A Problem Concerning a Character Sum

Edlyn Teske and Hugh C. Williams

Dedicated to the memory of Daniel Shanks (1917–1996)

CONTENTS

Let p be a prime congruent to -1 modulo 4, $\left(\frac{n}{p}\right)$ the Legendre symbol and $S(k) = \sum_{n=1}^{p-1} n^k \left(\frac{n}{p}\right)$. The problem of finding a prime p such that $S(3) > 0$ was one of the motivating forces behind the development of several of Shanks' ideas for computing in algebraic number fields, although neither he nor D. H. and Emma Lehmer were ever successful in finding such a p. In this paper we exhibit some techniques which were successful in producing, for each k such that $3 \leq k \leq 2000$, a value for p such that $S(k) > 0$.

1. INTRODUCTION

Shortly after the death of Daniel Shanks, the second author received a collection of correspondence between Shanks and D. H. and Emma Lehmer. This material covers the period 1968–1971, when Shanks was very active in developing ideas that would be of great significance to the development of computational algebraic number theory. Furthermore, it is evident from this correspondence that a rather simple looking problem served as a focus for his and the Lehmers' investigations during this time. In order to discuss their problem we first require some notation. We let d denote a fundamental discriminant of an imaginary quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ and let $h(d)$ denote the class number of $\mathbb{K}$. A brief letter, dated April 2, 1968, from the Lehmers to Shanks, mentions the problem of trying to produce a small value for the ratio

$$\lambda(p) = h(-p)/\sqrt{p},$$

where p is a prime congruent to 3 modulo 8:

> We are trying to get this ratio down to .041. According to a theorem of Chowla there are infinitely many such primes, but we have not seen one yet. Any candidates?

Williams' research was supported by NSERC of Canada grant A7649.

1991 Mathematics Subject Classification: 11Y40, 11Y99

1058-6458/1999 \$0.50 per page

During the following year the Lehmers and Shanks made a concerted effort to find small values for $\lambda(p)$. By August 23 they had found $p = 2426489587$ with $h(-p) = 2925$ and $\lambda(p) = 0.05940$, breaking the "0.06 barrier"; and by September 26 they had found the best candidate that they ever discovered, namely $p = 85702502803$ with $h(-p) = 16259$ and $\lambda(p) = 0.05546$. It is important to realize that at this time, the fast methods for evaluating class numbers that are used today did not exist. Indeed, Shanks was motivated by this problem to develop fast methods because the Lehmers were producing large values of p as possible candidates. Throughout this correspondence it is possible to see Shanks develop and refine the ideas which were to culminate in a very important paper [Shanks 1971], where he introduced the baby-step–giant-step method for evaluating $h(d)$ and his method of factorization of d, based essentially on the determination of ambiguous ideal classes in the class group of $\mathbb{K}$. He even recognized that his technique for evaluating $h(d)$ was likely to be of complexity $O(|d|^{1/4+\varepsilon})$ for any $\varepsilon > 0$, but it was Lenstra [1982] who showed later that it was of complexity $O(|d|^{1/5+\varepsilon})$ under the Extended Riemann Hypothesis (ERH). This was a considerable improvement over the previous method of counting classes, a technique of complexity $O(|d|^{1/2+\varepsilon})$. Inspired by his success with imaginary quadratic fields, Shanks [1972] went on to discover what he called the "infrastructure" of the class group of a real quadratic field and how it could be applied to solve the problem of determining its regulator and class number.

In response to a question by Shanks about where the "theorem of Chowla" could be found, D. H. and Emma Lehmer mentioned that it in fact appeared in a paper by Ayoub, Chowla and Walum [Ayoub et al. 1967]. In this paper the authors discussed the character sum

$$S(k) = \sum_{n=1}^{p-1} n^k \left(\frac{n}{p}\right), \tag{1–1}$$

where p is a prime congruent to 3 modulo 4 and $\left(\frac{n}{p}\right)$ is the Legendre symbol. They pointed out that, while $S(1) = -ph(-p)$, $S(2) = -p^2h(-p)$ and

$$S(k) < 0 \quad \text{whenever } k \geq p-2,$$

they could prove that $S(3) > 0$ infinitely often. It is not immediately clear why this should mean that $\lambda(p) < 0.041$ infinitely often and no proof of this was ever provided by the Lehmers; however, the basic idea behind their thinking is suggested in the paper by the Lehmers and Shanks [Lehmer et al. 1970] which originated as a result of their collaboration. We illustrate this below.

As usual, we define the Dirichlet L-function by

$$L(s,\chi) = \sum_{n=1}^{\infty} n^{-s}\chi(n).$$

Also, if $\chi(n)$ is the Kronecker symbol $\left(\frac{d}{n}\right)$, the analytic class number formula for $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ asserts that

$$\frac{2\pi h(d)}{w\sqrt{|d|}} = L(1,\chi), \tag{1–2}$$

where w is the number of roots of unity in $\mathbb{K}$ ($w = 2$ if $|d| > 4$). When $d = -p \equiv 1 \pmod 4$, then

$$\chi(n) = \left(\frac{d}{n}\right) = \left(\frac{n}{p}\right).$$

In [Ayoub et al. 1967] it is shown that for this character

$$S(3) = \frac{p^3\sqrt{p}}{2\pi}\left(-L(1,\chi) + \frac{3}{2\pi^2}L(3,\chi)\right); \tag{1–3}$$

hence $S(3) > 0$ if and only if

$$L(1,\chi) < \frac{3}{2\pi^2}L(3,\chi). \tag{1–4}$$

Recalling the Euler product representation of $L(s,\chi)$,

$$L(s,\chi) = \prod_q \frac{q^s}{q^s - \chi(q)}, \tag{1–5}$$

where the product is taken over all the primes q, we see that

$$\begin{aligned} L(3,\chi) &= \prod_{q\leq 41} \frac{q^3}{q^3-\chi(q)} \prod_{q>41} \frac{q^3}{q^3-\chi(q)} \\ &\leq \prod_{q\leq 41} \frac{q^3}{q^3-\chi(q)} \prod_{q>41} \frac{q^3}{q^3-1}. \end{aligned}$$

Now let a be 4 times the product of all the primes less than or equal to 41 and b be a fixed integer such that the Kronecker symbol $\left(\frac{b}{q}\right) = -1$ for all the prime divisors of a. We have $(a,b) = 1$ and for any prime $p = ax + b$ we get $\chi(q) = -1$ for $q \leq 41$ and

$$L(3,\chi) < \zeta(3) \prod_{q\leq 41} \frac{q^3-1}{q^3+1} = 0.84644.$$

Since (1–2) and (1–4) imply $\lambda(p) < 3L(3,\chi)/2\pi^3$ when $S(3) > 0$, we see that $\lambda(p) < 0.041$ for such primes. Unfortunately, it is not proved in [Ayoub et al. 1967] that $S(3) > 0$ for infinitely many primes selected from the arithmetic progression $\{ax + b\}$. However, it is possible, by referring to a later theorem of Joshi [1970], to prove the Lehmers' assertion that $\lambda(p) < 0.041$ infinitely often without even requiring that $S(3) > 0$ infinitely often.

The Lehmers and Shanks never did find a value of p for which either $\lambda(p) < 0.041$ or $S(3) > 0$. They did, however, find several values of p for which $S(4) > 0$ [Lehmer et al. 1970], and in a letter dated June 5, 1969, they noted that $S(5), S(6) > 0$ for $p = 163$. In fact it is stated at the end of [Ayoub et al. 1967] that results similar to the existence of an infinitude of primes p such that $S(3) > 0$ hold for other small values of k. Later Fine [1970] proved the following result.

Theorem 1.1. *For each real $k > 2$ there are infinitely many primes $p \equiv 3 \pmod 4$ for which $S(k) > 0$ and infinitely many for which $S(k) < 0$.*

Unfortunately, Fine's method is not easily adapted to the problem of finding values for p such that $S(k) > 0$. The purpose of this paper is to show how to find such values of p for small integer values of k. Our initial objective was to discover values of p such that $S(k) > 0$ for $3 < k \le 50$, but we were somewhat surprised to learn that we could extend our method to do this for all $3 < k \le 2000$. We also exhibit a value of p for which $S(3) > 0$ and $\lambda(p) < 0.041$ under the ERH.

We want to emphasize at this point that the fact that our last result is conditional on the ERH does not make our value for p any less worthy a candidate for $S(3) > 0$ than those for which we get $S(k) > 0$ when $k > 3$. Indeed, all of the results on $\lambda(p)$ or $L(1,\chi)$ here are dependent on the truth of the ERH and those in [Lehmer et al. 1970] are implicitly dependent either on the truth of the ERH or some heuristic estimation of $L(1,\chi)$ by the truncated Euler product. The fact is that we currently have no algorithm for evaluating the class number h of a quadratic field of discriminant d (real or imaginary) which is provably better than $O(|d|^{1/2+\varepsilon})$ in complexity. This complexity measure is far too large to allow for the rigorous computation of h for the size of $|d|$ that we have to work with here.

2. OUR INITIAL STRATEGY

As was done in [Ayoub et al. 1967], we can expand x^k in a Fourier expansion with period 1 to obtain

$$S(k) = p^k\sqrt{p}\sum_{m=1}^{\infty} b_m(k)\Big(\frac{m}{p}\Big),$$

where

$$\frac{b_m(k)}{2} = \int_0^1 x^k \sin 2\pi m x\, dx.$$

Now, on integrating by parts,

$$\begin{aligned}\frac{b_m(k)}{2} &= \frac{1}{(2\pi m)^{k+1}}\int_0^{2\pi m} y^k \sin y\, dy\\ &= -\frac{1}{2\pi m} - \frac{k(k-1)}{(2\pi m)^2}\frac{b_m(k-2)}{2}.\end{aligned}$$

Also, $b_m(1) = b_m(2) = -1/(\pi m)$. Hence,

$$b_m(k) = \sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor} \frac{2(2i)!\binom{k}{2i}(-1)^{i+1}}{(2\pi m)^{2i+1}}$$

and

$$\begin{aligned}S(k) &= \frac{-p^k\sqrt{p}}{\pi}\sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^i}{(2\pi)^{2i}}\sum_{m=1}^{\infty}\frac{1}{m^{2i+1}}\Big(\frac{m}{p}\Big)\\ &= \frac{-p^k\sqrt{p}}{\pi}\sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^i}{(2\pi)^{2i}}L(2i{+}1,\chi),\end{aligned}$$

where $\chi(m) = \big(\frac{m}{p}\big) = \big(\frac{-p}{m}\big)$.

In order to get $S(k) > 0$, we need

$$\sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^i}{(2\pi)^{2i}}L(2i{+}1,\chi) < 0$$

or

$$L(1,\chi) < A(k,\chi), \tag{2–1}$$

where we define

$$A(k,\chi) = \sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^{i+1}}{(2\pi)^{2i}}L(2i{+}1,\chi).$$

This is a simple generalization of (1–4). Now, as noted by Shanks, we have

$$\begin{aligned}\frac{\zeta(4i+2)}{\zeta(2i+1)} &= \prod_{q\ \text{prime}}\frac{q^{2i+1}}{q^{2i+1}+1} \le L(2i{+}1,\chi)\\ &\le \prod_{q\ \text{prime}}\frac{q^{2i+1}}{q^{2i+1}-1} = \zeta(2i+1);\end{aligned}$$

thus,

$$A(k,\chi) \ge Z(k),$$

where

$$Z(k) = \sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor} \frac{(2i)!\binom{k}{2i}(-1)^{i+1}}{(2\pi)^{2i}} Z_i,$$

and

$$Z_i = \begin{cases} \dfrac{\zeta(4i+2)}{\zeta(2i+1)} & \text{for } i \text{ odd,} \\ \zeta(2i+1) & \text{for } i \text{ even.} \end{cases}$$

Here are the values of $Z(k)$, for $3 \le k \le 1$:

k	$Z(k)$
3	0.12862752537709828076
4	0.25725505075419656153
5	0.34892030342097469308
6	0.40362328337743267542
7	0.42276531850520712827
8	0.40774773668593467139
9	0.35679221192851994858
10	0.26494076436913562769
11	0.12237264911914991262
12	−0.08727875488694594478
13	−0.39087550751914021317

We find that $Z(k)$ stays positive for $k \le 11$; thus, if $L(1,\chi) < 0.12237$, then $S(k) > 0$ for $3 \le k \le 11$. However, for values of $k > 11$, this approach will clearly not work because $L(1,\chi)$ is always positive. By changing slightly the model used for the finite probability space in [Elliott 1973] (see [Elliott 1980, Chapter 22]), it is a routine matter, using the methods of [Elliott 1973], to establish that there must exist a positive proportion of the primes $p \equiv -1 \pmod 4$ such that for any given real value of z, we get $L(1,\chi) < e^z$. Thus, not only must there exist an infinitude of primes p (congruent to -1 modulo 4) for which $S(k) > 0$ for $3 \le k \le 11$, but there must be a positive proportion of such primes. Undoubtedly, this result applies to all values of $k > 11$, but this would require a more extensive modification of Elliott's results.

Our first strategy was to extend the idea that the Lehmers employed to find the numbers mentioned in Section 1; that is, we try to find p such that $\chi(q) = -1$ for as many small primes q as possible. Suppose that $\chi(q) = -1$ for all primes $q \le Q$; then from (1–5)

$$L(s,\chi) = F_s(Q)T_s(Q,\chi),$$

where

$$F_s(Q) = \prod_{q\le Q} \frac{q^s}{q^s+1}, \quad T_s(Q,\chi) = \prod_{q>Q} \frac{q^s}{q^s-\chi(q)}.$$

We now need to estimate $T_s(Q,\chi)$. To this end we note that

$$-\log T_s(Q,\chi) = \sum_{q>Q} \log \frac{1-\chi(q)}{q^s} = \sum_{q>Q}\sum_{i=1}^{\infty} \frac{-\chi(q)^i}{iq^{is}};$$

hence,

$$\bigl|\log T_s(Q,\chi)\bigr| \le \sum_{i=1}^{\infty}\sum_{q>Q} \frac{1}{iq^{is}}. \tag{2–2}$$

We next examine the sum $\sum_{q>Q} q^{-s}$ $(s>1)$. If we let $\pi(x)$ represent the usual prime counting function, then by partial summation

$$\begin{aligned}\sum_{q>Q} \frac{1}{q^s} &= \sum_{m\ge Q} \pi(m)\bigl(m^{-s}-(m+1)^{-s}\bigr) - \pi(Q)/Q^s \\ &= s\sum_{m\ge Q}\int_m^{m+1} \pi(x)x^{-s-1}\,dx - \pi(Q)/Q^s \\ &= s\int_Q^{\infty} \pi(x)x^{-s-1}\,dx - \pi(Q)/Q^s.\end{aligned}$$

By a result of Rosser and Schoenfeld [1962], we have

$$\frac{x}{\log x} < \pi(x) < \frac{x}{\log x}\left(1+\frac{3}{x\log x}\right) \quad (x > 17).$$

Hence,

$$\begin{aligned}\sum_{q>Q}\frac{1}{q^s} &< \frac{1}{\log Q}\Bigl(1+\frac{3}{2\log Q}\Bigr)s\int_Q^{\infty} x^{-s}\,dx - \frac{Q}{Q^s\log Q} \\ &< Q^{-s+1}/\log Q \quad (s\ge 3,\ Q\ge 90).\end{aligned}$$

Substituting this into (2–2) we get

$$\bigl|\log T_s(Q,\chi)\bigr| < \frac{Q}{\log Q}\left(\sum_{i=1}^{\infty}\frac{Q^{-si}}{i}\right) < \frac{3Q^{-s+1}}{2\log Q},$$

for $s \ge 3$, $Q \ge 90$. Since $e^x < 1+2x$ and $e^{-x} > 1-2x$ for $0<x<1$, we get

$$\bigl|T_s(Q,\chi)-1\bigr| < 3Q^{-s+1}/\log Q$$

or

$$(-1)^jT_s(Q,\chi) > (-1)^j - 3Q^{-s+1}/\log Q \tag{2–3}$$

for any $j \in \mathbb{Z}$ as long as $s \ge 3$ and $Q \ge 90$.

From (2–3) it follows that

$$\begin{aligned}A(k,\chi) &= \sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor} \frac{(2i)!\binom{k}{2i}}{(2\pi)^{2i}} F_{2i+1}(Q)(-1)^{i+1}T_{2i+1}(Q,\chi) \\ &> B(k,Q),\end{aligned}$$

r	N_r	$h(-N_r)$	$L(1,\chi)$	$\lambda(N_r)$
3	19	1	0.720730	0.229415
5, 7	43	1	0.479088	0.152498
11, 13	67	1	0.383806	0.122169
17, ..., 37	163	1	0.246068	0.078326
41	222643	33	0.219714	0.069937
43, 47	1333963	79	0.214884	0.068399
53, 59	2404147	107	0.216796	0.069008
61	20950603	311	0.213457	0.067945
67, 71	51599563	487	0.212988	0.067796
73, 79	96295483	665	0.212896	0.067767
83	146161723	857	0.222696	0.070886
89	1408126003	2293	0.191969	0.061105
97, 101, 103	3341091163	3523	0.191477	0.060949
107, 109, 113	52947440683	13909	0.189899	0.060446
127	193310265163	26713	0.190873	0.060756
131, 137	229565917267	29351	0.192450	0.061258
139	915809911867	59801	0.196315	0.062489
149, ..., 163	1432817816347	70877	0.186020	0.059212
167, ..., 181	30059924764123	296475	0.169880	0.054074
191	3126717241727227	3201195	0.179853	0.057248
193, 197, 199	8842819893041227	5188215	0.173329	0.055172
211, 223	13688678408873323	6524653	0.175196	0.055766
227, ..., 241	22261805373620443	8035685	0.169196	0.053857
251	4908856524312968467	121139393	0.171769	0.054675
257, 263, 269	7961860547428719787	140879803	0.156852	0.049927

TABLE 1. N_r: least prime solutions

where

$$B(k,Q)=\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}}{(2\pi)^{2i}}(-1)^{i+1}F_{2i+1}(Q) - \frac{3}{\log Q}\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}}{(2Q\pi)^{2i}}F_{2i+1}(Q);$$

thus, if $L(1,\chi) < B(k,Q)$, then $S(k) > 0$.

In order to find values of $p \equiv 3 \pmod 4$ such that $\chi(q) = -1$ for all $q \le Q$ we made use of the number sieve MSSU; see [Lukes et al. 1995; 1996]. We let r be a prime and define N_r as the least positive prime integer satisfying $N_r \equiv 3 \pmod 8$ and

$$\left(\frac{-N_r}{q}\right) = -1 \quad \text{for all odd primes } q \le r.$$

By the heuristic reasoning of [Lukes et al. 1996], we would expect $\log N_r$ to be roughly

$$(r\log 2/\log r)^{1+o(1)}.$$

In somewhat over a month of MSSU time, Jacobson [1995, p. 128] computed Table 1 above. This table is an extension of parts of Tables III and IIIa in [Lehmer et al. 1970].

Note that for $41 \le r \le 269$ we have

$$\log N_r > (r\log 2)/\log r. \tag{2–4}$$

From Table 1 we see that for $p = N_{257}$ we have $S(k) > 0$ if $0.156852 < B(k,Q)$, with some Q between 90 and 270. We next computed a table of values for $B(k,Q)$ for $4 \le k \le 400$ and (Q) become very large and therefore difficult to work with. Because of this growth rate of the terms of $B(k,Q)$, it was necessary to compute it using 800 digits of precision in order to get accurate values. For a fixed k we found that the larger the value of Q, the larger $B(k,Q)$ would be, so that the largest number of values of k with $B(k,Q) > 0.156852$ could be obtained for $Q = 270$. In this case we found that the values of $B(k,Q)$ increased monotonically for $4 \le k \le 10$ and decreased monotonically for $10 \le k \le 400$. Since

$$B(4,270) = 0.25725344,$$
$$B(142,270) = 0.15685501 > 0.156852 > B(143,270),$$

we see that for $p = N_{257}$ we have $S(k) > 0$ for all k such that $4 \le k \le 142$.

3. A SECOND APPROACH

As the computation of the N_r values is very expensive and the concomitant rate of decrease of $L(1,\chi)$ is very slow, we developed a second strategy for finding values of p such that $S(k)>0$. The idea here was to allow for a greater degree of freedom than that afforded by insisting that $\chi(q)=-1$ for all primes $q\le Q$. To this end we define $F_s(Q,\chi)$ by

$$F_s(Q,\chi)=\prod_{q\le Q}\frac{q^s}{q^s-\chi(q)}$$

and

$$B(k,Q,\chi)=\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^{i+1}F_{2i+1}(Q,\chi)}{(2\pi)^{2i}} -\frac{3}{\log Q}\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}F_{2i+1}(Q,\chi)}{(2Q\pi)^{2i}}.$$

By using the same reasoning as that employed in Section 2, we see that $S(k)>0$ if $L(1,\chi)<B(k,Q,\chi)$ or

$$T_1(Q,\chi)<B(k,Q,\chi)/F_1(Q,\chi). \tag{3–1}$$

If we define

$$G_s(Q,\chi)=F_s(Q,\chi)/F_1(Q,\chi)=\prod_{q\le Q}\frac{q^{s-1}(q-\chi(q))}{q^s-\chi(q)}$$

and

$$C(k,Q,\chi)=\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}(-1)^{i+1}}{(2\pi)^{2i}}G_{2i+1}(Q,\chi) -\frac{3}{\log Q}\sum_{i=1}^{\lfloor\frac{k-1}{2}\rfloor}\frac{(2i)!\binom{k}{2i}G_{2i+1}(Q,\chi)}{(2Q\pi)^{2i}},$$

then by (3–1) we see that $S(k)>0$ if

$$T_1(Q,\chi)=L(1,\chi)/F_1(Q,\chi)<C(k,Q,\chi). \tag{3–2}$$

Now a result of Elliott [Shanks 1971] asserts that, if $Q>2$ and $F(Q,z,\chi)$ is the density of all positive d (here $\chi(q)=\bigl(\frac{-d}{q}\bigr)$) such that

$$T_1(Q,\chi)\le 1/(1+z) \quad\text{or}\quad T_1(Q,\chi)\ge 1+z,$$

with $0<z<2$, then there exist constants A, B such that

$$F(Q,z,\chi)<2A\exp\bigl(-BQ\log^2(1+z)\bigr).$$

Hence, for z between 0 and 2 it is very likely that $T_1(Q,\chi)<1+z$. This means that if k, Q, p and z are chosen such that $C(k,Q,\chi)\ge 1+z$, the chance that $T_1(Q,\chi)<C(k,Q,\chi)$ is very good. For example, if p is selected such that $\chi(q)=+1$ for $q=2,3,5$ and $\chi(q)=-1$ for $7\le q<Q=220$, then

$$C(k,Q,\chi)>1.011$$

for $18\le k\le 800$. (This was determined by computing $C(k,Q,\chi)$ to 2000 digits of precision.) But, by using the MSSU we found that

$$p=27542355520364791 \tag{3–3}$$

satisfies the conditions above and $h(-p)=25834697$; hence, since $F_1(220,\chi)=1.52969893$, we get

$$\begin{aligned}T_1(220,\chi)&=L(1,\chi)/F_1(220,\chi)\\&=1.01098973<1.011.\end{aligned}$$

Thus, for p given by (3–3) we have $S(k)>0$ for $18\le k\le 800$.

Naturally, this leads to the question of how best to specify the values of $\chi(q)$ for the small primes. After conducting a number of numerical experiments we discovered that the values of $C(k,Q,\chi)$ tended to be largest over the longest interval for k when $\chi(q)=1$ for only the first few primes and $\chi(q)=-1$ for the remainder of the primes $\le Q$. For example, if $\chi(q)=1$ for $q=2,3,5,7$; $Q=90$ and $\chi(q)=-1$ for all other primes $\le Q$, then $C(k,Q,\chi)>1.05$ for $57\le k\le 325$ and if $\chi(q)=1$ for $q=2,3,5$ only, then $C(k,Q,\chi)>1.05$ for $27\le k\le 319$ and if $\chi(q)=1$ for $q=2,3,5,7,11$, then $C(k,Q,\chi)>1.05$ for $122\le k\le 273$. If $\chi(q)=1$ for $q=79,83,89$ and $\chi(q)=-1$ for the remaining $q<220$, then $C(k,Q,\chi)>1.05$ only when $4\le k\le 67$. In all cases we observed that for fixed Q and χ, $C(k,Q,\chi)$ was strictly monotonically increasing for the small values of k, and after achieving its maximum became strictly monotonically decreasing. The location and the size of the maximum depended on Q and χ.

We also found it useful to make Q in (3–2) much larger than the limit to which we can sieve with the MSSU. This is because if Q^* denotes the upper bound on the prime moduli used by MSSU, then $T_1(Q^*,\chi)$ will likely not differ very much from $T_1(Q,\chi)$ when Q is much larger than Q^*. On the other hand we have found that, for k and χ fixed, $C(k,Q,\chi)$ grows with Q. This means that it is likely that $C(k,Q,\chi)>T_1(Q,\chi)$ for a larger interval of values of k than is the case if we work with $Q^*<Q$. For example, if we put $Q^*=230$ and $Q=1000$ and

specify that $\chi(q) = 1$ for $q = 2, 3, 5, 7$ and $\chi(q) = -1$ for all the remaining $q \leq Q^*$, then

$$p = 164093214527675999 \tag{3–4}$$

satisfies our conditions on $\chi(q)$ for $q \leq Q^*$. Here

$$F_1(Q^*, \chi) = 2.02182403$$

while

$$F_1(Q, \chi) = 2.01920199.$$

For this value of p we get $h(-p) = 263229907$; hence,

$$T_1(Q^*, \chi) = L(1, \chi)/F_1(Q^*, \chi) = 1.00970949$$

while

$$T_1(Q, \chi) = L(1, \chi)/F_1(Q, \chi) = 1.01102065.$$

On tabulating $C(k, Q^*, \chi)$ we found that if $29 \leq k \leq 969$, then $C(k, Q^*, \chi) > 1.0098 > T_1(Q^*, \chi)$. Hence, for p given by (3–4) we have that $S(k) > 0$ for $29 \leq k \leq 969$. Next, on tabulating $C(k, Q, \chi)$ for the χ values produced by p and $Q = 1000$, we found that if $29 \leq k \leq 35$, then $C(k, Q, \chi) > 1.0128 > T_1(Q, \chi)$ and $C(k, Q, \chi) > 1.085 > T_1(Q, \chi)$ for $35 \leq k \leq 2000$. Thus for p given by (3–4) we get $S(k) > 0$ for $29 \leq k \leq 2000$. That the value 1.085 is quite a lot larger than 1.011 suggests that if we had tabulated $C(k, Q, \chi)$ even further, we would likely have produced an even larger value for k such that $S(k) > 0$; however, at this point the computation of the $C(k, Q, \chi)$ values was very expensive because we were using 6000 digits of precision.

4. THE PROBLEM OF S(3)

We now know values of p for which $S(k) > 0$ for all $4 \leq k \leq 2000$, but we have not yet found a value of p for which $S(3) > 0$. From results in Section 2 we know that if

$$L(1, \chi) < Z(3) = \zeta(6)/(4\zeta(2)\zeta(3)) = 0.12863, \tag{4–1}$$

then $S(3) > 0$, and it follows that $\lambda(p) < 0.040945$. Jacobson [1995, pp. 140–141] used the MSSU to produce numbers $N \equiv -1 \pmod 4$ such that $\left(\frac{-N}{q}\right) = -1$ for $q = 2, 3, \ldots, 199$ and computed $F_1(Q, \chi)$ for $Q = 1000$ to search for likely values of N with small $L(1, \chi)$. For those that were prime, he computed $h(-N)$ and an accurate value of $\lambda(N)$. The best result he obtained was for the 20 digit

$$p = 19701513057844219387. \tag{4–2}$$

Here $h(-p) = 218285743$, $L(1, \chi) = 0.15449892$, and $\lambda(p) = 0.04917853$. An attempt by the authors to get an improved value by specifying only that $\left(\frac{-N}{q}\right) = -1$ for $q = 2, 3, \ldots, 149$ did not produce a better result for any prime value of N below Jacobson's number (4–2). Only after searching somewhat beyond $4.8 \cdot 10^{19}$ were we able to find better results: for the numbers

$$\left.\begin{aligned} p_1 &= 39686738412456114907, \\ p_2 &= 41974200404926400587, \\ p_3 &= 45505625249774422363, \end{aligned}\right\} \tag{4–3}$$

we have

$$h(-p_1) = 309519879, \quad L(1, \chi) = 0.15435322, \quad \lambda(p_1) = 0.04913215,$$

$$h(-p_2) = 317906469, \quad L(1, \chi) = 0.15415514, \quad \lambda(p_2) = 0.04906910,$$

$$h(-p_3) = 330452097, \quad L(1, \chi) = 0.15389547, \quad \lambda(p_3) = 0.04898645.$$

Given its size, p from (4–2) is a most remarkable number because there are so few values of primes $q \leq 401$ for which $\chi(q) = 1$. We have $\chi(q) = -1$ for all primes $q \leq 211$. Also, $\chi(q) = -1$ for $227 \leq q \leq 241$ and $\chi(257) = -1$, but $\chi(223) = \chi(251) = \chi(263) = 1$. This is not as good as N_{257} in Section 2, but then $\chi(q) = -1$ for $269 \leq q \leq 277$, $\chi(281) = 1$, $\chi(283) = \chi(293) = \chi(307) - 1$, $\chi(311) = 1$; furthermore, $\chi(q) = -1$ for $313 \leq q \leq 401$. This helps to explain the good value of $\lambda(p)$. While the above values of $\lambda(p)$ may seem at first glance to be rather getting close to 0.041, they are still a long distance away, relatively speaking. The results in Table 1 suggest that in order to get values of $\lambda(p)$ as small as 0.041, we would have to search for values of p very much beyond the limits mentioned above.

In a letter of March 5, 1969, the Lehmers described a method which they used to find a value of N such that $L(1, \chi)$ is small. They prespecified N to be such that $N \equiv 1 \pmod{131 \cdot 139}$ and $N \equiv 3 \pmod{137 \cdot 149}$; that is, they found A by the Chinese remainder theorem such that $A \equiv 1 \pmod{131 \cdot 139}$ and $A \equiv 3 \pmod{137 \cdot 149}$ and put $N = A + BX$ where $B = 131 \cdot 137 \cdot 139 \cdot 149$. They then employed their sieving device, the DLS-127, to find values for X such that $A + BX \equiv 3 \pmod 8$ and

$\left(\frac{-(A+BX)}{q}\right) = -1$ for all primes q with $3 \leq q \leq 127$. By this process they produced the 20 digit number

$$N = 84148631888752647283$$

for which $\chi(q) = -1$ for all $p \leq 149$ and $L(1,\chi) = 0.17009$, but N is unfortunately composite. In an attempt to find a better result than the ones of (4–2) and (4–3), we used the Lehmers' idea with $B = \prod_{251}^{353} q \approx 3.6 \cdot 10^{44}$ and A such that $\left(\frac{-A}{q}\right) = -1$ for all q dividing B. We then used the MSSU to sieve for values of X such that $\left(\frac{-(A+BX)}{q}\right) = -1$ for q up to 241. Our best result was the 62 digit prime

$$\begin{aligned} p = {} & 12600224234190799450242640167 2\backslash \\ & \quad 314388974220236275036810179959 63, \end{aligned}$$

for which Jacobson computed that

$$h(-p) = 171318502487356060544121730019,$$

using an improved version of the algorithm in [Jacobson 1999]. Thus, $L(1,\chi) = 0.15162297$, which is less than that for the numbers in (4–3), but it is still not sufficiently small to get $S(3) > 0$ or $\lambda(p) < 0.041$. Indeed, by August of 1968 Shanks and the Lehmers had reached the conclusion that the DLS-127 would never be able to find a value for p such that $S(3) > 0$. Shanks went so far as to estimate that such a value for p might have to satisfy $\chi(q) = -1$ for all primes $q \leq 1620$. However, the value of $F_1(1283) = 0.12854204$ is already less than the value of $L(1,\chi)$ needed by (4–1). If we use the empirical estimate (2–4) as a guide for estimating a lower bound on N_{1283}, we get $\log N_{1283} > 124$, suggesting that N_{1283} is likely to be a number of at least 54 digits, a number far too large for any current sieve device to find.

There is, however, thanks to a recent result of Bach [1995], another way to find a candidate for p. Because $F_1(1279)$ is quite close to $\zeta(6)/(4\zeta(2)\zeta(3))$, we simply found values for N such that $\left(\frac{-N}{q}\right) = -1$ for all $q \leq 1279$. We did this by specifying that for all prime values of $q \leq 1279$,

$$\begin{aligned} &N \equiv 3 \pmod 8, \\ &N \equiv 1 \pmod q \text{ when } q \equiv -1 \pmod 4, \\ &N \equiv r(q) \pmod q \text{ when } q \equiv 1 \pmod 4. \end{aligned}$$

Here $r(q)$ denotes a randomly selected quadratic nonresidue of q. Notice that if N satisfies these conditions we have $\left(\frac{-N}{q}\right) = -1$ for all $q \leq 1279$. The difficulty with this process is that the values we get for N are very large, 535 or more digits. However, testing the numbers for primality is very easy because $N-1$ is divisible by all the primes $q \equiv -1 \pmod 4$ $(q \leq 1279)$. Thus, it is easy to find a completely factored part of $N-1$ which exceeds $\sqrt{N}$, and the method of Pocklington mentioned in [Brillhart et al. 1975, Theorem 4] can easily be used to establish the primality of N. We produced 10 prime values for p in this way and selected the one such that $F_1(200000,\chi)$ was least, namely the 535 digit number

$$\begin{aligned} p = {} & 881974625057785931222613817074\backslash \\ & 917532086866157498333873986616\backslash \\ & 772405314952314649125430692674\backslash \\ & 421301535335822565110383045261\backslash \\ & 662288884171496652768853130693\backslash \\ & 547568926092470486468758067960\backslash \\ & 339622958266444317598747950276\backslash \\ & 228195628141063361018553506872\backslash \\ & 307865094282349696360084281769\backslash \\ & 391483388553654419029093991970\backslash \\ & 223187255252971434802826943154\backslash \\ & 408037354452295695797112414760\backslash \\ & 456576881727709666986157386200\backslash \\ & 364701289849665480127513654606\backslash \\ & 154630655217220710053068332795\backslash \\ & 778436402430725458959096262770\backslash \\ & 842000062867226918845060657043\backslash \\ & 02055090802961591761086 67. \end{aligned} \tag{4–4}$$

It remains to show that $L(1,\chi)$ for this p satisfies (4–1). We used the method of [Bach 1995] to estimate $L(1,\chi)$. We define

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

and $a_j = (Q+j)\log(Q+j)/C(Q)$, for $j = 0, 1, \ldots, Q-1$. Bach showed that under the ERH

$$\left| \log L(1,\chi) - \sum_{i=0}^{Q-1} a_i \log F_1(Q+i-1,\chi) \right| \leq A(Q,d),$$

where $A(Q,d) = (A \log|d| + B)/(\sqrt{q}\, \log Q)$ and A, B are explicit constants tabulated in [Bach 1995, Table 3]. For $Q = 275000000$ and $d = -p$, we computed

$$S(Q,p) = \sum_{i=0}^{Q-1} a_i \log F_1(Q+i-1,\chi)$$

by carrying 40 digits of precision, and found that

$$S(Q,p) = -2.074865302036.$$

We also found that

$$A(Q,p) = 0.0239249754.$$

Hence, since

$$e^{S(Q,p)} \cdot e^{-A(Q,p)} \le L(1,\chi) \le e^{S(Q,p)} \cdot e^{A(Q,p)},$$

we get

$$0.12260465 \le L(1,\chi) \le 0.12861391.$$

Thus, for p given by (4–4) we get $S(3) > 0$ and $\lambda(p) < 0.041$ under the ERH.

ACKNOWLEDGMENTS

We thank the LiDIA Group [LiDIA 1997] and the SIMATH Research Group [Zimmer 1997] in Darmstadt and Saarbrücken, respectively, for providing software and computing time. We also wish to express our gratitude to Mike Jacobson for providing the class number in Section 4 and to an anonymous referee for some very helpful suggestions.

REFERENCES

[Ayoub et al. 1967] R. Ayoub, S. Chowla, and H. Walum, "On sums involving quadratic characters", *J. London Math. Soc.* **42** (1967), 152–154.

[Bach 1995] E. Bach, "Improved approximations for Euler products", pp. 13–28 in *Number theory* (Halifax, 1994), edited by K. Dilcher, CMS Conference Proceedings **15**, Amer. Math. Soc., Providence, RI, 1995.

[Brillhart et al. 1975] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, "New primality criteria and factorizations of $2^m \pm 1$", *Math. Comp.* **29** (1975), 620–647. Table errata in **39** (1982), 747.

[Elliott 1973] P. D. T. A. Elliott, "On the distribution of the values of quadratic L-series in the half-plane $\sigma > \frac{1}{2}$", *Invent. Math.* **21** (1973), 319–338.

[Elliott 1980] P. D. T. A. Elliott, *Probabilistic number theory, II: Central limit theorems*, Grundlehren der Math. Wissenschaften **240**, Springer, Berlin, 1980.

[Fine 1970] N. J. Fine, "On a question of Ayoub, Chowla and Walum concerning character sums.", *Illinois J. Math.* **14** (1970), 88–90.

[Jacobson 1995] M. J. Jacobson, Jr., *Computational techniques in quadratic fields*, Master's thesis, University of Manitoba, 1995.

[Jacobson 1999] M. J. Jacobson, Jr., "Applying sieving to the computation of quadratic class groups", *Math. Comp.* (1999). To appear.

[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 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] J. Lenstra, H. W., "On the calculation of regulators and class numbers of quadratic fields", pp. 123–150 in *Journées arithmétiques,* 1980 (Exeter, 1980), edited by J. V. Armitage, London Math. Soc. Lecture Note Series **56**, Cambridge Univ. Press, Cambridge, 1982.

[LiDIA 1997] The LiDIA Group, "LiDIA: a C++ library for computational number theory, version 1.3", software, Technische Universität Darmstadt, Germany, 1997. See http://www.informatik.tu-darmstadt.de/TI/LiDIA.

[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.

[Rosser and Schoenfeld 1962] J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.* **6** (1962), 64–94.

[Shanks 1971] D. Shanks, "Class number, a theory of factorization, and genera", pp. 415–440 in *Proceedings of the* 1969 *Summer Institutes on Number Theory* (Stony Brook, NY, 1969), edited by D. J. Lewis, Proc. Sympos. Pure Math. **20**, Amer. Math. Soc., Providence, 1971.

[Shanks 1972] D. Shanks, "The infrastructure of a real quadratic field and its applications", pp. 217–224 in *Proceedings of the Number Theory Conference* (Boulder, CO, 1972), Univ. Colorado, Boulder, 1972.

[Zimmer 1997] H. G. Zimmer, "SIMATH: a computer algebra system for number theoretic applications", software, University of Saarland, Saarbrücken, 1997. See http://emmy.math.uni-sb.de/~simath/.

Edlyn Teske, Fachbereich Informatik, Technische Universität Darmstadt, Alexanderstraße 10, 64283 Darmstadt, Germany
Current address: University of Waterloo, Dept. of Combinatorics and Optimization, Waterloo, Ontario, N2L 3G1 Canada (eteske@cacr.math.uwaterloo.ca)

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

Received October 27, 1997; accepted in revised form May 8, 1998