An Investigation of Bounds for the Regulator of Quadratic Fields

Michael J. Jacobson, Jr., Richard F. Lukes and Hugh C. Williams

CONTENTS

It is well known that the nontorsion part of the unit group of a real quadratic field $\mathcal{K}$ is cyclic. With no loss of generality we may assume that it has a generator $\varepsilon_0 > 1$, called the fundamental unit of $\mathcal{K}$. The natural logarithm of ε_0 is called the regulator R of $\mathcal{K}$. This paper considers the following problems: How large, and how small, can R get? And how often?

The answer is simple for the problem of how small R can be, but seems to be extremely difficult for the question of how large R can get. In order to investigate this, we conducted several large-scale numerical experiments, involving the Extended Riemann Hypothesis and the Cohen–Lenstra class number heuristics. These experiments provide numerical confirmation for what is currently believed about the magnitude of R.

1. INTRODUCTION

Let D denote a square-free integer and let $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ be the quadratic field formed by adjoining $\sqrt{D}$ to the rationals $\mathbb{Q}$. Set

$$r = \begin{cases} 2 & \text{if } D \equiv 1 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Then $\Delta = (2/r)^2 D$ is the *discriminant* of $\mathcal{K}$. If

$$\omega = \tfrac{1}{2}(\Delta + \sqrt{\Delta}),$$

then

$$\mathcal{O} = \mathbb{Z} + \omega\mathbb{Z}$$

is the *maximal order* (the ring of algebraic integers) of $\mathcal{K}$. If $\alpha \in \mathcal{K}$ we denote, as usual, the norm of α by $N(\alpha) = \alpha\bar{\alpha}$, where $\bar{\alpha}$ is the conjugate of α.

If $\mathcal{O}^*$ is the group of units in $\mathcal{O}$ and $\Delta > 0$, we have $\mathcal{O}^* = \langle -1, \varepsilon_0 \rangle$, for a uniquely determined $\varepsilon_0 > 1$, called the *fundamental unit* of $\mathcal{K}$. Let $R = \log \varepsilon_0$ denote the *regulator* of $\mathcal{K}$. Since $\varepsilon_0 \in \mathcal{O}$,

1058-6458/96 \$0.50 per page

we have $\varepsilon_0 = \frac{1}{2}(x + y\sqrt{\Delta})$, where $x, y \in \mathbb{Z}$. Also, since $|N(\varepsilon_0)| = \varepsilon_0|\bar{\varepsilon}_0| = 1$, it is easy to see that

$$\varepsilon_0 - 1 < x < \varepsilon_0 + 1,$$
$$\frac{\varepsilon_0 - 1}{\sqrt{\Delta}} < y < \frac{\varepsilon_0 + 1}{\sqrt{\Delta}}.$$

Thus $x, y > 0$, and the regulator provides us with a good estimate for the value of $\log x$ and $\log(\sqrt{\Delta}y)$. Because of the importance of the fundamental unit, particularly in characterizing all solutions of diophantine equations of the form $N(\alpha) = k$, where $\alpha \in \mathcal{O}$ and $k \in \mathbb{Z}$, it is of considerable interest to study the size of R.

When $\Delta = x^2 + 4$, where $2 \nmid x$, it is not difficult to show that $\varepsilon_0 = \frac{1}{2}(x + \sqrt{\Delta})$. Thus, in this case, we have

$$\varepsilon_0 = \tfrac{1}{2}(\sqrt{\Delta - 4} + \sqrt{\Delta})$$

and

$$R = \log\bigl(\tfrac{1}{2}(\sqrt{\Delta - 4} + \sqrt{\Delta})\bigr).$$

In general, since $\varepsilon_0 = \frac{1}{2}(x + y\sqrt{\Delta})$ with $x, y > 0$ and $|\varepsilon_0\bar{\varepsilon}_0| = 1$, we have $x = \sqrt{y^2\Delta \pm 4}$ and

$$\varepsilon_o = \frac{\sqrt{y^2\Delta \pm 4} + y\sqrt{\Delta}}{2} \geq \frac{\sqrt{\Delta - 4} + \sqrt{\Delta}}{2}.$$

Hence

$$R \geq \log\bigl(\tfrac{1}{2}(\sqrt{\Delta - 4} + \sqrt{\Delta})\bigr). \tag{1.1}$$

Since $x^2 + 4$ is square-free infinitely often for odd x (see [Nagell 1922], for example), we see that equality in (1.1) is achieved infinitely often. Consequently, we know just how small R can be as a function of Δ.

The question of how large R can be is much more difficult. By a result of Hua [1982, p. 329], we can certainly say that

$$R < \sqrt{\tfrac{1}{2}\Delta}\,\bigl(\tfrac{1}{2}\log\Delta + 1\bigr),$$

but this is not very near to a sharp bound like (1.1). Thus, we are left with two questions:

(1) What is the largest value that R can attain as a function of Δ?
(2) How often does R become that large?

Both questions turn out to be extremely difficult, as we can see by examining the analytic class number formula

$$2Rh = \sqrt{\Delta}L(1, \chi_\Delta). \tag{1.2}$$

Here h is the class number of $\mathcal{K}$ and

$$L(1, \chi_\Delta) = \lim_{s\to 1} L(s, \chi_\Delta),$$

where the Dirichlet L-function is defined by

$$L(s, \chi_\Delta) = \sum_{n=1}^{\infty} \frac{\chi_\Delta(n)}{n^s} = \prod_p \Bigl(1 - \frac{\chi_\Delta(p)}{p^s}\Bigr)^{-1}. \tag{1.3}$$

The character χ_Δ here is the Kronecker symbol (Δ/n); the Euler product on the right of (1.3) is taken over all the primes p. Thus, in order for R to be large it is necessary for h to be small and $L(1, \chi_\Delta)$ to be large. How often h can be small and how large (and how often) $L(1, \chi_\Delta)$ can be are very deep and difficult questions in number theory. For example, the famous Gauss Conjecture asserts that $h = 1$ infinitely often, and the Extended Riemann Hypothesis (ERH) provides us with quite close bounds on $L(1, \chi_\Delta)$.

This article contains the results of some numerical experiments that we conducted in order to investigate problems (1) and (2). We first describe a large-scale computational trial that we implemented to verify the Cohen–Lenstra heuristics on the distribution of the odd part of the class number. We will next discuss further numerical experiments in which we attempted to see how closely the bounds of [Littlewood 1928] and [Shanks 1973] come to bracketing the value of $L(1, \chi_\Delta)$.

2. COMPUTATION OF R

The basic idea we used in our computation of h was to first compute R and then $L(1, \chi_\Delta)$ to sufficient accuracy that it is possible to use (1.2) to determine the integer h. In this section we discuss how we compute R using a version of Lenstra's idea [1982], as described in [Mollin and Williams, p. 290].

The first step of this process is to estimate the value of $L(1,\chi_\Delta)$. Here, instead of using a truncated Euler product and Oesterlé's results [1979] to estimate the error as in [Mollin and Williams], we use an idea due to Bach [Bach 1994]. This is based on using a weighted average of truncated Euler products to compute an approximation $S(Q,\Delta)$ of $\log L(1,\chi_\Delta)$ which, under the ERH, has relative error $O(\log\Delta/(\sqrt{Q}\log Q))$. For some preselected value of Q we compute

$$C(Q)=\sum_{i=0}^{Q-1}(i+Q)\log(i+Q)=\sum_{i=Q}^{2Q-1} i\log i$$

and weights

$$a_j=\frac{(Q+j)\log(Q+j)}{C(Q)}.$$

According to the explicit version of [Bach 1994, Theorem 9.2], under the ERH we have

$$\left|\log L(1,\chi_\Delta)-\sum_{i=0}^{Q-1} a_i\log B(Q+i)\right|\le A(Q,\Delta), \tag{2.1}$$

where

$$A(Q,\Delta)=\frac{A\log\Delta+B}{\log Q\sqrt{Q}}. \tag{2.2}$$

A and B can be determined, depending on the value of Q, by using Table 3 in [Bach 1994]. Also, $B(x)$ is defined by the truncated Euler product

$$B(x)=\prod_{p<x}\Big(1-\frac{(\Delta/p)}{p}\Big)^{-1},$$

where the product is taken over all primes $p<x$.

One of the real bottlenecks in computing estimates like

$$S(Q,\Delta)=\sum_{i=0}^{Q-1} a_i\log B(Q+i)$$

is the evaluation of the many Kronecker (Legendre) symbols (Δ/q). In order to accelerate this process, we first note the easily shown identity

$$S(Q,\Delta)=\sum_{p\le 2Q-1} w(p)\log\Big(1-\frac{(\Delta/p)}{p}\Big)^{-1},$$

where

$$w(p)=\begin{cases}1 & \text{for } p<Q,\\ \sum_{p-Q+1}^{Q-1} a_j & \text{for } Q\le p<2Q-1.\end{cases}$$

Our technique of determining $S(Q,\Delta)$ consisted of computing and storing in a large table the quadratic residues and nonresidues and the values of $w(p)\log(p/(p-1))$ and $w(p)\log(p/(p+1))$ for all the primes $p\le 10000$. We could then find the value of $w(p)\log(p/(p-(\Delta/p)))$ by little more than a single table look-up for each prime $p\le 10000$; thus, we could easily evaluate

$$S(Q,\Delta)=\sum_{p\le 2Q-1} w(p)\log\Big(\frac{p}{p-(\Delta/p)}\Big)$$

and then compute an estimate of $L(1,\chi_\Delta)$ by a single exponentiation.

After conducting some preliminary experiments we found that a value of $Q=2000$ was very often sufficient (for $\Delta<10^9$) to estimate $L(1,\chi_\Delta)$ in order to establish $h=1$. This is a huge improvement over the truncated product method used in [Stephens and Williams 1988], where all primes less than 18000 had to be used in the estimate (compared with only 4000 using Bach's method). In fact, we found that using $Q=5000$ (i.e., primes less than 10000) was often sufficient to establish $h\le 3$, and that this resulted in the best performance of our algorithm.

For fixed Q and Δ, put $E=\frac{1}{2}\sqrt{\Delta}\exp(S(Q,\Delta))$. Then $hR\approx E$. By using (1.2) and (2.1) we know (under the ERH) that

$$|E-hR|<L^2, \tag{2.3}$$

where

$$L^2=E\max\{e^{A(Q,\Delta)}-1,\,1-e^{-A(Q,\Delta)}\}.$$

In order to get some indication of the growth rate of L (for $Q = 5000$), we evaluated it for prime radicands D only, in various intervals: see Table 1.

interval	max(L)	avg(L)
1	26.01440	10.73694
101	99.76966	50.64988
201	120.47460	61.27755
301	135.44843	68.64010
401	146.94061	74.26657
501	157.06318	78.86076
601	166.13391	82.86471
701	172.31836	86.53736
801	176.91473	89.52843
901	183.47702	92.59853
1000	191.06620	95.27484

TABLE 1. Growth of L. Here and throughout the article, "interval i" is the set of all prime values of D such that $(i-1)\times 10^6 < D < i \times 10^6$. The second and third columns give the maximum and average values of L found in each interval.

With the value of L computed above we calculated the regulator by using the modified version of the second algorithm in [Mollin and Williams, § 7]. This algorithm determines a value for $h^*R < E + L^2$, where h^* is some integer. It then finds the value of h^* and thus R. In particular, if $R < E/\sqrt{L}$, this algorithm will determine R quickly. However, usually we have $R \geq E/\sqrt{L}$. In this case the set of all primes $q_1 = 2$, $q_2 = 3, \ldots, q_n < B = \sqrt{L} + L^2\sqrt{L}/E$ must be computed. It is then necessary to check for each of these primes $q < B$ whether any reduced principal ideal $\mathfrak{a}$ at a distance from $\mathfrak{a}_1 = (1)$ very close to h^*R/q is such that $\mathfrak{a} = \mathfrak{a}_1$. If so, q divides h^*; otherwise it doesn't. If $q \mid h^*$ we must also check the reduced principal ideals at distance h^*R/q^2, h^*R/q^3, etc., until we find one equal to $\mathfrak{a}_1$ at distance close to h^*R/q^α, but we do not find any at distance close to $h^*R/q^{\alpha+1}$. Then q^α exactly divides h^*: in symbols, $q^\alpha \,\|\, h^*$. Since $h^* < B$, we must ultimately find

$$h^* = \prod_{i=1}^{n} q_i^{\alpha_i}.$$

Of course, if we find that $q^\alpha \,\|\, h^*$, then $h^*/q^\alpha < B/q^\alpha$, allowing us to replace B by B/q^α.

It was this latter process that we modified. For each prime $q_u < B$, instead of finding a reduced principal ideal $\mathfrak{a}_m$ such that δ_m, the distance of $\mathfrak{a}_m$ from $\mathfrak{a}_1$ [Mollin and Williams, p. 285], is such that $\delta_m \approx h^*R/q_u$, we determine a reduced principal ideal $\mathfrak{a}_{j_u}$ such that

$$\frac{h^*R}{q_u} < \delta_{j_u} < \frac{h^*R}{q_u} + \delta_t.$$

Here δ_t is that distance such that $\delta_t < L < \delta_{t+1}$. We next produce a list $\mathcal{I}$ of reduced principal ideals $\mathfrak{a}_{t_0}, \mathfrak{a}_{t_1}, \mathfrak{a}_{t_2}, \ldots, \mathfrak{a}_{t_m}$ such that $\mathfrak{a}_{t_0} = \mathfrak{a}_t$, $\delta_{t_k} \approx 2\delta_{t_{k-1}}$ and

$$\delta_{t_{m-1}} < \tfrac{1}{2}h^*R < \delta_{t_m}.$$

In order to determine h^*R, the list $\mathcal{T}$ made up of each reduced principal ideal $\mathfrak{a}_k$ and its distance δ_k such that $\delta_k < L$ had to be computed and stored; hence, we may assume that this list is still in existence. If q_u divides h^*, then $\mathfrak{a}_{j_u}$ must be in $\mathcal{T}$ and

$$\delta_{j_u} = \frac{h^*R}{q_u} + \delta_k$$

when $\mathfrak{a}_{j_u} = \mathfrak{a}_k$. If, from the next prime, we have an ideal $\mathfrak{a}_{j_{u+1}}$ such that

$$\frac{h^*R}{q_{u+1}} < \delta_{j_{u+1}} < \frac{h^*R}{q_{u+1}} + \delta_t,$$

we notice that, if we have a reduced principal ideal $\mathfrak{a}_{i_u}$ with distance δ_{i_u} such that

$$\delta_{i_u} \approx \frac{h^*R}{q_u} - \delta_{j_{u+1}},$$

$$\delta_{i_u} < \frac{h^*R}{q_u} - \delta_{j_{u+1}}$$

and

$$\frac{h^*R}{q_u} < \delta_{i_u} + \delta_{j_{u+1}} < \frac{h^*R}{q_u} + \delta_t,$$

we can then set $\mathfrak{a}_{j_u}$ to be a reduced ideal equivalent to $\mathfrak{a}_{i_u}\mathfrak{a}_{j_{u+1}}$ with $\delta_{j_u} \approx \delta_{i_u} + \delta_{j_{u+1}}$ and

$$\frac{h^*R}{q_u} < \delta_{j_u} < \frac{h^*R}{q_u} + \delta_t.$$

Now suppose we let $h^*R/q_u - \delta_{j_{u+1}} = \rho\delta_t$, and put $s = \lfloor \rho \rfloor + 1$. If we represent s in binary as

$$s = b_r 2^r + b_{r-1}2^{r-1} + \ldots + b_o,$$

where $b_r = 1$ and $b_j = 0, 1$ for $j = 0, 1, 2, \ldots, r-1$, then

$$s\delta_t = b_r 2^r \delta_t + b_{r-1}2^{r-1}\delta_t + \cdots + b_o\delta_t.$$

In our list $\mathcal{I}$ we have $\delta_{t_k} \approx 2\delta_{t_{k-1}}$, so we can find $\mathfrak{a}_{i_u}$ with distance $\delta_{i_u} \approx \rho\delta_t$ by simply computing a reduced ideal equivalent to

$$\prod_{\substack{j=0\\ b_j=1}}^{r} \mathfrak{a}_{t_j}^{b_j}.$$

Thus, starting with $u = n$, we first find a reduced principal ideal $\mathfrak{a}_{j_u}$ with distance $\delta_{j_u} \approx E/q_n$; we can then determine $\mathfrak{a}_{j_{u-1}}, \mathfrak{a}_{j_{u-2}}, \ldots$ by the method described above. Whenever we get $\mathfrak{a}_{j_v} = \mathfrak{a}_k$, where $\mathfrak{a}_k \in \mathcal{T}$, then q_v divides h^*. We then replace E by E/q_v and B by B/q_v and repeat the process, starting at q_v, until we find α such that $q_v^\alpha \,\|\, h^*$. When this procedure has been done for all primes $q_1, q_2, \ldots, q_n < B$ or $B = 1$, we will have h^*.

To ensure that this modified algorithm is in fact faster than the unmodified algorithm or even Algorithm 7.1 of [Mollin and Williams], we programmed all three in C and ran them on an IBM RS6000/590 workstation. Algorithm 7.1 computes R with time complexity $O(D^{1/4+\varepsilon})$; the unmodified algorithm mentioned above and the modified version both execute in time $O(D^{1/5+\varepsilon})$ under the ERH. In both of these cases the computed value of R is provably correct; the ERH is needed only for the complexity estimate. The modified version was always faster than the unmodified version, and except for the smallest values of D was the fastest overall. Algorithm 7.1 was the best for small D.

3. EVALUATION OF h

For a given D with $Q = 5000$, put

$$\tilde{h} = \text{round}\left(\frac{\sqrt{\Delta}\exp(S(Q,\Delta))}{2R}\right),$$

where by round(x) we denote the nearest integer to x. When $\tilde{h}$ is large, say $\tilde{h} > D^{1/8}$, it is often very time-consuming to produce a new value for $S(Q,\Delta)$ (with a larger Q value) such that

$$h = \text{round}\left(\frac{\sqrt{\Delta}\exp(S(Q,\Delta))}{2R}\right).$$

This problem can, to a very large extent, be overcome by first finding a factor h_1 of h such that h/h_1 is small.

Since, by the heuristics of Cohen and Lenstra [1983; 1984], we expect that the class group of $\mathcal{K}$ is very frequently cyclic, finding such an h_1 is usually not very difficult. We simply select an ideal $\mathfrak{a}$ lying over a prime q where $(D/q) = 1$. We then compute a reduced ideal $\mathfrak{b} \sim \mathfrak{a}^{\tilde{h}}$. Often $\mathfrak{b} \sim (1)$, in which case we can put $m = \tilde{h}$. If $\mathfrak{b} \not\sim (1)$, we compute $\mathfrak{b}_i \sim \mathfrak{b}\mathfrak{a}^i$, $\mathfrak{b}_{-i} \sim \mathfrak{b}\overline{\mathfrak{a}}^i$ until we find $\mathfrak{b}_i \sim (1)$ or $\mathfrak{b}_{-i} \sim (1)$. In the first case we put $m = \tilde{h} + i$ and in the second we put $m = \tilde{h} - i$.

Since we were confining our attention to fields with $D < 10^9$, we were able to check for ideal principality by searching an ordered list of all the reduced principal ideals. This technique was feasible because fields with $\tilde{h}$ relatively large (say $\tilde{h} > 3$) have relatively few principal ideals.

The value of m here is very often the class number; however, we must search over all the divisors of m to find the least k such that $\mathfrak{a}^k \sim (1)$. We now know that k divides h. If k is too small, we repeat the above process for other prime ideals and take as our value of h_1 the least common multiple of all the k values that we find. We did this until we found $h_1 > \frac{1}{3}\tilde{h}$. This was possible in all but a few cases which were handled separately. We seldom had to use more than one trial ideal, but occasionally as many as 12 were needed.

We also experimented with using h^* instead of $\tilde{h}$. For fields with large h, the value of h^* is usually a better approximation to h than $\tilde{h}$; thus, fewer ideal multiplications are needed to find m. However, when h is large, often R is determined immediately from the list $\mathcal{T}$ [Mollin and Williams] and

h^* is never evaluated. Hence no significant savings occurred on using h^* instead of $\tilde{h}$.

Once the regulator R and a value for $h_1 > \tilde{h}/3$ had been determined, we used Algorithm 3.1 to find h.

Algorithm 3.1 (Class Number of $\mathbb{Q}(\sqrt{D})$). Input: Δ, the discriminant of a real quadratic field.
Output: h and R.
- Set $Q = 5000$. Compute $S(Q, \Delta)$, R, and h_1 as described above.
- Repeat:
  - Compute $F = \sqrt{\Delta}\exp(S(Q,\Delta))/(2Rh_1)$.
  - Set $\tilde{h}_2 = \text{round}\,(F)$ and $\kappa = F - \tilde{h}_2$.
  - If $A(Q,\Delta) < \log\bigl((\tilde{h}_2+1)/(\tilde{h}_2+|\kappa|)\bigr)$, output $h = \tilde{h}_2 h_1$ and terminate; otherwise, set $Q = Q + 5000$, recompute $S(Q,\Delta)$, and return to beginning of loop.

Only very rarely did we have to go beyond the $Q = 5000$ used in the initial approximation to $\log L(1, \chi_\Delta)$: typically, for less than 10 out of approximately 50000 fields examined in each interval, as compared to less than 120 fields using truncated Euler products with $Q = 18000$. A more significant improvement is the maximum Q values required in an interval, which are much smaller than those required by the truncated product method. This is important because Bach's method requires the whole approximation to be recomputed in these cases, whereas a truncated product approximation can be improved simply by adding more terms. However, since we rarely require more accuracy and, if we do, the Q value needed is usually fairly small, our algorithm still runs faster using Bach's method. In these cases we used the usual Jacobi algorithm to evaluate the Legendre symbols (Δ/q). We emphasize here that the values of these class numbers are dependent on the truth of the ERH; however, given the discussion in [Shanks 1971], it would be a most unusual event, should the ERH be false, for any of the class numbers computed by this technique to be incorrect, assuming that the calculations are carried out correctly.

The algorithms for determining h_1 and h were also coded in C and run on an IBM RS6000/590 workstation. Using Bach's method, our algorithms executed about 1.5 times as quickly as they did using the truncated Euler product method.

4. THE COHEN–LENSTRA HEURISTICS

Let $\boldsymbol{G}$ be the class group of $\mathcal{K}$ and let $\boldsymbol{G}^*$ be the odd part of $\boldsymbol{G}$. Cohen and Lenstra [1983; 1984] provide some heuristics on the distribution of various $\boldsymbol{G}^*$. For example, if we define

$$w(n) = \prod_{p^\alpha \,\|\, n} \frac{1}{p^\alpha(1-1/p)(1-1/p^2)\ldots(1-1/p^\alpha)},$$

the probability that $h^* = |\boldsymbol{G}^*|$ is equal to k is

$$\text{Prob}(h^* = k) = \frac{Cw(k)}{k}, \tag{4.1}$$

where $C = .754458173\ldots$ Since $w(1) = 1$, we see that this result would predict that $h^* = 1$ about 75% of the time, a figure supported by the computations in [Stephens and Williams 1988]. In fact, under this heuristic we would expect that the probability that h^* exceeds x is

$$\text{Prob}(h^* > x) = C \sum_{\substack{j>x \\ j \text{ odd}}}^{\infty} \frac{w(j)}{j}. \tag{4.2}$$

Now, if we put

$$W(x) = \sum_{\substack{n>x \\ n \text{ odd}}} w(n),$$

we can use standard analytic methods such as those employed in [Landau 1936] to show that there exist constants E_1 and E_2 such that

$$W(x) = E_1 \log x + E_2 + O\Bigl(\frac{\log x}{x}\Bigr), \tag{4.3}$$

where

$$E_1 = (2C)^{-1} = \eta_\infty(2)C_\infty,$$
$$C_\infty = \prod_{j=1}^{\infty} \zeta(j+1) = 2.294856589\ldots,$$
$$\eta_\infty(2) = \prod_{i=1}^{\infty} \left(1 - 2^{-i}\right) = .288788095\ldots$$

By using partial summation on (4.2) and the result of (4.3) we get

$$\mathrm{Prob}(h^* > x) = \frac{1}{2x} + O\Big(\frac{\log x}{x^2}\Big). \qquad (4.4)$$

Thus, under the Cohen–Lenstra heuristics we'd expect that h^* is most likely to be small. Since $\mathrm{Prob}(h^* = 1) \approx \frac{3}{4}$, we will write this as

$$1 - \mathrm{Prob}(h^* \le x) = \frac{1}{2x+2} + O\Big(\frac{\log x}{x^2}\Big).$$

Thus we would expect that

$$k+1 = \frac{1}{2}\left(\frac{1}{1 - \mathrm{Prob}(h^* \le k)}\right) + O\Big(\frac{\log k}{k^2}\Big), \qquad (4.5)$$

a result that can be used to test the accuracy of (4.4).

Let $h(p)$ be the class number of the field $\mathbb{Q}(\sqrt{D})$, where p is a prime. By using some further assumptions, Cohen was able to show that

$$\sum_{\substack{p \le x \\ p \equiv 1 \bmod 4}} h(p) \sim \tfrac{1}{8}x, \qquad (4.6)$$

a result conjectured by Hooley [1984] at about the same time.

In order to test the validity of (4.1), (4.5) and (4.6), we computed all the class numbers for all the fields $\mathbb{Q}(\sqrt{D})$ where $D < 10^8$ and all the fields $\mathbb{Q}(\sqrt{p})$ where p is a prime up to 10^9. This computation of over 10^8 class numbers required just under four weeks on the DECstation 5000/200. In order to describe its results, we introduce some notation.

For a finite group $\boldsymbol{G}$ we define

$$f_k(\boldsymbol{G}) = \begin{cases} 1 & \text{when } |\boldsymbol{G}| = k, \\ 0 & \text{otherwise} \end{cases}.$$

Let D denote any square-free positive integer, and let $\boldsymbol{G}^*(D)$ represent the odd part of the class group of $\mathbb{Q}(\sqrt{D})$. Put

$$\mathcal{D}_1(x) = \{D \le x \mid D \equiv 1 \bmod 4\},$$
$$\mathcal{D}_2(x) = \{D \le x \mid D \not\equiv 1 \bmod 4\},$$
$$\mathcal{P}_1(x) = \{p \le x \mid p \equiv 1 \bmod 4,\ p \text{ prime}\},$$
$$\mathcal{P}_2(x) = \{p \le x \mid p \equiv 3 \bmod 4,\ p \text{ prime}\}.$$

For each $\mathcal{D}(x) \in \{\mathcal{D}_1(x), \mathcal{D}_2(x), \mathcal{P}_1(x), \mathcal{P}_2(x)\}$, define

$$r_i(x) = \frac{\sum_{D \in \mathcal{D}(x)} f_i\left(\boldsymbol{G}^*(D)\right)}{\sum_{D \in \mathcal{D}(x)} 1}, \qquad q_i(x) = \frac{r_i(x) i}{Cw(i)},$$
$$t_i(x) = \frac{1}{2}\Big(\frac{1}{1 - s_i(x)}\Big), \qquad s_i(x) = \sum_{j \le i} r_i(x).$$

Also, put

$$H^*(x) = \sum_{d \in \mathcal{D}(x)} h^*(D).$$

Tables 2 and 3 provide values of $q_i(x)$ for various choices of i and x for $\Delta \equiv 1 \bmod 4$, $\Delta < 10^8$ and for $\Delta = p \equiv 1 \bmod 4$ and $p < 10^9$. The corresponding tables for $\mathcal{D}(x) = \mathcal{D}_2(x)$ and $\mathcal{P}_2(x)$ are so similar that in the interest of brevity we do not include them here. Tables 4 and 5 provide values of $t_i(x)$ for various choices of i and x and $\mathcal{D}(x) = \mathcal{D}_1(x)$ and $\mathcal{P}_1(x)$. Again, because of the similarity of the corresponding tables for $\mathcal{D}(x) = \mathcal{D}_2(x)$ and $\mathcal{P}_2(x)$, we do not include them here. Finally, Table 6 provides values for $H^*(x)$ and $8H^*(x)/x$ for $\mathcal{D}(x) = \mathcal{P}_1(x)$. The table for $\mathcal{D}(x) = \mathcal{P}_2(x)$ is very similar.

Notice that all of these results provide numerical support for the Cohen–Lenstra heuristics, and in particular that small values of h^* seem to occur infinitely often, even when we restrict the radicands of the fields to prime values. In these cases, of course, we have $h = h^*$.

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.06119	0.85263	0.95644	0.94918	0.70424	0.90228	0.47347
10000000	1.03676	0.89604	0.99125	0.99564	0.83023	0.97519	0.69086
20000000	1.03178	0.90683	0.99465	1.00142	0.84625	0.98812	0.74718
30000000	1.02923	0.91246	0.99592	1.00250	0.85705	0.99247	0.76587
40000000	1.02752	0.91613	0.99663	1.00194	0.86264	0.99791	0.78753
50000000	1.02634	0.91893	0.99664	1.00315	0.86638	0.99846	0.79660
60000000	1.02541	0.92078	0.99588	1.00446	0.87092	0.99982	0.80705
70000000	1.02461	0.92235	0.99632	1.00504	0.87567	1.00148	0.81494
80000000	1.02389	0.92374	0.99637	1.00623	0.87874	1.00372	0.82014
90000000	1.02333	0.92480	0.99702	1.00608	0.88182	1.00418	0.82863
100000000	1.02284	0.92605	0.99695	1.00581	0.88409	1.00528	0.83205

TABLE 2. Values of $q_i(x)$ for $\Delta \equiv 1 \bmod 4$.

x	$q_1(x)$	$q_3(x)$	$q_5(x)$	$q_7(x)$	$q_9(x)$	$q_{11}(x)$	$q_{27}(x)$
1000000	1.03912	0.87049	0.98999	1.05015	0.74868	0.89694	0.80228
10000000	1.02286	0.91026	1.00832	1.00988	0.89654	1.00820	0.83991
20000000	1.01992	0.91885	1.01125	1.01036	0.89047	1.00770	0.87678
30000000	1.01878	0.92317	1.00562	1.02080	0.89756	1.00138	0.88219
40000000	1.01746	0.92762	1.00621	1.02143	0.89815	1.01307	0.89369
50000000	1.01679	0.93026	1.00793	1.01899	0.90235	1.01437	0.89445
60000000	1.01614	0.93257	1.00686	1.01727	0.90852	1.01408	0.90140
70000000	1.01563	0.93519	1.00600	1.01803	0.91051	1.01274	0.90768
80000000	1.01515	0.93662	1.00488	1.01891	0.91308	1.01263	0.90514
90000000	1.01493	0.93712	1.00600	1.01489	0.91691	1.01078	0.89925
100000000	1.01468	0.93864	1.00478	1.01335	0.91944	1.00665	0.90274
200000000	1.01314	0.94558	1.00057	1.01216	0.92337	1.00713	0.90869
300000000	1.01241	0.94866	1.00118	1.00676	0.92586	1.00590	0.91010
400000000	1.01169	0.95144	1.00229	1.00406	0.92779	1.00362	0.91560
500000000	1.01122	0.95334	1.00100	1.00519	0.93096	1.00409	0.91528
600000000	1.01077	0.95493	1.00120	1.00534	0.93239	1.00461	0.92144
700000000	1.01045	0.95583	1.00199	1.00608	0.93323	1.00523	0.92348
800000000	1.01020	0.95683	1.00179	1.00619	0.93468	1.00506	0.92527
900000000	1.00998	0.95777	1.00186	1.00629	0.93499	1.00509	0.92732
1000000000	1.00976	0.95830	1.00239	1.00646	0.93604	1.00508	0.92706

TABLE 3. Values of $q_i(x)$ for $p \equiv 1 \bmod 4$.

5. THE SIZE OF $L(1, \chi)$

Littlewood [1928] and Shanks [1973] have shown that, under the ERH, we have

$$(1+o(1))\,(c_1 \log\log\Delta)^{-1} < L(1,\chi_\Delta) < (1+o(1))\,c_2 \log\log\Delta, \tag{5.1}$$

where c_1 and c_2 depend upon the parity of Δ:

$$c_1 = 12e^\gamma/\pi^2 \quad \text{and} \quad c_2 = 2e^\gamma \quad \text{when } 2 \nmid \Delta,$$
$$c_1 = 8e^\gamma/\pi^2 \quad \text{and} \quad c_2 = e^\gamma \quad \text{when } 2 \mid \Delta.$$

In his numerical examination of (5.1), Shanks [1973] defined for a fixed Δ the *upper* and *lower Littlewood indices* as

$$\mathrm{ULI} = L(1,\chi_\Delta)/\left(c_2 \log\log\Delta\right),$$
$$\mathrm{LLI} = L(1,\chi_\Delta)c_1 \log\log\Delta.$$

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.50786	5.42530	8.91565	12.81041	17.88166	22.96408	109.6509
10000000	2.29561	4.75574	7.38079	10.02841	13.58368	16.60010	55.01249
20000000	2.25667	4.64952	7.14116	9.61024	12.91103	15.64977	48.43620
30000000	2.23723	4.59746	7.02378	9.40226	12.59204	15.19731	45.43814
40000000	2.22443	4.56286	6.94593	9.26159	12.36781	14.88841	43.53718
50000000	2.21560	4.54032	6.89384	9.17287	12.22767	14.68742	42.23651
60000000	2.20874	4.52115	6.84708	9.09414	12.10904	14.52054	41.36938
70000000	2.20287	4.50462	6.81076	9.03188	12.02043	14.39801	40.61104
80000000	2.19765	4.48987	6.77728	8.97656	11.93639	14.28389	39.94645
90000000	2.19354	4.47810	6.75275	8.93314	11.87337	14.19501	39.48465
100000000	2.18998	4.46955	6.73308	8.89798	11.82131	14.12367	39.02412

TABLE 4. Values of $t_i(x)$ for $\Delta \equiv 1 \bmod 4$.

x	$t_1(x)$	$t_3(x)$	$t_5(x)$	$t_7(x)$	$t_9(x)$	$t_{11}(x)$	$t_{27}(x)$
1000000	2.31449	4.69162	7.22253	9.92777	12.95470	15.41109	55.48867
10000000	2.19018	4.39240	6.59663	8.67220	11.47744	13.64301	36.38335
20000000	2.16904	4.34869	6.50789	8.52074	11.18966	13.23712	34.28533
30000000	2.16105	4.33701	6.46395	8.47241	11.13404	13.14434	33.69292
40000000	2.15178	4.32065	6.42954	8.41497	11.03731	13.03696	32.98149
50000000	2.14711	4.31417	6.42053	8.39339	11.01621	13.01053	32.63839
60000000	2.14260	4.30673	6.40077	8.35532	10.97404	12.95108	32.35346
70000000	2.13905	4.30460	6.39342	8.34469	10.96322	12.93295	32.21378
80000000	2.13576	4.29791	6.37521	8.31590	10.92319	12.87703	32.04356
90000000	2.13419	4.29391	6.36986	8.29684	10.90465	12.84707	31.84695
100000000	2.13247	4.29399	6.36629	8.28698	10.89705	12.82721	31.69778
200000000	2.12197	4.28339	6.33025	8.22313	10.80130	12.69580	30.99612
300000000	2.11706	4.27754	6.31934	8.19169	10.75619	12.63083	30.63904
400000000	2.11217	4.27035	6.30698	8.16446	10.71624	12.57083	30.40868
500000000	2.10902	4.26615	6.29396	8.14535	10.69473	12.54227	30.24493
600000000	2.10600	4.26107	6.28353	8.12824	10.67037	12.50989	30.15319
700000000	2.10388	4.25650	6.27594	8.11728	10.65447	12.48937	30.07765
800000000	2.10222	4.25425	6.27045	8.10837	10.64429	12.47502	30.02542
900000000	2.10075	4.25251	6.26689	8.10267	10.63557	12.46310	29.98853
1000000000	2.09927	4.24886	6.26053	8.09245	10.62169	12.44402	29.92182

TABLE 5. Values of $t_i(x)$ for $p \equiv 1 \bmod 4$.

If (5.1) is true, then as Δ increases, we would expect that extreme values of the ULI and LLI would tend to approach 1.

In fact, Chowla [1949] has shown that, for any positive $\varepsilon < 1$, the inequalities ULI $> \frac{1}{2}(1-\varepsilon)$ and LLI $< 2(1-\varepsilon)$ hold, each for an infinite sequence of values of Δ. Furthermore, Joshi [1970] showed that, if c and d are relatively prime positive integers and $8 \mid d$, then as Δ runs through prime values congruent to c mod d, we have

$$\mathrm{ULI} > \frac{1-\varepsilon}{2} \prod_{p \mid d} \frac{1-1/p}{1-(p/c)/p}$$

and

$$\mathrm{LLI} < 2(1-\varepsilon) \prod_{p \mid d} \frac{1-1/p}{1-(p/c)/p}$$

x	$H^*(x)$	$8H^*(x)/x$
1000000	97521	0.78017
10000000	990162	0.79213
20000000	1988884	0.79555
30000000	2976321	0.79369
40000000	3984781	0.79696
50000000	4987508	0.79800
60000000	5987504	0.79833
70000000	6987254	0.79854
80000000	7972707	0.79727
90000000	8997355	0.79976
100000000	10010538	0.80084
200000000	20090934	0.80364
300000000	30153902	0.80410
400000000	40367003	0.80734
500000000	50551652	0.80883
600000000	60651064	0.80868
700000000	70801346	0.80916
800000000	80950648	0.80951
900000000	91082121	0.80962
1000000000	101284007	0.81027

TABLE 6. Values of $H^*(x)$ for $p \equiv 1 \bmod 4$.

infinitely often. Thus, if Δ is a prime and $\Delta \equiv 5 \bmod 8$, we would have

$$\mathrm{LLI} < \tfrac{4}{3}(1-\varepsilon)$$

infinitely often. Also, if Δ is a prime and $\Delta \equiv 1 \bmod 8$, we would have

$$\mathrm{ULI} > \tfrac{1}{2}(1-\varepsilon)$$

infinitely often. Assuming that the size of $L(1,\chi_\Delta)$ and h are independent, this result (together with the Cohen–Lenstra heuristics) suggests that we'd have

$$R > (1-\varepsilon)\tfrac{1}{4}c_2\sqrt{\Delta}\log\log\Delta \tag{5.2}$$

infinitely often. Figure 1 plots the frequency distribution of the values of

$$Z = \frac{R}{\sqrt{\Delta}\log\log\Delta}$$

for all prime values of $\Delta \equiv 1 \bmod 8$, where $8 \times 10^8 < \Delta < 10^9$. The vertical line on this figure intersects the Z axis at $\frac{1}{2}c_2$. Notice that a small but not insignificant portion of the frequency distribution is to the right of this line. The results of [Joshi 1970] are not as good as the extreme values suggested by the truth of the ERH, and Figure 1 provides some evidence that a better result than (5.2) might hold; thus, it is of some interest to conduct a numerical investigation into how large (small) the ULI (LLI) values can be.

Shanks tested (5.1) by attempting to produce values of Δ for which he might have locally extreme values for the LLI and ULI. For example, if $\Delta \equiv 5 \bmod 8$ and $(\Delta/q) = -1$ for all of the small primes q less than some bound p, then we would expect by (1.3) that $L(1,\chi_\Delta)$ would be small. On the other hand, if $\frac{1}{4}\Delta \equiv 7 \bmod 8$ and $(\Delta/q) = 1$ for all the primes $q \le p$, then we would expect $L(1,\chi_\Delta)$ to be large. Shanks made use of Lehmer's numerical sieving device, the DLS-157, to find such special values of Δ. He found no ULI larger than 1; in fact, the largest ULI that he found was .7333. Also, he found only a few LLI's less than 1 (these occurred for small values of Δ only). The values of the LLI's tended to remain stable on average,

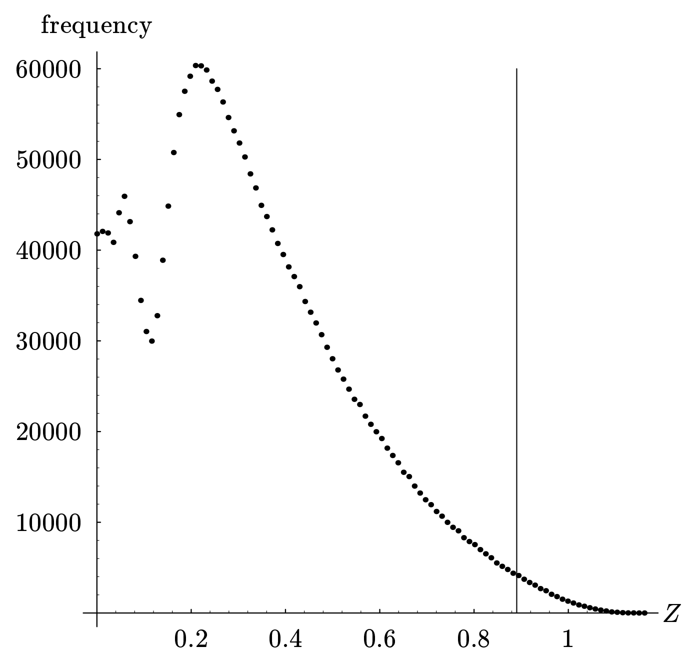

FIGURE 1. Frequency values of Z for $\Delta = p$, with $p \equiv 1 \bmod 8$ prime in the range $8 \times 10^8 < p < 10^9$.

or change very slowly; whereas the ULI's tended to increase very slowly for these special Δ values; thus, these numerical trials lend support to (5.1).

We used a new sieving device, the MSSU, to extend Shanks' computations. As this instrument has been described in some detail elsewhere [Lukes et al. 1995; Lukes et al. a], we will only mention here that it conducts its search for the kind of numbers that we sought at the rate of over 4×10^{12} per second, a considerably faster search rate than that of the DLS-157. For $D \equiv 5 \bmod 8$, we found all values of D such that $0 < D < 10^{19}$ and $(D/q) = -1$ for $q = 3, 5, 7, \ldots, 199$. For $D \equiv 1 \bmod 8$ we found all the values of D such that $0 < D < 4 \times 10^{19}$ and $(D/q) = 1$ for $q = 3, 5, 7, \ldots, 199$ and for $D \equiv 6 \bmod 8$ and $D \equiv -1 \bmod 4$ we found all the values of D such that $0 < D < 10^{19}$ and $(D/q) = 1$ for $q = 3, 5, 7, \ldots, 199$. We evaluated the class number, regulator, and $L(1, \chi_\Delta)$ for each of the several thousand numbers that resulted by using the Shanks heuristic [Mollin and Williams, p.283]. We then selected the "$L(1, \chi_\Delta)$-lochamps" and "LLI-lochamps" from the values of $D \equiv 5 \bmod 8$, namely those D with the property that their corresponding $L(1, \chi_\Delta)$ value (or LLI value) is less than that of any smaller D. From each of the other sets of D values we selected the "$L(1, \chi_\Delta)$-hichamps" and "ULI-hichamps," those D with the property that their corresponding $L(1, \chi_\Delta)$ value (or ULI value) is greater than that of any smaller D in the same set. For these D with the most extreme $L(1, \chi_\Delta)$, LLI, and ULI values we computed h, R, and $L(1, \chi_\Delta)$ using the techniques of Sections 2 and 3. In every case the results were the same as those produced by the Shanks heuristic. The largest ULI we found is $\mathrm{ULI} = 0.741429825\ldots$ (with $L(1, \chi_\Delta) = 4.98741315\ldots$, $h = 2$), for

$$D = 2323617473234474719.$$

The least LLI we found is $\mathrm{LLI} = 1.24745080\ldots$ (with $L(1, \chi_\Delta) = 0.158960540\ldots$, $h = 4$), for

$$D = 18974003020179917.$$

Since the techniques of Sections 2 and 3 for computing h require the truth of the ERH, the fact that both these techniques and the Shanks heuristic give the same results increases our confidence that the computed values are correct, even if the ERH is false. Also, the Shanks heuristic is much faster than the method of Sections 2 and 3, so it provided us with a relatively quick way to examine all the numbers produced by the sieve. Even if the class numbers computed by the Shanks heuristic are wrong, they will still be very close to the actual value, and their corresponding $L(1, \chi_\Delta)$ values will be quite accurate. At any rate, we would only expect the Shanks heuristic to give erroneous results for very large class numbers which, by the Cohen–Lenstra heuristics [Cohen and Lenstra 1984], are extremely rare.

Following Shanks we define the symbols aR_p and (aN_p) to represent the least integers congruent to a modulo 8 such that

$$\left(\frac{aR_p}{q}\right) = 1 \quad \text{and} \quad \left(\frac{aN_p}{q}\right) = -1$$

for all odd primes $q \le p$. We computed tables of aR_p for $a = 3, 6, 7$ and aN_p for $a = 5$. We also computed similar tables of aR_p and aN_p when we added the extra constraint that aR_p and aN_p be prime. We provide example tables here for the combined results for the prime values of $3R_p$ and $7R_p$ and for the prime values of $5N_p$, together with the ULI and LLI values. Corresponding tables for $a = 1$ can be found in the supplementary pages to [Lukes et al. a]. Notice that the tendency for the ULI's is to very slowly increase and for the LLI's is to remain stable with minor fluctuations about $\frac{4}{3}$. These tendencies were also displayed in all the other tables. Thus, the results that we have obtained completely support Shanks' earlier findings and therefore support the truth of (5.1). At least, we have not found anything that would lead us to believe that the ERH has been violated.

Although such values of D surely must exist, it seems to be very difficult to produce a value of D with a ULI close to 1. We attempted to do

p	R_p	R	h	$L(1,\chi)$	ULI
3	7	2.76865	1	1.04645	0.488140
5	19	5.82893	1	1.33724	0.512241
7	79	5.07513	3	1.71299	0.549523
11	331	36.25638	1	1.99283	0.567255
13	751	57.94214	1	2.11433	0.570617
17	1171	25.37280	3	2.22439	0.585134
19	7459	73.05341	3	2.53759	0.610832
23	10651	270.87206	1	2.62463	0.622710
29	18379	367.19773	1	2.70856	0.629349
$31, 37$	78439	813.56346	1	2.90486	0.642576
41	399499	1890.86355	1	2.99159	0.631650
43	1234531	3537.86780	1	3.18412	0.653616
$47, 53$	1427911	3841.39768	1	3.21468	0.657630
59	4355311	6958.99836	1	3.33454	0.665368
61	5715319	8109.80131	1	3.39226	0.673017
67	49196359	24407.90384	1	3.47987	0.662406
71	117678031	38495.70798	1	3.54866	0.665425
73	180628639	49263.42426	1	3.66548	0.682492
$79, 83$	452980999	78083.74919	1	3.66877	0.673261
$89, 97$	505313251	83941.62341	1	3.73419	0.684123
$101, \dots, 109$	9248561191	127289.80150	3	3.97079	0.698473
113	152524816291	6690.84067	239	4.09457	0.696458
$113, 127, 131$	348113924239	2445102.46006	1	4.14415	0.698553
137	916716646759	3976755.53799	1	4.15347	0.693040
139	1086257787619	637789.47424	7	4.28360	0.713513
149	4606472154439	707977.15943	13	4.28823	0.704162
151	4726529308939	9447793.54167	1	4.34569	0.713422
157	35032713351619	8533304.31730	3	4.32515	0.697114
$163, \dots, 179$	46257585588439	30459726.68748	1	4.47852	0.720076
181	251274765020899	23977422.86688	3	4.53784	0.719268
191	316934672172031	81024861.17467	1	4.55127	0.720036
$193, \dots, 229$	2871159201832639	246120736.62994	1	4.59324	0.714308
$233, \dots, 263$	632590969227841471	3833565622.42494	1	4.81993	0.722316

TABLE 7. $3R_p$ and $7R_p$: least prime solutions.

this by finding a D value with a large $L(1,\chi_\Delta)$ value. We used an unpublished idea of Lehmer which he employed to find the 20 digit value of D with a small $L(1,\Delta)$ value that appears in [Lehmer et al. 1970, p. 439]. We examined numbers of the form $D = A + BX$, where $B = \prod_{i=j}^{k} p_i$, for p_i the i-th prime, and $(A/p_i) = 1$, for $i = j, j+1, \dots, k$. In our case we used $B = 271 \cdot 277 \cdot \ldots \cdot 313 \approx 5.277 \times 10^{19}$ and the least nonsquare value of A. We then employed the MSSU to sieve on values of X by using as moduli 8 and primes $p_1, p_2, \dots, p_m$ with $p_m \le 269$ such that $A + XB \equiv 6 \bmod 8$ and

$$((A+XB)/p_i) = 1,$$

for $i = 1, 2, \dots, m$. Henri Cohen used the technique of [Cohen et al. 1993] to evaluate the $L(1,\chi_\Delta)$ values for some of these D values. The largest ULI occurred for

$$D = 1320870879580760303352202625261224 3246,$$

p	N_p	R	h	$L(1,\chi)$	LLI
3	5	0.48121	1	0.430408	0.44355
5	53	1.96572	1	0.540024	1.61246
7, 11	173	2.57081	1	0.390910	1.38799
13	293	2.83665	1	0.331438	1.24669
17	2477	6.47234	1	0.260093	1.15802
19, 23	9173	12.47223	1	0.260446	1.24696
29	61613	36.23370	1	0.291948	1.51764
31, 37, 41	74093	7.21597	5	0.265098	1.38758
43	170957	16.93918	3	0.245810	1.32491
47	360293	68.23691	1	0.227363	1.25504
53	679733	92.04349	1	0.223282	1.25592
59, 61	2004917	48.29722	3	0.204656	1.18549
67	69009533	869.69643	1	0.209383	1.31182
71	138473837	1369.29769	1	0.232725	1.47713
73	237536213	1725.64096	1	0.223931	1.43508
79	384479933	2087.35754	1	0.212907	1.37580
83	883597853	3018.26471	1	0.203076	1.33041
$89, \ldots, 113$	1728061733	4021.14004	1	0.193463	1.28086
127	9447241877	1252.37753	7	0.180389	1.22431
131, 137, 139	49107823133	18804.68086	1	0.169715	1.17733
149	1843103135837	119080.85359	1	0.175427	1.26915
151, 157	4316096218013	192239.83257	1	0.185066	1.35078
163, 167	15021875771117	344898.80858	1	0.177975	1.31520
173, 179	82409880589277	804942.51462	1	0.177339	1.33146
181	326813126363093	1551603.41110	1	0.171656	1.30445
191, 193	390894884910197	1650908.48845	1	0.167002	1.27101
197	1051212848890277	547589.04349	5	0.168892	1.29600
199, 211, 223	4075316253649373	5291574.72421	1	0.165780	1.28593
227	274457237558283317	45653225.95687	1	0.174286	1.39371
229	443001676907312837	6097479.67224	9	0.164899	1.32287
233	599423482887195557	65388978.22854	1	0.168914	1.35780
239	614530964726833997	64783176.97206	1	0.165280	1.32880
$241, \ldots, 263$	637754768063384837	22908547.79705	3	0.172116	1.38410

TABLE 8. $5N_p$: least prime solutions.

where $L(1,\chi_\Delta) = 5.324999338\ldots$ ($h = 1$). This is a large $L(1,\chi_\Delta)$, but when we evaluate the ULI we only get ULI $= .669706597\ldots$

6. CONCLUSION

Elliot [Elliot 1969] has shown that if $\varepsilon > 0$ is given, then there exist constants c_3 and c_4 (depending on ε) and a set $S = S(x)$ for $x \geq 2$, such that for all prime values of $\Delta \leq x$, $\Delta \notin S$, we have

$$\frac{c_3}{\log\log\Delta} \leq L(1,\chi) \leq c_4 \log\log\Delta.$$

Furthermore, S has cardinality at most $O(x^\varepsilon)$. In view of the Cohen–Lenstra heuristics and the numerical evidence presented above, this would seem to permit us to conjecture that there exists an infinite set of values of Δ for which

$$R \gg \frac{\sqrt{\Delta}}{\log\log\Delta}. \tag{6.1}$$

In fact it even appears that there must exist an infinite set of values of Δ such that

$$R \gg \sqrt{\Delta} \log\log \Delta.$$

At present the best result of this type is that of Halter–Koch [Halter-Koch 1989] where it is shown that there exists an infinite set of values of Δ such that

$$R \gg \log^4 \Delta. \tag{6.2}$$

This result is so much worse than (6.1) that it should be possible (without appealing to the ERH or the Gauss Conjecture) to get a better result than (6.2).

REFERENCES

[Bach 1994] E. Bach, "Improved approximations for Euler products", unpublished manuscript, 1994.

[Chowla 1949] S. Chowla, "Improvement of a theorem of Linnik and Walfisz", *Proc. London Math. Soc.* **50** (1949), 423–429.

[Cohen et al. 1993] H. Cohen, F. Diaz y Diaz, and M. Olivier, "Calculs de nombres de classes et de régulateurs de corps quadratiques en temps sous-exponentiel", pp. 35–46 in *Séminaire de Théorie des Nombres de Paris* 1990–1991, Progress in Math. **108**, Birkhäuser, Boston, 1993.

[Cohen and Lenstra 1983] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups", pp. 26–36 in *Number Theory*, CUNY, 1982 (edited by D. V. Chudnovsky), Lecture Notes in Math. **1052**, Springer, New York, 1983.

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number Theory*, Noordwijkerhout, 1983 (edited by H. Jager), Lecture Notes in Math. **1068**, Springer, New York, 1984.

[Elliot 1969] P. D. T. A. Elliot, "On the size of $L(1,\chi)$", *J. reine angew. Math.* **236** (1969), 26–36.

[Halter-Koch 1989] F. Halter-Koch, "Reell-quadratischer Zahlkörper mit größer Grundeinheit", *Abh. Math. Sem. Univ. Hamburg* **59** (1989), 171–181.

[Hooley 1984] C. Hooley, "On the Pellian equation and the class number of indefinite binary quadratic forms", *J. reine angew. Math.* **353** (1984), 98–131.

[Hua 1982] L. K. Hua, *Introduction to Number Theory*, Springer, New York, 1982.

[Joshi 1970] P. T. Joshi, "The size of $L(1,\chi)$ for real nonprincipal residue characters χ with prime modulus", *J. Number Theory* **2** (1970), 58–73.

[Landau 1936] E. Landau, "On a Titchmarsh–Estermann sum", *J. London Math. Soc.* **11** (1936), 242–245.

[Lehmer et al. 1970] D. H. Lehmer, E. Lehmer, and D. Shanks, "Integer sequences having prescribed quadratic character", *Math. Comp.* **24** (1970), 433–451.

[Lenstra 1982] H. W. Lenstra, Jr., "On the Calculation of Regulators and Class Numbers of Quadratic Fields", pp. 123–150 in *Number Theory Days*, Exeter, 1980, London Math. Soc. Lecture Note Series **56**, Cambridge U. Press, Cambridge, 1982.

[Littlewood 1928] J. E. Littlewood, "On the class number of the corpus $P(\sqrt{-k})$", *Proc. London Math. Soc.* **27** (1928), 358–372.

[Lukes et al. 1995] R. F. Lukes, C. D. Patterson, and H. C. Williams, "Numerical Sieving Devices: Their History and Some Applications", *Nieuw Archief voor Wiskunde* (4) **13** (1995), 113–139.

[Lukes et al. a] R. F. Lukes, C. D. Patterson, and H. C. Williams, "Some results on pseudosquares", to appear in *Math. Comp.*

[Mollin and Williams] R. A. Mollin and H. C. Williams, "Computation of the class number of a real quadratic field", *Utilitas Math.* **41** (1992), 259–308.

[Nagell 1922] T. Nagell, "Zur Arithmetik der Polynome", *Abh. Math. Sem. Univ. Hamburg* **1** (1922), 179–194.

[Oesterlé 1979] J. Oesterlé, "Versions effectives du théorème de Chebotarev sous l'hypothése de Riemann généralisée", pp. 165–167 in *Journées arithmétiques*, Luminy, 1978, Astérisque **61**, Soc. math. de France, Paris, 1979.

[Shanks 1971] D. Shanks, "Class number, a theory of factorization and genera", pp. 415–440 in *Number*

Theory Institute, Stony Brook, 1969, Proc. Symp. Pure Math. **20**, Amer. Math. Soc., Providence, 1971.

[Shanks 1973] D. Shanks, "Systematic examination of Littlewood's bounds on $L(1,\chi)$", pp. 267–283 in *Analytic number theory*, St. Louis, 1972 (edited by H. G. Diamond), Proc. Symp. Pure Math. **24**, Amer. Math. Soc., Providence, 1973.

[Stephens and Williams 1988] A. J. Stephens and H. C. Williams, "Computation of real quadratic fields with class number one", *Math. Comp.* **51** (1988), 809–824.

Michael J. Jacobson, Jr., Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2 (jacobs@cs.uni-sb.de)

Richard F. Lukes, Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2 (rflukes@cs.umanitoba.ca)

Hugh C. Williams, Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2 (Hugh_Williams@csmail.cs.umanitoba.ca)

Received January 4, 1995; accepted in revised form August 8, 1995