MATHEMATICS OF COMPUTATION
Volume 80, Number 274, April 2011, Pages 1099–1122
S 0025-5718(2010)02413-5
Article electronically published on September 2, 2010

CLASS NUMBERS OF RAY CLASS FIELDS OF IMAGINARY QUADRATIC FIELDS

OMER KUCUKSAKALLI

ABSTRACT. Let K be an imaginary quadratic field with class number one and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. In this paper we generalize an algorithm of Schoof to compute the class numbers of ray class fields $K_{\mathfrak{p}}$ heuristically. We achieve this by using elliptic units analytically constructed by Stark and the Galois action on them given by Shimura's reciprocity law. We have discovered a very interesting phenomenon where p divides the class number of $K_{\mathfrak{p}}$. This is a counterexample to the elliptic analogue of Vandiver's conjecture.

INTRODUCTION

Let $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ be the p-th real cyclotomic field. Its ring of integers has an explicit subgroup of units $\mathcal{C}$, called the cyclotomic units. It is a well-known fact that $\mathcal{C}$ has finite index in the full unit group and the order of the quotient

$$B_{\mathbf{Q}_{(p)}} = \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C}$$

is equal to $h_{\mathbf{Q}_{(p)}}$, the class number of $\mathbf{Q}_{(p)}$. The class group $\mathrm{Cl}(\mathbf{Q}_{(p)})$ and $B_{\mathbf{Q}_{(p)}}$ are both finite $\mathbf{Z}[G]$-modules where $G = \mathrm{Gal}(\mathbf{Q}_{(p)}/\mathbf{Q})$. Hence they admit a Jordan-Hölder filtration with simple factors. It turns out that their submodules with Jordan-Hölder factors of fixed order q have the same number of elements as well. Using this fact, Schoof investigates the class numbers of $\mathbf{Q}_{(p)}$ heuristically [3]. He presents a table of orders of subgroups of $\mathrm{Cl}(\mathbf{Q}_{(p)})$ with Jordan-Hölder factors of order $q < 80,000$ for primes $p < 10,000$. On the other hand, general purpose algorithms could give the class number $h_{\mathbf{Q}_{(p)}}$, in a reasonable amount of time, only for $p \leq 113$.

Let K be an imaginary quadratic field with class number one and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. There is a beautiful analogy between the ray class fields $\mathbf{Q}_{(p)}$ and $K_{\mathfrak{p}}$. Similar to the cyclotomic case, $K_{\mathfrak{p}}$ is obtained by the coordinates of $\mathfrak{p}$-division points of a CM elliptic curve. Moreover, Stark gives an explicit group of units $\mathcal{E}$, namely the elliptic units, such that the quotient

$$B_{K_{\mathfrak{p}}} = \mathcal{O}^*_{K_{\mathfrak{p}}}/\mathcal{E}$$

is finite and its order is equal to the class number of $K_{\mathfrak{p}}$ [4].

In this paper we generalize Schoof's algorithm to the elliptic case. We have found all simple Jordan-Hölder factors of $B_{K_{\mathfrak{p}}}$ with *small* order. More precisely, we have the following result.

Received by the editor May 14, 2009 and, in revised form, January 1, 2010.
2010 *Mathematics Subject Classification.* Primary 11Y40.

Theorem 1. *For each K, we give a table containing all simple Jordan-Hölder factors of order $q < 2000$ of $B_{K_\mathfrak{p}}$ for $\mathfrak{p} \subset \mathcal{O}_K$ of norm $p < 700$. Our tables also contain the number $\tilde{h}_{K_\mathfrak{p}}$, the order of the largest submodule of $B_{K_\mathfrak{p}}$ (and therefore of $\mathrm{Cl}(K_\mathfrak{p})$) all of whose Jordan-Hölder factors have order less than 2000.*

The number $\tilde{h}_{K_\mathfrak{p}}$ divides the class number of $K_\mathfrak{p}$ since it is the order of a subgroup. Moreover, our computation implies that either

$$\#\mathrm{Cl}(K_\mathfrak{p}) = \tilde{h}_{K_\mathfrak{p}} \qquad \text{or} \qquad \#\mathrm{Cl}(K_\mathfrak{p}) > 2000 \cdot \tilde{h}_{K_\mathfrak{p}},$$

but we do not know for sure the class number of $K_\mathfrak{p}$ for any $\mathfrak{p}$ of norm $p > 40$. However, according to Cohen-Lenstra heuristics, we argue that each table is a table of class numbers with probability at least 96%.

Our ranges for the norm of conductors and the size of Jordan-Hölder factors are rather small compared to those of Schoof. This is due to the lack of algebraic expressions for elliptic units (see Remark 2.5).

We have discovered a very interesting phenomenon where p divides the class number of $K_\mathfrak{p}$. This is a counterexample to the elliptic analogue of a well-known conjecture in the theory of cyclotomic number fields, namely Vandiver's conjecture.

Theorem 2. *Let K be the imaginary quadratic field with discriminant $d_K = -163$. The class number of $K_{\mathfrak{p}_{307}}$ is divisible by 307 where $\mathfrak{p}_{307} \subset \mathcal{O}_K$ is a degree one prime ideal of norm 307.*

In the first section we give the construction of Stark's elliptic units and the Galois action on them by using Shimura's reciprocity law. In the second section, we show that Schoof's algorithm can be extended to the elliptic case and give an example to illustrate the algorithm. In the last section, we explain our main results and the data we collect from our algorithm.

At the end, we give a table for each K containing the order of the largest submodule of $B_{K_\mathfrak{p}}$ (and therefore of $\mathrm{Cl}(K_\mathfrak{p})$) with Jordan-Hölder factors of order less than 2000.

1. Elliptic units

Let K be an imaginary quadratic field with class number one, and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. In this section we explain how to compute Stark's elliptic units in the ray class field $K_\mathfrak{p}$ with high precision.

Theorem 1.1. *There are only 9 imaginary quadratic fields with class number one. The discriminants d_K of these fields are given by*

$$\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

Proof. See Stark [5]. □

First we fix some notation. Define

$$w = \begin{cases} \sqrt{d_K}/2 & \text{if } d_K = -4, -8, \\ (\sqrt{d_K}+1)/2 & \text{otherwise,} \end{cases}$$

so that $\mathcal{O}_K = \mathbf{Z}[w]$ for each K. Also, define $w_\mathfrak{p}$ to be the smallest nonnegative integer that satisfies the congruence

$$w \equiv w_\mathfrak{p} \pmod{\mathfrak{p}}.$$

It is easy to see that $0 \leq w_\mathfrak{p} \leq p-1$.

The ray class field $K_{\mathfrak{p}}$ is an Abelian extension of K with Galois group isomorphic to $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$ by class field theory. Set $G_{K_{\mathfrak{p}}} = \mathrm{Gal}(K_{\mathfrak{p}}/K)$. The map

$$\psi : xw + y \longmapsto xw_{\mathfrak{p}} + y$$

gives a surjective homomorphism from $\mathcal{O}_K$ onto $\mathbf{F}_p$ with $\mathrm{Ker}(\psi) = \mathfrak{p}$. The unit group $\mathcal{O}_K^* = \mu_K$ is finite of order

$$W_K = \begin{cases} 6 & \text{if } d_K = -3, \\ 4 & \text{if } d_K = -4, \\ 2 & \text{otherwise.} \end{cases}$$

Since any ideal in $\mathcal{O}_K$ is principal, the group $I_K(\mathfrak{p})$ of all fractional $\mathcal{O}_K$-ideals relatively prime to $\mathfrak{p}$ is

$$I_K(\mathfrak{p}) = \{(\alpha) : \alpha \in K, \alpha \not\equiv 0 \pmod{\mathfrak{p}}\}.$$

Observe that two elements generate the same ideal only if they differ by a unit. Let ζ_K be a root of unity in $\mathcal{O}_K$ generating μ_K. We have $\zeta_K^{(W_K/2)} = -1$. It implies that

$$\psi : \mu_K \longrightarrow \mathbf{F}_p^*$$

is an injection unless $W_K = 6$. In that case consider the identity $\zeta_6^2 = \zeta_6 - 1$. It follows that $\psi(\zeta_6)$ cannot be ± 1. Hence the map ψ is an injection for all K. Now we can construct a well-defined map

$$\begin{aligned} \widehat{\psi} : \quad I_K(\mathfrak{p}) \quad &\longrightarrow \mathbf{F}_p^*/\psi(\mu_K) \\ (xw + y) \quad &\longmapsto xw_{\mathfrak{p}} + y. \end{aligned}$$

It is easy to show that $\widehat{\psi}$ is a homomorphism and we have

$$\begin{aligned} \mathrm{Ker}(\widehat{\psi}) &= \{(\alpha) : \alpha \equiv \zeta \pmod{\mathfrak{p}}, \zeta \in \mu_K\} \\ &= \{(\alpha) : \alpha \equiv 1 \pmod{\mathfrak{p}}\} \\ &= P_{K,1}(\mathfrak{p}). \end{aligned}$$

Therefore the Galois group of $K_{\mathfrak{p}}/K$ is given by

$$G_{K_{\mathfrak{p}}} \cong \mathbf{F}_p^*/\psi(\mu_K)$$

which is cyclic and has order $(p-1)/W_K$. Let m be an integer relatively prime to p. Consider the class in $I_K(\mathfrak{p})/P_{K,1}(\mathfrak{p})$ containing the ideal $m\mathcal{O}_K$. We denote the corresponding element in $G_{K_{\mathfrak{p}}}$ by σ_m. Suppose that the ideal $\mathfrak{q}$ is generated by $\pi_{\mathfrak{q}} \equiv m \pmod{\mathfrak{p}}$. Then we have $\sigma_{\mathfrak{q}} = \sigma_m$ where $\sigma_{\mathfrak{q}}$ is the Artin symbol.

The construction of Stark's elliptic units relies on the family of modular functions $\phi(u, v, z)$ defined by infinite products [4, p. 207].

Proposition 1.2. *The function $\phi(u, v, z)$ satisfies the following transformation properties:*

(1) $\phi(u, v+1, z) = -e^{\pi i u}\phi(u, v, z)$,
(2) $\phi(u+1, v, z) = -e^{-\pi i v}\phi(u, v, z)$,
(3) $\phi(u, v, z+1) = e^{\pi i/6}\phi(u, u+v, z)$,
(4) $\phi(u, v, -1/z) = e^{-\pi i/2}\phi(v, -u, z)$.

Proof. These properties follow from Kronecker's second limit formula. See Stark [4, pp. 207-208] for details. □

Let a, b be integers, not both divisible by p. The function $\phi(a/p, b/p, z)$ is invariant under the action of $\Gamma(12p^2)$ and by definition it is modular of level $12p^2$. We fix a $\mathbf{Z}$-basis $[p, w_{\mathfrak{p}} - w]$ for the ideal $\mathfrak{p} \subset \mathcal{O}_K$. Observe that the imaginary part of the quotient $p/(w_{\mathfrak{p}} - w)$ is positive.

Theorem 1.3. *Let a be an integer relatively prime to p. There exists $\pi(a) \in \mathcal{O}_{K_{\mathfrak{p}}}$ of norm p such that*

$$\left[\phi\left(\frac{a}{p}, 0, \theta\right)^{W_K}\right]^{12p} = \pi(a)^{12p}$$

where $\theta = p/(w_{\mathfrak{p}} - w)$. The element $\pi(a)$ generates the unique prime ideal $\mathfrak{P} \subset \mathcal{O}_{K_{\mathfrak{p}}}$ lying above $\mathfrak{p}$. The quotient $\pi(a)/\pi(1)$ is the W_K-th power of a unit $\epsilon_a \in \mathcal{O}^*_{K_{\mathfrak{p}}}$ and

$$\sigma_m(\epsilon_a)^{W_K} = \frac{\pi(ma)}{\pi(m)} = \left(\frac{\epsilon_{ma}}{\epsilon_m}\right)^{W_K}$$

for all $\sigma_m \in G_{K_{\mathfrak{p}}}$.

Proof. See Stark [4, pp. 226 and 229] □

In order to compute the elliptic units $\sigma_m(\epsilon_a)$, we start by applying Shimura's reciprocity law [4, Theorem 3] to the element $\phi(m/p, 0, \theta)$. Let $\mathfrak{q} = (x_{\mathfrak{q}} w + y_{\mathfrak{q}})$ be a degree one prime ideal in $\mathcal{O}_K$ of norm q not dividing $6pd_K$. We denote the conjugate of this prime by $\bar{\mathfrak{q}} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})$ where we can take $x_{\bar{\mathfrak{q}}} = x_{\mathfrak{q}}$. This implies that

$$y_{\bar{\mathfrak{q}}} = \begin{cases} -y_{\mathfrak{q}} & \text{if } d_K = -4, -8, \\ -(x_{\mathfrak{q}} + y_{\mathfrak{q}}) & \text{otherwise.} \end{cases}$$

We take $(x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})[p, w_{\mathfrak{p}} - w]$ as a $\mathbf{Z}$-basis for $\bar{\mathfrak{q}}\mathfrak{p} \subset \mathcal{O}_K$ and therefore the integral matrix B is defined by

$$B\begin{pmatrix} p \\ w_{\mathfrak{p}} - w \end{pmatrix} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})\begin{pmatrix} p \\ w_{\mathfrak{p}} - w \end{pmatrix}.$$

Comparing the coefficients of w, one can obtain that

$$B = \begin{bmatrix} x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\bar{\mathfrak{q}}} & -p x_{\mathfrak{q}} \\ * & -(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}}) \end{bmatrix}.$$

Note that $\det(B) = q$, and therefore

$$qB^{-1} = \begin{bmatrix} -(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}}) & p x_{\mathfrak{q}} \\ * & x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\bar{\mathfrak{q}}} \end{bmatrix}.$$

Denote by $\sigma_{\mathfrak{q}}$ the Artin symbol of $\mathfrak{q}$ in $\mathrm{Gal}(K_{(12p^2)}/K)$. Shimura's reciprocity law implies that $\phi\,(m/p, 0, \theta)$ is an element of the ray class field $K_{(12p^2)}$, and

$$\begin{aligned} \phi\left(\frac{m}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}} &= \phi\left(\left(\frac{m}{p}, 0\right) qB^{-1}, \theta\right) \\ &= \phi\left(-\frac{m(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}})}{p}, m x_{\mathfrak{q}}, \theta\right) \\ &= \phi\left(-\frac{m(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}})}{p}, 0, \theta\right)\left(-e^{\pi i\left(-\frac{m(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}})}{p}\right)}\right)^{m x_{\mathfrak{q}}} \\ &= \phi\left(-\frac{m(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}})}{p}, 0, \theta\right)\left(e^{\frac{2\pi i}{p}\left(-\frac{x_{\mathfrak{q}}(x_{\mathfrak{q}} w_{\mathfrak{p}} + y_{\mathfrak{q}})}{2}\right)}\right)^{m^2} (-1)^{m x_{\mathfrak{q}}}. \end{aligned} \tag{1.1}$$

The action of $\sigma_{\mathfrak{q}}$ on the roots of unity is given by $\zeta^{\sigma_{\mathfrak{q}}} = \zeta^q$. Theorem 1.3 implies that $\phi\left(m/p, 0, \theta\right)^{W_K}$ is in $K_{\mathfrak{p}}$ up to a $12p$-th root of unity. Suppose that

$$q \equiv 1 \pmod{12p}.$$

This implies that $\sigma_{\mathfrak{q}}$ acts trivially on the $12p$-th root of unity and

$$\frac{\left[\phi\left(\frac{m}{p}, 0, \theta\right)^{W_K}\right]^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{m}{p}, 0, \theta\right)^{W_K}} = \left[\frac{\phi\left(\frac{m}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{m}{p}, 0, \theta\right)}\right]^{W_K}$$

is in $K_{\mathfrak{p}}$. Moreover, this element is the W_K-th power of a unit in the same field by Theorem 1.3. The field K contains the W_K-th roots of unity. This allows us to take W_K-th root of elements within the field $K_{\mathfrak{p}} \supset K$. Therefore

$$\frac{\phi\left(\frac{m}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}}}{\phi\left(\frac{m}{p}, 0, \theta\right)} = \phi\left(\frac{m}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}-1}$$

is in $\mathcal{O}^*_{K_{\mathfrak{p}}}$.

Let a be an integer relatively prime to p. By the Chebotarev's density theorem, we can pick a prime ideal $\mathfrak{q} = (x_{\mathfrak{q}} w + y_{\mathfrak{q}}) \subset \mathcal{O}_K$ of norm $q \equiv 1 \pmod{12p}$ so that $-(x_{\mathfrak{q}} w + y_{\mathfrak{q}}) \equiv a \pmod{\mathfrak{p}}$. The Artin symbol $\sigma_{\mathfrak{q}}$ of such a prime ideal is an element in $\mathrm{Gal}(K_{(12p^2)}/K)$ so that $\sigma_{\mathfrak{q}}|_{K(\zeta_{12p})}$ is the identity and $\sigma_{\mathfrak{q}}|_{K_{\mathfrak{p}}} = \sigma_a$. The independence of these two conditions follow from the next fact.

Lemma 1.4. *$K_{\mathfrak{p}} \cap K(\zeta_n) = K$ for any root of unity ζ_n.*

Proof. Assume otherwise. Then there exists an intermediate field $K \subsetneq L \subseteq K_{\mathfrak{p}}$ which is abelian over $\mathbf{Q}$, because $L \subset K(\zeta_n)$. This is a contradiction since the intersection of $K_{\mathfrak{p}}$ and its complex conjugate $K_{\bar{\mathfrak{p}}}$ is only K. □

We want to thank the referees whose comments were helpful to clarify the following part. We define the integer $k(a)$ by

$$k(a) = \frac{x_{\mathfrak{q}} a}{2}$$

modulo p. Observe that if c is odd and $c/2 = d \pmod{p}$, then $e^{\frac{2\pi i}{p}\frac{c}{2}} = -\zeta_p^d$. Using equation (1.1), we find that

$$\phi\left(\frac{m}{p}, 0, \theta\right)^{\sigma_{\mathfrak{q}}-1} = \frac{\phi\left(\frac{ma}{p}, 0, \theta\right)}{\phi\left(\frac{m}{p}, 0, \theta\right)} \left((-1)^{a x_{\mathfrak{q}}} {\zeta_p}^{k(a)}\right)^{m^2} (-1)^{m x_{\mathfrak{q}}}$$

is in $\mathcal{O}^*_{K_{\mathfrak{p}}}$. The unit ϵ_a of Theorem 1.3 is well defined up to a W_K-th root of unity. We fix

$$\epsilon_a = \frac{\phi\left(\frac{a}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)} {\zeta_p}^{k(a)} \in \mathcal{O}^*_{K_{\mathfrak{p}}}$$

by choosing $m = 1$ and dropping $(-1)^{(a+1)x_{\mathfrak{q}}}$.

Lemma 1.5. *Let g be an odd primitive root modulo p. Then for all i, we have*

$$\sigma_g^i(\epsilon_g) = \frac{\phi\left(\frac{g^{i+1}}{p}, 0, \theta\right)}{\phi\left(\frac{g^i}{p}, 0, \theta\right)} \zeta_p{}^{k(g)g^{2i}}.$$

Proof. Let $\mathfrak{q} \subset \mathcal{O}_K$ be a degree one prime ideal of norm $q \equiv 1 \pmod{12p}$ with generator $\pi_\mathfrak{q} = x_\mathfrak{q} w + y_\mathfrak{q}$ satisfying $\pi_\mathfrak{q} \equiv -g \pmod{\mathfrak{p}}$ for some odd primitive root g modulo p. The restriction $\sigma_\mathfrak{q}|_{K_\mathfrak{p}}$ is the automorphism σ_g in the Galois group $G_{K_\mathfrak{p}}$. Using equation (1.1), together with the definition of $k(g)$, we obtain

$$\begin{aligned} \phi\left(\frac{g^i}{p}, 0, \theta\right)^{\sigma_\mathfrak{q}} &= \phi\left(\frac{g^{i+1}}{p}, 0, \theta\right) \left((-1)^{g x_\mathfrak{q}} \zeta_p^{k(g)}\right)^{g^{2i}} (-1)^{g^i x_\mathfrak{q}} \\ &= \phi\left(\frac{g^{i+1}}{p}, 0, \theta\right) \zeta_p^{k(g)g^{2i}}. \end{aligned}$$

The result follows easily by induction. □

The following lemma is only for computational purposes. It gives us more freedom to compute $k(g)$ by relaxing the condition on the prime ideal $\mathfrak{q} \subset \mathcal{O}_K$. Finding $k(g)$ from the original definition consumes more time since we need to find $\mathfrak{q} = (\pi_\mathfrak{q})$ with the property $\pi_\mathfrak{q} \equiv -g \pmod{\mathfrak{p}}$.

Lemma 1.6. *Let g be an odd primitive root modulo p. Let $\mathfrak{q} = (x_\mathfrak{q} w + y_\mathfrak{q}) \subset \mathcal{O}_K$ be a degree one prime ideal of norm $q \equiv 1 \pmod{12p}$ such that $\sigma_\mathfrak{q}|_{K_\mathfrak{p}}$ is not trivial. Set $a \equiv -(x_\mathfrak{q} w + y_\mathfrak{q}) \pmod{\mathfrak{p}}$. Then*

$$k(g) = \frac{g^2 - 1}{a^2 - 1} k(a) \pmod{p}$$

where $k(a) = (x_\mathfrak{q} a)/2 \pmod{p}$.

Proof. Let g be an odd primitive root modulo p. There exists an integer i such that $a = g^i \pmod{p}$. Using Lemma 1.5, we see that ϵ_{g^2} is equal to $\epsilon_g \sigma_g(\epsilon_g)$ up to a p-th root of unity. Moreover, their W_K-th powers are equal by Theorem 1.3. It follows that $\epsilon_{g^2} = \epsilon_g \sigma_g(\epsilon_g)$ since p and W_K are relatively prime. Comparing the powers of the p-th root of unity, one gets $k(g^2) = k(g)(1 + g^2)$ modulo p. In general, we have

$$k(g^i) = k(g)\left(1 + g^2 + \cdots + g^{2(i-1)}\right) \pmod{p}$$

and it follows that

$$k(g) = \frac{k(a)}{\left(1 + g^2 + \cdots + g^{2(i-1)}\right)} \pmod{p}.$$

Multiplying both numerator and denominator with $g^2 - 1$, we get

$$k(g) = \frac{g^2 - 1}{a^2 - 1} k(a) \pmod{p}.$$ □

Let g be a primitive root modulo p. The *group of elliptic units*, denoted by $\mathcal{E}$, is the multiplicative $\mathbf{Z}[G_{K_\mathfrak{p}}]$-module generated by the unit ϵ_g together with the W_K roots of unity in K. The group $\mathcal{E}$ does not depend on the choice of g. For any subgroup H of $G_{K_\mathfrak{p}}$, we define the H-norm map by $N_H = \sum_{\sigma \in H} \sigma$.

Lemma 1.7. *There is an isomorphism*

$$\mathbf{Z}[G_{K_\mathfrak{p}}]/(N_{G_{K_\mathfrak{p}}}) \cong \mathcal{E}/\mu_K.$$

Moreover, $\mathcal{E}^H = N_H(\mathcal{E})\mu_K$ *for any subgroup* H *of* $G_{K_\mathfrak{p}}$.

Proof. The group of elliptic units $\mathcal{E}$ is of finite index in the full unit group $\mathcal{O}_{K_\mathfrak{p}}^*$ [4, p. 229]. It follows that the $\mathbf{Z}$-rank of $\mathcal{E}$ equals $r = \#G_{K_\mathfrak{p}} - 1$, the $\mathbf{Z}$-rank of the full unit group. Let us consider the $G_{K_\mathfrak{p}}$-homomorphism

$$\mathbf{Z}[G_{K_\mathfrak{p}}] \longrightarrow \mathcal{E}/\mu_K$$

given by $\varphi \mapsto \epsilon_g^\varphi$ which is surjective by definition. Any multiple of $N_{G_{K_\mathfrak{p}}}$ is in the kernel of this map. Therefore

$$\mathbf{Z}[G_{K_\mathfrak{p}}]/(N_{G_{K_\mathfrak{p}}}) \cong \mathcal{E}/\mu_K$$

since both sides are isomorphic to $\mathbf{Z}^r$ as $\mathbf{Z}$-modules.

Now we consider $\mathcal{E}^H$, the H-invariant submodule of $\mathcal{E}$. Clearly, $N_H(\mathcal{E})\mu_K$ is a subset of $\mathcal{E}^H$. Let ϵ be an element in $\mathcal{E}^H$. There exists $x \in \mathbf{Z}[G_{K_\mathfrak{p}}]$ such that

$$\epsilon = \epsilon_g^x \zeta_{W_K}^i$$

for some generator ϵ_g of elliptic units. Invariance of ϵ under H implies that $\epsilon^{h-1} = 1$ for all $h \in H$. It follows that $\epsilon_g^{x(h-1)} = 1$ and therefore $x(h-1)$ is a multiple of $N_{G_{K_\mathfrak{p}}}$ for all $h \in H$. This happens only if x belongs to $N_H\mathbf{Z}[G_{K_\mathfrak{p}}]$ and therefore $\epsilon = \epsilon_g^x \zeta_{W_K}^i$ is in $N_H(\mathcal{E})\mu_K$. □

Even though the group of elliptic units $\mathcal{E}$ is defined by adjoining W_K roots of unity to the multiplicative $\mathbf{Z}[G_{K_\mathfrak{p}}]$-module generated by ϵ_g, the unit group μ_K naturally appears in $\mathcal{E}$. In fact we have the following result.

Lemma 1.8. *Let* $\mathfrak{p} \subset \mathcal{O}_K$ *be a degree one prime ideal of norm* $p \nmid 6d_K$. *Suppose that* $p < 700$ *if* $d_K = -3$ *and is arbitrary otherwise. Then* $N_{G_{K_\mathfrak{p}}}(\epsilon_g)$ *generates* μ_K.

Proof. Let g be a primitive root modulo p. Without loss of generality, let us assume that g is odd. Consider the product

$$\prod_{i=1}^{(p-1)/2} \sigma_g^{i-1}(\epsilon_g) = \prod_{i=1}^{(p-1)/2} \frac{\phi\left(\frac{g^i}{p}, 0, \theta\right)}{\phi\left(\frac{g^{i-1}}{p}, 0, \theta\right)} \zeta_p^{\,k(g)g^{2(i-1)}}.$$

It is easy to see that this product involves $W_K/2$ copies of $N_{G_{K_\mathfrak{p}}}(\epsilon_g)$, the norm of ϵ_g. The sum of the powers of ζ_p,

$$\sum_{i=1}^{(p-1)/2} k(g)g^{2(i-1)} = k(g)\frac{1-g^{p-1}}{1-g^2},$$

is congruent to zero modulo p. Therefore the power of the p-th root of unity in the product is zero. Canceling the repeating terms we obtain

$$\prod_{i=1}^{(p-1)/2} \sigma_g^{i-1}(\epsilon_g) = \frac{\phi\left(\frac{g^{(p-1)/2}}{p}, 0, \theta\right)}{\phi\left(\frac{1}{p}, 0, \theta\right)}.$$

Since g is odd, it is a primitive root not only modulo p but also modulo $2p$. Therefore we have $g^{(p-1)/2} \equiv -1 \pmod{2p}$. Now we use the transformation properties of ϕ

given by Proposition 1.2. The second property implies that $\phi(u+2,0,\theta)=\phi(u,0,\theta)$ and we obtain

$$\prod_{i=1}^{p-1}\sigma_g^{i-1}(\epsilon_g)=\frac{\phi\left(\frac{-1}{p},0,\theta\right)}{\phi\left(\frac{1}{p},0,\theta\right)}.$$

Using the fourth property twice, we see that $\phi(-u,-v,z)=-\phi(u,v,z)$. Hence the above quotient is equal to -1. It follows that $N_{G_{K_\mathfrak{p}}}(\epsilon_g)^{(W_K/2)}=-1$. If W_K is not 6, then μ_K is generated by the $G_{K_\mathfrak{p}}$-norm of ϵ_g. For $W_K=6$, this fact is verified by computation. We have found that the $G_{K_\mathfrak{p}}$-norm of ϵ_g is equal to a primitive sixth root of unity for each $\mathfrak{p}$ of norm $p<700$. □

In order to compute Stark's elliptic units with high precision, it is enough to compute $\phi(u,0,\theta)$ with high precision by Lemma 1.5. By definition

$$\phi(u,0,z)=-i\tau^{\frac{6u^2-6u+1}{12}}(1-\tau^u)\prod_{m=1}^{\infty}(1-\tau^{m+u})(1-\tau^{m-u})$$

where $\tau=e^{2\pi iz}$. One can obtain an approximation by using the first M terms of this infinite product. We want to determine the value of M to assure a certain level of accuracy.

We should use θ with the imaginary part as big as possible so that our approximation is better with the same number of terms. Let A be an element in the modular group Γ such that $A\theta$ is in the fundamental domain $D=\{z\in\mathbf{C}:\mathrm{Im}(z)>0,|z|\geq 1,|\mathrm{Re}(z)|\leq 1/2\}$. The transformation properties (3) and (4) given in Proposition 1.2 imply that

$$\phi(u,v,\theta)=\omega(A)\phi((u,v)A^{-1},A\theta)$$

where $\omega(A)$ is a 12-th root of unity which can be obtained from the decomposition of A in terms of the generators $S=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ and $T=\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)$ of Γ. Without loss of generality, we assume that θ is in the fundamental domain D. This implies that the imaginary part of θ is bigger than $\sqrt{3}/2$ and therefore

$$|\tau|<e^{-\pi\sqrt{3}}\approx 0.00433342.$$

Lemma 1.9. *We have the following bounds:*

$$e^{B(M)}>\left|\prod_{m=M+1}^{\infty}(1-\tau^{m+u})\right|>e^{-B(M)}$$

where $-2\leq u\leq 2$ *and*

$$B(M)=\frac{|\tau|^{M-1}}{(1-|\tau|)(1-|\tau|^{M-1})}.$$

Proof. The proof is straightforward and omitted. □

We use the first M terms in the infinite product to approximate $\phi(u,0,\theta)$ and the corresponding error is

$$E(M)=\left|\prod_{m=M+1}^{\infty}(1-\tau^{m+u})(1-\tau^{m-u})\right|.$$

We can pick u with the property $0 \leq u < 2$ since $\phi(u+2,0,\theta) = \phi(u,0,\theta)$. Lemma 1.9 implies that

$$e^{2B(M)} > E(M) > e^{-2B(M)}$$

and therefore $E(M) = 1 + O(|\tau|^{M-1})$. In our computations, we want to work with values of $\phi(u,0,\theta)$ which are accurate at least 500 decimal places. If we pick $M = 220$, then $E(M)$ is approximately 1 with error less than 10^{-500}. Therefore it is enough to use the first 220 terms for the required precision.

2. Elliptic analogue of Schoof's algorithm

It is a well-known fact that the quotient $B_{K_\mathfrak{p}} = \mathcal{O}^*_{K_\mathfrak{p}}/\mathcal{E}$ is finite and its order is equal to the class number of $K_\mathfrak{p}$. In fact we have something stronger.

Theorem 2.1. *Let H be a subgroup of $G_{K_\mathfrak{p}}$. Then we have*

$$\#\mathrm{Cl}(K_\mathfrak{p}^H) = [\mathcal{O}^*_{K_\mathfrak{p}^H} : \mathcal{E}^H].$$

Proof. This is a generalization of Stark's proof [4, p. 229] for $H = \{1\}$. The class number formula for $K_\mathfrak{p}^H$ [4, pp. 200-201] reads

$$\#\mathrm{Cl}(K_\mathfrak{p}^H)\mathrm{Reg}(\mathcal{O}^*_{K_\mathfrak{p}^H}) = \prod_{\chi \neq 1} L'(0,\chi)$$

where the product runs over nontrivial characters of $\mathrm{Gal}(K_\mathfrak{p}^H/K)$. Let e be the order of the subgroup H and suppose that $\#G_{K_\mathfrak{p}} = (p-1)/W_K = e\tilde{e}$. The Galois group $\mathrm{Gal}(K_\mathfrak{p}^H/K)$ is isomorphic to $G_{K_\mathfrak{p}}/H$. In fact we have

$$\mathrm{Gal}(K_\mathfrak{p}^H/K) = \{\sigma_g^i|_{K_\mathfrak{p}^H} : 0 \leq i \leq \tilde{e}-1\}$$

where σ_g is a generator of $G_{K_\mathfrak{p}}$ for some primitive root g modulo p. Each nontrivial character χ has conductor $\mathfrak{p}$, and therefore primitive. By [4, Theorem 2], we have

$$L'(0,\chi) = -\frac{1}{W_K}\sum_{i=0}^{\tilde{e}-1} \chi(\sigma_g^i)\log\left(|N_H(\pi(g^i))|^2\right)$$

where $N_H = \sum_{\tau \in H}\tau$ is the H-norm and $\pi(g^i)$ is given by Theorem 1.3. In order to use the theory of group determinants, let us define

$$f : \sigma_g^i \longmapsto \log\left(|N_H(\pi(g^i))|^2\right)$$

a function of $\mathrm{Gal}(K_\mathfrak{p}^H/K)$. Now we have

$$\begin{aligned}
\#\mathrm{Cl}(K_\mathfrak{p}^H)\mathrm{Reg}(\mathcal{O}^*_{K_\mathfrak{p}^H}) &= \prod_{\chi\neq 1} L'(0,\chi) \\
&= \pm\frac{1}{(W_K)^{\tilde{e}-1}}\prod_{\chi\neq 1}\sum_{i=0}^{\tilde{e}-1}\chi(\sigma_g^i)f(\sigma_g^i) \\
&= \pm\frac{1}{(W_K)^{\tilde{e}-1}}\det\left[f(\sigma_g^{i-j}) - f(\sigma_g^i)\right]_{i,j\neq 0}
\end{aligned}$$

by [6, Lemma 5.26]. It is easy to see that

$$f(\sigma_g^{i-j}) - f(\sigma_g^i) = \log\left(\left|N_H\left(\frac{\pi(g^{i-j})}{\pi(g^i)}\right)\right|^2\right).$$

Both elements $\pi(g^{i-j}), \pi(g^i)$ are of norm p and their quotient is an elliptic unit. In fact we have

$$\frac{\pi(g^{i-j})}{\pi(g^i)} = \left[\sigma_g^i(\epsilon_{g^{-j}})\right]^{W_K}$$

by definition. Finally, we obtain

$$\begin{aligned} \#\mathrm{Cl}(K_{\mathfrak{p}}^H)\mathrm{Reg}(\mathcal{O}_{K_{\mathfrak{p}}^H}^*) &= \pm \det\left[2\log\left|N_H\left(\sigma_g^i(\epsilon_{g^{-j}})\right)\right|\right]_{i,j\neq 0} \\ &= \mathrm{Reg}(\mathcal{E}^H) \end{aligned}$$

since $N_H(\mathcal{E})\mu_K = \mathcal{E}^H$ by Lemma 1.7. Therefore the index of $\mathcal{E}^H$ in the full unit group of $K_{\mathfrak{p}}^H$ is exactly the class number of $K_{\mathfrak{p}}^H$. □

Every finite $\mathbf{Z}[G_{K_{\mathfrak{p}}}]$-module admits a Jordan-Hölder filtration whose simple factors are one-dimensional vector spaces over the residue fields of various local rings $\mathbf{Z}_l[X]/(\varphi)$ (see Schoof [3, Section 3] for details). Let f be the order of the irreducible polynomial φ. The *order* of a simple Jordan-Hölder factor is the order $q = l^f$ of the residue field and its *degree* d is the order of X modulo φ.

Let B and C be the submodules of $B_{K_{\mathfrak{p}}}$ and $\mathrm{Cl}(K_{\mathfrak{p}})$, respectively, all of whose simple Jordan-Hölder factors have some fixed order $q = l^f$. We thank René Schoof for his useful remark for the fact that B and C have the same number of elements. Before giving his explanation, we need the following result.

Proposition 2.2. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm $p < 700$ not dividing $6d_K$. Let H be a subgroup of $G_{K_{\mathfrak{p}}}$. Then the sequence of H-invariants*

$$0 \longrightarrow \mathcal{E}^H \longrightarrow \mathcal{O}_{K_{\mathfrak{p}}^H}^* \longrightarrow B_{K_{\mathfrak{p}}}^H \longrightarrow 0$$

is exact. In particular, $B_{K_{\mathfrak{p}}}^G = 0$.

Proof. The prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is totally and tamely ramified in the extension $K_{\mathfrak{p}}/K$. Let $\mathfrak{P} \subset K_{\mathfrak{p}}$ be the unique prime ideal lying above $\mathfrak{p}$. We have found that $\epsilon_g \equiv g \pmod{\mathfrak{P}}$ for each $K_{\mathfrak{p}}$ within our range. Now the proof of this proposition can be adapted from its cyclotomic analogue [3, Proposition 5.1 (i)]. □

Each submodule B or C is the product of the Jordan-Hölder factors of degree d where d runs over the divisors of $(p-1)/W_K$. Combining Theorem 2.1 with Proposition 2.2, we obtain

$$\#\mathrm{Cl}(K_{\mathfrak{p}}^H) = \#B_{K_{\mathfrak{p}}}^H.$$

Simple Jordan-Hölder factors of $B_{K_{\mathfrak{p}}}$ and $\mathrm{Cl}(K_{\mathfrak{p}})$ of degree d are invariant under the unique subgroup of $G_{K_{\mathfrak{p}}}$ of index d. The statement $\#B = \#C$ now follows from the fact that the degree d part of $\mathrm{Cl}(K_{\mathfrak{p}})$ (or $B_{K_{\mathfrak{p}}}$) is precisely the part that appears in the subfield of degree

$$d = \#\mathrm{Gal}(K_{\mathfrak{p}}^H/K),$$

but not in any proper subfield (see Schoof [3, p. 920] for details).

This enables us to work with $B_{K_{\mathfrak{p}}}$ instead of $\mathrm{Cl}(K_{\mathfrak{p}})$ in order to investigate the class number of $K_{\mathfrak{p}}$. The advantage of switching from $\mathrm{Cl}(K_{\mathfrak{p}})$ to $B_{K_{\mathfrak{p}}}$ is that we can understand Jordan-Hölder factors of $B_{K_{\mathfrak{p}}}$ in an easier fashion. Before giving the main tool to investigate those factors, we first prove a lemma.

Lemma 2.3. *Let $M > 1$ be a power of a prime l and $F = K_{\mathfrak{p}}(\zeta_{W_K M})$. Then the natural map*

$$\psi : \mathcal{O}^*_{K_{\mathfrak{p}}}/\mu_K(\mathcal{O}^*_{K_{\mathfrak{p}}})^M \longrightarrow F^*/(F^*)^M$$

is injective.

Proof. This is the elliptic analogue of [3, Lemma 2.1]. The map ψ is well defined since any trivial element in the first quotient is mapped to a trivial element.

The number field $F = K_{\mathfrak{p}}(\zeta_{W_K M})$ lies in the ray class field $K_{(W_K Mp)}$ and therefore it is an abelian extension of K. Let $\Delta = \mathrm{Gal}(F/K_{\mathfrak{p}})$ be its Galois group. In order to prove our lemma, we need to be careful with the roots of unity in the ground field K. Observe that $K_{\mathfrak{p}} \cap \mathbf{Q}(\zeta_{2M})$ is either $\mathbf{Q}$ or K by Lemma 1.4.

Case 1: Suppose that $K_{\mathfrak{p}} \cap \mathbf{Q}(\zeta_{2M}) = \mathbf{Q}$. Let τ be an element in Δ which inverts ζ_{2M}. Let x be an element in $K_{\mathfrak{p}}$ such that $x = y^M$ for some $y \in F$. Since τ fixes elements in $K_{\mathfrak{p}}$, we have $\tau(x) = x$ and therefore $\tau(y)^M = y^M$. This implies that $\tau(y) = y\zeta_M^{c_\tau}$ for some integer c_τ. Pick $\tilde{y} = y\zeta_{2M}^{c_\tau}$. It follows that

$$\tau(\tilde{y}) = \tau(y)\zeta_{2M}^{-c_\tau} = y\zeta_{2M}^{c_\tau} = \tilde{y}$$

and $(-1)^{c_\tau} x = \tilde{y}^M$.

Suppose that $x \in \mathcal{O}^*_{K_{\mathfrak{p}}}$ is in the kernel of ψ. Then $x = y^M$ for some $y \in \mathcal{O}^*_F$. Without loss of generality, we can assume that $\tau(y) = y$. Let σ be an arbitrary element of Δ. There exists an integer c_σ such that $\sigma(y) = y\zeta_M^{c_\sigma}$. Applying $\sigma\tau$ and $\tau\sigma$ to the element y we obtain

$$\sigma\tau(y) = \sigma(y) = y\zeta_M^{c_\sigma} \qquad \text{and} \qquad \tau\sigma(y) = \tau(y\zeta_M^{c_\sigma}) = y\zeta_M^{-c_\sigma},$$

respectively. The Galois group Δ is Abelian and therefore τ and σ commute with each other. It follows that $[\sigma\tau(y)]^2 = y^2$. Now we have

$$\sigma(y^2) = y^2$$

since $\sigma\tau(y) = \sigma(y)$. The unit y^2 belongs to $K_{\mathfrak{p}}$ since it is invariant under Δ. If M is odd, then using the facts that $y^M, y^2 \in \mathcal{O}^*_{K_{\mathfrak{p}}}$, we get $y \in \mathcal{O}^*_{K_{\mathfrak{p}}}$. Therefore the map ψ is injective.

If M is even, then y is an element of a quadratic extension of $K_{\mathfrak{p}}$ lying in $F = K_{\mathfrak{p}}(\zeta_{W_K M})$. Such an extension corresponds to a quadratic extension of $\mathbf{Q}$ lying in $\mathbf{Q}(\zeta_{W_K M})$. There are seven such fields, namely $\mathbf{Q}(\sqrt{\pm 2}), \mathbf{Q}(\sqrt{\pm 3}), \mathbf{Q}(\sqrt{\pm 6})$ and $\mathbf{Q}(\sqrt{-1})$. This implies that $y^2 \in \langle -1, 2, 3\rangle (K^*_{\mathfrak{p}})^2$ by Kummer theory. Since y is a unit, this implies that $y^2 = \pm u^2$ for some $u \in \mathcal{O}^*_{K_{\mathfrak{p}}}$. We have $\pm x = u^M$ and this finishes the proof of the first case.

Case 2: Suppose that $K_{\mathfrak{p}} \cap \mathbf{Q}(\zeta_{2M}) = \mathbf{Q}(\sqrt{-3})$. Then $M > 1$ must be a power of three. We denote the real cyclotomic $\mathbf{Q}(\zeta_{W_K M} + \zeta_{W_K M}^{-1})$ field by $\mathbf{Q}_{(W_K M)}$. The field $F = K_{\mathfrak{p}}(\zeta_{W_K M})$ is the compositum of the two fields $K_{\mathfrak{p}}$ and $\mathbf{Q}_{(W_K M)}$. Moreover, $K_{\mathfrak{p}} \cap \mathbf{Q}_{(W_K M)} = \mathbf{Q}$. It follows that

$$\Delta \cong \mathrm{Gal}(\mathbf{Q}_{(W_K M)}/\mathbf{Q})$$

which is cyclic of order M. One can show that $\mathrm{Gal}(\mathbf{Q}_{(W_K M)}/\mathbf{Q})$ is generated by

$$\sigma_7 : \zeta_{W_K M} \mapsto \zeta_{W_K M}^7.$$

Suppose that $x \in \mathcal{O}^*_{K_{\mathfrak{p}}}$ is in the kernel of ψ. Then $x = y^M$ for some $y \in \mathcal{O}^*_F$. There exists an integer c such that $\sigma_7(y) = y\zeta_M^c$. Let $d = -c/2 \pmod{3M}$. Pick

$\tilde{y} = y\zeta_{3M}^d$. It follows that

$$\sigma_7(\tilde{y}) = \sigma_7(y)\zeta_{3M}^{7d} = y\zeta_{3M}^d = \tilde{y}.$$

The element $\tilde{y}$ belongs to $\mathcal{O}_{K_\mathfrak{p}}^*$ since it is invariant under σ_7. Now $\zeta_3^d x = \tilde{y}^M$ and therefore the map ψ is injective.

Case 3: Suppose that $K_\mathfrak{p} \cap \mathbf{Q}(\zeta_{2M}) = \mathbf{Q}(\sqrt{-1})$. Then $M > 1$ must be a power of two. The field $F = K_\mathfrak{p}(\zeta_{W_K M})$ is the compositum of the two fields $K_\mathfrak{p}$ and $\mathbf{Q}_{(W_K M)}$. Moreover, $K_\mathfrak{p} \cap \mathbf{Q}_{(W_K M)} = \mathbf{Q}$. It follows that

$$\Delta \cong \mathrm{Gal}(\mathbf{Q}_{(W_K M)}/\mathbf{Q})$$

which is cyclic of order M. One can show that $\mathrm{Gal}(\mathbf{Q}_{(W_K M)}/\mathbf{Q})$ is generated by

$$\sigma_5 : \zeta_{W_K M} \mapsto \zeta_{W_K M}^5.$$

Suppose that $x \in \mathcal{O}_{K_\mathfrak{p}}^*$ is in the kernel of ψ. Then $x = y^M$ for some $y \in \mathcal{O}_F^*$. There exists an integer c such that $\sigma_5(y) = y\zeta_M^c$. Let $d = -c$. Pick $\tilde{y} = y\zeta_{4M}^d$. It follows that

$$\sigma_5(\tilde{y}) = \sigma_5(y)\zeta_{4M}^{5d} = y\zeta_{4M}^d = \tilde{y}.$$

The element $\tilde{y}$ belongs to $\mathcal{O}_{K_\mathfrak{p}}^*$ since it is invariant under σ_5. Now $\zeta_4^d x = \tilde{y}^M$ and therefore the map ψ is injective. □

This lemma enables us to identify the group $\mathcal{O}_{K_\mathfrak{p}}^*/\mu_K(\mathcal{O}_{K_\mathfrak{p}}^*)^M$ with a subgroup of $F^*/(F^*)^M$. The field $F = K_\mathfrak{p}(\zeta_{W_K M})$ contains μ_M, the group of M-th roots of unity. Therefore we have

$$\mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}_{K_\mathfrak{p}}^*}\right)/F\right) \cong \mathrm{Hom}_Z\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K}, \mu_M\right) \tag{2.1}$$

by Kummer theory.

Now we are ready to give the main tool to investigate the Jordan-Hölder factors of $B_{K_\mathfrak{p}}$. Let R be the group ring $(\mathbf{Z}/M\mathbf{Z})[G_{K_\mathfrak{p}}]$. For any R-module A, the additive groups

$$A^\perp = \mathrm{Hom}_R(A, R) \qquad \text{and} \qquad A^{\mathrm{dual}} = \mathrm{Hom}_\mathbf{Z}(A, \mathbf{Q}/\mathbf{Z})$$

are R-modules via $(\lambda f)(a) = \lambda f(a) = f(\lambda a)$ for $\lambda \in R$ and $a \in A$. The module R^{dual} is free of rank 1 over R and this implies that any finite R-module is Jordan-Hölder isomorphic to its dual $A^\perp$ by [3, Proposition 1.2 (i)]. Recall that $B_{K_\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}^*/\mathcal{E}$ by definition and the group of elliptic units $\mathcal{E}$ is generated by the unit ϵ_g as a multiplicative Galois module.

Theorem 2.4. *Let $M > 1$ be a power of a prime l and let I denote the augmentation ideal of the group ring $R = (\mathbf{Z}/M\mathbf{Z})[G_{K_\mathfrak{p}}]$. There is a natural isomorphism of $G_{K_\mathfrak{p}}$-modules*

$$B_{K_\mathfrak{p}}[M]^\perp \cong I/\{f_\mathcal{R}(\epsilon_g) : \mathcal{R} \in S\}$$

where S denotes the set of unramified prime ideals $\mathcal{R}$ of $F = K_\mathfrak{p}(\zeta_{W_K M})$ of degree one.

Proof. This is the elliptic analogue of [3, Theorem 2.2]. In order to understand the structure of $B_{K_\mathfrak{p}}[M]^\perp$ we start with the exact sequence

$$0 \longrightarrow \mathcal{E}/\mu_K \longrightarrow \mathcal{O}_{K_\mathfrak{p}}^*/\mu_K \longrightarrow B_{K_\mathfrak{p}} \longrightarrow 0$$

which is obtained by the definition of $B_{K_\mathfrak{p}}$ together with the fact that $\mathcal{E}$ contains μ_K. Applying the snake lemma, we get

$$0 \longrightarrow B_{K_\mathfrak{p}}[M] \longrightarrow \frac{\mathcal{E}}{\mu_K \mathcal{E}^M} \longrightarrow \frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K (\mathcal{O}_{K_\mathfrak{p}}^*)^M}.$$

Then we apply the exact functor $\perp$ (see Schoof [3, Proposition 1.1]) to this exact sequence and obtain

$$\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K (\mathcal{O}_{K_\mathfrak{p}}^*)^M}\right)^\perp \longrightarrow \left(\frac{\mathcal{E}}{\mu_K \mathcal{E}^M}\right)^\perp \longrightarrow \left(B_{K_\mathfrak{p}}[M]\right)^\perp \longrightarrow 0. \tag{2.2}$$

Consider the R-homomorphism from $\left(\mathcal{E}/\mu_K \mathcal{E}^M\right)^\perp$ to R given by $f \mapsto f(\epsilon_g)$. The image of this map lies in the augmentation ideal I of R since $f(\epsilon_g)$ is annihilated by the $N_{G_{K_\mathfrak{p}}}$. The unit ϵ_g generates $\mathcal{E}$ and $f(\epsilon_g) = 0$ if and only if f is trivial. This implies that the above map is injective. It follows that

$$\left(\frac{\mathcal{E}}{\mu_K \mathcal{E}^M}\right)^\perp \cong I$$

since the orders of these two groups are equal. Therefore the exact sequence (2.2) gives us

$$B_{K_\mathfrak{p}}[M]^\perp \cong I/\left\{f(\epsilon_g) : f \in D^\perp\right\} \quad \text{where} \quad D = \frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K (\mathcal{O}_{K_\mathfrak{p}}^*)^M}.$$

Now we explain the correspondence between $D^\perp$ and the Galois group of the Kummer extension given by (2.1). There is an explicit isomorphism between $D^\perp$ and D^{dual} given by [3, Proposition 1.1 (i)]. We have further isomorphisms as follows:

$$\begin{aligned} D^{\mathrm{dual}} = \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K (\mathcal{O}_{K_\mathfrak{p}}^*)^M}, \mathbf{Q}/\mathbf{Z}\right) &\cong \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K}, \mathbf{Z}/M\mathbf{Z}\right) \\ &\cong \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K}, \mu_M\right) \\ &\cong \mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}_{K_\mathfrak{p}}^*}\right)/F\right). \end{aligned}$$

Here the first isomorphism is natural and the second one depends on a choice of M-th root of unity. The last isomorphism is given by (2.1). Every element in the Galois group of this Kummer extension is equal to $\tau_\mathcal{R}$, the Artin symbol of an unramified prime ideal $\mathcal{R} \subset F$ of degree one. Let us denote the corresponding element in $D^\perp$ by $f_\mathcal{R}$. Therefore we have

$$B_{K_\mathfrak{p}}[M]^\perp \cong I/\{f_\mathcal{R}(\epsilon_g) : \mathcal{R} \in S\}$$

as we have stated in the theorem. □

Let $u \in \mathcal{O}_{K_\mathfrak{p}}^*$ and let $\mathcal{R} \subset F$ be an unramified prime ideal of degree one. The Artin symbol $\tau_\mathcal{R}$ satisfies $(\sqrt[M]{u})^{\tau_\mathcal{R}} \equiv (\sqrt[M]{u})^r \pmod{\mathcal{R}}$ by definition. Kummer theory implies that $(\sqrt[M]{u})^{\tau_\mathcal{R}-1}$ is an M-th root of unity. Combining these two facts, we see that

$$(\sqrt[M]{u})^{\tau_\mathcal{R}-1} \equiv \left(\sqrt[M]{u}\right)^{(r-1)} \equiv u^{(r-1)/M} \pmod{\mathcal{R}}$$

is an M-th root of unity in $\mathbf{Z}/r\mathbf{Z}$.

Define the map $\chi : R \to \mathbf{Z}/M\mathbf{Z}$ which sends $\sum c_\sigma \sigma$ to c_1, the coefficient of the identity element. In the proof of Theorem 2.4, the isomorphism

$$D^\perp \cong \mathrm{Hom}_{\mathbf{Z}}\left(\frac{\mathcal{O}_{K_\mathfrak{p}}^*}{\mu_K}, \mathbf{Z}/M\mathbf{Z}\right)$$

is obtained by $f \mapsto \chi f$ (see Schoof's remark after [3, Proposition 1.1]). If

$$f_{\mathcal{R}}(\epsilon_g) = \sum_{\sigma \in G_{K_\mathfrak{p}}} c_\sigma \sigma,$$

then it is easy to see that $c_\sigma = \chi f_{\mathcal{R}}(\sigma^{-1}(\epsilon_g))$. Fix a primitive M-th root of unity ζ_M in F. The coefficients c_σ can be uniquely determined from the equation

$$\sigma^{-1}(\epsilon_g)^{(r-1)/M} \equiv \zeta_M^{c_\sigma} \pmod{\mathcal{R}}.$$

Construction of the prime ideals $\mathcal{R}$ can be done using class field theory. We start with a degree one prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ with norm $r \equiv 1 \pmod{W_K M}$ and check if its generator $\pi_\mathfrak{r}$ satisfies $(\pi_\mathfrak{r})^{W_K} \equiv 1 \pmod{\mathfrak{p}}$. These two conditions imply that $\mathfrak{r}$ totally splits in F.

Even though we can easily obtain the prime ideals $\mathcal{R}$, it is not easy to find $\sigma(\epsilon_g) \pmod{\mathcal{R}}$ for an arbitrary $\sigma \in G_{K_\mathfrak{p}}$. The main reason is that, unlike the cyclotomic case, we do not have an algebraic expression for ϵ_g.

Finding $\sigma(\epsilon_g)$ Modulo $\mathfrak{R}$. Let $\mathfrak{R} \subset K_\mathfrak{p}$ be the prime ideal lying under $\mathcal{R}$. Since ϵ_g is in $K_\mathfrak{p}$, it is enough to work with $\mathfrak{R}$. We use r-adic numbers $\mathbf{Q}_r$ to find $\sigma(\epsilon_g) \pmod{\mathfrak{R}}$ for any $\sigma \in G_{K_\mathfrak{p}}$.

Let g be a primitive root modulo p, and let σ_g be the corresponding element generating the Galois group $G_{K_\mathfrak{p}}$. Given $\alpha \in \mathcal{O}_{K_\mathfrak{p}}$, define the polynomial

$$P_\alpha(x) = \prod_{i=0}^{n-1} (x - \sigma_g^i(\alpha)) \in \mathcal{O}_K[x]$$

where $n = (p-1)/W_K$ is the degree of the extension $K_\mathfrak{p}/K$. Let $\mathfrak{r} \subset \mathcal{O}_K$ be a degree one prime ideal which splits totally in the extension $K_\mathfrak{p}/K$. The polynomial P_{ϵ_g} is factored into linear factors

$$P_{\epsilon_g}(x) = \prod_{i=0}^{n-1} (x - e_i)$$

in the polynomial ring $\mathbf{Q}_r[x]$. We fix an embedding of $K_\mathfrak{p}$ into $\mathbf{Q}_r$ by mapping ϵ_g to e_0. Given $\alpha \in K_\mathfrak{p}$, we denote the corresponding element in $\mathbf{Q}_r$ by $\tilde{\alpha}$. Let $\mathfrak{R} \subset K_\mathfrak{p}$ be the unique prime ideal lying above $\mathfrak{r}$ such that $\epsilon_g \pmod{\mathfrak{R}^n}$ is congruent to $e_0 \pmod{r^n}$ for all $n \geq 1$.

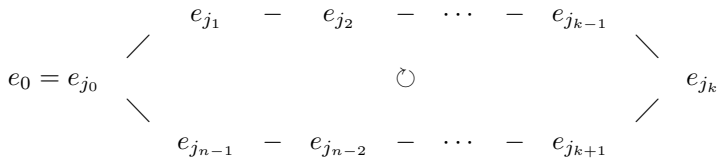
For each $0 \leq i \leq n-1$, there exists j_i such that $\sigma_g^i(\tilde{\epsilon_g}) = e_{j_i}$. We already have $j_0 = 0$. In order to determine j_1, let us consider the factorization of the polynomial

$$P_{\epsilon_g \sigma_g(\epsilon_g)}(x) = \prod_{k=0}^{n-1} (x - h_k)$$

in $\mathbf{Q}_r[x]$. We determine those $1 \leq i \leq n-1$ for which the product $e_0 e_i$ is equal to h_k for some $0 \leq k \leq n-1$. There are only two such values; one of them is for

$\tilde{\epsilon_g}\sigma_g(\tilde{\epsilon_g})$ and the other one is for $\sigma_g^{-1}(\tilde{\epsilon_g}\sigma_g(\tilde{\epsilon_g}))$. We apply this algorithm until we obtain a cycle

connecting each e_i to those two values (see Example 2.7). Now we need to determine if $\sigma^i(\tilde{\epsilon_g})$ is obtained by going clockwise or counterclockwise. We use the factorization of the polynomial $P_{\epsilon_g\sigma_g(\epsilon_g)\sigma_g^3(\epsilon_g)}(x)$ in the ring $\mathbf{Q}_r[x]$ to check which direction is correct. Finally, we obtain the cycle



with the property $\sigma_g^i(\tilde{\epsilon_g}) = e_{j_i}$. Now it is easy to see that the integer value $\sigma_g^i(\epsilon_g) \pmod{\mathcal{R}}$ is given by $e_{j_i} \pmod{r}$ for all $0 \le i \le n-1$. We require that $n = [K_\mathfrak{p} : K]$ is bigger than or equal to 6 so that this process makes sense. Note that the class number of $K_\mathfrak{p}$ can be computed easily if the degree of the extension $K_\mathfrak{p}/K$ is less than 6.

Remark 2.5. Since we need to go through this process every time, our algorithm for the elliptic case is slower than Schoof's original algorithm for real cyclotomic fields. That's why our ranges for the norm of conductors and the size of Jordan-Hölder factors are rather small compared to those of Schoof.

Remark 2.6. Each time we factor a polynomial r-adically, we first check if it has distinct roots in the ring $(\mathbf{Z}/r\mathbf{Z})[x]$. If that is the case, Hensel's lemma guarantees that these linear factors can be lifted to the ring $\mathbf{Q}_r[x]$. Otherwise we skip the prime ideal $\mathfrak{r} \subset \mathcal{O}_K$ and proceed to the next one.

Example 2.7. We illustrate this process by giving an example. Let K be the imaginary quadratic field with discriminant $d_K = -43$. Let $\mathfrak{p}_{13} \subset \mathcal{O}_K$ be the degree one prime ideal with basis $[13, 2-w]$. Fix $g = 7$, an odd primitive root modulo 13. We compute the elliptic unit ϵ_g and its Galois conjugates with high precision and we obtain

$$\begin{aligned}
&\epsilon_g \approx -1.218 + 7.156\,\mathrm{I}, && \sigma_g^3(\epsilon_g) \approx -0.526 - 0.582\,\mathrm{I},\\
&\sigma_g(\epsilon_g) \approx -0.388 + 0.288\,\mathrm{I}, && \sigma_g^4(\epsilon_g) \approx 0.106 + 0.409\,\mathrm{I},\\
&\sigma_g^2(\epsilon_g) \approx 1.595 - 0.899\,\mathrm{I}, && \sigma_g^5(\epsilon_g) \approx 0.430 + 0.183\,\mathrm{I}.
\end{aligned}$$

The minimal polynomial of ϵ_g over K is given by

$$\begin{aligned}
P_{\epsilon_g}(x) \;=\; & x^6 + (-2w+1)x^5 + (3w+1)x^4\\
& +(w+2)x^3 + 5x^2 + (-w+1)x - 1
\end{aligned}$$

Let $\mathfrak{r} \subset \mathcal{O}_K$ be the degree one prime ideal of norm $r = 47$ with basis $[47, 25-w]$. The ideal $\mathfrak{r}$ is generated by $\pi_\mathfrak{r} = 2w-3$ and $\pi_\mathfrak{r} \equiv 1 \pmod{\mathfrak{p}}$. Hence it splits totally

in the extension $K_{\mathfrak{p}_{13}}/K$ by the class field theory. Factoring $P_{\epsilon_g}(x)$ r-adically we get $P_{\epsilon_g}(x) = \prod_{i=0}^{5}(x - e_i)$ where

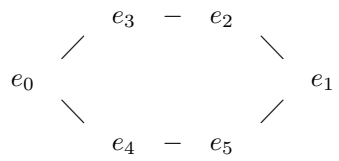
$$\begin{aligned} e_0 &\approx 34 + 40 \cdot 47 + 1 \cdot 47^2, & e_3 &\approx 5 + 40 \cdot 47 + 29 \cdot 47^2, \\ e_1 &\approx 22 + 9 \cdot 47 + 26 \cdot 47^2, & e_4 &\approx 26 + 15 \cdot 47 + 36 \cdot 47^2, \\ e_2 &\approx 24 + 10 \cdot 47 + 28 \cdot 47^2, & e_5 &\approx 32 + 12 \cdot 47 + 41 \cdot 47^2. \end{aligned}$$

The r-adic precision should be high enough so that all products $e_i e_j$ are different from each other. We fix an embedding of $K_{\mathfrak{p}}$ into $\mathbf{Q}_r$ by $\tilde{\epsilon_g} = e_0$. We also fix a prime ideal $\mathfrak{R} \subset K_{\mathfrak{p}}$ lying above $\mathfrak{r}$ such that $\epsilon_g \equiv 34 \pmod{\mathfrak{R}}$.

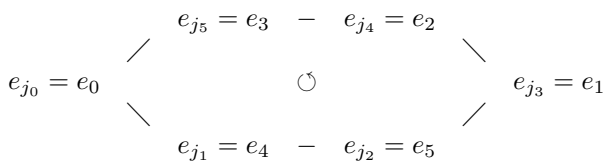
For each $0 \leq i \leq 5$, there exists j_i such that $\sigma_g^i(\tilde{\epsilon_g}) = e_{j_i}$. We already have $j_0 = 0$. In order to determine j_1, let us consider the factorization of the polynomial $P_{\epsilon_g \sigma_g(\epsilon_g)}(x) = \prod_{k=0}^{5}(x - h_k)$ in $\mathbf{Q}_r[x]$. We have

$$\begin{aligned} h_0 &\approx 38 + 17 \cdot 47 + 3 \cdot 47^2, & h_3 &\approx 11 + 24 \cdot 47 + 23 \cdot 47^2, \\ h_1 &\approx 33 + 10 \cdot 47 + 18 \cdot 47^2, & h_4 &\approx 26 + 25 \cdot 47 + 35 \cdot 47^2, \\ h_2 &\approx 46 + 2 \cdot 47 + 21 \cdot 47^2, & h_5 &\approx 29 + 12 \cdot 47 + 39 \cdot 47^2. \end{aligned}$$

It turns out that $e_0 e_3 = h_5$ and $e_0 e_4 = h_0$. We place e_3 and e_4 next to e_0 and then search for what comes after e_3. Observe that we just need to check the products e_3e_1, e_3e_2, e_3e_5 since we have already used the values e_0 and e_4. We have $e_3e_2 = h_4$ and therefore e_3 is followed by e_2. Then we see that $e_2e_1 = h_3$ which means e_2 is followed by e_1. Finally, we place e_5 to the remaining spot and obtain the following diagram:



Now we need to determine if $\sigma_g^i(\tilde{\epsilon_g})$ is obtained by going clockwise or counterclockwise. For this purpose, we use the factorization of the polynomial $P_{\epsilon_g \sigma_g(\epsilon_g) \sigma_g^3(\epsilon_g)}(x)$. It turns out that $e_0e_2e_1$ is an r-adic root of this polynomial and hence the orientation must be counterclockwise:



Now the roots of $P_{\epsilon_g}(x)$ are ordered in a compatible way with the Galois action. The integer value $\sigma_g^i(\epsilon_g) \pmod{\mathfrak{R}}$ is given by $e_{j_i} \pmod{r}$ for all $0 \leq i \leq n-1$.

The Algorithm. Let $\mathcal{R}$ be an unramified prime ideal of $F = K_{\mathfrak{p}}(\zeta_{W_K M})$ of degree one with underlying primes $\mathfrak{R} \subset K_{\mathfrak{p}}$ and $\mathfrak{r} \subset K$. In order to compute $f_{\mathcal{R}}(\epsilon_g)$ we need to make choices for elements ϵ_g and ζ_M modulo $\mathcal{R}$. If we change $\mathcal{R}$ lying above $\mathfrak{R}$, then it corresponds to a different choice of ζ_M, and $f_{\mathcal{R}}(\epsilon_g)$ would change by a unit of $\mathbf{Z}/M\mathbf{Z}$. Changing $\mathfrak{R}$ over $\mathfrak{r}$ is equivalent to changing ϵ_g with one of its conjugates. Such a change corresponds to multiplying $f_{\mathcal{R}}(\epsilon_g)$ with a power of σ_g,

another unit in $(\mathbf{Z}/M\mathbf{Z})[G_{K_\mathfrak{p}}]$. Therefore the ideal generated by elements $f_\mathcal{R}(\epsilon_g)$ only depends on the prime ideals $\mathfrak{r}$ in the ground field K. There is an isomorphism

$$(\mathbf{Z}/M\mathbf{Z})[G_{K_\mathfrak{p}}] \cong (\mathbf{Z}/M\mathbf{Z})[X]/(X^{(p-1)/W_K} - 1)$$

given by $\sigma_g \mapsto X$. Let $f_\mathfrak{r}(X)$ denote the image of $f_\mathcal{R}(\epsilon_g)$ under this isomorphism which is well defined up to a unit. We denote the augmentation ideal of both rings by I. The following theorem is a direct consequence of Theorem 2.4.

Theorem 2.8. *Using the notation above, we have that*

$$B_{K_\mathfrak{p}}[M]^\perp = I/\langle f_\mathfrak{r}(X) : \mathfrak{r} \in S_M \rangle$$

where S_M is the set of prime ideals $\mathfrak{r} = (\pi_\mathfrak{r})$ in $\mathcal{O}_K$ of norm r satisfying $(\pi_\mathfrak{r})^{W_K} \equiv 1 \pmod{\mathfrak{p}}$ and $r \equiv 1 \pmod{W_K M}$.

We want to determine if $B_{K_\mathfrak{p}}$ admits a Jordan-Hölder factor of order $q = l^f$ or not. Any finite R-module is Jordan-Hölder isomorphic to its dual and we have

$$B_{K_\mathfrak{p}}^\perp = \prod_l \prod_\varphi (B_{K_\mathfrak{p}}^\perp)_\varphi$$

by the Jordan-Hölder filtration given by [3, Section 3]. The irreducible polynomials φ are obtained by factoring $X^m - 1$ in the l-adic polynomial ring $\mathbf{Z}_l[X]$ where m is given by $(p-1)/W_K = l^a m$ with $\gcd(m, l) = 1$.

Fix p and $q = l^f$. The possible degree d of these factors all divide

$$\delta = \gcd\left((p-1)/W_K, q-1\right).$$

If $\delta = 1$, then $B_{K_\mathfrak{p}}^\perp$ does not admit any Jordan-Hölder factor of order q by [3, Proposition 3.1]. Otherwise we compute

$$f_\mathfrak{r}(X) \pmod{X^\delta - 1}$$

for several primes $\mathfrak{r}$ with $M = l$. Computing the greatest common divisors of these elements recursively, we look for a common divisor φ dividing $\frac{X^\delta - 1}{X - 1}$ of degree exactly f. If we guarantee that there is no such factor, we stop. Theorem 2.8 implies that $B_{K_\mathfrak{p}}^\perp$ does not admit any Jordan-Hölder factors of order q.

If there is a repeating factor φ which appears in every calculation with $\deg(\varphi) = f$ (possibly more than one), then we believe that $B_{K_\mathfrak{p}}$ admits a nontrivial Jordan-Hölder factor of order q and we proceed to the second and third steps of Schoof's algorithm. These steps are executed very rarely and we illustrate them by giving an example.

Example 2.9. Let K be the imaginary quadratic field with discriminant $d_K = -67$. Let $\mathfrak{p}_{421} \subset \mathcal{O}_K$ be the degree one prime ideal with basis $[421, 85 - w]$. Fix $g = 23$, an odd primitive root modulo 421. Computing $f_\mathfrak{r}(X) \pmod{X^\delta - 1}$ for several primes $\mathfrak{r} \in S_3$ with $\delta = 2$, we see that the nontrivial factor $\varphi = X + 1$ appears every time. We start to believe that $(B_{K_{\mathfrak{p}_{421}}})_\varphi$ is nontrivial. We write the degree of the extension 210 as a product $l^a m$ where m is coprime to $l = 3$. This gives us that $a = 1$ and $(B_{K_{\mathfrak{p}_{421}}})_\varphi$ is a module over the ring $\mathbf{Z}_3[X]/(\varphi(X^3)) \cong \mathbf{Z}_3[X]/(X^3 + 1)$.

Following Schoof, we introduce a new variable for simpler computations. Observe that X has order 6 in the local ring $\mathbf{Z}_3[X]/(X^3 + 1)$. We pick $1 + T = X^2$ as in Iwasawa theory so that the maximal ideal of the local ring

$$\mathbf{Z}_3[T]/((1+T)^3 - 1) \cong \mathbf{Z}_3[X]/(X^3 + 1)$$

is of the form $(T, 3)$. Now we perform the second step of Schoof's algorithm and compute elements in $(\mathbf{Z}/M\mathbf{Z})[T]/((1+T)^3-1)$ for $M \in \{3, 9, 27, ...\}$.

$\mathfrak{r} = (r, w - w_{\mathfrak{r}})$	$M = 3$	$M = 9$	$M = 27$
$(248509, w - 14797)$	T^2	$T^2 + 6T$	$10T^2 + 24T$
$(297757, w - 78203)$	0	$6T^2 + 6$	$15T^2 + 18T + 15$
$(306991, w - 59125)$	0	$3T^2$	$3T^2$
$(317197, w - 24608)$	T^2	$T^2 + 6T + 3$	$T^2 + 24T + 3$
$(354727, w - 104164)$	0	$3T^2 + 3T + 3$	$12T^2 + 3T + 12$
$(458569, w - 272363)$	$2T^2$	$2T^2 + 3T + 6$	$20T^2 + 12T + 15$

For $M = 3$, we compute the ideal $\mathcal{I}^{(3)}$ generated by $f_{\mathfrak{r}}$ in the corresponding column. After several tries, we believe that $\mathcal{I}^{(3)}$ is generated by T^2. We have a surjective map

$$(\mathbf{Z}/3\mathbf{Z})[T]/(T^2) \twoheadrightarrow \left((B_{K_{\mathfrak{p}_{421}}})_{\varphi}[3]\right)^{\perp}$$

which we believe to be an isomorphism. For $M = 9$, the ideal $\mathcal{I}^{(9)}$ is generated by T^2 and 3. The module $(\mathbf{Z}/9\mathbf{Z})[T]/(T^2, 3)$ is isomorphic to $(\mathbf{Z}/3\mathbf{Z})[T]/(T^2)$ and this concludes the second step of Schoof's algorithm.

We suspect that $(B_{K_{\mathfrak{p}_{421}}})_{\varphi}$ is isomorphic to $\mathbf{Z}_3[T]/(T^2, 3)$. In order to verify this we apply the third step of Schoof's algorithm. We use the surjective map above with [3, Proposition 1.2 (iv)]. We have $R = (\mathbf{Z}/3\mathbf{Z})[T]/((1+T)^3-1)$ and $J = (T^2)$ so that $\mathrm{Ann}_R(J) = (T)$. Since $1 + T = X^2$, we have $T = X^2 - 1$. Define

$$h_{\varphi}(X) = \frac{X^{210} - 1}{X^3 + 1}(X^2 - 1),$$

an element in $(Z/3\mathbf{Z})[X]/(X^{210} - 1)$. We want to show that the elliptic unit

$$\epsilon_{\varphi} = \epsilon_g^{h_{\varphi}(\sigma_g)}$$

is a third power of another unit in $K_{\mathfrak{p}}$. Let K_6 be the unique subfield of $K_{\mathfrak{p}}$ such that $[K_6 : K] = 6$. Observe that X^3+1 divides X^6-1. This implies that the norm map from $K_{\mathfrak{p}}$ to K_6, divides $h_{\varphi}(X)$ and therefore $\epsilon_{\varphi} \in K_6$. In fact the minimal polynomial of ϵ_{φ} is given by

$$\begin{aligned} F(t) = t^6 &+ (25552848w + 62631721)t^5 \\ &+ (63659755470266w - 10490555538824)t^4 \\ &+ (825954922943743w - 12797162812861606)t^3 \\ &+ (-4136459180619w - 1293163421150)t^2 \\ &+ (23197957w - 46562185)t + 1. \end{aligned}$$

Let r be a rational prime, not congruent to 1 modulo 3, which splits totally in $K_{\mathfrak{p}}$. We embed our field $K_{\mathfrak{p}}$ into r-adic integers $\mathbf{Q}_r$ and compute the correct third roots of ϵ_{φ} and its conjugates with high precision. Then we compute

$$\prod_{i=1}^{6} \left(t - \sqrt[3]{\sigma_g^i(\epsilon_{\varphi})}\right).$$

The coefficients of this polynomial are very close to algebraic integers in $\mathcal{O}_K$. In fact we have

$$\begin{aligned} G(t) = t^6 &+ (-96w - 140)t^5 + (7630w + 53784)t^4 \\ &+ (6920w - 233277)t^3 + (-3819w - 23252)t^2 \\ &+ (-127w + 144)t + 1. \end{aligned}$$

To make sure that our computations are correct, we also check if the polynomial $G(t)$ divides $F(t^3)$ in $\mathcal{O}_K[t]$. This shows that $\epsilon_\varphi = u^3$ for some $u \in K_6 \subset K_{\mathfrak{p}}$ and we conclude that the module $(B^{\perp}_{K_{\mathfrak{p}_{421}}})_\varphi$ is actually isomorphic to $\mathbf{Z}_3[T]/(T^2, 3)$.

3. Results

In this section we explain our main results and the data we collect from our algorithm. First, we give the proof of Theorem 2 and discuss briefly Hurwitz numbers, the elliptic analogue of Bernoulli numbers. Then we give some statistical information about our tables and explain how to obtain the structure of $(B_{K_{\mathfrak{p}}})_\varphi$ for each Jordan-Hölder factor listed in the tables. Last, we apply Cohen-Lenstra heuristics to our case and argue that each table at the end is a table of class numbers with probability at least 96%.

Proof of Theorem 2. Let K be the imaginary quadratic field with $d_K = -163$ and let $\mathfrak{p}_{307}$ be a degree one prime ideal in $\mathcal{O}_K$ of norm 307. Computing $f_{\mathfrak{r}}(X)$ for several primes $\mathfrak{r} \in S_{307}$, we observe that the factor $\varphi = X + 92$ appears every time. Define

$$h_\varphi(X) = \frac{X^{153} - 1}{X + 92},$$

an element in $(\mathbf{Z}/307\mathbf{Z})[X]/(X^{153} - 1)$. In order to show that the class number of $K_{\mathfrak{p}_{307}}$ is divisible by 307, we need to verify that the elliptic unit

$$\epsilon_\varphi = \epsilon_g^{h_\varphi(\sigma_g)}$$

is a 307th power of a unit u in the same field. The unit u will be automatically nonelliptic since there is no polynomial $f \in \mathbf{Z}[X]$ such that $h_\varphi(X) = 307f$.

We can obtain ϵ_φ with accuracy as high as we want as an imaginary number. However, the correct 307-th root of ϵ_φ in $K_{\mathfrak{p}} \subset \mathbf{C}$ is not obvious. Therefore we work with $\mathbf{Q}_r$, r-adic rational numbers, for some special prime $r \in \mathbf{Z}$. The rational prime r must split totally in $K_{\mathfrak{p}}$ so that $K_{\mathfrak{p}}$ can be embedded into $\mathbf{Q}_r$. We also require that $r \not\equiv 1 \pmod{307}$ which makes taking the 307-th root in $\mathbf{Q}_r$ unique. For example, $r = 25801$ is such a prime for $\mathfrak{p} = [307, 148 - w]$.

Factoring the minimal polynomial of $\epsilon_g \in K_{\mathfrak{p}}$ in the polynomial ring $\mathbf{Z}_r[x]$ with 1000 digit r-adic precision, we obtain ϵ_g and all of its conjugates r-adically. Then we compute

$$\prod_{i=1}^{153} \left(t - \sqrt[307]{\sigma_g^i(\tilde{\epsilon_\varphi})} \right)$$

which has r-adic coefficients which are very close to elements in $\mathcal{O}_K \subset \mathbf{Q}_r$. This *proves* that $\epsilon_\varphi = u^{307}$ for some nonelliptic unit u in $\mathcal{O}^*_{K_{\mathfrak{p}_{307}}}$. We have also performed another experimental check. Let $G(t)$ be the resulting polynomial in $\mathcal{O}_K[t]$ obtained by rounding these coefficients. We have factored $G(t)$ over $(\mathcal{O}_K/\mathfrak{q})[t]$ for 5000 degree one prime ideals $\mathfrak{q} \subset \mathcal{O}_K$. Using Chebotarev's density theorem, we *conclude* that $G(t)$ generates an Abelian extension of K of degree 153.

Recall that $B_{K_\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}^*/\mathcal{E}$ for all $K_\mathfrak{p}$. The unit u is a nontrivial element of this quotient group and of its order is equal to 307, a prime number. This implies that 307 divides the order of $B_{K_{\mathfrak{p}_{307}}}$ and finally we obtain $307|\#\mathrm{Cl}(K_{\mathfrak{p}_{307}})$ using the fact that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ have the same number of elements. □

There are interesting families of numbers, namely Bernoulli and Hurwitz numbers, for fields $\mathbf{Q}_{(p)}$ and $K_\mathfrak{p}$, respectively. These numbers are related to the p-divisibility of the class number of the corresponding field. If p divides the class number of p-th cyclotomic field $\mathbf{Q}(\zeta_p)$, then it divides the numerator of a Bernoulli number with even index less than $p-1$ [6, Theorem 6.17]. It is a well-known fact the class group of the real cyclotomic field $\mathbf{Q}_{(p)}$ injects into the class group of $\mathbf{Q}(\zeta_p)$. Therefore we easily obtain the following result: If an odd prime p divides the class number of $\mathbf{Q}_{(p)}$, then p divides the numerator of a Bernoulli number with even index less than $p-1$. It is a conjecture of Vandiver that p never divides the class number of $\mathbf{Q}_{(p)}$.

In order to illustrate the situation in the elliptic case, we first give the definition of Hurwitz numbers following Robert [2]. Let K be an imaginary quadratic field and let $\mathcal{O}_K$ be its ring of integers considered as a lattice in complex numbers. The Hurwitz numbers attached to $\mathcal{O}_K$ are the numbers

$$G_k(\mathcal{O}_K) = \sum_{\substack{\lambda \in \mathcal{O}_K \\ \lambda \neq 0}} \frac{1}{\lambda^k}$$

given by the Eisenstein series of $\mathcal{O}_K$ of weight $k > 2$. Hurwitz numbers are closely related to the coefficients of the Laurent series expansion of the Weierstrass $\wp$-function. In fact we have

$$\wp(z;\mathcal{O}_K) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\mathcal{O}_K) z^{2k}.$$

Theorem 3.1. *Let K be an imaginary quadratic field and let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm p not dividing $6d_K$. If p divides the class number of $K_\mathfrak{p}$, then p divides the numerator of $G_k(\mathcal{O}_K)$ for some k divisible by W_K with $0 < k < p-1$.*

Proof. This is a result of Robert's work [2]. A proof, specialized to the case where K has class number one, can be found in [1]. □

Now we apply this to $K_{\mathfrak{p}_{307}}$. Let K be the imaginary quadratic field with $d_K = -163$. The minimal Weierstrass equation of the elliptic curve $E \cong \mathbf{C}/\mathcal{O}_K$ over $\mathbf{Q}$ is given by

$$E : y^2 + y = x^3 - 2174420x + 1234136692.$$

We have used the PARI command `ellwp(E,z)` in order to obtain the Laurent series

$$\wp(z;\mathcal{O}_K) = \frac{1}{z^2} + 434884z^2 - \frac{705220967}{4} z^4 + \cdots$$

and therefore the Hurwitz numbers $G_k(\mathcal{O}_K)$. Theorem 2 implies that 307 divides the class number of $K_{\mathfrak{p}_{307}}$. It turns out that 307 divides the numerator of $G_{94}(\mathcal{O}_K)$. This is the only Hurwitz number $G_k(\mathcal{O}_K)$ with even index $0 < k < 306$ whose numerator is divisible by 307.

Tables. Our analogue of Schoof's algorithm gives us the largest submodule of $B_{K_\mathfrak{p}}$ with Jordan-Hölder factors of order less than 2000. We denote the order of this submodule by $\tilde{h}_{K_\mathfrak{p}}$. The observation we make after Proposition 2.2 implies that the number $\tilde{h}_{K_\mathfrak{p}}$ is equal to the largest submodule $\mathrm{Cl}(K_\mathfrak{p})$ with Jordan-Hölder factors of order less than 2000.

There are 9 imaginary quadratic fields K with class number one. For each ground field K, we have worked with degree one prime ideals $\mathfrak{p} \subset K$ of norm p not dividing $6d_K$ and less than 700. In total there are 535 ray class fields $K_\mathfrak{p}$. For 455 of these, we have found that $\tilde{h}_{K_\mathfrak{p}} = 1$. The remaining 80 are given in the tables at the end of this chapter.

In our tables, we use the same format of the main table in Schoof's paper. The numbers $\tilde{h}_{K_\mathfrak{p}}$ are given as a product of the orders of simple Jordan-Hölder factors. The degree d of each factor is indicated in the third column, respectively. If a simple Jordan-Hölder factor $\mathbf{F}_l[X]/(\varphi(X))$ of order q occurs with multiplicity greater than 1, we write $\tilde{h}_{K_\mathfrak{p}}$ as a product $q^{s_0}q^{s_1}\cdots q^{s_n}$ with respective degrees $d, dl, ..., dl^n$ to indicate the orders of $(B^\perp_{K_\mathfrak{p}})_\varphi$ modulo $\varphi(X^{l^i})$ are $q^{s_0+\cdots+s_i}$ for $0 \le i \le n$.

If $(B_{K_\mathfrak{p}})_\varphi$ has a Jordan-Hölder filtration of length 1, then it is isomorphic to $(Z/lZ)[X]/(\varphi(X))$ as a Galois module. In such a case, $(B_{K_\mathfrak{p}})_\varphi$ has f copies of $\mathbf{Z}/l\mathbf{Z}$ as an abelian group where f is the degree of the irreducible polynomial $\varphi \in \mathbf{Z}_l[X]$. There are 6 cases in which $(B_{K_\mathfrak{p}})_\varphi$ has a Jordan-Hölder filtration of length bigger than 1. We list them in the table below together with the structure of $(B^\perp_{K_\mathfrak{p}})_\varphi$. The use of parameter T is explained in Example 2.9.

d_K	p	q	d	length	$(B^\perp_{K_\mathfrak{p}})_\varphi$
19	271	4	3	2	$\mathbf{Z}_2[\zeta_3]/4\mathbf{Z}_2[\zeta_3]$
43	397	3	2	2	$\mathbf{Z}_3[T]/(T+3,9)$
67	421	3	2	2	$\mathbf{Z}_3[T]/(T^2,3)$
67	457	3	2	2	$\mathbf{Z}_3[T]/(T-3,9)$
67	461	4	2	2	$\mathbf{Z}/9\mathbf{Z}$
163	641	5	4	3	$\mathbf{Z}/125\mathbf{Z}$

In order to obtain the structure of $(B_{K_\mathfrak{p}})_\varphi$ for these cases, one can use [3, Proposition 1.2 (*iii*)] which implies that $(B_{K_\mathfrak{p}})_\varphi \cong (B^\perp_{K_\mathfrak{p}})_\varphi$ whenever the length of $(B^\perp_{K_\mathfrak{p}})_\varphi$ is at most 2. There is only one case with Jordan-Hölder filtration of length bigger than 2, namely $d_K = -163, p = 641, l = 5$. In this case, the annihilator of the module $(B^\perp_{K_\mathfrak{p}})_\varphi$ is principal and we still have $(B_{K_\mathfrak{p}})_\varphi \cong (B^\perp_{K_\mathfrak{p}})_\varphi$ by [3, Proposition 1.2 (*ii*)].

It is not true in general that $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are isomorphic as Galois modules. A counterexample for real cyclotomic fields is given by a degree 3 extension of $\mathbf{Q}$ lying in $\mathbf{Q}_{(p)}$ (see Schoof [3, p. 929]). We have looked for a similar example in the elliptic case and in fact we have found one. Let K be the imaginary quadratic field with $d_K = -163$ and let $\mathfrak{p}_{2659} \subset \mathcal{O}_K$ be a degree one prime ideal of norm 2659. The ray class field $K_{\mathfrak{p}_{2659}}$ has a unique subfield K_3 such that $[K_3 : K] = 3$. Starting with a generator of elliptic units and then taking its trace from $K_{\mathfrak{p}_{2659}}$ to K_3, we obtain the minimal polynomial of this extension $K_3/\mathbf{Q}$ as follows:

$$f_{K_3/\mathbf{Q}} = x^6 + 389x^5 + 18196x^4 - 7076416x^3 \\ - 488496804x^2 + 48339551084x + 3971404926677.$$

The software PARI gives us

$$\mathrm{Cl}(K_3) \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})$$

as an Abelian group. Let $\varphi = X^2 + X + 1 \in \mathbf{Z}_2[X]$. Since φ is the only irreducible polynomial dividing $\frac{X^3-1}{X-1}$, the Galois module $\mathrm{Cl}(K_{\mathfrak{p}_{2659}})_\varphi$ is isomorphic to $\mathrm{Cl}(K_3)$ and it is annihilated by 2. On the other hand, $(B_{K_{\mathfrak{p}_{2659}}})_\varphi$ has 16 elements and is a subset of $(\mathbf{Z}/16\mathbf{Z})[X]/(X^2 + X + 1)$. It is clear that $(B_{K_{\mathfrak{p}_{2659}}})_\varphi$ is not annihilated by 2. Therefore $B_{K_\mathfrak{p}}$ and $\mathrm{Cl}(K_\mathfrak{p})$ are not isomorphic as Galois modules in general. However, they have isomorphic Galois cohomology groups.

Proposition 3.2. *Let $\mathfrak{p} \subset \mathcal{O}_K$ be a degree one prime ideal of norm $p < 700$ not dividing $6d_K$. There are canonical isomorphisms*

$$\widehat{H}^i(H, \mathrm{Cl}(K_\mathfrak{p})) \xrightarrow{\cong} \widehat{H}^{i+2}(H, B_{K_\mathfrak{p}})$$

for each $i \in \mathbf{Z}$. In particular, for each choice of a generator of H there are natural isomorphisms $\widehat{H}^i(H, \mathrm{Cl}(K_\mathfrak{p})) \cong \widehat{H}^i(H, B_{K_\mathfrak{p}})$ for each $i \in \mathbf{Z}$.

Proof. The prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is totally and tamely ramified in the extension $K_\mathfrak{p}/K$. The proof can be adapted from its cyclotomic analogue [3, Proposition 5.1 (*ii*)] using Proposition 2.2. □

Cohen-Lenstra Heuristics. Following Schoof [3, Section 6], we estimate the behavior of Jordan-Hölder factors of the ideal class group $\mathrm{Cl}(K_\mathfrak{p})$ that have very large order. According to Cohen-Lenstra heuristics, the probability that the class group of $K_\mathfrak{p}$ does not admit any simple Jordan-Hölder factor of order q at all is at least

$$H_{K_\mathfrak{p}}(p, q) = \left(\prod_{k \geq 2} 1 - q^{-k} \right)^{n_{p,q}}.$$

Observe that not all the primes p lead to extensions $K_\mathfrak{p}/K$. If the rational prime p is inert in the extension $K/\mathbf{Q}$, then we define $H_{K_\mathfrak{p}}(p, q)$ to be 1. It is easy to see that $H_{K_\mathfrak{p}}(p, q) \geq H_{\mathbf{Q}_{(p)}}(p, q)$ for all values of p and q. The tables at the end contain the numbers $\tilde{h}_{K_\mathfrak{p}}$, the order of the subgroup of $\mathrm{Cl}(K_\mathfrak{p})$ that admits only Jordan-Hölder factors of order $q < Q = 2000$, for $\mathfrak{p}$ of norm $p < P = 700$. The numbers $\tilde{h}_{K_\mathfrak{p}}$ are all equal to the class numbers of the corresponding fields with probability at least

$$\mathcal{P}_K = \prod_{p<P} \prod_{q>Q} H_{K_\mathfrak{p}}(p, q).$$

The calculation given in [3, pp. 933-934] is suitable for our purpose and we have

$$-\log(\mathcal{P}_K) < c\frac{\pi_K(700)}{2000}$$

where $c = 1.29573095...$ and $\pi_K(n)$ is the number of odd primes which split in K less than n. The number $\pi_K(n)$ corresponds to the number of extensions $K_\mathfrak{p}$ for each K. The largest set of $K_\mathfrak{p}$ appears for $d_K = -67$ and there are 63 ray class fields $K_\mathfrak{p}$ with conductor $\mathfrak{p}$ of norm less than 700. Therefore we have

$$\mathcal{P}_K > 0.96000621...$$

for each ground field K.

Tables

$d_K = -3$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
337	5	4	601	5	4
433	3	2	613	3	2

$d_K = -4$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
281	11	10	521	11	5
353	3	2	541	4	3
421	4	3	577	$17 \cdot 37$	$16, 36$

$d_K = -7$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
317	3	2	487	4	3
379	4	3	613	4	3
463	4	3	631	43	21

$d_K = -8$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
281	3	2	601	5	4
577	$5 \cdot 19$	$4, 9$	643	4	3
593	5	2	673	5	2

$d_K = -11$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
257	5	4	421	$7 \cdot 211$	$3, 35$
317	3	2	449	$5 \cdot 9$	$4, 8$
353	67	22	521	11	5

$d_K = -19$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
61	7	6	389	3	2
131	16	5	577	$4 \cdot 97$	$3, 96$
137	5	4	593	5	4
163	4	3	617	$3 \cdot 5$	$2, 4$
229	4	3	619	7	3
271	$4^2 \cdot 11$	$3, 5$	691	4	3

$d_K = -43$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
41	$5 \cdot 11$	$4, 5$	397	$3 \cdot 3$	$2, 6$
53	3	2	401	$5 \cdot 9$	$4, 4$
229	13	6	431	31	5
269	3	2	557	5	2
307	4	3	613	307	102
337	$3 \cdot 5$	$2, 4$	661	$3 \cdot 67$	$2, 11$
353	$5 \cdot 49$	$4, 8$			

$d_K = -67$

p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
17	5	4	421	$3 \cdot 3$	$2, 6$
37	4	3	449	61	4
151	11	5	457	$3 \cdot 3$	$2, 6$
173	5	2	461	3^2	2
193	49	48	613	19	3
389	3	2	617	67	11

	p	$\tilde{h}_{K_\mathfrak{p}}$	d	p	$\tilde{h}_{K_\mathfrak{p}}$	d
$d_K = -163$	97	7	3	373	7	3
	113	3	2	409	7	6
	151	61	5	421	$4 \cdot 7$	$3, 6$
	173	3	2	439	13	3
	223	7	3	457	$5 \cdot 419$	$2, 19$
	281	5	4	641	5^3	4
	307	307	153	661	7	3
	367	37	3			

Acknowledgements

I would like to thank my advisor S. Wong without whom this paper would not have been possible. He has answered all my questions with great patience and taught me how to write a mathematics paper.

I gratefully thank to R. Schoof, F. Hajir and T. Weston for useful discussions. Special thanks to F. Hajir for introducing me to Stark's paper [4] as a project during my first years in graduate school.

Computations were performed on ABACUS, a Linux cluster at the University of Massachusetts, Amherst. I acknowledge the grant NSF-DMS-0619492 for its purchase and I would like to thank H. Johnston who helped me to run my PARI scripts on this machine.

I thank the referees for their comments which were helpful to clarify several statements and correct some mistakes in the paper.

References

1. Á. Lozano-Robledo, *Bernoulli numbers, Hurwitz numbers, p-adic L-functions and Kummer's criterion.* RACSAM Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Mat. 101 (2007), no. 1, 1–32. MR2324575 (2008d:11124)
2. G. Robert, *Nombres de Hurwitz et Unités Elliptiques.* Ann. Scient. Éc. Norm. Sup. (1978), 4^e série, 11, 297-389. MR521636 (80k:12010)
3. R. Schoof, *Class numbers of real cyclotomic fields of prime conductor.* Math. Comp. 72 (2003), no. 242, 913–937 MR1954975 (2004f:11116)
4. H. M. Stark, *L-Functions at s=1. IV. First Derivatives at s=0.* Adv. in Math. 35 (1980), no. 3, 197–235. MR563924 (81f:10054)
5. H. M. Stark, *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. J. 14 1967 1–27. MR0222050 (36:5102)
6. L. C. Washington, *Introduction to Cyclotomic Fields; second edition.* Graduate Texts in Math. 83, Springer-Verlag, Berlin, Heidelberg, New York, 1997. MR1421575 (97h:11130)
7. PARI/GP, version `2.3.2`, `http://pari.math.u-bordeaux.fr/`, Bordeaux, 2006.

University of Massachusetts, Amherst, Department of Mathematics and Statistics, Amherst, Massachusetts 01003

Current address: Middle East Technical University, Department of Mathematics, 06531 Ankara, Turkey

E-mail address: `omerks@gmail.com`