Canad. J. Math. Vol. **52** (2), 2000 pp. 369–380

An Upper Bound on the Least Inert Prime in a Real Quadratic Field

Andrew Granville, R. A. Mollin and H. C. Williams

Abstract. It is shown by a combination of analytic and computational techniques that for any positive fundamental discriminant $D > 3705$, there is always at least one prime $p < \sqrt{D}/2$ such that the Kronecker symbol $\left(D/p\right) = -1$.

1 Introduction

Let D be the fundamental discriminant of a real quadratic field and let

$$\begin{aligned}\mathcal{S} = \{&5, 8, 12, 13, 17, 24, 28, 33, 40, 57, 60, 73, 76, 88, 97, 105, 124, 129,\\ &136, 145, 156, 184, 204, 249, 280, 316, 345, 364, 385, 424, 456, 520,\\ &609, 616, 924, 940, 984, 1065, 1596, 2044, 2244, 3705\}.\end{aligned}$$

At the end of Chapter 6 of [5], the second author made the following conjecture.

Conjecture If D is a positive fundamental discriminant for which the Kronecker symbol $(D/p) = 0$ or 1 for every $p \le \sqrt{D}/2$ then $D \in \mathcal{S}$.

He also verified the truth of this conjecture for all $D < 10^7$ and suggested that a combination of analytic and computational techniques might suffice to establish the truth of the conjecture. In this paper we justify this optimism by so proving the conjecture.

One can easily prove the conjecture under the assumption of the Extended Riemann Hypothesis (ERH), as follows. Theorem 3 of Bach [1] states that if G is a nontrivial subgroup of $(\mathbb{Z}/m)^*$ such that $n \in G$ for all positive $n < x$ relatively prime to m, then $x < 3\log^2 m$. For a fundamental discriminant D we let $G = \{g \in (\mathbb{Z}/D)^* : (D/g) = 1\}$ and $y = \lfloor 3\log^2 D \rfloor + 1 > 3\log^2 D$. By Bach's result there must exist some $n \in (\mathbb{Z}/D)^*$ such that $0 < n \le y$ and $(D/n) = -1$. It follows that there must exist some prime p (dividing n) for which $(D/p) = -1$ and $p \le n \le 3\log^2 D + 1$. Since $3\log^2 D + 1 < \sqrt{D}/2$ when $D > 10^7$, we see that the conjecture must hold under the ERH.

Our unconditional proof of the conjecture comes in two parts. First we verify the truth of the conjecture up to quite large values of D (up to 10^{18}) by making use of a numerical sieving device. Second we prove the conjecture for all D beyond where the computations left off, via certain explicit estimates in analytic number theory.

Received by the editors October 29, 1998.
The first author is a Presidential Faculty Fellow. His research is partially supported by the NSF. The research of the other two authors is partially supported by NSERC of Canada.
AMS subject classification: 11Y11, 11Y40.

p	L	p	L
3	33	127	13461106065
5, 7	105	131	30741261145
11	345	137	40527839121
13	1065	139	275130569065
17	1785	149	275592648265
19, 23, 29, 31	3705	151	474533053553
37	106401	157	974494345825
41	108969	163	3613629418305
43	287049	167	5980467148705
47, 53, 59	369105	173, 179	16279597994529
61, 67	7401849	181, 191	90437661760345
71	11128425	193, 197	143685718819185
73	33692785	199, 211	723969210943185
79	34242945	223	1179371456358865
83	158402409	227, 229	4061838728897569
89, 97, 101	472585905	233, 239	50557062201005305
103	1426585329	241, 251	73018770354975481
107, 109	5296689489	257	$> 2.6 \cdot 10^{17}$

Table 1: Least $L \equiv 1 \pmod 8$ with $(L/q) = 0$ or 1 for all odd $q \leq p$.

Since D is a fundamental discriminant, we have either $D \equiv 1 \pmod 4$ or $4|D$ with $D/4 \equiv 2, 3 \pmod 4$. Since $(D/2) = -1$ for $D \equiv 5 \pmod 8$, we need only consider values of D such that $D = L \equiv 1 \pmod 8$ or $D = 4L$, where $L \equiv 2, 3 \pmod 4$.

To deal with the small discriminants we computed the three tables below (corresponding to $L \equiv 1 \pmod 8$, 2 and 3 (mod 4), respectively). We used the Manitoba Scalable Sieving Unit (see Lukes *et al.* [4]) over a period of four or five months to produce Tables 1, 2 and 3 below.

From Table 1 we see that if $D = L \equiv 1 \pmod 8$ and $D \leq 2.6 \times 10^{17}$ then there exists $q \leq 257 < \sqrt{D}/2$ (since $D > 10^7$) for which $(D/q) = -1$, so verifying the conjecture in this range for odd discriminants D.

From Tables 2 and 3 we see that if $D = 4L$ where $L \equiv 2$ or 3 (mod 4), and $D \leq 4 \times 2.6 \times 10^{17} = 1.04 \times 10^{18}$, then there exists odd $q \leq 283 < \sqrt{D}/2$ (since $D > 10^7$) for which $(D/q) = (L/q) = -1$, so verifying the conjecture in this range for even discriminants D.

Both the growth rate of the L values in Tables 1, 2, 3, and the truth of the conjecture under the ERH strongly suggest that the conjecture must be true unconditionally. In the remainder of the paper we furnish a proof of the following theorem.

Theorem 1.1 *Suppose that D is a fundamental discriminant. If $D \geq 10^{18}$, or if D is odd and $D \geq 10^{16}$, then there exists a prime $p \leq \sqrt{D}/2$ for which $(D/p) = -1$.*

In view of the results mentioned above, this means that the conjecture is true unconditionally.

p	L	p	L
3, 5	6	127, 131	6941299170
7	30	137, 139, 149	13803374706
11	70	151	95257780930
13	114	157	461441566546
17	246	163, 167, 173	614275135530
19	1050	179	1323134476426
23	1290	181, 191	2716216673394
29, 31	3094	193	47007322131630
37	16930	197, 199	160631220621466
41	30430	211	238205916998674
43	48174	223	611465805367330
47	62934	227, 229	1873686407687494
53, 59	214230	233, 239	5644324196384910
61	569130	241, 251	18038239971912966
67, 71, 73	860574	263	20425607181761226
79	9361374	257, 269, 271	43208475923671906
83, 89, 97, 101	11993466	277, 281	95444433358852510
103	287638530	283	$> 2.6 \cdot 10^{17}$
107, 109	697126530		

Table 2: Least $L \equiv 2 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \leq p$.

There is an elementary and clever proof in Western and Miller ([9, pp. xi–xii]) that if q is any odd prime and p is the least odd prime such that $(p/q) = -1$, then $p < \sqrt{q} + 1$. However, it is not obvious how this argument could be modified to prove that $p < C\sqrt{q}$ with constant $C < 1$. Norton [6] has shown by much deeper arguments that $p < 1.1q^{1/4}(\log q + 4)$, thereby establishing the truth of Theorem 1.1 when D is a prime.

By the method developed in this paper it is possible to prove a result like: "For any $C > 0$ there exists a calculable constant D_C, such that if $D \geq D_C$ is a fundamental discriminant then there exists a prime $p \leq C\sqrt{D}$ for which $(D/p) = -1$." However if C is much smaller than $1/2$ then the value of D_C we obtain is so large that we will not be able to determine whether the result holds for a large range of smaller D. In fact the function $C\sqrt{D}$ can be replaced by any function of the form D^λ for any given $\lambda > 1/2\sqrt{e}$.

In our proof we will prove a version of the Polya-Vinogradov inequality (Theorem 2.2 below) suitable for us to obtain small bounds. We could replace the use of the Polya-Vinogradov inequality by Burgess's character sum estimates [2]. Noting that the conductors of the characters we are investigating are squarefree, one can prove: "For any $\lambda > 1/4\sqrt{e}$ there exists a calculable constant D_λ, such that if $D \geq D_\lambda$ is a fundamental discriminant, then there exists a prime $p \leq D^\lambda$ for which $(D/p) = -1$." However, "back of the envelope" calculations suggest that D_λ will be enormous, well beyond the range of computation.

p	L	p	L
3	3	131, 137	25856763139
5, 7, 11	15	139, 149	147774098679
13	91	151	156883882611
17, 19, 23, 29	399	157	268065962395
31, 37	14611	163	1088511866311
41	21099	167	1680435020859
43	41155	173	5947699157079
47	43059	179, 181, 191, 193	9551743094859
53, 59, 61, 67	182919	197, 199	126316077604831
71	2190279	211	444079813923295
73	3777855	223, 227, 229, 233	1062483479555355
79, 83	8042479	239, 241, 251	4833899440864935
89, 97, 101	12129315	257, 263, 269, 271	40801368051299571
103, 107, 109	78278655	277	$> 2.6 \cdot 10^{17}$
127	6091232455		

Table 3: Least $L \equiv 3 \pmod 4$ with $(L/q) = 0$ or 1 for all odd $q \le p$.

2 Preliminary Results

For a given D we define $B = \sqrt{D}/2$ and we will assume in the sequel that $(D/p) = 0, 1$ for every prime $p \le B$. Thus, if $(D/n) = -1$, then n must be divisible by a prime which exceeds B. Indeed, if $n \le N \le B^2 = D/4$, then there must be a unique prime divisor p of n such that $(D/p) = -1$. It follows that

$$\sum_{n \le N} \left(\frac{D}{n}\right) = \sum_{\substack{n<N \\ (n,D)=1}} 1 - 2 \sum_{\substack{B<p\le N \\ (D/p)=-1}} \sum_{\substack{n=mp\le N \\ (m,D)=1}} 1. \tag{2.1}$$

Our goal is to show that (2.1) cannot hold. To do this we will need to find explicit inequalities for the three main terms here. We begin with the easiest, the first term on the right side of (2.1):

Let $\nu(s)$ denote the number of distinct primes that divide $s \in \mathbb{Z}$. If prime p does not divide r then

$$\sum_{\substack{m\le x \\ (m,rp)=1}} 1 = \sum_{\substack{m\le x \\ (m,r)=1}} 1 - \sum_{\substack{pm\le x \\ (m,r)=1}} 1.$$

Therefore by induction on $\nu(R)$ one can establish the following elementary sieve lemma.

Lemma 2.1 *Let R and X be positive integers; then*

$$\left| \sum_{\substack{m\le X \\ (m,R)=1}} 1 - \frac{\phi(R)}{R} X \right| < 2^{\nu(R)-1},$$

where $\phi(m)$ is Euler's phi function.

Therefore

$$\sum_{\substack{n\le N\\(n,D)=1}} 1 \ge \frac{\phi(D)}{D}N - 2^{\nu(D)-1}. \tag{2.2}$$

Next we develop an upper bound for the character sum in (2.1). To do this we will derive a version of the Polya-Vinogradov inequality

$$\left|\sum_{n\le N}\left(\frac{D}{n}\right)\right| < \sqrt{D}\log D$$

in which the upper bound depends more explicitly on the prime divisors of D.

Theorem 2.2 *For any real numbers M and N and for any primitive character modulo q, we have*

$$\Big|\sum_{M<n\le M+N}\chi(n)\Big| \le \frac{2\sqrt{q}}{\pi}\frac{\phi(q)}{q}\left(\log q + c_1 + \sum_{p\mid q}\frac{\log p}{p-1}\right) + \frac{2^{\nu(q)+2}}{\pi\sqrt{q}}, \tag{2.3}$$

where $c_1 := \gamma - \log 2 + \pi/2 - 1 = .454864811\ldots$.

Putting $\chi(n) = (D/n)$ and $M = 0$ in (2.3), we deduce that

$$\left|\sum_{n\le N}\left(\frac{D}{n}\right)\right| \le \frac{2\sqrt{D}}{\pi}\frac{\phi(D)}{D}\left(\log D + c_1 + \sum_{p\mid D}\frac{\log p}{p-1}\right) + \frac{2^{\nu(D)+2}}{\pi\sqrt{D}}, \tag{2.4}$$

which is what we shall use to bound the left side of (2.1).

Obtaining bounds on the double sum in (2.1) is a somewhat delicate process which will require different techniques when $D \ge 10^{32}$ and $D < 10^{32}$. We postpone this investigation until the next section. We dedicate the remainder of this section to the proof of Theorem 2.2:

In order to do this we first modify slightly the proof in Chapter 23 of Davenport [3] to derive for any primitive character $\chi \pmod q$ the inequality

$$\Big|\sum_{M<n\le M+N}\chi(n)\Big| \le \frac{2}{\sqrt{q}}\sum_{\substack{1\le a\le q/2\\(a,q)=1}}\frac{1}{\sin(\pi a/q)}.$$

Now for $0 < x \le \pi/2$, the function $1/\sin x - 1/x$ is increasing; consequently, $1/\sin x \le 1/x + (1 - 2/\pi)$. It follows from the inequality above that

$$\Big|\sum_{M<n\le M+N}\chi(n)\Big| \le \frac{2\sqrt{q}}{\pi}\sum_{\substack{1\le a\le q/2\\(a,q)=1}}\frac{1}{a} + \left(1-\frac{2}{\pi}\right)\frac{\phi(q)}{\sqrt{q}}. \tag{2.5}$$

Also,

$$\sum_{\substack{1\le a\le x\\(a,q)=1}}\frac{1}{a}=\sum_{d|q}\mu(d)\sum_{1\le db\le x}\frac{1}{db}=\sum_{d|q}\frac{\mu(d)}{d}\sum_{1\le b\le x/d}\frac{1}{b}, \tag{2.6}$$

For any real positive x, let $f(x)=\sum_{m\le x}\frac{1}{m}-\log x-\gamma$, where $\gamma=.5772156649\ldots$ is Euler's constant. It is well known that $f(x)\to 0$ as $x\to\infty$. Moreover

$$0<f(x)-f(x+1)=\log\left(1+\frac{1}{x}\right)-\frac{1}{x+1}<\frac{1}{x}-\frac{1}{(x+1)}.$$

Telescoping gives

$$0<f(x)-f(x+k)<\frac{1}{x}-\frac{1}{x+k},$$

and letting $k\to\infty$, we find that

$$0<f(x)<\frac{1}{x}. \tag{2.7}$$

From (2.6) and (2.7) we therefore deduce

$$\left|\sum_{\substack{1\le a\le x\\(a,q)=1}}\frac{1}{a}-\sum_{d|q}\frac{\mu(d)}{d}\big(\log(x/d)+\gamma\big)\right|\le\sum_{d|q}\frac{\mu^2(d)}{d}|f(x/d)|\le\frac{2^{\nu(q)}}{x}. \tag{2.8}$$

It is well known that

$$\sum_{d|q}\mu(d)/d=\phi(q)/q$$

and it is easy to establish by induction on $\nu(q)$ that

$$-\sum_{d|q}\frac{\mu(d)\log d}{d}=\frac{\phi(q)}{q}\sum_{p|q}\frac{\log p}{p-1},$$

where the latter sum is over all the distinct prime divisors of q. Thus, from (2.8) we deduce that

$$\left|\sum_{\substack{1\le a\le x\\(a,q)=1}}\frac{1}{a}-\frac{\phi(q)}{q}\left(\log x+\gamma+\sum_{p|q}\frac{\log p}{p-1}\right)\right|\le\frac{2^{\nu(q)}}{x}. \tag{2.9}$$

By referring back to (2.5) and using (2.9) with $x=q/2$, we get Theorem 2.2.

3 Two Inequalities

We first prove a somewhat technical sifting lemma.

Lemma 3.1 *If $x \geq 4.7 \times 10^{15}$ and s is the product of all the primes $\leq 14 \log x$, then*

$$\pi(x) \leq \frac{1}{3}\#\{n \leq x : (n, s) = 1\},$$

where, as usual, $\pi(x)$ is the prime counting function.

Proof Set $y := 14 \log x$. Let R denote the product of the primes $\leq Y (< y)$; clearly $R|s$. By repeated applications of Lemma 2.1, it is easy to deduce that

$$\sum_{\substack{n \leq x \\ (n,s)=1}} 1 \geq \sum_{\substack{n \leq x \\ (n,R)=1}} 1 - \sum_{Y < p \leq y} \sum_{\substack{pm \leq x \\ (m,R)=1}} 1 \geq \frac{\phi(R)}{R}\left\{x - \sum_{Y < p \leq y} \frac{x}{p}\right\} - 2^{\nu(R)-1}\pi(y). \tag{3.1}$$

Put $Y = \sqrt{y} > 22.47$. By (3.17) and (3.20) of Rosser and Shoenfeld [7], we get

$$\sum_{Y < p \leq y} \frac{1}{p} \leq \log 2 + \frac{3}{4(\log Y)^2}. \tag{3.2}$$

By (3.30) of [7] we find that

$$\phi(R)/R > e^{-\gamma}/(\log Y + 1/\log Y). \tag{3.3}$$

Furthermore, by Theorem 2 of [7] we get

$$2^{\nu(R)-1}\pi(y) = 2^{\pi(Y)-1}\pi(y) \leq 2^{Y/(\log Y - 3/2)-1} y/(\log y - 3/2) < x/3\log^2 x. \tag{3.4}$$

Also, since $\pi(x) < x/(\log x - 3/2)$ (Theorem 2 of [7]), we see by (3.1), (3.2), (3.3) and (3.4) that if the lemma is false, then

$$3\frac{3}{(\log x - 3/2)} + \frac{x}{3\log^2 x} > \frac{e^{-\gamma}x}{(\log Y + 1/\log Y)}\left(1 - \log 2 - \frac{3}{4\log^2 Y}\right),$$

which does not hold for $x \geq 10^{36}$, by computation.

We now consider the case of $x < 10^{36}$. We note from (3.1) that if the lemma is false then

$$3\frac{x}{(\log x - 3/2)} + \pi(y)2^{\pi(Y)-1} > x\prod_{p \leq Y}\left(1 - \frac{1}{p}\right)\left\{1 - \sum_{Y < p \leq y}\frac{1}{p}\right\}. \tag{3.5}$$

Since $x < 10^{36}$, we have $y < 1161$ and $\pi(y) \leq \pi(1160) = 191$. If we put $Y = 186$, we find that (3.5) is false for $x \geq 1.16 \times 10^{18}$. For $x < 1.16 \times 10^{18}$, we have $y < 583$ and $\pi(y) \leq \pi(582) = 106$. If we put $Y = 160$, we find that (3.5) is false for $x \geq 1.06 \times 10^{16}$. Continuing in this fashion, we have $y < 517$ and $\pi(y) \leq 97$ and (3.5) is false for $Y = 144$ and $x \geq 5.3 \times 10^{15}$. Thus, we may assume $y < 507$ and $\pi(y) \leq 96$. Taking $Y = 150$, we get that (3.5) is false for $x \geq 4.7 \times 10^{15}$. ∎

We will also require an explicit prime number theorem.

Lemma 3.2 *If $x \geq B \geq 1.2 \times 10^6$, then*

$$\pi(x) - \pi(B) \leq .0024\frac{B}{\log B} + 1.0011\big(\mathrm{Li}(x) - \mathrm{Li}(B)\big).$$

Proof We note that Schoenfeld [8] has shown that for $x > 1.16 \times 10^6$, we have

$$.9987x < \theta(x) < 1.0011x.$$

Thus, we have

$$\begin{aligned}\pi(x) - \pi(B) = \int_B^x \frac{d\theta(t)}{\log t} &= \left[\frac{\theta(t)}{\log t}\right]_B^x + \int_B^x \frac{\theta(t)dt}{t\log^2 t} \\ &\leq -\frac{\theta(B)}{\log B} + 1.0011\left(\frac{x}{\log x} + \int_B^x \frac{dt}{\log^2 t}\right) \\ &\leq \left(1.011\frac{B}{\log B} - \frac{\theta(B)}{\log B}\right) + 1.0011\big(\mathrm{Li}(x) - \mathrm{Li}(B)\big) \\ &\leq .0024\frac{B}{\log B} + 1.0011\big(\mathrm{Li}(x) - \mathrm{Li}(B)\big).\end{aligned}$$

■

4 Proof of the Theorem when $D \geq 10^{32}$

In this section we will show that (2.1) cannot hold when $D \geq 10^{32}$. We first define for any positive z and integer m

$$g_m(z) = \sum_{\substack{x \leq z \\ (m,x)=1}} 1$$

and note that if s is any prime divisor of m, then

$$g_m(z) = g_{m/s}(z) - \#\{sn : n \leq z/s, (n, m/s) = 1\}. \tag{4.1}$$

We next set $y_1 := (12/\pi)(\log D + \log\log D + .3664215)$, $y_2 = 14\log B$, $N = By_1$.

Since $B \geq 5 \times 10^{15}$, it is not difficult to show that

$$y_2 > \left(y_1\left(1 + \frac{1}{2\log y_1}\right) + \log D\right) \Big/ \left(1 - \frac{1}{\log y_1}\right).$$

Since $y_2 > y_1 > 41$, we see from (3.15) and (3.16) of[7] that

$$\theta(y_2) \geq y_2(1 - 1/\log y_2) > y_1(1 + 1/2\log y_1) + \log D \geq \theta(y_1) + \log D. \tag{4.2}$$

It follows that the product of the primes in the interval $(y_1, y_2]$ is greater than the product of the primes in D. Now let R denote the product of all the distinct primes $\leq y_2$ and let r

denote the (squarefree) product of all the distinct primes $\le N/B = y_1$ and those ($> y_1$) which divide D. Next, let q be the largest prime that divides r.

If $r|R$, then $g_r(z) \ge g_R(z)$. If $r \nmid R$, then there must exist a least prime p that divides R but does not divide r. There must also exist a prime s such that $s|r$ and $s \nmid R$; hence, $s > y_2$. Since $q \ge s$, we get $q > y_2 \ge p$. It follows that

$$\#\{qn : n < z/q, (n, r/q) = 1\} \le \#\{pn : n \le z/p, (n, r/q) = 1\}.$$

By applying (4.1) twice, we find that

$$g_{rp/q}(z) \le g_{r/q}(z) - \#\{qn : n \le z/q, (n, r/q) = 1\} = g_r(z).$$

By iterating this procedure, we finally get

$$g_{tR}(z) \le g_r(z)$$

for some t; hence, we always have

$$g_r(z) \ge g_R(z). \tag{4.3}$$

We now examine the double sum term in (2.1). By Lemma 3.1 with $x = N/m \ge B > 4.7 \times 10^{15}$ and $s = R$ and (4.3) we get

$$\begin{aligned} 2 \sum_{\substack{B<p\le N \\ (D/p)=-1}} \sum_{\substack{n=mp\le N \\ (m,D)=1}} 1 &\le 2 \sum_{\substack{m\le N/B \\ (m,D)=1}} \pi\left(\frac{N}{m}\right) \le \frac{2}{3} \sum_{\substack{m\le N/B \\ (m,D)=1}} \sum_{\substack{k\le N/m \\ (k,R)=1}} 1 \\ &\le \frac{2}{3} \sum_{\substack{m\le N/B \\ (m,D)=1}} \sum_{\substack{k\le N/m \\ (k,r)=1}} 1 \le \frac{2}{3} \sum_{\substack{n\le N \\ (n,r)=1}} 1. \end{aligned} \tag{4.4}$$

The last inequality follows from taking $n = mk \le m(N/m) = N$ and noting that any $n \le N$ has at most one such representation. This is because m will be the product of powers of primes $\le N/B = y_1$ which divide n, and all such primes divide r.

Since the squarefree kernel of D divides r, we have $g_D(z) \ge g_r(z)$; hence, by (2.1) and (4.4) we get

$$\sum_{\substack{n\le N \\ (n,D)=1}} 1 \le 3\left|\sum_{n\le N}\left(\frac{D}{n}\right)\right|. \tag{4.5}$$

Substituting (2.2) and (2.4) into (4.5) and multiplying through by $D/\phi(D)$, we obtain the inequality

$$N \le \frac{6\sqrt{D}}{\pi}\left(\log D + c_1 + \sum_{p|D} \frac{\log p}{p-1}\right) + 2^{\nu(D)} \frac{D}{\phi(D)}\left(\frac{1}{2} + \frac{12}{\pi\sqrt{D}}\right). \tag{4.6}$$

Define

$$\gamma_D := \sum_{p|D} \frac{\log p}{p-1}.$$

Note that if $D_{k+1} > D \geq D_k$, where D_k is the product of the first k primes, then $\gamma_D - \log\log D \leq \gamma_{D_k} - \log\log D_k$, since D must have $\leq k$ distinct prime factors.

We now consider the value of $\gamma_{D_k} - \log\log D_k$. From (2.8) of [7], a constant E is defined by

$$E = -\gamma + \sum_p \frac{\log p}{p(p-1)};$$

hence, by (3.16) and (3.23) of [7], we can easily derive

$$\gamma_{D_k} - \log\log D_k \leq \frac{1}{\log x} - \log\left(1 - \frac{1}{\log x}\right) - \gamma \tag{4.7}$$

for $x = p_k$ (the k-th prime) > 41. For $D \geq 10^{32}$, we have $p_k \geq 79$ and by (4.7)

$$\gamma_{D_k} - \log\log D_k < -.08846604.$$

We may therefore assume that

$$\gamma_D < \log\log D - .08846604. \tag{4.8}$$

We also notice that $2p/(p-1) < p^{1/3}$ for any $p \geq 11$, so that $2^{\nu(D)}D/\phi(D) \leq (9.35)D^{1/3}$. Putting this and (4.8) into (4.6) we get

$$N < \frac{6\sqrt{D}}{\pi}(\log D + \log\log D + .3664215) = By_1 = N,$$

a contradiction. Thus, if $D \geq 10^{32}$, we see that (2.1) cannot hold. It follows that we have proved Theorem 1.1 for all values of $D \geq 10^{32}$.

5 Proof of the Theorem when $D \leq 10^{32}$

We will assume in what follows that $D \leq U$ for some given U, beginning with $U = 10^{32}$. We now rewrite (2.1) as

$$\sum_{\substack{n\leq N\\(n,D)=1}} 1 \leq \left|\sum_{n\leq N}\left(\frac{D}{n}\right)\right| + 2\sum_{\substack{m\leq N/B\\(m,D)=1}} \big(\pi(N/m) - \pi(B)\big). \tag{5.1}$$

Putting $y = N/B$, we see by Lemma 3.2 that

$$2\sum_{\substack{m\leq N/B\\(m,D)=1}} \big(\pi(N/m) - \pi(B)\big) \leq 2\sum_{\substack{m\leq y\\(m,A)=1}} \left\{.0024\frac{B}{\log B} + 1.0011\big(\mathrm{Li}(N/B) - \mathrm{Li}(B)\big)\right\} \tag{5.2}$$

for any integer A which divides B. By combining (5.1) and (5.2) with (2.2) and (2.4), dividing through by N and noting that $\sqrt{D} > 2$ and $2B = \sqrt{D}$, we obtain the inequality

$$\frac{\phi(D)}{D}\left(1-\frac{y_D}{y}\right) \le \frac{2^{\nu(D)}}{By}\left(\frac{2}{\pi B}+\frac{1}{2}\right) + \frac{2}{By}\sum_{\substack{m\le y\\(m,A)=1}}\left(.0024\frac{B}{\log B}+1.0011\big(\mathrm{Li}(By/m)-\mathrm{Li}(B)\big)\right), \tag{5.3}$$

where $y_D := (4/\pi)\left(\log D + c_1 + \gamma_D\right)$.

Define A to be the product of all prime $s \le 19$ dividing D and define R to be the product of the primes between 23 and the largest prime q such that $\Delta := AR \le U$. We have $\nu(D) \le \nu(\Delta)$, $\gamma_D \le \gamma_\Delta$ and $\phi(D)/D \ge \phi(\Delta)/\Delta$. Putting $y_\Delta := (4/\pi)\left(2\log(2B) + c_1 + \gamma_\Delta\right) \ge y_D$, we see by (5.3) that

$$\frac{\phi(\Delta)}{\Delta}\left(1-\frac{y_\Delta}{y}\right) \le \frac{2^{\nu(\Delta)}}{By}\left(\frac{2}{\pi B}+\frac{1}{2}\right) + \frac{2}{By}\sum_{\substack{m\le y\\(m,A)=1}}\left\{.0024\frac{B}{\log B}+1.0011\big(\mathrm{Li}(By/m)-\mathrm{Li}(B)\big)\right\}. \tag{5.4}$$

We can easily test whether (5.4) holds. Our strategy will be the following. For each of the 256 divisors of $2\times3\times5\times7\times11\times13\times17\times19$, we can compute R and then take y to be some convenient value. We then determine a range for B for which (5.4) is false for every such A, adjust U and iterate.

To begin we took $y = 500$ and found that (5.4) is false for every possible A value when $B > 10^{11}$. This implies, then, that for (2.1) to hold, we must have $D < 4\times10^{22}$. Using this bound as our new U-value, we found that (5.4) is false for all possible values of A whenever $B > 2\times10^9$. This means that we need now only consider values of $D \le 1.6\times10^{19}$. Using this as our new U-value, we discovered that (5.4) is false for every possible value of A when $B > 6\times10^8$; hence $D \le 1.44\times10^{18}$. After adjusting our U-value to 1.44×10^{18} and our y-value to 700 we verified that (5.4) is false for every A when $B \ge 5\times10^8$; this implies that we may assume $D \le 10^{18}$. Unfortunately, our next iteration gives a negligible improvement; however, if we work with only odd D, we must have A odd. In this case we found that (5.4) is false for every such $A(U = 10^{18}, y = 500)$ when $B \ge 5\times10^7$; hence $D \le 10^{16}$. Thus, we have now proved Theorem 1.1 and, as a consequence, the conjecture.

Acknowledgements The authors would like to thank Carl Pomerance for some very useful conversations. They would also like to express their appreciation to Wasyl Baluta and Edlyn Teske for their assistance in producing Tables 1, 2, 3.

References

[1] E. Bach, *Explicit bounds for primality testing and related problems.* Math. Comp. **55**(1990), 355–380.
[2] D. A. Burgess, *n character sums and L-series, I.* Proc. London Math. Soc. **12**(1962), 193–206.

[3] H. Davenport, *Multiplicative Number Theory.* 2nd edn, Springer-Verlag, New York, 1980.
[4] R. F. Lukes, C. D. Patterson and H. C. Williams, *Some results on pseudosquares.* Math. Comp. **65**(1996), 361–372.
[5] R. A. Mollin, *Quadratics.* CRC Press, Boca Raton, 1995.
[6] K. K. Norton, *Bounds for sequences of consecutive power residues.* Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, RI, 1973, 213–220.
[7] J. B. Rosser and L. Schoenfeld, *Approximate formulae for some functions of prime numbers.* Illinois J. Math. **6**(1962), 64–94.
[8] L. Schoenfeld, *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$.* Math. Comp. **30**(1976), 337–360, 900.
[9] A. E. Western and J. C. P. Miller, *Tables of Indices and Primitive Roots.* Royal Society, Cambridge, 1968.

Department of Mathematics
University of Georgia
Athens, GA 30602
USA
email: andrew@math.uga.edu

Department of Mathematics and Statistics
University of Calgary
Calgary, AB
T2N 1N4
email: ramollin@math.ucalgary.ca

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba
R3T 2N2
email: williams@cs.umanitoba.ca