Annals of Mathematics, 129 (1989), 363–382

Limitations to the equi-distribution of primes I

By JOHN FRIEDLANDER[†] and ANDREW GRANVILLE[†]

Abstract

For any fixed $N > 0$ we show that there exist arbitrarily large values of a and x for which

$$\sum_{\substack{q < x/\log^N x \\ (q,a)=1}} |\psi(x;q,a) - x/\phi(q)| \gg_N x.$$

This disproves conjectures of Elliott and Halberstam, and of Montgomery. We also establish a number of related results.

1. Introduction

In 1837, Dirichlet proved that if a and q are co-prime integers then there are infinitely many primes $\equiv a \pmod q$. His ideas combined with those of Hadamard and de la Vallée Poussin yielded the asymptotic formula

$$\psi(x;q,a) = \frac{x}{\phi(q)}\{1 + o(1)\} \tag{1.1}$$

as $x \to \infty$ where $\psi(x;q,a) = \sum_{\substack{n \le x \\ n \equiv a \ (\mathrm{mod}\ q)}} \Lambda(n)$, Λ is Von Mangoldt's function, and ϕ is Euler's totient function.

In 1936 Walfisz [20] used a theorem of Siegel [17] to show that for any fixed $N > 0$, the estimate (1.1) holds uniformly throughout the range

$$q < \log^N x \quad \text{and} \quad (a,q) = 1. \tag{1.2}$$

This is the largest range for which an estimate of the form (1.1) is known to hold uniformly; however under the assumption of the Generalized Riemann Hypothesis (GRH) one can prove that the estimate

$$\psi(x;q,a) = \frac{x}{\phi(q)} + O(x^{1/2}\log^2 x) \tag{1.3}$$

[†]Research of both authors partially supported by NSERC.

holds uniformly for all

$$q < x \quad \text{and} \quad (a, q) = 1, \tag{1.4}$$

(see [7], p. 125). Evidently this implies that (1.1) would hold in the range

$$q < x^{1/2}/\log^{2+\varepsilon} x \quad \text{and} \quad (a, q) = 1$$

for any fixed $\varepsilon > 0$. Although an unconditional proof of these estimates is out of reach at present, it is possible to obtain such results in an average sense. In 1965 Bombieri [1] and Vinogradov [19] established such a result which in the slightly stronger form of Bombieri, states that for any fixed $A > 0$, there exists a value of $B = B(A) > 0$ such that

$$\sum_{q \le Q} \max_{(a,q)=1} |\psi(x; q, a) - x/\phi(q)| \ll_A x/\log^A x \tag{1.5}$$

where

$$Q = x^{1/2}/\log^B x. \tag{1.6}$$

Much important progress in number theory could be made if the range of the estimate (1.1) or even if the value of Q in (1.6) could be made larger. To this end Montgomery [13], [14] has conjectured that for any $\varepsilon > 0$,

$$\left|\psi(x; q, a) - \frac{x}{\phi(q)}\right| \ll_\varepsilon (x/q)^{1/2+\varepsilon} \log x \tag{1.7}$$

holds uniformly in the range (1.4), which would imply that (1.1) holds uniformly for all

$$q < x/\log^{2+\varepsilon} x \quad \text{and} \quad (a, q) = 1. \tag{1.8}$$

Elliott and Halberstam [9] have made a considerably weaker conjecture in connection with (1.5). They considered the related estimate

$$\sum_{q \le Q} \phi(q) \max_{(a,q)=1} \left\{\pi(x; q, a) - \frac{\operatorname{li} x}{\phi(q)}\right\}^2 \ll_A \frac{x^2}{\log^A x} \tag{1.9}$$

and conjectured that for any given $A > 1$, (1.9) holds for any $Q < x/\log^{A+1} x$, "or something only slightly weaker".

We will use a technique of Maier [12] to show that Montgomery's conjecture is false, as is the Elliott and Halberstam conjecture (1.9) when one takes $Q = x/\log^B x$ for any fixed $B > 0$.

Henceforth define R to be the set of integers q that are free of prime factors $< \log q$. We prove:

Proposition 1. *Fix $B > 1$. There exist arbitrarily large values of Q such that for any subset S of R, where each $q \in S$ is in the range*

$$Q/\log^{1/8} Q < q < Q \tag{1.10}$$

there exist values of a and x with

$$Q \log^B Q < x < 3Q \log^B Q \tag{1.11}$$

for which

$$\sum_{\substack{q \in S \\ (q,a)=1}} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \gg_B \sum_{q \in S} \frac{x}{\phi(q)}. \tag{1.12}$$

Remark 1. Under the assumption of GRH (in fact rather weaker assumptions suffice) we may change "There exist arbitrarily large Q" to "For all sufficiently large Q" in the above.

Remark 2. The implied constant in (1.12) is given explicitly by the proof.

Remark 3. The expected analogous statement holds where ψ is replaced by π.

Remarks similar to the above are applicable to all of the following theorems. From Proposition 1 we easily deduce:

THEOREM 1. *Fix $B > 1$. There exist arbitrarily large values of a and x for which*

$$\text{(i)} \quad \sum_{\substack{T<q<4T \\ (q,a)=1}} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \gg_B \frac{x}{\log\log x} \tag{1.13}$$

where $T = x/4\log^B x$.

$$\text{(ii)} \quad \sum_{\substack{q<x/\log^B x \\ (q,a)=1}} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \gg_B x. \tag{1.14}$$

We deduce from Theorem 1, Remark 3, and Cauchy's inequality:

COROLLARY 1. *Fix A, B and let $Q = x/\log^B x$. If $A > 0$ the estimate* (1.5) *fails while if $A > 2$ the estimate* (1.9) *fails.*

Thus the Elliott-Halberstam conjecture is false. However the oft-quoted [10 et al.] weaker version of the conjecture that (1.5) holds with $Q = x^{1-\varepsilon}$ is still open.

If we take $S = \{q\}$ where q is a prime, in Proposition 1, then we have:

COROLLARY 2. *For any fixed $B > 0$ the estimate* (1.1) *cannot hold uniformly for the range*

$$q < x/\log^B x \quad \text{and} \quad (a, q) = 1. \tag{1.15}$$

Thus Montgomery's conjectured estimate (1.7) is incorrect. Moreover, even if we replace the right hand side of (1.7) by something of the form $(x/q)^{1-\varepsilon}\log^N x$ (for some ε, $N > 0$), this estimate is still incorrect.

In Theorem 3 we shall see, assuming GRH, that the estimate (1.1) actually fails frequently in the range (1.15).

By sacrificing the fixed value of a in Theorem 1, we can considerably improve our lower bounds:

THEOREM 2. *Fix $B > 1$. There exist arbitrarily large values of y such that for any value of Q in the range*

$$y/\log^B y < Q < y/\log y \log\log y \tag{1.16}$$

there exists x $(= x(Q))$ in the range

$$y < x < 3y \tag{1.17}$$

such that

$$\sum_{Q<q<2Q} \max_{(a,q)=1} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \gg_B \sum_{Q<q<2Q} \frac{x}{\phi(q)}. \tag{1.18}$$

Remark. Under the assumption of the Generalized Riemann Hypothesis we can get a slightly better explicit constant in (1.18).

These results leave a "hole" in the conjectured results about primes in arithmetic progressions. Of course, it has long been known (the Brun-Titchmarsh Theorem) that the estimate

$$\pi(x; q, a) \ll \frac{x}{\phi(q)\log(x/q)}$$

holds uniformly in the range (1.4). It seems likely that one has the stronger

Conjecture 1. Fix $\varepsilon > 0$. (a) The estimate $\psi(x; q, a) \ll_\varepsilon x/\phi(q)$ holds in the range (1.8).

(b) The estimate $\psi(x; q, a) = x/\phi(q) + O((x/q)^{1/2}x^\varepsilon)$ holds in the range (1.4).

We also make a weaker conjecture to replace the Elliott-Halberstam conjecture for very large moduli (we believe that (1.5) does hold for $Q = x^{1-\varepsilon}$).

Conjecture 2. Fix $\varepsilon > 0$. The estimate

$$\sum_{Q<q<2Q} \max_{(a,q)=1} \psi(x; q, a) \ll_\varepsilon \sum_{Q<q<2Q} x/\phi(q)$$

holds for $Q < x/\log^{2+\varepsilon} x$.

Conjecture 2 implies that Theorem 2 is essentially the strongest possible result, up to the implicit constant in (1.18). The analogous conjecture with a fixed will be studied in our next paper.

Finally we have:

THEOREM 3. *Assume that the Generalized Riemann Hypothesis holds. For any positive-valued* $g(x)$ *tending to* 0 *as* $x \to \infty$ *let* Q_g *be the set of integers* q *with more than* $\exp(g(q)\log_2 q)$ *distinct prime factors. (Henceforth* $\log_k x$ *is the k-fold iterated logarithm.) Fix* $\varepsilon > 0$ *and* $N > 1$. *Then, for all sufficiently large* $q \notin Q_g$, *and for any value of* y *in the range*

$$q \log q < y < q \log^N q, \tag{1.19}$$

we have

$$\left|\psi(x; q, a) - \frac{x}{\phi(q)}\right| \gg_{N, \varepsilon, g} \frac{x}{\phi(q)} \tag{1.20}$$

for at least $q/\exp((\log q)^{\varepsilon})$ *distinct values of* $a \pmod q$, *with* $(a, q) = 1$, *for some* $x = x(a)$ *in the range*

$$y \le x \le 2y. \tag{1.21}$$

Remark. Pomerance [15] has shown that if $g(x) = 1/\log_3 x$ and $q \notin Q_g$ then there exists a, with $(a, q) = 1$, for which the least prime in the arithmetic progression $a \pmod q$ is

$$\ge (e^{\gamma} + o(1))\phi(q)\log q \log_2 q \log_4 q/(\log_3 q)^2.$$

Although our two methods are very different, neither is applicable to moduli that are the product of the first k primes. It would be interesting if one could sacrifice some of the strength of Theorem 3, or of Pomerance's result, in order to get similar results for such moduli.

The method that we use in all of our proofs derives from an idea of Maier [12]: He saw that certain significant deviations from what is expected in the number of uncancelled integers in the sieve of Eratosthenes-Legendre could be used to show that for any fixed $N > 0$, the estimate

$$\psi(x + \log^N x) - \psi(x) \sim \log^N x$$

cannot hold as $x \to \infty$.

In a second paper we shall extend our results by putting "good" bounds on

$$\sum_{\substack{q \le Q \\ (q, a)=1}} \left|\psi(x; q, a) - \frac{x}{\phi(q)}\right|$$

for arbitrarily large values of a and x, where Q is a certain function of x, smaller asymptotically than x divided by any fixed power of $\log x$.

(*Note added* Oct. 1988: In a paper [21] to appear, A. Hildebrand and H. Maier have made interesting progress on the corresponding problem of primes in short intervals. By using their Proposition 2 and very slightly modifying our proofs it is possible to make unconditional those results in this paper that assume the Generalized Riemann Hypothesis.

We have also learned (private communication) that Hildebrand and Maier have been led to the circle of ideas which are exposed in this paper, but had not found time to develop these before receiving our preprint. In view of this and in view of the fact that the ideas in [21] will play a crucial role, it is now intended that the sequel paper referred to in the text will be a four person effort.)

2. Notation and lemmas

The positive constants c and ε may take different values from one line to the next.

The functions $\Psi(x, y)$ and $\Phi(x, y)$ count the number of integers $\leq x$, free of prime factors $> y$, $< y$ respectively. Dickman's function $\rho(u)$ and Buchstab's function $\omega(u)$ are defined to be the continuous solutions of the differential difference equations

$$(2.1)\qquad (u\omega(u))' = \omega(u-1) \qquad (u \geq 2),$$
$$u\rho'(u) = -\rho(u-1) \qquad (u \geq 1)$$

with starting values

$$(2.2)\qquad \omega(u) = 1/u \qquad (1 \leq u \leq 2),$$
$$\rho(u) = 1 \qquad (0 \leq u \leq 1).$$

In 1930 Dickman [8] showed that for any fixed $u > 0$,

$$\Psi(x, y) \sim x\rho(u) \qquad (x = y^u,\ x \to \infty),$$

and, in 1937, Buchstab [5] showed that for any fixed $u > 1$,

$$\Phi(x, y) \sim \frac{x}{\log y}\omega(u) \qquad (x = y^u,\ x \to \infty).$$

In the early 1950's, de Bruijn ([2], [4]) gave more precise estimates for these functions, from which the following are easily deduced:

Lemma 1 (a). *The estimate*

$$(2.3)\qquad \psi(x, y) = x\rho(u)\left\{1 + O\left(\frac{\log(u+1)}{\log y}\right)\right\}$$

holds uniformly for the range

$$x \geq y \geq \exp(\log^{2/3} x) \quad \textit{where } u = \log x / \log y. \tag{2.4}$$

(b) *The estimate*

$$\Phi(x, y) = xV(y)\left\{e^{\gamma}\omega(u) + O\left(\frac{1}{\log y}\right)\right\} + O\left(\frac{y}{\log y}\right) \tag{2.5}$$

holds uniformly for the range

$$x \geq y \geq 2 \quad \textit{where } u = \log x / \log y \tag{2.6}$$

and, henceforth,

$$V(y) = \prod_{p<y}\left(1 - \frac{1}{p}\right).$$

We shall have need of a number of facts about ρ and ω: De Bruijn [3] showed that

$$\rho(u) = \exp(-u(\log u + \log\log u + O(1))), \tag{2.7a}$$

and in [2] that

$$\omega(u) \to e^{-\gamma} \quad \text{as } u \to \infty. \tag{2.7b}$$

We define $W(u) = \omega(u) - e^{-\gamma}$ $(u \geq 1)$, so that $W(u) \to 0$ as $u \to \infty$. More precisely, it follows immediately from (5.13) of Jurkat and Richert [11] that

$$|W(u)| \leq \rho(u-1)/u \quad \text{for all } u \geq 1. \tag{2.8}$$

Define $W^*(u) = \max_{v \geq u}|W(v)|$ and let u^* be the smallest value $\geq u$ at which that maximum is attained. We conjecture that (2.8) is essentially the best possible (i.e. $W^*(u) = \rho(u)^{1+o(1)}$) though this seems to be difficult to prove.[†] Cheer and Goldston [6] have very recently proved that

$$u \leq u^* \leq u + 2 \quad \text{for all } u \geq 1, \tag{2.9}$$

and that in every interval of unit length there are either one or two zeros of $W(u)$, and either one or two extrema. Moreover each extremum is either a maximum with $W(u) > 0$ or a minimum with $W(u) < 0$.

We also have from (2.1), (2.7), (2.8),

$$|W(u)|, |W'(u)| = o(1). \tag{2.10}$$

[†](Note added: This does follow from the work [21] of Hildebrand and Maier.)

We define, for any $\alpha \geq 1$, $M \geq 0$,

$$G_M(\alpha) = \int_0^M \rho(t)|W(\alpha+t)|\,dt$$

and

$$G_M^*(\alpha) = \int_0^M \rho(t)W^*(\alpha+t)\,dt; \tag{2.11}$$

by (2.7), (2.8) these converge as $M \to \infty$.

We note a number of corollaries to Lemma 1 that we shall need:

LEMMA 2 (Van Lint and Richert [18]). *The estimate*

$$\sum_{\substack{n \leq x \\ p|n \Rightarrow p \leq y}} \frac{1}{n} = \log y \int_0^u \rho(t)\,dt + O(1) \tag{2.12}$$

holds uniformly in the range (2.6).

Recall that R is the set of positive integers q containing no prime factor $< \log q$.

LEMMA 3. (a) $$\sum_{\substack{x<q\leq x+t \\ q\in R}} 1 = \frac{e^{-\gamma}t}{\log\log x} + O\left(\frac{x}{(\log\log x)^2}\right) \text{ for } 0 \leq t \leq x.$$

(b) $$\sum_{\substack{x<q<2x \\ q\in R}} \frac{1}{q} = \frac{e^{-\gamma}\log 2}{\log\log x}\left\{1 + O\left(\frac{1}{\log\log x}\right)\right\}.$$

Proof. Lemma 3(a) follows immediately from Lemma 1(b), (2.7), and (2.8) while Lemma 3(b) can be derived from 3(a) by partial summation.

LEMMA 4. *The estimates*

(a) $$\sum_{\substack{1\leq n \leq x \\ p|n \Rightarrow p \leq y}} \frac{1}{n}\left|W\left(N + \frac{\log n}{\log y}\right)\right| = G_u(N)\log y + O(1)$$

and

(b) $$\sum_{\substack{1\leq n \leq x \\ p|n \Rightarrow p \leq y}} \frac{1}{n}W^*\left(N + \frac{\log n}{\log y}\right) = G_u^*(N)\log y + O(1)$$

hold uniformly for $N \geq 1$ *in the range* (2.6).

Proof. The proof of each part of Lemma 4 is straightforward. It requires forming a Riemann-Stieltjes integral of the left hand side of each using the sum in equation (2.12), and bounding the error term (after partial summation) by use of (2.10) and the error term in Lemma 2.

For a given positive integer q define $\Phi_q(x, y)$ to be the number of positive integers $\leq x$ all of whose prime factors which are $< y$ also divide q. Let $V_q(y) = \prod_{\substack{p<y \\ p\nmid q}}(1 - 1/p)$. We shall prove an estimate similar to Lemma 1(b):

LEMMA 5. *Let $f(x)$ be a positive-valued function tending to 0 as $x \to \infty$. Then the estimate*

$$\Phi_q(x, y) = xV_q(y)\left\{e^{\gamma}\omega(u) + O\left(f(y) + \frac{\log_2 y}{\log y}\right)\right\} \tag{2.13}$$

holds uniformly in the range

$$u, y \geq 2, \qquad x = y^u \tag{2.14}$$

where q is any positive integer which has less than $\exp(f(y)\log y)$ distinct prime factors smaller than y.

Proof. We may assume, without loss of generality, that all the prime factors of q are $< y$ and that $f(y) > 3\log_2 y/\log y$ (if necessary by adding $3\log_2 y/\log y$ to $f(y)$). We shall write $\sum'$ for a sum over integers all of whose prime factors divide q.

Now, using the identity

$$\Phi_q(x, y) = \sum_{x/y \geq n \geq 1}' \Phi(x/n, y)$$

we get, from Lemma 1(b),

$$\begin{aligned}\Phi_q(x, y) &= \sum_{x/y\geq n\geq 1}' xV(y)\frac{1}{n}\left(e^{\gamma}\omega\left(u - \frac{\log n}{\log y}\right) + O\left(\frac{1}{\log y}\right)\right) + O\left(\frac{y}{\log y}\right) \\ &= e^{\gamma}xV(y)(\Sigma_1 + \Sigma_2 - \Sigma_3) + O\left(\frac{y}{\log y}\Sigma_4\right)\end{aligned}$$

where

$$\begin{aligned}\Sigma_1 &= \sum_{n\geq 1}' \frac{1}{n}\left(\omega(u) + O\left(\frac{1}{\log y}\right)\right), \\ \Sigma_2 &= \sum_{x/y\geq n}' \frac{1}{n}\left(\omega\left(u - \frac{\log n}{\log y}\right) - \omega(u)\right), \\ \Sigma_3 &= \sum_{n>x/y}' \frac{1}{n}\omega(u), \quad \text{and} \\ \Sigma_4 &= \sum_{x/y\geq n}' 1.\end{aligned} \tag{2.15}$$

Now $|\omega(u - \log n/\log y) - \omega(u)| \ll \log n/\log y$ by (2.10) and so

$$|\Sigma_2| \ll \frac{1}{\log y} \sum_{n \geq 1}' \frac{\log n}{n} = \frac{1}{\log y} \sum_{p|q} \log p \sum_{j \geq 1} \frac{1}{p^j} \sum_{m \geq 1}' \frac{1}{m}$$

(by taking $n = mp^j$ for each $p^j | n$)

$$(2.16) \qquad = \left(\sum_{m \geq 1}' \frac{1}{m} \right) \left(\frac{1}{\log y} \sum_{p|q} \frac{\log p}{p-1} \right) \ll f(y) \sum_{n \geq 1}' \frac{1}{n}$$

by the prime number theorem.

We shall use Rankin's upper bound moment method [16] to complete the proof. Let $\sigma = 1 + \log f(y)/f(y)\log y$. As $f(y) > 3\log_2 y/\log y$ we see that, for y sufficiently large, $1 > \sigma > 2/3$. Let

$$r = y^{\sigma - 1} \prod_{p|q} \frac{1 - p^{-1}}{1 - p^{-\sigma}}.$$

If $p \leq \exp(2/(1-\sigma)) = M$ then $p^{-\sigma} - p^{-1} \ll (1-\sigma)\log p/p$, so that

$$\sum_{\substack{p|q \\ p \leq M}} (p^{-\sigma} - p^{-1}) \ll (1 - \sigma) \sum_{p \leq M} \frac{\log p}{p} \ll 1.$$

Also, by partial summation (after some work),

$$\sum_{\substack{p|q \\ p > M}} p^{-\sigma} \ll 1/f(y).$$

Thus

$$(2.17) \qquad r \leq \exp\left\{ -(1-\sigma)\log y + O\left(\frac{1}{f(y)} \right) \right\}$$

$$= \exp\left\{ \frac{\log f(y)}{f(y)} (1 + o(1)) \right\} \ll f(y).$$

Therefore by (2.10), since $x/y \geq y$ we have,

$$(2.18) \qquad |\Sigma_3| \ll \sum_{n \geq 1}' \frac{1}{n} \left(\frac{n}{x/y} \right)^{1-\sigma} = (x/y)^{\sigma - 1} \prod_{p|q} (1 - p^{-\sigma})^{-1}$$

$$\ll \frac{V_q(y)}{V(y)} r \ll \frac{V_q(y)}{V(y)} f(y)$$

by (2.17), and

$$(2.19) \qquad |\Sigma_4| \ll \sum_{n\geq 1}{}' \left(\frac{x/y}{n}\right)^{\sigma} = (x/y)^{\sigma}\prod_{p|q}(1-p^{-\sigma})^{-1}$$

$$\ll \frac{x}{y}\frac{V_q(y)}{V(y)} r \ll xV_q(y)f(y)/(y/\log y)$$

again by (2.17).

Adding (2.15), (2.16), (2.18), and (2.19) we complete the proof.

An elementary argument gives:

Lemma 6. *For any fixed $n \geq 0$, we have the estimate*

$$\sum_{\substack{r\leq x\\(r,q)=1}} r^n = \frac{\phi(q)}{q}\frac{x^{n+1}}{n+1} + O(2^{v(q)}x^n),$$

where $v(q)$ is the number of distinct prime factors of q.

Lemma 7. *For any co-prime positive integers m and n,*

$$\max_{(a,mn)=1}\left|\psi(x;mn,a) - \frac{x}{\phi(mn)}\right| \geq \frac{1}{\phi(n)}\max_{(b,m)=1}\left|\psi(x;m,b) - \frac{x}{\phi(m)}\right| - \frac{(\log n + v(n)\log x)}{\phi(n)}.$$

Proof. If $(b,m)=1$ then

$$\sum_{\substack{a\equiv b(\bmod m)\\(a,n)=1\\1\leq a\leq mn}} \psi(x;mn,a) = \psi(x;m,b) - \sum_{\substack{t\equiv b(\bmod m)\\(t,n)>1\\t\leq x}} \Lambda(t).$$

Therefore

$$\max_{(a,mn)=1}\left|\psi(x;mn,a) - \frac{x}{\phi(mn)}\right| \geq \frac{1}{\phi(n)}\sum_{\substack{a\equiv b(\bmod m)\\(a,n)=1\\1\leq a\leq mn}}\left|\psi(x;mn,a) - \frac{x}{\phi(mn)}\right|$$

$$\geq \frac{1}{\phi(n)}\left|\psi(x;m,b) - \frac{x}{\phi(m)}\right| - \frac{1}{\phi(n)}\sum_{(t,n)>1}\Lambda(t).$$

But $\sum_{(t,n)>1}\Lambda(t) \leq \sum_{p|n}\log p([\log x/\log p]+1) \leq \log n + v(n)\log x$, and we have proved the result.

An easy corollary of Lemmas 1 and 2 of [12] (which however are in turn based on deep ideas of Linnik and Gallagher) is:

LEMMA 8. *There exists a constant $c > 0$ such that there are arbitrarily large values of z for which*

$$\psi(x+h; P(z), a) - \psi(x; P(z), a) = \frac{h}{\phi(P(z))}\left\{1 + O\left(\frac{1}{z}\right)\right\}$$

in the range

$$(a, P(z)) = 1, \ \ x \geq P(z)^D \ \ \text{and} \ \ x \geq h \geq x/2,$$

where

$$z \geq D \geq c \log z, \tag{2.20}$$

and henceforth

$$P(z) = \prod_{p<z} p.$$

3. The Maier matrix method

We shall suppose that z is a value given by Lemma 8, and that D lies in the range (2.20). Choose $q \in R$ in the range

$$e^z < q \ll P(z)^D / z \log z, \tag{3.1}$$

note that $(q, P(z)) = 1$, and define $N_q = \log(P^D/q)/\log z$. Let $M(= M(z, D, q))$ be the "Maier matrix" with $(r, s)^{\text{th}}$ entry

$$\Lambda(rP + qs)$$

(where $P = P(z) = \prod_{p<z} p$) for r and s in the range

$$P^{D-1} < r \leq 2P^{D-1} \tag{3.2}$$
$$1 \leq s \leq P^D/q.$$

The sum of elements of the s^{th} column of M is

$$\psi(2P^D + qs; P, qs) - \psi(P^D + qs; P, qs)$$

which equals $O(Dz)$ if $(s, P) > 1$ and equals $P^{D-1}/V(z)\{1 + O(1/z)\}$ if $(s, P) = 1$ by Lemma 8. As there are $\Phi(P^D/q, z)$ columns s with $(s, P) = 1$, we get, from Lemma 1(b), that the sum of the entries of M is

$$P^{D-1}\frac{P^D}{q}\left\{e^\gamma \omega(N_q) + O\left(\frac{1}{\log z}\right)\right\}. \tag{3.3}$$

Now, the sum of the entries in the r^{th} row of M is

$$\psi(P^D + rP; q, rP) - \psi(rP; q, rP).$$

Set $a_r = rP$ and $x_r = P^D + a_r$ and note that $3P^D \ge x_r > a_r \ge P^D$ in the range (3.2). We consider the sum

$$\Sigma_q = \sum_{\substack{P^{D-1} < r \le 2P^{D-1} \\ (r,q)=1}} \left\{ \left| \psi(x_r; q, a_r) - \frac{x_r}{\phi(q)} \right| + \left| \psi(a_r; q, a_r) - \frac{a_r}{\phi(q)} \right| \right\}.$$

Now $v(q) = O(\log P^D / \log_2 P^D)$ in the range (3.1), and so

$$\text{(3.4)} \qquad \frac{P^D}{\phi(q)} 2^{v(q)} = O\left(\frac{P^D}{q} e^{v(q)} \right) = o\left(\frac{P^D}{q} \frac{P^{D-1}}{\log z} \right).$$

Thus, by Lemma 6, together with (3.4), we have

$$\text{(3.5a)} \qquad \sum_{\substack{P^{D-1} < r \le 2P^{D-1} \\ (r,q)=1}} \frac{x_r - a_r}{\phi(q)} = \frac{P^D}{q} P^{D-1} \left\{ 1 + O\left(\frac{1}{\log z} \right) \right\}$$

and

$$\text{(3.5b)} \qquad \sum_{P^{D-1} < r \le 2P^{D-1}} \frac{x_r + a_r}{\phi(q)} = 4 \frac{P^D}{q} P^{D-1} \left\{ 1 + O\left(\frac{1}{\log z} \right) \right\}$$

as $q/\phi(q) = 1 + O(1/\log_2 q)$ for any $q \in \mathbf{R}$.

The number of pairs (r, s) for which $rP + qs$ takes a prescribed value is $\ll 1 + P^{D-1}/q$, and hence the sum of elements of M from those rows r for which $(r, q) > 1$ is

$$\ll \sum_{p \mid q} \log p \sum_{\substack{n = p^a \\ n \le 3P^D}} (1 + P^{D-1}/q) \ll D^2 z^2 (1 + P^{D-1}/q).$$

With this preparation we see that

$$\text{(3.6a)} \qquad \Sigma_q \ge \left| \text{sum of the elements of } M - \sum_{\substack{P^{D-1} < r \le 2P^{D-1} \\ (r,q)=1}} \frac{x_r - a_r}{\phi(q)} \right.$$

$$\left. - O\left(D^2 z^2 (1 + P^{D-1}/q) \right) \right|$$

$$\ge P^{D-1} \frac{P^D}{q} \left\{ e^\gamma |W(N_q)| + O\left(\frac{1}{\log z} \right) \right\}$$

by (3.3) and (3.5a),

$$\geq \left\{ \frac{e^{\gamma}|W(N_q)|}{4} + O\left(\frac{1}{\log z}\right) \right\} \sum_{P^{D-1} < r \leq 2P^{D-1}} \frac{x_r + a_r}{\phi(q)} \tag{3.6b}$$

by (3.5b).

Proof of Proposition 1. In Section 2 we noted that the function $W(u)$ has at most two zeros in any interval of unit length; consequently there is a subinterval $I = [A - \frac{1}{56}, A + \frac{15}{56}]$ of $[B + \frac{1}{8}, B + 1]$ which contains no zeros of $W(u)$. Therefore $|W(u)| \geq c_B$, for some fixed $c_B > 0$, for all u in this interval.

Now let $\lambda = A/B - 1$, so that $0 < \lambda < 1$ and we can take $D = z^{\lambda}$ above. Choose Q so that $Q \log^B Q = P^D$ and so, by the prime number theorem,

$$\log \log Q = (1 + \lambda) \log z + o(1).$$

Therefore, in the range (1.10), we find that,

$$A + o\left(\frac{1}{\log z}\right) < N_q < A + \frac{1}{4} + o\left(\frac{1}{\log z}\right)$$

and so, for z sufficiently large, $N_q \in I$. Thus, for each such q,

$$|W(N_q)| \geq c_B. \tag{3.7}$$

Let us suppose that Proposition 1 is incorrect so that for all a and x in the range (1.11) we have

$$\sum_{\substack{q \in S \\ (a,q)=1}} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \leq \frac{e^{\gamma}}{5} c_B \sum_{q \in S} \frac{x}{\phi(q)}. \tag{3.8}$$

Then we have that

$$\sum_{q \in S} \Sigma_q \leq \frac{e^{\gamma}}{5} c_B \sum_{q \in S} \sum_{P^{D-1} < r \leq 2P^{D-1}} \frac{x_r + a_r}{\phi(q)}. \tag{3.9}$$

On the other hand, by (3.6b) and (3.7) we have

$$\sum_{q \in S} \Sigma_q \geq \left\{ \frac{e^{\gamma}}{4} c_B + O\left(\frac{1}{\log z}\right) \right\} \sum_{q \in S} \sum_{P^{D-1} < r \leq 2P^{D-1}} \frac{x_r + a_r}{\phi(q)}$$

which contradicts (3.9) for sufficiently large z.

Remark. If Lemma 8 were true for all sufficiently large z (as for example would be the case if one assumes the Generalized Riemann Hypothesis) then the proposition would hold for all sufficiently large Q. For, given such Q and B, we choose z and D to satisfy $Q \log^B Q = \exp(z^{1+\lambda}) = P^D$ and the above argument carries through.

Proof of Theorem 1. We take S to be the set

(i) $\{q \in R: 3Q/4 < q < 4Q/5\}$, (ii) $\{q \in R: Q/\log^{1/8} Q < q < 4Q/5\}$

in Proposition 1. Now, by (1.11), $4Q/5 < 4x/5\log^B Q < x/\log^B x$ for x sufficiently large, and $3Q/4 > x/4\log^B Q > x/4\log^B x$. Therefore, in (i), if $q \in S$ then $T < q < 4T$, and, in (ii), if $q \in S$ then $q \leq x/\log^B x$. Also

$$\text{(i)} \qquad \sum_{q \in S} \frac{x}{\phi(q)} \geq \frac{x}{Q} \sum_{\substack{3Q/4 < q < 4Q/5 \\ q \in R}} 1 \gg x/\log\log x \quad \text{by Lemma 3(a),}$$

which completes the proof, by (1.12).

$$\text{(ii)} \quad \sum_{q \in S} \frac{x}{\phi(q)} \gg x \sum_{i=2}^{\lfloor \frac{1}{16}\log\log Q \rfloor} \sum_{\substack{x_i < q < 2x_i \\ q \in R}} \frac{1}{q} \quad \text{where } x_i = 2^{-i}Q,$$

$$\gg x \quad \text{by Lemma 3(b), which completes the proof, by (1.12).}$$

4. The proof of Theorem 2

We again use the Maier matrix method. Choose z as in Lemma 8, and $D = c \log z$ (as in (2.20)). Set $y = P(z)^D$. For a given value of q let q_1 and q_2 be the largest integers dividing q such that q_1 has all its prime factors $\leq z$ and $q_2 \in R$. By Lemma 7, if $q = q_1 q_2$ then

$$(4.1) \qquad \max_{(a,q)=1} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right|$$
$$\geq \frac{1}{\phi(q_1)} \max_{(a,q)=1} \left| \psi(x; q_2, a) - \frac{x}{\phi(q_2)} \right| + O(\log x).$$

Then, for any u,

$$(4.2) \qquad S_x = \sum_{Q<q<2Q} \max_{(a,q)=1} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right|$$
$$\geq \sum_{\substack{n \leq z^u \\ p|n \Rightarrow p \leq z}} \frac{1}{\phi(n)} \sum_{\substack{\frac{Q}{n} < q_2 < \frac{2Q}{n} \\ q_2 \in R}} \max_{(a,q_2)=1} \left| \psi(x; q_2, a) - \frac{x}{\phi(q_2)} \right|$$
$$+ O(Q \log x).$$

(Note: Here we take $q = q_1 q_2$ with $n = q_1$; by (1.16) and (1.17) we have

$(q_1, q_2) = 1.)$

$$\geq \sum_{\substack{n \leq z^u \\ p|n \Rightarrow p \leq z}} \frac{1}{n} \sum_{\substack{\frac{Q}{n} < q < \frac{2Q}{n} \\ q \in R \\ (b,q)=1}} \left| \psi(x; q, b) - \frac{x}{\phi(q)} \right| + o(x)$$

for any fixed $b = b(x)$.
Therefore, with the notation of Section 3,

$$\max_{y<x<3y} S_x \geq \frac{1}{2P^{D-1}} \sum_{P^{D-1}<r\leq 2P^{D-1}} (S_{x_r} + S_{a_r}) \tag{4.3}$$

$$\geq \sum_{\substack{n \leq z^u \\ p|n \Rightarrow p \leq z}} \frac{1}{n} \sum_{\substack{\frac{Q}{n} < q < \frac{2Q}{n} \\ q \in R}} \frac{\Sigma_q}{2P^{D-1}} + o(y)$$

by taking $b(x_r) = b(a_r) = a_r$ in (4.2),

$$\geq \frac{y}{2} \sum_{\substack{n \leq z^u \\ p|n \Rightarrow p \leq z}} \frac{1}{n} \sum_{\substack{\frac{Q}{n} < q < \frac{2Q}{n} \\ q \in R}} \frac{1}{q} \left\{ e^{\gamma} |W(N_q)| + O\left(\frac{1}{\log z}\right) \right\} + o(y)$$

by (3.6a).

Now, by (2.10), $|W'|$ is bounded and so, for $Q/n < q < 2Q/n$ we have

$$\left| W(N_q) - W(N_{Q/n}) \right| \ll |N_q - N_{Q/n}| \ll \frac{1}{\log z}. \tag{4.4}$$

Hence, by (4.3), (4.4) and Lemma 3(b) we get,

$$\max_{y<x<3y} S_x \tag{4.5}$$

$$\geq \frac{y}{2} \frac{\log 2}{\log\log y} \sum_{\substack{n \leq z^u \\ p|n \Rightarrow p \leq z}} \frac{1}{n} \left\{ \left| W\left(N_Q + \frac{\log n}{\log z} \right) \right| + O\left(\frac{1}{\log z}\right) \right\} + o(y)$$

$$\geq \frac{\log 2}{2} \frac{y}{\log\log y} \left\{ G_u(N_Q) \log z + O(1) \right\} + o(y)$$

by Lemma 4(a) and Lemma 2. Finally as $y \geq x/3$, $x \geq y \geq e^z$, the result follows.

Remark. If we assume GRH then we may take different values of D and z (with $P(z)^D$ fixed) in the above, so that, in (4.3), we can replace $|W(N_q)|$ by $W^*(N_q)$, (i.e. by suitable choices of D and z we can replace N_q by N_q^*). Thus, in (4.5), we can replace $G_u(N_Q)$ by $G_u^*(N_Q)$.

5. Moduli q with small prime factors

Proof of Theorem 3. We shall take ε, N, y and $q \notin Q_g$ as given by the hypothesis. Pick $M \geq 2\max\{1, N/\varepsilon\}$ so that $|W(M)|$ is maximized and let $z = (y/2q)^{1/M}$. Let Δ be any fixed number satisfying

(5.1) $$0 < \Delta < \tfrac{1}{6}e^{\gamma}|W(M)|.$$

We shall assume that for at most $q/\exp((\log q)^{\varepsilon})$ distinct values of $a \pmod q$ there exists some value of $x(= x(a))$ in $[y, 2y]$ for which

(5.2) $$\left|\psi(x; q, a) - \frac{x}{\phi(q)}\right| > \Delta\frac{x}{\phi(q)},$$

and then establish a contradiction.

Let $P = P_q(z) = \prod_{\substack{p<z \\ p\nmid q}} p$ so that $(q, P) = 1$. Note that as $\log q < y/q < \log^N q$ by hypothesis, thus

(5.3a) $$\log^{1/M} q < 2^{1/M} z < \log^{N/M} q$$

and so

(5.3b) $$\log^{1/M} y \ll z \ll \log^{N/M} y \leq \log^{\varepsilon/2} y.$$

As $v(q) \leq \exp(g(q)\log_2 q)$, we see that $\prod_{\substack{p<z \\ p|q}} p \leq z^{v(q)} \leq e^{o(z)}$, by (5.3a).

Therefore, by the prime number theorem,

(5.4) $$\log P = z + o(z).$$

Finally let $D = \log y/\log P$.

After this preparation we may set up our Maier matrix in a similar way to that used in the proof of Theorem 1: The $(r, s)^{\text{th}}$ element of M $(= M(\varepsilon, N, y, q))$ is $\Lambda(rP + qs)$ where r and s go over the ranges

(5.5) $$P^{D-1} < r \leq 3P^{D-1}/2,$$
$$1 \leq s \leq P^D/2q.$$

The sum of the elements in the s^{th} column is

$$\psi\left(\tfrac{3}{2}P^D + qs; P, qs\right) - \psi\left(P^D + qs; P, qs\right)$$

which equals $O(Dz)$ if $(s, P) > 1$, and equals

$$P^{D-1}/2V_q(z) + O\left(P^{D/2}\log^2(P^D)\right)$$

if $(s, P) = 1$, by (1.3).

Now the number of s for which $(s, P) = 1$ is $\Phi_q(P^D/2q, z) = \Phi_q(z^M, z)$, and so, by Lemma 5, the sum of the elements in M is

$$\frac{P^{D-1}}{2} \cdot \frac{P^D}{2q}\{e^\gamma \omega(M) + o(1)\}. \tag{5.6}$$

Now, the sum of the elements in row r is

$$\psi\left(\frac{P^D}{2} + rP; q, rP\right) - \psi(rP; q, rP). \tag{5.7}$$

Henceforth let $a_r = rP$ and $x_r = P^D/2 + a_r$, so that, for each r in the range (5.5), we have $y \le a_r < x_r \le 2y$, and the a_r's are distinct (mod q). We shall consider the sum

$$\Sigma = \Sigma^*\left\{\left|\psi(x_r; q, a_r) - \frac{x_r}{\phi(q)}\right| + \left|\psi(a_r; q, a_r) - \frac{a_r}{\phi(q)}\right|\right\}$$

where Σ^* denotes a sum over those values of r in the range (5.5) with $(r, q) = 1$. Arguing as in Section 3, we have

$$\begin{aligned} \Sigma &\ge \left|\text{sum of the elements of } M - \Sigma^* \frac{x_r - a_r}{\phi(q)} \right. \\ &\qquad \left. - O\left(D^2 z^2 (1 + P^{D-1}/q)\right)\right| \\ &\ge \frac{P^{D-1}}{2}\frac{P^D}{2q}\{e^\gamma |W(M)| + o(1)\} \\ &\ge \left\{\frac{1}{6}e^\gamma |W(M)| + o(1)\right\}\Sigma^* \frac{x_r + a_r}{\phi(q)} \end{aligned} \tag{5.8}$$

since, by Lemma 6,

$$\Sigma^* \frac{P^D}{2\phi(q)} = \frac{P^{D-1}}{2}\frac{P^D}{2q} + O\left(\frac{P^D}{\phi(q)}2^{v(q)}\right),$$

and

$$\Sigma^* \frac{P^D + 4rP}{2\phi(q)} = 6\frac{P^{D-1}}{2}\frac{P^D}{2q} + O\left(\frac{P^D}{\phi(q)}2^{v(q)}\right),$$

while $v(q) = z^{o(1)}$ yields

$$\frac{P^D}{\phi(q)}2^{v(q)} = \frac{P^D}{q}\frac{q}{\phi(q)}2^{v(q)} = \frac{P^D}{q}P^{o(1)} \ll \frac{P^D}{q}\frac{P^{D-1}}{\log z}.$$

On the other hand, under our assumption in (5.2),

$$\sum \leq \Delta \sum{}^{*} \frac{x_r + a_r}{\phi(q)} + 2 \sum_{a \in A} \max_{y \leq x \leq 2y} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| \tag{5.9}$$

where A is some set of integers of cardinality $\leq q/\exp((\log q)^{\varepsilon})$.

Now, trivially we have $0 \leq \psi(x; q, a) \leq (x/q + 1)\log x$ and so

$$\begin{aligned} \sum_{a \in A} \max_{y \leq x \leq 2y} \left| \psi(x; q, a) - \frac{x}{\phi(q)} \right| &\ll |A| y q^{-1} \log y \\ &\ll \frac{P^D}{q} P^{D-1} \frac{P \log y}{\exp\left((\log y)^{\varepsilon}\right)}. \end{aligned} \tag{5.10}$$

Now, by (5.3b) and (5.4), we have $\log P \ll z \ll \log^{\varepsilon/2} y$ and so $P \log y = o(\exp((\log y)^{\varepsilon}))$.

Thus, comparing (5.8) and (5.9), using (5.10), we get a contradiction for any fixed Δ in the range (5.1).

UNIVERSITY OF TORONTO, TORONTO, ONTARIO, CANADA

REFERENCES

[1] E. BOMBIERI, On the large sieve, Mathematika **12** (1965), 201–225.
[2] N. G. DE BRUIJN, On the number of uncancelled elements in the sieve of Eratosthenes, Nederl. Akad. Wetensch. Proc. **53** (1950), 803–812.
[3] ______, The asymptotic behaviour of a function occurring in the theory of primes, J. Indian Math. Soc. (N.S.) **15** (1951), 25–32.
[4] ______, On the number of positive integers $\leq x$ and free of prime factors $> y$, Nederl. Akad. Wetensch. Proc. Ser. A., I, **54** (1951), 50–60; II, **69** (1966), 239–247 = Indag. Math. **28** (1966), 239–247.
[5] A. A. BUCHSTAB, Asymptotic estimates of a general number-theoretic function (Russian), Mat. Sb. (N.S.), **2** (44) (1937), 1239–1246.
[6] A. Y. CHEER and D. A. GOLDSTON, A differential delay equation arising from the sieve of Eratosthenes, preprint (1988).
[7] H. DAVENPORT, *Multiplicative Number Theory*, (2nd Edn.), Springer-Verlag, New York, 1980.
[8] K. DICKMAN, On the frequency of numbers containing prime divisors of a certain relative magnitude, Ark. Mat. Astr. Fys., **22** (1930), 1–14.
[9] P. D. T. A. ELLIOTT and H. HALBERSTAM, A conjecture in prime number theory, Symp. Math. IV (Rome 1968/69), 59–72.
[10] H. HALBERSTAM and H.-E. RICHERT, *Sieve Methods*, Academic Press, London, 1974.
[11] W. B. JURKAT and H.-E. RICHERT, An improvement of Selberg's sieve method I, Acta Arith. **11** (1965) 217–240.
[12] H. MAIER, Primes in short intervals, Michigan Math. J. **32** (1985), 221–225.
[13] H. L. MONTGOMERY, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. **227**, Springer, New York (1971).
[14] ______, Problems concerning prime numbers, Proc. Symp. Pure Math. **28** (1976), 307–310.

[15] C. Pomerance, A note on the least prime in an arithmetic progression, J. Number Theory, **12** (1980), 218–223.
[16] R. A. Rankin, The difference between consecutive prime numbers, J. London Math. Soc. **13** (1938), 242–247.
[17] C. L. Siegel, Uber die Classenzahl quadratischer korper, Acta Arith. **1** (1935), 83–86.
[18] J. H. Van Lint and H.-E. Richert, Uber die Summe $\sum_{\substack{n \le x \\ p(n) < y}} \frac{\mu^2(n)}{\phi(n)}$, Nederl. Akad. Wetensch. Proc. Ser. A67 = Indag. Math. **26** (1964), 582–587.
[19] A. I. Vinogradov, The density conjecture for Dirichlet *L*-series, Izv. Akad. Nauk. SSSR Ser. Mat. **29** (1965), 903–934.
[20] A. Walfisz, Zur additiven Zahlentheorie II, Math. Zeit. **40** (1936), 592–607.
[21] A. Hildebrand and H. Maier, Irregularities in the distribution of primes in short intervals (to appear).

(Received September 6, 1988)