JOURNAL OF NUMBER THEORY **42**, 297–312 (1992)

Computation of the First Factor of the Class Number of Cyclotomic Fields

GILBERT FUNG

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

ANDREW GRANVILLE

Department of Mathematics, University of Georgia, Athens, Georgia 30602

AND

HUGH C. WILLIAMS*

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

Communicated by H. L. Montgomery

Received August 15, 1989; revised September 17, 1990

We show how to compute the values of $h_1(p)$, the first factor of the class number of the cyclotomic field $\mathscr{Q}(\exp 2i\pi/p)$, for each prime $p \leqslant 3000$, and determine the set of prime divisors for each $p \leqslant 1000$. We confirm, for these values, a number of well known conjectures about $h_1(p)$. We give some reasons why we believe that Kummer's conjectured asymptotic estimate for $h_1(p)$ is likely to be wrong. We show how an extension of the recent work of Goldfeld, Cross, and Zagier might be used to establish that $h_1(p)$ is monotone increasing for all $p \geqslant 19$.

1. INTRODUCTION

Let p denote any odd prime, let $h(p)$ be the class number of the cyclotomic field $\mathscr{Q}(\xi_p)$ (where ξ_p is a primitive pth root of unity), and let $h_2(p)$ be the class number of the real subfield $\mathscr{Q}(\xi_p + \xi_p^{-1})$. Kummer established that the ratio $h_1(p) = h(p)/h_2(p)$ is an integer which is called the "relative class number" or the "first factor of the class number." He went on to show that p divides $h(p)$ if and only if p divides $h_1(p)$; and so in order to determine whether p is a "regular" prime (i.e., p divides $h(p)$), one

* Research supported by NSERC of Canada Grant A 7649.

0022-314X/92 $5.00

need only investigate whether p divides $h_1(p)$. Computationally this result is very important as there is no easy way to compute $h(p)$. As Kummer put it, "If p is too large then the effective computation of the second factor is very tricky as we must first find a system of fundamental units. The computation of the first factor, ..., does not offer this difficulty; I have computed it for all prime numbers up to 100" [14, p. 472].

(Actually Kummer computed $h_1(p)$, by hand, for all primes $p \leqslant 163$, only making three mistakes.)

The computational situation has not changed much in that there is still no easy way known for finding a system of fundamental units. On the other hand, Kummer perhaps underestimated the difficulties involved with computing $h_1(p)$, most of which arise because it grows faster than exponentially. Actually Kummer did write, "One can see that these numbers are growing with extraordinary speed. The asymptotic rule for the growth of the first factor of the class numbers $h_1(p)$ is given by the formula:

$$h_1(p) \sim 2p\left(\frac{p}{4\pi^2}\right)^{(p-1)/4} = G(p), \tag{1}$$

of which I save the proof and other developments for another occasion" [14, p. 473].

Kummer never did publish a proof of (1), and it seems likely that it is incorrect—we discuss this further in Section 4. In 1974 Lepistö [18] gave the bounds

$$\begin{aligned} -\frac{1}{2}\log p - 4\log\log p - 12.93 - \frac{4.66}{\log p} \\ \leqslant \log\left(\frac{h_1(p)}{G(p)}\right) \leqslant 5\log\log p + 15.49 + \frac{4.66}{\log p} \end{aligned} \tag{2}$$

and so one can see that the growth of $h_1(p)$ is indeed fast. Previously Ankeny and Chowla [1] had established that $h_1(p) = G(p)\,p^{o(1)}$ from which one can immediately deduce that $h_1(p) = 1$ for only finitely many primes. One can also deduce a considerably stronger result: There exists a constant p_0 such that $h_1(q) > h_1(p)$ whenever $q > p \geqslant p_0$. In 1971 Montgomery (see [29, p. 204]) and Uchida [27] made the first of these results effective by showing independently that $h_1(p) = 1$ if and only if $p \leqslant 19$ (which was conjectured by Kummer). In 1974 Lepistö made the second of these results effective, under the assumption of the generalized Riemann Hypothesis (that is, he gave the numerical value $p_0 = 2*10^{13}$): He could have actually given a value to p_0 under the weaker assumption that there are no Siegel zeros. It does not yet seem possible to find a value for

p_0 unconditionally though some recent work of Goldfeld [8] and Gross and Zagier [11] helps us to come close. In Section 5 we shall prove:

THEOREM 1. *Suppose that we can find an elliptic curve E over* $\mathcal{Q}$ *for which the associated L-function has a zero of order* $\geqslant 6$ *at* $s=1$. *Then we can find an explicit constant* p_0 *for which* $h_1(q) > h_1(p)$ *whenever* $q > p \geqslant p_0$.

Presumably, it would then be a matter of computation to show that p_0 can be taken to be 19.

Our main purpose in this paper is to extend the computations of $h_1(p)$ as far as possible. We do this by using a method of Fee and Granville [7] to compute norms in algebraic number fields.

2. FORMULAE FOR COMPUTING $h_1(p)$

Kummer [14] established that

$$h_1(p) = \frac{1}{(2p)^{(p-3)/2}} \left| \prod_{\substack{j=1 \\ j \text{ odd}}}^{p-1} R(\xi_{p-1}^j) \right|, \tag{3}$$

where $R(x) = \sum_{j=0}^{p-2} g_j x^j$ with g a primitive root $(\bmod p)$ and g_j the least positive residue of $g^j \pmod p$.

Hasse [13] showed that

$$h_1(p) = G(p) \prod_{\chi \text{ odd character } (\bmod p)} L(1;\chi) \tag{4}$$

and we also have the formula

$$h_1(p) = \frac{1}{(2p)^{(p-3)/2}} \left| \prod_{\chi \text{ odd character } (\bmod p)} \sum_{k=1}^{p-1} \chi(k) k \right|. \tag{5}$$

Maillet considered the matrix M_p which has the (i, j)th entry equal to the least positive residue of $i/j \pmod p$ for $1 \leqslant i, j \leqslant (p-1)/2$. Chowla and Weil showed that

$$h_1(p) = \frac{1}{p^{(p-3)/2}} \,|\text{determinant of } M_p|. \tag{6}$$

Finally Carlitz and Olson [4] defined the matrix N_p which has the (i, j)th entry $[ij/p] - [(i-1)j/p]$ for $3 \leqslant i, j \leqslant (p-1)/2$ and showed that

$$h_1(p) = |\text{determinant of } N_p|. \tag{7}$$

In fact Kummer [14] and Pajunen [23] used (3) to compute $h_1(p)$, Newman [22] used (7), whereas Lehmer and Masley [17] used a rather more complicated formula (as shall we);

$$h_1(p) = \prod_{ef=p-1:f\,\mathrm{odd}} h_e(p), \tag{8}$$

where $h_e(p)$, called the relative class number of degree e, is given by

$$h_e(p) = p^{\delta} \frac{W_e(p)}{\phi_\tau(2)\gamma}, \tag{9}$$

where $\delta = \delta_e = [e/(p-1)]$, $\tau = \tau_e = e/(e, \mathrm{ind}_g 2)$, $\gamma = \gamma_e = \phi(e)/\phi(\tau)$, $\phi_\tau(\chi)$ is the τth cyclotomic polynomial, and

$$W_e(p) = \prod_{\substack{m=1\\(m,e)=1}}^{e} \left\{ \sum_{n=1}^{(p-1)/2} (\varepsilon_n - \varepsilon_{n-1})\, \xi_{p-1}^{((p-1)/e)mn} \right\} \tag{10}$$

with

$$\varepsilon_n = \begin{cases} 1 & \text{if } g^n - p[g^n/p] < p/2 \\ 0 & \text{otherwise.} \end{cases}$$

The real expense of using this formula comes in the computation of (10) for each e dividing $p-1$ with $(p-1)/e$ odd. A straightforward approach using multiprecise arithmetic is unrealistic once p is large. In [17], Lehmer and Masley used a vector manipulation method that amounts to carefully storing the coefficients of each power of $\xi_{p-1}^{(p-1)/e}$, as we multiply the terms of (10) together, and continually reducing the exponents by replacing $\xi_{p-1}^{(p-1)/2}$ with -1. Due to the fact that the numbers involved grow very quickly, this takes of order $p^5 \log^2 p$ elementary operations; and so it is prohibitively expensive when p is large (Lehmer and Masley did all $p < 521$).

We use the technique of "computation by homomorphisms" to evaluate the product in (10).

Define the homomorphism $\theta_t\colon \mathbf{Z}[\xi_{p-1}] \to \mathbf{Z}/\phi_{p-1}(t)\mathbf{Z}$ for each integer $t \geq 2$, where θ_t is the identity on $\mathbf{Z}$ and $\theta_t(\xi_{p-1}) = t$.

Let $\alpha_n = \varepsilon_n - \varepsilon_{n-1}$ for each $n = 1, 2, \ldots, (p-1)/2$, and let $\beta_{r,n}$ be the least non-negative residue of $rn \pmod{p-1}$.

Define

$$a_r(x) = \sum_{n=1}^{(p-1)/2} \alpha_n x^{\beta_{r,n}} \qquad \text{for } r = 1, 2, \ldots, p-1.$$

Then

$$W_e(p) = \prod_{\substack{m=1 \\ (m,e)=1}}^{e} a_{((p-1)/e)m}(\xi_{p-1}). \tag{11}$$

Now, for each r, $a_r(\xi_{p-1}) \equiv a_r(t) \pmod{A(t-\xi_{p-1})}$ where $A = \mathbf{Z}[\xi_{p-1}]$. Thus $(t-\xi_{p-1})$ divides

$$N = W_e(p) - \prod_{\substack{m=1 \\ (m,e)=1}}^{e} a_{((p-1)/e)m}(t)$$

in the ring A and so, $\phi_{p-1}(t)$ (which is the norm of $t-\xi_{p-1}$) divides N (which is an integer). This implies that

$$W_e(p) \equiv \prod_{\substack{m=1 \\ (m,e)=1}}^{e} a_{((p-1)/e)m}(t) \qquad (\text{mod}\, \phi_{p-1}(t)). \tag{12}$$

Thus the idea is to choose t sufficiently large so that

$$\phi_{p-1}(t) > 2W_e(p) \tag{13}$$

which will mean that $W_e(p)$ is the least residue, in absolute value, of $\prod_{m=1,\,(m,e)=1}^{e} a_{((p-1)/e)m}(t)$ (mod $\phi_{p-1}(t)$). The only remaining complication then is to choose t so that we can guarantee (13) holds (of course *before* actually computing $2W_e(p)$). Now each $h_e(p)$ is an integer and so, by (9), (8), and (2), we have

$$\begin{aligned} 2W_e(p) &= 2\,\frac{\phi_\tau(2)^\gamma}{p^\delta}\, h_e(p) \\ &\leqslant 2\,\frac{\phi_\tau(2)^\gamma}{p^\delta}\, h_1(p) \\ &\leqslant 2\,\frac{\phi_\tau(2)^\gamma}{p^\delta}\, 2p \left(\frac{p}{4\pi^2}\right)^{(p-1)/4} (\log p)^5\, e^{(15.49+4.66)/\log p}. \end{aligned} \tag{14}$$

Thus we selected t so that $\phi_{p-1}(t)$ is greater than the left hand side of (14) for each e in (8). This explains our

Algorithm to Compute $h_1(p)$.

1. Select t so that $\phi_{p-1}(t)$ is greater than the left hand side of (14) for each value of e in (8).

2. Let z_i be the least positive residue of t^i (mod $\phi_{p-1}(t)$) for $i = 0, 1, 2, ..., p-2$.

3. Use the formula $a_r(t) \equiv \sum_{n=1}^{(p-1)/2} \alpha_n z_{\beta_{r,n}} \pmod{\phi_{p-1}(t)}$ to compute each $a_r(t) \pmod{\phi_{p-1}(t)}$.
4. Use (12) to compute each $W_e(p)$.
5. Use (9) and (8) to determine $h_1(p)$.

This algorithm only takes of order $p^2 \log^4 p$ elementary operations to compute $h_1(p)$. Moreover, we have a head start in determining the factorization of $h_1(p)$ into primes as we already have the factorization into the values $h_e(p)$.

3. Some Results

We used the algorithm described at the end of the last section to compute $h_1(p)$ for each prime p such that $100 < p < 3000$. These computations were performed at the University of Manitoba on a Micro Vax II computer by using ALGEB, a multi-precise language which was developed by David Ford at Concordia University. It required 7 hours and 33 minutes of CPU time to compute $h_1(p)$ for all primes p which lie between 100 and 1000; 2 days, 21 hours, and 40 minutes of CPU time for p which lie between 1000 and 2000; and 14 days, 21 hours, and 27 minutes of CPU time for the remaining primes. It seems likely that on a larger machine or with more time we could have gone considerably further.

It was shown in [16] that if q^t is the power of the prime q dividing any $h_e(p)$, then either q divides e or $q \equiv 1 \pmod{e}$. So in order to factor $h_e(p)$ we simply checked whether it had any factors $< 100{,}000$ and then tested the remaining cofactor using Pollard's "$p-1$ method" [24] (as we know each remaining prime power factor is $\equiv 1 \pmod{e}$). We chose not to work too hard in trying to factor those that remain. We have deposited Tables I and II in the UMT (unpublished Mathematical Tables) File maintained by the Editorial office of *Mathematics of Computation*. In Table I we give the values of $h_1(p)$ for each p such that $100 < p < 3000$, and in Table II we give, for each p such that $521 < p < 1000$, the values of $h_e(p)$ for each e, followed by the prime factors that we could find, followed by the remaining composite cofactor (if any).

In 1870 Kummer [14a] showed that

$$2 \text{ divides } h(p) \text{ if and only if } 2 \text{ divides } h_1(p). \tag{15}$$

It is thus of interest to determine when $h_1(p)$ is even. Kummer himself showed that for the primes $p \leqslant 163$, only $h_1(29)$, $h_1(113)$, and $h_1(163)$ are even; he also showed that $h_2(29)$ and $h_2(113)$ are odd whereas $h_2(163)$ is even. In Table III we give the primes p such that $100 < p < 3000$ for which $h_1(p)$ is even, and also the power of 2 that exactly divides $h_1(p)$.

TABLE III

p	k	p	k	p	k
113	3	827	6	1789	4
163	2	853	2	1879	2
197	3	883	6	1951	2
239	6	937	2	2011	4
277	4	941	8	2131	2
311	10	953	3	2143	3
337	6	967	3	2161	4
349	4	1009	8	2221	4
373	5	1021	8	2297	3
397	6	1051	6	2311	5
421	4	1093	3	2381	6
463	3	1117	5	2521	3
491	6	1163	3	2591	3
547	2	1171	4	2689	2
607	4	1399	4	2797	4
659	3	1429	3	2803	2
683	5	1471	3	2843	3
701	3	1499	3	2857	3
709	4	1699	2	2927	6
751	4	1777	4		

Note. 2^k denotes the exact power of 2 that divides $h_1(p)$.

Kummer established many important results about class numbers. Perhaps the most striking was to show that p is regular if and only if p does not divide the numerator of any Bernoulli number B_{2n} with $2 \leqslant 2n \leqslant p-3$. ($B_n$ is defined by the power series $x/(e^x-1) = \sum_{n \geqslant 0} B_n(x^n/n!)$.) Wagstaff [30] and Tanner and Wagstaff [26] have done extensive computations on the p-divisibility of Bernoulli numbers (for p up to 150,000). Due to the following result, essentially due to Vandiver [28], their computations provide an important check on our computations:

LEMMA 1 (Vandiver). *If prime p divides the Bernoulli number B_{2n}, with $2 \leqslant 2n \leqslant p-3$ then p divides $h_e(p)$ where $e = (p-1)/(p-1, 2n-1)$.*

By Kummer's results we know that if p divides $h(p)$ then p must divide both $h_1(p)$ and some Bernoulli number; and by Vandiver's result we can find values of e for which p divides $h_e(p)$, given values of $2n$ for which p divides B_{2n}. There are a number of conjectures that further describe the p-divisibility.

(A) *Vandiver's conjecture: p does not divide $h_2(p)$.*

(Apparently this conjecture appeared originally in a letter from Kummer to Kronecker [15].) Of course this implies that p divides $h(p)$ to the same power that it divides $h_1(p)$. This conjecture was verified for $p < 150{,}000$ in [26, 30].

(B) *p divides $h_1(p)$ to the same power that it divides the product $B_2 B_4 \cdots B_{p-1}$.*

This appears in the paper of Lehmer and Masley [17]. We verified it for $p \leqslant 3000$.

(C) *p^2 does not divide B_{2n} for any $2 \leqslant 2n \leqslant p-3$.*

Conjectures (B) and (C) were shown to hold for $p < 125{,}000$, in [26], and it is possible that this is always the case. If so, then one can easily deduce that the power of p dividing any given $h_e(p)$ equals the number of values of n, with $2 \leqslant 2n \leqslant p-3$ and $(p-1, 2n-1) = f$, for which p divides B_{2n}. (The anonymous referee has noted that, under the heuristic assumption of the even Bernoulli numbers being "randomly distributed" modulo p^2, we should expect that p^2 divides B_{2n} for some $2 \leqslant 2n \leqslant p-3$, for around $(\log\log x/2)$ primes $p \leqslant x$. Nonetheless, as no such example has yet been found, such arguments are no less speculative than the simple belief in the converse!)

Given Kummer's conjecture(Eq. (1)) in Section 1, it is of interest to compute values of the ratio $h_1(p)/G(p)$. A prime p is a "high champion" if $h_1(p)/G(p) > h_1(q)/G(q)$ for all primes $q < p$; a prime is a "low champion" if $h_1(p)/G(p) < h_1(q)/G(q)$ for all primes $q < p$ with the exception of those primes $q < 23$. Tables IV(A) and IV(B) give high champions and low champions up to 3000.

TABLE IV(A)

High Champion Values of $h_1(p)/G(p)$

p	$h_1(p)/G(p)$
3	0.6046
5	0.7896
7	0.9567
11	1.1092
23	1.2730
73	1.2822
89	1.2863
179	1.3190
233	1.4310
761	1.4696
1451	1.4893
2741	1.4981

TABLE IV(B)

Low Champion Values of $h_1(p)/G(p)$

p	$h_1(p)/G(p)$
23	1.2730
29	1.1951
31	0.8899
79	0.8458
157	0.7430
211	0.7097
439	0.6848

TABLE V

p	$2n$	e	p	$2n$	e	p	$2n$	e
523	400	174	631	226	14	773	732	772
541	86	108	647	236	646	797	220	796
547	270	546	647	242	646	809	330	808
547	486	546	647	554	646	809	628	808
557	222	556	653	48	652	811	544	270
577	52	192	659	224	658	821	744	820
587	90	586	673	408	672	827	102	826
587	92	586	673	502	224	839	66	838
593	22	592	677	628	676	877	868	292
607	592	202	683	32	22	881	544	880
613	522	612	691	12	690	887	418	886
617	20	616	691	200	690	929	520	928
617	174	616	727	378	726	929	820	928
617	338	616	751	290	750	953	156	952
619	428	618	757	514	28	971	166	194
631	80	630	761	260	760			

In Table V we give the irregular primes $521 < p < 1000$, the values of n for which B_{2n} is divisible by p, and the corresponding values of e for which $h_e(p)$ is divisible by p.

In Table VI we give the number of primes p, in the range $100 < p < 3000$, for which $h_1(p)$ is exactly divisible by 2^k as well as the smallest 3 primes in each category.

In Table VII we give the number of primes p in the range $100 < p < 3000$ such that $h_1(p)$ is divisible by 3, 5, 7, 11, 13, ..., 29, as well as the smallest 3 primes in each category.

TABLE VI

k	Number up to 3000	Smallest 3 such primes		
2	10	163	547	853
3	18	113	197	463
4	14	277	349	421
5	4	373	683	1117
6	9	239	337	397
7	0			
8	3	941	1009	1021
9	0			
10	1	311		
>10	0			

TABLE VII

k	Number up to 3000	Smallest 3 such primes		
3	81	107	131	139
5	96	101	103	127
7	57	151	211	223
11	38	151	167	191
13	49	127	157	191
17	41	109	137	229
19	28	199	359	541
23	20	331	647	727
29	18	773	829	887

4. Kummer's Conjecture for the Size of $h_1(p)$

In a further paper [10] the second author develops the arguments that we sketch here. The idea is to establish that (1) is false by using certain tools of analytic number theory. Now, from Hasse's formula (4), we have that

$$\log (h_1(p)/G(p)) = \lim_{s \to 1+} \sum_{\chi \text{ odd character } (\text{mod } p)} \log L(s;\chi) = \frac{p-1}{2} f_p,$$

where

$$f_p = \lim_{x \to \infty} f_p(x),$$

and

$$f_p(x) = \sum_{m \geq 1} \frac{1}{m} \left\{ \sum_{\substack{q \text{ prime}, q^m \leq x \\ q^m \equiv 1 \ (\text{mod } p)}} \frac{1}{q^m} - \sum_{\substack{q \text{ prime}, q^m \leq x \\ q^m \equiv -1 \ (\text{mod } p)}} \frac{1}{q^m} \right\}. \tag{16}$$

Thus (1) is equivalent to the statement that $f_p = o(1/p)$. As the prime powers are very sparse (i.e., the number of $q^m \leq x$ with $m \geq 2$ is small) it is easy to show that

$$\sum_{m \geq 2} \frac{1}{m} \sum_{\substack{q \text{ prime} \\ q^m \equiv -1 \text{ or } 1 \ (\text{mod } p)}} \frac{1}{q^m} \ll \frac{1}{p \log p}$$

for all but $O(x^{1/2} \log^2 x)$ primes $p \leq x$. Therefore we are left, in almost all cases, with only the $m=1$ term in (16). For a given prime p, we can use a Riemann–Stieltjes integral to show that

$$g_p - g_p(T) = \int_{t=T}^{\infty} \frac{d\{\pi(t;p,1) - \pi(t;p,-1)\}}{t},$$

where $\pi(t;p,a)$ is the number of primes $\leqslant t$ that are $\equiv a \pmod{p}$, and g_p is defined as f_p except with only the $m=1$ term,

$$= \left[\frac{\pi(t;p,1) - \pi(t;p,-1)}{t}\right]_T^{\infty} + \int_T^{\infty} \frac{\pi(t;p,1) - \pi(t;p,-1)}{t^2}\,dt. \tag{17}$$

Now the Generalized Riemann Hypothesis implies that

$$\pi(t;p,1) - \pi(t;p,-1) \ll \frac{t}{(p-1)\log^2 t} \tag{18}$$

whenever $t \geqslant p^2 \log^2 p$; and, under the assumption of a well-known conjecture of Elliot and Halberstam [6] this may be extended to $t > p^{1+\varepsilon}$, for any fixed $\varepsilon > 0$, for all but $O(x/\log^3 x)$ primes $p \leqslant x$. In any case, if (18) holds for all $t \geqslant T$ then, by (17),

$$f_p - f_p(T) \ll \frac{1}{(p-1)\log T}.$$

Therefore, in most cases, the Eq. (1) is equivalent to the statement that, for each $\varepsilon > 0$,

$$\sum_{\substack{q \text{ prime}, q \equiv 1 \pmod{p} \\ q < p^{1+\varepsilon}}} \frac{1}{q} - \sum_{\substack{q \text{ prime}, q \equiv -1 \pmod{p} \\ q < p^{1+\varepsilon}}} \frac{1}{q} = o\left(\frac{1}{p}\right). \tag{19}$$

We have seen, so far, that $\sum_{q>T} (1/q)$, whether in the arithmetic progression $1 \pmod{p}$ or in the arithmetic progression $-1 \pmod{p}$, comes to essentially the same total. We expect that to happen when the sum is extended all the way down to $T_p = 3p-1$ in most cases. But then if $2p+1$ is prime and $2p-1$ is not, we have $f_p = 1/(2p+1) + o(1/p)$ which contradicts (1).

Such an argument needs some justification and this can be done by assuming that there are $\gg x/\log^2 x$ primes $p \leqslant x$ for which $2p+1$ is prime and then by using Selberg's sieve. In fact we prove in [10]:

Theorem 1. *Assume*

(1) (*Elliot and Halberstam* [6]) *For all* $\delta > 0$, $\sum_{p < x^{1-\delta}} |\pi(t;p,1) - \pi(t;p,-1)| \ll x/\log^4 x$;

(2) (*Hardy and Littlewood* [12]) *There are* $\gg x/\log^2 x$ *primes* $p \leqslant x$ *for which* $2p+1$ *is prime.*

Then, for any $\varepsilon > 0$, *there are* $\gg x/\log^2 x$ *primes* $p \leqslant x$ *for which*

$$h_1(p) \geqslant G(p)(e^{1/4} - \varepsilon).$$

Some justification is given in [10] to the conjecture that

$$(\log\log p)^{-1/2+o(1)} \leqslant h_1(p)/G(p) \leqslant (\log\log p)^{1/2+o(1)},$$

and that both bounds are, from time to time, attained.

5. The Monotonicity of $h_1(p)$

In order to show that $h_1(p) > h_1(q)$ whenever $p > q \geqslant p_0$ we need to find bounds on $h_1(p)$ for each p. This may be done by a modification of the argument of the previous section: Our starting point is Eq. (16). Let $\delta = -1$ or 1. Just as in Section 4 we can show that there exists an explicity computable constant $c_1 > 0$ such that

$$\sum_{m \geqslant 2} \frac{1}{m} \sum_{\substack{q \text{ prime} \\ q^m \equiv \delta \pmod p}} \frac{1}{q^m} \leqslant \frac{c_1}{p-1}. \tag{20}$$

(Actually, using the method of Section 2 of [10], one can get the upper bound $2/(p-1) + \pi(p)/p^2 + \sum_{q>p} (1/q^2)$, where $\pi(x)$ is the number of primes $\leqslant x$.)

For the "small" primes in the arithmetic progressions $\pm 1 \pmod p$ we may use the well-known Brun–Titchmarsh Theorem: There exists a constant $c_2 > 0$ such that $\pi(t; p, a) \leqslant (c_2/(p-1))(t/\log(t/p))$ whenever $t > p$. Therefore, by using a Riemann–Stieltjes integral in a similar way to (17) we get

$$\begin{aligned}\sum_{\substack{q \text{ prime}, q \leqslant T \\ q \equiv \delta \pmod p}} \frac{1}{q} &= \left[\frac{\pi(t; p, a)}{t}\right]_{2p-1}^{T} + \int_{2p-1}^{T} \frac{\pi(t; p, a)}{t^2}\, dt \\ &\leqslant \frac{c_2}{p-1} \left\{\frac{1}{\log(T/p)} + \log\log(T/p) - \log\log\left(\frac{2p-1}{p}\right)\right\} \\ &\leqslant \frac{1}{p-1} \{c_2 \log\log T + c_3\} \end{aligned} \tag{21}$$

for an easily computed constant C_3. In fact Montgomery and Vaughan [21] have shown that we may take $c_2 = 2$ in the Brun–Titchmarsh Theorem.

Finally we need to compute $g_p - g_p(T)$. To do this we again use (17) and note that the Siegel–Walfisz Theorem tells us that for any $N>0$, there exists a constant $c_4 = c_4(N)$, for which

$$|\pi(t; p, 1) - \pi(t; p, -1)| \leqslant \frac{c_4}{p-1} \frac{t}{\log^2 t},$$

where $p \leqslant \log^N t$. Therefore, by (17),

$$|g_p - g_p(T)| \leqslant \frac{c_4}{p-1} \left\{ \frac{1}{\log^2 T} + \frac{1}{\log T} \right\} \tag{22}$$

for $T \geqslant \exp(p^{1/N})$.

Combining (20), (21), and (22), for $T = \exp(p^{1/N})$, we get

$$|f_p| \leqslant \frac{1}{p-1} \left\{ \frac{1}{N} \log p + O(1) \right\}$$

and so

$$p^{-\varepsilon} \ll \frac{h_1(p)}{G(p)} \ll p^{\varepsilon},$$

where $\varepsilon = 1/N$. This is essentially the argument given by Ankeny and Chowla [1] to show that $h_1(p) = G(p)\, p^{o(1)}$; and so $h_1(p) > h_1(q)$ whenever $p > q > p_0$, for some value of p_0.

The problem with this argument is that we need c_4 explicitly in order to determine p_0 explicitly. It is well known (see Davenport [5, p. 123]) that $c_4(N)$ can be given explicitly for every $N>0$ provided that there is no "Siegel zero" of the non-principal real character $(\operatorname{mod} p)$. This is certainly true if, for instance, the Generalized Riemann Hypothesis is true. Actually, if $p \equiv 1 \pmod 4$ then it turns out, in estimating $\pi(t; p, 1) - \pi(t; p, -1)$ using the formula [5, p. 123, Eq. (9)]

$$\psi(t; p, a) = \frac{1}{p-1} \left(t - \left(\frac{a}{p}\right) \frac{t^{\beta}}{\beta} \right) + O\left(\frac{t}{\exp(c\sqrt{\log t})} \right), \tag{23}$$

where $(\cdot/p)$ is the Legendre symbol, and β is the Siegel zero of the real character $(\operatorname{mod} p)$ (if it exists), that the contribution of the Siegel zeros cancel as $(-1/p) = 1$, and so $c_4(N)$ can still be found explicitly for all values of $N>0$. (This can also be deduced by noting, in (4), that the real character $(\operatorname{mod} p)$ is even). However, in general, we can only give $c_4(N)$ explicitly for $N<2$. In this case we take $T = \exp(p^{1/N})$ and so, by (20), (21), and (22) we get $|\log(h_1(p)/G(p))| \leqslant c_5 p^{1/N}$ for some explicit constant c_5. With a bit more care we can replace $p \leqslant \log^N t$, for any $N<2$ by

$p \leqslant \log^2 t/(\log\log t)^g$ for some fixed $g > 0$; and also note that if $p \equiv 3 \pmod 4$ and the non-principal real character (mod p) has the Siegel zero β then

$$\psi(t; p, 1) - \psi(t; p, -1) = -\frac{2}{p-1}\frac{t^\beta}{\beta} + O\left(\frac{t}{\exp(c\sqrt{\log t})}\right)$$

and so we only get a "bad" lower bound. This is how Lepistö [18] arrived at his bounds (2). Unfortunately (2) is not quite good enough to ensure that $h_1(p)$ is monotonic from some *eplicit* p_0 onwards, but we can deduce from (2) and a corresponding lower bound for when $p \equiv 1 \pmod 4$ or for when the non-principal real character (mod p) has no Siegel zero, the following result.

PROPOSITION 1. *There exists an explicitly computable constant* p_1 *such that* $h_1(q) > h_1(p)$ *whenever* $q > p \geqslant p_1$, *unless* $q = p+2$, $q \equiv 3 \pmod 4$ *and the non-principal real character* (mod q) *has a Siegel zero.*

So let's see what happens for the exceptional case in the proposition.

First we see that by (23), there exist explicit constants c_5 and c_6 such that, $|\pi(t; p, 1) - \pi(t; p, -1)| \leqslant (c_5/(p-1))(t/\log^2 t)$ whenever $p \leqslant \exp(c_6\sqrt{\log t})$ and so, taking $T = \exp(\log^2 p/c_6^2)$, we get $h_1(p) \leqslant c_7 G(p)\log^2 p$ for some explicit constant c_7. Let's suppose that we have an explicit constant c_8 for which $|\pi(t; q, 1) - \pi(t; q, -1)| \leqslant (c_8/(q-1))(t/\log t(\log\log t)^2)$ whenever $q \leqslant \log^2 t(\log\log t)^4 \log\log\log t$. Then, by taking T so that $q = \log^2 T(\log_2 T)^4 \log_3 T$ in (17) and (21) we find that

$$h_1(q) > c_9 G(q)\log^2 q(\log\log q)^{1/2}/q^{1/2}$$

for some explicit constant $c_9 > 0$. But then

$$\begin{aligned} h_1(q) &> c_9 \log^2 q \frac{(\log\log q)^{1/2}}{q^{1/2}}\left(\frac{q}{4\pi^2}\right)^{(q-1)/4} \\ &= \frac{c_9}{2\pi}\log^2 q(\log\log q)^{1/2}\left(\frac{q}{4\pi^2}\right)^{(q-3)/4} \\ &> \frac{c_9}{2\pi}(\log\log q)^{1/2} G(p)\log^2 p \qquad \text{as } q = p+2 \\ &> c_7 G(p)\log^2 p > h_1(p), \end{aligned}$$

if p is greater than some explicitly computable p_0. From this we can deduce

PROPOSITION 2. *Assume that there is an explicit constant* $c_{10} > 0$ *such that if* χ *is a non-principal real character* (mod q) *for any prime* q *and* $L(\beta, \chi) = 0$ *for some real* β, *then* $\beta \leqslant 1 - c_{10}(\log q \log\log q)^2/q^{1/2}$. *Then there exists a computable value of* p_0 *such that* $h_1(q) > h_1(p)$ *whenever* $q > p \geqslant p_0$.

Proof. If

$$q \leqslant \log^2 t(\log\log t)^4 \log\log\log t$$

then

$$t^{\beta} \leqslant t/\exp\left(5c_{10}(\log\log\log t)^{3/2}\right)$$

and so, by (23),

$$|\pi(t; q, 1) - \pi(t; q, -1)| \leqslant \frac{c_8}{q-1} \frac{t}{\log t(\log\log t)^2}$$

for some explicitly computable constant c_8. The result follows from above. ∎

The assumption made in Proposition 2 seems to be quite a strong one. However, a recent result of Goldfeld [8] gives some hope:

GOLDFELD'S THEOREM [8]. *Let E be an elliptic curve over $\mathbf{Q}$ and suppose that the L-function associated to E has a zero of order g at $s=1$. Then there exists an explicitly computable $c_{11} > 0$ such that if χ is a non-principal real character* (mod q) *for any prime q and $L(\beta, \chi) = 0$ for some real β then*

$$\beta \leqslant 1 - c_{11}(\log q)^{g-3}/q^{1/2} \exp\left(21\sqrt{g \log\log q}\right).$$

Recently Gross and Zagier [11] used a stronger form of Goldfeld's Theorem to solve "Gauss's class number problem"—that is, for every $\varepsilon > 0$, they showed the existence of an effectively computable constant $c_\varepsilon > 0$ such that the class number of $Q(\sqrt{-D})$ is $> c_\varepsilon(\log D)^{1-\varepsilon}$. Clearly Theorem 1 follows from Proposition 2 and Goldfeld's Theorem.

ACKNOWLEDGMENTS

The authors thank David Ford for making his ALGEB language available to them, and the anonymous referee for his or her careful comments.

REFERENCES

1. N. C. ANKENY AND S. CHOWLA, The class number of the cyclotomic field, *Proc. Nat. Acad. Sci. U.S.A.* **35** (1949), 529–532.
2. N. C. ANKENY, S. CHOWLA, AND H. HASSE, On the class number of the maximal real subfield of a cyclotomic field, *J. Reine Angew. Math.* **217** (1965), 217–220.
3. B. J. BIRCH AND H. P. F. SWINNERTON-DYER, Notes on elliptic curves, *J. Reine Angew. Math.* **218** (1965), 79–108.
4. L. CARLITZ AND F. R. OLSON, Maillet's determinant, *Proc. Amer. Math. Soc.* **6** (1955), 265–269.
5. H. DAVENPORT, "Multiplicative Number Theory, 2nd Ed.," Springer-Verlag, New York, 1980.

6. P. D. T. A. ELLIOTT AND H. HALBERSTAM, A conjecture in prime number theory, *in* "Sympos. Math.," Vol. 4, pp. 59–72, Academic Press, Orlando, FL, 1968–1969.
7. G. J. FEE AND A. GRANVILLE, The prime factors of Wendt's binomial circulant determinant, *Math. Comp.* **57** (1991), 839–848.
8. D. M. GOLDFELD, The class number of quadratic fields and the conjectures of Birch and Swinnerton–Dyer, *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **3** (1976), 623–663.
9. D. M. GOLDFELD, Gauss' class number problem for imaginary quadratic fields, *Bull. Amer. Math. Soc.* **13** (1985), 23–37.
10. A. GRANVILLE, On the size of the first factor of the class number of a cyclotomic field, *Invent. Math.* **100** (1990), 321–338.
11. B. GROSS AND D. ZAGIER, Points de Heegner et derivées de fonctions L, *C. R. Acad. Sci. Paris* **297** (1983), 85–87.
12. G. HARDY AND J. E. LITTLEWOOD, Some problems of 'partitio numerorum' III. On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.
13. H. HASSE, "Über die Klassenzahl abelscher Zahlkörper," Akademie-Verlag, Berlin, 1952.
14. E. E. KUMMER, Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers, *J. Math. Pures Appl.* **16** (1851), 377–498; "Collected Works," Vol. I, p. 459.
14a. E. E. KUMMER, Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $a^{\lambda}=1$ gebildeten complexen Zahlen, und über den zweiten Factor der Klassenzahl, *Monatsber. Akad. Wiss., Berlin* (1870), 855–880.
15. E. E. KUMMER, Letter to Kronecker, *in* "Collected Works," Vol. I, p. 85.
16. D. H. LEHMER, Prime factors of cyclotomic class numbers, *Math. Comp.* **31** (1977), 599–607.
17. D. H. LEHMER AND J. M. MASLEY, Table of the cyclotomic class number $h^*(p)$ and their factors for $200 < p < 521$, *Math. Comp.* **32** (1978), 577–582.
18. T. LEPISTÖ, On the growth of the first factor of the class number of the prime cyclotomic field, *Ann. Acad. Sci. Fenn. Ser. A I Math.* **577** (1974), 21pp.
19. J. M. MASLEY AND H. L. MONTGOMERY, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.* **286/287** (1976), 248–256.
20. T. METSÄNKYLÄ, Calculation of the first factor of the class number of the cyclotomic field, *Math. Comp.* **23** (1969), 533–538.
21. H. L. MONTGOMERY AND R. C. VAUGHAN, The large sieve, *Mathematika* **20** (1973), 119–134.
22. M. NEWMAN, A table of the first factor for prime cyclotomic fields, *Math. Comp.* **24** (1970), 215–219.
23. S. PAJUNEN, Computation of the growth of the first factor for prime cyclotomic fields, *BIT* **16** (1976), 85–87.
24. J. M. POLLARD, Theorems on factorization and primality testing, *Math. Proc. Cambridge Philos. Soc.* **76** (1974), 521–528.
25. E. SEAH, L. C. WASHINGTON AND H. C. WILLIAMS, The calculation of a large cubic class number with an application to real cyclotomic fields, *Math. Comp.* **41** (1983), 303–305.
26. J. W. TANNER AND S. S. WAGSTAFF, JR., New congruences for the Bernoulli numbers, *Math. Comp.* **48** (1987), 341–350.
27. K. UCHIDA, Class numbers of imaginary abelian number fields, III, *Tôhoku Math. J.* **23** (1971), 573–580.
28. H. S. VANDIVER, On the first factor of the class number of a cyclotomic field, *Bull. Amer. Math. Soc.* **25** (1919), 458–461.
29. L. C. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, New York, 1982.
30. S. S. WAGSTAFF, JR., The irregular primes to 125,000, *Math. Comp.* **32** (1978), 583–591.