mathfrak{a}\in\mathfrak{C}} \chi(\sigma_{\mathfrak{a}}) D\mathfrak{B}_{\rho,\mathfrak{a}}\right) = 0$.*

Proof. Recall that v is our fixed prime of H above $\mathfrak{p}$. Let $\widetilde{A}$ denote the reduced curve modulo v. It suffices to show that the reduction modulo v of the function $\sum_{\mathfrak{a}\in\mathfrak{C}} \chi(\sigma_{\mathfrak{a}}) D\mathfrak{B}_{\rho,\mathfrak{a}}$ has some poles on $\widetilde{A}$ with non-zero residue modulo v.

By (3.4), the function $D\mathfrak{B}_{\rho,\mathfrak{a}}$ can be written as a rational function on A

$$\frac{1}{2}\Omega_v \frac{d}{dz}\log\left(\frac{\prod_{i=1}^r R_{\lambda_i,\mathfrak{a}}(\eta_A(\mathfrak{a})(P))^{2n_i}}{\prod_{i=1}^r R_{\lambda_i,\mathfrak{a}\mathfrak{p}}(\eta_A(\mathfrak{a}\mathfrak{p})(P))^{n_i}}\right). \tag{3.5}$$

As (2.2), we have the relations

$$R_{\lambda_i,\mathfrak{a}}(\eta_A(\mathfrak{a})(P)) = \prod_{W\in A_{\mathfrak{a}}} R_{\lambda_i}(P\oplus W),\ R_{\lambda_i,\mathfrak{a}}(\eta_A(\mathfrak{a}\mathfrak{p})(P)) = \prod_{U\in A_{\mathfrak{a}\mathfrak{p}}} R_{\lambda_i}(P\oplus U).$$

Therefore, (3.5) is equal to

$$\frac{1}{2}\Omega_v\sum_{i=1}^r -2n_i\left(\sum_{W\in A_{\mathfrak{a}}}\sum_{M\in V_{\lambda_i}}\frac{-2y(P\oplus W)+a_1x(P\oplus W)+a_3}{x(P\oplus W)-x(M)}\right)$$
$$+\frac{1}{2}\Omega_v\sum_{i=1}^r n_i\left(\sum_{U\in A_{\mathfrak{a}\mathfrak{p}}}\sum_{M\in V_{\lambda_i}}\frac{-2y(P\oplus U)+a_1x(P\oplus U)+a_3}{x(P\oplus U)-x(M)}\right).$$

We now analyze its possible poles of the reduction of this function on $\widetilde{A}$. For the second term, we see that they could come from the points $M-U$ for all $M\in V_{\lambda_i}$ and $U\in A_{\mathfrak{a}\mathfrak{p}}$. By the t-expansions of x and y, we can easily compute that the residue at each $M-U$ is equal to $-n_i\Omega_v$. This is a $\mathfrak{p}$-adic unit because we chose $n_i=\pm1$ in the proof of Lemma 2.6. However, as $A_{\mathfrak{p}}$ reduces to zero modulo v, the residue at such a pole on $\widetilde{A}$ is a multiple of 2, and hence reduces to zero modulo v.

For the first term, we note that x is an even function, in particular $x(M)=x(-M)$. Thus this term is equal to

$$-\frac{1}{2}\Omega_v\sum_{i=1}^r n_i\left(\sum_{W\in A_{\mathfrak{a}}}\sum_{M\in A_{\lambda_i}\setminus\{0\}}\frac{-2y(P\oplus W)+a_1x(P\oplus W)+a_3}{x(P\oplus W)-x(M)}\right).$$

Clearly the poles must come from the points $M-W$ for $M\in A_{\lambda_i}\setminus\{0\}$ and $W\in A_{\mathfrak{a}}$. The residue at each $M-W$ is equal to $n_i\Omega_v$, which is a $\mathfrak{p}$-adic unit. Since reduction modulo v is injective on the set of these $M-W$, each of these $M-W$ gives a pole of the reduced function on $\widetilde{A}$. Note that as $i=1,\cdots,r$, all of these poles on $\widetilde{A}$ are distinct because M is a non-zero element of A_{λ_i}.

Hence the set of poles of the reduction of the function $D\mathfrak{B}_{\rho,\mathfrak{a}}$ on $\widetilde{A}$ is given by the reduction modulo v of

$$\{M-W \mid M\in A_{\lambda_i}\setminus\{0\},\ W\in A_{\mathfrak{a}}\}, \tag{3.6}$$

and their residues are non-zero modulo v. Clearly the same is true for the sum $\sum_{\mathfrak{a}\in\mathfrak{C}}\chi(\sigma_{\mathfrak{a}})D\mathfrak{B}_{\rho,\mathfrak{a}}$ because each $\chi(\sigma_{\mathfrak{a}})$ is an h-th root of unity and thus a $\mathfrak{p}$-adic unit. □

4. Vanishing of the μ-invariant for $X(H_\infty)$. We will show that the Iwasawa invariants of $X(H_\infty)$ and the $\mathfrak{p}$-adic L-function m are equal. As a corollary, Theorem 1.1 follows immediately from Theorem 3.2. This equality is a well-known result (for example, see [10]) for the primes $p\neq 2$, but it can easily be extended to $p=2$ in our case, thanks to our assumptions that 2 splits in K and $(2,h)=1$.

For the remainder of this section, we denote by μ and λ the μ-invariant and the λ-invariant of $X(H_\infty)$, respectively. Recall that $\Gamma = \mathrm{Gal}(H_\infty/H)$. For each $n \geq 0$, we define $\Gamma_n = \Gamma^{p^n}$ and $H_n = H_\infty^{\Gamma_n}$. We write $M(H_n)$ for the maximal abelian 2-extension of H_n which is unramified outside of the primes of H_n above $\mathfrak{p}$. Then it is easily seen that the Γ_n-coinvariants of $X(H_\infty)$ is given by

$$X(H_\infty)_{\Gamma_n} = \mathrm{Gal}(M(H_n)/H_\infty).$$

We have the following asymptotic formula of Iwasawa

$$\mathrm{ord}_2([M(H_n) : H_\infty]) = 2^n\mu + \lambda n + c, \ n \gg 0, \tag{4.1}$$

where $c \in \mathbb{Z}$ is a constant independent of n. One can compute this 2-adic valuation using the methods of Coates and Wiles [7]. Let $\mathfrak{P}$ be any prime of H_n lying above $\mathfrak{p}$, and let $U_{n,\mathfrak{P}}$ denote the group of principal units of the completion $H_{n,\mathfrak{P}}$. Write $U_n = \prod_{\mathfrak{P}|\mathfrak{p}} U_{n,\mathfrak{P}}$ and $\Phi_n = \prod_{\mathfrak{P}|\mathfrak{p}} H_{n,\mathfrak{P}}$. Let E_n be the group of units of H_n. As E_n is canonically embedded into U_n, let $\overline{E}_n$ be the $\mathbb{Z}_2$-submodule of U_n generated by E_n, and let D_n be the $\mathbb{Z}_2$-submodule of U_n generated by E_n and $(1+2^2)$. Let $R_\mathfrak{p}(H_n)$ denote the $\mathfrak{p}$-adic regulator for H_n/K. Let $\Delta(H_n/K)$ denote the discriminant of H_n/K, and choose any generator $\Delta_\mathfrak{p}(H_n/K)$ of the ideal $\Delta(H_n/K)\mathcal{O}_\mathfrak{p}$.

Theorem 4.1. *We have*

$$\mathrm{ord}_2([M(H_n) : H_\infty]) = \mathrm{ord}_2\left(\frac{h(H_n)R_\mathfrak{p}(H_n)}{\omega(H_n)\sqrt{\Delta_\mathfrak{p}(H_n/K)}}\prod_{\mathfrak{P}|\mathfrak{p}}(1-(N\mathfrak{P})^{-1})\right) + n + 2$$

where $h(H_n)$ is the class number of H_n, $\omega(H_n)$ is the number of roots of unity in H_n and $N\mathfrak{P}$ is the absolute norm of $\mathfrak{P}$.

Proof. Let C_n denote the idéle class group of H_n. Let $Y_n = \bigcap_{m \geq n} N_{H_m/H_n} C_m$. Let $L(H_n)$ be the maximal unramified extension of H_n in $M(H_n)$. Class field theory gives an isomorphism

$$(Y_n \cap U_n)/\overline{E}_n \xrightarrow{\sim} \mathrm{Gal}(M(H_n)/L(H_n)H_\infty).$$

Noting that $L(H_n) \cap H_\infty = H_n$ because H_∞/H_n is totally ramified at $\mathfrak{P}$, we obtain an exact sequence

$$0 \to (Y_n \cap U_n)/\overline{E}_n \to \mathrm{Gal}(M(H_n)/H_\infty) \to \mathrm{Gal}(L(H_n)/H_n) \to 0\ .$$

It is easy to check (see Lemma 5 and 6 of [7]) that $Y_n \cap U_n = \mathrm{Ker}(N_{\Phi_n/K_\mathfrak{p}}|_{U_n})$ and $\overline{E}_n = \mathrm{Ker}(N_{\Phi_n/K_\mathfrak{p}}|_{D_n})$, which follows that $[Y_n \cap U_n : \overline{E}_n] = [U_n : D_n]$. Using methods analogous to Lemma 7 and Lemma 8 of [7], one can obtain

$$[U_n : D_n] = \mathrm{ord}_2\left(\frac{R_\mathfrak{p}(H_n)}{\omega(H_n)\sqrt{\Delta_\mathfrak{p}(H_n/K)}}\prod_{\mathfrak{P}|\mathfrak{p}}(N\mathfrak{P})^{-1}\right) + n + 2. \tag{4.2}$$

The theorem now follows on noting $\prod_{\mathfrak{P}|\mathfrak{p}}(N\mathfrak{P})^{-1}$ and $\prod_{\mathfrak{P}|\mathfrak{p}}(1-(N\mathfrak{P})^{-1})$ have the same order, and that $\mathrm{Gal}(L(H_n)/H_n)$ is the 2-primary part of the ideal class group of H_n. $\square$

We now begin the computation of the Iwasawa invariants of our $\mathfrak{p}$-adic L-function m. Given $n \geq 0$, let ϵ be a non-trivial character of $\mathrm{Gal}(H_n/K)$, say $\epsilon = \chi\theta$, where χ is a character of G and θ is a character of $\mathrm{Gal}(H_n/H)$. Let $\mathfrak{f}_\epsilon$ denote the conductor of ϵ with $(f_\epsilon) = \mathfrak{f}_\epsilon \cap \mathbb{Z}$. As before, we define

$$L_{\mathfrak{p},\mathfrak{f}_\epsilon}(s,\epsilon) = \int_{\mathrm{Gal}(H_\infty/K)} \epsilon^{-1}\kappa^s dm$$

where m is the $\mathfrak{p}$-adic L-function defined in the previous section.

For each $n \geq 0$, we denote by $\mathfrak{C}_n$ a set of integral ideals $\mathfrak{a}$ of K prime to $\mathfrak{p}\mathfrak{q}$, whose Artin symbols $\tau_\mathfrak{a}$ give precisely the Galois group $G = \mathrm{Gal}(H_n/K)$. For the convention, we take $\mathfrak{C}_0 = \mathfrak{C}$. For $\mathfrak{a} \in \mathfrak{C}_n$, we denote by $\delta(\mathfrak{a})$ the Siegel unit as defined in II.2.2 of [10]. We also denote by $\varphi_{\mathfrak{f}_\epsilon}(\mathfrak{a})$ the Robert's invariant as defined in II.2.6 of [10]. Then we put

$$G(\epsilon) = \frac{\theta(\mathfrak{p}^m)}{2^m} \sum_\tau \chi(\tau)(\tau(\zeta_m))^{-1}$$

where the sum runs over $\tau \in \mathrm{Gal}(H_n K(\mathfrak{p}^{*\infty})/K)$ with $\tau|_{K(\mathfrak{p}^{*\infty})} = (\mathfrak{p}^m, K(\mathfrak{p}^{*\infty})/K)$, m is an integer such that $\mathfrak{p}^m \parallel \mathfrak{f}_\epsilon$, and ζ_m is a primitive p^m-th root of unity. Define also

$$S(\epsilon) = \begin{cases} \sum_{\mathfrak{a}\in\mathfrak{C}_n} \epsilon(\mathfrak{a}) \log(\varphi_{\mathfrak{f}_\epsilon}(\mathfrak{a})) & \text{if } \mathfrak{f}_\epsilon \neq 1 \\ \frac{1}{h}\sum_{\mathfrak{a}\in\mathfrak{C}} \epsilon(\mathfrak{a}) \log(\delta(\mathfrak{a})) & \text{if } \mathfrak{f}_\epsilon = 1. \end{cases}$$

Then, following the methods of [10, Theorem II.5.2], we obtain

$$L_{\mathfrak{p},\mathfrak{f}_\epsilon}(0,\epsilon) = \frac{-1}{12 f_\epsilon \omega_{\mathfrak{f}_\epsilon}} G(\epsilon^{-1}) S(\epsilon) \left(1 - \frac{\epsilon^{-1}(\mathfrak{p})}{2}\right)$$

where $\omega_{\mathfrak{f}_\epsilon}$ denotes the number of roots of unity in K congruent to 1 modulo $\mathfrak{f}_\epsilon$.

On the other hand, the analytic class number formula, together with Kronecker's theorem (see §0.2.7, §I.2.2 and §IV.3.9 (6) of [20]), gives

$$\frac{h(H_n)R_\mathfrak{p}(H_n)}{\omega(H_n)} = \frac{hR_\mathfrak{p}(K)}{\omega(K)} \prod_{\epsilon\neq 1} \frac{S(\epsilon)}{12 f_\epsilon \omega_{\mathfrak{f}_\epsilon}}.$$

Clearly, $R_\mathfrak{p}(K) = 1$ and $\omega(K) = 2$. Thus, by Theorem 4.1, we have

$$\mathrm{ord}_2([M(H_n):H_\infty]) = \mathrm{ord}_2\left(\frac{1}{\sqrt{\Delta_\mathfrak{p}(H_n/K)}} \prod_{\epsilon\neq 1} \frac{S(\epsilon)}{12 f_\epsilon w_{\mathfrak{f}_\epsilon}} \prod_{\mathfrak{P}|\mathfrak{p}} (1-(N\mathfrak{P})^{-1})\right) + n + 1.$$

Furthermore, we have $\prod_{\mathfrak{P}|\mathfrak{p}}(1-(N\mathfrak{P})^{-1}) = \frac{1}{2}\prod_{\epsilon\neq 1}\left(1 - \frac{\epsilon^{-1}(\mathfrak{p})}{2}\right)$, and the conductor-discriminant formula gives that $\prod_{\epsilon\neq 1} G(\epsilon)$ is $\Delta_\mathfrak{p}(H_n/K)^{-1/2}$ up to a $\mathfrak{p}$-adic unit. It follows that

$$\mathrm{ord}_2([M(H_n):H_\infty]) = \mathrm{ord}_2\left(\prod_{\epsilon\neq 1} L_{\mathfrak{p},\mathfrak{f}_\epsilon}(0,\epsilon)\right) + n.$$

Define as before $G_{\mathfrak{p}}(\epsilon; w) \in \mathcal{I}_{\mathfrak{p}}[[w]]$ to be the formal power series associated to $L_{\mathfrak{p},\mathfrak{f}_\epsilon}(s, \epsilon)$. In particular, we have

$$L_{\mathfrak{p},\mathfrak{f}_\epsilon}(0, \epsilon) = G_{\mathfrak{p}}(\epsilon; 0) = (\theta^{-1}(u) - 1)^{-e} G_{\mathfrak{p}}(\chi; \theta^{-1}(u) - 1)$$

where $e = 0$ or 1 according as $\chi \neq 1$ or $\chi = 1$ and u is a fixed topological generator of $1 + 4\mathbb{Z}_2$. Noting that $\mathrm{ord}_2\left(\prod_{\theta\neq 1}(\theta^{-1}(u) - 1)\right) = n$, we obtain

$$\mathrm{ord}_2([M(H_n) : H_\infty]) = \mathrm{ord}_2\left(\prod_{\epsilon\neq 1} G_{\mathfrak{p}}(\chi; \theta^{-1}(u) - 1)\right). \tag{4.3}$$

For each $\chi \in G^*$, we denote by μ_χ and λ_χ the μ-invariant and λ-invariant of $G_{\mathfrak{p}}(\chi; w)$, respectively. We define $\mu^{\mathrm{an}} = \sum_{\chi\in G^*} \mu_\chi$ and $\lambda^{\mathrm{an}} = \sum_{\chi\in G^*} \lambda_\chi$. For sufficiently large n, Theorem 3.2 tells us that $\mathrm{ord}_2\left(G_{\mathfrak{p}}(\chi; \theta^{-1}(u) - 1)\right) = \mathrm{ord}_2((\theta^{-1}(u) - 1)^{\lambda_\chi})$, and hence

$$\mathrm{ord}_2\left(\prod_{\epsilon\neq 1} G_{\mathfrak{p}}(\chi; \theta^{-1}(u) - 1)\right) = \lambda^{\mathrm{an}} n + c'$$

where $c' \in \mathbb{Z}$ is a constant independent of n. By (4.1) and (4.3), we conclude that

$$\mu = \mu^{an} = 0,\ \lambda = \lambda^{an},\ c = c'.$$

This completes the proof of Theorem Theorem 1.1.

5. Numerical examples for the prime $q < 500$. Before giving numerical examples for $X(H_\infty)$, we point out the following well-known general lemma.

LEMMA 5.1. *Let K be an imaginary quadratic field, and p any rational prime which splits in K and does not divide the class number of K. Let K_∞ be the unique $\mathbb{Z}_p$-extension of K unramified outside one of the primes $\mathfrak{p}$ of K above p. Then K_∞ has no non-trivial abelian p-extension unramified outside the primes above $\mathfrak{p}$.*

Proof. In a similar notation to that used for the case $p = 2$, let $X(K_\infty)$ be the Galois group over K_∞ of the maximal abelian p-extension of K_∞ unramified outside the primes above $\mathfrak{p}$. Then, as usual in Iwasawa theory, we have $X(K_\infty)_\Gamma = \mathrm{Gal}(R/K_\infty)$ where R denotes the maximal abelian p-extension which is unramified outside $\mathfrak{p}$. Thus R must be the maximal pro-p extension of K contained in the union of the ray class fields of K modulo $\mathfrak{p}^n$ for all $n \geq 1$. Thus, as p does not divide h, class field theory tells us that $\mathrm{Gal}(R/K)$ must be the maximal pro-p quotient of

$$\varprojlim_n \left((\mathcal{O}/\mathfrak{p}^n)^\times/\{\pm 1\}\right)$$

which is isomorphic to $\mathbb{Z}_p$. Thus $R = K_\infty$, and the proof of the lemma is complete by Nakayama's lemma. □

Clearly, the assumption of the above lemma is valid for our situation when $p = 2$ and $K = \mathbb{Q}(\sqrt{-q})$ with q any prime congruent to 7 modulo 8. The simplest example is given by $K = \mathbb{Q}(\sqrt{-7})$, which has class number 1, in which case $X(H_\infty) = X(K_\infty) = 0$. Somewhat surprisingly, the numerical calculations below show that we seem to quite often have $X(H_\infty) = 0$ for arbitrary primes $q \equiv 7 \bmod 8$. However, we point out that when 2 divides the class number of H, it is easily seen that we must necessarily have $X(H_\infty) \neq 0$, and therefore of infinite order. Andrzej Dabrowski has kindly informed us that 2 does divide the class number of H for the primes $q = 751$, $q = 1367$ and $q = 1399$.

We give a list of numerical examples for the primes $q < 500$. By using SAGE calculation, we obtain the class numbers of K and H and the $\mathfrak{p}$-adic regulator $R_\mathfrak{p} = R_\mathfrak{p}(H/K)$ for H/K. By Theorem 4.1, we then obtain the index $[M(H) : H_\infty]$. Recall that $M(H)$ denotes the maximal abelian 2-extension of H which is unramified outside the primes of H lying above $\mathfrak{p}$. If we have $[M(H) : H_\infty] = 0$, Nakayama's lemma implies immediately that $X(H_\infty) = 0$. We note that the prime $q = 431$ is the first example in which $X(H_\infty) \neq 0$.

q	$h(K)$	$h(H)$	$\mathrm{ord}_2(R_\mathfrak{p})$	$\mathrm{ord}_2([M(H) : H_\infty])$
7	1	1	0	0
23	3	1	2	0
31	3	1	2	0
47	5	1	4	0
71	7	1	6	0
79	5	1	4	0
103	5	1	4	0
127	5	1	4	0
151	7	1	6	0
167	11	1	10	0
191	13	1	12	0
199	9	1	8	0
223	7	1	6	0
239	15	1	14	0
263	13	1	12	0
271	11	1	10	0
311	19	1	18	0
359	19	1	18	0
367	9	1	8	0
383	17	1	16	0
431	21	1	25	5
439	15	1	14	0
463	7	1	6	0
479	25	1	24	0
487	7	1	6	0

For example, when $q = 23$, by SAGE calculation we obtain $H = \mathbb{Q}(\alpha)$ where

$$\alpha^6 - 3\alpha^5 + 5\alpha^4 - 5\alpha^3 + 5\alpha^2 - 3\alpha + 1 = 0.$$

The two fundamental units are then given by

$$\alpha^5 - 2\alpha^4 + 2\alpha^3 - \alpha^2 + 2\alpha,\ \alpha^4 - 2\alpha^3 + 3\alpha^2 - 2\alpha + 2,$$

and the $\mathfrak{p}$-adic regulator $R_\mathfrak{p}$ is given by

$$2^2 + 2^4 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{13} + 2^{17} + 2^{20} + O(2^{23}).$$

6. Proof of Corollary 1.2 and Theorem 1.3. Finally, we give simple proofs that Theorem 1.1 implies Corollary 1.2 and Theorem 1.3. For the corollary, let J/H be any quadratic extension and let $J_\infty = JK_\infty$. Define $\Delta = \mathrm{Gal}(J_\infty/H_\infty)$. If Δ is trivial, then $J \subseteq H_\infty$, and so there is nothing more to prove. Hence we may assume that Δ is cyclic of order 2. The group ring $\mathbb{Z}_2[\Delta]$ is then a commutative local ring with maximal ideal $\mathfrak{m}$ generated by 2 and $\delta - 1$, where δ denotes the non-trivial element of Δ. We will use Nakayama's lemma which asserts that, for any $\mathbb{Z}_2[\Delta]$-module M, if there are elements $x_1, \cdots, x_m \in M$ whose images in $M/\mathfrak{m}M$ generate $M/\mathfrak{m}M$ over $\mathbb{F}_2$, then they generate M itself over $\mathbb{Z}_2$. We note that, by maximality, $M(J_\infty)$ is clearly Galois over K_∞. We have an exact sequence

$$0 \longrightarrow X(J_\infty) \longrightarrow \mathrm{Gal}(M(J_\infty)/H_\infty) \longrightarrow \Delta \longrightarrow 0.$$

Thus, as usual, Δ acts on $X(J_\infty)$ by inner automorphisms. In particular, it follows from this action that

$$X(J_\infty)/(\delta - 1)X(J_\infty) = \mathrm{Gal}(R/J_\infty) \tag{6.1}$$

where R denotes the maximal abelian extension of H_∞ contained in $M(J_\infty)$. Our claim is that, under the hypothesis that $X(H_\infty)$ is a finitely generated $\mathbb{Z}_2$-module, $\mathrm{Gal}(R/J_\infty)$ is a finitely generated $\mathbb{Z}_2$-module. It follows that $X(J_\infty)/\mathfrak{m}X(J_\infty)$ is a finite dimensional vector space over $\mathbb{F}_2$, and hence, by Nakayama's lemma, $X(J_\infty)$ is a finitely generated $\mathbb{Z}_2$-module.

Let S be the set of all primes of H_∞, which do not lie above $\mathfrak{p}$, and which are ramified in J_∞. If $S = \emptyset$, J_∞ is contained in $M(H_\infty)$, in particular $M(J_\infty) = M(H_\infty)$, and hence there is nothing to prove. Otherwise, the set S is finite. This is because, by a basic elementary property of the $\mathbb{Z}_2$-extension K_∞/K, there are only finitely many primes of K_∞ lying above each prime of K, and thus the same is true for the primes of H_∞ lying above a prime of H. Hence, as there are only finitely many primes of H which ramifies in J, it follows that S is finite. Moreover, the inertia subgroup in $\mathrm{Gal}(R/H_\infty)$ of each prime in S must be of order 2. Now let R' be the fixed field of the subgroup of $\mathrm{Gal}(R/H_\infty)$ generated by the inertia subgroups of all primes in S. Obviously, we have

$$[R : R'] \leq 2^{\#(S)} \tag{6.2}$$

and $\mathrm{Gal}(R/R')$ is annihilated by 2. But R'/H_∞ is an abelian 2-extension which is unramified outside $\mathfrak{p}$, and therefore we have $R' \subset M(H_\infty)$. Hence, by our hypothesis and (6.2), $\mathrm{Gal}(R/H_\infty)$ is a finitely generated $\mathbb{Z}_2$-module, and so is $\mathrm{Gal}(R/J_\infty)$. This completes the proof of Corollary 1.2.

For Theorem 1.3, let F and F_∞ be the fields defined as in (1.4). Then again the same classical argument (cf. the proof of Lemma 2.1 of [3]) shows that E has good reduction everywhere over F. By Corollary 1.2, the Galois group $X(F_\infty)$ is a finitely generated torsion module over the Iwasawa algebra $\Lambda(\Gamma)$ of $\Gamma = \mathrm{Gal}(F_\infty/F)$. Hence, followed by classical arguments (for example, see [4]), one can easily obtain

$$S_{\mathfrak{p}^\infty}(E/F_\infty) = \mathrm{Hom}(X(F_\infty), E_{\mathfrak{p}^\infty}).$$

Then Theorem 1.3 clearly follows immediately from Corollary 1.2.

Acknowledgements. The authors would like to thank John Coates for very helpful comments on this paper. The second author is supported by the SFB 1085 "Higher invariants" (University of Regensburg) funded by the DFG. The third author (Y.L.) would like to thank Ye Tian for the constant encouragement. The third author Y.L. is supported by NSFC grant A010102-11671380.

REFERENCES

[1] D. Bernardi, C. Goldstein and N. Stephens, *Notes p-adiques sur les courbes elliptiques*, J. Reine Angew. Math., 351 (1984), pp. 129–170.

[2] J. Buhler and B. Gross, *Arithmetic on elliptic curves with complex multiplication II*, Invent. Math., 79 (1985), pp. 11–29.

[3] J. Choi and J. Coates, *Iwasawa theory of quadratic twists of* $X_0(49)$, to appear in Acta Mathematica Sinica, English series.

[4] J. Coates, *Infinite descent on elliptic curves with complex multiplication*, Progress in Mathematics 35 (1983), Birkhäuser, pp. 321–350.

[5] J. Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull. London Math. Soc., 23 (1991), pp. 321–350.

[6] J. Coates and C. Goldstein, *Some remarks on the main conjecture for elliptic curves with complex multiplication*, American J. of Mathematics, 105 (1983), pp. 337–366.

[7] J. Coates and A. Wiles, *Kummer's criterion for Hurwitz numbers*, Algebraic number theory, Kyoto 1976, Japan Society for the Promotion of Science (1977), pp. 9–23.

[8] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math., 39 (1977), pp. 223–251.

[9] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Australian Math. Soc., 26 (1978), pp. 1–25.

[10] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication*, Perspectives in Mathematics, vol.3, Academic Press (1987).

[11] R. Gillard, *Fonctions L p-adiques des des corps quadratiques imaginaires et de leurs extensions abèliennes*, J. Reine Angew. Math., 358 (1985), pp. 76–91.

[12] R. Gillard, *Transformation de Mellin-Leopoldt des fonctions elliptiques*, J. Number Theory, 25:3 (1987), pp. 379–393.

[13] C. Goldstein and N. Schappacher, *Series d'Eisenstein et fonctions L de courbes elliptiques a multiplication complexe*, Crelle, 327 (1981), pp. 184–218.

[14] B. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Mathematics, 776, Springer (1980).

[15] B. Gross, *Minimal models for elliptic curves with complex multiplication*, Compositio Math., 45 (1983), pp. 155–164.

[16] Y. Kezuka, *On the main conjectures of Iwasawa theory for certain elliptic curves with complex multiplication*, thesis, University of Cambridge.

[17] L. Schneps, *On the* μ*-invariant of p-adic L-functions attached to elliptic curves with complex multiplication*, J. Number Theory, 25:1 (1987), pp. 20–33.

[18] H. Oukhaba and S. Viguié, *On the* μ*-invariant of Katz p-adic L-functions attached to imaginary quadratic fields*, Forum Math., 28:3 (2016), pp. 507–525.

[19] W. Sinnott, *On the* μ*-invariant of the* Γ*-transform of a rational function*, Invent. Math., 75 (1984), pp. 273–282.

[20] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$, Progress in Mathematics, 47 (1984), Birkhäuser.