Bernoulli-Hurwitz numbers, Wieferich primes and Galois representations

Álvaro Lozano-Robledo

Department of Mathematics. Cornell University. Ithaca, NY 14853.

Abstract

Let K be a quadratic imaginary number field with discriminant $D_K \neq -3, -4$ and class number one. Fix a prime $p \geq 7$ which is unramified in K. Given an elliptic curve $A/\mathbb{Q}$ with complex multiplication by K, let $\overline{\rho_A}\colon \operatorname{Gal}(\overline{K}/K(\mu_{p^\infty})) \to \operatorname{SL}(2, \mathbb{Z}_p)$ be the representation which arises from the action of Galois on the Tate module. Herein it is shown that, for all but finitely many inert primes p, the image of a certain deformation $\rho_A\colon \operatorname{Gal}(\overline{K}/K(\mu_{p^\infty})) \to \operatorname{SL}(2, \mathbb{Z}_p[[X]])$ of $\overline{\rho_A}$ is "as large as possible", that is, it is the full inverse image of a Cartan subgroup of $\operatorname{SL}(2, \mathbb{Z}_p)$. If p splits in K, then the same result holds as long as certain Bernoulli-Hurwitz number is a p-adic unit which, in turn, is equivalent to a prime ideal not being a Wieferich place. The proof rests on the theory of elliptic units of Robert and Kubert-Lang, and on the two-variable main conjecture of Iwasawa theory for quadratic imaginary fields.

Key words: Elliptic curves, p-adic Galois representations, elliptic units, Bernoulli-Hurwitz numbers, Wieferich places, complex multiplication.
1991 MSC: 11F80 (primary), 11G05, 11G16 (secondary).

1 Introduction

Fix a prime $p \geq 7$, let K be a number field and write $\widetilde{K}$ for the extension of K generated by the roots of unity in $\overline{K}$ of p-power order (i.e. $\widetilde{K} = K(\mu_{p^\infty})$). Let A be an elliptic curve over K with $j(A) \neq 0, 1728$. In [13], Rohrlich obtains a representation

$$\rho_A\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \operatorname{SL}(2, \mathbb{Z}_p[[X]])$$

such that $\overline{\rho_A} := \rho_A|_{X=0}\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \to \operatorname{SL}(2, \mathbb{Z}_p)$ is equivalent to the natural representation of $\operatorname{Gal}(\overline{K}/\widetilde{K})$ on $T_p(A)$, the Tate module of A. In light of the

Email address: `alozano@math.cornell.edu` (Álvaro Lozano-Robledo).

well-known results about the image of $\overline{\rho_A}$ due to Deuring, Serre, Tate et al. ([3], [19], [18]), one would naturally want to know how large is the image of the representation ρ_A.

Let $\widetilde{\rho}_A\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2,\mathbb{F}_p)$ be the representation induced by the action of Galois on the points of order p on A. In [14], Rohrlich proved in the case $K = \mathbb{Q}$ that if $\widetilde{\rho}_A$ is surjective and $\nu_p(j(A)) = -1$ then ρ_A is surjective, where ν_p is the usual p-adic valuation on $\mathbb{Q}$. This result has been generalized in [8] to elliptic curves defined over arbitrary number fields with non-integral j-invariant at a prime above p. In the present paper, we are interested in the complex multiplication case.

From now on, we let K be a quadratic imaginary number field with discriminant $D_K \neq -3, -4$ and class number $h_K = 1$. Fix a prime $p \geq 7$ which is not ramified in K. Given an elliptic curve $A/\mathbb{Q}$ with complex multiplication by K (and precisely by the ring of integers $\mathcal{O}_K$) the theory of complex multiplication describes the image of the map $\overline{\rho_A}\colon \operatorname{Gal}(\overline{K}/\widetilde{K}) \to \mathrm{SL}(2,\mathbb{Z}_p)$ as a Cartan subgroup $\mathfrak{C}'$ of $\mathrm{SL}(2,\mathbb{Z}_p)$, unique up to isomorphism. We write $K(p)$ for the ray class field of K of conductor $p\mathcal{O}_K$, and let h_p be the class number of $K(p)$. In a previous article, the author proved the following:

Theorem 1.1 ([9], Thm. 1.1) *If $p \nmid h_p$ then the image of ρ_A is "as large as possible", that is, it is the full inverse image of $\mathfrak{C}'$ under the natural projection $\pi_X\colon \mathrm{SL}(2,\mathbb{Z}_p[[X]]) \to \mathrm{SL}(2,\mathbb{Z}_p)$ sending $X \mapsto 0$.*

The aim of this article is to remove the hypothesis that $p \nmid h_p$. In order to do this, we will make use of Kummer-type criteria for quadratic imaginary fields developed by G. Robert (in [12]) and R. Yager (in [21]), in terms of special values of L-functions (or alternatively, in terms of Bernoulli-Hurwitz numbers as defined below). Moreover, we will use the two-variable "main conjecture" (now a Theorem by [16]) of Iwasawa theory for imaginary quadratic fields to improve the results of [21] by working out an eigenspace-by-eigenspace Kummer's criterion (see Theorem 6.6 and 6.7 below for the precise statements).

Let $A/\mathbb{Q}$ be as above and let $A'/\mathbb{Q}$ be another elliptic curve defined over K, with complex multiplication by $\mathcal{O}_K$ and minimal conductor among all elliptic curves with this property. Notice that, under our assumptions, A' is a certain quadratic twist of A. Let L be the period lattice of A', and choose an element $\Omega_\infty \in L$ such that $L = \Omega_\infty \mathcal{O}_K$ (the existence of Ω_∞ is guaranteed by the fact that $h_K = 1$). Let ψ be the Grössencharacter attached to the curve A'/K and write $L(\overline{\psi}^k, s)$ for the primitive complex Hecke L-function attached to $\overline{\psi}^k$ for each integer $k \geq 1$. Let e be the number of roots of unity in K. Damerell's theorem shows that the Bernoulli-Hurwitz numbers defined by

$$\mathrm{BH}_k^j := \left(\frac{2\pi}{\sqrt{|D_K|}}\right)^j \frac{e \cdot L(\overline{\psi}^{k+j}, k)}{\Omega_\infty^{k+j}}, \quad k \geq 1,\ j \geq 0$$

belong to $\overline{K}$ and if $0 \leq j < k$ they belong to K. If the prime p is split in K and $(p) = \wp\wp'$, Yager has shown that the numbers BH_k^j belong to $K_\wp$, the completion of K at $\wp$, and are $\wp$-integral if $0 \leq j \leq p-1$ and $1 < k \leq p$ (see [22]). For even k, the numbers BH_k^0 coincide with the usual values of Eisenstein series $G_k(L)$, studied by Hurwitz. Our terminology follows that of Katz (see [6]). The main result of this article is:

Theorem 1.2 *Let $p \geq 7$ be unramified in K and suppose one of the following holds:*

(1) The prime p is inert in K and BH_2^0 is a p-adic unit;
(2) The prime p is split in K and the numbers BH_2^0, BH_p^{p-2} are p-adic units.

Then the image of ρ_A is as large as possible, that is, it is the full inverse image of a Cartan subgroup of $\mathrm{SL}(2, \mathbb{Z}_p)$. In particular, the image of ρ_A is as large as possible for all but finitely many inert primes p.

For $p \geq 7$, the number $\mathrm{BH}_2^0 = G_2(L)$ is not a p-adic unit only in two particular cases, namely $(D_K, p) = (-163, 181)$ and $(-67, 19)$. Furthermore, we provide (a) explicit recursive formulas to calculate all Bernoulli-Hurwitz numbers (see Remark 6.17) and (b) a simple criterion to determine whether BH_p^{p-2} is a p-adic unit in terms of Wieferich places of K, which we describe next. Let p be a split prime in K (of class number 1) and let π and π' be respectively generators of the prime ideals $\wp$ and $\wp'$ of $\mathcal{O}_K$ lying above p. Let $\nu_\wp$ be the usual $\wp$-adic valuation on K. We say that $\wp$ is a Wieferich place (in base π') if $\nu_\wp((\pi')^{p-1} - 1) > 1$ (cf. [20]). Notice that one always has $\nu_\wp((\pi')^{p-1} - 1) \geq 1$.

Theorem 1.3 (Also Corollary 6.9) *Let p be a prime that splits in K. The Bernoulli-Hurwitz number BH_p^{p-2} is a p-adic unit if and only if $\wp = (\pi)$ is not a Wieferich place in base π'.*

In proving Theorem 1.3 we will actually show that the characteristic power series of a certain Iwasawa Λ-module is a unit if and only if $\wp$ is not a Wieferich place (see Corollary 6.9). Wieferich places seem to be rather sparse (see [20] for known results). In fact, a naive heuristic argument suggests that, for each quadratic field K, there should be about $\frac{1}{2}\log(\log x)$ split primes $p \leq x$ such that a prime $\wp$ above p is a Wieferich place in base π'. A computation reveals that in the range $7 \leq p \leq 50000$ there is at most one Wieferich place for all quadratic imaginary fields K (of class number 1 and $D_K \neq -3$) and there are no Wieferich places for $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-11})$ in the given range (see the table above Remark 6.17). Hence, for a fixed elliptic curve A/K, the image of the representation ρ_A is as large as possible for all primes $7 \leq p \leq 50000$ except for, perhaps, two primes.

Remark 1.4 *Theorems 1.2 and 1.3 show that the set of exceptional primes for which the image of ρ_A may not be as large as possible is rather sparse (at least heuristically). In fact, the conditions of Theorem 1.2 are sufficient but not necessary (as a consequence of the fact that Kummer's criterion for K only provides sufficient conditions for the class number of $K(p)$ being prime to p, in the split case), and the image of ρ_A may be as large as possible even for some of those primes excluded by the theorems. As an example, let $K = \mathbb{Q}(\sqrt{-11})$ and $p = 5$. Then $\mathrm{BH}_5^3 = 135/2$ is not a 5-adic unit but a calculation with [10] shows that the class number of $K(5)$ is identically 1. See also [12], Appendix B, for other examples where some Bernoulli-Hurwitz numbers vanish modulo p but the class number of the appropriate ray class field is prime to p.*

Acknowledgements

I would like to thank David Rohrlich for his encouragement throughout this project and Ravi Ramakrishna for several suggestions and inspiring conversations. Also, I thank Rodney Yager for clarifying for me several subtle aspects of [22], and Felipe Voloch for providing me with the heuristic distribution of Wieferich places. Finally, I would like to express my gratitude to the anonymous referee for numerous suggestions and corrections.

2 Surjectivity of a Galois Representation

Let $p \geq 7$ be unramified in K. For any ring R, let $P_R\colon \mathrm{SL}(2,R) \to \mathrm{PSL}(2,R)$ be the natural projection. We write $\mathfrak{C}$ for the image of $\mathfrak{C}'$ under $P_{\mathbb{Z}_p}$, and the ring $\mathbb{Z}_p[[X]]$ will be denoted by Λ. Let $P\rho_A = P_\Lambda \circ \rho_A\colon \mathrm{Gal}(\overline{K}/\widetilde{K}) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}_p[[X]])$, then a simple lemma (see [9], Lemma 2.1) reduces the proof of Theorem 1.2 to showing that the image of $P\rho_A$ is the full inverse image of $\mathfrak{C}$ under the natural projection $P\pi_X\colon \mathrm{PSL}(2,\mathbb{Z}_p[[X]]) \longrightarrow \mathrm{PSL}(2,\mathbb{Z}_p)$ which sends X to 0.

Lemma 2.1 *Let $A/\mathbb{Q}$ be an elliptic curve and let $A'/\mathbb{Q}$ be a quadratic twist of A. Suppose that the image of ρ_A is the full inverse image of $\mathfrak{C}$ under the natural projection $P\pi_X$. Then, $\rho_{A'}$ enjoys the same property, i.e. the image of $\rho_{A'}$ is the full inverse image of $\mathrm{Im}\,\overline{\rho_{A'}}$ under π_X.*

PROOF. Let A' be a quadratic twist of A by the quadratic character χ. Then, $\rho_{A'} \cong \rho_A \otimes \chi$. Therefore

$$P\rho_A \cong P\rho_{A'} \quad \text{and} \quad P\overline{\rho_A} \cong P\overline{\rho_{A'}}. \tag{1}$$

Suppose that the image of ρ_A is the full inverse image of $\mathrm{Im}\,\overline{\rho_A}$ under π_X. Then, the image of $P\rho_A$ is the full inverse image of $\mathrm{Im}\,P\overline{\rho_A}$ under $P\pi_X$ and the same property holds for A', by Eq. (1). Thus, by Lemma 2.1 of [9], the image of $\rho_{A'}$ is the full image of $\mathrm{Im}\,\overline{\rho_{A'}}$ under π_X. This concludes the proof of the Lemma.

Hence, by the previous Lemma, we may assume that $A/\mathbb{Q}$ is an elliptic curve with complex multiplication by $\mathcal{O}_K$ and minimal conductor with this property, because any other elliptic curve with the same properties will be a quadratic twist of A.

Notice that $P\rho_A$ is a continuous group homomorphism, therefore the image is a closed subgroup of $\mathrm{PSL}(2, \mathbb{Z}_p[[X]])$. The kernel of $P\rho_A$ determines a fixed field ℓ, in particular $\mathrm{Gal}(\ell/\widetilde{K}) \hookrightarrow \mathrm{PSL}(2, \mathbb{Z}_p[[X]])$. For $i \geq 1$, let $\ell_i \subseteq \ell$ be the fixed field determined by the kernel of the reduction map

$$\mathrm{Gal}(\ell/\widetilde{K}) \hookrightarrow \mathrm{PSL}(2, \mathbb{Z}_p[[X]]) \to \mathrm{PSL}(2, \mathbb{Z}_p[[X]]/(p, X)^i).$$

In [9], the author showed that in order to show that the image of $P\rho_A$ is as large as possible it suffices to prove that the image of $P\rho_A$ on the "second layer", i.e. on the group $\mathrm{PSL}(2, \Lambda/(p, X)^2)$, is the inverse image of a full Cartan subgroup (this can be shown by using an argument involving the Frattini quotient of the kernel of $P\pi_X$). It follows that in order to prove Theorem 1.2, it is enough to show that $[\ell_2 : \ell_1] = p^4$. See [9], Section 2, for further details.

3 Siegel Functions and Elliptic Units

Theorem 2 in [14] provides an explicit description of the extension ℓ_2/ℓ_1 which will be one of the key ingredients to prove that $[\ell_2 : \ell_1] = p^4$. Before stating this theorem we introduce the Siegel functions. We follow Robert and Kubert-Lang in defining invariants as in [11] and [7], respectively.

Definition 3.1 *Let $L = \langle w_1, w_2 \rangle$ be a lattice in $\mathbb{C}$.*

(1) The Siegel functions g^{12} are defined by

$$g^{12}(z, L) = \mathfrak{k}^{12}(z, L)\Delta(L)$$

where $\mathfrak{k}(z,L) = e^{\eta(z,L)z/2}\sigma(z,L)$ *is a Klein form. In particular,* $g^{12}(z,L)$ *is an even function* (see [7] p. 26-29 for the precise definitions).

(2) *Let* I *be the free abelian group on integral ideals of* K *which are prime to* $6p$. *We express* $a \in I$ *as formal sums* $a = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathfrak{A}$ *with* $a(\mathfrak{A}) \in \mathbb{Z}$ *for all ideals* $\mathfrak{A} \subseteq \mathcal{O}_K$, *and define the degree and norm of* a *by the formulas* $\deg(a) = \sum_{\mathfrak{A}} a(\mathfrak{A})$, $N(a) = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathbf{N}(\mathfrak{A})$ *where* $\mathbf{N}(\mathfrak{A}) = |\mathcal{O}_K/\mathfrak{A}|$ *denotes the absolute norm of the ideal* $\mathfrak{A}$. *Also, for* $a \in I$ *write:*

$$g_p^{12}(a;\mathcal{O}_K) := \prod_{\mathfrak{A}=(\alpha)} g^{12}\left(\frac{\alpha}{p},\mathcal{O}_K\right)^{a(\mathfrak{A})}.$$

The primitive Robert group $\mathfrak{R}_p^*$ *is the group of all elements:*

$$g_p^{12}(a;\mathcal{O}_K), \quad a \in I \text{ such that } \deg(a) = 0,\ N(a) = 0.$$

Let $K(p)$ be the ray class field of conductor p of K, and let $\mathcal{E}_p$ be the group of units in the ring of integers of $K(p)$. Notice that $\mathcal{E}_p$ contains μ_p, the group of pth roots of unity (because $\mu_p \subseteq K[\mu_p] \subseteq K(p)$). For $p \geq 5$, the group of Robert units also contains μ_p (see [9], Lemma 4.3). The following is a theorem due to Robert ([11]), although we are using the notation of Kubert-Lang (for details about the dictionary of invariants, see [9], Theorem 4.5).

Theorem 3.2 *The Robert groups of elliptic units* $\mathfrak{R}_p^*$ *is a subgroup of* $\mathcal{E}_p$. *Moreover, the index is given by*

$$[\mathcal{E}_p \colon \mathfrak{R}_p^*] = \lambda \cdot h_p$$

where $\lambda = 2^\alpha \cdot 3^\beta$, *for some non-negative integers* α, β, *and* h_p *is the class number of* $K(p)$.

We also introduce several structure modules as in [14] and [9].

Definition 3.3 *Let* $p \geq 7$ *be a prime and define* $R = \mathbb{F}_p^2 \backslash \{(0,0)\}$.

(1) M *is the* $\mathbb{Z}$*-module of all functions* $m \colon R \to \mathbb{Z}$ *with* $m(r) = m(-r)$.

(2) *We write* N *for the* $\mathbb{Z}$*-submodule of* M *consisting of all those* $m \in M$ *that reduce modulo* p *to a function defined by a homogeneous polynomial of degree two over* $\mathbb{F}_p$.

(3) *We define a submodule* Q *consisting of all elements of* M *which satisfy the "quadratic relations" of Kubert-Lang (see [7], p. 59), i.e.* $m \in M$ *belongs to* Q *if and only if* $\sum_{r\in R} m(r)n(r) \equiv 0 \mod p$ *for all* $n \in N$. *Note that* $pM \subsetneq N \subsetneq Q$ *(for the last inclusion, see* Proposition 3 *of [14]).*

(4) *Let* $K = \mathbb{Q}(\sqrt{-d})$ *and let* τ *be a complex number in the upper half plane, defined by:*

$$\tau = \begin{cases} \sqrt{-d} & , \text{ if } -d \equiv 2,3 \mod 4, \\ \frac{1+\sqrt{-d}}{2} & , \text{ if } -d \equiv 1 \mod 4. \end{cases}$$

Let $\iota\colon \mathbb{F}_p \times \mathbb{F}_p \to \mathcal{O}_K/p\mathcal{O}_K$ be the bijection defined by:

$$\iota(r_1, r_2) = \begin{cases} r_1\tau + r_2, & \text{if } p \text{ is inert in } K; \\ r_1\pi + r_2\pi', & \text{if } p \text{ splits and } p\mathcal{O}_K = \wp \cdot \wp'; \end{cases}$$

where π is a fixed generator of $\wp$ and π' is the complex conjugate of π. Let $I\colon \mathbb{F}_p \times \mathbb{F}_p \to \mathcal{O}_K$ be a fixed lift of ι. For $r \in R$ we define:

$$g_r = g^{12}\left(\frac{I(r)}{p}, \mathcal{O}_K\right).$$

Notice that if I' is a different lift of ι, then for any $r \in R$, the values $g^{12}(\frac{I(r)}{p}, \mathcal{O}_K)$ and $g^{12}(\frac{I'(r)}{p}, \mathcal{O}_K)$ only differ by a pth root of unity (for this see [7], Remark on p. 30).

(5) *For every $m \in M$, we define a product of values of Siegel functions by:*

$$g^m = \prod_{r \in R} g_r^{m(r)}.$$

(6) *If $m \in M$, the degree and the norm of m are defined by:*

$$\deg(m) = \sum_{r \in R} m(r), \quad \mathrm{Norm}(m) = N(m) = \sum_{r \in R} m(r)\mathbf{N}(I(r))$$

Define, also, the following submodules of M:

$$M_0 = \{m \in M \mid \deg(m) = 0\}, \quad M_{0,p} = \{m \in M_0 \mid \mathrm{Norm}(m) \equiv 0 \bmod p\}$$

$$Q_0 = Q \cap M_0, \quad N_0 = N \cap M_0.$$

From the definitions, $\mathrm{Gal}(\ell_1/\widetilde{K})$ is isomorphic to a Cartan subgroup of $\mathrm{PSL}(2, \mathbb{F}_p)$, so ℓ_1 corresponds to the extension of $\widetilde{K}$ obtained by adjoining the x-coordinates of p-torsion points on A. Therefore $\ell_1 = \widetilde{K(p)} = (K(p))(\mu_{p^\infty})$ where $K(p)$, as before, denotes the ray class field of K of conductor (p). In particular, $\mu_p \subset \ell_1$. We summarize the most relevant results of [14] and [9] in the following theorem:

Theorem 3.4 *With the notation of the previous definitions:*

(1) *(Rohrlich, [14], Thm. 2) The extension of fields ℓ_2/ℓ_1 (as defined in Section 2) is generated by pth roots of values of Siegel units. More precisely, $\ell_2 = \ell_1(\{(g^m)^{1/p} : m \in N\})$.*

(2) *([9], Proposition 5.4) Let p be inert in K. If $q \in Q$ then $g^q \in K(p)$ and if $m \in M_{0,p}$ then g^m is an elliptic unit in $\mathfrak{R}_p^*$. Furthermore, the map*

$$\begin{aligned} \Psi_0\colon M_{0,p}/pM_{0,p} &\longrightarrow \mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p) \\ m + pM_{0,p} &\mapsto g^m \mod \mu_p(\mathfrak{R}_p^*)^p \end{aligned}$$

is an isomorphism of $\mathbb{F}_p$*-modules.*

(3) *([9], Remark 3.12, Lemma 3.15) The natural inclusion* $Q_0 \subset M_{0,p}$ *as* $\mathbb{Z}$*-modules induces a map* $\gamma\colon Q_0/pQ_0 \to M_{0,p}/pM_{0,p}$*. There is an isomorphism of* $\mathbb{F}_p$*-modules* $N/pQ \cong N_0/pQ_0$*, and moreover, the image of* N_0/pQ_0 *via the map* γ *has size* p^4*.*

The definition of Ψ_0 in the split case is quite a bit more delicate and some new definitions are needed. Let $\overline{R} = R/\{\pm 1\}$ and let ι be the map defined in Def. 3.3.(4). For $r \in R$, the class of r in $\overline{R}$ is denoted by $\bar{r}$. For each $\bar{r}$ in $\overline{R}$, let us fix a principal integral ideal $\mathfrak{A}_{\bar{r}}$ of $\mathcal{O}_K$ relatively prime to 6 and not divisible by p, such that $\mathfrak{A}_{\bar{r}} = (a)$ with $a \in \mathcal{O}_K$ and $a \equiv \pm\iota(r) \mod p$. For an integral ideal $\mathfrak{B} = (b)$ we define $\bar{r}(\mathfrak{B})$ to be the element $\bar{r}$ of $\overline{R}$ such that $b \equiv \pm\iota(r) \mod p$. We denote by $\overline{R}_\wp$ the set of those $\bar{r} \in \overline{R}$ such that $\wp$ divides $\mathfrak{A}_{\bar{r}}$, and we define $\overline{R}_{\wp'}$ similarly. Last, $\overline{R}^*$ will denote the set of those $\bar{r} \in \overline{R}$ such that $\mathfrak{A}_{\bar{r}}$ is relatively prime to p.

Next we describe the distribution relations satisfied by the elliptic units (as in [7], Thm. 1.4, p. 237) in terms of elements of M. The symbol $\mathbf{1}_{\bar{r}}$ will denote the characteristic function $R \to \mathbb{Z}$ for the elements $\pm r$, i.e. $\mathbf{1}_{\bar{r}}(s) = 1$ if $s = \pm r$ and is 0 otherwise.

Definition 3.5 *(1) If* p *is split in* K*, we define elements of* M *by:*

$$m_\wp := 2\sum_{\bar{r}\in\overline{R}_\wp} \mathbf{1}_{\bar{r}}, \qquad m_{\wp'} := 2\sum_{\bar{r}\in\overline{R}_{\wp'}} \mathbf{1}_{\bar{r}}$$

$$m_{\beta,\wp} := \sum_{i=0}^{p-1} \mathbf{1}_{(\beta,i)} - \mathbf{1}_{(\beta c_\wp,0)}, \quad m_{\beta,\wp'} := \sum_{i=0}^{p-1} \mathbf{1}_{(i,\beta)} - \mathbf{1}_{(0,\beta c_\wp)}$$

where β *runs through a set of representatives of* $\mathbb{F}_p^*/\{\pm 1\}$ *and* $c_\wp \equiv \pi + \pi' \mod p$*. For* $\chi\colon \mathbb{F}_p^*/\{\pm 1\} \to \mathbb{Z}_p^*$ *we also define elements of* $\mathcal{M} = M \otimes \mathbb{Z}_p$ *by:*

$$m_{\chi,\wp} = \sum_\beta \chi(\beta) m_{\beta,\wp}$$

where the sum is over a set of representatives of $\mathbb{F}_p^*/\{\pm 1\}$*, and let* $m_{\chi,\wp'}$ *be defined analogously.*

(2) *If* p *is inert in* K *simply put* $S_p = \mathfrak{R}_p^*$*. If* p *is split in* K *with* $p\mathcal{O}_K = \wp\wp'$ *and* $\wp = (\pi)$*, we define* S_p *to be the Robert group of* p*-units, i.e.* S_p *is the multiplicative group generated by* $\mathfrak{R}_p^*$ *and all powers of* π *and* π'*. Similarly, if* p *is inert, write* $\mathcal{E}_p'$ *for the group of units* $\mathcal{E}_p$ *in* $K(p)$*. If* p *is split then we define* $\mathcal{E}_p'$ *to be the group of* p*-units in* $K(p)$*.*

Theorem 3.6 ([9], §6) *Let* $\chi\colon \mathbb{F}_p^*/\{\pm 1\} \to \mathbb{Z}_p^*$ *be a non-trivial character and let* χ_0 *be the trivial character. If* p *is split in* K *then the elements of* $\mathcal{M}$ *given* *by*

$$m_{\chi,\wp},\ m_{\chi,\wp'},\ m_\pi := \frac{p-1}{2} m_\wp - m_{\chi_0,\wp},\ m_{\pi'} := \frac{p-1}{2} m_{\wp'} - m_{\chi_0,\wp'}$$

belong to $M_{0,p}$*. Furthermore:*

(1) The map $\Psi_0 : M_{0,p}/pM_{0,p} \to S_p/(\mu_p(S_p)^p)$ *given by* $m + pM_{0,p} \mapsto g^m \bmod \mu_p(S_p)^p$ *is a well-defined homomorphism of* $\mathbb{F}_p$*-vector spaces.*
(2) If p is split and we let P be the subspace generated by the elements $m_\pi, m_{\pi'}$ *in* $M_{0,p}/pM_{0,p}$*, then* Ψ_0 *restricted to P is injective and the image of P via* Ψ_0 *is the subspace of* $S_p/(\mu_p(S_p)^p)$ *generated multiplicatively by* $\pi,\ \pi'$*.*
(3) If p is inert, the map Ψ_0 *is injective. Otherwise, if p splits, the* $p-3$ *elements in the set*

$$\{m_{\chi,\wp},\ m_{\chi,\wp'} |\ \chi\colon \mathbb{F}_p^*/\{\pm 1\} \to \mathbb{Z}_p^* \text{ non-trivial }\}$$

are linearly independent modulo $p\mathcal{M}_{0,p}$*. Let H be the* $\mathbb{Z}_p$*-module spanned by them. The image of H in* $\mathcal{M}_{0,p}/p\mathcal{M}_{0,p}$*, denoted by* $\mathcal{H}$*, is precisely the kernel of* Ψ_0*.*
(4) The image of N_0/pQ_0 *in* $M_{0,p}/pM_{0,p}$*, via the map* γ *of Thm. 3.4, has trivial intersection with the kernel* $\mathcal{H}$ *of* Ψ_0*.*

Therefore, the combination of results in the previous theorem shows that in order to prove that $[\ell_2 : \ell_1] = p^4$ in the inert case, it suffices to show that the image of the composition

$$\Psi\colon N_0/pQ_0 \to M_{0,p}/pM_{0,p} \to S_p/(\mu_p(S_p)^p) \to \mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p) \hookrightarrow \ell_1^\times/(\ell_1^\times)^p$$

is 4 dimensional, where $\mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p) \to \ell_1^\times/(\ell_1^\times)^p$ is the natural map, which one easily checks to be injective. Notice that Ψ simply sends the coset of $n \in N_0$ to the coset of g^n in $\ell_1^\times$. Using Theorems 3.4 and 3.6, we see that to show Theorem 1.2 it suffices to prove the following:

Proposition 3.7 *Assume hypothesis (1) or hypothesis (2) of Theorem 1.2 according as p is inert or split in K. Then the image of* N_0/pQ_0 *in* $S_p/(\mu_p(S_p)^p)$ *injects into the group* $\mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p)$*. Thus,* $[\ell_2 : \ell_1] = p^4$*.*

By Theorem 3.2, when $p \nmid h_p$, the map $S_p/(\mu_p(S_p)^p) \to \mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p)$ is an injection, and we obtain Theorem 1.1.

4 The Galois Action

Let $G = \text{Gal}(K(p)/K) \cong (\mathcal{O}_K/p\mathcal{O}_K)^\times/\{\pm 1\}$. We define a group action of G on the set $\overline{R} := R/\{\pm 1\}$ by

$$\alpha \cdot r = \iota^{-1}(\alpha \cdot \iota(r))$$

for $\alpha \in (\mathcal{O}_K/p\mathcal{O}_K)^\times/\{\pm 1\}$, where ι is the bijection of Definition 3.3. We extend the action of G to M by defining $\alpha \cdot m(r) = m(\alpha \cdot r)$, for $m \in M$. Notice that M_0 is a $\mathbb{Z}[G]$-submodule of M. Moreover:

$$\begin{aligned} N(\alpha \cdot m) &= \sum_{r \in R} \alpha \cdot m(r)\mathbf{N}(I(r)) = \sum_{r \in R} m(\alpha \cdot r)\mathbf{N}(I(r)) \\ &= \sum_{r \in R} m(r)\mathbf{N}(\alpha^{-1} I(r)) = \mathbf{N}(\alpha^{-1})N(m) \end{aligned}$$

Thus, $M_{0,p}$ is also a $\mathbb{Z}[G]$-submodule of M. It is easy to see from the definitions that N and Q are all $\mathbb{Z}[G]$-submodules.

The primitive Robert group of units also carries a G action. To see this, let $(\mathcal{O}_K/p)^\times/\{\pm 1\} \to \text{Gal}(K(p)/K)$ be the isomorphism given by the Artin map $(\alpha) \to ((\alpha), K(p)/K)$. The action of Galois on values of the Siegel function is as follows (see [7]):

$$g^{12}\left(\frac{\beta}{p}, \mathcal{O}_K\right)^{((\alpha),K(p)/K)} = g^{12}\left(\frac{\alpha \cdot \beta}{p}, \mathcal{O}_K\right) \tag{2}$$

It is clear from equation (2) that if $u = g_p^{12}(a; \mathcal{O}_K)$ belongs to $\mathfrak{R}_p^*$ for some $a = \sum_{\mathfrak{A}} a(\mathfrak{A})\mathfrak{A}$, then

$$u^{((\alpha),K(p)/K)} = (g_p^{12}(a; \mathcal{O}_K))^{((\alpha),K(p)/K)} = g_p^{12}(\alpha \cdot a; \mathcal{O}_K)$$

where $\alpha \cdot a = \sum_{\mathfrak{A}} a(\mathfrak{A})\alpha\mathfrak{A}$. Since $\deg(\alpha \cdot a) = \deg(a) = 0$ and $N(\alpha \cdot a) = \mathbf{N}(\alpha)N(a) = 0$, we conclude that u^α belongs to $\mathfrak{R}_p^*$. Thus $(\mathfrak{R}_p^*)^G = \mathfrak{R}_p^*$.

Lemma 4.1 *The homomorphism $\Psi_0\colon M_{0,p}/pM_{0,p} \to S_p/(\mu_p(S_p)^p)$ of Theorem 3.6.(1), is a homomorphism of $\mathbb{F}_p[G]$-modules. Consequently, the homomorphism $\Psi\colon N_0/pQ_0 \to \ell_1^\times/(\ell_1^\times)^p$ is also compatible with the G-action.*

PROOF. It suffices to show that Ψ_0 is compatible with the G action. Recall that $\Psi_0(m + pM_{0,p}) = g^m \cdot (\mu_p(S_p)^p)$. Hence, for all $m \in M_{0,p}$ and $\alpha \in (\mathcal{O}_K/p)^\times/\{\pm 1\}$:

$$(g^m)^{[\alpha]} = (\prod_{r \in R} g_r^{m(r)})^{[\alpha]} = \prod_{r \in R} (g_{\alpha \cdot r})^{m(r)} = g^{\alpha \cdot m}$$

as desired, where $[\alpha] = ((\alpha), K(p)/K)$ for simplicity.

Lemma 4.2 *The image of N_0/pQ_0 in $M_{0,p}/pM_{0,p}$ is isomorphic to the direct sum $N/pM \oplus pM_0/pM_{0,p}$ of $\mathbb{F}_p[G]$-submodules. Furthermore, the 1-dimensional submodule $pM_0/pM_{0,p}$ injects into $\ell_1^\times/(\ell_1^\times)^p$.*

PROOF. The decomposition of the image of N_0/pQ_0 in $M_{0,p}/pM_{0,p}$ follows from the decomposition $N/pQ \cong N/pM \oplus pM/pQ$ (cf. [14]) and the fact that $N/pQ \cong N_0/pQ_0$. Moreover, it is easy to check that N/pM and $pM_0/pM_{0,p}$ are both $\mathbb{F}_p[G]$-modules.

Finally, in [14], Rohrlich shows that the extension field ℓ_{pM} of ℓ_1 defined by $\ell_{pM} = \ell_1(\{(g^m)^{1/p} : m \in pM\})$ is the extension obtained by adjoining to ℓ_1 the x-coordinates of $A[p^2]$, the p^2-torsion of the elliptic curve A. Thus, $\mathrm{Gal}(\ell_{pM}/\widetilde{K})$ is isomorphic to a non-split Cartan subgroup of $\mathrm{PSL}(2, \mathbb{Z}/p^2\mathbb{Z})$. As a consequence ℓ_{pM}/ℓ_1 is an extension of degree p, and $pM_0/pM_{0,p}$ injects into $\ell_1^\times/(\ell_1^\times)^p$.

By Lemma 4.1, the map Ψ is a homomorphism of $\mathbb{F}_p[G]$-modules. In particular, the kernel of the map $M_{0,p}/pM_{0,p} \to \ell_1^\times/(\ell_1^\times)^p$ is an invariant $\mathbb{F}_p[G]$-submodule. By Lemma 4.2, the $\mathbb{F}_p[G]$-submodule $pM_0/pM_{0,p}$ injects into $\ell_1^\times/(\ell_1^\times)^p$. Therefore, in order to prove that N_0/pQ_0 also injects into $\ell_1^\times/(\ell_1^\times)^p$, it suffices to show that its $\mathbb{F}_p[G]$-submodule isomorphic to N/pM injects via Ψ. We will write $S^{(p)} := S_p/(\mu_p(S_p)^p)$, $\mathcal{E}^{(p)} := \mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p)$ and let $B^{(p)}$ be the kernel of the natural $\mathbb{F}_p[G]$-map $S^{(p)} \to \mathcal{E}^{(p)}$. We will also write $N^{(p)} := \Psi_0(N/pM) \subset S^{(p)}$. Since Ψ_0 is injective on N_0/pQ_0 (by part (4) of Thm. 3.6) we conclude that $N^{(p)}$ is a 3-dimensional $\mathbb{F}_p[G]$ submodule of $S^{(p)}$. As a consequence, in order to prove Proposition 3.7, it suffices to show:

Lemma 4.3 *The intersection of $N^{(p)}$ with the kernel $B^{(p)}$ is trivial.*

5 Decomposition using Orthogonal Idempotents

If χ is an irreducible character of $G = (\mathcal{O}_K/(p))^\times/\{\pm 1\}$ then $B^{(p)}_\chi$ is the corresponding χ-component. Remember that $B^{(p)}$ is defined to be the kernel of the natural map $S^{(p)} \to \mathcal{E}^{(p)}$ and, as a consequence of Theorem 3.2, one has the index $[\mathcal{E}'_p : S_p] = \lambda \cdot h_p$ with $p \nmid \lambda$. Thus, in order to show that $p \nmid h_p$, the class number of $K(p)$, it suffices to show that $B^{(p)}_\chi = 0$ for all irreducible characters χ. This is precisely the strategy followed by Robert to prove a Kummer criterion for quadratic imaginary fields.

Thus, we shall need to understand the representations of G. The following lemma describes the irreducible representations over $\mathbb{F}_p$ of the group $G = (\mathcal{O}_K/(p))^\times/\{\pm 1\}$ for $p \geq 5$ inert in K.

Lemma 5.1 *Let $p \geq 5$ be inert in K and let $G = (\mathcal{O}_K/(p))^\times/\{\pm 1\}$. Let $\sigma^k \colon G \to (\mathcal{O}_K/(p))^\times$ be defined such that $\sigma^k(\alpha) = \alpha^k$, with k even and $2 \leq k \leq p^2 - 1$. The irreducible representations of G over $\mathbb{F}_p$, up to equivalence, are:*

(1) σ^k with $(p+1)|k$: in this case $\sigma^k \colon G \to \mathbb{F}_p^\times$ is a group character (we will also denote it by χ_k). Notice that $\alpha^{p+1} \equiv \mathbf{N}(\alpha) \mod p$. Thus, for $k \equiv 0 \mod p+1$, the map σ^k is given by

$$\alpha \mapsto (\mathbf{N}(\alpha))^{\frac{k}{p+1}} \mod p.$$

(2) σ^k with $(p+1) \nmid k$: in this case $\sigma^k \colon G \to \mathrm{GL}(\mathcal{O}_K/(p))$ and the character of σ^k is $\chi_k(\alpha) = Trace(\sigma^k(\alpha)) = \alpha^k + \alpha^{pk} \equiv 2\Re(\alpha^k) \mod p$.

The previous lemma is stated in [12], *Lemme* 9, p. 305. Let χ_k, for $2 \leq k \leq p^2 - 1$, be the irreducible character attached to the representation σ^k. The degree of χ_k is 1 when $(p+1)|k$ and 2 otherwise. We define a system of orthogonal idempotents:

$$\mathbf{1}_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1}) g \in \mathbb{F}_p[G]$$

so that $\sum_k \mathbf{1}_{\chi_k} = 1 \in \mathbb{F}_p$, where the sum is over all even k as above. Moreover, if $\mathcal{S}$ is an $\mathbb{F}_p[G]$-module, we define submodules $\mathcal{S}_\chi := \mathbf{1}_\chi \cdot \mathcal{S}$ and one has a direct sum decomposition $\mathcal{S} = \oplus_\chi \mathcal{S}_\chi$.

The following lemma describes the irreducible representations of G in the split case, when $(p) = (\pi)(\pi')$. As before, let $A[\alpha]$ be the kernel of multiplication by $\alpha \in \mathcal{O}_K$ on A. Also, we define $A[\alpha^\infty] = \bigcup_{n \geq 1} A[\alpha^n]$.

Lemma 5.2 ([22], p. 415) *Let $G_\infty = \mathrm{Gal}(K(A[p^\infty])/K)$ and let $\kappa_1 : G_\infty \to \mathbb{Z}_p^\times$, $\kappa_2 : G_\infty \to \mathbb{Z}_p^\times$ be the characters giving the actions of G_∞ on $A[\pi^\infty]$ and $A[\pi'^\infty]$ respectively. Let χ_1 (resp. χ_2) be the restriction of κ_1 (resp. κ_2) to $\Delta = \mathrm{Gal}(K(A[p])/K)$ (here we identify Δ with the maximal finite subgroup of G_∞). Then χ_1 and χ_2 generate $\mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$. Moreover, if $\mathcal{S}$ is any $\mathbb{Z}_p[\Delta]$-module and we define $\mathcal{S}_{(i_1,i_2)}$ to be the submodule of $\mathcal{S}$ on which Δ acts via $\chi_1^{i_1}\chi_2^{i_2}$, then we have a canonical decomposition*

$$\mathcal{S} = \bigoplus_{i_1, i_2 \mod (p-1)} \mathcal{S}_{(i_1,i_2)}.$$

6 Kummer's Criterion and Bernoulli-Hurwitz Numbers

6.1 *The inert case*

Let $L \subset \mathbb{C}$ be the lattice associated to the elliptic curve A and let G_k be the Eisenstein series of weight $k > 2$. We recall the reader that, in Section 2, we restricted our attention to the elliptic curve $A/\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ and of minimal conductor with this property.

The *Hurwitz numbers* attached to the elliptic curve A are the numbers:

$$G_k(L) = \sum_{w \in L \setminus \{0\}} \frac{1}{w^k}$$

where the sum is over all the non-zero elements of L, and $k > 2$ is divisible by e, the number of roots of unity in the field of complex multiplication K (in our case $e = 2$, so k is even). The definition of $G_2(L)$ is of course more delicate:

$$G_2(L) = \lim_{t \to 0^+} \sum_{w \in L \setminus \{0\}} \frac{1}{w^2 |w|^{2t}}$$

and we refer the reader to [24] for further details. The numbers $G_2(L)$ are given in the following table:

D_K	-3	-4	-7	-8	-11	-19	-43	-67	-163
$G_2(L)$	0	0	1/2	1/2	2	2	12	$2 \cdot 19$	$4 \cdot 181$

The values $G_k(L)$ can be reinterpreted as special values of Hecke L-functions (we use the notation BH_k^0 of the introduction).

Proposition 6.1 *Let K be a quadratic imaginary field of class number $h_K = 1$ and let k be an integer divisible by e, the number of roots of unity in K. Then $L(\overline{\psi}^k, k)/\Omega_\infty^k$ is rational and $\mathrm{BH}_k^0 = e \cdot L(\overline{\psi}^k, k)/\Omega_\infty^k = G_k(L)$.*

PROOF. By the properties of the Grössencharacter, if $k \equiv 0 \mod e$ then $\psi^k(\mathfrak{A}) = \alpha^k$ where α is any generator of $\mathfrak{A}$. Also recall that $L = \Omega_\infty \mathcal{O}_K$ and $\mathcal{O}_K$ is assumed to be a PID, so every non-zero ideal has exactly e generators. Then, for $k \geq 4$ with $e|k$, one has:

$$\begin{aligned} G_k(L) &= \sum_{w \in L \setminus \{0\}} \frac{1}{w^k} = \sum_{\alpha \in \mathcal{O}_K \setminus \{0\}} \frac{1}{(\Omega_\infty \alpha)^k} \\ &= \frac{e}{\Omega_\infty^k} \sum_{\mathfrak{A} = (\alpha) \neq (0)} \frac{\overline{\alpha}^k}{\mathbf{N}(\mathfrak{A})^k} = \frac{e}{\Omega_\infty^k} L(\overline{\psi}^k, k). \end{aligned}$$

And one can proceed similarly in the case $k = 2$:

$$
\begin{aligned}
G_2(L) &= \lim_{t \to 0^+} \sum_{w \in L \setminus \{0\}} \frac{1}{w^2 |w|^{2t}} = \lim_{t \to 0^+} \sum_{\alpha \in \mathcal{O}_K \setminus \{0\}} \frac{1}{(\Omega_\infty \alpha)^2 |\Omega_\infty \alpha|^{2t}} \\
&= \lim_{t \to 0^+} \frac{e}{\Omega_\infty^{2+2t}} \sum_{\mathfrak{A} = (\alpha) \neq (0)} \frac{\overline{\alpha}^2}{\mathbf{N}(\mathfrak{A})^{2+t}} = \lim_{t \to 0^+} \frac{e}{\Omega_\infty^{2+2t}} L(\overline{\psi}^2, 2+t) \\
&= \frac{e}{\Omega_\infty^2} L(\overline{\psi}^2, 2).
\end{aligned}
$$

where, to calculate the limit, we have used the fact that $L(\overline{\psi}^2, s)$ has an analytic continuation to the whole complex plane.

Lemma 6.2 ([12], Cor. 14, Prop. 16) *Let $p \geq 5$ be inert in K and let $0 < k < p^2 - 1$ be even. If $k \neq p + 1$ then $G_k(L)$ is p-integral. If $k = p + 1$ then $pG_k(L)$ is p-integral and in fact, it is a p-unit ($pG_k(L) \not\equiv 0 \mod p$).*

Next, we state Robert's theorem, specialized to our case. Recall that we assumed that K is a quadratic imaginary field of class number one, and $D_K \neq -3$ or -4.

Theorem 6.3 (Robert, [12]) *Let $p \geq 5$ be an inert prime of K and let $0 < k < p^2 - 1$ be even. Suppose that:*

(1) If $(p + 1)|k$ but $k \neq p + 1$, then $G_k(L) \not\equiv 0 \mod p$;
(2) If $(p + 1) \nmid k$, then $G_k(L) \not\equiv 0 \mod p$ or $G_{p(k)}(L) \not\equiv 0 \mod p$, where $0 < p(k) < p^2 - 1$ is an even integer congruent to $pk \mod p^2 - 1$.

Let χ_k be the irreducible character attached to the representation σ^k. Then $B^{(p)}_{\chi_k} = 0$. Hence, if every even k satisfies the condition above, then $p \nmid h_p$.

The previous result is a combination of the following results in [12]: Theorem 1, Lemma 27 and Proposition B.1. Notice that in our case $h_K = 1$.

Corollary 6.4 *Let K be as before. Let $p \geq 5$ be inert in K (and $p \neq 181$ if $D_K = -163$). Then $B^{(p)}_{\chi_2} = B^{(p)}_{\chi_{p+1}} = 0$.*

PROOF. By Lemma 6.2, $pG_{p+1}(L)$ is invertible modulo p, thus, by the Theorem, the component $B^{(p)}_{\chi_{p+1}}$ is trivial.

For the case $k = 2$, one has the well-known values of $G_2(L)$ (see the table above). Notice that the only divisors larger than 3 are $p = 19$, which splits for $D_K = -67$ and $p = 181$ which is inert for $D_K = -163$. However, we have excluded the pair $p = 181$, $D_K = -163$ from our main theorem.

Remark 6.5 *After some calculations, one can check that for $D_K = -163$, in fact,*

$$G_2(L) \equiv G_{362}(L) \equiv 0 \mod 181,$$

so we cannot use part (2) of Theorem 6.3 to conclude that $B^{(181)}_{\chi_2} = 0$.

6.2 The split case

Let p be split and let $\wp, \wp'$ be the primes of K above p. Even though Robert proved a Kummer-type criterion for the class number of the ray class field $K(\wp)$, his work does not cover the field $K(p)$. However, R. Yager took care of this case in [21]. In this subsection we make use of Yager's work on the "two-variable main conjecture" ([22]) to show an eigenspace-by-eigenspace analysis of the class number of $K(p)$ similar to that of Theorem 6.3.

Theorem 6.6 *Suppose that $k+j \equiv 0 \mod 2$ with $k > j \geq 0$ and suppose that BH^j_k is a p-adic unit. Then $B^{(p)}_{(i_1,i_2)} = 0$, where $(i_1, i_2) \equiv (k, -j) \mod (p-1)$.*

Before we give the proof of the theorem, we need to introduce the key ingredient, which is Theorem 30 of [22]. Let A/K be as before, let $p \geq 5$ be a split prime of K, put $K_n = K(A[p^{n+1}])$ and $K_\infty = \bigcup_{n\geq 0} K_n$. We write $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ for the Galois group of K_∞ over K_0, and $\Delta = \mathrm{Gal}(K_0/K)$. Then $G_\infty = \mathrm{Gal}(K_\infty/K) = \Gamma \times \Delta$. Let $U_{n,\nu}$ be the local units of the completion of K_n at a prime ν lying above $\wp$ which are congruent to 1 modulo ν, and put $U_n = \prod_{\nu|\wp} U_{n,\nu}$. Let $\mathfrak{R}^*_{p,n}$ be Robert's group of elliptic units for K_n. We denote by $\mathfrak{R}^{*1}_{p,n}$ the subgroup of $\mathfrak{R}^*_{p,n}$ formed by those elements which are congruent to 1 modulo each prime of K_n lying above $\wp$ and denote by $\overline{\mathfrak{R}^{*1}_{p,n}}$ their closure in U_n. As in Lemma 5.2, we write $(U_n/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)}$ for the eigenspace of $U_n/\overline{\mathfrak{R}^{*1}_{p,n}}$ on which Δ acts via $\chi_1^{i_1}\chi_2^{i_2}$. Let us define:

$$Y_{(i_1,i_2)} = \varprojlim (U_n/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)}$$

where the inverse limit is taken relative to the norm maps. Let $\Lambda = \mathbb{Z}_p[[T_1, T_2]]$ be a ring of formal power series in two variables. Then $Y_{(i_1,i_2)}$ can be regarded as a Λ-module as follows. Choose a topological generator u of $(1 + p\mathbb{Z}_p)^\times$ and let γ_1 and γ_2 be topological generators of Γ such that $\kappa_1(\gamma_1) = \kappa_2(\gamma_2) = u$ and $\kappa_1(\gamma_2) = \kappa_2(\gamma_1) = 1$ (the definition of κ_1 and κ_2 is in the statement of Lemma 5.2). The group $Y_{(i_1,i_2)}$ can be endowed with a unique Λ-module structure such that $\gamma_1 y = (1 + T_1)y$ and $\gamma_2 y = (1 + T_2)y$ for all $y \in Y_{(i_1,i_2)}$. In what follows, $\overline{\mathcal{O}}^\infty_\wp$ will denote the ring of integers of a certain unramified extension of the completion of K at $\wp$ (as defined in [22], p. 419).

Theorem 6.7 ([16]; [22], Thm. 30) *Let i_1 and i_2 be integers modulo $p-1$. Then there is a power series $\mathcal{G}_{(i_1,i_2)}(T_1, T_2) \in \overline{\mathcal{O}}^\infty_\wp[[T_1, T_2]]$ such that:*

(1) For each pair of integers k, j with $k > j \geq 0$ and $(k, -j) \equiv (i_1, i_2) \mod p-1$ one has

$$\mathcal{G}_{(i_1,i_2)}(u^k - 1, u^j - 1) = \left(1 - \frac{\psi(\wp)^{k+j}}{\mathbf{N}\wp^{j+1}}\right)\left(1 - \frac{\overline{\psi}(\wp')^{k+j}}{\mathbf{N}\wp'^k}\right)(k-1)! \cdot \frac{\mathrm{BH}_k^j}{\Omega_\wp^{(k+j)}}$$

where $\Omega_\wp$ is a certain $\wp$-adic unit in $\overline{K_\wp}$, the closure of the completion of K at $\wp$. Moreover, there is an element $G_{(i_1,i_2)}(T_1, T_2) \in \Lambda$ which generates the same ideal in $\overline{\mathcal{O}}_\wp^\infty[[T_1, T_2]]$ as $\mathcal{G}_{(i_1,i_2)}$.

(2) If $(i_1, i_2) \not\equiv (1, 1) \mod p-1$ then $Y_{(i_1,i_2)}$ is isomorphic to $\Lambda/G_{(i_1,i_2)}\Lambda$, as Λ-modules.

(3) If $(i_1, i_2) \equiv (1, 1) \mod p-1$ then there is an integer $M \geq 0$ such that $Y_{(1,1)}$ is isomorphic to $\mathcal{H}/G_{(1,1)}H$ where we define $\mathcal{H}$ to be the ideal of Λ generated by $1+T_1-u$ and $(1+T_2)^{p^M} - u^{p^M}$ and H is the ideal generated by $1+T_1-u$ and $1+T_2-u$.

The integer M of Theorem 6.7, part (3), can be defined as follows. Let r_m be the index of the subgroup generated by π' in $(\mathcal{O}_K/\wp^{m+1})$, for all $m \geq 0$. Then there exists an integer M such that $r_m = r_0 p^m$ for $m < M$ and $r_m = r_0 p^M$ for $m \geq M$. Alternatively, M is one unit less than the $\wp$-adic valuation of $(\pi')^{p-1} - 1$. In particular, a prime ideal $\wp$ is a Wieferich place (in base π') if and only if $M > 0$.

Proposition 6.8 *If $M = 0$ then $G_{(1,1)}(T_1, T_2)$ is a unit power series in $\Lambda = \mathbb{Z}_p[[T_1, T_2]]$, where $G_{(1,1)}$ is the power series appearing in Theorem 6.7. Thus, if $M = 0$ then $Y_{(1,1)}$ is trivial.*

PROOF. All referenced results (those with a numbering ≥ 22) in this proof can be found in [22]. Let $M = 0$ and put $U^\infty = \varprojlim U_n$. By Lemma 24, there is an injection $W = W_{(1,1)} : U^\infty_{(1,1)} \to \Lambda$ and the image is the ideal of Λ generated by $1+T_1-u$ and $1+T_2-u$, where u is a topological generator of $(1+p\mathbb{Z}_p)^\times$. Let α_1 and α_2 be elements of $U^\infty_{(1,1)}$ such that

$$W(\alpha_1) = 1 + T_1 - u, \quad W(\alpha_2) = 1 + T_2 - u.$$

By Lemma 28, $H_{(1,1)}$ is also the ideal $H = (1+T_1-u, 1+T_2-u)$ of Λ. Let D be the Λ-submodule of the completion of elliptic units in $U^\infty_{(1,1)}$ defined as in p. 440-441 of [22]. By Theorem 29,

$$W_{(1,1)}(D_{(1,1)}) = \Omega_\wp \cdot (\phi_{(1,1)})^{-1} \cdot \mathcal{G}_{(1,1)} \cdot H_{(1,1)}. \tag{3}$$

where $\Omega_\wp$ is a $\wp$-adic unit and $\phi_{(1,1)}(T_1, T_2)$ is a unit power series. Let e_1, e_2 be elements of $D_{(1,1)}$ such that $W_{(1,1)}(e_1) = \Omega_\wp \cdot (\phi_{(1,1)})^{-1} \cdot \mathcal{G}_{(1,1)} \cdot (1+T_1-u)$ and $W_{(1,1)}(e_2) = \Omega_\wp \cdot (\phi_{(1,1)})^{-1} \cdot \mathcal{G}_{(1,1)} \cdot (1+T_2-u)$. Let $\mathcal{G}_\beta^{(1,1)}$ be the unique power series whose existence is proven in Theorem 22, for every $\beta \in U^\infty$. Then, by Theorem 27,

$$\mathcal{G}_{e_1}^{(1,1)} = \Omega_\wp \cdot \mathcal{G}_{(1,1)} \cdot (1 + T_1 - u), \quad \mathcal{G}_{e_2}^{(1,1)} = \Omega_\wp \cdot \mathcal{G}_{(1,1)} \cdot (1 + T_2 - u).$$

By Theorem 22:

$$\mathcal{G}_{e_1\alpha_2}^{(1,1)} = (1 + T_2 - u)\mathcal{G}_{e_1}^{(1,1)} = (1 + T_1 - u)\mathcal{G}_{e_2}^{(1,1)} = \mathcal{G}_{e_2\alpha_1}^{(1,1)}$$

and so, again by Theorem 27, $W_{(1,1)}(e_1\alpha_2) = W_{(1,1)}(e_2\alpha_1)$. Since $W_{(1,1)}$ is an injection, we conclude that $e_1\alpha_2 = e_2\alpha_1$ and α_1/α_2 belongs to $D_{(1,1)}$. Thus $W(\alpha_1) - W(\alpha_2) = T_1 - T_2 \in W_{(1,1)}(D_{(1,1)})$ and by Eq. (3) there are $A, B \in \Lambda$ such that

$$T_1 - T_2 = \Omega_\wp \cdot (\phi_{(1,1)})^{-1} \cdot \mathcal{G}_{(1,1)} \cdot (A \cdot (1 + T_1 - u) + B \cdot (1 + T_2 - u)).$$

Let π be a generator of $\wp$. If we let $T_1 = 2\pi$ and $T_2 = \pi$ then the $\wp$-adic valuation of the left hand side of the last displayed equation is 1 and the $\wp$-adic valuation of $(A(2\pi, \pi) \cdot (1 + 2\pi - u) + B(2\pi, \pi) \cdot (1 + \pi - u))$ is at least 1, and so it must be equal to 1 and $\mathcal{G}_{(1,1)}(2\pi, \pi)$ must be a $\wp$-adic unit, and so $\mathcal{G}_{(1,1)}(T_1, T_2)$ must be a unit power series. Since $G_{(1,1)}(T_1, T_2)$ generates the same ideal as $\mathcal{G}_{(1,1)}$, we conclude that $G_{(1,1)}$ is also a unit power series, as desired.

The following corollary provides a proof of Theorem 1.3.

Corollary 6.9 *The series $G_{(1,1)}$ is a unit power series if and only if $M = 0$. Hence, $\wp$ is a Wieferich place (in base π') if and only if BH_p^{p-2} is not a p-adic unit.*

PROOF. The previous proposition shows that if $M = 0$ then $G_{(1,1)}$ (and $\mathcal{G}_{(1,1)}$) is a unit power series and the value of $\mathcal{G}_{(1,1)}$ given by Theorem 6.7, part (1), shows that for $k = p$, $j = p-2$, one has $(p, p-2) \equiv (1, -1) \mod p-1$ and the number BH_p^{p-2} must be a p-adic unit. On the other hand, if $M > 0$ then Theorem 6.7 states that, in particular, $G_{(1,1)}(T_1, T_2) \cdot (1 + T_1 - u, 1 + T_2 - u)\Lambda$ is a Λ-submodule of $(1 + T_1 - u, (1 + T_2)^{p^M} - u^{p^M})\Lambda$. As a consequence, the series $G_{(1,1)}$ belongs to the ideal of Λ generated by

$$1 + T_1 - u \quad \text{and} \quad \frac{(1 + T_2)^{p^M} - u^{p^M}}{1 + T_2 - u}.$$

Then $G_{(1,1)}$ is not a unit of Λ (because the constant term belongs to $p\mathbb{Z}_p$) and $\mathcal{G}_{(1,1)}$ is not a unit power series either. Thus the value $\mathcal{G}_{(1,1)}(u^p - 1, u^{p-2} - 1)$ is not a $\wp$-adic unit and the number BH_p^{p-2} cannot be a $\wp$-adic unit either. Since BH_p^{p-2} is a rational number, it is not a p-adic unit.

6.3 The (two-variable) Main Conjecture

In this subsection, we remind the reader of the statement of the two-variable Main Conjecture of Iwasawa theory for imaginary quadratic fields. We refer the reader to [16] for more details and the proof of the conjecture. Let K_n, K_∞ be as before, let H_n be the maximal unramified p-extension of K_n and put $H_\infty = \bigcup_{n\geq 0} H_n$. Let M_∞ be the maximal abelian p-extension of K_∞ unramified outside $\wp$, and let $\mathcal{X}_\infty$ denote the Galois group of M_∞/K_∞. Let A_n be the p-part of $\mathrm{Cl}(K_n)$, so that $A_n \cong \mathrm{Gal}(H_n/K_n)$, and write $\mathcal{A} = \varprojlim A_n$, where the inverse limit is taken over the usual norm maps on the class groups. Then $\mathrm{Gal}(H_\infty/K_\infty) \cong \mathcal{A}$. Let $Y_{(i_1,i_2)}$ be as before, and similarly define $\mathcal{A}_{(i_1,i_2)}$ and $(\mathcal{X}_\infty)_{(i_1,i_2)}$. Finally, let $\mathcal{E}^1_{p,n}$ be the global units of K_n which are congruent to 1 modulo each prime of K_n lying above $\wp$, let $\mathfrak{R}^{*1}_{p,n} = \mathcal{E}^1_{p,n} \cap \mathfrak{R}^*_{p,n}$ and let $\overline{\mathcal{E}^1_{p,n}}, \overline{\mathfrak{R}^{*1}_{p,n}}$ denote their closure in U_n. Class field theory provides a very useful exact sequence between all these elements:

$$0 \to \varprojlim(\overline{\mathcal{E}^1_{p,n}}/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)} \to Y_{(i_1,i_2)} \to (\mathcal{X}_\infty)_{(i_1,i_2)} \to \mathcal{A}_{(i_1,i_2)} \to 0 \qquad (4)$$

Before we state the Main Conjecture, we remind the reader of some terminology. A finitely generated Λ-module is called pseudo-null if it is annihilated by an ideal of height 2. A pseudo-isomorphism of Λ-modules is a map with pseudo-null kernel and cokernel. It follows from the classification theorem for Λ-modules that for every finitely generated torsion Λ-module Y we can find $g_i \in \Lambda$, for some $1 \leq i \leq n$, such that Y and $\oplus_{i=1}^n \Lambda/g_i\Lambda$ are pseudo-isomorphic. The characteristic ideal $(\prod g_i)\Lambda$ is a well-defined invariant of Y which we will denote by $\mathrm{char}(Y)$. A generator of $\mathrm{char}(Y)$ is usually called a characteristic power series, and it satisfies the following properties (see, for example, [15], §0.2):

- $\mathrm{char}(Y)Y$ is pseudo-null, and
- if $Y' \subseteq Y$ then $\mathrm{char}(Y/Y')\,\mathrm{char}(Y') = \mathrm{char}(Y)$.

The modules that appear in Eq. (4) are finitely generated torsion Λ-modules and:

Theorem 6.10 (Main Conjecture, Rubin, [16], Thm. 4.1) *For all characters $\chi_1^{i_1}\chi_2^{i_2}$ of Δ,*

$$\mathrm{char}((\mathcal{X}_\infty)_{(i_1,i_2)}) = \mathrm{char}(Y_{(i_1,i_2)})$$

and

$$\mathrm{char}\left(\varprojlim(\overline{\mathcal{E}^1_{p,n}}/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)}\right) = \mathrm{char}\left(\mathcal{A}_{(i_1,i_2)}\right).$$

We will also make use of the following theorem:

Theorem 6.11 (Rubin, [16], Thm. 3.3) *Let $K_0 = K(A[p])$, let $\mathcal{E}_p$ be the group of units in the ring of integers of K_0, and let $\mathfrak{R}^*_p$ be the group of elliptic units in $\mathcal{E}_p$. For every irreducible character $\chi_1^{i_1}\chi_2^{i_2}$ of $\Delta \cong \mathrm{Gal}(K_0/K)$,*

$$\left|\mathrm{Cl}(K_0)_{(i_1,i_2)}\right| = \left|(\mathcal{E}_p/\mathfrak{R}^*_p)_{(i_1,i_2)})\right|.$$

Now we are ready to show the last two results that we will need for the proof of Theorem 6.6.

Lemma 6.12 *Let $f(T_1,T_2) \in \Lambda$ and let Y be a finitely generated torsion Λ-module with no non-zero pseudo-null submodules and* $\mathrm{char}(Y) = f(T_1,T_2)$*. Then, Y/Y^p is non-trivial if and only if $f(T_1,T_2)$ is not a unit over $\mathbb{F}_p[[T_1,T_2]]$.*

PROOF. By the classification of finitely generated torsion Λ-modules, and since Y does not have non-zero pseudo-null submodules (by assumption), we deduce that Y is isomorphic (and not just pseudo-isomorphic) to $\oplus_{i=1}^n \Lambda/g_i\Lambda$ for some $g_i \in \Lambda$ with $(\prod g_i)\Lambda = f\Lambda$. Without loss of generality, we may assume $f = \prod g_i$. Thus:

$$Y/Y^p \cong \bigoplus_{i=1}^n \Lambda/(p, g_i(T_1,T_2))\Lambda \cong \bigoplus_{i=1}^n \mathbb{F}_p[[T_1,T_2]]/(\overline{g_i(T_1,T_2)})$$

where $\overline{g_i(T_1,T_2)}$ is the reduction of g_i modulo $p\Lambda$. Thus, Y/Y^p is non-trivial if and only if $\mathbb{F}_p[[T_1,T_2]]/(\overline{g_i(T_1,T_2)})$ is non-trivial for some $1 \le i \le n$ and, in turn, this is equivalent to $\overline{g_i(T_1,T_2)}$ being a non-unit of $\mathbb{F}_p[[T_1,T_2]]$, for some $1 \le i \le n$. Finally, $f = \prod g_i$ is a non-unit over $\mathbb{F}_p[[T_1,T_2]]$ if and only if there is an i, with $1 \le i \le n$, such that g_i is a non-unit over $\mathbb{F}_p[[T_1,T_2]]$.

Remark 6.13 *The modules $\overline{\mathcal{E}}_\infty = \varprojlim \overline{\mathcal{E}^1_{p,n}}$ and $\overline{\mathfrak{R}}_\infty = \varprojlim \overline{\mathfrak{R}^{*1}_{p,n}}$ satisfy:*

$$\mathrm{rank}_\Lambda(\overline{\mathcal{E}}_\infty) = \mathrm{rank}_\Lambda(\overline{\mathfrak{R}}_\infty) = 1$$

and $(\overline{\mathcal{E}}_\infty)_{\mathrm{torsion}} = (\overline{\mathfrak{R}}_\infty)_{\mathrm{torsion}} = 0$ (see [16], Cor. 7.8). Thus, $\overline{\mathcal{E}}_\infty/\overline{\mathfrak{R}}_\infty$ is a torsion Λ-module with no non-zero pseudo-null submodules. The Λ-module $Y_{(i_1,i_2)}$ does not have non-zero pseudo-null submodules by Theorem 6.7, and $(\mathcal{X}_\infty)_{(i_1,i_2)}$ does not have non-zero pseudo-null submodules by Theorem 5.3, part (v), of [16] (this result is due to Perrin-Riou). As a consequence of the exact sequence Eq. (4), the torsion Λ-module $\mathcal{A}_{(i_1,i_2)}$ does not have non-zero pseudo-null submodules either.

Proposition 6.14 *Suppose that the component $B^{(p)}_{(i_1,i_2)}$ of the kernel of the map $\mathfrak{R}^*_p/(\mu_p(\mathfrak{R}^*_p)^p) \to \mathcal{E}_p/(\mu_p(\mathcal{E}_p)^p)$ is non-trivial. Then, $Y_{(i_1,i_2)}/(Y_{(i_1,i_2)})^p$ is non-trivial also.*

PROOF. Put $C_1 = (\mathcal{E}_p/\mathfrak{R}^*_p)$. Suppose the component $B^{(p)}_{(i_1,i_2)}$ is non-trivial. Then, by definition, $(C_1/C_1^p)_{(i_1,i_2)}$ is non-trivial. In particular, $(C_1)_{(i_1,i_2)}$ has a non-trivial element of order p, and therefore p divides the order of $(\mathcal{E}_p/\mathfrak{R}^*_p)_{(i_1,i_2)}$. By Theorem 6.11, p also divides the order of $\mathrm{Cl}(K_0)_{(i_1,i_2)}$.

As before, for $n \geq 0$, let A_n be the p-part of the class group $\mathrm{Cl}(K_n)$ and put $\mathcal{A}_{(i_1,i_2)} = \varprojlim (A_n)_{(i_1,i_2)}$. Then, by the considerations at the beginning of the proof, we conclude that $(A_0)_{(i_1,i_2)}$ is non-trivial. Notice that the norm maps $A_{n+1} \to A_n$ are surjective (see [23], Thm 10.1), therefore they are also surjective when restricted to the $\chi_1^{i_1}\chi_2^{i_2}$-component. Thus, $\mathcal{A}_{(i_1,i_2)}$ and $\mathcal{A}_{(i_1,i_2)}/\mathcal{A}^p_{(i_1,i_2)}$ are non-trivial also.

Let $f(T_1,T_2)$ be the characteristic power series of $\mathcal{A}_{(i_1,i_2)}$. Remark 6.13 shows that $\mathcal{A}_{(i_1,i_2)}$ does not have non-zero pseudo-null submodules. Since $\mathcal{A}_{(i_1,i_2)}/\mathcal{A}^p_{(i_1,i_2)}$ is non-trivial, $f(T_1,T_2)$ is a non-unit over $\mathbb{F}_p[[T_1,T_2]]$, by Lemma 6.12. By the Main Conjecture,

$$f(T_1,T_2) = \mathrm{char}\left(\mathcal{A}_{(i_1,i_2)}\right) = \mathrm{char}\left(\varprojlim (\overline{\mathcal{E}^1_{p,n}}/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)}\right).$$

Thus, if we put $D_{(i_1,i_2)} = \varprojlim (\overline{\mathcal{E}^1_{p,n}}/\overline{\mathfrak{R}^{*1}_{p,n}})_{(i_1,i_2)}$, then $D_{(i_1,i_2)}$ is a torsion Λ-module with no non-zero pseudo-null submodules (see Remark 6.13) and $\mathrm{char}(D_{(i_1,i_2)}) = f(T_1,T_2)$ is a non-unit over $\mathbb{F}_p[[T_1,T_2]]$. Since $D_{(i_1,i_2)} \subseteq Y_{(i_1,i_2)}$ (notice that the injective map $D_{(i_1,i_2)} \to Y_{(i_1,i_2)}$ in Eq. (4) is just the natural inclusion),

$$\mathrm{char}(Y_{(i_1,i_2)}) = \mathrm{char}(D_{(i_1,i_2)})\,\mathrm{char}(Y_{(i_1,i_2)}/D_{(i_1,i_2)})$$

and, therefore, $f(T_1,T_2)$ divides $\mathrm{char}(Y_{(i_1,i_2)})$. Hence $\mathrm{char}(Y_{(i_1,i_2)})$ is a non-unit over $\mathbb{F}_p[[T_1,T_2]]$. Finally, the object $Y_{(i_1,i_2)}$ is a torsion Λ-module with no non-zero pseudo-null submodules (see Remark 6.13) so, by Lemma 6.12, the quotient $Y_{(i_1,i_2)}/(Y_{(i_1,i_2)})^p$ is non-trivial, as desired.

6.4 Proof of Theorem 6.6

We will prove the contrapositive of the statement of the theorem. Suppose that k, j are integers with $k + j \equiv 0 \mod 2$ and $k > j \geq 0$. Further, suppose that $B^{(p)}_{(i_1,i_2)}$ is non-trivial, where $(k, -j) \equiv (i_1, i_2) \mod p-1$. By Proposition 6.14, there exists a non-trivial element in $Y_{(i_1,i_2)}/(Y_{(i_1,i_2)})^p$.

First assume that $(i_1, i_2) \equiv (1,1) \mod p-1$. Then Corollary 6.9 implies that $M > 0$ and BH_p^{p-2} is not a p-adic unit, as claimed.

Suppose that $(i_1, i_2) \not\equiv (1,1) \mod p-1$. Then, by Theorem 6.7, $Y_{(i_1,i_2)} \cong \Lambda/G_{(i_1,i_2)}(T_1,T_2)\Lambda$ with $G = G_{(i_1,i_2)}(T_1,T_2)$ as in the statement of the theorem, and

$$Y_{(i_1,i_2)}/(Y_{(i_1,i_2)})^p \cong \Lambda/(p, G_{(i_1,i_2)})\Lambda \cong \mathbb{F}_p[[T_1,T_2]]/(\overline{G_{(i_1,i_2)}})$$

where $\overline{G}$ is the reduction modulo $p\Lambda$ of G. Since

$$\mathcal{G}_{(i_1,i_2)}(u^k-1, u^j-1) = \left(1 - \frac{\psi(\wp)^{k+j}}{\mathbf{N}\wp^{j+1}}\right)\left(1 - \frac{\overline{\psi}(\wp')^{k+j}}{\mathbf{N}\wp'^k}\right)(k-1)! \cdot \frac{\mathrm{BH}_k^j}{\Omega_\wp^{(k+j)}}$$

we conclude that if BH_k^j was a p-adic unit then $\mathcal{G}_{(i_1,i_2)}(u^k-1,u^j-1)$ would be a $\wp$-adic unit and the series $\mathcal{G}_{(i_1,i_2)}$ would be a unit of $\overline{\mathcal{O}}_\wp^\infty[[T_1,T_2]]$. Since $G_{(i_1,i_2)} \in \Lambda$ generates the same ideal, then $\overline{G_{(i_1,i_2)}}$ would be necessarily a unit of $\mathbb{F}_p[[T_1,T_2]]$ and the ideal $(\overline{G_{(i_1,i_2)}})$ would generate all of $\mathbb{F}_p[[T_1,T_2]]$. Hence, if BH_k^j was a p-adic unit, the space $Y_{(i_1,i_2)}/(Y_{(i_1,i_2)})^p$ would be trivial, and a contradiction occurs for we have previously shown the existence of a non-trivial element. Thus, BH_k^j must have positive p-adic valuation, and this finishes the proof of Theorem 6.6.

6.5 The spaces $B^{(p)}_{(2,0)}$, $B^{(p)}_{(0,2)}$ and $B^{(p)}_{(1,1)}$

Proposition 6.15 *If $\mathrm{BH}_2^0 = G_2(L)$ is a p-adic unit then the subspaces $B^{(p)}_{(2,0)}$ and $B^{(p)}_{(0,2)}$ are trivial. Consequently, the spaces $B^{(p)}_{(2,0)}$ and $B^{(p)}_{(0,2)}$ may be non-trivial only if K is the quadratic field with $D_K = -67$ and $p = 19$.*

PROOF. Let p be a split prime of K. Let $\wp$ be a prime above p and let $\mathcal{E}_\wp$ be the group of units in the ring of integers of $K(\wp)$ and let $\mathfrak{R}_\wp^*$ be the subgroup of Robert's elliptic units. We remind the reader that, even though $\mu_p \subset \mathfrak{R}_p^*$, the roots of unity are not included in $\mathfrak{R}_\wp^*$ (and, in fact, they are not in $\mathcal{E}_\wp$ either). Put $\mathcal{E}_\wp^{(p)} = \mathcal{E}_\wp/(\mathcal{E}_\wp)^p$ and $R_\wp^{(p)} = \mathfrak{R}_\wp^*/(\mathfrak{R}_\wp^*)^p$ and let $B_\wp$ be the kernel of the natural map $R_\wp^{(p)} \to \mathcal{E}_\wp^{(p)}$. Let k be an integer multiple of e and let σ^k the kth power of the isomorphism $\sigma : G_\wp = \mathrm{Gal}(K(\wp)/K) \cong (\mathcal{O}_K/\wp)^\times/\{\pm 1\}$, regarded as an irreducible representation of $G_\wp$ over $\mathbb{F}_p$. In [12] it is shown that if k is an even integer and $G_k(L)$ is a p-adic unit then the subspace $(B_\wp)_{\sigma^k}$ is trivial. In particular, if $\mathrm{BH}_2^0 = G_2(L)$ is a p-adic unit, then $(B_\wp)_{\sigma^2}$ is trivial. Notice that this result is independent of the chosen prime above p. Hence, if σ' is the irreducible representation $\mathrm{Gal}(K(\wp')/K) \cong (\mathcal{O}_K/\wp')^\times/\{\pm 1\}$ then if $G_2(L)$ is a p-adic unit then also $(B_{\wp'})_{\sigma'^2}$ is trivial.

Recall that $B^{(p)}$ is defined as the kernel of

$$S^{(p)} = S_p/(\mu_p(S_p)^p) \longrightarrow \mathcal{E}^{(p)} = \mathcal{E}'_p/(\mu_p(\mathcal{E}'_p)^p)$$

where, in the split case, S_p and $\mathcal{E}'_p$ are, respectively, the group of p-Robert units and the group of p-units in $K(p)$. Notice that the map is definitely injective on the subgroup generated by the powers of π and π', so the kernel $B^{(p)}$ coincides with the kernel of

$$R^{(p)} = \mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p) \longrightarrow \mathcal{E}^{(p)}.$$

Let χ_1, χ_2 be the characters of $\mathrm{Gal}(K(A[p])/K)$ defined in Lemma 5.2. Notice that the kernel of $\mathrm{Gal}(K(A[p])/K) \to \mathrm{Gal}(K(p)/K) = \mathrm{Gal}(K(x(A[p]))/K)$ has order 2, and χ_1^2 and χ_2^2 are therefore trivial on such kernel. Thus, making a slight abuse of notation, we may also consider χ_1^2 and χ_2^2 as representations of $G = \mathrm{Gal}(K(p)/K)$. Notice that the restriction of χ_1^2 (resp. χ_2^2) to $\mathrm{Gal}(K(\wp)/K)$ (resp. $\mathrm{Gal}(K(\wp')/K)$) is σ^2 (resp. σ'^2). Then, $(\mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p))_{(2,0)}$ is the $\mathbb{F}_p[G]$-submodule of $\mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p)$ such that the action of the Galois group G is given by χ_1^2. Hence $(\mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p))_{(2,0)}$ is in fact isomorphic to $(R_\wp^{(p)})_{\sigma^2}$ and $(\mathfrak{R}_p^*/(\mu_p(\mathfrak{R}_p^*)^p))_{(0,2)}$ is isomorphic to $(R_{\wp'}^{(p)})_{\sigma'^2}$. Therefore, by the previous discussion, if $G_2(L)$ is a p-adic unit then $B_{(2,0)}^{(p)}$ and $B_{(0,2)}^{(p)}$ are trivial, as claimed.

In accordance with the theory, when $D_K = -67$, one has $\mathrm{BH}_2^0 = 2 \cdot 19$ and

$$\mathrm{BH}_{18}^{16} = \frac{2 \cdot 19 \cdot 291007 \cdot 5899501 \cdot 1016672133973}{3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13}.$$

Since $(0, -2) \equiv (18, 16) \mod 18$, this means that in this case both $B_{(2,0)}^{(19)}$ and $B_{(0,2)}^{(19)}$ may be non-trivial.

Proposition 6.16 *If BH_p^{p-2} is a p-adic unit (or equivalently, if $\wp$ is not a Wieferich place) then $B_{(1,1)}^{(p)}$ is trivial.*

PROOF. The proposition is an immediate consequence of Theorem 6.6 and Corollary 6.9.

The following table lists all split primes less than 50000 such that a prime $\wp$ lying above p is a Wieferich place of K (with discriminant D_K).

D_K	-3	-4	-7	-8	-11	-19	-43	-67	-163
p	$13, 181, 2521$	29789	19531	(none)	5	11	1741	24421	1523

Remark 6.17 *The values* BH_k^j *can also be computed using the recursive relations among the Bernoulli-Hurwitz numbers, which can be deduced from the work of A. Weil [24]. In particular, the Hurwitz numbers* $\mathrm{BH}_k^0 = G_k(L)$ *for even* $k \geq 8$ *can all be deduced from* BH_2^0*,* BH_4^0 *and* BH_6^0 *and the recurrence formula ([24], p. 35):*

$$\mathrm{BH}_k^0 = \frac{6}{(k-6)(k+1)(k-1)} \sum_{\text{even } h=4}^{k-4} (h-1)(k-h-1)\,\mathrm{BH}_h^0 \cdot \mathrm{BH}_{k-h}^0 \,.$$

Once enough Hurwitz numbers BH_k^0 *have been calculated, one can calculate the Bernoulli-Hurwitz numbers of the form* BH_{2m+1}^1 *using the formula ([24], p. 45):*

$$\mathrm{BH}_{2m+1}^1 = \frac{2m+3}{2}\,\mathrm{BH}_{2m+2}^0 - \frac{1}{2}\sum_{r=1}^{m} \mathrm{BH}_{2r}^0 \cdot \mathrm{BH}_{2m-2r+2}^0 \,.$$

Finally, applying $j-1$ *times the differential operator* $\mathfrak{D}$ *of Weil, as defined in [24], p. 42, on the previous equation, one obtains the following recurrence formula for all* BH_k^j*:*

$$\lambda(k,j) = (1-k)(2-k)\cdots(j-k), \quad C_k^j = \lambda(k,j)\,\mathrm{BH}_k^j$$

$$\lambda(k,j-1)\,\mathrm{BH}_k^j = \frac{2m+3}{2} C_{k+1}^{j-1} - \frac{1}{2}\sum_{r=1}^{(k-j)/2}\sum_{h=0}^{j-1}\binom{j-1}{h} C_{2r+j-1-h}^{j-1-h} \cdot C_{k-j-2r+2+h}^{h}.$$

Using these formulas one can effectively compute the value BH_p^{p-2} *for all split primes, although these calculations tend to be computationally demanding. For example, one can calculate* $\mathrm{BH}_5^3 = 135/2 = 2^{-1} \cdot 3^3 \cdot 5$ *for* $K = \mathbb{Q}(\sqrt{-11})$*, and* $\mathrm{BH}_{11}^9 = (11 \cdot 17 \cdot 6781)/(2^2 \cdot 3^2 \cdot 5^2 \cdot 7)$ *for* $K = \mathbb{Q}(\sqrt{-19})$.

7 Proof of Theorem 1.2

We reduced the proof of Proposition 3.7 (and hence Theorem 1.2) to showing Lemma 4.3. Namely, under the conditions of Theorem 1.2, we need to prove that the intersection of $N^{(p)}$ and the kernel $B^{(p)}$ is trivial. The $\mathbb{F}_p[G]$-module $N^{(p)}$ is isomorphic (via Ψ_0^{-1}) to N/pM, where N is the submodule of M consisting of all the functions $m\colon R \to \mathbb{Z}$ which reduce modulo p to a homogeneous polynomial of degree 2 over $\mathbb{F}_p$. We use the orthogonal idempotents to decompose N/pM as:

$$N/pM \cong \oplus_\chi (N/pM)_\chi.$$

Therefore, it suffices to show that if $(N/pM)_\chi$ is non-trivial then $B_\chi^{(p)}$ is necessarily trivial.

7.1 The inert case

Let p be inert in K. We claim that, in fact:

$$N/pM \cong (N/pM)_{\chi_2} \oplus (N/pM)_{\chi_{p+1}} \tag{5}$$

Furthermore, if N/pM decomposes as in Eq. (5), then, as a direct consequence of Corollary 6.4, the intersection of $N^{(p)}$ and $B^{(p)}$ would be automatically trivial. Thus, we just need to prove Eq. (5).

Let $m_{\text{norm}} \in M/pM$ be defined by:

$$m_{\text{norm}}(r) = m_{\text{norm}}(r_1, r_2) \equiv \mathbf{N}(I(r)) \equiv \mathbf{N}(r_1\tau + r_2) \mod p.$$

It is clear that $m_{\text{norm}} \mod p$ is given by a homogeneous quadratic polynomial of degree 2 and so, $m_{\text{norm}} \in N/pM$. Moreover, if α is an element of $G = (\mathcal{O}_K/(p))^\times/\{\pm 1\}$ then:

$$\alpha \cdot m_{\text{norm}}(r) = m_{\text{norm}}(\alpha \cdot r) \equiv \mathbf{N}(\alpha \cdot I(r)) \equiv \mathbf{N}(\alpha) \cdot m_{\text{norm}}(r) \mod p$$

It follows that the 1 dimensional $\mathbb{F}_p$-space spanned by m_{norm} is G-invariant, and the representation afforded by the module is equivalent to the representation σ^{p+1}.

Next we describe the complement of $\langle m_{\text{norm}} \rangle$ in N/pM. We extend scalars and regard N/pM as a $\overline{\mathbb{F}_p}[G]$-module, where $\overline{\mathbb{F}_p}$ is a fixed algebraic closure of $\mathbb{F}_p$. Recall that $K = \mathbb{Q}(\sqrt{-d})$ and we defined τ by:

$$\tau = \begin{cases} \sqrt{-d} & , \text{ if } -d \equiv 2, 3 \mod 4, \\ \frac{1+\sqrt{-d}}{2} & , \text{ if } -d \equiv 1 \mod 4. \end{cases}$$

In particular, τ can be regarded as a scalar in $\overline{\mathbb{F}_p}$. Define elements of N/pM by the formulas:

$$m_1(r_1, r_2) \equiv (r_1\tau + r_2)^2, \quad m_2(r_1, r_2) \equiv (r_1\overline{\tau} + r_2)^2 \mod p.$$

For $\alpha \in G$ one has $\alpha \cdot m_1(r) \equiv \alpha^2 m_1(r) \mod p$ and $\alpha \cdot m_2(r) \equiv \overline{\alpha}^2 m_2(r) \mod p$ where the appearances of α^2 are to be regarded as scalar multiplication by $\alpha^2 \in \overline{\mathbb{F}_p}$, and $\overline{\alpha}$ denotes complex conjugation. Hence, the space spanned by m_1 and m_2 is a two dimensional $\overline{\mathbb{F}_p}[G]$-module, and the representation afforded by it coincides with the representation σ^2 (compare the traces). Since, m_1, m_2 and m_{norm} span N/pM, we conclude that the $\mathbb{F}_p[G]$-complement of $\langle m_{\text{norm}} \rangle$ in N/pM is no other than $(N/pM)_{\chi_2}$, which concludes the proof.

7.2 The split case

Let p be split in K. We claim that:

$$N/pM \cong (N/pM)_{(2,0)} \oplus (N/pM)_{(0,2)} \oplus (N/pM)_{(1,1)} \tag{6}$$

The results in Proposition 6.15 and 6.16, together with Eq. (6) are sufficient to establish the main Theorem 1.2 in the split case. In order to show this decomposition, we define elements of the $\mathbb{F}_p$-module N/pM as follows. Here we fix an integer n such that $n^2 \equiv D_K \mod p$, set $\widehat{\tau} = (1+n)/2$, $\widehat{\tau}' = (1-n)/2$, so that if $\pi = a + b\tau$ then $\pi \equiv a + b\widehat{\tau} \mod p$ and $\pi' \equiv a + b\widehat{\tau}' \mod p$. Then we have:

$$\begin{aligned} m_{\text{norm}}(r) = m_{\text{norm}}(r_1, r_2) &\equiv \mathbf{N}(I(r)) \equiv \mathbf{N}(r_1\pi + r_2\pi') \mod p \\ m_1(r) &\equiv (\pi' \cdot I(r))^2, \quad m_2(r) \equiv (\pi \cdot I(r))^2 \mod p \end{aligned}$$

Let $\overline{\chi_1} : (\mathcal{O}_K/(p))^\times \to (\mathcal{O}_K/\wp)^\times \cong \mathbb{F}_p^\times$ be given by $\alpha \mod p \mapsto \alpha \mod \wp$ and similarly define $\overline{\chi_2}$ which sends $\alpha \mod p \mapsto \alpha \mod \wp'$. It is plain that $\overline{\chi_1}$ and $\overline{\chi_2}$ are the mod p reductions of the characters χ_1 and χ_2 of Lemma 5.2. It is also easy to check that the norm homomorphism from $(\mathcal{O}_K/(p))^\times$ down to $\mathbb{F}_p^\times$ is given by $\overline{\chi_1} \cdot \overline{\chi_2}$. Also note that $\pi'\alpha \equiv \pi'\chi_1(\alpha) \mod p$ and $\pi\alpha \equiv \pi\chi_2(\alpha) \mod p$.

The Galois action of $\alpha \in G = (\mathcal{O}_K/(p))^\times/\{\pm 1\}$ is as follows:

$$\begin{aligned} \alpha \cdot m_{\text{norm}}(r) &\equiv \mathbf{N}(\alpha) \cdot m_{\text{norm}}(r) \equiv \overline{\chi_1}(\alpha)\overline{\chi_2}(\alpha) m_{\text{norm}}(r) \mod p, \\ \alpha \cdot m_1(r) &\equiv (\pi'\alpha \cdot I(r))^2 \equiv \overline{\chi_1}(\alpha)^2 m_1(r) \mod p, \\ \alpha \cdot m_2(r) &\equiv \overline{\chi_2}(\alpha)^2 m_2(r) \mod p. \end{aligned}$$

It follows that the 1 dimensional $\mathbb{F}_p$-spaces spanned by m_{norm}, m_1 and m_2 are G-invariant, and the representation afforded by these modules are respectively equivalent to the representation $\chi_1\chi_2$, χ_1^2 and χ_2^2. Since N/pM is three dimensional and G acts differently on each of the 1-dimensional subspaces listed above, these must be linearly independent and span all of N/pM. This proves the decomposition of equation (6) and concludes the proof of the theorem.

References

[1] A. Brumer, *On the units of algebraic number fields*, Mathematika, 14, (1967), 121-124.

[2] R. M. Damerell, *L-functions of elliptic curves with complex multiplication, I and II*, Acta Arith. XVII and XIX, (1970-71).

[3] M. Deuring, *Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins*, Nachrichten der Akademie der Wissenschaften in Göttingen. Mathematisch-Physikalische Klasse, (1953), 85-94; II, ibid., (1955) 13-42; III, ibid., (1956), 37-76; IV, ibid., (1957), 55-80.

[4] M. Deuring, *Die Klassenkörper der komplexen Multiplikation*, Enzyklopädie der mathematischen Wissenschaften: Mit Einschluss ihrer Anwendungen, Band I-2, Heft 10, Teil II. Stuttgart: Teubner 1958.

[5] K. Iwasawa, *On Leopoldt's conjecture*, Seminar Note on Algebraic Number Theory, R.I.M.S. Kyoto U. (1984), 45-53.

[6] N. Katz, *The Congruences of Clausen - von Staudt and Kummer for Bernoulli-Hurwitz numbers*, Math. Ann. 216, (1975), 1-4.

[7] D. S. Kubert, S. Lang, *Modular Units*, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer-Verlag, New York, 1981.

[8] Á. Lozano-Robledo, *On the surjectivity of Galois representations attached to elliptic curves over number fields*, Acta Arithmetica, Vol. 117, No. 3, (2005), 283-291.

[9] Á. Lozano-Robledo, *On elliptic units and p-adic Galois representations attached to elliptic curves*, Journal of Number Theory, Vol. 117, issue 2, (2006), 439-470.

[10] The PARI Group, PARI/GP, Version 2.1.1, 2000, Bordeaux, available from http://www.parigp-home.de/

[11] G. Robert, *Unités Elliptiques*, Bulletin de la Societe Mathematique de France, Memoire 36, Dec 1973.

[12] G. Robert, *Nombres de Hurwitz et Unités Elliptiques*, Ann. scient. Éc. Norm. Sup., 4^{e} série, t. 11, (1978), 297-389.

[13] D. E. Rohrlich, *A deformation of the Tate module*. Journal of Algebra 229, (2000), 280-313.

[14] D. E. Rohrlich, *Modular units and the surjectivity of a Galois representation.* Journal of Number Theory 107, (2004), 8-24.

[15] K. Rubin, *On the main conjecture of Iwasawa theory for imaginary quadratic fields*, Invent. math. 93, (1988), 701-713.

[16] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. math. 103, (1991), 25-68.

[17] J. W. Sands, *Kummer's and Iwasawa's version of Leopoldt's conjecture*, Canad. Math. Bull. 31 (1988), no. 3, 338346.

[18] J.-P. Serre, J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics 88, (1968), 492-517.

[19] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae 15 (1972), 259-331.

[20] J. F. Voloch, *Elliptic Wieferich Primes*, Journal of Number Theory 81, (2000), 205-209.

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

[22] R. I. Yager, *On two variable p-adic L-functions*, Ann. of Math. 115, (1982), 411-449.

[23] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag (1996).

[24] A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Springer-Verlag (1976).