On the size of the first factor of the class number of a cyclotomic field

Andrew Granville
Department of Mathematics, University of Toronto,
Toronto, Ontario, M5S 1A1, CANADA.

Abstract

We show that Kummer's conjectured asymptotic estimate for the size of the first factor of the class number of a cyclotomic field is untrue under the assumption of two well-known and widely believed conjectures of analytic number theory.

1. Introduction

In 1850 Kummer [13] published a review of the main results that he and others had discovered about cyclotomic fields. In this elegant report he claimed that he had found an explicit "law for the asymptotic growth" of $h_1(p)$, the so-called first factor of the class number of the cyclotomic field, and would provide a proof elsewhere. This proof never appeared and we believe that Kummer's claim is incorrect. More precisely, let p denote any odd prime, let $h(p)$ be the class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$ (where ζ_p is a primitive pth root of unity) and $h_2(p)$ be the class number of the real subfield $\mathbf{Q}(\zeta_p+\zeta_p^{-1})$. Kummer proved that the ratio $h_1(p) = h(p)/h_2(p)$ is an integer which he called the first factor of the class number, and he claimed that

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

as $p \to \infty$. In support of this conjecture, Ankeny and Chowla [1] established that $h_1(p) = G(p)p^{o(1)}$; and Pajunen [18] that $\frac{2}{3}G(p) < h_1(p) < \frac{3}{2}G(p)$ for each prime $p \le 641$. However such evidence is, we believe, misleading.

Hasse [11] showed that the value of $h_1(p)$ is equal to $G(p)$ times the product of the L-functions of the odd characters $\chi \pmod p$ at $s = 1$. By considering the value of this expression as s goes towards 1 from above, one can deduce that

$$h_1(p) = G(p)\exp\{\frac{p-1}{2}f_p\}$$

where

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

and

$$f_p(x) = \sum_{m\ge1}\frac{1}{m}\left(\sum_{\substack{q \text{ prime}, q^m\le x\\ q^m\equiv1(\mathrm{mod}\,p)}}\frac{1}{q^m} - \sum_{\substack{q \text{ prime}, q^m\le x\\ q^m\equiv-1(\mathrm{mod}\,p)}}\frac{1}{q^m}\right).$$

Therefore Kummer's conjecture (i.e. equation (1)) may be restated as

$$f_p = o(1/p). \tag{2}$$

The expression for f_p allows us to employ any of a number of results of analytic number theory to estimate its value. For instance, we shall see at the start of section 3 that a simple application of the Siegel-Walfisz Theorem implies that

$$f_p = f_p(2^p) + o(1/p) \tag{3}$$

for every odd prime p. Therefore we may restrict our attention to the finite sum $f_p(2^p)$. A similar argument using the Bombieri-Vinogradov Theorem would allow us to restrict our

attention to the much smaller sum $f_p(p^{2+\delta})$ for any $\delta > 0$, for all but a 'small' set of primes p. However we will need something slightly stronger. By using a well-known conjecture of Elliott and Halberstam we will show that for any $\delta > 0$,

$$f_p = f_p(p^{1+\delta}) + o(1/p),$$

for all but at most $x/\log^3 x$ primes $p \le x$. By some elementary arguments, in section 2, we will exclude from this sum all prime powers q^m with $m \ge 2$, for all but a few primes p. Thus Kummer's conjecture will be shown to imply that for each $\delta > 0$,

$$\sum_{\substack{q \text{ prime}, q \le p^{1+\delta} \\ q \equiv 1 (\mathrm{mod} p)}} \frac{1}{q} - \sum_{\substack{q \text{ prime}, q \le p^{1+\delta} \\ q \equiv -1 (\mathrm{mod} p)}} \frac{1}{q} = o(\frac{1}{p}), \tag{4}$$

for all but at most $2x/\log^3 x$ primes $p \le x$.

The idea, in showing that (4) cannot always hold, is to concentrate on those primes p which contain exactly one "small" prime in the arithmetic progressions $\pm 1 \pmod p$ and for which, otherwise, the sum of the reciprocals of the primes in the arithmetic progressions $\pm 1 \pmod p$, up to $p^{1+\delta}$, is very small. We shall assume the well-known conjecture of Hardy and Littlewood [10] that there are $\gg x/log^2 x$ primes $p \le x$ for which $2p+1$ is also prime (or we could take $2p-1$), and will deduce the required estimate for a proportion of these primes, using one of the standard sieve methods. Thus we will show that for such primes p,

$$f_p = 1/(2p+1) + o(1/p),$$

(or $-1/(2p-1) + o(1/p)$ if $2p-1$ is prime) which contradicts (2).

We now give explicitly the conjectures that we need: First a weak form of a conjecture of Hardy and Littlewood [10]:

Conjecture HL. *There are $\gg x/log^2 x$ primes $p \le x$ for which $2p+1$ is also prime.*

Define $\pi(x)$ to be the number of primes $\le x, \pi(x;q,a)$ the number of those primes that belong to the arithmetic progression $a \pmod q$, $\phi(q)$ to be Euler's totient function and $E(x;q,a) = \pi(x;q,a) - \pi(x)/\phi(q)$. Also let $E(x;q) = E(x;q,1) - E(x;q,-1) (= \pi(x;q,1) - \pi(x;q,-1))$. Now the Bombieri-Vinogradov Theorem tells us that, for any given $\varepsilon > 0$ and $A > 0$ we have the estimate $\sum_{q<x^{1/2-\varepsilon}} |E(x;q)| \ll_{\varepsilon,A} \frac{x}{log^A x}$. Recently this has been strengthened by Bombieri, Friedlander and Iwaniec [2], so that the sum may extend a little beyond $x^{1/2}$ although the error term is not as strong. We need more than this however and so use a weak form of the Elliott-Halberstam Conjecture [5]:

Conjecture EH. *For any fixed $\varepsilon > 0, A > 0$,*

$$\sum_{q<x^{1-\varepsilon}} |E(x;q)| \ll_{\varepsilon,A} \frac{x}{log^A x}. \tag{5}$$

Remark: In a recent paper, Friedlander and the author [7] showed that a certain strong form of the Elliott-Halberstam Conjecture (with $q < x/\log^B x$ and $|E(x;q)|$ replaced by $\max_{(a,q)=1} |E(x;q,a)|$ in (5)) fails to hold; however, we do believe that (5) is true.

By using the methods that are outlined above we shall prove at the end of section 4:

Theorem 1. *At least one of the above stated conjectures of Elliott and Halberstam (Conjecture* **EH***), of Hardy and Littlewood (Conjecture* **HL***) and of Kummer (equation (1)) is false.*

Remark: In order to only prove Theorem 1 the statement of Conjecture EH can be weakened to:

. *There exists an explicitly computable value of $\varepsilon > 0$ (depending on the implicit constant in Conjecture HL) and a value of $A > 3$ for which (5) holds.*

We certainly believe the Conjectures EH and HL to be true and that (1) is false. Moreover our method, outlined above, indicates that for some subsequence of primes p, we have $h_1(p) = \{e^{1/4} + o(1)\}G(p)$ (and for some subsequence of those primes p with $2p-1$ prime, we have $h_1(p) = \{e^{-1/4} + o(1)\}G(p)$). It is of interest to determine what actually is the set of limit points of the sequence

$$\Omega = \{h_1(p)/G(p)\}_{p \text{ prime}}.$$

If, instead of as above, we consider the set of those primes p for which each of $2p+1, 6p+1$ and $8p+1$ is prime then we shall be able to deduce that $f_p = 1/(2p+1) + 1/(6p+1) + 1/(8p+1) + o(1/p)$ for some subsequence of these primes (under the assumption of some suitable generalization of Conjecture EH). Then $e^{19/48}$ can be seen to be a limit point of Ω (Similarly, when each of $2p-1, 6p-1, 8p-1$ are prime we can get the limit point $e^{-19/48}$). More generally we define the set of integers $\{0 < r_1 < r_2 < ... < r_k\}$ to be *admissible* if, for each prime q, there exists an integer $a(= a_q), 1 \le a \le q-1$, such that q does not divide $(r_1 - a)(r_2 - a)...(r_k - a)$. A weak form of Hardy and Littlewood's prime k-tuplets Conjecture states

Conjecture HL2. *If $\{0 < r_1 < ... < r_k\}$ is an admissible set of integers then*

a) *There exist $\gg x/log^{k+1}x$ primes $p \le x$ for which each of $r_1p+1, r_2p+1, ..., r_kp+1$ is prime.*

b) *There exist $\gg x/log^{k+1}x$ primes $p \le x$ for which each of $r_1p-1, r_2p-1, ..., r_kp-1$ is prime.*

Define the measure of a finite set of non-zero integers R to be

$$m(R) = \sum_{r \in R} \frac{1}{r}.$$

We shall show, analogously to the above:

Theorem 2. *If Conjectures* **EH** *and* **HL2** *are both true then, for any admissible set of integers R, the numbers $e^{m(R)/2}$ and $e^{-m(R)/2}$ are both limit points of the sequence Ω.*

In section 7 we establish a recent conjecture made by Paul Erdös:

Theorem 3. *There is a sequence of admissible sets $R_1, R_2, \ldots$ such that $\lim_{n\to\infty} m(R_n) = \infty$.*

As any subset of an admissible set is itself admissible we give, in section 8, the elementary consequence (of Theorem 3) that for any real number $a > 0$, there is some sequence of admissible sets whose measures have limit a. Then we deduce from Theorem 2

Theorem 4. *If Conjectures* **EH** *and* **HL2** *are both true then Ω has the set of limit points $[0, \infty]$.*

As a consequence of Theorem 4 it becomes interesting to try to understand how large and how small the ratio $h_1(p)/G(p)$ can get, as a function of p. In section 9 we give some justification to the following

Conjecture A. *For all primes p,*

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

These bounds are best possible in the sense that there exists an infinite sequence of primes p for which

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

and another infinite sequence of primes p for which

$$h_1(p) = G(p)(\log\log p)^{1/2+o(1)}.$$

In section 10 we will show, under the assumption of a stronger version of Conjecture EH, that (1) holds for almost all primes p. We also improve the result $h_1(p) = G(p)p^{o(1)}$ of Ankeny and Chowla:

Theorem 5. *For any sufficiently large constant $c > 0$, the bounds $\frac{1}{c}G(p) < h_1(p) < cG(p)$ hold for a positive proportion $\rho(c)$ of the primes $p \le x$, where $\rho(c)$ tends to 1 as c goes to ∞. The estimate $h_1(p) = G(p)(\log p)^{O(1)}$ holds for all primes p that don't belong to a certain set P_1: Under the assumption of the Generalized Riemann Hypothesis P_1 is the empty set; Unconditionally P_1 contains only primes that are $\equiv 3 \pmod 4$ and it contains no more than one prime in any interval of the form $[x, x^2]$ (so that there are $\ll \log\log x$ primes $p \le x$ belonging to P_1).*

In a forthcoming paper with Gilbert Fung and Hugh C. Williams [8], we compute the values of $h_1(p)$ for each prime $p < 3000$ and give partial factorizations for $p < 2000$. As might be expected from Conjecture A we found that in such ranges the ratio $h_1(p)/G(p)$ is generally fairly close to 1. Indeed there is perhaps no chance of ever finding a prime p for which $h_1(p)$ and $G(p)$ differ by a factor of as much as 2 (as the value of $(\log\log p)^{1/2}$ grows extremely slowly), and so one might never get any indication that (1) is incorrect from explicit computation.

Acknowledgements: I am grateful to John Friedlander, as well as Gilbert Fung, Sid Graham, Kumar Murty and Hugh Williams, for useful conversations concerning this paper.

2. Dealing with the prime powers $q^m \equiv \pm 1 \pmod p$ for $m \geq 2$.

For a given odd prime p define

$$s_p = \sum_{m\geq 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 \pmod p \\ q \text{ prime}}} \frac{1}{q^m}.$$

The main result of this section is

Proposition 1. *The equation $s_p = o(1/p)$ holds for all primes p that do not belong to some set P_2 which contains $\ll x^{1/2}\log^2 x$ primes $p \leq x$.*

This result, together with (3), implies that

$$f_p = g_p(2^p) + o(1/p)$$

for all primes p outside P_2, where we define

$$g_p(x) = \sum_{\substack{q \text{ prime}, q\leq x \\ q\equiv 1 \pmod p}} \frac{1}{q} - \sum_{\substack{q \text{ prime}, q\leq x \\ q\equiv -1 \pmod p}} \frac{1}{q}.$$

Lemma 1. *For any prime p,*

$$\sum_{m\geq 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 \pmod p \\ q^m > p\log^2 p}} \frac{1}{q^m} = O\left(\frac{1}{p\log p}\right).$$

Proof: For any prime $q > p$,

$$\sum_{m\geq 2} \frac{1}{mq^m} \;\leq\; \frac{1}{2}\left(\frac{1}{q^2} + \frac{1}{q^3} + \ldots\right) \;<\; \frac{1}{q^2};$$

and for any prime $q < p$,

$$\sum_{q^m > p^2} \frac{1}{mq^m} \ \le \ \frac{1}{2p^2}\left(1 + \frac{1}{q} + \frac{1}{q^2} + ...\right) \ \le \ \frac{1}{p^2}.$$

Therefore

$$\sum_{m\ge 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 (\mathrm{mod} p) \\ q^m > p^2}} \frac{1}{q^m} \ \le \ \sum_{q>p} \frac{1}{q^2} + \sum_{q\le p} \frac{1}{p^2} \ \ll \ \frac{1}{p \log p} \tag{6}$$

by the Prime Number Theorem.

Now, for any fixed $m \ge 2$ there are $r (\le 2m)$ solutions (mod p) of the congruence $X^m \equiv \pm 1$ (mod p). Therefore if $b_1, b_2, ..., b_r$ are all such solutions then

$$\sum_{\substack{q^m \equiv \pm 1 (\mathrm{mod} p) \\ p \log^2 p < q^m \le p^2}} \frac{1}{q^m} \ \le \ \sum_{i=1}^{r} \sum_{\substack{q \equiv b_i (\mathrm{mod} p) \\ q \le p^{2/m}}} \frac{1}{p \log^2 p} \ \le \ \frac{r}{p \log^2 p} \ \le \ \frac{2m}{p \log^2 p}.$$

(Note that, as $m \ge 2$, there is at most one solution of $q \equiv b_i$ (mod p) with $q \le p^{2/m}$.)

Now if $q^m \le p^2$ then $m \le 4 \log p$ and so

$$\sum_{m\ge 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 (\mathrm{mod} p) \\ p \log^2 p < q^m \le p^2}} \frac{1}{q^m} \ \le \ \sum_{m=2}^{[4 \log p]} \frac{1}{m} \frac{2m}{p \log^2 p} \ \le \ \frac{8}{p \log p}.$$

This bound, together with (6), completes the proof of Lemma 1.

The Proof of Proposition 1: By Lemma 1 it suffices to show that

$$s'_p = \sum_{m\ge 2} \frac{1}{m} \sum_{\substack{q^m \equiv \pm 1 (\mathrm{mod} p) \\ q^m \le p \log^2 p}} \frac{1}{q^m} = o(\frac{1}{p})$$

for all primes p outside a set P_2. Now

$$\sum_{\substack{x < p \le 2x \\ p \text{ prime}}} s'_p \ \le \ \sum_{m\ge 2} \frac{1}{m} \sum_{\substack{q \text{ prime} \\ x \le q^m < 3x \log^2 x}} \frac{1}{q^m} \sum_{\substack{x < p \le 2x, p \text{ prime} \\ p | q^{2m} - 1}} 1.$$

Clearly no more than two primes p in the range $x < p \le 2x$ can divide any such $q^{2m} - 1$ and so

$$\sum_{\substack{x < p \le 2x \\ p \text{ prime}}} s'_p \ \le \ \sum_{q \text{ prime}} \sum_{\substack{x \le q^m < 3x \log^2 x \\ m \ge 2}} \frac{1}{q^m} \ \le \ \sum_{\substack{q \text{ prime} \\ q < 2x^{1/2} \log x}} \frac{2}{x} \ \ll \ \frac{1}{x^{1/2}}.$$

So, if $s'_p \geq \varepsilon/p$ for $\gg x^{1/2}\log x$ primes p in the range $x < p \leq 2x$ then $\sum_{\substack{x<p\leq 2x\\ p \text{ prime}}} s'_p \gg \frac{\log x}{2x^{1/2}}$, giving a contradiction. The result follows from summing over the intervals $[2^{-i-1}x, 2^{-i}x]$.

We note here a result of Ankeny and Chowla [1] that we will use later:

Lemma 2. *For all primes p, $s_p \ll 1/p$.*

Proof: By Lemma 1, we need only consider those prime powers $q^m \equiv \pm 1 \pmod p$ which are $< p\log^2 p$. Now, for any $m \geq 2$, there are at most $2m$ values of q with $q^m \equiv \pm 1 \pmod p$ and $< p\log^2 p$, and so we maximize our sum by assuming that $p \pm 1$ and $2p \pm 1$ are squares, $3p \pm 1, 4p \pm 1$ and $5p \pm 1$ are cubes, etcetera. Therefore

$$\sum_{m\geq 2}\frac{1}{m}\sum_{\substack{q^m\equiv\pm 1 \pmod p\\ q^m < p\log^2 p}}\frac{1}{q^m} \leq \sum_{m\geq 2}\frac{1}{m}\sum_{r=\frac{1}{2}(m^2-m)}^{\frac{1}{2}(m^2+m)-1}\left(\frac{1}{rp+1}+\frac{1}{rp-1}\right) \ll \frac{1}{p}.$$

3. The contribution of the "large" primes.

We start the section by proving (3) which gives a good idea of the methods used here. Define $g_p(x)$ as in the previous section and let

$$g_p = \lim_{x\to\infty} g_p(x).$$

By the method of Riemann-Stieltjes integration we have, for any $x \geq y \geq 3$,

$$\begin{aligned} g_p(x) - g_p(y) &= \int_{t=y}^{x} \frac{d\left(\pi(t;p,1)-\pi(t;p,-1)\right)}{t} = \int_{t=y}^{x}\frac{dE(t;p)}{t} \\ &= \left[\frac{E(t;p)}{t}\right]_y^x + \int_y^x \frac{E(t;p)}{t^2}dt \end{aligned} \tag{7}$$

after integrating by parts. The Siegel-Walfisz Theorem gives that

$$E(x;p) \ll \frac{x}{p\log^2 x} \quad \text{for} \quad x \geq 2^p,$$

and so

$$|g_p(x) - g_p(2^p)| \ll \frac{1}{p^3} + \int_{t=2^p}^{x}\frac{dt}{pt\log^2 t} \ll \frac{1}{p^2}.$$

Therefore $g_p = g_p(2^p) + O(1/p^2)$. This, together with Lemma 1, gives the unconditional estimate

$$f_p = f_p(2^p) + O\left(\frac{1}{p\log p}\right) \tag{3}'$$

which implies (3).

In order to reduce the size of the sum that we are considering we need stronger uniform estimates for $E(x;p)$ than those that are available. Thus we must restrict our search to all but a few primes by using some sort of averaging result on primes in arithmetic progressions (for example, the aforementioned Bombieri-Vinogradov Theorem). We will prove

Proposition 2. *Assume that Conjecture* **EH** *is true. Fix $\delta > 0$. The equation $g_p - g_p(p^{1+\delta}) = o(1/p)$ holds for all primes p, outside some set P_3 which contains $\ll x/\log^3 x$ primes $p \le x$.*

Proof: By summing in (7) we have

$$\sum_{\substack{x<p\le 2x\\ p \text{ prime}}} |g_p - g_p(p^{1+\delta})| \ll \left[\frac{S(t;x)}{t}\right]_{x^{1+\delta}}^{\infty} + \int_{x^{1+\delta}}^{\infty} \frac{S(t;x)}{t^2}dt$$

where $S(t;x) = \sum_{\substack{x<p\le 2x\\ p \text{ prime}}} |E(t;p)|$

$$\ll \frac{1}{\log^5 x} + \int_{x^{1+\delta}}^{\infty} \frac{dt}{t\log^5 t} \ll \frac{1}{\log^4 x},$$

by taking $A = 5$ and $0 < \varepsilon < \delta/(1+\delta)$ in (5). The result follows immediately.

Now, if we combine Propositions 1 and 2 then we can deduce

Corollary 1. *Assume that Conjecture* **EH** *is true. For any fixed $\delta > 0$,*

$$f_p = g_p(p^{1+\delta}) + o(1/p) \tag{8}$$

for all but $O(x/\log^3 x)$ primes $p \le x$.

4. The contribution of the "small" primes.

In this section we will use sieve estimates to get crude upper bounds on $g_p(p^{1+\delta}) - g_p(2p+1)$, which will suffice for our purposes. Define

$$N_k^{\pm}(x) = \#\{p : x < p \le 2x \ \text{ and } \ p, 2p+1 \text{ and } kp \pm 1 \text{ are all prime}\}.$$

It follows from both Brun's and Selberg's sieves (see [9], Theorem 5.7) that if $k < x^2$ then

$$N_k^+(x) \ll \left\{ \prod_{p \mid k(k-2)} \left(\frac{p}{p-1}\right) \right\} \frac{x}{\log^3 x} \qquad \text{if} \ \ k \ge 2,$$

and

$$N_k^-(x) \ll \left\{ \prod_{p \mid k(k+2)} \left(\frac{p}{p-1}\right) \right\} \frac{x}{\log^3 x} \qquad \text{if} \ \ k \ge 1.$$

Therefore

$$\begin{aligned} \sum_{\substack{x<p\le 2x \\ p,2p+1 \text{ prime}}} p \left| g_p(p^{1+\delta}) - \frac{1}{2p+1} \right| &\ll \sum_{\substack{x<p\le 2x \\ p,2p+1 \text{ prime}}} \sum_{\substack{q \equiv \pm 1 \pmod p \\ q \text{ prime } \le p^{1+\delta} \\ q \ne 2p+1}} \frac{p}{q \mp 1} \\ &\le \sum_{k=2}^{x^\delta} \frac{N_{2k}^+(x)}{2k} + \sum_{k=1}^{x^\delta - 1} \frac{N_{2k}^-(x)}{2k} \\ &\ll \frac{x}{\log^3 x} \sum_{k=1}^{x^\delta} \left\{ \frac{1}{k} \prod_{p \mid k(k+1)} \left(\frac{p}{p-1}\right) \right\}. \end{aligned} \tag{9}$$

Now, by a method from [16] one can show that

$$\sum_{k \le y} \prod_{p \mid k(k+1)} \frac{p}{p-1} = (C_1 + o(1))y$$

as $y \to \infty$, where $C_1 = \prod_{p \text{ prime}} \{1 + 2/p(p-1)\}$. Then, by partial summation, we get

$$\sum_{k \le y} \frac{1}{k} \prod_{p \mid k(k+1)} \frac{p}{p-1} = (C_1 + o(1)) \log y$$

and so, by (9), there exists a constant $c_2 > 0$ such that

$$\sum_{\substack{x<p\le 2x \\ p,2p+1 \text{ prime}}} p \left| g_p(p^{1+\delta}) - \frac{1}{2p+1} \right| \le c_2 \delta \frac{x}{\log^2 x}. \tag{10}$$

From this we can deduce

Lemma 3. *Fix $\lambda > 0$ and $\varepsilon > 0$. There exists a $\delta > 0$ such that, for sufficiently large values of x, there are $\le \lambda x/\log^2 x$ primes $p \le x$ such that $2p+1$ is prime and*

$$\left| g_p(p^{1+\delta}) - \frac{1}{2p+1} \right| \ge \frac{\varepsilon}{2p}.$$

Proof: Choose $\delta = \varepsilon\lambda/3c_2$ in equation (10) and the result follows immediately.

Finally we prove

Proposition 3. *Suppose that Conjectures* **EH** *and* **HL** *are both true. Then there are $\gg x/\log^2 x$ primes $p \le x$ for which $f_p = \left(\frac{1}{2} + o(1)\right)\frac{1}{p}$.*

Proof: By Conjecture HL there exists a constant c_3 such that there are $\ge c_3 x/\log^2 x$ primes $p \le x$ for which $2p+1$ is also prime. Fix $\varepsilon > 0$. Letting $\lambda = c_3/2$ in Lemma 3 we find that there are $\ge c_3 x/2\log^2 x$ primes $p \le x$ such that $2p+1$ is prime and

$$\left| g_p(p^{1+\delta}) - \frac{1}{2p+1} \right| < \frac{\varepsilon}{2p}.$$

Then, by Corollary 1, we see that there are $\ge c_3 x/3\log^2 x$ primes $p \le x$ for which $2p+1$ is prime and $|f_p - 1/2p| < \varepsilon/p$, which completes the proof.

Proof of Theorem 1: This follows immediately from the equivalence of equations (1) and (2), and from Proposition 3.

In order to justify the remark following the statement of Theorem 1 we note that in the proof of Proposition 2 (for a set P_3 containing $\ll x/\log^{2+\tau} x$ primes $p \le x$) we need only take $A > 3 + \tau$. Also if we choose the value of ε in the proof of Proposition 3 to be *fixed*, but less than 1, then $f_p > \{1 - \varepsilon + o(1)\}/2p$ for $\ge c_3 x/3\log^2 x$ primes $p \le x$. However fixing ε in Proposition 3 corresponds to fixing δ in Lemma 3 and so, by the proof of Corollary 1, fixing ε in Conjecture EH.

5. Unconditional results ?

The method that is outlined above is unlikely to lead to an unconditional disproof of (1) as it requires the existence of a "small" prime in one of the arithmetic progressions $\pm 1 \pmod p$ (It seems to be out of the range of current methods to even prove that there are infinitely many primes p for which there is a prime $< \frac{1}{5} p \log p$ in either of the arithmetic progressions $\pm 1 \pmod p$ - The result with a constant around $1/4$ can probably be proved by using a method similar to that in [14]). It may however be possible to instead look at numbers that are the product of at most two primes.

Define, as above, the function f_p extended to any positive integer p. Chen's method [3] enables one to show that there are $\gg x/\log^2 x$ integers $p \leq x$ with ≤ 2 prime factors, both $> x^{1/10}$, such that $2p+1$ is prime. We can try to proceed towards an unconditional proof that $|f_p| \gg 1/p$ for some such integers p, by a similar method to that outlined above:

1) The contribution of the prime powers to the sums is usually insignificant (as in section 2).

2) The contribution of primes, other than $2p+1$, that are $< p^{1+\delta}$, is insignificant for a proportion of such integers (as in section 4).

3) For the primes $> p^2$ we may use the aforementioned result of Bombieri, Friedlander and Iwaniec [2], in place of Conjecture EH, in the proof of a version of Proposition 2.

4) We are left with the primes between $p^{1+\delta}$ and p^2 that are $\equiv \pm 1 \pmod p$. These seem to be the most difficult to handle. There is perhaps some hope that an application of the large sieve may allow us to deal with at least a proportion of the remaining values of p, although I have been unable to do this.

6. Arbitrary admissible sets

In this section we outline the proof of

Proposition 4. *Suppose that Conjectures* **EH** *and* **HL2** *are both true, and that* $R = \{r_1, r_2, ..., r_k\}$ *is a given admissible set. Then*

a) *There are* $\gg x/\log^{k+1} x$ *primes* $p \le x$ *for which* $f_p = \{m(R) + o(1)\}\frac{1}{p}$.

b) *There are* $\gg x/\log^{k+1} x$ *primes* $p \le x$ *for which* $f_p = \{-m(R) + o(1)\}\frac{1}{p}$.

Theorem 2 follows from Proposition 4 by noting again that $\log(h_1(p)/G(p)) = \frac{p-1}{2} f_p$. The proof of Proposition 4 is much like that given in sections 2-4 for the case $R = \{2\}$:

1) We use Proposition 1 exactly as before.

2) We take (5) with $A = k + 4$ in the proof of Proposition 2 (rather than with $A = 5$ as before) to show that $g_p - g_p(p^{1+\delta}) = o(1/p)$ holds for all primes p, outside some set P_3 which contains $\ll x/\log^{k+2} x$ primes $p \le x$.

3) Let $\sigma = 1$ in a), -1 in b). We will consider those primes p for which $rp + \sigma$ is prime for every $r \in R$. Assuming Conjecture HL2 there are $\gg x/\log^{k+1} x$ such primes p that are $\le x$. Now, for any integer $\ell \ge 1$, let

$$N_\ell^{\pm}(x) = \#\{p : x < p \le 2x, \text{ and } p,\ rp + \sigma \text{ for each } r \in R \text{ and } \ell p \pm 1 \text{ are all prime}\}.$$

As in section 4 we know, by using any sieve method, that for $\ell < x^{1/2}$ and $\tau = \pm 1$, we have

$$N_\ell^\tau \ll_R C_\ell^\tau \frac{x}{\log^{k+2} x} \qquad \text{except when } \sigma = \tau \text{ and } \ell \in R,$$

$$\text{and the constant} \quad C_\ell^\tau = \prod_{p \mid \ell \prod_{r\in R}(\ell - r\tau\sigma)} \left(\frac{p}{p-1}\right).$$

As before it does take some work to show that

$$\sum_{\ell \le y} \frac{1}{\ell} C_\ell^\tau = \{C_R + o(1)\} \log y,$$

where $C_R = \prod_{p \text{ prime}} \{1 + \omega_p(R)/p(p-1)\}$ and

$$\omega_p(R) = \#\{\ell : 0 \le \ell \le p-1 \text{ and } p \mid \ell \prod_{r\in R}(\ell - r\tau\sigma)\}.$$

Therefore, for any given $\varepsilon, \lambda > 0$ we have, similar to Lemma 3, a value of δ such that whenever x is sufficiently large, there are $\le \lambda x/\log^{k+1} x$ primes $p \le x$ for which each $rp + \sigma$ is prime (i.e. for each $r \in R$) and

$$\left| g_p(p^{1+\delta}) - \sum_{r\in R} \frac{\sigma}{rp + \sigma} \right| \ge \frac{\varepsilon}{2p}.$$

4) Finally, as in the proof of Proposition 3, we have

$$f_p = \sum_{r \in R} \frac{\sigma}{rp + \sigma} + o(\frac{1}{p})$$

for $\gg x/\log^{k+1} x$ primes $p \leq x$, and

$$\sum_{r \in R} \frac{\sigma}{rp + \sigma} = \{\sigma m(R) + o(1)\}\frac{1}{p}.$$

7. Erdös's Conjecture: Admissible sets with arbitrarily large measure.

In a lecture given during the recent NATO Advanced Study Institute at Banff, Alberta in the Spring of 1988, Professor Erdös conjectured that our Theorem 3 held - that is that there exist admissible sets with arbitrarily large measure. He was interested in this question in connection with an entirely different question - champion numbers with respect to certain functions connected with the prime divisors of an integer - see his paper with J.L. Nicolas [6].

The main problem that one encounters in trying to prove Theorem 3 is that the seemingly most likely method to succeed - one based in some way on the beautiful construction of Hensley and Richards [12] - is difficult to do. We look at the problem in a rather different way:

The reason that we wish to construct admissible sets $R = \{r_1, r_2, ..., r_k\}$ is so as to find primes p for which each of $r_1p+1, r_2p+1, ..., r_kp+1$ is prime. We do, of course, know that such sets R exist for each *given* prime p, which we can construct as follows:

For the given prime p and for any finite set of primes $Q = \{q_1 < q_2 < .. < q_\ell\}$ in the arithmetic progression $1 \pmod p$, define R_0 to be the set $\{r_1, r_2, ..., r_\ell\}$ where $r_i = (q_i - 1)/p$ for each i. We must ask ourselves: Is R_0 an admissible set and, if not, why not ?

Suppose that t is a prime where $t \neq p$ and $t \notin Q$. Let a_t be the least non-negative residue of $-1/p \pmod t$ and so $r \not\equiv a_t \pmod t$ for every $r \in R_0$ (else t divides $q = rp+1 \in Q$ and, as t and q are both prime, so $t = q \in Q$, giving a contradiction). Therefore if R_0 is not admissible then it is because it lacks a suitable congruence class either for a prime in Q or for the prime p. The idea now is to remove elements from R_0 so as to (i) Create suitable values of a_t for each $t \in Q \cup \{p\}$ and (ii) Maximize the measure of the remaining set R. We do this by using the following recursive algorithm:

Let $q_0 = p$. For $i = 0, 1, 2, ..., \ell$ choose a_{q_i} to be the value of b in the range $1 \leq b \leq q_i - 1$ that maximizes the measure of the set

$$\{r \in R_i : r \not\equiv b (\text{mod } q_i)\},$$

and then call this set R_{i+1}; clearly

$$m\left(R_{i+1}\right) \geq \left(1-\frac{1}{q_i-1}\right) m\left(R_i\right).$$

By going through this procedure $\ell+1$ times we end up with an admissible set $R=R_{\ell+1}$ where

$$m(R) \geq p \prod_{q \in Q \cup\{p\}}\left(1-\frac{1}{q-1}\right) \sum_{q \in Q} \frac{1}{q-1}. \tag{11}$$

It remains to choose p and Q so that the quantities in (11) are as large as we like:

Now, for any prime p pick values of x and y with $x>y^2$ and $y \geq 2^p$, and let Q be the set of primes between y and x that are $\equiv 1 \pmod{p}$. Then, by a simple application of the Siegel-Walfisz Theorem we have,

$$\sum_{q \in Q} \frac{1}{q-1}=\frac{1}{p-1} \log \left(\frac{\log x}{\log y}\right)+O\left(\frac{1}{p \log ^2 y}\right).$$

By taking the exponential of both sides we can deduce

$$\prod_{q \in Q}\left(1-\frac{1}{q-1}\right)=\left(\frac{\log y}{\log x}\right)^{\frac{1}{p-1}}\left\{1+O\left(\frac{1}{p \log ^2 y}\right)\right\}.$$

Then, by (11),

$$m(R) \geq \frac{\log \left(\frac{\log x}{\log y}\right)}{\left(\frac{\log x}{\log y}\right)^{\frac{1}{p-1}}}\left\{1+O\left(\frac{1}{p^2}\right)\right\}. \tag{12}$$

Proof of Theorem 3: Fix $M>1$. For each prime p we let $y=2^p$ and $x=y^N$ where $N=e^{2M}$. Then, by (12),

$$m(R) \ \geq \ \frac{2M}{N^{\frac{1}{p-1}}}\{1+O(\frac{1}{p^2})\} \ \geq \ 2M\{1+O(\frac{M}{p})\} \ > \ M,$$

for all sufficiently large p.

It is certainly of interest to find out how large the measure of an admissible set can be with respect to its largest element:

For each prime p in the interval $[x, 2x]$, let Q_p be the set of primes in $[y, z]$ that belong to the arithmetic progression 1 (mod p) (Here $y=x^3$ and $z=e^{3x^2}$). Define

$$\Sigma=\sum_{\substack{x<p \leq 2x \\ p \text{ prime}}}\left|\sum_{q \in Q_p} \frac{1}{q-1}-\frac{1}{p-1} \log \left(\frac{x^2}{\log x}\right)\right|.$$

Now, for each prime p,

$$\sum_{q\in Q_p}\frac{1}{q-1}=\int_{t=y}^{z}\frac{d\pi(t;p,1)}{t-1}$$
$$=\frac{1}{p-1}\left\{\log\left(\frac{x^2}{\log x}\right)+\int_y^z\frac{dt}{t(t-1)\log t}\right.$$
$$\left.+\left[\frac{E(t;p,1)}{t-1}\right]_y^z+\int_y^z\frac{E(t;p,1)}{(t-1)^2}dt\right\}.$$

Now $\int_y^z dt/t(t-1)\log t\ll 1/x^3\log x$ and so, summing over the primes in [x,2x], we get

$$\Sigma\ \ll\ \frac{1}{x^3\log x}+\left[\frac{S(t;x)}{t}\right]_y^z+\int_y^z\frac{S(t;x)}{t^2}dt$$
$$\ll\ \frac{1}{\log^2 x}$$

from using the Bombieri-Vinogradov Theorem in the form $S(t;x)\ll t/\log^3 t$ whenever $t>x^3$. Therefore we certainly have a prime p in the interval $[x,2x]$ for which

$$\sum_{q\in Q_p}\frac{1}{q-1}=\frac{1}{p-1}\log\left(\frac{x^2}{\log x}\right)+O\left(\frac{1}{x\log x}\right).$$

Therefore, by (12),

$$m(R_p)\ \geq\ \frac{\log\left(\frac{x^2}{\log x}\right)}{\left(\frac{x^2}{\log x}\right)^{\frac{1}{x}}}\left\{1+O\left(\frac{1}{x^2}\right)\right\}$$
$$\geq\ 2\log x+O(\log\log x).$$

However $R_p\subset[1,z]$ and so, as $\log\log z=2\log x+O(1)$ we have proved

Proposition 5. *For any sufficiently large x there is an admissible set S, which is a subset of $[1,x]$, with $m(S)\geq\{1+o(1)\}\log\log x$.*

We believe that Proposition 5 is the best possible such result in the sense that any admissible subset S of $[1,x]$ has $m(S)\leq\{1+o(1)\}\log\log x$. We can prove a result in this direction quite easily:

It is well known that, by any sieve method, if we remove one arithmetic progression (mod p) from $[1,x]$ for each prime p then we will be left with $\ll x/\log x$ integers. But any admissible set R has the property that it does not contain any integer in at least one arithmetic progression (mod p) for every prime p, and so, for all x, $|R\cap[1,x]|\ll x/\log x$. Then, by partial summation, we see that we can prove

Lemma 4. *There exists a constant $c_4 > 0$ such that if S is an admissible subset of $[1, x]$, then $m(S) \le c_4 \log\log x$.*

With some care it may be shown that we can take the constant $c_4 = 2$ in Lemma 4, provided that x is sufficiently large.

8. The set of limit points.

Let $\mathcal{M}$ be the set of measures $m(R)$ of admissible sets R, and let $\overline{\mathcal{M}}$ be the closure of $\mathcal{M}$; that is the set of limit points of sequences of elements of $\mathcal{M}$ that do converge. We prove

Proposition 6. *Assume that Conjectures* **EH** *and* **HL2** *are both true. If $a \in \overline{\mathcal{M}}$ then $-a$ and a are limit points of the sequence $\{pf_p\}_{p \text{ prime}}$.*

Proof: Fix $\varepsilon > 0$. Let $\sigma = -1$ or 1, according to whether we're proving the result for $-a$ or a. Let $R_1, R_2, ...$ be a sequence of admissible sets for which $\lim_{n\to\infty} m(R_n) = a$. Thus, if n is sufficiently large then $|m(R_n) - a| < \varepsilon/2$. Now, by Proposition 4, there are $\gg x/\log^{|R_n|+1} x$ primes $p \le x$ for which $|pf_p - \sigma m(R_n)| < \varepsilon/2$ for all sufficiently large values of x. Therefore for any such prime p, $|pf_p - \sigma a| < \varepsilon$.

Proposition 7. $\overline{\mathcal{M}} = [0, \infty]$.

Proof: By noting that $\{n\}$ is an admissible set for every even integer n, we see that $1/n \in \mathcal{M}$ and so $0 \in \overline{\mathcal{M}}$. Moreover, by Theorem 3, $\infty \in \overline{\mathcal{M}}$.

Let a be any fixed positive real number and choose ε in the range $a > \varepsilon > 0$. Fix n to be an integer $> 1/\varepsilon$ and let c_n be the measure of the set of integers $\le n$. By Theorem 3 we can pick an admissible set R with $m(R) > a + c_n$. Now let S be the subset of integers in R that are $> n$: Note that $m(S) \ge m(R) - c_n > a$. If S is the set $\{s_1 < s_2 < ... < s_\ell\}$ then define T to be the set $\{s_1 < s_2 < ... < s_k\}$ where k is chosen so that $m(T) \ge a$ but $a > m(T) - 1/s_k$. Therefore T is admissible (as any subset of an admissible set is admissible) as $T \subset R$, and $|m(T) - a| < 1/s_k < 1/n < \varepsilon$. Therefore $a \in \overline{\mathcal{M}}$.

Proof of Theorem 4: By Propositions 6 and 7 we see that the set of limit points of the sequence $\{pf_p\}_{p \text{ prime}}$ is $[-\infty, \infty]$. The result follows from noting, once again, that $h_1(p)/G(p) = \exp(\frac{p-1}{2} f_p)$.

9. On the maximal and minimal order of $h_1(p)/G(p)$.

The methods of this section are highly conjectural and are only intended as a guide to making a plausible conjecture as to the maximal and minimal order of $h_1(p)/G(p)$. Now, for $a = 1$ and -1 it seems likely that

$$E(x;p,a) \ll \left(\frac{x}{p}\right)^{1/2} \exp((\log x)^{1/2}) \quad \text{whenever} \quad x > p,$$

and

$$\pi(x;p,a) \ll \frac{x}{p\log x} \qquad \text{whenever} \quad x > p\log^3 p.$$

By taking the first of these estimates when $x > p\exp(3(\log p)^{1/2}) = x_0$, and the second for when $x_0 \geq x > p\log^3 p$, we can use partial summation and Lemma 2 to show that

$$f_p = g_p(p\log^3 p) + O\left(\frac{1}{p(\log p)^{1/2}}\right).$$

Now, by the Brun-Titchmarsh Theorem there exists a constant $c_5 > 0$ for which $\pi(x;p,a) \leq c_5 x/(p-1)\log(x/p)$ for all $x \geq 2p-1$. Therefore, by using a Riemann-Stieltjes integral, it is easy to deduce that

$$g_p(p\log^3 p) \leq \sum_{\substack{q\equiv \pm 1 \pmod p \\ 2p-1\leq q\leq p\log^3 p}} \frac{1}{q} \;\leq\; \frac{c_5}{p}\{\log\log\log p + O(1)\}.$$

Therefore $|f_p| \leq \frac{c_5}{p}\{\log\log\log p + O(1)\}$, and so

$$(\log\log p)^{-c_5/2} \ll \frac{h_1(p)}{G(p)} \ll (\log\log p)^{c_5/2}. \tag{13}$$

Montgomery and Vaughan [17] have shown that we may take $c_5 = 2$ and it is conjectured that one may take $c_5 = 1 + o(1)$. This gives the bounds in Conjecture A.

On the other hand, suppose that R is an admissible set containing k elements from $[1,z]$. In [10] explicit constants were given for Conjecture HL2 and it can easily be shown that these are $> 1/(\log z)^{2k}$; that is we would certainly expect $> x/(\log x\log z)^{2k}$ primes $p \leq x$ for which $rp \pm 1$ is prime for each $r \in R$. Taking, say, $x = z^{10z}$ this gives more than z^{7z} such primes p. So let p be such a prime with $p \approx z^{10z}$ (and so $z \approx \log p/10\log\log p$). Now, by Proposition 7 we can pick such a set R with

$$m(R) \geq \{1+o(1)\}\log\log z \geq \{1+o(1)\}\log\log\log p,$$

and so, using the methods of earlier in the paper, we'd expect $f_p = \frac{\{\sigma+o(1)\}\log\log\log p}{p}$, for $\sigma = \pm 1$. Thus we see that $h_1(p)/G(p)$ essentially attains the bounds given in Conjecture A.

10. The usual order of $h_1(p)/G(p)$.

A strong form of Conjecture EH would state that

Conjecture EH2. *We have the estimate*

$$S(t;x) \ll \frac{t}{\log^3 t}$$

uniformly for any $t \geq x\exp((\log x)^{1/2}) = t_0$.

Then, by a similar argument to Proposition 2,

$$\sum_{\substack{x<p\leq 2x\\ p \text{ prime}}} |g_p - g_p(t_0)| \ \ll \ \frac{1}{\log^2 x}.$$

Also

$$\begin{aligned}\sum_{\substack{x<p\leq 2x\\ p \text{ prime}}} |pg_p(t_0)|^2 \ &\ll \sum_{k,\ell<t_0/x} \frac{1}{k\ell} \#\{x<p\leq 2x : p, kp\pm 1 \text{ and } \ell p\pm 1 \ \text{ are all prime}\}\\ &\ll \frac{x}{\log^2 x},\end{aligned}$$

by using either Brun's or Selberg's sieve and then summing (as in the proof of Lemma 3). Combining these two bounds with Proposition 1 gives

Proposition 8. *Assume that Conjecture* **EH2** *is true. Then (1) holds for all primes except those belonging to a certain set* P_5. *For any given function* $\psi(x)$ *that* $\to\infty$ *as* $x\to\infty$ *there are* $O\left(\psi(x)\frac{x}{\log^2 x}\right)$ *primes* $p\leq x$ *that are contained in* P_5 *if* x *is sufficiently large.*

Combining the above equations with Proposition 3 gives

Proposition 9. *Assume that Conjectures* **EH2** *and* **HL** *are both true. Then, for any fixed* $\lambda, 1/2>\lambda>0$, *there are*

a) $\asymp_\lambda \frac{x}{\log^2 x}$ *primes* $p\leq x$ *for which* $f_p\geq \lambda/p$.

b) $\asymp_\lambda \frac{x}{\log^2 x}$ *primes* $p\leq x$ *for which* $f_p\leq -\lambda/p$.

We now look at what can be proved without assuming any hypothesis:

Proof of Theorem 5: Using Lemma 2, equation (7) with $x=\infty$ and $y=2p-1$, and the Brun-Titchmarsh Theorem, we see that

$$f_p = \int_{x_p}^{\infty} \frac{E(t;p)}{t^2}dt + O\left(\frac{\log\log p}{p}\right) \tag{14}$$

where $x_p = \exp(\log^4 p)$. We can bound $E(t;p)$ when $t\geq x_p$ by using the following well known results of analytic number theory (see [4], p.94 and 123):

Lemma 5. *There exists a constant $c_6 > 0$ such that if P_6 is the set of primes for which $L(s, \chi_p)$ (where χ_p is the real non-principal character (mod p)) has a zero β in the range*

$$\beta > 1 - c_6/\log p \tag{15}$$

then i) P_6 is empty if the Generalized Riemann Hypothesis holds; and ii) P_6 contains at most one prime in any interval of the form $[x, x^2]$ unconditionally. If $p \in P_6$ then the above value of β is unique and we have

$$E(x;p) = \frac{\chi_p(-1)-1}{p-1}\ \frac{x^\beta}{\beta \log x}\ +\ O\left(\frac{x}{p\log^2 x}\right) \tag{16}$$

in the range $x > \exp(\log^3 p)$. If $p \notin P_6$ then $E(x;p) = O\left(\frac{x}{p\log^2 x}\right)$ in the same range.

Note that if $p \in P_6$ and $p \equiv 1 \pmod 4$ then $\chi_p(-1) = 1$ (as χ_p is essentially the Legendre symbol (mod p)) and so, by (16), we have $E(x;p) = O\left(\frac{x}{p\log^2 x}\right)$. Thus, if $p \notin P_1 = \{p \in P_6 : p \equiv 3 \pmod 4\}$ we get, using Lemma 5, that

$$\int_{x_p}^\infty \frac{E(t;p)}{t^2}dt\ \ll\ \frac{1}{p}\ \int_{x_p}^\infty \frac{dt}{t\log^2 t}\ \ll\ \frac{1}{p\log^3 p}.$$

Therefore, by (14), $f_p \ll \frac{\log\log p}{p}$. This gives the first part of Theorem 5.

By using sieve methods, as in section 4, one can easily prove, analogously to (10), the inequality

$$\sum_{\substack{x<p\le 2x\\ p\ \text{prime}}} p\left|g_p(p^3)\right|\ \ll \frac{x}{\log x}.$$

By using the Bombieri-Vinogradov Theorem, instead of Conjecture EH, in the proof of Proposition 2, one can show that

$$\sum_{\substack{x<p\le 2x\\ p\ \text{prime}}} p\left|g_p - g_p(p^3)\right|\ \ll \frac{x}{\log^2 x};$$

and finally, from the proof of Proposition 1,

$$\sum_{\substack{x<p\le 2x\\ p\ \text{prime}}} p\left|f_p - g_p\right|\ \ll \frac{x}{\log^2 x}.$$

Adding these three inequalities together gives

$$\sum_{\substack{x<p\le 2x\\ p\ \text{prime}}} p\left|f_p\right|\ \ll \frac{x}{\log x},$$

so that $|f_p| \ge \frac{2\log c}{p}$ for $\ll x/(\log c \log x)$ primes p in the interval $x < p \le 2x$.

11. References

1. N.C. Ankeny and S. Chowla, The class number of the cyclotomic field, Proc. Nat. Acad. Sci., **35** (1949) 529-532.
2. E. Bombieri, J.B. Friedlander and H.Iwaniec, Primes in Arithmetic Progessions to Large Moduli, Acta Math. **156** (1986) 203-251; II, Math. Ann. **277** (1987) 361-393; III, J. Amer. Math. Soc., **2** (1989) 215-224.
3. J. Chen, On the representation of a large even integer as the sum of a prime and the product of at most two primes, Sci. Sinica, **16** (1973) 157-176.
4. H. Davenport, Multiplicative Number Theory, (2nd.Edn.), Springer-Verlag, New York, 1980.
5. P.D.T.A. Elliott and H. Halberstam, A conjecture in prime number theory, Symp. Math., **4** (1968-69) 59-72.
6. P. Erdös and J.L. Nicolas, On functions connected with prime divisors of an integer, Number Theory and Applications (NATO ASI series, ed. R.A.Mollin, 1989) 381-391.
7. J.B. Friedlander and A. Granville, Limitations to the equi-distribution of primes I, Ann. of Math., **129** (1989) 363-382.
8. G. Fung, A. Granville and H.C. Williams, Computations of the first factor of the class number of cyclotomic fields, (to appear).
9. H. Halberstam and H.E. Richert, Sieve Methods, Academic Press, New York, 1974.
10. 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.
11. H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952.
12. D. Hensley and I. Richards, Primes in Intervals, Acta Arithm., **25** (1974) 375-391.
13. E.E. Kummer, Mémoire sur la théorie des nombres complexes composés de racines de l'unité et des nombres entiers, J. de math. pures et appl., **16** (1851) 377-498; Collected Works, Vol.I., p.459.
14. H. Maier, Small differences between prime numbers, Michigan Math J., **35** (1988) 323-344.
15. J.M. Masley and H.L. Montgomery, Cyclotomic Fields with unique factorization, J. reine angew Math., **286/287** (1976) 248-256.
16. H.L. Montgomery, Topics in Multiplicative Number Theory, Lecture Notes in Math., 227, Springer, New York, (1971).
17. H.L. Montgomery and R.C. Vaughan, The large sieve, Mathematika, **20** (1973) 119-134.
18. S. Pajunen, Computation of the growth of the first factor for prime cyclotomic fields, BIT, **16** (1976) 85-87.

Dept. of Mathematics, University of Toronto, Toronto, Ontario, M5S 1A1, CANADA.

(Current Address) School of Mathematics, The Institute for Advanced Study, Princeton, NJ 08540, USA.