On the Computation of the Class Number of an Algebraic Number Field

By Johannes Buchmann and H. C. Williams*

Abstract. It is shown how the analytic class number formula can be used to produce an algorithm which efficiently computes the class number $h$ of an algebraic number field $F$. The method assumes the truth of the Generalized Riemann Hypothesis in order to estimate the residue of the Dedekind zeta function of $F$ at $s = 1$ sufficiently well that $h$ can be determined unambiguously. Given the regulator $R$ of $F$ and a known divisor $h^*$ of $h$, it is shown that this technique will produce the value of $h$ in $O(|d_F|^1 + e/(h^* R)^2)$ elementary operations, where $d_F$ is the discriminant of $F$. Thus, if $h < |d_F|^{1/8}$, then the complexity of computing $h$ (with $h^* = 1$) is $O(|d_F|^{1/4 + e})$.

1. Introduction. Let $F$ be an algebraic number field of degree $n$ over the rationals $Q$. It is well known that the class number $h$ of $F$ can be expressed by means of the analytic class number formula

$$h = C_F \lim_{s \to 1} (s - 1) \zeta_F(s)$$

with

$$C_F = \frac{w \sqrt{|d_F|}}{2^{r_1}(2\pi)^{r_2} R}.$$ 

Here we make use of the following notation:

- $w$ is the number of roots of unity in $F$,
- $d_F$ is the discriminant of $F$,
- $r_1$ is the number of real embeddings of $F$,
- $r_2$ is the number of pairs of complex embeddings of $F$,
- $R$ is the regulator of $F$, and
- $\zeta_F(s)$ is the Dedekind zeta function for $F$.

Also, it can be shown (see, for example, Wintner [17]) that

$$\rho = \lim_{s \to 1} (s - 1) \zeta_F(s) = \prod_{p \in P} E(p),$$

where $P$ is the set of rational primes and

$$E(p) = (1 - p^{-1}) \prod_{p|p} (1 - N(p)^{-1})^{-1}$$

is the Euler factor belonging to $p$.

Clearly, the formula (1.1) can be used to compute $h$ if it is possible to approximate $\rho$ sufficiently well that the absolute value of the error in evaluating the

Received September 7, 1988.
*Research supported by NSERC of Canada Grant #A7649.

©1989 American Mathematical Society
0025-5718/89 $1.00 + $.25 per page
right-hand side is less than 1/2. This technique has been used quite effectively to compute large tables of quadratic and cubic class numbers. (See Williams and Broere [16], and Tennenhouse and Williams [15].) Thus, the question arises as to whether this method can be used to determine the class number of an arbitrary number field.

We first note that the numbers \( r_1, r_2 \) can be easily computed from the defining polynomial

\[
f(t) = t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t].
\]

The discriminant \( d_F \) can be determined by means of the algorithm of Ford and Zassenhaus (see Ford [8] and Böffgen [1]) which even yields an integral basis of the maximal order \( \mathcal{O}_F \) of \( F \). Once this basis is known, the number of roots of unity can be easily evaluated. Of course, whenever \( r_1 > 0 \), then \( w = 2 \); but, in the totally complex case, we can use the algorithm of Fincke and Pohst [7] to enumerate all the algebraic integers whose conjugates are all in absolute value 1.

On the other hand, the computation of the regulator of an arbitrary algebraic number field is a very difficult task indeed. Algorithms for solving this problem are due to Pohst, Weiler and Zassenhaus [12] and Buchmann [2]. The complexity of the regulator computation is analyzed in Buchmann [3]. In this paper we assume that \( R \) has already been evaluated.

The purpose of this paper is to present a method to compute \( h \) by developing a sufficiently good approximation \( F(Q) \) of \( \rho \), where

\[
F(Q) = \prod_{p \leq Q} E(p) \cdot \prod_{p > Q} E(p)
\]

for some \( Q > 1 \). We do this by assuming the truth of the Riemann Hypothesis on the Dedekind zeta function of the normal closure \( L \) of \( F \). Our method is quite distinct from that of Eckhardt [6] which does not employ any hypothesis. Also, as in the quadratic and cubic cases, this technique is much more efficient than the unconditional one.

2. Some Results Concerning \( E(p) \). If we write our approximation to \( h \) as

\[
\tilde{h}(Q) = C_F F(Q),
\]

the error is

\[
|h - \tilde{h}(Q)| = C_F |\rho - F(Q)| = C_F F(Q) |T(Q) - 1|,
\]

where

\[
T(Q) = \prod_{p > Q} E(p)
\]

is the tail of the Euler product (1.2). In order, therefore, to estimate the error (2.2), we must estimate \( T(Q) - 1 \). In order to do this, we must investigate the properties of the Euler factors.

Each Euler factor can be written in the form

\[
E(p) = \left(1 + \frac{a_1(p)}{p} + \cdots + \frac{a_{n-1}(p)}{p^{n-1}}\right)^{-1}.
\]
Since the norm of each prime ideal $p$ dividing a rational prime $p$ can only take the values
\[ N(p) = p^f \]
with $0 < f \leq n$, it follows that there can be only a finite number of the sets \( \{a_1(p), a_2(p), \ldots, a_{n-1}(p)\} \) which are distinct. Thus, there is a $Q_0 \in \mathbb{Z}_{\geq 1}$ depending only on $n$ such that for every $p > Q_0$
\begin{equation}
|E(p)^{-1} - 1| < 1.
\end{equation}

From this point further, we assume that all constants depend only on a polynomial in $n$, not on $d_F$. We further assume that $Q > Q_0$ and that all summations $\sum_{p > Q}$ are over the primes which are unramified in $L$. Now
\[ -\log T(Q) = \sum_{p > Q} \log \left( 1 + \frac{a_1(p)}{p} + \cdots + \frac{a_{n-1}(p)}{p^{n-1}} \right), \]
and because of (2.3) we can use the power series expansion of the logarithm to get
\[ -\log T(Q) = \sum_{p > Q} \sum_{j=1}^{\infty} \left( \frac{a_1(p)}{p} + \frac{a_2(p)}{p^2} + \cdots + \frac{a_{n-1}(p)}{p^{n-1}} \right)^j \frac{(-1)^{j+1}}{j}. \]

This last equation can be justified by proving that the three infinite series are convergent. In fact, because of the finiteness of the number of distinct Euler factors, we can find constants $c_1, c_2 > 0$ such that
\[ \sum_{k=2}^{n-1} \left| \frac{a_k(p)p^{-k+2}}{\kappa} \right| \leq c_1 \quad \text{and} \quad \sum_{k=1}^{n-1} \left| \frac{a_k(p)p^{-k+1}}{\kappa} \right| \leq c_2 \]
for every $p > Q$. We also assume that $Q > 2c_2$. We then have
\[ \sum_{p > Q} \frac{1}{p^2} \sum_{k=2}^{n-1} \left| \frac{a_k(p)}{p^{k-2}} \right| \leq \sum_{p > Q} \frac{c_1}{p^2} \leq \frac{c_1}{Q} \]
and
\[ \sum_{p > Q} \sum_{j=2}^{\infty} \frac{1}{j p^j} \sum_{k=1}^{n-1} \left| \frac{a_k(p)}{p^{k-1}} \right|^j \leq \sum_{p > Q} \sum_{j=2}^{\infty} \left( \frac{c_2}{p} \right)^j \leq \sum_{p > Q} \frac{c_2^2}{p^2} \left( \frac{1}{1 - c_2/p} \right) \leq \frac{2c_2^2}{Q}, \]
the last inequality in both results following from the easily verified inequality $\sum_{p > Q} 1/p^2 < 1/Q$.

It remains to estimate the series
\[ \sum_{p > Q} \frac{a_1(p)}{p}. \]

We will do this by extending the method of Cornell and Washington [5]. For this purpose we let $G$ be the Galois group of the normal closure $L$ of $F$ viewed as a
permutation group on \(n\) letters, and we let \(C_1, C_2, \ldots, C_m\) be its conjugacy classes. By \(P_j\) we denote the set of all unramified prime numbers \(p\) in \(L\) such that the Frobenius automorphism of the extension \(\mathcal{O}_L/p\) of \(\mathbb{Z}/p\mathbb{Z}\) (for any prime ideal \(p\) of \(\mathcal{O}_L\) dividing \(p\)) is induced by an element of \(C_j\). Here, \(\mathcal{O}_L\) denotes the maximal order of \(L\). All the prime numbers \(p \in P_j\) have the same Euler factor

\[
E_j(p) = \left(1 + \frac{a_{1j}}{p} + \frac{a_{2j}}{p^2} + \cdots + \frac{a_{n-1,j}}{p^{n-1}}\right)^{-1}.
\]

As we wish to estimate \(\sum_{p>q} a_{1j}(p)/p\), we must now determine the value of \(a_{1j}\).

**Proposition 2.1.** Let \(j \in \{1, 2, \ldots, m\}\), and let \(N_j\) be the number of fixed points of any permutation \(\pi_j \in C_j\). Then \(a_{1j} = 1 - N_j\).

Proof. We can write

\[
E_j(p) = \frac{p^{n-1}(p-1)}{(p^{f_{1j}} - 1) \cdots (p^{f_{k_{j,j}} - 1})},
\]

where \((f_{1j}, \ldots, f_{k_{j,j}})\) is the cycle type of any \(\pi_j \in C_j\), i.e., \(\pi_j\) can be decomposed into \(k_{j}\) cycles of length \(f_{1j}, f_{2j}, \ldots, f_{k_{j,j}}\). Assume that \((f_{1j}, f_{2j}, \ldots, f_{k_{j,j}})\) is ordered such that \(f_{1j}\) is minimal. We are now able to distinguish two cases.

**Case 1.** \(f_{1j} > 1\). In this case, \(\pi_j\) has no fixed point. Also,

\[
E_j(p) = \frac{p^{n-1}}{p^{f_{1j}} - 1 + p^{f_{2j}} - 1 + \cdots + 1} = \frac{p^{n-1}}{p^{f_{1j}} - 1} \cdot \frac{p^{n-2}}{p^{f_{2j}} - 1} \cdots \frac{1}{p^{f_{k_{j,j}} - 1}}.
\]

Since \(p\) is assumed to be unramified, we have \(\sum_{i=1}^{k_{j}} f_{ij} = n\); hence, upon multiplying out the denominator of (2.4) we see that the coefficient of \(p^{n-2}\) is precisely 1.

**Case 2.** \(f_{1j} = 1\). In this case it is easy to see that \(-a_{1j}\) is the number of values of \(i\) for which \(f_{ij} = 1\) (\(2 \leq i \leq k_{j}\)). It follows that \(a_{1j} = 1 - N_j\). \(\square\)

**Proposition 2.2.** For the values of \(m\) and \(a_{1j}\) defined above we have

\[
\sum_{j=1}^{m} a_{1j} |C_j| = 0.
\]

Proof. For a permutation \(\pi \in G\) denote by \(\theta(\pi)\) the number of fixed points of \(\pi\). By Proposition 2.1 we have

\[
\sum_{j=1}^{m} a_{1j} |C_j| = |G| - \sum_{\pi \in G} \theta(\pi).
\]

But by Burnside’s Orbit Lemma (see Grove [9]) we know that \(\sum_{\pi \in G} \theta(\pi) = |G|\), and this proves our assertion. \(\square\)

Also, we note that since

\[
E(p) \geq \frac{p^{n-1}}{p^{f_{1j}} - 1 + p^{f_{2j}} - 1 + \cdots + 1} > \frac{p - 1}{p},
\]

we have

\[
F(Q) \gg (\log Q)^{-1}
\]

by Mertens’ Theorem (see Hardy and Wright [10, p. 351]).
3. Determination of the Value of $Q$. In order to find the value of $Q$ needed to correctly determine $h$, we define as in [5] the function

$$A(t) = \sum_{Q < p < t} a_1(p).$$

This can evidently be rewritten in the form

$$A(t) = \sum_{j=1}^{m} \sum_{p \in P_j} a_{1j} = \sum_{j=1}^{m} a_{1j} \pi_j(t),$$

where $\pi_j(t)$ is the number of primes less than $t$ in $P_j$. We now use Oesterlé [13, Théorème 3], which asserts that under the Generalized Riemann Hypothesis for the Dedekind zeta function of $L$ we have

$$\left| \pi_j(t) - \frac{|C_j|}{|G|} \text{li}(t) \right| \leq \frac{|C_j|}{|G|} \tilde{C}(t) \sqrt{t} \log t,$$

where

$$\tilde{C}(t) = \log |d_L| \left( \frac{1}{\pi \log t} + \frac{5.3}{(\log t)^2} \right) + n_L \left( \frac{1}{2\pi} + \frac{2}{\log t} \right) .$$

Here, $d_L$ is the discriminant of $L$ and $n_L$ is the degree of $L$ over $\mathbb{Q}$. It follows from Proposition 2.2 that

$$|A(t)| = \left| \sum_{j=1}^{m} a_{1j} \left( \pi_j(t) - \frac{|C_j|}{|G|} \text{li}(t) \right) \right| \leq C(t) \sqrt{t} \log t$$

with

$$C(t) = \tilde{C}(t) \left( \sum_{j=1}^{m} |a_{1j}||C_j| \right) / |G| .$$

Notice that $C(t)$ is a monotone decreasing function of $t$. By using the argument used in [5], we obtain

$$(3.1) \left| \sum_{p > Q} \frac{a_t(p)}{p} \right| \leq C(Q) \frac{4 + 3 \log Q}{\sqrt{Q}},$$

which shows that $\sum_{p > Q} a_t(p)/p$ is in fact convergent and, moreover, yields an upper bound for the limit. By using (3.1) and some results from Section 2, we have

**Theorem 3.1.** For $T(Q)$ defined above we have

$$|\log T(Q)| \leq \frac{4 + 3 \log Q}{\sqrt{Q}} C(Q) + \frac{c_1 + 2c_2^2}{Q} .$$

Notice that if we put $Q = (\log |d_L|)^2$, we see from (1.1), (1.2), (2.5) and Theorem 3.1 that

$$(3.2) hR \gg (|d_F|^{1/2}(\log \log |d_L|)^{-1}).$$

We will now show how Theorem 3.1 can be used to compute $h$. We first suppose that we know a factor $h^*$ of $h$. Such a factor can be determined by randomly selecting one or several ideals of $\mathcal{O}_F$ and determining the order $h^*$ of the subgroup
of the class group generated by the ideal classes represented by these ideals. We then put \( H = h/h^* \) and define

\[
\bar{H} = \bar{H}(Q) = \text{Ne} \left( \frac{F(Q)}{C FRh^*} \right).
\]

Here, \( \text{Ne}(x) \) denotes the nearest positive integer to \( x \). We also put \( \kappa = \kappa(Q) = \frac{F(Q)}{C FRh^*} - \bar{H} \).

Our objective is to determine for what values of \( Q \) we have \( \bar{H}(Q) = H \), i.e., \( h = h^* \bar{H} \). For this purpose we define

\[
\psi(Q) = C(Q) \left( \frac{4 + 3 \log Q}{\sqrt{Q}} \right) + \frac{c_1 + 2c_2}{Q}
\]

and prove

**Theorem 3.2.** If \( \psi(Q) < \log((\bar{H} + 1)/(\bar{H} + |\kappa|)) \), then \( H = \bar{H} \).

**Proof.** We know from Theorem 3.1 that \( |\log T(Q)| < \psi(Q) \); hence, it follows from our assumption that

\[
|\log T(Q)| < \log \left( \frac{\bar{H} + 1}{\bar{H} + |\kappa|} \right).
\]

Consequently,

\[
\frac{\bar{H} + |\kappa|}{\bar{H} + 1} < T(Q) < \frac{\bar{H} + 1}{\bar{H} + |\kappa|}.
\]

But since

\[
\frac{\bar{H} + 1}{\bar{H} + |\kappa|} \leq \frac{\bar{H} + 1}{\bar{H} + \kappa}
\]

and

\[
\frac{\bar{H} + |\kappa|}{\bar{H} + 1} > \frac{\bar{H} - 1}{\bar{H} - |\kappa|} \geq \frac{\bar{H} - 1}{\bar{H} + \kappa},
\]

we get

\[
\frac{\bar{H} - 1}{\bar{H} + \kappa} < T(Q) < \frac{\bar{H} + 1}{\bar{H} + \kappa}.
\]

Now \( H = (\bar{H} + \kappa)T(Q) \); thus, it follows from (3.3) that \( \bar{H} - 1 < H < \bar{H} + 1 \). □

We also point out here that since \( |d_L| \) can be bounded by a power of \( |d_F| \) which depends only on \( n \), we have

\[
\psi(Q) < (c_3 \log |d_F|)/Q^{1/2}
\]

for some constant \( c_3 \) which is independent of \( d_F \).

**4. An Algorithm for Determining** \( h \). Using Theorem 3.2, we can now develop an algorithm for computing \( h \). We denote by \( \{p_i\}_{i \in \mathbb{N}} \) the sequence of prime integers, choose an interval length \( c \) (say 500), and define

\[
F_i = \prod_{j=c(t-1)+1}^{ci} E(p_j).
\]
We now have

**Algorithm 4.1.** Compute $h$, given $h^*$ and $R$.

1. $i ← 1$, $F ← 1/(CFh^*R)$.
2. $F ← F \cdot F_i$.
3. $\tilde{H} = \text{Ne}(F)$, $\kappa ← F - \tilde{H}$.
4. If $\psi(p_{1,c}) \geq \log((\tilde{H} + 1)/(\tilde{H} + |\kappa|))$, then go to 2.
5. Otherwise, $h ← h^*\tilde{H}$, and the algorithm terminates.

We need only explain how $F_i$ is to be computed in Step 2 of this algorithm; that is, how do we compute the Euler factor $E(p)$ for a given prime $p$. We first assume that $p$ does not divide the index $I$ of the equation order generated by a root of the defining polynomial $f(t)$. We then compute positive integers $f_1, \ldots, f_k$ such that $f(t)$ can be decomposed modulo $p$ into the product of $k$ irreducible polynomials $g_1(t), g_2(t), \ldots, g_k(t)$ of degree $f_1, f_2, \ldots, f_k$, respectively. It is well known that the Euler factor of $p$ is

$$E(p) = \frac{p^{n-1}(p-1)}{(p^{f_1}-1) \cdots (p^{f_k}-1)}.$$ 

The decomposition type (the values of $f_1, f_2, \ldots, f_k$) can be determined by taking greatest common divisors of $t^p - t$ and $f(t)$ for $n \geq d \geq 1$ as described in Knuth [11, Algorithm D, p. 429]. This algorithm will execute in a time interval which is polynomial in $\log p$ (and $n$).

If $p$ does divide $I$, then the method of Buchmann and Lenstra [4] can be used to determine the decomposition type of $p$. This algorithm also requires a polynomial function of $\log p$ (and $n$) elementary operations in order to successfully terminate.

We also need to analyze the total complexity of this algorithm. As this will depend on the choice of the defining polynomial $f(t)$, we must first show that such a polynomial exists with bounded coefficients. We will do this in the next section.

**5. The Defining Polynomial.** Assume that we know an integral basis $\omega_1, \omega_2, \ldots, \omega_n$ of $F$ with $\omega_1 = 1$. On reducing the corresponding basis of the Minkowski lattice of $\mathcal{O}_{F}$ by means of the LLL-reduction algorithm, we may assume that

$$|\omega_j^{(i)}| \leq 2^{n/4}|d_F|^{1/2} \quad (1 \leq i, j \leq n),$$

where $\omega_j^{(i)}$ $(i = 1, 2, 3, \ldots, n)$ are the algebraic conjugates of $\omega_j$. We define $F_i = \mathbb{Q}(\omega_1, \ldots, \omega_i)$, and we assume that $\mathbb{Q} = F_1 \neq F_2 \neq \cdots \neq F_m = F_{m+1} = \cdots = F_n = F$. Since $[F_i : F_{i-1}] \geq 2$ for $2 \leq i \leq m$, it follows that

$$n = [F : \mathbb{Q}] = \prod_{i=2}^{m} [F_i : F_{i-1}] \geq 2^{m-1};$$

hence, $m \leq \log_2 n + 1$.

We next apply the usual technique to construct a primitive element $\theta_i$ of $F_i$ over $\mathbb{Q}$. We can take $\theta_2 = \omega_2$ and then apply induction. Assume that we know $\theta_{i-1}$, and put $\alpha = \theta_{i-1}$, $\beta = \omega_i$. Denote by $g(t)$ the minimal polynomial of $\alpha$ over $\mathbb{Q}$ and by $h(t)$ the minimal polynomial of $\beta$ over $\mathbb{Q}$. Let

$$g(t) = (t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_m)$$

and

$$h(t) = (t - \beta_1)(t - \beta_2) \cdots (t - \beta_n).$$
and
\[ h(t) = (t - \beta_1)(t - \beta_2) \cdots (t - \beta_\nu) \]
be the decomposition of \( g \) and \( h \) in some splitting field \( M \) of \( fg \) over \( F_1 \). Let \( \alpha = \alpha_1 \), \( \beta = \beta_1 \), and take an element \( \gamma \in \mathcal{O}_{F_1} \) such that
\[ \alpha_j + \gamma \beta_k \neq \alpha + \gamma \beta \quad (1 \leq j \leq \mu; 2 \leq k \leq \nu). \]
Then we can put \( \gamma_i = \gamma; \theta_i = \alpha + \gamma_i \beta \). In order for \( \gamma \) (\( = \gamma_i \)) to satisfy (5.1), it is sufficient that
\[ \gamma_i \neq \frac{\alpha - \alpha_j}{\beta_k - \beta} \quad (i \leq j \leq \mu; 2 \leq k \leq \nu), \]
which means that it suffices to take
\[ (5.2) \quad \gamma_i = \max_{1 \leq j \leq \mu} \left[ \binom{\alpha - \alpha_j}{\beta_k - \beta} \right] + 1. \]

We now need to estimate \(|\gamma_i|\). In each step of this construction, \( \beta \) is one of the basis elements \( \omega_j \). Thus the algebraic number \( \beta_k - \beta \) is of degree at most \( n(n - 1) \), and
\[ (5.3) \quad |\beta_k - \beta|^{-1} < C^{n^2}/N(\beta_{\mu} - \beta) \leq C^{n^2} \]
with \( C = 2^{n/4 + 1}|d_F|^{1/2} \). If \( B_{i-1} > 2 \) is a bound on the conjugates of \( \alpha = \theta_{i-1} \), then from (5.2) and (5.3) we get
\[ |\gamma_i| < 3C^{n^2}B_{i-1}; \]
consequently, the conjugates of \( \theta_i \) are bounded by \( B_i = B_{i-1}(1 + 3C^{n^2}) \). Since \( \theta_2 = \omega_2 \), we can take \( B_2 = C \), and we eventually get \( B = C(1 + 3C^{n^2})^{\log_2 n + 1} \) as a bound on the conjugates of the generating element \( \theta = \theta_m \). The discriminant of this element is then bounded by \( \tilde{B} = 2B^{2n} \), and we have proved

**Proposition 5.1.** There exists a defining polynomial \( f \) of \( F \) whose discriminant is bounded by a polynomial in \( d_F \) which only depends on the degree \( n \) of \( F \) over \( \mathbb{Q} \). This polynomial can be computed from a reduced integral basis of \( F \).

6. **Complexity of the Algorithm.** We will now assume that \( F \) is given by a defining polynomial \( f \) with the properties described in Proposition 5.1. Under this assumption we will analyze the complexity of our technique.

As we have seen above, the work needed to compute each factor of
\[ F(Q) = \prod_{p \leq q} E(p) \]
is polynomial in \( \log |d_F| \). Thus, we must find a bound for the number of primes which occur in this product. We first prove

**Proposition 6.1.** If \( \psi(Q) < \log((H + 1)/(H + |\kappa|)) \), then \( H = \tilde{H} \).

**Proof.** By Theorem 3.1 and our assumption we have
\[ \frac{H + |\kappa|}{H + 1} < T(Q) < \frac{H + 1}{H + |\kappa|}. \]
Also,
\[
\frac{H + |\kappa|}{H + 1} > \frac{H}{H + 1 - |\kappa|} \geq \frac{H}{H + 1 + |\kappa|}
\]
and
\[
\frac{H + 1}{H + |\kappa|} < \frac{H}{H - 1 + |\kappa|},
\]
hence,
\[
\frac{H}{H + 1 + |\kappa|} < T(Q) < \frac{H}{H - 1 + |\kappa|}.
\]
By using the fact that $\tilde{H} = HT(Q)^{-1} - \kappa$, we get $H - 1 < \tilde{H} < H + 1$. □

**COROLLARY.** We have $\psi(Q) < \log((\tilde{H} + 1)/(|\kappa|))$ if and only if $\psi(Q) < \log((H + 1)/(H + |\kappa|))$.

**Proof.** From Proposition 6.1 and Theorem 3.2 we see that both inequalities imply that $H = \tilde{H}$. □

Now
\[
\log \frac{H + 1}{H + |\kappa|} > \log \left(1 + \frac{1}{2H + 1}\right) > \frac{1}{2H + 2}.
\]
Hence, if $Q$ is sufficiently large that
\begin{equation}
(6.1) \quad \psi(Q) < \frac{1}{2H + 2},
\end{equation}
it follows from the Corollary of Proposition 6.1 that $H = \tilde{H}(Q)$. By a theorem of Siegel [14] we know that
\begin{equation}
(6.2) \quad 2H + 2 < c_4|d_F|^{1/2}(|d_F|)^{n-1}/R\beta^*,
\end{equation}
where $c_4$ is a constant which is independent of the value of $d_F$. Thus, from (3.4) and (6.2) we see that for any $\varepsilon > 0$ there exists a number $K$ such that
\[
K = O(|d_F|^{1+\varepsilon}/(\beta^* R)^2)
\]
and (6.1) holds for any $Q > K$.

Thus, we have proved

**THEOREM 6.1.** Algorithm 4.1 computes the class number $h$ of $F$ in
\[
O(|d_F|^{1+\varepsilon}/(\beta R)^2)
\]
elementary operations.

If $h < |d_F|^\alpha$, then by (3.2) we have
\[
R \gg (|d_F|^{1/2-\alpha+\varepsilon});
\]
by Theorem 6.1 we can compute $h$ (using $h^* = 1$) in $O(|d_F|^{2\alpha+\varepsilon})$ operations. Thus, Algorithm 4.1 will find $h$ quite quickly when $h$ is small, say $h < |d_F|^{1/8}$. For large values of $h$ it is necessary first to determine a value for $h^*$ which will render the quantity $|d_F|/(h^* R)^2$ sufficiently small that Algorithm 4.1 can efficiently compute $H$. 

7. Acknowledgments. The authors gratefully acknowledge several helpful suggestions concerning this work from Larry Grove and Richard Blecksmith.

Mathematisches Institut
Universität Düsseldorf
4000 Düsseldorf
Federal Republic of Germany

Department of Computer Science
University of Manitoba
Winnipeg R3T 2N2, Manitoba
Canada


