MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 184
OCTOBER 1988, PAGES 809-824

Computation of Real Quadratic Fields with Class Number One

By A. J. Stephens and H. C. Williams*

Abstract. A rapid method for determining whether the real quadratic field $\mathscr{K} = \mathscr{Q}(\sqrt{D})$ has class number one is described. The method makes use of the infrastructure idea of Shanks to determine the regulator of $\mathscr{K}$ and then uses the Generalized Riemann Hypothesis to rapidly estimate $L(1, \chi)$ to the accuracy needed for determining whether or not the class number of $\mathscr{K}$ is one. The results of running this algorithm on a computer for all prime values of D up to 10^9 are also presented, together with further results on runs on intervals of size 10^7 starting at 10^i $(i = 9, 10, \ldots, 16)$.

1. Introduction. Let D be a square-free positive integer and let $\mathscr{K} = \mathscr{Q}(\sqrt{D})$ be the real quadratic field formed by adjoining $\sqrt{D}$ to the rationals $\mathscr{Q}$. While it is known that there are only 9 complex quadratic fields with class number one, it has been conjectured since Gauss that there are an infinite number of real quadratic fields with class number h equal to one. In spite of the immense amount which has been learned about quadratic fields since the time of Gauss, this conjecture seems still to be extremely difficult to prove. An interesting recent development concerning this problem is the collection of heuristics introduced by Cohen and Lenstra [1]. Among other things their results suggest that the probability that the odd part of the class group of $\mathscr{K}$ is one is about 75.446%.

If p is a prime and h is the class number of $\mathscr{Q}(\sqrt{p})$, then $2 \nmid h$. Thus, in view of the Cohen-Lenstra heuristics, we would expect that the probability that $h(\mathscr{Q}(\sqrt{p})) = 1$ is 75.446%. In Tennenhouse and Williams [9] this was tested numerically for all primes up to 10^8. Unfortunately, the techniques used to find the results presented in Table 1 of [9] required hundreds of hours of computer time to run. In this paper we describe a further numerical investigation into this problem for all primes up to 10^9. Our new algorithms run much more quickly than those used in [9]; however, we must assume the Generalized Riemann Hypothesis (GRH) on $\zeta_{\mathscr{K}}$ in order to determine whether or not $h = 1$. This assumption, together with several refinements of our previous algorithms, allowed us to examine over 50000000 fields $\mathscr{Q}(\sqrt{p})$ with $p < 10^9$ in a little less than 80 hours of computer time.

The purpose of this paper is to describe our improved algorithms and to present the results of our computer run. Our basic plan of attack is similar to that of [9]. We use the analytic class number formula

$$2hR = \sqrt{\Delta} L(1, \chi),$$

Received November 3, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R11, 11R29, 11Y40; Secondary 11Y65.
*Research supported by NSERC of Canada grant # A7649.

where R is the regulator and Δ is the discriminant of $\mathscr{K}$. Setting $r = 1$ when $D \equiv 2,3 \pmod 4$ and $r = 2$ when $D \equiv 1 \pmod 4$, we have $\Delta = 4D/r^2$. The problem is now one of determining R and then finding $L(1,\chi)$ to sufficient accuracy to guarantee whether or not $h = 1$. In Section 2 we describe a very expeditious algorithm for determining R in $O(D^{1/4+\varepsilon})$ elementary operations. In Section 3 we discuss how to use the Euler product representation

$$L(1,\chi) = \prod_q q/(q - (\Delta/q)),$$

where the product is taken over all primes q and (Δ/q) is the Kronecker symbol, to approximate $L(1,\chi)$ to the desired level of accuracy.

2. Computation of R. In this section we will derive our algorithm for determining R. This algorithm is based on the infrastructure ideas of Shanks [6] as implemented by Williams and Wunderlich [11] and Stephens and Williams [7], [8]. For a somewhat different approach to Shanks' ideas we refer the reader to the papers of Lenstra [3] and Schoof [5]. Our main objective here will be to improve somewhat the regulator algorithm presented in Section 3 of [7]. As much of this material is given in [11], [7] and [8], our treatment will be quite brief. Proofs of the many statements given here can be found in these papers.

As in [11], [7] and [8], we let $P_0, Q_0 \in \mathbf{Z}$ be such that $Q_0 \mid D - P_0^2$ and put $\phi = \phi_0 = (P_0 + \sqrt{D})/Q_0$. By putting** $q_0 = [\phi_0]$ and using the well-known formulas

$$\begin{aligned} P_{k+1} &= q_k Q_k - P_k, \\ Q_{k+1} &= (D - P_{k+1}^2)/Q_k, \\ q_{k+1} &= [(P_{k+1} + \sqrt{D})/Q_{k+1}] \geq 1 \qquad (k = 0, 1, 2, \ldots), \end{aligned} \tag{2.1}$$

we can expand ϕ into the simple continued fraction

$$\phi = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots + \cfrac{1}{q_{m-1} + \cfrac{1}{\phi_m}}}},$$

where $\phi_m = (P_m + \sqrt{D})/Q_m$.

If we put $\theta_1 = 1$ and

$$\theta_n^{-1} = \prod_{i=1}^{n-1} \phi_i, \tag{2.2}$$

then

$$\theta_n \bar{\theta}_n = (-1)^{n-1} Q_{n-1}/Q_0 \tag{2.3}$$

and

$$\theta_n = (-1)^{n-1}(G_{n-2} - \sqrt{D} B_{n-2})/Q_0, \tag{2.4}$$

**Here, as is usual, we use $[\alpha]$ to denote that integer such that $\alpha - 1 < [\alpha] \leq \alpha$. We also use $\bar{\alpha}$ to denote the conjugate of $\alpha \in \mathscr{K}$.

where

$$G_k = Q_0A_k - P_0B_k = P_{n+1}B_k + Q_{k+1}B_{k-1}. \tag{2.5}$$

Here, $A_{-2} = 0$, $A_{-1} = 1$, $B_{-2} = 1$, $B_{-1} = 0$ and

$$A_{i+1} = q_{i+1}A_i + A_{i-1}, \quad B_{i+1} = q_{i+1}B_i + B_{i-1} \qquad (i = -1, 0, 1, 2, \dots). \tag{2.6}$$

If we put $\psi_i = |(\overline{\phi}_i)^{-1}|$ and $\Psi_n = |\overline{\theta}_n|$, then by (2.1)

$$\psi_i = |(P_i + \sqrt{D})/Q_{i-1}|$$

and

$$\Psi_n = \prod_{i=1}^{n-1} \psi_i. \tag{2.7}$$

Also, by (2.4) and (2.5) we have

$$\begin{aligned} \Psi_n &= |(G_{n-2} + \sqrt{D}B_{n-2})/Q_0| \\ &= |(B_{n-2}(P_{n-1} + \sqrt{D}) + Q_{n-1}B_{n-3})/Q_0|. \end{aligned} \tag{2.8}$$

For $\alpha, \beta \in \mathscr{K}$, denote by $[\alpha, \beta]$ the module $\alpha\mathbf{Z} + \beta\mathbf{Z}$. For $\omega = (r - 1 + \sqrt{D})/r$, we have

$$\mathscr{O}_{\mathscr{K}} = [1, \omega],$$

where $\mathscr{O}_{\mathscr{K}}$ is the maximal order of $\mathscr{K}$. If we put $\phi_0 = \omega$, then

$$\mathfrak{a}_i = [Q_{i-1}/r, (P_{i-1} + \sqrt{D})/r]$$

is a principal ideal of $\mathscr{O}_{\mathscr{K}}$. Further, if

$$(U)\mathfrak{c} = \mathfrak{a}_s\mathfrak{a}_t, \tag{2.9}$$

where $U \in \mathbf{Z}$ and $\mathfrak{c}$ is a primitive ideal of $\mathscr{O}_{\mathscr{K}}$, then $\mathfrak{c} = \mathfrak{c}_1$ is a principal ideal of $\mathscr{O}_{\mathscr{K}}$. Let $\mathfrak{c}_1 = [Q'_0/r, (P'_0 + \sqrt{D})/r]$; if we expand $\phi'_0 = (P'_0 + \sqrt{D})/Q'_0$ into a continued fraction, there must be a least m (≥ 0) such that $0 < Q'_m \leq d = [\sqrt{D}]$. As pointed out in [7] and [8], we have $\mathfrak{c}_{m+1} = \mathfrak{a}_k$ for some $k \geq 1$ and

$$\Psi_k = \Psi_s\Psi_t\Psi'_{m+1}/U. \tag{2.10}$$

If $\lambda = \log(\Psi'_{m+1}/U)$, then by using the results needed to obtain (3.5) of [7], we have

$$-\log Q_{s-1}Q_{t-1} \leq \lambda < \log 2. \tag{2.11}$$

For the sake of brevity, we will use $\mathfrak{a}_s * \mathfrak{a}_t$ to denote the pair $(\mathfrak{a}_k, \Psi'_{m+1}/U)$ produced by this process. The algorithm of Shanks given in Section 3 of [7] can be used to find $\mathfrak{c}$ and U and the formulas (2.6) and (2.8) can be used to find

$$\Psi'_{m+1} = |B'_{m-1}(P'_m + \sqrt{D}) + Q'_mB'_{m-2}|/Q'_0.$$

Since B'_k increases with increasing k and $B'_{m-1} < Q'_0/\sqrt{D}$ (Theorem 4.2 of [7]), this computation is easily performed.

In the continued fraction expansion of ω there is a least $p \in \mathbf{Z}^+$ such that

$$\mathfrak{a}_{p+1} = \mathfrak{a}_1.$$

Indeed, for this value of p we have $\mathfrak{a}_i = \mathfrak{a}_j$ if and only if $p \mid i-j$. Also, $\Psi_{p+1} = \varepsilon$ (> 1), the fundamental unit of $\mathscr{K}$, and

$$R = \log \Psi_{p+1}$$

is the regulator of $\mathscr{K}$. If we define

$$\delta_m = \delta(\mathfrak{a}_m, \mathfrak{a}_1) = \log \Psi_m,$$

then $R = \delta_{p+1}$. For $\mathfrak{a} = [\alpha, \beta]$ an ideal of $\mathscr{O}_{\mathscr{K}}$, define $\bar{\mathfrak{a}}$ to be the conjugate ideal $[\overline{\alpha}, \overline{\beta}]$. By [8] we know that $\bar{\mathfrak{a}}_m = \mathfrak{a}_{p+2-m}$ when $m \leq p+1$; thus, by using the method used to derive (3.1) of [8] we have

$$\delta'_m = \delta(\bar{\mathfrak{a}}_m, \mathfrak{a}_1) = R - \delta_m + \log(Q_{m-1}/r). \tag{2.12}$$

We also note that δ_m is a strictly increasing function of m and that δ'_m is a strictly decreasing function of m. Further, by results in [8] we know that $\delta_m > (m-2)\log\tau$, where $\tau = (1+\sqrt{5})/2$. We now have

LEMMA 2.1. *If $\mathfrak{a}_i = \bar{\mathfrak{a}}_k$ and $1 < i, k \leq t$, then we must have either*

$$Q_m = Q_{m+1} \quad \textit{for some positive } m < t-1 \tag{2.13}$$

or

$$P_n = P_{n+1} \quad \textit{for some positive } n \leq t-1. \tag{2.14}$$

Proof. By Corollary 2.1.1 of [8] we have $\mathfrak{a}_i = \bar{\mathfrak{a}}_k = \mathfrak{a}_{wp+2-k}$; thus

$$wp = i + k - 2 \qquad (w \geq 1)$$

and

$$p \leq 2t - 2.$$

Since $p = 2n$ or $p = 2m+1$, the lemma follows. □

Again, by results given in [8] we see that if m is the least positive integer such that (2.13) holds then

$$R = \log|\Psi_{m+2}/\overline{\Psi}_{m+1}|;$$

hence, by (2.3) we get

$$R = \log(\psi_{m+1}Q_0/Q_m) + 2\delta_{m+1}. \tag{2.15}$$

If n is the least positive integer such that (2.14) holds, then

$$R = \log|\Psi_{n+1}/\overline{\Psi}_{n+1}|$$

and

$$R = \log(Q_0/Q_n) + 2\delta_{n+1}. \tag{2.16}$$

Suppose we select some $\mathfrak{a}_s$ such that $\kappa + \log D < \delta_s < R$ $(\kappa > 0)$ and $Q_{s-1} < \sqrt{D}$. Put $(\mathfrak{b}_1, \chi_1) = \mathfrak{a}_s * \mathfrak{a}_s$. If $\delta_1^* = \delta(\mathfrak{b}_1, \mathfrak{a}_1)$ and $\lambda_1 = \log\chi_1$, then by (2.10) and (2.11) we have

$$\delta_1^* = 2\delta_s + \lambda_1 \tag{2.17}$$

and

$$-\log D < \lambda_1 < \log 2. \tag{2.18}$$

If we define $(\mathfrak{b}_{i+1}, \lambda_{i+1}) = \mathfrak{b}_i * \mathfrak{b}_1$, $\delta_i^* = \delta(\mathfrak{b}_i, \mathfrak{a}_i)$ and $\lambda_{i+1} = \log \chi_{i+1}$, we get

$$\delta_{i+1}^* = \delta_i^* + \delta_1^* + \lambda_{i+1} \tag{2.19}$$

and

$$-\log D < \lambda_{i+1} < \log 2. \tag{2.20}$$

It follows from (2.17), (2.18), and (2.20) that

$$\delta_1^* + \lambda_{i+1} = 2\delta_s + \lambda_1 + \lambda_{i+1} > 2\kappa > 0;$$

hence, δ_j^* increases without limit with increasing j. If $M = (\log 4\sqrt{D})/2$, then $M > \log 2$ and

$$R + M > \delta_s + \lambda_1;$$

thus $R + M + \delta_s > \delta_1^*$. It follows that there must exist some $j \geq 1$ such that

$$\delta_j^* \leq R + \delta_s + M < \delta_{j+1}^*. \tag{2.21}$$

THEOREM 2.2. *Let* $\mathscr{S} = \{\mathfrak{a}_1, \bar{\mathfrak{a}}_i \mid 1 \leq i \leq t\}$. *If* (2.21) *holds and* $\delta_{t+1} > M + \delta_s$, *then* $\mathfrak{b}_j \in \mathscr{S}$.

Proof. We first note that if

$$\delta_t' \leq \delta_j^* \leq \delta_t + R,$$

then $\mathfrak{b}_j \in \mathscr{S}$. From (2.21), (2.19), and (2.17) we get

$$R + M - \delta_s - \lambda_1 - \lambda_{j+1} < \delta_j^* \leq R + \delta_s + M < R + \delta_{t+1}. \tag{2.22}$$

If $Q_t/Q_0 < \sqrt{D}$, then

$$2M > \log 4\sqrt{D} = 2\log 2 + \log\sqrt{D} > \lambda_1 + \lambda_{j+1} + \log(Q_t/Q_0).$$

If $Q_t/Q_0 > \sqrt{D}$, then by (2.1), $Q_{t+1}/Q_0 < \sqrt{D}$ and

$$2M > \lambda_1 + \lambda_{j+1} + \log(Q_{t+1}/Q_0).$$

Thus, by (2.22) and (2.12) we have

$$\delta_j^* > R - \delta_s - M + \log(Q_t/Q_0) > \delta_{t+1}'$$

or

$$\delta_j^* > R - \delta_s - M + \log(Q_{t+1}/Q_0) > \delta_{t+2}'.$$

Now if $\delta_j^* = \delta_{t+1}'$, we have $Q = Q_t > \sqrt{D}$, where $\mathfrak{b}_j = [Q/Q_0, (P + \sqrt{D})/Q_0]$. Since this is not possible by construction of $\mathfrak{b}_j$, we can only have $\delta_j^* \geq \delta_t'$. Thus $\mathfrak{b}_j \in \mathscr{S}$. □

COROLLARY. *Suppose* $\delta_{t+1} > M + \delta_s$ *and* (2.21) *holds. If* $\mathfrak{b}_j = \mathfrak{a}_i$ *for some* i $(1 \leq i \leq t)$, *then*

$$R = \delta_j^* - \delta_i.$$

If $\mathfrak{b}_j \neq \mathfrak{a}_i$ *for some* i $(1 \leq i \leq t)$, *then* $\mathfrak{b}_j = \bar{\mathfrak{a}}_i$ *for some* i $(1 \leq i \leq t)$ *and*

$$R = \delta_j^* - \delta_i - \log(Q_{i-1}/Q_0).$$

Proof. The first part of the Corollary follows easily from the theorem. If $\mathfrak{b}_j \neq \mathfrak{a}_i$ $(1 \leq i \leq t)$, then by the theorem we must have $\mathfrak{b}_j = \bar{\mathfrak{a}}_i$ for some i $(1 \leq i \leq t)$; hence, $\delta_j^* < R$. From (2.12) it follows that

$$R = \delta_j^* + \delta_i - \log(Q_{i-1}/Q_0). \square$$

We are now able to present our

ALGORITHM FOR COMPUTING $R(D > 10^6)$.

Initialization

Select a value for a constant c $(c > 1)$. Put $L = [cD^{1/4}] + 1$, $T = 1 + [\log 4\sqrt{D}/(2\log\tau)]$.

Step 1

By developing the continued fraction of ω, compute and store those ideals $\mathfrak{a}_i = [Q_{i-1}/r, (P_{i-1} + \sqrt{D})/r]$, where $i \leq t$ and $Q_{i-1} \leq d$. These ideals are stored as pairs (Q_{i-1}, P_{i-1}) which are sorted lexicographically. Call this list of ideals $\mathscr{T}$. Here, $t = s + T$, where s is selected such that $s = L$ or $L+1$, whichever has $Q_{s-1} \leq d$. (In view of (2.1) this must occur for at least one of the values L or $L+1$.) If $P_n = P_{n+1}$ for a minimal positive $n \leq t - 1$, then

$$R = \log(Q_0/Q_n) + 2\log\Psi_{n+1}$$

and we can terminate the algorithm. If $Q_m = Q_{m+1}$ for a minimal positive $m \leq t - 2$, then

$$R = \log(Q_0\psi_{m+1}/Q_m) + 2\log\Psi_{m+1}$$

and we can terminate the algorithm.

Step 2

Compute $(\mathfrak{b}_1, \chi_1) = \mathfrak{a}_s * \mathfrak{a}_s$. Put $X_1 = 1$, $j = 1$.

Step 3 (test step)

If $\mathfrak{b}_j \in \mathscr{T}$, then

$$R = 2j\log\Psi_s + j\log\chi_1 + \log X_j - \log\Psi_i$$

and we can terminate the algorithm. If $\bar{\mathfrak{b}}_j \in \mathscr{T}$, then

$$R = 2j\log\Psi_s + j\log\chi_1 + \log X_j + \log\Psi_i - \log(Q_{i-1}/Q_0)$$

and we can terminate the algorithm.

Step 4

Put

$$(b_{j+1}, \chi_{j+1}) = b_j * b_j,$$
$$X_{j+1} = X_j\chi_{j+1},$$
$$j \leftarrow j + 1$$

and go to Step 3.

Proof of Correctness. Certainly, if the value of R is determined by Step 1, then it is correct by (2.15) or (2.16). Suppose that this is not the case; then $\delta_s < R$.

Also, since $(D^{1/4}-2)\log\tau > .4 + \log D$ when $D > 10^6$, we have $\delta_s > \kappa + \log D$ ($\kappa = .4 > 0$). By the Corollary of Lemma 2.1 of [8] we have

$$\delta_{t+1} = \delta_{s+T+1} > \delta_s + T\log\tau > \delta_s + M,$$

where $M = \log 4\sqrt{D}/(2\log\tau)$. Thus, by Theorem 2.2 we must get some j such that $\mathfrak{b}_j \in \mathscr{T}$. From (2.19) we have

$$\begin{aligned}\delta_j^* &= j\delta_1^* + \sum_{i=2}^{j}\lambda_i = 2j\delta_s + j\lambda_1 + \sum_{i=2}^{j}\lambda_i \\ &= 2j\log\Psi_s + j\log\chi_1 + \log X_j;\end{aligned}$$

thus, by the Corollary of Theorem 2.2 we see that the algorithm computes R correctly. We also point out that by virtue of Lemma 2.1 we cannot have both $\mathfrak{b}_j$ and $\bar{\mathfrak{b}}_i$ in $\mathscr{T}$. □

This algorithm has the same order of complexity $O(D^{1/4+\varepsilon})$ as that given in [7]. The main difference here is that by using the same amount of storage space, we can step through our new algorithm in steps of size about $2\delta_s$ instead of δ_s. In practice, this improves the speed of the algorithm by a factor of about 35%.

3. Determination of When $h = 1$. Given the value of R, one can use the method of Williams and Broere [10] to determine h. However, the difficulty in using this technique is that it is very time-consuming. Since our concern here is to examine a great many fields, a more expeditious method is needed. As mentioned in the introduction, the problem is to estimate $L(1,\chi)$ sufficiently accurately that it should be possible to ascertain whether or not $h = 1$. In order to do this here, we make use of Oesterlé's [4] effective version of the Chebotarev density theorem. It must be emphasized, however, that for any given field $\mathscr{K} = \mathscr{Q}(\sqrt{D})$, this assumes the truth of the GRH on $\zeta_{\mathscr{K}}$. Thus, the method that we will describe here is correct if the GRH holds for all of the values of the radicand D that we consider.

For a given field $\mathscr{K}$ we set

$$F(Q) = \prod_{\substack{q=2 \\ q \text{ prime}}}^{Q} q/(q-(\Delta/q))$$

and

$$T(Q) = \prod_{\substack{q>Q \\ q \text{ prime}}} q/(q-(\Delta/q));$$

then

$$h = (F(Q)T(Q)\sqrt{\Delta})/2R. \tag{3.1}$$

Put $\tilde{h} = \mathrm{Ne}(F(Q)\sqrt{\Delta}/2R)$, where by $\mathrm{Ne}(x)$ we denote the nearest integer to x. Our problem is to be able to determine that value of Q such that if $\tilde{h} = 1$, then $h = 1$, and if $\tilde{h} \neq 1$, then $h \neq 1$.

Now if $\varepsilon(q) = (\Delta/q)$, we have

$$|\log T(Q)| = \left| -\sum_{q>Q} \log(1 - \varepsilon(q)/q) \right| < \left| \sum_{q>Q} (\varepsilon(q)/q + 1/q^2) \right|$$
$$< \left| \sum_{q>Q} \varepsilon(q)/q \right| + 1/Q.$$

By setting

$$C(x) = \log \Delta\{1/(\pi \log x) + 5.3/(\log x)^2\} + 4/\log x + 1/\pi,$$

we can use the idea of Cornell and Washington [2] to show that

$$\left| \sum_{q>Q} \varepsilon(q)/q \right| \leq C(Q)(4 + 3\log Q)/\sqrt{Q}.$$

If we put

$$B(Q) = C(Q)(4 + 3\log Q)/\sqrt{Q} + 1/Q,$$

then $|\log T(Q)| < B(Q)$ under the GRH on $\zeta_{\mathscr{K}}$.

We now require two simple lemmas.

LEMMA 3.1. *If* $|\log x| < \log(2/(1 + |y|))$, *where* $|y| < 1/2$, *then*

$$1/(2 + y) < x < 2/(1 + y).$$

Proof. Since

$$\log((1 + |y|)/2) < \log x < \log(2/(1 + |y|)),$$

we have

$$(1 + |y|)/2 < x < 2/(1 + |y|).$$

Now

$$(1 + |y|)/2 > 1/(2 - |y|) \geq 1/(2 + y),$$

and

$$2/(1 + |y|) \leq 2/(1 + y);$$

hence, the lemma follows. □

LEMMA 3.2. *If* $\tau = (F(Q)\sqrt{\Delta})/2R - \tilde{h}$ *and* $1/(2+\tau) < T(Q) < 2/(1+\tau)$, *then* $h = 1$ *if and only if* $\tilde{h} = 1$.

Proof. We first note that from (3.1) we get

$$h - \tilde{h} = h(1 - T(Q)^{-1}) + \tau \quad \text{and} \quad \tilde{h} = hT(Q)^{-1} - \tau.$$

Since $|\tau| < 1/2$, we have

$$\tau < (1 + \tau)/2 < T(Q)^{-1} < 2 + \tau;$$

thus, if $h = 1$, we get $0 < \tilde{h} < 2$ and therefore $\tilde{h} = 1$.

If $\tilde{h} = 1$, then

$$h = (\tau + 1)T(Q) < 2$$

and $h = 1$. □

If we now combine the results obtained above, we see that if $\Delta \leq B$, where B is some preassigned bound, and

$$\tau = (F(Q)\sqrt{\Delta})/2R - \tilde{h}, \qquad A(Q) < \log 2/(1 + |\tau|),$$

where

$$A(Q) = \frac{4\log B}{\pi\sqrt{Q}\log Q} + \frac{21.2\log B}{\sqrt{Q}(\log Q)^2} + \frac{15.9\log B}{\sqrt{Q}\log Q} + \frac{3\log B}{\pi\sqrt{Q}} + \frac{16}{\sqrt{Q}\log Q} + \frac{4}{\pi\sqrt{Q}} + \frac{12}{\sqrt{Q}} + \frac{3\log Q}{\pi\sqrt{Q}} + \frac{1}{Q},$$

then $h = 1$ if and only if $\tilde{h} = 1$.

In Tables 3.1 and 3.2 below we give for selected values of t and B, a prime Q such that $A(Q) < \log(2/(1+t))$ and the number of such primes $\pi(Q)$ up to Q.

$B = 10^9$ (for $D < 10^9$, $D \equiv 1 \pmod 4$)		
t	prime Q	π(Q)
.001	15299	1787
.005	15461	1806
.01	15667	1828
.05	17443	2006
.1	20111	2263
.2	26729	2934
.3	36653	3886
.4	52103	5328
.5	77929	7656

TABLE 3.1

$B = 4 \times 10^9$ (for $D < 10^9$, $D \equiv 2, 3 \pmod 4$)		
t	prime Q	π(Q)
.001	16673	1929
.005	16843	1949
.01	17077	1969
.05	19001	2159
.1	21787	2444
.2	29101	3163
.3	39901	4196
.4	56671	5746
.5	84731	8257

TABLE 3.2

Thus, if we wish to determine whether or not $h = 1$, we need only select the appropriate B, a value of t and evaluate $\tilde{h}$ and τ. If $|\tau| < t$ and $\tilde{h} = 1$, then $h = 1$; if $|\tau| < t$ and $\tilde{h} \neq 1$, then $h \neq 1$. If $|\tau| > t$, select the next t value until a value of τ is obtained such that $|\tau| < t$. In the next section we will discuss several details involved in the computer implementation of this algorithm.

4. Computer Implementation and Results. The algorithms for determining R and when $h = 1$ were coded in assembly language (double-precision floating point was used for the accumulation of R and $F(Q)$) and run on an Amdahl 5870 computer. In this section we discuss some of the techniques which were used to get the best possible performance out of these algorithms.

In order to calculate $\log \Psi_k$ or $\log X_k$ efficiently, we did not compute $\sum_{i=1}^{k-1} \log \psi_i$ or $\sum_{i=1}^{k} \log \chi_i$, i.e., a sum of logarithms. Since the logarithm routine is fairly expensive, we instead accumulated the products $\prod_{i=1}^{k-1} \psi_i$ and $\prod_{i=1}^{k} \chi_i$ and then took the logarithm of the product. However, since these products can get large enough to overflow a floating-point register, it was necessary to keep the exponent and fractional parts of the products separate. Each time a new term was multiplied to a product's fractional part, the resulting exponent was separated out and added to an integer sum-of-exponents variable (the fraction's exponent was set to 0). Taking $\log(\text{frac} \times 16^{\text{exp}}) = \log(\text{frac}) + (\text{exp}) \log 16$ was easy as $\log 16$ was precalculated. Thus only one log call was ever needed to evaluate a particular $\log \Psi_k$ or $\log X_k$.

As was done in [7] and [8], instead of actually conducting a preliminary sort in Step 1 of the Regulator Algorithm and then using a binary search, say, to determine whether or not $\mathfrak{b} \in \mathscr{T}$, we used hashing techniques. In practice, these searches can be much more rapidly undertaken by hashing on the last byte of the Q values.

In order to determine a good value of c to be used in the initialization step of the Regulator Algorithm, we conducted some preliminary numerical experiments. We summarize the results of these in Table 4.1.

I	J	c	t_1	t_3
10^7	10^6	1	21.40	—
		1.25	20.89	25.24
		1.5	20.92	24.70
		1.75	21.47	24.60
		2	22.18	25.01
		2.25	24.12	—
10^9	5×10^5	1	26.59	35.17
		1.25	25.28	31.97
		1.5	24.94	30.59
		1.75	25.24	30.02
		2	25.94	30.16

TABLE 4.1

For the value of c given in the third column we give the total time t_i in seconds needed to compute R for all of the primes $\equiv i \pmod 4$ in the interval $[I, I + J]$. As

a result of these calculations, we used $c = 1.5$ when $D \equiv 1 \pmod 4$ and $c = 1.75$ when $D \equiv 3 \pmod 4$.

Tests showed that the early implementations of our algorithms were very slow. In fact, over 95% of the time was being spent in the evaluation of $F(Q)$. This was because our routine for evaluating (Δ/q) was too slow, no matter what we tried. (We used variations on both the Jacobi method and the Euler criterion/power algorithm technique.) Our solution to this problem was to calculate $F(Q)$ for all D in a fixed interval under the assumption that $|\tau| \leq .01$. We did this by first precalculating all the quadratic residues for all the primes up to Q when $t = .01$ (see Tables 3.1 and 3.2). We could then use this information to rapidly accumulate $F(Q)$ for each D in the interval by multiplying each $F(Q)$ by $q/(q - (\Delta/q))$ with a single array look up. If it was necessary to go to a larger Q value ($|\tau| > .01$), we simply continued our computations on those particular D by using the Euler criterion/power algorithm technique to determine (Δ/q). By using an interval size 10^6 we cut our estimate of time needed to run this part of our program on all prime values of D up to 10^9 from 225 hours to 38 hours.

We also ran tests to see how frequently the use of $t = .01$ was good enough for determining when $h = 1$. We provide the results of these tests in Table 4.2. For these tests we used an interval size of 10^5.

Here, n_i is the number of primes $\equiv i \pmod 4$ in the interval between I and $I + 10^5$ for which we could determine whether or not $h = 1$ using the $|\tau|$ value given in the second column. Notice that 99% of the primes could be dealt with when $t = .1$ and over 90% could be handled with $t = .01$.

I	$\lvert\tau\rvert$	n_1	n_3
10^7	.01	2778 (90%)	2820 (92%)
	.05	251 (8%)	194 (6%)
	.1	30 (1%)	25 (1%)
	.2	12	17
	.3	4	3
	.4	0	0
	.5	0	0
		3075	3059
10^9	.01	2196 (91%)	2235 (92%)
	.05	173 (7%)	151 (6%)
	.1	29 (1%)	24 (1%)
	.2	10	6
	.3	1	4
	.4	1	1
	.5	1	0
		2411	2421

TABLE 4.2

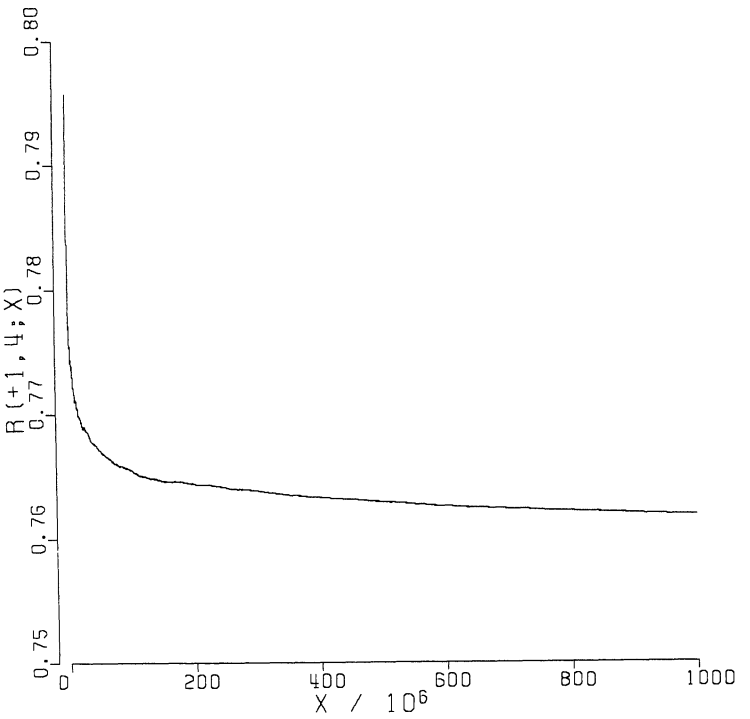

FIGURE 4.1

As mentioned above, we ran our programs for all prime values of $D < 10^9$. For those prime values $\equiv 1 \pmod 4$ we required a total of about 36 hours of computer time and for those $\equiv 3 \pmod 4$ we required a total of about 39.5 hours.

Denote by $\pi(i, 4; x)$ the number of primes up to x which are congruent to $i \pmod 4$ and denote by $f(i, 4; x)$ the number of those primes counted by $\pi(i, 4; x)$ such that the class number of the corresponding real quadratic field is one. Put

$$R(i, 4; x) = f(i, 4; x)/\pi(i, 4; x).$$

x/10^6	π(-1,4;x)	f(-1,4;x)	R(-1,4;x)	π(+1,4;x)	f(+1,4;x)	R(+1,4;x)
10	332398	255697	0.7692495	332180	256346	0.7717081
50	1500681	1148210	0.7651260	1500452	1151040	0.7671288
100	2880950	2201430	0.7641334	2880504	2205113	0.7655303
150	4222411	3223457	0.7634162	4221984	3228344	0.7646509
200	5540116	4226819	0.7629477	5538820	4233706	0.7643697
250	6840343	5216929	0.7626707	6838974	5225613	0.7640931
300	8126606	6195760	0.7624044	8125718	6206614	0.7638235
350	9402353	7166342	0.7621860	9401172	7177686	0.7634884
400	10668718	8129627	0.7620060	10667607	8142331	0.7632762
450	11927101	9086081	0.7618013	11925936	9100975	0.7631246
500	13179058	10037729	0.7616424	13176808	10052888	0.7629229
550	14423312	10983002	0.7614757	14422043	11000483	0.7627548
600	15662772	11925126	0.7613675	15661930	11943522	0.7625830
650	16897400	12863448	0.7612679	16895994	12882297	0.7624468
700	18127414	13799009	0.7612233	18125516	13817870	0.7623435
750	19352799	14730095	0.7611351	19350381	14749979	0.7622578
800	20573718	15658228	0.7610792	20572460	15679417	0.7621557
850	21791649	16584780	0.7610613	21790316	16605975	0.7620805
900	23005255	17505721	0.7609444	23003959	17528770	0.7619893
950	24215752	18425396	0.7608847	24215718	18449756	0.7618918
1000	25424042	19343291	0.7608267	25423491	19368166	0.7618217

TABLE 4.3

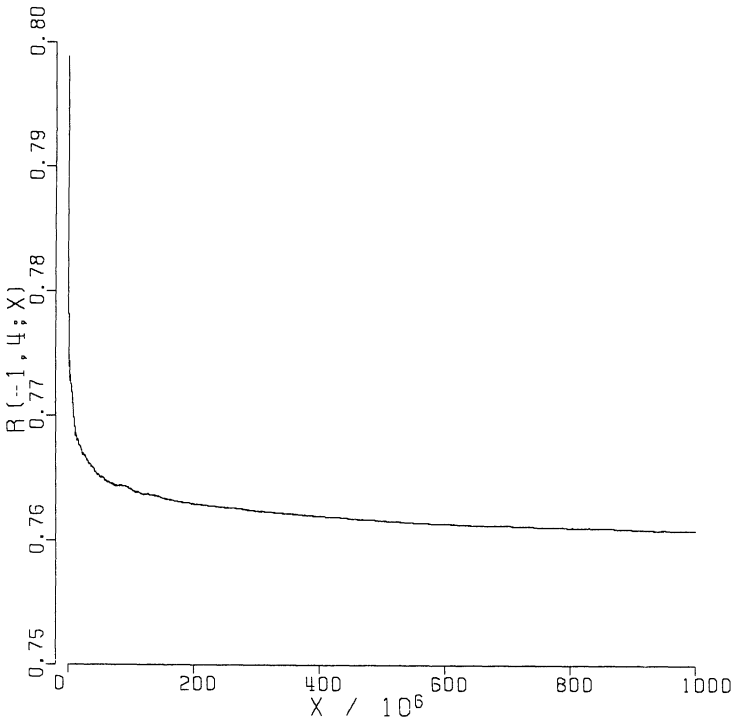

FIGURE 4.2

In Table 4.3 we give some excerpts from our calculations of $R(i,4;x)$. During the process of conducting these investigations we noticed two errors in Table 1 of [9]. The values for $f(1,4;x)$ are all too small by 1 because the program used to produce this table did not get the correct value of h for $D=5$. (It obtained $h=0$, not 1, and since the program only produced a count, this error was not noticed at the time.) The values for $\pi(1,4;x)$, $f(1,4;x)$ and $r(1,4;x)$ are incorrect for $x=25\times 10^6$; this was due to an error in copying from the larger table produced by machine to the smaller Table 1.

We also provide some graphs of $R(i,4;x)$ in Figures 4.1 and 4.2.

At the suggestion of Henri Cohen we also attempted to fit our values of $R(i,4;x)$ $(i=1,-1)$ to a curve of the form $a+bx^{-\alpha}$. This was done by using a golden ratio search technique to determine that α value which yielded the minimum error, where by the error we mean the sum of the squares of the vertical deviations of the data points $(x^{-\alpha}, R(i,4;x))$ with $x=10^5 j$ and $j=1,2,3,\ldots,10^4$ from the least-squares straight line fitted to those points. In Figures 4.3 and 4.4 we show plots of $R(i,4;x)$ against $x^{-\alpha}$ for the α value that we obtained. On the same figures we have also drawn the least-squares straight line described above. Notice that in both cases the y-intercept is somewhat larger than .75446. This, of course, could be the result of the naivety of our assumption that $R(i,4;x)$ can be accurately described by a curve as simple as $y=a+bx^{-\alpha}$.

For given fixed interval size I let

$$\pi'(i,4;x)=\pi(i,4;x+I)-\pi(i,4;x),$$
$$f'(i,4;x)=f(i,4;x+I)-f(i,4;x),$$
$$R'(i,4;x)=f'(i,4;x)/\pi'(i,4;x).$$

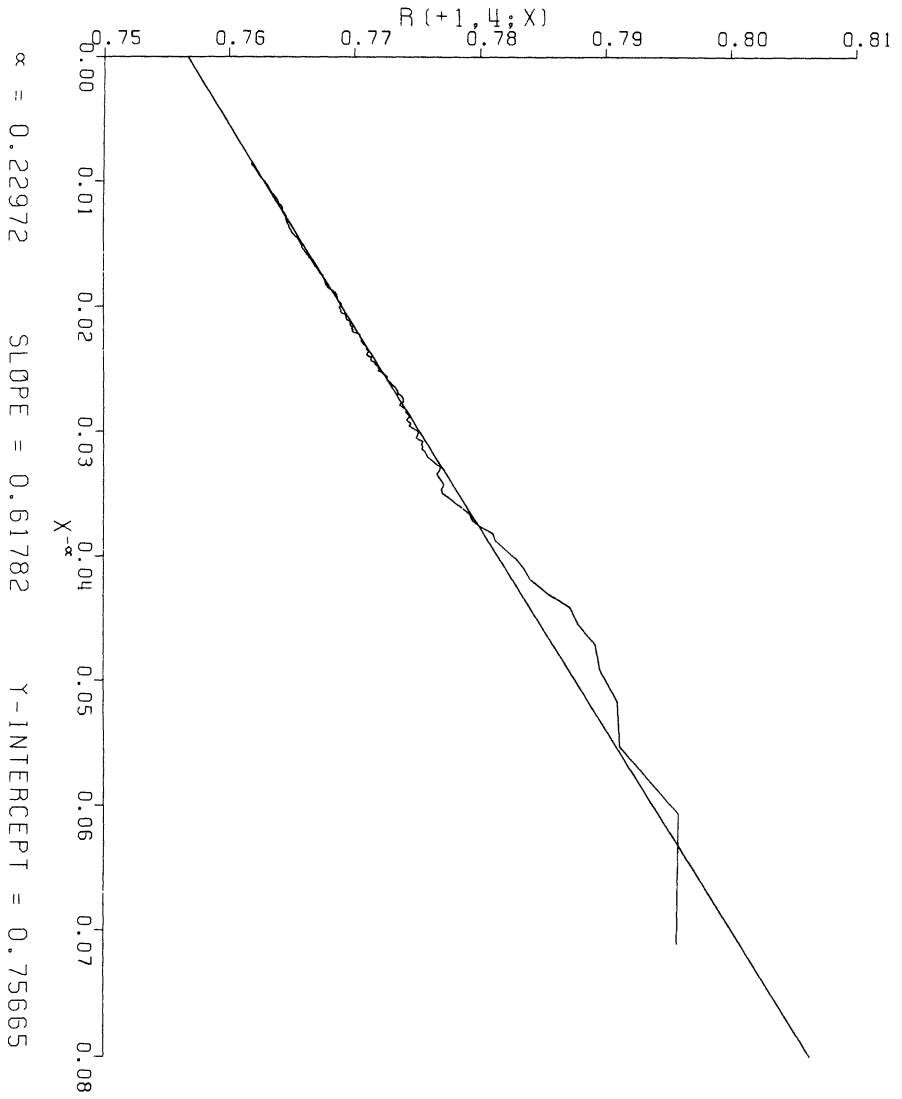

FIGURE 4.3

To get a further idea of how the real quadratic fields of class number one are distributed, we wrote a higher-precision version of the programs described above and sampled intervals of size $I = 10^7$ at values of $x = 10^i$ $(i = 9, 10, 11, \ldots, 16)$. In Table 4.4 we present the results of these calculations. By $t(i, 4; x)$ we denote the time in minutes that our programs required to determine $R'(i, 4; x)$. In spite of some fluctuations, it still appears that the overall tendency of $R(i, 4; x)$ is to decrease. Indeed, none of the calculations presented here seems to provide any inconsistency with the belief that $R(i, 4; x)$ tends to approach .75446 very, very slowly.

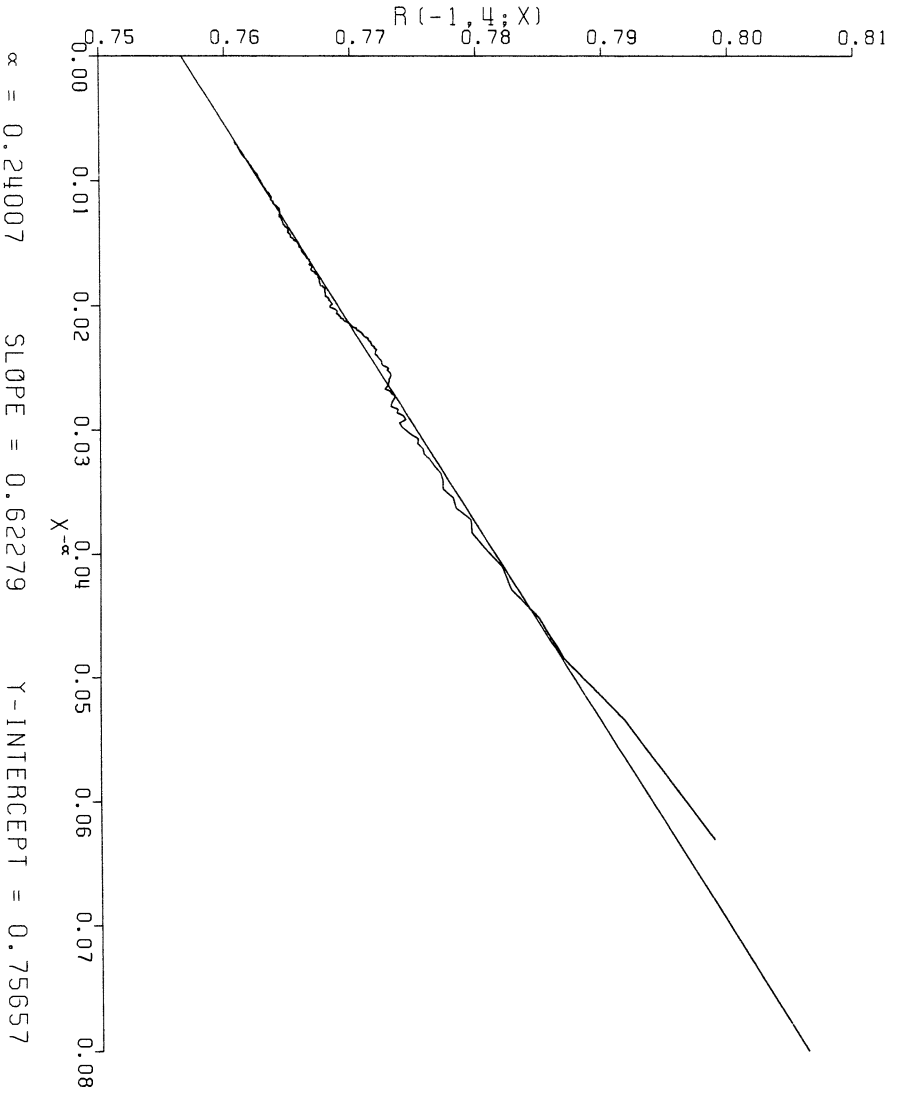

FIGURE 4.4

$x/10^9$	π'(-1, 4; x)	f'(-1, 4; x)	R'(-1, 4; x)	t(-1, 4; x)	π'(1, 4; x)	f'(1, 4; x)	R'(1, 4; x)	t(1, 4; x)
1	241505	183299	.75899	53	240944	183084	.74986	50
10	271319	164904	.75881	61	217331	164650	.75760	55
10^2	197381	149300	.75641	72	197020	149039	.75647	63
10^3	180913	136536	.75504	94	180813	136567	.75513	82
10^4	167168	126296	.75550	138	167144	126234	.75524	117
10^5	155353	117451	.75603	226	155229	117163	.75478	200
10^6	144816	109113	.75346	465	144578	109414	.75678	430
10^7	135906	102648	.75529	976	135991	102811	.75601	963

TABLE 4.4

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

1. H. COHEN & H. W. LENSTRA, JR., "Heuristics on class groups of number fields," *Number Theory* (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer-Verlag, Berlin and New York, 1984, pp. 33–62.

2. G. CORNELL & L. C. WASHINGTON, "Class numbers of cyclotomic fields," *J. Number Theory*, v. 21, 1985, pp. 260–274.

3. H. W. LENSTRA, JR., "On the calculation of regulators and class numbers of quadratic fields," *London Math. Soc. Lecture Note Ser.*, v. 56, 1982, pp. 123–150.

4. J. OESTERLÉ, "Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée," *Astérisque*, v. 61, 1979, pp. 165–167.

5. R. J. SCHOOF, "Quadratic fields and factorization," *Computational Methods in Number Theory* (H. W. Lenstra, Jr. and R. Tijdemann, eds.), Math. Centrum Tracts, Number 155, Part II, Amsterdam, 1983, pp. 235–286.

6. D. SHANKS, "The infrastructure of a real quadratic field and its applications," *Proc. 1972 Number Theory Conference* (*Univ. Colorado, Boulder*, 1972), pp. 217–224, Univ. Colorado, Boulder, 1972.

7. A. J. STEPHENS & H. C. WILLIAMS, "Some computational results on a problem concerning powerful numbers," *Math. Comp.*, v. 50, 1988, pp. 619–632.

8. A. J. STEPHENS & H. C. WILLIAMS, "Some computational results on a problem of Eisenstein," *Proc. International Number Theory Conf.*, Laval University, Québec, 1987. (To appear.)

9. M. TENNENHOUSE & H. C. WILLIAMS, "A note on class-number one in certain real quadratic and pure cubic fields," *Math. Comp.*, v. 46, 1986, pp. 333–336.

10. H. C. WILLIAMS & J. BROERE, "A computational technique for evaluating $L(1, \chi)$ and the class number of a real quadratic field," *Math. Comp.*, v. 30, 1976, pp. 887–893.

11. H. C. WILLIAMS & M. C. WUNDERLICH, "On the parallel generation of the residues for the continued fraction factoring algorithm," *Math. Comp.*, v. 48, 1987, pp. 405–423.