CLASS NUMBERS OF RING CLASS FIELDS OF PRIME CONDUCTOR

OMER KUCUKSAKALLI

Abstract. Let K be an imaginary quadratic field with class number one and let p be a prime not dividing $6d_K$. In this paper we generalize an algorithm of Schoof to compute l-parts of the class numbers of ring class fields L of conductor $p < 200$ for $l < 1000$. We achieve this by using elliptic units analytically constructed by Stark and the Galois action on them given by Shimura's reciprocity law.

Introduction

Computing the class number h_L of a number field L is one of the most important problems in number theory. There are general purpose algorithms which can do this but computations take an extremely long time unless the degree and the discriminant d_K of the field are both small.

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 $\mathcal{C}$ whose index in the full unit group equals the class number of $\mathbf{Q}_{(p)}$. Schoof [5] uses the Galois structure of the quotient $\mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C}$ in order to investigate $h_{\mathbf{Q}_{(p)}}$ for primes $p < 10,000$. On the other hand, general purpose algorithms could give the class number, in a reasonable amount of time, only for $p \leq 113$.

Let K be an imaginary quadratic field with class number one. In our previous paper [4], we have generalized Schoof's algorithm to the ray class fields $K_{\mathfrak{p}}$ of degree one prime conductor of norm $p < 700$ not dividing $6d_K$. We have achieved this by using Stark's elliptic units (whose index in the full unit group is $h_{K_{\mathfrak{p}}}$) and the cyclic Galois structure.

In this paper, we generalize Schoof's algorithm to a different family of number fields. Let p be a prime not dividing $6d_K$ and let $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$ be the order of conductor p. The j-invariant $j(\mathcal{O})$ is an algebraic integer and $L = K(j(\mathcal{O}))$ is an Abelian extension of K. The number field L is called the ring class field of conductor p and has many interesting applications in number theory [2, § 11].

Date: May 9, 2011.

2010 *Mathematics Subject Classification.* Primary 11G16, 11Y40.

Key words and phrases. Elliptic units, Schoof's algorithm, Shimura reciprocity law.

It turns out that the extension L/K is cyclic, a necessary condition for Schoof's algorithm. Moreover L has an explicit subgroup of elliptic units $\mathcal{E}$ such that the order of the quotient $B_L = \mathcal{O}_L^*/\mathcal{E}$ is equal to h_L. The advantage of using the Galois module B_L, instead of $\mathrm{Cl}(L)$, is that it can be analyzed easily using Schoof's generalized algorithm. Given a prime l, we have found all Jordan-Hölder factors of B_L of order divisible by l and obtain the following result.

Main Result. *Let K be an imaginary quadratic field with class number one. Let $p < 200$ be a prime not dividing $6d_K$ and let L be the ring class field of K of conductor p. Let $\tilde{h}_L$ be the product of l-parts of h_L for primes $l < 1000$. For each K, we give two tables (separate for split and inert cases) containing numbers $\tilde{h}_L$.*

In the first section, we give some basic facts about the ring class fields. In the second section, we give the construction of Stark's elliptic units. In the third section, we show that Schoof's algorithm can be extended to the ring class field case and give an example to illustrate the algorithm. At the end, we give the tables promised above.

1. Ring Class Fields

Let K be an imaginary quadratic field with class number one. Baker [1], Heegner [3] and Stark [7] proved that there are only nine such fields. The discriminants d_K of these fields are given by

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

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.

Let p be a prime not dividing $6d_K$. Let $I_K(p)$ be the set of all fractional $\mathcal{O}_K$-ideals relatively prime to p. Let $P_{K,1}(p)$ be the subgroup of $I_K(p)$ of all principal ideals (α) with $\alpha \equiv 1 \pmod{(p)}$. This is the principal ray class modulo (p) and we have the ray class group $G = I_K(p)/P_{K,1}(p)$. If J is a subgroup of G, we let $K(J)$ denote the class field of K corresponding to G/J. If $J = \{1\}$, then we obtain the ray class field $K_{(p)}$.

The ring class field $L = K(j(\mathcal{O}))$ can be obtained by class field theory as well. By definition, the congruence subgroup $P_{K,\mathbf{Z}}(p)$ is generated by principal ideals of the form (α), where the algebraic integer α satisfies $\alpha \equiv a \pmod{(p)}$ for some integer a relatively prime to p. If $J = P_{K,\mathbf{Z}}(p)/P_{K,1}(p)$,

then the class field $L = K(J)$ is the ring class field of conductor p. The Galois group $\mathrm{Gal}(L/K)$ is isomorphic to $I_K(p)/P_{K,\mathbf{Z}}(p)$ and its order is given by

$$n = \begin{cases} 2(p-1)/W & \text{if } p \text{ is split,} \\ 2(p+1)/W & \text{if } p \text{ is inert} \end{cases}$$

where W is the number of roots of unity in K. See [2, 7.24]. The number field L is a Galois extension of $\mathbf{Q}$ and its Galois group can be written as a semi-direct product

$$\mathrm{Gal}(L/\mathbf{Q}) \cong \mathrm{Gal}(L/K) \rtimes \mathrm{Gal}(K/\mathbf{Q}),$$

where the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathrm{Gal}(L/K)$ by sending any automorphism to its inverse [2, 9.3]. The construction of elliptic units relies on the norm maps $N_{K_{(p)}/L}$. Next we write these norm maps explicitly for both the split and inert case.

1.1. **Split Case.** Let $\mathfrak{p} \subset K$ be a degree one prime ideal of norm p not dividing $6d_K$. Denote its conjugate by $\bar{\mathfrak{p}}$. Define $w_{\mathfrak{p}}$ to be an integer satisfying the congruence $w \equiv w_{\mathfrak{p}} \pmod{\mathfrak{p}}$. The map

$$\psi : xw + y \longmapsto (xw_{\mathfrak{p}} + y, xw_{\bar{\mathfrak{p}}} + y)$$

gives a surjective homomorphism from $\mathcal{O}_K$ onto $\mathbf{F}_p^2$ with $\mathrm{Ker}(\psi) = (p)$. Two elements in $\mathcal{O}_K$ generate the same ideal only if they differ by a unit. Hence we can construct a well-defined map

$$\begin{aligned} \widehat{\psi} : \quad I_K(p) \quad &\longrightarrow (\mathbf{F}_p^*)^2/\psi(\mathcal{O}_K^*) \\ (xw+y) \quad &\longmapsto (xw_{\mathfrak{p}} + y, xw_{\bar{\mathfrak{p}}} + y). \end{aligned}$$

One can show that $\widehat{\psi}$ is a homomorphism with $\mathrm{Ker}(\widehat{\psi}) = P_{K,1}(p)$. The Galois group of $K_{(p)}/K$ is isomorphic to $(\mathbf{F}_p^*)^2/\psi(\mathcal{O}_K^*)$ by class field theory. Let g be a primitive root modulo p. By Chebotarev's density theorem, we can pick a prime ideal $\mathfrak{q}$, not dividing $6pd_K$, with the property $\widehat{\psi}(\mathfrak{q}) = (g, g)$. Set $\sigma = \sigma_{\mathfrak{q}}$. Since $[K_{(p)} : L] = (p-1)/2$, the norm of an element α from $K_{(p)}$ to L is given by

$$N_{K_{(p)}/L}(\alpha) = \prod_{i=1}^{(p-1)/2} \sigma^i(\alpha).$$

Observe that $\mathrm{Gal}(L/K) = \{\sigma_{\mathfrak{q}} : \widehat{\psi}(\mathfrak{q}) = (1, i)\}$. It follows that $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of $\mathbf{F}_p^*$ and is therefore cyclic.

1.2. **Inert Case.** Let $(p) \subset K$ be a degree two prime ideal not dividing $6d_K$. Then $\mathcal{O}_K/(p) \cong \mathbf{F}_{p^2}$. Similar to the split case, we have a surjective homomorphism

$$\begin{aligned} \widehat{\psi}: \quad I_K(p) \quad &\longrightarrow \mathbf{F}_{p^2}^*/\psi(\mathcal{O}_K^*) \\ (xw+y) \quad &\longmapsto xw+y. \end{aligned}$$

with $\mathrm{Ker}(\widehat{\psi}) = P_{K,1}(p)$. The Galois group of $K_{(p)}/K$ is isomorphic to $\mathbf{F}_{p^2}^*/\psi(\mathcal{O}_K^*)$, a cyclic group of order $(p^2-1)/W$. Let $\sigma \in \mathrm{Gal}(K_{(p)}/K)$ be a generator. Recall that $n = [L:K] = 2(p+1)/W$. The norm of an element α from $K_{(p)}$ to L is given by

$$N_{K_{(p)}/L}(\alpha) = \prod_{i=1}^{(p-1)/2} \sigma^{ni}(\alpha).$$

It is obvious that $\mathrm{Gal}(L/K)$ is cyclic and generated by $\sigma|_L$.

We finish this section by giving a corollary of the fact that $\mathrm{Gal}(L/\mathbf{Q})$ is a generalized dihedral group.

Corollary 1.1. *Let K be an imaginary quadratic field with class number one and let L be the ring class field of conductor p. If p is a prime not dividing $6d_K$ and $p^* = (\frac{-1}{p})p$ then for any m-th root of unity ζ_m,*

$$L \cap K(\zeta_m) = \begin{cases} K(\sqrt{p^*}) & \text{if } p|m, \\ K & \text{otherwise.} \end{cases}$$

Proof. It is a well known fact that ζ_p is contained in the ray class field $K_{(p)}$. We see that $[K_{(p)}:L] = (p-1)/2$ when we compute the norm map $N_{K_{(p)}/L}$. The unique degree 2 subfield of the p-th cyclotomic field $\mathbf{Q}(\zeta_p)$ is given by $\mathbf{Q}(\sqrt{p^*})$. Therefore $L \supset K(\sqrt{p^*})$.

Let $F = L \cap K(\zeta_m)$ and assume that $F \supsetneq K$. The number field F is Abelian over $\mathbf{Q}$, since $F \subset K(\zeta_m)$. The action of the complex conjugation is trivial on $\mathrm{Gal}(F/K)$ only if $[F:K] = 2$. Therefore

$$\mathrm{Gal}(F/\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}).$$

There exists $\alpha \in F$ such that $F = K(\alpha)$ and $\alpha^2 \in K$. Since $\mathrm{Gal}(F/\mathbf{Q})$ is not cyclic we can assume $\alpha^2 \in \mathbf{Q}$. The extension F/K is ramified only above p. Since $F \supseteq K(\sqrt{p^*}) \supseteq K$ and $[F:K] = 2$, this finishes the proof. □

2. Elliptic Units

We fix a $\mathbf{Z}$-basis $[pw, p]$ for the ideal $(p) \subset \mathcal{O}_K$. We can consider w as a complex number and assume that the imaginary part of $w = pw/p$ is positive. Let $\mathfrak{c}$ be an element of the ray class group G of conductor (p) and let (α) be an integral ideal in $\mathfrak{c}$. We may write $\alpha = p(uw+v)$ where u and

v are rational and indeed pu and pv are integral. Given a complex number z, with positive imaginary part, define $\gamma = uz + v$. Let $\phi(u, v, z)$ be the function on the upper half plane defined by the infinite product

$$\phi(u,v,z) = \xi(u,v,z) \prod_{m=1}^{\infty} \left(1 - e^{2\pi i(mz+\gamma)}\right)\left(1 - e^{2\pi i(mz-\gamma)}\right) \tag{2.1}$$

where $\xi(u, v, z) = -ie^{\pi iz/6}e^{\pi iu\gamma}(e^{\pi i\gamma} - e^{-\pi i\gamma})$. It satisfies the following transformation properties which follow from Kronecker's second limit formula [6, pp. 207-208]:

$$\begin{aligned}
\phi(u, v+1, z) &= -e^{\pi iu}\phi(u, v, z),\\
\phi(u+1, v, z) &= -e^{-\pi iv}\phi(u, v, z),\\
\phi(u, v, z+1) &= e^{\pi i/6}\phi(u, u+v, z),\\
\phi(u, v, -1/z) &= e^{-\pi i/2}\phi(v, -u, z).
\end{aligned}$$

One can easily see that the function $\phi(u, v, z)$ is invariant under the action of $\Gamma(12p^2)$ and is modular of level $12p^2$. By [6, Lemma 7], the elements $\phi(u, v, w)^{12p}$ depend only upon $\mathfrak{c}$ and we define $E(\mathfrak{c}) = \phi(u, v, w)^{12p}$. If J is a subgroup of G, set $E(\mathfrak{c}') = \prod_{\mathfrak{c}\in\mathfrak{c}'} E(\mathfrak{c})$ for any coset $\mathfrak{c}'$ of J. For the reader's convenience, we state [6, Theorem 2] specialized to our case.

Theorem 2.1. *Let G be the ray class group of conductor (p) and let J be a subgroup G. There is an algebraic integer $\pi(\mathfrak{c}')$ in the class field $K(J)$ such that $\pi(\mathfrak{c}')^{12p} = E(\mathfrak{c}')^W$. If χ is a ray class character modulo (p) with $\chi(J) = 1$, then*

$$L'(0,\chi) = -\frac{1}{W}\sum_{\mathfrak{c}'\in G/J} \chi(\mathfrak{c}')\log(|\pi(\mathfrak{c}')|^2).$$

The explicit reciprocity law is given by $\pi(J)^{N(\mathfrak{q})} \equiv \pi(\mathfrak{c}') \pmod{\mathfrak{q}}$ where $\mathfrak{q}$ is a prime ideal in $\mathfrak{c}'$. Moreover $\pi(J)^{1/W}$ generates an Abelian extension of K.

Now we consider the elliptic units in the ring class field L. Suppose that $J = P_{K,\mathbf{Z}}(p)/P_{K,1}(p)$. Then the class field $K(J)$ is the ring class field L of K of conductor p. If p is inert in K, then the elements $\pi(\mathfrak{c}')$ are of norm p^2 over $\mathbf{Q}$. See [6, Theorem 1]. There is a unique prime ideal $\mathfrak{P} \subset \mathcal{O}_L$ above (p) and generated by any of the $\pi(\mathfrak{c}')$'s. Thus the quotient of any two $\pi(\mathfrak{c}')$'s is a unit. If p is split, then the elements $\pi(\mathfrak{c}')$ (and therefore their quotients) are units [6, Theorem 1].

The norm of any prime ideal of K, not dividing $6d_K$, is congruent to 1 modulo W (including the cases $W = 4$ and $W = 6$). Therefore the quotient of any two $\pi(\mathfrak{c}')$'s is the W-th power of an element in L by [6, Theorem 1].

We set

$$\frac{\pi(\mathfrak{c}')}{\pi(J)} = \epsilon_{\mathfrak{c}'}^{W}.$$

Let $G_L = \mathrm{Gal}(L/K)$ be the Galois group of the extension L/K. Let σ be a generator of G_L and let $\pi(\mathfrak{c}') = \sigma(\pi(J))$ for some coset $\mathfrak{c}'$ of J. The *group of elliptic units*, denoted by $\mathcal{E}$, is the multiplicative G_L-module generated by a unit $\epsilon = \epsilon_{\mathfrak{c}'}$ together with the W roots of unity in K. The group $\mathcal{E}$ does not depend on the choice of $\mathfrak{c}'$. Moreover the index of $\mathcal{E}$ in the full unit group is finite and equals to the class number of L. In fact we have something stronger.

Theorem 2.2. *Let H be a subgroup of G_L. Then $\#\mathrm{Cl}(L^H) = [\mathcal{O}_L^{*\,H} : \mathcal{E}^H]$.*

Proof. This is a generalization of Stark's proof for the ray class fields of K of a degree one prime conductor [6, p.229]. The proof of this theorem can be adapted from [4, Theorem 2.1]. We only need to see that any non-trivial ray class character with $\chi(J) = 1$ is primitive of conductor (p). This is trivially true if p is inert. Assume otherwise and let $\mathfrak{p}$ be a split prime of K of norm p. The ray class fields $K_{\mathfrak{p}}$ and $K_{\bar{\mathfrak{p}}} = \overline{K_{\mathfrak{p}}}$ have trivial intersection K. It follows that $L \cap K_{\mathfrak{p}} = K$. Therefore any non-trivial character χ of the ring class field L have conductor (p). □

The group ring $\mathbf{Z}[G_L]$ is a free $\mathbf{Z}$-module of rank $n = [L : K]$. The G_L-homomorphism $\mathbf{Z}[G_L] \to \mathcal{E}$ given by $x \mapsto \epsilon^x$ induces an isomorphism of Galois modules

$$\mathcal{E}/\mathcal{O}_K^* \cong \mathbf{Z}[G_L]/(N_{L/K}) \tag{2.2}$$

where $N_{L/K} = 1 + \sigma + \ldots + \sigma^{n-1}$. Consider

$$\psi = 1 + 2\sigma + \ldots + n\sigma^{n-1} \in \mathbf{Z}[G_L]$$

and set $\eta = \epsilon^{\psi}$. We claim that the unit η is not a power of another element in $\mathcal{E}$. To see this, assume $\eta = (\epsilon^{\varphi})^m$ for some $\varphi \in \mathbf{Z}[G_L]$ and some integer $m > 1$. It follows that $\psi - m\varphi$ is a multiple of the norm map by (2.2). This gives us a contradiction since ψ is not trivial in $(\mathbf{Z}/m\mathbf{Z})[G_L]/(N_{L/K})$.

We can use this fact to show an interesting divisibility property of the class number h_L in the split case.

Corollary 2.3. *Let p be a prime which splits in K and let L be the corresponding ring class field. Then $[L : K]/W$ divides h_L.*

Proof. If p splits in K then the element $\pi(J)$ is a unit by [6, Theorem 1]. We have

$$\left(\epsilon^W\right)^{\psi} = \frac{\pi(J)^n}{N_{L/K}(\pi(J))}. \tag{2.3}$$

The norm of $\pi(J)$ is a unit in K and therefore $\pi(J)^n = \eta^W \zeta_W^a$ for some integer a. Since η is not a power of another element in $\mathcal{E}$, we conclude by Theorem 2.2 that $[L:K]/W$ divides h_L. □

For the split case we have found that $[L:K]/2$ divides h_L experimentally. However we do not have a proof for this.

This corollary enables us to construct ring class fields with class number divisible by any prescribed integer.

Corollary 2.4. *For any integer $m > 0$ and each imaginary quadratic field K of class number one, there exists infinitely many ring class fields L of K with class number h_L divisible by m.*

Proof. Consider the ray class field $K_{(mW^2)}$. By Chebotarev's density theorem, there are infinitely many primes which totally split in this extension. Any such prime p satisfies the congruence $p \equiv 1 \pmod{mW^2}$. The ring class field L of K of conductor p has class number h_L divisible by m. □

2.1. **Computing the elliptic units.** In this section we explain how to compute Stark's elliptic units with required precision. We start our discussion by recalling some fundamental facts about modular functions. A function $f(z)$ on the upper half plane is called a modular function of level N if it is preserved under the action of $\Gamma(N)$. Let $\mathcal{F}_N$ be the field of all such functions whose q-expansions at every cusp have coefficients in $\mathbf{Q}(\zeta_N)$. It is a well known fact that

$$\mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1) \cong \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})/\pm I.$$

See [6, § 4] for a proof. The action of this Galois group on $\mathcal{F}_N$ can be described easily. If $\det(A) = 1$, then $f(z) \circ A = f(Az)$, and if $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, then the corresponding automorphism is induced by $\zeta_N \mapsto \zeta_N^d$.

Let u and v be elements in $(1/p)\mathbf{Z}$. Then $f(z) = \phi(u, v, z)$ is a modular function of level $N = 12p^2$, thanks to the transformation properties. Stark provides us with a Shimura type reciprocity law [6, Theorem 3] which states that $\phi(u, v, w)$ is an element of the ray class field $K_{(12p^2)}$, and

$$\phi(u, v, w)^{\sigma_{\mathfrak{q}}} = \left[\phi(u, v, z) \circ (qB^{-1})\right]_{z=Bw}. \tag{2.4}$$

Here $\sigma_{\mathfrak{q}}$ is the Frobenius automorphism attached to the degree one prime ideal $\mathfrak{q} = (x_{\mathfrak{q}} w + y_{\mathfrak{q}})$ of norm q, not dividing $6pd_K$. By definition, it satisfies

the congruence

$$\alpha^{\sigma_{\mathfrak{q}}} \equiv \alpha^q \pmod{\mathfrak{q}}$$

for all integers α in $K_{(12p^2)}$. In particular $\zeta^{\sigma_{\mathfrak{q}}} = \zeta^q$ for any root of unity. Pick $x_{\bar{\mathfrak{q}}} = x_{\mathfrak{q}}$ and

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

Then the conjugate of $\mathfrak{q}$ is given by $\bar{\mathfrak{q}} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})$. The integral matrix B is defined by $B\binom{pw}{p} = (x_{\bar{\mathfrak{q}}} w + y_{\bar{\mathfrak{q}}})\binom{pw}{p}$. Note that $B\binom{pw}{p} = \binom{\mu}{\nu}$ is a $\mathbf{Z}$-basis for $\bar{\mathfrak{q}}(p) \subset \mathcal{O}_K$ and $\mu/\nu = w$. One can find that

$$B = \begin{bmatrix} -y_{\mathfrak{q}} & -N_{K/\mathbf{Q}}(w) x_{\mathfrak{q}} \\ x_{\mathfrak{q}} & y_{\bar{\mathfrak{q}}} \end{bmatrix}$$

by comparing the coefficients of w. In order to compute the right hand side of (2.4), we need to find $\phi(u, v, z) \circ (qB^{-1})$ and then plug in $Bw = w$ to the resulting function.

The matrix qB^{-1} is of determinant q and therefore an element of the general linear group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. Observe that $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ is generated by elements $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $M_d = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ where d is an integer coprime to N. The transformation properties of $\phi(u, v, z)$ imply that

$$\begin{aligned} \phi(u, v, z) \circ S &= e^{-\pi i/2} \phi((u, v)S, z), \\ \phi(u, v, z) \circ T &= e^{\pi i/6} \phi((u, v)T, z). \end{aligned}$$

The function $\phi(u, v, z)$ has coefficients in $\mathbf{Q}(\zeta_N)$. The action of M_d on $\phi(u, v, z)$ is induced by the automorphism $\sigma : \zeta_N \mapsto \zeta_N^d$. Each root of unity in the coefficients of $\phi(u, v, z)$ has a single factor of v except $-i$ in the beginning. Note that $\sigma(-i) = -i(-1)^{(d-1)/2}$. Therefore

$$\begin{aligned} \phi(u, v, z) \circ M_d &= (-1)^{(d-1)/2} \phi(u, vd, z) \\ &= (-1)^{(d-1)/2} \phi((u, v)M_d, z). \end{aligned}$$

One can compute $\phi(u, v, z) \circ (qB^{-1})$ by using a decomposition of qB^{-1} in terms of T, S and M_d.

The integral ideal $(1) \subset \mathcal{O}_K$ is in J, so we write $1 = (0, 1/p)\binom{pw}{p}$. Let $u_1 = 0$ and $v_1 = 1/p$. The element $\pi(J)$ of Theorem 2.1 is of the form

$$\pi(J) = \left(\prod_{i=1}^{(p-1)/2} \phi(u_i, v_i, w)^W \right) \zeta_{12}^s \zeta_p^t$$

where $u_i, v_i \in (1/p)\mathbf{Z}$ can be determined by the explicit norm map and reciprocity law. We can assume that $q \equiv 1 \pmod{12}$ since $L \cap K(\zeta_{12}) = K$.

If $\mathfrak{q}$ is in $\mathfrak{c}'$, then

$$\epsilon^W = \pi(J)^{\sigma_\mathfrak{q}-1} = \left(\prod_{i=1}^{(p-1)/2} \phi(u_i, v_i, w)^W\right)^{\sigma_\mathfrak{q}-1} \zeta_p^{t(q-1)}.$$

The field K contains the W-th roots of unity. This allows us to take W-th root of elements within the field $L \supset K$ and we obtain

$$\epsilon = \left(\prod_{i=1}^{(p-1)/2} \phi(u_i, v_i, w)^{\sigma_\mathfrak{q}-1}\right) \zeta_p^{t(q-1)/W}.$$

Note that $t(q-1)/W$ is well-defined modulo p since $p \nmid W$. We pick an automorphism τ of $K_{(12p^2)}$ which acts trivially on ϵ but non-trivially on ζ_p. This is possible because $L \cap K(\zeta_p) = K(\sqrt{p^*})$. Computing $\epsilon^{\tau-1}$, one easily obtains the integer $t(q-1)/W$ modulo p. Observe that the conjugates $\sigma^i(\epsilon)$ can be found in this fashion as well.

In order to compute the elliptic units, we need to compute $\phi(u, v, w)$. The function ϕ is given by an infinite product (2.1). Now we find the number terms that is enough to compute $\phi(u, v, w)$ with required precision.

Lemma 2.5. *Let u, v be real numbers and $\gamma = uz+v$. Suppose that $|u| \leq 1$. For all integer $M \geq 1$, we have the following bounds*

$$e^{B(M)} > \prod_{m=M+1}^{\infty} |1 - e^{2\pi i(mz+\gamma)}| > e^{-B(M)}$$

where $B(M) = |q_z|^M/((1-|q_z|)(1-|q_z|^M))$ and $q_z = e^{2\pi iz}$.

Proof. We start by taking the logarithm

$$\log \prod_{m=M+1}^{\infty} |1 - e^{2\pi i(mz+\gamma)}| = \sum_{m=M+1}^{\infty} \log|1 - e^{2\pi i(mz+\gamma)}|.$$

Then we use the inequality $|1 - e^{2\pi i(mz+\gamma)}| > 1 - |q_z|^{m+u}$ and the Taylor series expansion $\log(1-x) = -\sum \frac{x^n}{n}$ to get

$$\begin{aligned}
\sum_{m=M+1}^{\infty} \log|1 - e^{2\pi i(mz+\gamma)}| &> \sum_{m=M+1}^{\infty} \log(1 - |q_z|^{m+u}) \\
&> \sum_{m=M+1}^{\infty} \log(1 - |q_z|^{m-1}) \\
&= -\sum_{m=M}^{\infty} \sum_{n=1}^{\infty} \frac{|q_z|^{mn}}{n}.
\end{aligned}$$

Rearranging the terms and applying the summation formula for geometric series twice, we obtain

$$\begin{aligned} -\sum_{m=M}^{\infty}\sum_{n=1}^{\infty}\frac{|q_z|^{mn}}{n} &= -\sum_{n=1}^{\infty}\frac{1}{n}\frac{|q_z|^{nM}}{1-|q_z|^n} \\ &> -\sum_{n=1}^{\infty}\frac{|q_z|^{nM}}{1-|q_z|} = -B(M). \end{aligned}$$

This finishes the proof of the bound on the right hand side. The proof for the other side is similar. □

The transformation properties of ϕ enable us to pick $0 \leq u, v < 1$ to compute $\phi(u, v, w)$. We use the first M terms in the infinite product (2.1) for an approximation and the corresponding error is

$$E(M) = \left| \prod_{m=M+1}^{\infty} \left(1 - e^{2\pi i(mz+\gamma)}\right)\left(1 - e^{2\pi i(mz-\gamma)}\right) \right|$$

with $z = w$. Lemma 2.5 implies that $e^{2B(M)} > E(M) > e^{-2B(M)}$. It follows that $E(M) = 1 + O(|e^{2\pi iw}|^M)$. The imaginary part of w is $\sqrt{|d_K|}/2$ and therefore $|e^{2\pi iw}| = e^{-\pi\sqrt{|d_K|}/2}$. An easy computation gives that we should pick $M \approx (N \log 10)/(\pi\sqrt{|d_K|})$ for accurate values of $\phi(u, v, w)$ at least N decimal places.

3. Schoof's algorithm

Let $\mathbf{Q}_{(p)} = \mathbf{Q}(\zeta_p + \zeta_p^{-1})$ be the p-th real cyclotomic field. It is a well known fact that the subgroup of cyclotomic units, denoted by $\mathcal{C}$, is of finite index in the full unit group of $\mathbf{Q}_{(p)}$. Moreover this index is precisely the class number of $\mathbf{Q}_{(p)}$. Using this fact, Schoof [5] introduces an algorithm to heuristically compute the class numbers $h_{\mathbf{Q}_{(p)}}$ for primes $p < 10,000$.

Schoof's algorithm consists of three steps and investigates the Jordan-Hölder factors of Galois module $B_{\mathbf{Q}_{(p)}} = \mathcal{O}^*_{\mathbf{Q}_{(p)}}/\mathcal{C}$ of given size l^f where l is prime. Step 1 terminates very fast if such a Jordan-Hölder factor does not appear. If the first step does not terminate after several trials, for example after 10 trials, then we believe that there is such a factor and proceed to the following steps. In Step 2, we check how many Jordan-Hölder factors of size l^f may appear. It provides us with a surjective homomorphism which we believe to be an isomorphism. In Step 3, we *prove* that this map is actually an isomorphism by finding polynomials with coefficients that are very close to integers. Once we verify the isomorphism, we can find the corresponding part of the class number.

Let K be an imaginary quadratic field with class number one and let p be a prime not dividing $6d_K$. Let L be the ring class field of conductor p with Galois group $G_L = \mathrm{Gal}(L/K)$. Following Schoof, we use the $\mathbf{Z}[G_L]$-module $B_L = \mathcal{O}_L^*/\mathcal{E}$ in order to investigate the class number h_L. For this purpose, we need a lemma first.

Lemma 3.1. *Let M be a power of a prime l and $F = L(\zeta_{WM})$. Then the natural map*

$$\mathcal{O}_L^*/\mathcal{O}_K^*(\mathcal{O}_L^*)^M \longrightarrow F^*/(F^*)^M$$

is injective.

Proof. This is the ring class field analogue of [5, Lemma 2.1]. The map is well defined since any trivial element in the first quotient is mapped to a trivial element.

The number field F is the compositum of two Abelian extensions of K, hence Abelian over K. In order to prove our lemma, we need to be careful with $L \cap \mathbf{Q}(\zeta_{2M})$. Observe that, by Corollary 1.1, there are three possibilities for this intersection: $\mathbf{Q}$, K or $\mathbf{Q}(\sqrt{p^*})$. The proof for the first two cases can be adapted from its ray class field analogue [4, Lemma 2.3].

Now suppose that $L \cap \mathbf{Q}(\zeta_{2M}) = \mathbf{Q}(\sqrt{p^*})$. Then M must be a power of p. Recall that p is a prime not dividing $6d_K$, so $(W, M) = 1$. The field $F = L(\zeta_{WM}) = L(\zeta_M)$ is a cyclic extension of L. Let g be a primitive root modulo M. The Galois group $\Delta = \mathrm{Gal}(F/L)$ is generated by σ^2 where $\sigma : \zeta_M \mapsto \zeta_M^g$. Suppose that $x \in \mathcal{O}_L^*$ is in the kernel of the natural map in the corollary. Then $x = y^M$ for some $y \in \mathcal{O}_F^*$. There exists an integer c such that $\sigma^2(y) = y\zeta_M^c$. Note that $g^2 - 1 \not\equiv 0 \pmod{M}$ since p is coprime to 6. Let $d \equiv -c/(g^2-1) \pmod{M}$. Pick $\tilde{y} = y\zeta_M^d$. It follows that $\sigma^2(\tilde{y}) = \sigma^2(y)\zeta_M^{g^2 d} = \tilde{y}$. The element $\tilde{y}$ belongs to $\mathcal{O}_L^*$ since it is invariant under σ^2. Now $x = \tilde{y}^M$ and therefore the map is injective. □

Let R be the group ring $(\mathbf{Z}/M\mathbf{Z})[G_L]$ where $M > 1$ is a power of a prime l. For any R-module A, define the additive group

$$A^\perp = \mathrm{Hom}_R(A, R)$$

as an R-module via $(\lambda f)(a) = \lambda f(a) = f(\lambda a)$ for $\lambda \in R$ and $a \in A$. If A is finite and R is a finite Gorenstein ring, then it is Jordan-Hölder isomorphic to $A^\perp$. See [5, Proposition 1.2].

The lemma above enables us to identify the group $\mathcal{O}_L^*/\mathcal{O}_K^*(\mathcal{O}_L^*)^M$ with a subgroup of $F^*/(F^*)^M$. The field $F = L(\zeta_{WM})$ contains μ_M, the group of

M-th roots of unity. Therefore we have

$$\mathrm{Gal}\left(F\left(\sqrt[M]{\mathcal{O}_L^*}\right)/F\right) \cong \mathrm{Hom}_{\mathbf{Z}}\left(\mathcal{O}_L^*/\mathcal{O}_K^*, \mu_M\right). \tag{3.1}$$

by Kummer theory. Let $\mathcal{R}$ be an unramified degree one prime ideal of F. For each Frobenius automorphism $\tau_{\mathcal{R}} \in \mathrm{Gal}(F(\sqrt[M]{\mathcal{O}_L^*})/F)$, we attach an element $f_{\mathcal{R}}(\epsilon) = \sum c_\sigma \sigma$ in the group ring $R = (\mathbf{Z}/M\mathbf{Z})[G_L]$, whose coefficients c_σ are determined by

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

This correspondence gives us an isomorphism

$$B_L[M]^\perp \cong I/\{f_{\mathcal{R}}(\epsilon) : \mathcal{R} \in S\}$$

where I is the augmentation ideal of R and S is the set of unramified prime ideals $\mathcal{R}$ of $F = L(\zeta_{WM})$ of degree one. See [4, Theorem 2.4] for the details of this isomorphism.

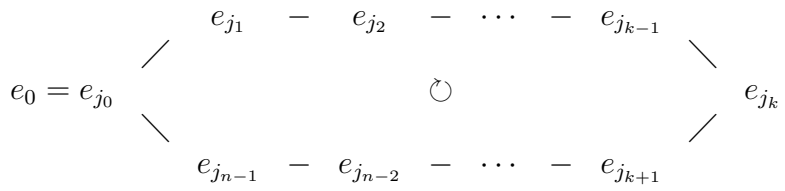
In order to construct prime ideals $\mathcal{R}$, we find degree one prime ideals $\mathfrak{r} \subset \mathcal{O}_K$ with norm $r \equiv 1 \pmod{WM}$ such that $\mathfrak{r}$ is trivial in the ray class group G/J. These two conditions imply that $\mathfrak{r}$ totally splits in F.

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

Let σ be a generator of G_L. The minimal polynomials of ϵ and $\epsilon\sigma(\epsilon)$ over K, say $P_\epsilon(x)$ and $P_{\epsilon\sigma(\epsilon)}(x)$ respectively, can be factored into linear factors in $\mathbf{Q}_r$. Suppose that

$$P_\epsilon(x) = \prod_{i=0}^{n-1}(x - e_i) \quad \text{and} \quad P_{\epsilon\sigma(\epsilon)}(x) = \prod_{i=0}^{n-1}(x - h_i)$$

where e_i's and h_i's are in $\mathbf{Q}_r$. There exists an integer $1 \le i \le n-1$ such that $e_0 e_i \in \{h_0, h_1, \ldots, h_{n-1}\}$. Indeed there are exactly two such i's. We find adjacent e_i's in each case and obtain a cyclic graph with n vertices. Moreover we can determine the direction of our graph by using the minimal polynomial of $\epsilon\sigma(\epsilon)\sigma^3(\epsilon)$. Finally we obtain the directed graph



with the property that the integer value $\sigma^i(\epsilon) \pmod{\mathcal{R}}$ is given by $e_{j_i} \pmod{r}$ for all $0 \le i \le n-1$. See [4, § 2] for details.

We use polynomial notation by replacing σ, a generator of G_L, with X and regard $f_{\mathcal{R}}(\epsilon)$ as an element of $(\mathbf{Z}/M\mathbf{Z})[X]/(X^n - 1)$. Given a prime l, we

apply the first step of Schoof's algorithm and find all Jordan-Hölder factors divisible by l simultaneously. Note that we expect to receive Jordan-Hölder factors of degree one, unlike the previous cases. For instance, a prime divisor $l > 3$ of n gives us $\varphi = X - 1$ for the first step of the algorithm. Observe that

$$\overline{\psi} = -(X-1)^{l-2} = 1 + 2X + \ldots + (l-1)X^{l-2} \in (\mathbf{Z}/l\mathbf{Z})[X].$$

Let F be the intermediate field $K \subset F \subset L$ such that $[F : K] = l$. If L is a ring class field corresponding a split prime, then $N_{L/F}(\epsilon)^{\overline{\psi}}$ is an l-th power of another unit in $\mathcal{O}_F^*$ which does not belong $\mathcal{E}$ (see Corollary 2.3).

Since B_L is a finite $\mathbf{Z}[G_L]$-module, it admits a Jordan-Hölder filtration whose simple factors are one-dimensional vector spaces over the residue fields (see Schoof [5, Section 3] for details). The first step of the algorithm gives an irreducible factor φ of $X^n - 1 \in (\mathbf{Z}/l\mathbf{Z})[X]$ which corresponds to the residue field of a simple Jordan-Hölder factor. Let f be the degree of φ. The *order* of this 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 .

Following Schoof, we introduce a new variable for simpler computations in the second step. Pick $T = X^d - 1$ as in Iwasawa theory so that the maximal ideal of the local ring $\mathbf{Z}_l[X]/\varphi(X^{l^a})$ is of the form (T, l) where l^a is the l-part of n. Now we give an example to illustrate the algorithm and a difficulty we have encountered.

Example 3.2. Let $d_K = -43$ and $p = 193$. The degree of the ring class field L over K is $n = 2^6 \cdot 3$. Applying the first step of Schoof's algorithm we find several irreducible polynomials φ for $l = 2, 3, 13$. Set $\zeta = X^{64}$, a cube root of unity modulo $X^n - 1$. For each φ from the first step, we obtain corresponding ideals $J \subset R$ from the second step of the algorithm:

l	φ	d	J	M
2	$X - 1$	1	$(T^6 + 4T^3 + 32T, 2T^4 + 4T^2, 8T^2, 64T)$	64
2	$X^2 + X + 1$	3	$(T^2 + (4\zeta + 4)T + 4\zeta + 6, 8)$	8
3	$X - 1$	1	$(3T)$	3
13	$X + 2$	12	(13)	13
13	$X + 7$	12	(13)	13

We suspect that $(B_L^{\perp})_{\varphi}$ is isomorphic to $(\mathbf{Z}/M\mathbf{Z})[T]/J$. In order to verify this, we use the third step of Schoof's algorithm with r-adic integers. Let r be a rational prime, not congruent to 1 modulo l, which splits totally in L. We embed our field L into r-adic integers $\mathbf{Q}_r$ and compute the unique M-th roots of certain elliptic units (see [4, Example 2.9]). However there may not exist such a prime r for some cases: $l = 2$ or $l = 3, W = 6$. Dropping the condition $r \not\equiv 1 \pmod{l}$ would result in ambiguities while computing M-th roots. For example, in our case $(l = 2, \varphi = x - 1)$ there are 2^{64} different possibilities for the 64-th roots of certain elliptic units. For such cases, we

only perform the second step of the algorithm but with a very large number of $f_{\mathcal{R}}(\epsilon)$.

The third step of Schoof's algorithm *shows* that the class number h_L is divisible by $2^{14} \cdot 4^6 \cdot 3^2 \cdot 13^2$ (more than a hundred billion). In order to determine how many Jordan-Hölder factors appear in each level, we lift $f_{\mathcal{R}}(\epsilon)$ to rings $R = (\mathbf{Z}/M\mathbf{Z})[X]/\varphi(X^{l^b})$ for $0 \leq b \leq a$. Let $l = 2$ and $\varphi = X - 1$, then we have the following table:

b	d	J	$\lvert R/J \rvert$
1	2	$(8T)$	2^3
2	4	$(4T^2, 8T)$	2^7
3	8	$(T^6 + 4T^3, 2T^4 + 4T^2, 8T)$	2^{11}
4	16	$(T^6 + 4T^3, 2T^4 + 4T^2, 8T^2, 16T)$	2^{12}
5	32	$(T^6 + 4T^3, 2T^4 + 4T^2, 8T^2, 32T)$	2^{13}
6	64	$(T^6 + 4T^3 + 32T, 2T^4 + 4T^2, 8T^2, 64T)$	2^{14}

Let H be a subgroup of $G_L = \mathrm{Gal}(L/K)$ and $F = L^H$ be the corresponding fixed field. The above table enables us to obtain $\tilde{h}_F$, the order of the submodule of ${\mathcal{O}_L^*}^H/\mathcal{E}^H$ with Jordan-Hölder factors of order divisible by $l < 1000$. By Theorem 2.2, $\tilde{h}_F$ is the product of l-parts of the class number h_F for $l < 1000$.

Let $F = L^H$ be the intermediate field such that $[F : K] = 12$. We conclude that 2^7 contributes to the class number h_F using the table above. A similar check for $l = 2$ and $\varphi = X^2 + X + 1$, shows that 5 copies of Jordan-Hölder factor of order 4 appear at level $d = 12$. Therefore $\tilde{h}_F = 2^7 \cdot 4^5 \cdot 3^2 \cdot 13^2$ (around 200 million).

4. Tables

Our analogue of Schoof's algorithm gives us $\tilde{h}_L$, the order of the submodule of $B_L = \mathcal{O}_L^*/\mathcal{E}$ with Jordan-Hölder factors of order divisible by $l < 1000$. There are 9 imaginary quadratic fields K with class number one. For each ground field K, we have worked with primes $p < 200$ not dividing $6d_K$. Computations were performed with the help of software PARI [8].

In the split case, we have found that the number $\tilde{h}_L$ is divisible by $n/2 = [L : K]/2$ and can be trivial only if $[L : K]$ is 2. There are two such ring class fields ($d_K = -3, p = 7$ and $d_K = -4, p = 5$) and one can easily check that their class number is trivial. On the other hand, we encounter more trivial cases in the inert case.

Ring class fields with trivial $\tilde{h}_L$

$-d_K$	p	$-d_K$	p	$-d_K$	p
3	$5, 7(\text{split}), 11, 17, 41$	8	$5, 7, 29$	43	7
4	$5(\text{split}), 7, 11, 19, 43, 67, 163$	11	$7, 17$	67	11
7	$5, 13, 19, 61$	19	67	163	$7, 19$

The numbers $\tilde{h}_L$ for other ring class fields are listed below. In our tables, we use the same format of the main table in Schoof's paper. The numbers $\tilde{h}_L$ 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 $\tilde{h}_L$ 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 $(B_L^{\perp})_{\varphi}$ modulo $\varphi(X^{l^i})$ are $q^{s_0+...+s_i}$ for $0 \leq i \leq n$.

$d_K = -3$, p split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
13	2	2	79	$5 \cdot 13$	$2, 13$	157	$2^3 \cdot 13$	$2, 13$
19	3	3	97	$2 \cdot 2 \cdot 2 \cdot 2$	$2, 4, 8, 16$	163	$3 \cdot 3 \cdot 3$	$3, 9, 27$
31	$3 \cdot 5$	$2, 5$	103	$5 \cdot 17$	$2, 17$	181	$2 \cdot 3 \cdot 3 \cdot 9 \cdot$	$2, 2, 3, 4,$
37	$2^2 \cdot 3$	$2, 3$	109	$2 \cdot 3 \cdot 3 \cdot$	$2, 2, 3,$		$5^2 \cdot 3^2 \cdot 11 \cdot 11$	$5, 6, 10, 10$
43	7	7		$3^2, \cdot 3$	$6, 9$	193	$2^2 \cdot 2^2 \cdot 2 \cdot 9 \cdot$	$2, 4, 8, 8,$
61	$2^2 \cdot 5^2$	$2, 5$	127	$5 \cdot 3 \cdot 7^2$	$2, 3, 7$		$9 \cdot 2 \cdot 17 \cdot$	$8, 16, 16,$
67	11	11	139	$3 \cdot 23$	$2, 23$		$17 \cdot 2 \cdot 2$	$16, 32, 64$
73	$2 \cdot 3 \cdot 2$	$2, 3, 4$	151	$7 \cdot 5^2 \cdot 5$	$2, 5, 25$	199	$3^2 \cdot 3^3 \cdot 3 \cdot 11$	$2, 3, 6, 11$

$d_K = -4$, p split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
13	3	3	89	$2 \cdot 3 \cdot 2^2 \cdot 11$	$2, 2, 4, 11$	157	$3 \cdot 3 \cdot$	$2, 3,$
17	$2 \cdot 2 \cdot 2$	$2, 4, 8$	97	$2 \cdot 3^2 \cdot 4 \cdot$	$2, 3, 3,$		$25 \cdot 13^2$	$3, 13$
29	$3 \cdot 7$	$2, 7$		$2 \cdot 2 \cdot 49$	$4, 8, 8$	173	$7 \cdot 43$	$2, 43$
37	$3 \cdot 4 \cdot 3$	$3, 3, 9$	101	$7 \cdot 5 \cdot 5$	$2, 5, 25$	181	$5 \cdot 3 \cdot 25 \cdot$	$2, 3, 6,$
41	$2 \cdot 5$	$2, 5$	109	$3 \cdot 3 \cdot 3 \cdot 3$	$2, 3, 9, 27$		$3 \cdot 5^2$	$9, 10$
53	$3 \cdot 13$	$2, 13$	113	$2^2 \cdot 2^5 \cdot 7 \cdot 2^4$	$2, 4, 7, 8$	193	$2, 3, 3,$	$2 \cdot 3^2 \cdot 4 \cdot$
61	$3 \cdot 3 \cdot 5 \cdot 3^2$	$2, 3, 5, 6$	137	$2^2 \cdot 2 \cdot 17 \cdot$	$2, 4, 17,$		$4, 8, 16$	$2 \cdot 2 \cdot 2$
73	$2 \cdot 3 \cdot 2^2 \cdot$	$2, 3, 4,$		10201	34	197	$5 \cdot 7 \cdot 7$	$2, 7, 49$
	$7 \cdot 7 \cdot 3$	$6, 6, 9$	149	$7 \cdot 37$	$2, 37$			

$d_K = -7$, p split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
11	5	5	79	$5 \cdot 3^2 \cdot 4 \cdot$	$2, 3, 3,$	151	$7 \cdot 3 \cdot$	$2, 3,$
23	$3 \cdot 11$	$2, 11$		$4 \cdot 13$	$6, 13$		$5 \cdot 5$	$5, 25$
29	$2 \cdot 7$	$2, 7$	107	$3 \cdot 53$	$2, 53$	163	$3 \cdot 121 \cdot 3 \cdot$	$3, 6, 9,$
37	$2 \cdot 3^2 \cdot 3^2$	$2, 3, 9$	109	$2 \cdot 3 \cdot 3 \cdot 3$	$2, 3, 9, 27$		$3 \cdot 3$	$27, 81$
43	$3 \cdot 7$	$3, 7$	113	$2^4 \cdot 2^2 \cdot 7 \cdot$	$2, 4, 7,$	179	$5 \cdot 89$	$2, 89$
53	$2^2 \cdot 13$	$2, 13$		$2^2 \cdot 2$	$8, 16$	191	$13 \cdot 5 \cdot 19$	$2, 5, 19$
67	$3 \cdot 3 \cdot 25 \cdot$	$2, 3, 3,$	127	$5 \cdot 3^2 \cdot 7 \cdot 3^2$	$2, 3, 7, 9$	193	$2^2 \cdot 3 \cdot 3 \cdot$	$2, 2, 3,$
	$3 \cdot 11$	$6, 11$	137	$2 \cdot 3^2 \cdot$	$2, 2,$		$2^6 \cdot 2 \cdot 2 \cdot$	$4, 8, 16,$
71	$7 \cdot 5 \cdot$	$2, 5,$		$2 \cdot 17^2$	$4, 17$		$2 \cdot 961 \cdot 2$	$32, 32, 64$
	$7 \cdot 7^2$	$7, 14$	149	$2^2 \cdot 37$	$2, 37$	197	$2^3 \cdot 7 \cdot 7$	$2, 7, 49$

$d_K = -8$, p split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
11	5	5	83	$3 \cdot 41$	$2, 41$	139	$3 \cdot 3 \cdot 4 \cdot$	$2, 3, 3,$
17	$2 \cdot 2 \cdot 2$	$2, 4, 8$	89	$2^2 \cdot 2^3 \cdot 11$	$2, 4, 11$		$4 \cdot 23$	$6, 23$
19	$3 \cdot 9$	$3, 9$	97	$2 \cdot 5 \cdot 3 \cdot 2 \cdot$	$2, 2, 3, 4,$	163	$3 \cdot 3 \cdot 3^2 \cdot$	$2, 3, 6,$
41	$2 \cdot 2 \cdot 5$	$2, 4, 5$		$9 \cdot 2 \cdot 9 \cdot 2$	$4, 8, 12, 16$		$3 \cdot 3 \cdot 3$	$9, 27, 81$
43	$3 \cdot 7$	$3, 7$	107	$3 \cdot 53$	$2, 53$	179	$5 \cdot 89$	$2, 89$
59	$3 \cdot 29$	$2, 29$	113	$2^2 \cdot 2^2 \cdot 7 \cdot$	$2, 4, 7,$	193	$2 \cdot 5 \cdot 3 \cdot$	$2, 2, 3,$
67	$3^3 \cdot 11$	$3, 11$		$2 \cdot 2$	$8, 16$		$2 \cdot 25 \cdot 2 \cdot$	$4, 6, 8,$
73	$2^3 \cdot 3 \cdot 2^2 \cdot$	$2, 3, 4,$	131	$5 \cdot 5^2 \cdot 13$	$2, 5, 13$		$2 \cdot 2$	$16, 32$
	$2 \cdot 3$	$8, 9$	137	$2 \cdot 3 \cdot 2 \cdot 17$	$2, 2, 4, 17$			

$d_K = -11,\ p$ split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
5	2	2	89	$2^2 \cdot 2^2 \cdot 2 \cdot 11$	$2, 4, 8, 11$	181	$2^2 \cdot 7 \cdot 3^2 \cdot$	$2, 2, 3,$
23	11	11	97	$2 \cdot 3 \cdot 3 \cdot 2 \cdot$	$2, 2, 3, 4,$		$4^2 \cdot 5 \cdot 4 \cdot$	$3, 5, 6,$
31	$3 \cdot 3 \cdot 5^2$	$2, 3, 5$		$3^4 \cdot 2 \cdot 2$	$6, 8, 16$		$3 \cdot 4$	$9, 12$
37	$2^3 \cdot 3 \cdot 3$	$2, 3, 9$	103	$5 \cdot 3 \cdot 17$	$2, 3, 17$	191	$3 \cdot 13 \cdot$	$2, 2,$
47	$5 \cdot 23$	$2, 23$	113	$2 \cdot 2 \cdot 7 \cdot 2$	$2, 4, 7, 8$		$5 \cdot 19$	$5, 19$
53	$2^2 \cdot 13$	$2, 13$	137	$2 \cdot 2 \cdot 9 \cdot 17$	$2, 4, 4, 17$	199	$3^2 \cdot 3 \cdot 4 \cdot$	$2, 3, 3,$
59	$3 \cdot 29$	$2, 29$	157	$2 \cdot 3^2 \cdot 3^2 \cdot 13$	$2, 2, 3, 13$		$4 \cdot 3 \cdot 11$	$6, 9, 11$
67	$3 \cdot 11$	$3, 11$	163	$3 \cdot 3 \cdot 3 \cdot 3$	$3, 9, 27, 81$			
71	$7 \cdot 5 \cdot 7$	$2, 5, 7$	179	$5 \cdot 89$	$2, 89$			

$d_K = -19,\ p$ split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
5	2^2	2	73	$2 \cdot 3 \cdot 2 \cdot 3$	$2, 3, 4, 9$	163	$3 \cdot 3 \cdot 3 \cdot 3$	$3, 9, 27, 81$
7	3	3	83	$3 \cdot 41$	$2, 41$	191	$13 \cdot 5 \cdot 19$	$2, 5, 19$
11	5	5	101	$2 \cdot 11 \cdot 9 \cdot$	$2, 2, 4,$	197	$2^2 \cdot 7 \cdot 7 \cdot$	$2, 2, 7,$
17	$2 \cdot 2 \cdot 2$	$2, 4, 8$		$5^3 \cdot 5^2$	$5, 25$		$169 \cdot 7$	$14, 49$
23	$3 \cdot 11$	$2, 11$	131	$5 \cdot 5 \cdot 13$	$2, 5, 13$	199	$3^2 \cdot 3^3 \cdot 4 \cdot$	$2, 3, 3,$
43	$5 \cdot 3^2 \cdot 7^2 \cdot$	$2, 3, 7,$	137	$2 \cdot 5 \cdot 2 \cdot 17$	$2, 2, 4, 17$		$4^2 \cdot 3^4 \cdot 11$	$6, 9, 11$
	$29 \cdot 29$	$14, 14$	139	$3 \cdot 3 \cdot 3 \cdot 23$	$2, 3, 6, 23$			
61	$2^3 \cdot 3 \cdot 5 \cdot$	$2, 3, 5,$	149	$2 \cdot 17 \cdot 37$	$2, 2, 37$			
	$31 \cdot 31$	$30, 30$	157	$2 \cdot 5 \cdot 3 \cdot 13$	$2, 2, 3, 13$			

$d_K = -43,\ p$ split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
11	$3 \cdot 5^2$	$2, 5$	83	$3^2 \cdot 41$	$2, 41$	139	$3 \cdot 3 \cdot 3^2 \cdot 23$	$2, 3, 6, 23$
13	$2^3 \cdot 3$	$2, 3$	97	$2^3 \cdot 3^3 \cdot 4 \cdot$	$2, 3, 3,$	167	$11 \cdot 83$	$2, 83$
17	$2 \cdot 3 \cdot 2 \cdot 2$	$2, 2, 4, 8$		$2^3 \cdot 4 \cdot 2^2 \cdot$	$4, 6, 8,$	173	$2 \cdot 29 \cdot 43$	$2, 2, 43$
23	$3 \cdot 11$	$2, 11$		$49 \cdot 2^2 \cdot 2$	$8, 16, 32$	181	$2 \cdot 11 \cdot 3^2 \cdot$	$2, 2, 3,$
31	$3 \cdot 3 \cdot 5$	$2, 3, 5$	101	$2^5 \cdot 5 \cdot 5$	$2, 5, 25$		$5 \cdot 3$	$5, 9$
41	$2 \cdot 3 \cdot 2 \cdot 5$	$2, 2, 4, 5$	103	$5 \cdot 3 \cdot 7 \cdot$	$2, 3, 3,$	193	$2^3 \cdot 3^2 \cdot 4 \cdot 2^4 \cdot$	$2, 3, 3, 4,$
47	$3 \cdot 5 \cdot 23$	$2, 2, 23$		$7 \cdot 17$	$3, 17$		$4 \cdot 2^4 \cdot 4^3 \cdot$	$6, 8, 12,$
53	$2^2 \cdot 7 \cdot 13$	$2, 2, 13$	107	$3 \cdot 53$	$2, 53$		$13 \cdot 13 \cdot 2 \cdot$	$12, 12, 16,$
59	$3 \cdot 29$	$2, 29$	109	$2^3 \cdot 3 \cdot$	$2, 3,$		$4 \cdot 2 \cdot 2$	$24, 32, 64$
67	$3^2 \cdot 4 \cdot$	$3, 3,$		$3 \cdot 3$	$9, 27$	197	$2^3 \cdot 5 \cdot 9 \cdot$	$2, 2, 4,$
	$4 \cdot 11$	$6, 11$	127	$5 \cdot 3 \cdot$	$2, 3,$		$7 \cdot 7$	$7, 49$
79	$5 \cdot 3^2 \cdot 13$	$2, 3, 13$		$7 \cdot 3$	$7, 9$			

$d_K = -67,\ p$ split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
17	$2^3 \cdot 2^2 \cdot$	$2, 4,$	73	$2 \cdot 5 \cdot 3 \cdot$	$2, 2, 3,$	157	$2 \cdot 17 \cdot 3 \cdot 13$	$2, 2, 3, 13$
	$2^2 \cdot 2^2$	$8, 16$		$2 \cdot 3$	$4, 9$	163	$3 \cdot 4^2 \cdot 4 \cdot$	$3, 3, 6,$
19	$3 \cdot 9 \cdot$	$3, 9,$	83	$3 \cdot 41$	$2, 41$		$3 \cdot 3 \cdot 3$	$9, 27, 81$
	$19 \cdot 19$	$18, 18$	89	$2^2 \cdot 3 \cdot$	$2, 2,$	167	$11 \cdot 83$	$2, 83$
23	$3 \cdot 11$	$2, 11$		$2^3 \cdot 11$	$4, 11$	173	$2^3 \cdot 3^2 \cdot 9 \cdot 43$	$2, 2, 4, 43$
29	$2^4 \cdot 7$	$2, 7$	103	$3 \cdot 5 \cdot 3 \cdot$	$2, 2, 3,$	181	$2^2 \cdot 5 \cdot 3 \cdot$	$2, 2, 3,$
37	$2^2 \cdot 3 \cdot 3 \cdot$	$2, 2, 3,$		$4^2 \cdot 3^2 \cdot 17$	$3, 6, 17$		$2 \cdot 5 \cdot 3$	$4, 5, 9$
	$4^3 \cdot 4^2 \cdot 3 \cdot$	$3, 6, 9,$	107	$3 \cdot 53$	$2, 53$	193	$2 \cdot 5 \cdot 3^2 \cdot 2 \cdot$	$2, 2, 3, 4,$
	$19 \cdot 19$	$18, 18$	127	$5 \cdot 3 \cdot 7 \cdot 3$	$2, 3, 7, 9$		$25 \cdot 2 \cdot 2 \cdot 2$	$6, 8, 16, 32$
47	$5 \cdot 23$	$2, 23$	131	$5 \cdot 5 \cdot 13$	$2, 5, 13$	199	$3^3 \cdot 3^6 \cdot 3 \cdot$	$2, 3, 6,$
59	$3 \cdot 29$	$2, 29$	149	$2 \cdot 23 \cdot 37$	$2, 2, 37$		$3 \cdot 11$	$9, 11$
71	$5 \cdot 5 \cdot$	$2, 5,$	151	$7^2 \cdot 3^3 \cdot$	$2, 3,$			
	$7 \cdot 5$	$7, 10$		$5^2 \cdot 5^2$	$5, 25$			

$d_K = -163,\ p$ split

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
41	$2^4 \cdot 2^2 \cdot 5 \cdot$	$2, 4, 5,$	97	$2 \cdot 3^2 \cdot 3 \cdot$	$2, 2, 3,$	173	$2^3 \cdot 3 \cdot$	$2, 2,$
	$2^3 \cdot 49$	$8, 8$		$4 \cdot 2 \cdot 2$	$3, 8, 16$		$5 \cdot 43$	$2, 43$
43	$3 \cdot 7$	$3, 7$	113	$2 \cdot 13 \cdot 2 \cdot$	$2, 2, 4,$	179	$5 \cdot 89$	$2, 89$
47	$5 \cdot 23$	$2, 23$		$7 \cdot 2 \cdot 49$	$7, 8, 8$	197	$2^4 \cdot 7 \cdot$	$2, 2,$
53	$2^2 \cdot 11 \cdot 13$	$2, 2, 13$	131	$5 \cdot 5^2 \cdot 13$	$2, 5, 13$		$7 \cdot 7$	$7, 49$
61	$2^2 \cdot 7 \cdot 3^2 \cdot 5$	$2, 2, 3, 5$	151	$7 \cdot 3 \cdot 4 \cdot$	$2, 3, 3,$	199	$3^2 \cdot 3^2 \cdot 3^2 \cdot$	$2, 3, 6,$
71	$7 \cdot 5 \cdot 7$	$2, 5, 7$		$5 \cdot 4 \cdot 5$	$5, 6, 25$		$3 \cdot 19 \cdot 19 \cdot$	$9, 9, 9,$
83	$3 \cdot 41$	$2, 41$	167	$3^2 \cdot 11 \cdot 83$	$2, 2, 83$		$289 \cdot 11$	$9, 11$

$d_K = -3,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
23	3	2	71	$7 \cdot 9$	$2, 4$	113	3	2	173	3^2	2
29	3	2	83	3	2	131	$5 \cdot 9^2$	$2, 4$	179	$5 \cdot 7 \cdot$	$2, 6,$
47	5	2	89	4	3	137	3	2		$7 \cdot 81$	$6, 10$
53	5	2	101	5	2	149	$7 \cdot 81$	$2, 10$	191	13	2
59	3	2	107	$3^2 \cdot 3^2 \cdot 3$	$2, 6, 18$	167	11	2	197	11	2

$d_K = -4,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
23	$3 \cdot 4$	$2, 3$	71	$7 \cdot 4 \cdot$	$2, 3,$	103	5	2	151	$7 \cdot 9$	$2, 4$
31	3	2		$4 \cdot 4^2$	$6, 12$	107	$3 \cdot 4^2 \cdot$	$2, 3,$	167	$11 \cdot 1681$	$2, 21$
47	5	2	79	$3 \cdot 5 \cdot$	$2, 2,$		4^2	6	179	5	2
59	$3 \cdot 4 \cdot$	$2, 3,$		5^2	10	127	5	2	191	13	2
	$16 \cdot 4$	$5, 6$	83	$3 \cdot 4 \cdot$	$2, 3,$	131	5	2	199	3^2	2
				$4 \cdot 169$	$6, 14$	139	3	2			

$d_K = -7,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
17	5	2	59	$3 \cdot 121$	$2, 12$	101	$3 \cdot 3^2$	$2, 6$	157	3	2
31	3	2	73	7	2	103	5	2	167	$11 \cdot 4 \cdot 4$	$2, 3, 6$
41	7	2	83	$3 \cdot 3^2$	$2, 6$	131	$5 \cdot 25$	$2, 3$	173	7	2
47	$5 \cdot 4 \cdot$	$2, 3,$	89	11	2	139	$2 \cdot 101 \cdot$	$2, 20,$	181	3	2
	$9 \cdot 9$	$4, 12$	97	3^2	2		101	20	199	$3^2 \cdot 5 \cdot 5$	$2, 2, 10$

$d_K = -8,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
13	3	2	61	5	2	109	5	2	173	5	2
23	$3 \cdot 3^2$	2, 6	71	$3 \cdot 7 \cdot 5 \cdot$	2, 2, 4,	127	$3 \cdot 5$	2, 2	181	3	2
31	3	2		$5 \cdot 3^3$	4, 6	149	$3 \cdot 3^2$	2, 6	191	13	2
37	5	2	79	5	2	151	7	2	197	5	2
47	5	2	101	$3 \cdot 4 \cdot 4$	2, 3, 6	157	13	2	199	$3^2 \cdot 9 \cdot 49$	2, 4, 4
53	$3 \cdot 4$	2, 3	103	$5 \cdot 9$	2, 4	167	11	2			

$d_K = -11,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
13	5	2	73	5	2	109	19	2	151	7	2
19	$11 \cdot 11$	10, 10	79	$5 \cdot 5^2$	2, 10	127	5	2	167	$11 \cdot 4 \cdot$	2, 3,
29	$5 \cdot 4 \cdot 4$	2, 3, 6	83	$3 \cdot 49 \cdot$	2, 4,	131	$5 \cdot 4^2$	2, 3		$25 \cdot 169$	6, 7
41	3	2		3^4	6	139	$3 \cdot 11 \cdot$	2, 5,	173	$11 \cdot 4$	2, 3
43	3	2	101	11	2		$11 \cdot 169$	5, 14	193	7	2
61	$3 \cdot 5$	2, 2	107	3	2	149	11	2	197	3^2	2

$d_K = -19,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
13	3	2	71	$7 \cdot 121 \cdot$	2, 3,	103	$3 \cdot 5 \cdot 9$	2, 2, 4	167	$3 \cdot 11 \cdot 4 \cdot$	2, 2, 3,
29	13	2		$5 \cdot 5$	4, 4	107	$3 \cdot 3^2$	2, 6		$25 \cdot 3 \cdot 4$	3, 6, 6
31	3	2	79	$5 \cdot 16 \cdot$	2, 5,	109	$3 \cdot 5$	2, 2	173	$7 \cdot 7 \cdot 7$	2, 6, 6
37	7	2		$16 \cdot 16$	10, 20	113	$7 \cdot 7 \cdot 7$	2, 3, 3	179	$5 \cdot 4 \cdot 4$	2, 3, 6
41	$5 \cdot 4 \cdot$	2, 3,	89	$3^2 \cdot 4 \cdot$	2, 3,	127	$5 \cdot 9$	2, 4	181	$3 \cdot 5$	2, 2
	4	6		$4 \cdot 25 \cdot$	6, 6,	151	7	2	193	5	2
53	$3 \cdot 5$	2, 2		64	9						
59	3	2	97	3	2						

$d_K = -43,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
5	7	2	61	11	2	131	5	2	179	$5 \cdot 9^2 \cdot 5^2$	2, 4, 10
19	$5 \cdot 16 \cdot$	2, 5,	71	$7 \cdot 25$	2, 3	137	13	2	191	13	2
	5	10	73	5	2	149	23	2	199	$3^2 \cdot 5 \cdot$	2, 4,
29	$13 \cdot 81$	2, 10	89	11	2	151	$7 \cdot 1369$	2, 38		$5 \cdot 9$	4, 4
37	11	2	113	$3 \cdot 5$	2, 2	157	$3 \cdot 11$	2, 2			

$d_K = -67,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
5	3	2	43	1849	22	101	$43 \cdot 4 \cdot 4$	2, 3, 6	179	5	2
7	3	2	53	$29 \cdot 4^2 \cdot 4$	2, 3, 6	109	$3 \cdot 5$	2, 2	191	$13 \cdot 4$	2, 3
13	11	2	61	$3 \cdot 5$	2, 2	113	3^2	2	197	73	2
31	3	2	79	5	2	137	$19 \cdot 25$	2, 6			
41	$3^2 \cdot 121$	2, 6	97	7	2	139	3	2			

$d_K = -163,\ p$ inert

p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d	p	$\tilde{h}_L$	d
5	$3 \cdot 5$	2, 2	59	$3 \cdot 13 \cdot$	2, 4,	101	$5 \cdot 11 \cdot$	2, 2,	139	3	2
11	$4 \cdot 4$	3, 6		13	4		$4 \cdot 4$	3, 6	149	$3 \cdot 19 \cdot$	2, 2,
13	17	2	67	9	4	103	5	2		$4 \cdot 4$	3, 6
17	13	2	73	$3 \cdot 5$	2, 2	107	$3 \cdot 49 \cdot$	2, 4,	157	43	2
23	3	2	79	$5 \cdot 49$	2, 8		121	6	181	$5 \cdot 7 \cdot 7^2$	2, 2, 14
29	$3^3 \cdot 16 \cdot$	2, 5,	89	$3 \cdot 7 \cdot$	2, 2,	109	$3 \cdot 11$	2, 2	191	$13 \cdot 5 \cdot 5 \cdot$	2, 4, 4,
	$3^2 \cdot 16$	6, 10		$25 \cdot 11 \cdot$	3, 5,	127	5	2		$25 \cdot 25$	24, 24
31	3	2		$11 \cdot 25$	5, 15	137	$23 \cdot 4 \cdot$	2, 3,	193	19	2
37	5^2	2					4	6			

Acknowledgements

I thank the referees for their comments which were helpful to improve the quality of the paper.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers I.* Mathematika 13 (1966), 204–216.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* John Wiley and Sons, 1989.

[3] K. Heegner, *Diophantische Analysis und Modulfunktionen.* Math. Z. 56, (1952). 227–253.

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

[5] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor.* Math. Comp. 72 (2003), no. 242, 913–937.

[6] H. M. Stark, *L-Functions at s=1. IV. First Derivatives at s=0.* Adv. in Math. 35 (1980), no. 3, 197–235.

[7] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one.* Michigan Math. J. 14 (1967) 1–27.

[8] PARI/GP, version `2.3.2`, `http://pari.math.u-bordeaux.fr/`, Bordeaux, 2006.

Middle East Technical University, Department of Mathematics, 06531 Ankara Turkey.

E-mail address: `komer@metu.edu.tr`