The Size of the Fundamental Solutions of Consecutive Pell Equations

Michael J. Jacobson, Jr. and Hugh C. Williams

CONTENTS

1. Introduction
2. The Size Ratio Can be Arbitrarily Large
3. Some Further Results on The Size Ratio
4. Maximizing The Size Ratio
5. Some Experimental Results
References
Acknowledgements

Let D be a positive integer such that D and D−1 are not perfect squares; denote by X_0, Y_0, X_1, Y_1 the least positive integers such that $X_0^2 - (D-1)Y_0^2 = 1$ and $X_1^2 - DY_1^2 = 1$; and put $\rho(D) = \log X_1/\log X_0$. We prove here that $\rho(D)$ can be arbitrarily large. Indeed, we exhibit an infinite family of values of D for which $\rho(D) \gg D^{1/6}/\log D$. We also provide some heuristic reasoning which suggests that there exists an infinitude of values of D for which $\rho(D) \gg \sqrt{D}\log\log D/\log D$, and that this is the best possible result under the Extended Riemann Hypothesis. Finally, we present some numerical evidence in support of this heuristic.

1. INTRODUCTION

The very entertaining book [Roberts 1992], on the properties of particular integers, discusses on pp. 260–263 the two Pellian equations

$$x^2 - 1620y^2 = 1 \quad \text{and} \quad x^2 - 1621y^2 = 1,$$

as had been done earlier in [Carmichael 1959, footnote on p. 33] and [Beiler 1964, p. 255]. Roberts remarks: "The first of these has smallest solution with $x = 161$, $y = 4$ and the second has smallest solution with x of 76 digits! ... Is it mysterious that neighboring integers can act so very differently?" Let $D-1$ and D be nonsquare positive integers, let

$$X^2 - (D-1)Y^2 = 1$$

have minimal solution X_0, $Y_0 \in \mathbb{Z}$ with

$$X_0 + \sqrt{D-1}\,Y_0 > 1,$$

and let

$$X^2 - DY^2 = 1$$

have minimal solution X_1, $Y_1 \in \mathbb{Z}$ with

$$X_1 + \sqrt{D}\,Y_1 > 1.$$

In view of the observation quoted above, it seems appropriate to define $\rho(D) = \log X_1/\log X_0$ and

William's research is partially supported by NSERC of Canada Research Grant #A7649.

Keywords: Pell equation, continued fractions, real quadratic field

AMS Subject Classification: Primary, 11D09; Secondary, 11R11, 11R27, 11Y40

© A K Peters, Ltd.
1058-6458/2000 $0.50 per page

ask: For what values of D might we expect $\rho(D)$ to be large, and just how large, as a function of D, could $\rho(D)$ become? For example, if $D = 1621$, we find that $\rho(D) = 34.35$, but if $D = 118681$, we get $\rho(D) = 633.84$.

We first note that if

$$X^2 - DY^2 = 1 \tag{1–1}$$

and $X + \sqrt{D}Y > 1$, then

$$0 < X - \sqrt{D}Y = (X + \sqrt{D}Y)^{-1} < 1;$$

hence, $2X = X+\sqrt{D}Y+X-\sqrt{D}Y > 1$, and $X > 0$. Also, $2\sqrt{D}Y = X + \sqrt{D}Y - (X - \sqrt{D}Y) > 0$. Since

$$2X = X + \sqrt{D}Y\left(1 + \frac{1}{(X+\sqrt{D}Y)^2}\right),$$

we get

$$\log X + \log 2 = \log(X + \sqrt{D}Y) + \log\left(1 + \frac{1}{(X+\sqrt{D}Y)^2}\right).$$

If $S = \log(X + \sqrt{D}Y) > (\log D)/2$, then

$$S - \log 2 + 1/\sqrt{D} > S - \log 2 + e^{-2S} > \log X > S - \log 2;$$

thus

$$\log X \approx S - \log 2,$$

particularly when D (or S) is large. Thus, if D is large, we can replace $\log X$ by $\log(X+\sqrt{D}Y)-\log 2$ in $\rho(D)$; and, if we define $\varepsilon(D)$ to be the least value of $X+\sqrt{D}Y(> 1)$, where $X, Y \in \mathbb{Z}$ and X, Y satisfy (1–1), then

$$\rho(D) \approx \frac{\log \varepsilon(D)}{\log \varepsilon(D-1)}.$$

We will show that $\rho(D)$ can become arbitrarily large; indeed, there exists an infinite family of values of D such that $\rho(D) \gg D^{1/6}/\log D$. However, this result, as we shall indicate later, seems to be far from the truth concerning how large $\rho(D)$ can become as a function of D. In fact, under a number of plausible hypotheses, we suggest that there exists an infinitude of values of D for which $\rho(D) \gg \sqrt{D}\log\log D/\log D$; and that under the extended Riemann hypothesis, this is the best result we could expect. Finally, we will provide some numerical evidence to support this heuristic.

2. THE SIZE RATIO CAN BE ARBITRARILY LARGE

In order to make $\rho(D)$ as large as possible, we need $\varepsilon(D)$ to be large and $\varepsilon(D-1)$ to be small. We can guarantee the latter condition by insisting that $D-1$ be of a certain Richaud-Degert type; in this case $D-1 = M^2+m$, where $m \mid 2M$. We have (see [Mollin 1996, Section 3.2], for example)

$$\varepsilon(D-1) = \frac{\left(M + \sqrt{D-1}\right)^2}{m}.$$

Also, $X_0 \le 2M^2/m + 1 < D$ when $m > 1$. The next step is to attempt to make $\varepsilon(D)$ large. Yamomoto [1971] showed that the form $D = (p^n q + p + 1)^2 - 4p$ where p, q are primes such that $p < q$ has $\log \varepsilon(D) \gg (\log \sqrt{D})^3$; unfortunately, $D-1$ is not of Richaud-Degert type here. However, it is easy to modify Yamomoto's form to

$$D = \left(\frac{Rr^n - r + 4}{4}\right)^2 + r. \tag{2–1}$$

If we insist only that r, R be odd, $r > 1$, $Rr^{n-1} \equiv 1 \pmod 4$, and $R > 3r$, then it is easy to produce the first few partial quotients in the simple continued fraction expansion of $\sqrt{D}$.

We will use $\langle q_0, q_1, \ldots, q_n\rangle$ to denote the continued fraction

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_n}}}}.$$

As is usual, we put $P_0 = 0$, $Q_0 = 1$, $q_0 = \lfloor\sqrt{D}\rfloor$ and define

$$\begin{aligned} P_{i+1} &= q_i Q_i - P_i, \\ Q_{i+1} &= (D - P_{i+1}^2)/Q_i, \\ q_{i+1} &= \lfloor (P_{i+1} + \sqrt{D})/Q_{i+1} \rfloor \end{aligned}$$

for $i = 0, 1, 2, \ldots$. Then

$$\sqrt{D} = \langle q_0, q_1, q_2, \ldots, q_{n-1}, \theta_n\rangle,$$

where $\theta_n = (P_n + \sqrt{D}\,)/Q_n$, is a means of expressing the simple continued fraction expansion of $\sqrt{D}$. We also mention that at some point we must find that either $P_r = P_{r+1}$ or $Q_s = Q_{s+1}$; in either event we get (see [Stephens and Williams 1988], for example)

$$\varepsilon(D) > \left(\prod_{i=1}^{t} \frac{P_i + \sqrt{D}}{Q_i}\right)^2 \tag{2–2}$$

for $t = r$ or s.

It is easy to see that for D given by (2–1) we have $q_0 = \frac{1}{4}(Rr^n - r + 4)$. We can also establish by induction that for $k = 0, 1, 2, \ldots, n-1$ we have

$$\begin{aligned}
P_{3k+1} &= \tfrac{1}{4}(Rr^n - 2r^{k+1} + r + 4),\\
Q_{3k+1} &= r^{k+1},\\
q_{3k+1} &= \tfrac{1}{2}(Rr^{n-k-1} - 1),\\
P_{3k+2} &= \tfrac{1}{4}(Rr^n - r - 4),\\
Q_{3k+2} &= r^{n-k-1}R,\\
q_{3k+2} &= \tfrac{1}{2}(r^{k+1} - 1),\\
P_{3k+3} &= \tfrac{1}{4}(Rr^n - 2Rr^{n-k-1} + r + 4),\\
Q_{3k+3} &= \tfrac{1}{4}(Rr^n - r^{n-k-1}R - r^{k+2} + r + 4),\\
q_{3k+3} &= 2.
\end{aligned}$$

Since no two consecutive P or Q values are equal for $0 \le k \le n-1$, we find from (2–2) that

$$\varepsilon(D) > \prod_{k=0}^{n-1} \left(\frac{(r^{n-k-1}R - 1)(r^{k+1} - 1)}{2} \right)^2. \qquad (2\text{–}3)$$

Since

$$\begin{aligned}
\left(\tfrac{1}{4}(Rr^n - r + 4) + \tfrac{1}{2}\right)^2 - D &= \tfrac{1}{2}\left(\tfrac{1}{4}(2Rr^n - 2r + 8) + \tfrac{1}{2}\right) - r\\
&= \tfrac{1}{4}(Rr^n - 5r + 5) > 0
\end{aligned}$$

for $n \ge 1$, we get

$$\sqrt{D} < \tfrac{1}{4}(Rr^n - r + 6). \qquad (2\text{–}4)$$

Also, since $r \ge 3$, we get

$$r^{k+1} > 2 + \frac{4}{3r^{n-k} - 2} \quad (0 \le k \le n-1).$$

Hence,

$$3r^{n+1} - 6r^{n-k} > 2r^{k+1}$$

and

$$R(r^n - 2r^{n-k-1}) > 3r^{n+1} - 6r^{n-k} > 2r^{k+1}.$$

From this we see that

$$Rr^n > 2r^{n-k-1}R + 2r^{k+1}$$

and

$$Rr^n + r \ge 2r^{n-k-1}R + 2r^{k+1} + 4.$$

It follows that

$$2(Rr^n - r^{n-k-1}R - r^{k+1} + 1) \ge Rr^n - r + 6$$

and

$$\begin{aligned}
\frac{(r^{n-k-1}R - 1)(r^{k+1} - 1)}{2} &= \frac{Rr^n - r^{n-k-1}R - r^{k+1} + 1}{2}\\
&\ge \frac{Rr^n - r + 6}{4} > \sqrt{D},
\end{aligned}$$

by (2–4). By (2–3) we get

$$\varepsilon(D) > \left(\sqrt{D}\right)^{2n} = D^n.$$

If we put $r \equiv 5 \pmod 8$ and select n to be even, then $r^n \equiv 1 \pmod{2(r-1)}$. Furthermore, if R is selected such that $R \equiv r - 4 \pmod{2(r-1)}$, then $2r - 2 \mid r^n R - r + 4$ and

$$\rho(D) > \frac{\log \varepsilon(D) - \log 2}{\log X_0} > n - \frac{\log 2}{\log D}. \qquad (2\text{–}5)$$

Thus, $\rho(D)$ can be arbitrarily large for an infinite number of values of D. We have therefore shown that there exists an infinitude of values of D such that $\rho(D) \gg \log D$.

3. SOME FURTHER RESULTS ON THE SIZE RATIO

We say that any positive nonsquare integer d such that $d \equiv 0, 1 \pmod 4$ is a *quadratic discriminant*. If $\alpha, \beta \in \mathcal{K} = \mathbb{Q}(\sqrt{d})$, we let $[\alpha, \beta]$ denote the $\mathbb{Z}$-module $\{\alpha x + \beta y \mid x, y \in \mathbb{Z}\}$. We define the order $\mathcal{O}_d$ of the real quadratic field $\mathcal{K}$ by $\mathcal{O}_d = [1, \omega_d]$, where

$$\omega_d = \begin{cases} \sqrt{d}/2 & \text{when } 4 \mid d,\\ (\sqrt{d} + 1)/2 & \text{when } d \equiv 1 \pmod 4. \end{cases}$$

Here d is the discriminant of $\mathcal{O}_d$, and if $d = d_0 f^2$, where d_0 is the discriminant of $\mathcal{K}$, then f is the *conductor* of $\mathcal{O}_d$ and d_0 is the *fundamental discriminant* belonging to d. We denote the fundamental unit of $\mathcal{O}_d$ by $\varepsilon_d (> 1)$. If, for any nonsquare $D > 0$, we put

$$d = \begin{cases} D & \text{when } D \equiv 1, 0 \pmod 4\\ 4D & \text{when } D \equiv 2, 3 \pmod 4, \end{cases} \qquad (3\text{–}1)$$

then

$$\varepsilon(D) = \varepsilon_d^{\nu}$$

for some positive integer ν.

We can improve upon (2–5) by modifying slightly the proof of Yamomoto's Theorem 3.1 to produce the following theorem.

Theorem 3.1. *Let r_i, for $i = 1, 2, \ldots, k$, be positive integers which are relatively prime in pairs. If there exists an infinitude of real quadratic fields $\mathcal{K}$ such*

that each r_i can be decomposed in $\mathcal{K}$ into the product of two principal ideals $\mathfrak{r}_i$ and $\mathfrak{r}_i'$ and each rational prime divisor of r_i can be decomposed into the product of two distinct prime ideals, then

$$\log \varepsilon \gg \left(\log \sqrt{d_0}\right)^{k+1},$$

where d_0 and ε are respectively the discriminant and fundamental unit of $\mathcal{K}$.

Since, for our values of D given by (2–1), we have $Q_1 = r$, $Q_{3n-1} = R$, we see that if $(r, R) = 1$ and $(R, D) = 1$, we can use Yamomoto's reasoning to show that the conditions of Theorem 3.1 can be fulfilled for an infinitude of fields $\mathcal{K} = \mathbb{Q}(\sqrt{D})$, where D is given by (2–1) with $r \equiv 5 \pmod 8$, $(r(r+4), R) = 1$, $R > 3r > 0$, $R \equiv r - 4 \bmod (2(r-1))$ and $2 \mid n$. Since $\varepsilon(D) = \varepsilon^\nu$ for some positive integer ν, we must have

$$\rho(D) \gg (\log D)^3 \tag{3–2}$$

for such values of D.

Halter-Koch [1989] extended Yamomoto's Theorem 3.1 to show that there exists an infinite family of real quadratic fields for which $\log \varepsilon \gg \left(\log \sqrt{d_0}\right)^4$; thus, one might expect to produce a better result than (3–2). Unfortunately, a subtle error in the proof of his Main Theorem in [Halter-Koch 1989, Section 3] invalidates his result. In order to get a better result than (3–2), we proceed in another direction.

We consider $\varepsilon(D_0)$ and $\varepsilon(D)$, where $D = f^2 D_0$. We must have $\varepsilon(D) = \varepsilon(D_0)^m$ for some positive integer m. If we put $\varepsilon(D_0) = X + \sqrt{D_0}Y$, we can define integers X_n, Y_n by

$$X_n + \sqrt{D_0}Y_n = \varepsilon(D_0)^n.$$

If $\varepsilon(D) = W + Z\sqrt{D} = W + fZ\sqrt{D_0}$, we see that m must be the least positive integer such that $f \mid Y_m$. The problem of determining m can be very difficult in general. We know that m must divide $\Phi_f(D_0)$, where

$$\Phi_f(D_0) = f \prod_{p \mid f} \left(1 - \frac{(D_0/p)}{p}\right) \tag{3–3}$$

and (D_0/p) denotes the Kronecker symbol, but this is often as much as can be said. The problem of the divisibility of Y_n by certain integers was considered by Lehmer [1928]. If p is any prime divisor of D_0 which does not divide $Y_1 (= Y)$, then $p \parallel Y_p$ and $p \nmid Y_i$ if $(i, p) = 1$ [Lehmer 1928, Theorem 9]. From this it follows that $p^k \parallel Y_{p^k}$ and $p^k \nmid Y_i$ when $1 \le i < p^k$ [Lehmer 1928, Theorem 10]. Since $\{Y_n\}$ is a divisibility sequence, we see that if the square-free kernel $\bar{f}$ of f is such that $\bar{f} \mid D_0$ and $\left(\bar{f}, Y_1\right) = 1$, then $m = f$ and

$$\log \varepsilon(D) = f \log \varepsilon(D_0). \tag{3–4}$$

If we put $D_0 = k^2\bar{f}^2 + \bar{f}$, then D_0 is of Richaud-Degert type and

$$\varepsilon(D_0) = \frac{\left(k\bar{f} + \sqrt{D_0}\right)^2}{\bar{f}} = 2\bar{f}k^2 + 1 + 2k\sqrt{D_0}.$$

To ensure that $\varepsilon(D-1)$ is small, we need $D-1 = f^2 D_0 = k^2 f^2 \bar{f}^2 + f^2\bar{f} - 1$ to be of Richaud-Degert type. This will occur if $f^2\bar{f} - 1 \mid k^2 f^2 \bar{f}^2$. We can guarantee this if we put $k = f^2\bar{f} - 1$. In this case we get $\bar{f} \mid D_0$ and $\left(Y_1, \bar{f}\right) = 1$ when $\bar{f}$ is odd. In the simple case where $f = p^n$ and p is an odd prime, we put

$$\begin{aligned} D_n &= p^{2n+2}\left(p^{2n+1} - 1\right)^2 + p^{2n+1} \\ &< p^{2n}\left(p^{2n+2}\right)^2 = p^4 p^{6n}. \end{aligned}$$

We see by (3–4) that

$$\log \varepsilon(D_n) = p^n \log D_0 > p^n > \frac{D_n^{1/6}}{p^{2/3}}.$$

Now

$$\varepsilon(D_n - 1) = \frac{\left(p^{n+1}\left(p^{2n+1} - 1\right) + \sqrt{D_{n-1}}\right)^2}{\left(p^{2n+1} - 1\right)} < D_n;$$

thus,

$$\frac{\log \varepsilon(D_n)}{\log \varepsilon(D_n - 1)} \gg D_n^{1/6} / \log D_n,$$

and therefore

$$\rho\left(D_n\right) \gg D_n^{1/6} / \log D_n.$$

We have proved the following theorem.

Theorem 3.2. *There exists an infinite family of values of D such that $\rho(D) \gg D^{1/6} / \log D$.*

4. MAXIMIZING THE SIZE RATIO

In this section we will attempt to produce some information on just how large $\rho(D)$ might become as a function of D. We will first attempt to find an upper bound on the size of $\rho(D)$. We note that the least possible value of $\log \varepsilon(D) = \log(X + Y\sqrt{D})$ must exceed $\frac{1}{2} \log D$.

We must now examine the problem of maximizing X_1 or $\varepsilon(D)$ or ε_d, where d is the discriminant defined by (3–1). By the Analytic Class Number Formula (see [Cohn 1962], for example), we have

$$2hR = \sqrt{d}L(1,\chi_d),$$

where $R = \log \varepsilon_d$, h is the class number of $\mathcal{O}_d$, and

$$L(1,\chi_d) = \prod_q \left(\frac{q}{q-(d/q)}\right) = \frac{2}{2-(d/2)}E(d)$$

is the Euler product representation of $L(1,\chi_d)$. The product is taken over all primes q, (d/q) is the Kronecker symbol, and

$$E(d) = \prod_q \left(\frac{q}{q-(d/q)}\right), \tag{4–1}$$

where the product is taken over all the odd primes.

If d_0 is the fundamental discriminant belonging to $\mathcal{O}_d$, then

$$h = \Phi_f(d_0)h(d_0)/u,$$

where $h(d_0)$ is the class number of $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d_0})$, u is the unit index of $\mathcal{O}_d$ over $\mathcal{O}_{d_0}$ ($\varepsilon_d = \varepsilon^u$, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{d})$), and $\Phi_f(d_0)$ is given by (3–3).

In order to maximize ε_d, we need $h = 1$; hence, since $u \mid \Phi_f(d_0)$, we need $h(d_0) = 1$ and $\Phi_f(d_0) = u$. Also, since $\varepsilon(D) = \varepsilon_d^\nu$, we would like to maximize ν as well. If we let $\varepsilon_d = (T + U\sqrt{d})/2$, the value of ν can be determined from Table 1, where we use $N(\alpha)$ to denote the norm $\alpha\bar{\alpha}$ of $\alpha \in \mathcal{K}$.

Remark. Whenever $3 \mid \nu$, we have $D \equiv 5 \pmod 8$.

From these remarks it follows that

$$\log \varepsilon(D) = B(d)E(d), \tag{4–2}$$

$D \bmod 4$	$T \bmod 2$	$U \bmod 2$	$N(\varepsilon_d)$	ν
-1	–	–	1	1
0	–	0	1	1
0	–	1	–	2
2	–	0	1	1
2	–	1	-1	2
1	0	0	1	1
1	0	0	-1	2
1	1	1	1	3
1	1	1	-1	6

TABLE 1. Values of ν such that $\varepsilon(D) = \varepsilon_d^\nu$.

where $B(d) = \left(\sqrt{d}/h\right)\left(\nu/(2-d/2)\right)$ and

$$\nu/(2-d/2) \le 2.$$

By results of Littlewood [1928] and Shanks [1973], we know that

$$E(d) < \{1 + o(1)\}e^\gamma \log\log d,$$

under the extended Riemann hypothesis, or ERH. Thus, since $\rho(D) = \left(\log \varepsilon(D)/\log \varepsilon(D-1)\right)\left(1+o(1)\right)$, we get

$$\rho(D) < \frac{4e^\gamma \sqrt{D}\log\log D}{\log D}\left(1 + o(1)\right). \tag{4–3}$$

We now investigate the problem of maximizing $\rho(D)$. Since $X_0 = \sqrt{(D-1)Y_0^2 + 1}$, in order to make $\rho(D)$ large, we would want Y_0 to be small. The least possible value for Y_0 is 1, but this would mean that $D = X_0^2$, which is not permitted. The next possible candidate for Y_0 is 2, which means that X_0 must be odd. Putting $X_0 = 2M+1$, we get $D = M^2 + M + 1$.

We now look at the problem of getting the largest possible value for $B(d)/\sqrt{d}$. If $h = 1$, then $h(d_0) = 1$. By genus theory this means that d_0 can only be a prime, the double of a prime congruent to $-1 \pmod 4$ or the product of two such primes. Thus, a good strategy to employ to maximize $B(d)/\sqrt{d}$ would be to select D such that D is a prime.

For $f(x) = x^2 + x + 1$, put $P(n) = \#\{f(k) \mid f(k)$ prime for $k = 1, 2, \ldots, n\}$. By Hardy and Littlewood's Conjecture F [Fung and Williams 1990], we expect that

$$P(n) \sim C(-3)L(n)$$

where

$$L(n) = 2\int_1^n \frac{dx}{\log f(x)}$$

and

$$C(-3) = 1.12073275 \quad \text{[Shanks 1960]}.$$

Also, by the Cohen-Lenstra heuristics [1984], we would expect that these prime values of $f(x)$ for which $h(f(x)) = 1$ should have density of about 0.75446. In Table 2 we provide some results of a trial run of computing $P(n)$ and $H(n) = \#\{f(k) \mid f(k)$ prime; $h(f(k)) = 1$; $k = 1, 2, \ldots, n\}$ for all $n \le 10^6$. This lends some numerical support to this expectation.

We also note that if $q \mid d_0$ and $q \equiv -1 \pmod 4$, then $2 \nmid \nu$ unless $4 \mid D$. Furthermore, if $3 \mid \nu$, the

n	$P(n)$	$L(n)$	$P(n)/L(n)$	$H(n)$	$H(n)/P(n)$
100000	10751	9628.12018	1.11663	8255	0.76784
200000	20154	18034.36084	1.11753	15455	0.76685
300000	29139	26084.99959	1.11708	22263	0.76403
400000	37935	33920.92844	1.11834	28985	0.76407
500000	46514	41604.59464	1.11800	35438	0.76188
600000	55013	49171.13232	1.11881	41860	0.76091
700000	63445	56642.96762	1.12009	48107	0.75825
800000	71716	64035.60199	1.11994	54362	0.75802
900000	79992	71360.35885	1.12096	60680	0.75858
1000000	88118	78625.85310	1.12073	66776	0.75780

TABLE 2. Values of $P(n)$ and $H(n)$.

value of $1/(2-(d/2))$ is only $1/3$ because $d \equiv 5 \pmod 8$. We see, then, that the best possible value for $B(d)$ as a function of D is $2\sqrt{D}$. As it is difficult to guarantee *a priori* that $3 \mid \nu$ we are most easily able to say that we will get a maximal value of $B(d)$ when D is a prime congruent to 1 (mod 8).

Following Shanks [1973], we define the Upper Littlewood Index, or ULI, as

$$\text{ULI} = L(1, \chi_d)/(2e^{\gamma} \log\log d) = 1 + o(1)$$

for $d \equiv 1 \pmod 4$. Then $R = \sqrt{d}\,(e^{\gamma} \log\log d)\text{ULI}$, and for prime values of $D = M^2 + M + 1 \equiv 1 \pmod 8$ such that $h(D) = 1$, we get

$$\begin{aligned}\rho(D) &\approx \frac{2\sqrt{D}e^{\gamma} \log\log D(\text{ULI})}{1/2 \log D} \\ &= \frac{4e^{\gamma}\sqrt{D} \log\log D}{\log} D(\text{ULI}).\end{aligned}$$

Thus, the ULI here provides a measure of just how close $\rho(D)$ can get to the likely maximum given in (4–3). We know (see Joshi [1970]) that if D is a prime and $D \equiv 1 \pmod 8$, then ULI $> (1-\eta)/2$ infinitely often for any positive $\eta < 1$. Thus, it would certainly seem that there is an infinitude of values of D such that

$$\rho(D) \gg \frac{\sqrt{D} \log\log D}{\log D}, \tag{4–4}$$

but a proof of this requires us to prove, among other things, the existence of an infinitude of primes D of the form M^2+M+1 such that $h(D) = 1$. At present this seems to be well beyond the boundaries of what modern number theory can achieve.

5. SOME EXPERIMENTAL RESULTS

While Theorem 3.2 provides the best result we currently have concerning the growth of $\rho(D)$, the remarks in the previous section suggest that it is far from the best possible result. In this section we will provide some numerical evidence in support of (4–4). We will do this by attempting to find values of D for which $\rho(D)$ is as large as it can be. To see how close we can get $\rho(D)$ to its maximum (under the ERH) (4–3), by (4–2) we now need to maximize $E(D) = (\text{ULI}) \log\log D$. In general, this is a very difficult problem, but the method used in [Jacobson et al. 1995] to obtain large ULI values can be adapted for use here. We should select M such that

$$\left(\frac{M^2 + M + 1}{q}\right) = 1 \tag{5–1}$$

for as many of the primes q, particularly the small values of q, as possible. We also will need $M^2 + M + 1$ to be a prime and $8 \mid M(M+1)$ or $M \equiv 0, -1 \pmod 8$. To this end we now define M_p, N_p and H_p for a given prime p. Consider the set of positive integers $\mathcal{S} = \{M\}$ such that

1. $M \equiv 0, -1 \pmod 8$
2. $((M^2 + M + 1)/q) = 1$ for all odd primes $q \le p$.

We define M_p to be the least element in $\mathcal{S}$, N_p to be the least prime in $\mathcal{S}$ and H_p to be the least prime in $\mathcal{S}$ such that $h(H_p^2 + H_p + 1) = 1$.

Since for any prime q, we have

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + x + 1}{q}\right) = -1,$$

it is easy to see that when $q > 3$ there are exactly $(q - (-3/q) - 2)/2$ values of x modulo q such that $((x^2 + x + 1)/q) = 1$. Thus, if we put

$$Q = 8 \prod_{q \le p} q,$$

where the product is taken over the odd primes, then the number of elements of $\mathcal{S}$ which are less than or equal to Q is given by

$$4 \prod_{q>3}^{p} \frac{q - (-3/q) - 2}{2}.$$

If we assume that these values are more-or-less equidistributed, we get

$$T(n) \approx \left(\frac{1}{6} \prod_{q>3}^{p} \frac{q - (-3/q) - 2}{2q} \right) n,$$

where $T(n)$ is the number of values of $\mathcal{S}$ which are less than or equal to n. Furthermore, if we refer again to Hardy and Littlewood's conjecture F, we would expect

$$Q(n) \sim \tfrac{1}{4} C(-3) \prod_{q>3}^{p} \frac{(q - 2 - (-3/q))}{2\,(q - 1 - (-3/q))} L(n),$$

where $Q(n)$ is the number of values of $x \in \mathcal{S}$ less than or equal to n such that $x^2 + x + 1$ is a prime. Thus, to find M_p and N_p, for even modest values of p, we would expect to have to search through many positive integer values. This is a task that can be readily accomplished by using a numerical sieving device.

We made use of the MSSU [Lukes et al. 1995; 1996] to find values for M_p, N_p and H_p for all $p \le 233$. The entire computation took just over 12 days. Table 3 records our results.

For all the values of $D = H_p^2 + H_p + 1$ in Table 3 we certainly have

$$\rho(D) > \frac{\sqrt{D} \log\log D}{\log D}. \tag{5–2}$$

We next attempted to find quite large values of D such that (5–2) holds. However, as the MSSU slows down considerably for values of p in excess of 200, we made use of a strategy originally employed by Lehmer [1928, pp. 222–223]. We considered $D_p = M^2 + M + 1$, where $M = B_p X + A_p$,

$$B_p = \prod_{q \ge 191}^{p} q$$

and

$$\left(\frac{A_p^2 + A_p + 1}{q} \right) = 1$$

for all primes q $(191 \le q \le p)$. As the B_p and A_p values for any given p are fixed, we could use the MSSU to find values of X such that $B_p X + A_p \equiv 0, -1 \pmod 8$ and

$$\left(\frac{(B_p X + A_p)^2 + (B_p X + A_p) + 1}{q} \right) = 1$$

for all odd primes $q \le 181$. As the sieve will find such values of X quite quickly, we could afford to generate quite a lot of them in order to search for prime values of D_p such that $h(D_p) = 1$. For example, when $p = 233$ (so $A_p = 359$) we generated 50 values of X, but for only 2 of these values is D_p a prime and $h(D_p) = 1$ for only one of those.

The table below summarizes the results of our computations. The values of X here are such that D_p is prime and $h(D_p) = 1$; the symbol n_p denotes the number of decimal digits of D_p.

p	A_p	X	n_p	ULI
211	6	1930606338268662	54	0.55800898
223	6	477020716317042	58	0.57045097
227	6	698133317203686	63	0.56122233
229	6	832043694532638	67	0.53703765
233	359	3034198402422072	73	0.54638899
239	1542	18161128276718634	80	0.55182559

We made use of the technique of [Jacobson 1999] to evaluate $h(D_p)$ for these large values of D_p. The table's last entry concerns a very large value of D_p; we provide more details concerning this number at the top of page 639.

The computation of R and $h(D_p)$ for the six D_p values in the preceding table was carried out on a 296 MHz SUN UltraSPARC-II processor with 1024 MB of main memory using C++ routines which will be publicly available in release 1.4 of the LiDIA computer algebra library [LiDIA 1997]. The CPU time required for these computations ranged from just over 6 minutes for the 54-digit D_{211} to about 2.05

p	M_p	N_p	H_p	ULI(H_p)
3	8	8 (0)	8 (0)	0.34592830
5	15	15 (0)	15 (0)	0.39889102
7	104	119 (1)	279 (3)	0.47687007
11	104	119 (1)	560 (6)	0.55217105
13	104	560 (2)	560 (2)	0.55217105
17	560	560 (0)	560 (0)	0.55217105
19	1560	1560 (0)	1560 (0)	0.56112822
23	1560	1560 (0)	1560 (0)	0.56112822
29	3464	3464 (0)	3464 (0)	0.55515102
31	19095	66639 (3)	157415 (10)	0.60773389
37	61424	66639 (1)	157415 (5)	0.60773389
41	61424	178359 (4)	178359 (4)	0.56951979
43	71784	178359 (1)	178359 (1)	0.56951979
47	71784	957144 (4)	8756559 (29)	0.59779093
53	228255	957144 (2)	10595024 (22)	0.60250433
59	228255	1081080 (1)	10595024 (6)	0.60250433
61	1081080	1081080 (0)	28280615 (9)	0.62862349
67	1081080	1081080 (0)	28280615 (3)	0.62862349
71	23735999	28280615 (1)	28280615 (1)	0.62862349
73	28280615	28280615 (0)	28280615 (0)	0.62862349
79	28280615	28280615 (0)	28280615 (0)	0.62862349
83	28280615	28280615 (0)	28280615 (0)	0.62862349
89	28280615	28280615 (0)	28280615 (0)	0.62862349
97	39529280	39529280 (0)	39529280 (0)	0.63935724
101	3020217759	4328058944 (3)	4328058944 (3)	0.66479727
103	3020217759	4328058944 (2)	4328058944 (2)	0.66479727
107	3020217759	4328058944 (2)	4328058944 (2)	0.66479727
109	3020217759	4328058944 (2)	4328058944 (2)	0.66479727
113	4328058944	4328058944 (0)	4328058944 (0)	0.66479727
127	27559966224	211959196344 (6)	211959196344 (6)	0.58832886
131	86936942519	1956241743015 (34)	1956241743015 (34)	0.61535648
137	86936942519	1956241743015 (12)	1956241743015 (12)	0.61535648
139	86936942519	1956241743015 (6)	1956241743015 (6)	0.61535648
149	86936942519	3101501785640 (8)	3101501785640 (8)	0.64232546
151	86936942519	4640009799215 (7)	4640009799215 (7)	0.63013461
157	1772215317599	8436198739695 (5)	8436198739695 (5)	0.63258650
163	1772215317599	8436198739695 (5)	8436198739695 (5)	0.63258650
167	3044985940815	42043856056104 (4)	42043856056104 (4)	0.59866969
173	3044985940815	66221372694959 (4)	72449567456784 (5)	0.63189010
179	3044985940815	66221372694959 (2)	79095695036280 (3)	0.60373327
181	3044985940815	79095695036280 (1)	79095695036280 (1)	0.60373327
191	178466469858039	336161276892959 (2)	336161276892959 (2)	0.62104302
193	286833996987264	336161276892959 (1)	336161276892959 (1)	0.62104302
197	286833996987264	336161276892959 (1)	336161276892959 (1)	0.62104302
199	336161276892959	336161276892959 (0)	336161276892959 (0)	0.62104302
211	2679591249464415	11730619043063480 (4)	11730619043063480 (4)	0.64636237
223	2679591249464415	11730619043063480 (1)	11730619043063480 (1)	0.64636237
227	11730619043063480	11730619043063480 (0)	11730619043063480 (0)	0.64636237
229	11730619043063480	11730619043063480 (0)	11730619043063480 (0)	0.64636237
233	11730619043063480	11730619043063480 (0)	11730619043063480 (0)	0.64636237

TABLE 3. M_p, N_p, and H_p values for $p \leq 233$. The parentheses contain the number of values of M ($\geq M_p$) satisfying conditions 1 and 2 following Equation (5–1) that must be found before we get N_p or H_p.

$$D_{239} = 1277940310026058671502549282465791604406740386372469703971977730388605965505368 1$$
$$R = 1828710892199575366719923026577114267694 5.486446669$$
$$L(1,\chi) = 10.23103953006555$$
$$\rho(D_{239}) = 3985513948589296828176189144643791044 88.73182644883$$

Quantities relative to D_{239}.

days for the 80-digit D_{239}. In order to guarantee the correctness of our results under the ERH, we also performed the verification described in [Jacobson 1999, Chapter 3] for the four smallest D_p values. The algorithm used to compute the regulator assumes that a certain finite set of prime ideals called the factor base contains a complete generating system of the class group. A theorem of Bach [1990] gives an upper bound on the norms of the prime ideals which form such a generating system. Thus, to verify that the factor base used contains a generating system, we need to show that every prime ideal less than Bach's bound but not in the factor base is equivalent to some power-product of prime ideals in the factor base.

Unfortunately, this computation currently appears to be infeasible for our largest two discriminants. In order to be able to compute the regulators, we were forced to use much smaller factor bases than required by Bach's theorem, and as a result there were too many prime ideals which had to be verified. Hence, we proceeded as follows. For both discriminants, every ideal in the factor base used was principal since the class number computed was 1. If these factor bases did not contain complete generating systems, then by Bach's theorem there would have to be prime ideals with norm less than Bach's bound but not in the factor bases which were not principal and the actual class number would be greater than 1. Thus, if we run the algorithm again using a larger factor base which is guaranteed by Bach's theorem to contain a generating system, and we still get class number 1, we can conclude that 1 must be the actual class number under the ERH. The difficulty of the linear algebra prevents us from computing the class number and regulator simultaneously using such large factor bases, but for the purposes of verification we can simply use the regulator computed using the smaller factor base. The linear algebra required to compute only the class number is much simpler than that required to simultaneously compute R, and in particular is manageable even with these larger factor base sizes. In order to verify the computation for D_{233} we needed to use a factor base containing 5800 prime ideals and for D_{239} we needed 6900. The CPU time required was about 9 hours for D_{233} and just under 1.4 days for D_{239}.

Thus, we see from the data above that it is possible to find values of $\rho(D)$ satisfying (5–2), even for quite large values of D. The mystery here resides in how to prove that (5–2) is true infinitely often.

ACKNOWLEDGEMENTS

The authors thank the Centre for Applied Cryptographic Research at the University of Waterloo for their support and for the use of their computing facilities.

REFERENCES

[Bach 1990] E. Bach, "Explicit bounds for primality testing and related problems", *Math. Comp.* **55**:191 (1990), 355–380.

[Beiler 1964] A. H. Beiler, *Recreations in theory of numbers: the queen of mathematics entertains*, Dover, New York, 1964.

[Carmichael 1959] R. D. Carmichael, *The theory of numbers and Diophantine analysis*, Dover Publications Inc., New York, 1959.

[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, Berlin, 1984.

[Cohn 1962] H. Cohn, *A second course in number theory*, Wiley, New York, 1962.

[Fung and Williams 1990] G. W. Fung and H. C. Williams, "Quadratic polynomials which have a high

density of prime values", *Math. Comp.* **55**:191 (1990), 345–353.

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

[Jacobson 1999] M. J. Jacobson, Jr., *Subexponential class group computation in quadratic orders*, Shaker Verlag, Aachen, 1999. Ph.D. Thesis, Technische Universität Darmstadt, Germany.

[Jacobson et al. 1995] M. J. Jacobson, Jr., R. F. Lukes, and H. C. Williams, "An investigation of bounds for the regulator of quadratic fields", *Experiment. Math.* **4**:3 (1995), 211–225.

[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.

[Lehmer 1928] D. H. Lehmer, "On the multiple solutions of the Pell equation", *Annals of Math.* **30** (1928), 66–72.

[LiDIA 1997] The LiDIA Group, "LiDIA: a C++ library for computational number theory", software, Technische Universität Darmstadt, Germany, 1997. See http://www.informatik.tu-darmstadt.de/TI/LiDIA.

[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 Arch. Wisk.* (4) **13**:1 (1995), 113–139.

[Lukes et al. 1996] R. F. Lukes, C. D. Patterson, and H. C. Williams, "Some results on pseudosquares", *Math. Comp.* **65**:213 (1996), 361–372, S25–S27.

[Mollin 1996] R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, FL, 1996.

[Roberts 1992] J. Roberts, *Lure of the integers*, Mathematical Association of America, Washington, DC, 1992.

[Shanks 1960] D. Shanks, "On the conjecture of Hardy & Littlewood concerning the number of primes of the form $n^2 + a$", *Math. Comp.* **14** (1960), 320–332.

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

[Stephens and Williams 1988] A. J. Stephens and H. C. Williams, "Some computational results on a problem concerning powerful numbers", *Math. Comp.* **50**:182 (1988), 619–632.

[Yamamoto 1971] Y. Yamamoto, "Real quadratic number fields with large fundamental units", *Osaka J. Math.* **8** (1971), 261–270.

Michael J. Jacobson, Jr., Department of Computer Science, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada (jacobs@cs.umanitoba.ca)

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

Received June 1, 1999; accepted in revised form May 26, 2000