

MATHEMATIKA

A JOURNAL OF PURE AND APPLIED MATHEMATICS

VOL. 20. PART 2.

DECEMBER, 1973.

No. 40.

THE LARGE SIEVE

H. L. MONTGOMERY AND R. C. VAUGHAN

1. *Statement of results.* Let $S(x)$ be a trigonometric polynomial,

$$S(x) = \sum_{M+1}^{M+N} a_n e(nx), \quad (1.1)$$

where $N > 0$ and M are integers, the a_n are arbitrary complex numbers, and $e(x) = e^{2\pi i x}$. In its basic form, the large sieve of Linnik and Rényi is an inequality of the form

$$\sum_{r=1}^R |S(x_r)|^2 \leq \Delta(N, \delta) \sum_{M+1}^{M+N} |a_n|^2. \quad (1.2)$$

Here the x_r are arbitrary real numbers which are distinct modulo 1, and δ is a measure of their spacing,

$$\delta = \min_{r \neq s} \|x_r - x_s\|, \quad (1.3)$$

where the minimum is taken over all possible pairs r, s with $r \neq s$, and $\|x\|$ denotes the distance from x to the nearest integer. The factor $\Delta(N, \delta)$ must depend on both N and δ . In fact $\Delta(N, \delta) \geq N$, for if $a_n = 1$ for all n and $x_1 = 1$, then the sum on the left is $\geq N^2$, while the sum on the right is equal to N . On the other hand,

$$\int_0^1 \sum_{r=1}^R |S(x_r + x)|^2 dx = R \sum_{M+1}^{M+N} |a_n|^2.$$

If it happens that the x_r are equally spaced then $\delta = R^{-1}$, so we deduce that $\Delta(N, \delta) \geq \delta^{-1}$.

THEOREM 1. Let $S(x)$ and δ be as in (1.1) and (1.3), respectively. Then

$$\sum_{r=1}^R |S(x_r)|^2 \leq (N + \delta^{-1}) \sum_{M+1}^{M+N} |a_n|^2. \quad (1.4)$$

Moreover, if

$$\delta_r = \min_{s \neq r} \|x_r - x_s\| \quad (1.5)$$

for all r , then

$$\sum_{r=1}^R (N + \tfrac{1}{2}\delta_r^{-1})^{-1} |S(x_r)|^2 \leq \sum_{n=1}^{M+N} |a_n|^2. \quad (1.6)$$

The inequality (1.4) contains several previous formulations of the large sieve. In particular, Gallagher [6], Bombieri and Davenport [2] (see also Ming-Chit [17]) and Bombieri [1] showed that $\pi N + \delta^{-1}$, $2 \max(N, \delta^{-1})$, and $N + 2\delta^{-1}$, respectively, are permissible expressions for $\Delta(N, \delta)$. Moreover, Bombieri and Davenport [3] have given examples in which $\Delta(N, \delta) = N + \delta^{-1} - 1$, so that (1.4) is extremely sharp.

The weighted sieve (1.6) is fundamentally more delicate than (1.4). The weights are particularly useful in arithmetic applications, because the Farey fractions are irregularly spaced.

COROLLARY 1. *Let $\mathcal{N}$ be a set of $\mathbb{Z}$ integers in an interval $[M + 1, M + N]$. For each prime p let $\omega(p)$ denote the number of residue classes modulo p which contain no element of $\mathcal{N}$. Then*

$$Z \leq L^{-1}, \quad (1.7)$$

where

$$L = \sum_{q \leq z} (N + \tfrac{1}{2}qz)^{-1} \mu(q)^2 \prod_{p|q} \frac{\omega(p)}{p - \omega(p)} \quad (1.8)$$

and z is an arbitrary positive number.

This sharpens Corollary 4.3 of Montgomery [19], which was derived in an awkward manner. The advantage of Corollary 1 over earlier results is that the error term occurs as the term $\tfrac{1}{2}qz$, instead of cz^2 . This leads to significant improvements when the $\omega(p)$ are small.

As an illustration of Corollary 1, we consider the Brun–Titchmarsh upper bound for the number of primes in a segment of an arithmetic progression. Let $\pi(x, k, l)$ be the number of primes $p \leq x$ with $p \equiv l \pmod{k}$. Then Klimov [11] has shown that Selberg's method gives

$$\pi(M + N, k, l) - \pi(M, k, l) \leq \frac{2N}{\phi(k) \log(N/k)} \left(1 + O\left(\frac{\log \log(N/k)}{\log(N/k)} \right) \right) \quad (1.9)$$

for $k \leq \tfrac{1}{3}N$. Bombieri and Davenport [2], using the large sieve, obtained a second proof of this. Subsequently van Lint and Richert [13] (see also Uchiyama [26]), by more precisely estimating the error terms in Selberg's method, were able to replace the $\log \log(N/k)$ in (1.9) by unity. (Selberg [24], [25] had much earlier stated such a result, without detailed proof.) Bombieri [1] gave a new proof of this sharper result, using a complicated weighted large sieve. In particular he showed that

$$\pi(M + N) - \pi(M) \leq 2N/(\log N - 3).$$

Corollary 1 enables us to obtain the following improved estimates which have no error terms.

THEOREM 2. *Let x and y be positive real numbers, and let k and l be relatively prime positive integers. Then*

$$\pi(x + y, k, l) - \pi(x, k, l) < \frac{2y}{\phi(k) \log(y/k)} \quad (1.10)$$

provided only that $y > k$. Moreover, there is a constant c such that if $y > ck$, then

$$\pi(x + y, k, l) - \pi(x, k, l) < \frac{2y}{\phi(k)(\frac{x}{k} + \log(y/k))}. \quad (1.11)$$

As a particular case of the above we note that if $M > 0$ and $N > 1$, then

$$\pi(M + N) - \pi(M) \leq 2N/\log N. \quad (1.12)$$

From this we shall deduce

COROLLARY 2. *If $M > 0$ and $N > 1$ are integers, then*

$$\pi(M + N) - \pi(M) \leq 2\pi(N). \quad (1.13)$$

There is a long standing conjecture that

$$\pi(M + N) \leq \pi(M) + \pi(N)$$

for $M > 1$, $N > 1$. However, Hensley and Richards [10] have cast doubt on this by showing that it is not consistent with the well known conjecture concerning the existence of prime k -tuples. It may be that (1.12) is essentially best possible.

Bombieri and Davenport [2] used the large sieve to show that if a given L -function $L(s, \chi_1)$ has a "Siegel zero", then the numbers

$$\psi(N, \chi) = \sum_{n \leq N} \Lambda(n) \chi(n), \quad (1.14)$$

with $\chi \neq \chi_0$, are not usually very large. However, their result does not conflict with our expectation that $\psi(N, \chi)$ is of order $(N \log q)^{\frac{1}{2}}$ on average. We use the sharper bound (1.6) to prove the following theorem. As a consequence, we show below that if there is a "Siegel zero", then $\psi(N, \chi)$ is $o((N \log q)^{\frac{1}{2}})$ on average.

THEOREM 3. *If $\psi(N, \chi)$ is given by (1.14) and $W = \frac{1}{200} N^{\frac{1}{2}}$, then for every sufficiently large N*

$$\sum_{q \leq W} \left(\log \frac{N^{\frac{1}{2}}}{q} \right) \sum_{\chi}^* |\psi(N, \chi)|^2 < N^2 \log N. \quad (1.15)$$

Here $\sum_{\chi}^*$ denotes a sum over all primitive characters χ modulo q .

The term $q = 1$ consisting solely of the principal character contributes $\frac{1}{2} N^2 \log N + o(N^2)$ to the left hand side of (1.15). Furthermore, if $L(s, \chi_1)$ has a "Siegel zero", where χ_1 is a primitive character modulo q , and $q_1 = N^{\delta}$, then $|\psi(N, \chi_1)| > (1 - \delta)N$. Hence χ_1 contributes at least $(\frac{1}{2} - 2\delta)N^2 \log N$. As a consequence one would have

$$\sum_{N^{\delta} < q \leq W} \sum_{\chi}^* |\psi(N, \chi)|^2 \ll \delta N^2 \log N. \quad (1.16)$$

It is plausible that this is false if δ is sufficiently small.

We prove Theorem 1 and Corollary 1 in the next section. In §§3–6 we prove Theorem 2. The proof is subdivided as follows. We first of all establish (1.11). Then we collect some elementary estimates which enable us to demonstrate (1.10) when y/k is sufficiently large. Finally we show that (1.10) follows from the sieve of Eratosthenes when y/k is small. We derive Corollary 2 in §7, and in §8 we prove Theorem 3.

2. Proofs of Theorem 1 and Corollary 1. Theorem 1 follows easily from the lemmas below. Of these, Lemma 1 is a standard result (see Hellinger and Toeplitz [9], or Hardy, Littlewood, and Pólya [8], Theorem 288). Lemma 2 is a recent discovery; it is Theorem 1 of Montgomery and Vaughan [20].

LEMMA 1. Suppose that $[c_{rn}]$ is an arbitrary $R \times N$ matrix and A is such that

$$\sum_{n=1}^N \left| \sum_{r=1}^R c_{rn} v_r \right|^2 \leq A \sum_{r=1}^R |v_r|^2$$

for all sets of complex numbers v_r . Then

$$\sum_{r=1}^R \left| \sum_{n=1}^N c_{rn} w_n \right|^2 \leq A \sum_{n=1}^N |w_n|^2$$

for all sets of complex numbers w_n .

We note that the above is self-dual, so that in fact the two inequalities are equivalent.

LEMMA 2. Suppose that the premises of Theorem 1 hold, and that the numbers u_r are arbitrary. Then

$$\left| \sum_{r=1}^R \sum_{\substack{s=1 \\ r \neq s}}^R u_r \bar{u}_s \csc \pi(x_r - x_s) \right| \leq \delta^{-1} \sum_{r=1}^R |u_r|^2, \quad (2.1)$$

and

$$\left| \sum_{r=1}^R \sum_{\substack{s=1 \\ r \neq s}}^R u_r \bar{u}_s \csc \pi(x_r - x_s) \right| \leq \frac{3}{2} \sum_{r=1}^R |u_r|^2 \delta_r^{-1}. \quad (2.2)$$

Here $\csc x = (\sin x)^{-1}$.

To prove (1.4) we appeal to Lemma 1 with $c_{rn} = e((M+n)x_r)$. It thus suffices to show that

$$\sum_{n=M+1}^{M+N} \left| \sum_{r=1}^R v_r e(nx_r) \right|^2 \leq (N + \delta^{-1}) \sum_{r=1}^R |v_r|^2. \quad (2.3)$$

Similarly, if we take $c_{rn} = (N + \frac{3}{2}\delta_r^{-1})^{-\frac{1}{2}} e((M+n)x_r)$, then (1.6) is a consequence

of the inequality

$$\sum_{n=M+1}^{M+N} \left| \sum_{r=1}^R v_r e(nx_r) \right|^2 \leq \sum_{r=1}^R |v_r|^2 (N + \tfrac{3}{2} \delta_r^{-1}). \quad (2.4)$$

This approach to the large sieve has been discussed recently by Elliott [5], Matthews [14], [15], [16], and by Kobayashi [12].

To prove (2.3) we square out the left hand side. The diagonal terms contribute the amount

$$N \sum_{r=1}^R |v_r|^2.$$

The non-diagonal terms may be written

$$\sum_{r=1}^R \sum_{\substack{s=1 \\ r \neq s}}^R v_r \bar{v}_s \sum_{n=M+1}^{M+N} e(n(x_r - x_s)), \quad (2.5)$$

and the inner sum is

$$\tfrac{1}{2} i \left(e((M + \tfrac{1}{2})(x_r - x_s)) - e((M + N + \tfrac{1}{2})(x_r - x_s)) \right) \csc \pi(x_r - x_s).$$

We now use (2.1) twice, once with $u_r = v_r e((M + \tfrac{1}{2})x_r)$, and once with

$$u_r = v_r e((M + N + \tfrac{1}{2})x_r).$$

This gives (2.3). The proof of (2.4) is the same, except that we use (2.2) in place of (2.1).

To prove Corollary 1 we take our x_r to be the numbers a/q , where $1 \leq a \leq q$, $(a, q) = 1$, and $q \leq z$. If $a'/q' \neq a/q$, then

$$\left\| \frac{a}{q} - \frac{a'}{q'} \right\| \geq \frac{1}{qq'} \geq \frac{1}{qz}.$$

Hence, by (1.6),

$$\sum_{q \leq z} (N + \tfrac{3}{2} qz)^{-1} \sum_{a=1}^q{}' |S(a/q)|^2 \leq \sum_{n=M+1}^{M+N} |a_n|^2. \quad (2.6)$$

We use $\sum'$ to denote a sum in which the variable of summation is restricted to those values which are coprime to q . Now let a_n be 1 or 0 according as n is or is not a member of $\mathcal{N}$. Then, on the hypothesis of Corollary 1, we have (Montgomery [18])

$$Z^2 \mu(q)^2 \prod_{p|q} \frac{\omega(p)}{p - \omega(p)} \leq \sum_{a=1}^q{}' |S(a/q)|^2. \quad (2.7)$$

We now combine (2.6) and (2.7), and note that the right hand side of (2.6) is Z . This proves (1.7).

3. Proof of (1.11). We require the following lemma.

LEMMA 3. *Let u and v be any positive real numbers. Then*

$$\sum_{\substack{q \leq u \\ (q, k)=1}} (1 + vq)^{-1} \frac{\mu(q)^2}{\phi(q)} \geq \frac{\phi(k)}{k} \sum_{q \leq u} (1 + vq)^{-1} \frac{\mu(q)^2}{\phi(q)}.$$

Proof. We multiply the sum on the left by

$$\sum_{r: k} \frac{\mu(r)^2}{\phi(r)} = \frac{k}{\phi(k)}$$

to obtain a sum which clearly includes all the terms in the sum on the right.

To prove (1.11) we take

$$M = \left\lfloor \frac{x - l}{k} \right\rfloor \quad (3.1)$$

and

$$N = \left\lfloor \frac{x + y - l}{k} \right\rfloor - M. \quad (3.2)$$

Let $\mathcal{N}$ be the set of those integers n for which $M < n \leq M + N$, $kn + l$ is prime, and $kn + l > z$. Then $\omega(p) \geq 1$ whenever $p \leq z$ and $p \nmid k$. Thus by Corollary 1,

$$\pi(x + y, k, l) - \pi(x, k, l) \leq L^{-1} + \pi(z) \quad (3.3)$$

where

$$L = \sum_{\substack{q \leq z \\ (q, k)=1}} (N + \tfrac{3}{2}qz)^{-1} \mu(q)^2 / \phi(q). \quad (3.4)$$

We suppose, as we may, that

$$z = (\tfrac{2}{3}N)^{\frac{1}{2}}. \quad (3.5)$$

Then by Lemma 3,

$$\pi(x + y, k, l) - \pi(x, k, l) < \frac{kN}{\phi(k)J} + N^{\frac{1}{2}}, \quad (3.6)$$

where

$$J = \sum_{q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q).$$

Ward ([27], (2.2) with $u = 1$) showed that

$$\sum_{q \leq v} \mu(q)^2 / \phi(q) = \log v + \gamma + \sum_p \frac{\log p}{p(p-1)} + o(1)$$

as $v \rightarrow \infty$. On summing by parts we see that

$$J = \log z + \gamma + \sum_p \frac{\log p}{p(p-1)} - \log 2 + o(1)$$

as $z \rightarrow \infty$, and so by (3.5),

$$J = \tfrac{1}{2} \log N + \gamma + \sum_p \frac{\log p}{p(p-1)} - \tfrac{1}{2} \log \tfrac{3}{2} - \log 2 + o(1)$$

as $N \rightarrow \infty$. Moreover $\gamma > 0.577$,

$$\sum_p \frac{\log p}{p(p-1)} > 0.737$$

(see Rosser and Schoenfeld [21]), $\log 2 < 0.694$, and $\frac{1}{2} \log \frac{3}{2} < 0.203$, so that

$$J > \frac{1}{2} \log N + 0.417$$

for N larger than an effectively computable constant. This with (3.6) completes the proof of (1.11).

Recently A. Selberg (unpublished) succeeded in using elementary techniques to obtain a bound like (1.11), but with $\frac{5}{8}$ replaced by $\frac{4}{5}$.

4. Elementary lemmas. The lemmas below contain little that is new. They are, however, essential to our proof of (1.10).

LEMMA 4. *For every positive real x ,*

$$\sum_{\substack{r \leq x \\ (r, 6) = 1}} \frac{1}{r} = \frac{1}{3} \log x + \frac{1}{3} \gamma + \frac{1}{3} \log 2 + \frac{1}{6} \log 3 - \sum_{t|6} \frac{\mu(t)}{x} \left\{ \frac{x}{t} \right\} + \frac{1}{2} \theta x^{-2},$$

where $\theta = \theta(x)$ satisfies $|\theta| \leq 1$, and $\{y\} = y - [y]$.

Proof. We have

$$\sum_{\substack{r \leq x \\ (r, 6) = 1}} \frac{1}{r} = \sum_{t|6} \frac{\mu(t)}{t} \sum_{n \leq (x/t)} \frac{1}{n}. \quad (4.1)$$

By the Euler-Maclaurin expansion (see, for instance, Theorem 421 of Hardy and Wright [8]),

$$\sum_{n \leq y} \frac{1}{n} = \log y + \gamma - (\{y\} - \frac{1}{2}) y^{-1} + \frac{1}{6} \theta_1 y^{-2}.$$

We take $y = (x/t)$ and insert this in (4.1) to obtain our result.

LEMMA 5. *If z is real and positive, then*

$$\sum_{q \leq z} \mu(q)^2 / \phi(q) \geq \log z + \gamma + \frac{1}{2} \log 2 + \frac{1}{6} \log 3 - A(z, 6) z^{-1} - \frac{16.5}{4} z^{-2},$$

where

$$A(z, k) = \sum_{m|k} \frac{m}{\phi(m)} \sum_{t|k} \mu(t) \left\{ \frac{z}{mt} \right\}. \quad (4.2)$$

Proof. We note that

$$\sum_{q \leq z} \mu(q)^2 / \phi(q) = \sum_{m|6} \sum_{\substack{q \leq z \\ (q, 6) = m}} \mu(q)^2 / \phi(q) = \sum_{m|6} \frac{1}{\phi(m)} \sum_{\substack{r \leq z/m \\ (r, 6) = 1}} \mu(r)^2 / \phi(r).$$

Let $s(n)$ denote the largest squarefree divisor of n , $s(n) = \prod_{p|n} p$. Then

$$\sum_{\substack{r \leq y \\ (r, 6) = 1}} \mu(r)^2 / \phi(r) = \sum_{\substack{r \leq y \\ (r, 6) = 1}} \mu(r)^2 r^{-1} \prod_{p|n} \left(\sum_{h=0}^{\infty} p^{-h} \right) = \sum_{\substack{s(r) \leq y \\ (r, 6) = 1}} 1/r \geq \sum_{\substack{r \leq y \\ (r, 6) = 1}} 1/r.$$

Thus

$$\sum_{q \leq z} \mu(q)^2 / \phi(q) \geq \sum_{m|6} \frac{1}{\phi(m)} \sum_{\substack{r \leq z/m \\ (r, 6) = 1}} \frac{1}{r}.$$

To estimate the inner sum we appeal to Lemma 4 with $x = z/m$. This gives the required lower bound.

LEMMA 6. Let $A(z, k)$ be given by (4.2). Then $A(z, 6) \leq 3$.

Proof. From (4.2) it is clear that $A(z, k)$ is periodic with period k^2 as a function of z , $A(z, k) = A([z], k) + \{z\}$ for squarefree k , and $A(-z, k) = -A(z, k)$ when $k > 1$ and z is not an integer. Also, if $p \nmid l$, then

$$A(z, pl) = A(z, l) + \frac{1}{p-1} A(z/p, l) - \frac{p}{p-1} A(z/p^2, l).$$

From this last identity we deduce that

$$\sup_z |A(z, pl)| \leq \frac{2p}{p-1} \sup_z |A(z, l)|.$$

It is easily seen that $\sup_z |A(z, 2)| = 1$. Hence $\sup_z |A(z, 6)| \leq 3$. In fact $\sup_z A(z, 6) = \frac{5}{2}$, as one will find by direct calculation.

LEMMA 7. Suppose that $z \geq 6$. Then

$$\sum_{q \leq z} \mu(q)^2 / \phi(q) \geq \log z + 1.07. \quad (4.3)$$

Proof. We suppose initially that $z \geq 100$. By Lemma 6 we have $A(z, 6)z^{-1} \leq 0.03$. The lemma then follows from Lemma 5 on noting that $\gamma > 0.577$, $\frac{1}{2} \log 2 > 0.346$, $\frac{1}{6} \log 3 > 0.183$, $\frac{1.65}{4} z^{-2} \leq 0.005$.

To establish the lemma when $6 \leq z < 100$ we make a direct calculation. We first note that the right hand side of (4.3) is increasing when $Q \leq z < Q+1$, Q an

integer. Then, on writing

$$B(Q) = \sum_{q \leq Q} \mu(q)^2 / \phi(q) - \log(Q+1),$$

we see that it suffices to show that $B(Q) > 1.07$ when $6 \leq Q < 100$.

We give below a table of values of $B(Q)$. We, the authors, have independently computed $B(Q)$ for $6 \leq Q \leq 100$, while Professor Weinberger of the University of Michigan has made a corroboratory calculation with the aid of an IBM 3600/67 computer. The numbers displayed below lie between $B(Q) - 10^{-4}$ and $B(Q)$. We note that $B(Q) > B(Q-1) - Q^{-1}$; this together with the values given below make it clear that $B(Q) > 1.07$ whenever $6 \leq Q < 100$.

Q	$B(Q)$	Q	$B(Q)$
5	0.9582	30	1.2985
6	1.3040	35	1.3365
7	1.3372	40	1.3314
8	1.2194	45	1.3485
9	1.1140	50	1.3125
10	1.2687	55	1.2945
12	1.2017	60	1.2897
14	1.3086	65	1.2817
16	1.3084	70	1.3383
18	1.2597	75	1.3262
20	1.2151	80	1.3336
22	1.3075	85	1.3265
24	1.2696	90	1.3230
26	1.2760	95	1.3357
28	1.2045	100	1.2954

LEMMA 8. Suppose that $z \geq 100$. Then

$$\sum_{q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q) > \log z + 0.361.$$

Proof. Let

$$D(u) = \sum_{q \leq u} \mu(q)^2 / \phi(q). \quad (4.4)$$

Then, on integrating by parts, we find that

$$\begin{aligned} \sum_{6 \leq q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q) &= z \int_{6^-}^z (z + u)^{-1} dD(u) \\ &= \frac{1}{2} D(z) - \frac{z D(5)}{z + 6} + z \int_6^z D(u) (z + u)^{-2} du \end{aligned}$$

which, by Lemma 7, is

$$> \frac{1}{2}(\log z + 1.07) - \frac{zD(5)}{z+6} + z \int_6^z (\log u + 1.07)(z+u)^{-2} du.$$

Hence, integrating by parts again, and using (4.4) with $u = 5$, we see that the above is

$$> \sum_{q \leq 5} \frac{\mu(q)^2}{\phi(q)} \left(\frac{z}{z+q} - \frac{z}{z+6} \right) + \frac{z}{z+6} (\log 6 + 1.07) + \int_6^z \frac{z}{z+u} \frac{du}{u}.$$

When $1 \leq q \leq 5$ and $z \geq 100$,

$$\frac{z}{z+q} - \frac{z}{z+6} = \frac{z}{z+q} \left(\frac{6-q}{z+6} \right) > 0.9 \times \frac{6-q}{z+6},$$

so that

$$\sum_{q \leq 5} \frac{\mu(q)^2}{\phi(q)} \left(\frac{z}{z+q} - \frac{z}{z+6} \right) > \frac{9.67}{z+6}.$$

We note also that

$$\int_6^z \frac{z}{z+u} \frac{du}{u} = \log z + \log \left(1 + \frac{6}{z} \right) - \log 12 > \log z + \frac{6}{z+6} - \log 12.$$

On combining the above, we obtain

$$\begin{aligned} \sum_{q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q) &> \log z + 1.07 - \log 2 + \frac{15.67 - 6(\log 6 - 1.07)}{z+6} \\ &> \log z + 0.361, \end{aligned}$$

provided that $z \geq 100$.

LEMMA 9. If $N \geq 15000$ and $z = (\frac{2}{3}N)^{\frac{1}{2}}$, then

$$\pi(z) + N \left(\sum_{q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q) \right)^{-1} < \frac{2N - 2}{\log N}. \quad (4.5)$$

Proof. We have $z \geq 100$, so that by Lemma 8

$$\sum_{q \leq z} (1 + qz^{-1})^{-1} \mu(q)^2 / \phi(q) > \frac{1}{2} \log N - \frac{1}{2} \log \frac{2}{3} + 0.361 > \frac{1}{2} \log N + 0.15.$$

When z is this large, $\pi(z) < \frac{1}{3}z < \frac{1}{3}N^{\frac{1}{2}}$. Hence the left hand side of (4.5) is less than

$$\frac{1}{3}N^{\frac{1}{2}} + 2N(\log N + \frac{3}{10})^{-1} = \frac{1}{3}N^{\frac{1}{2}} + \frac{2N}{\log N} \left(1 - \frac{3}{3 + 10 \log N} \right).$$

Since $\log N > 9.6$,

$$\frac{3}{3 + 10 \log N} > \frac{1}{4 \log N},$$

so that it suffices to show that

$$\frac{1}{3}N^{\frac{1}{2}} < \frac{N}{2(\log N)^2} - \frac{2}{\log N}.$$

As $4 \log N < 3N$ it is enough to show that $(\log N)^2 < N^{\frac{1}{2}}$. If $u \geq 10$, then $\log u < \frac{1}{4}u$. Taking $N = u^4$ gives $(\log N)^2 < N^{\frac{1}{2}}$ when $N \geq 10^4$. This establishes the lemma.

5. *Proof of (1.10) when $y > 16000k$.* To establish (1.10) when y/k is large, we combine (3.3) and (3.4) with Lemma 3. Thus

$$\pi(x+y, k, l) - \pi(x, k, l) < \frac{k}{\phi(k)} \left\{ \pi(z) + N \left(\sum_{q \leq z} \left(1 + \frac{3qz}{2N} \right)^{-1} \frac{\mu(q)^2}{\phi(q)} \right)^{-1} \right\}. \quad (5.1)$$

Also, by (3.1) and (3.2),

$$N = \left[\frac{x+y-l}{k} \right] - \left[\frac{x-l}{k} \right], \quad (5.2)$$

so that $N > 15000$. We now take $z = (\frac{1}{3}N)^{\frac{1}{2}}$, whence (5.1) and Lemma 9 give

$$\pi(x+y, k, l) - \pi(x, k, l) < \frac{2k(N-1)}{\phi(k) \log N}. \quad (5.3)$$

By (5.2) we see that $N-1 \leq y/k \leq N+1$. Thus if $y/k \geq N$, then

$$\frac{N-1}{\log N} < \frac{N}{\log N} \leq \frac{y/k}{\log(y/k)},$$

whilst if $N-1 \leq y/k < N$, then

$$\frac{N-1}{\log N} \leq \frac{y/k}{\log(y/k)}.$$

We combine this with (5.3) to complete the proof.

6. *Proof of (1.10) when $k < y \leq 20000k$.* We begin by establishing the following form of the sieve of Eratosthenes.

LEMMA 10. *On the hypothesis of Theorem 2,*

$$\pi(x+y, k, l) - \pi(x, k, l) \leq \frac{y}{k} \prod_{p|P(z, k)} \left(1 - \frac{1}{p} \right) + 2^{\pi(z)} + \pi(z)$$

where $P(z, k)$ is the product of all those prime numbers which neither exceed z nor divide k .

Proof. It is easily seen that

$$\begin{aligned}\pi(x+y, k, l) - \pi(x, k, l) &\leq \sum_{x < nk + l \leq x+y} \sum_{r | (nk+l, P(z, k))} \mu(r) + \pi(z) \\ &= \sum_{r | P(z, k)} \mu(r) \left(\frac{y}{kr} + \theta \right) + \pi(z),\end{aligned}$$

where $|\theta| \leq 1$. This gives the lemma.

For convenience we write $v = y/k$,

$$E = \pi(x+y, k, l) - \pi(x, k, l)$$

and

$$F = \frac{2y}{\phi(k) \log(y/k)}.$$

By Lemma 10 we have

$$\begin{aligned}E &\leq \frac{y}{k} \prod_{p | P(z, k)} \left(1 - \frac{1}{p} \right) + 2^{\pi(z)} + \pi(z) \\ &\leq \frac{y}{\phi(k)} \prod_{p \leq z} \left(1 - \frac{1}{p} \right) + \frac{y}{k} \cdot \frac{k}{y} (2^{\pi(z)} + \pi(z)) \\ &\leq \frac{y}{\phi(k)} \left(\prod_{p \leq z} \left(1 - \frac{1}{p} \right) + \frac{1}{v} (2^{\pi(z)} + \pi(z)) \right) \\ &= \frac{1}{2} F(\log v) \left(\prod_{p \leq z} \left(1 - \frac{1}{p} \right) + \frac{1}{v} (2^{\pi(z)} + \pi(z)) \right).\end{aligned}$$

On taking $z = 2, 3, 5$ and 13 respectively we obtain $E < F$ if at least one of the following is true:

$$(\log v) \left(\frac{1}{4} + \frac{3}{2v} \right) < 1, \quad (6.1)$$

$$(\log v) \left(\frac{1}{6} + \frac{3}{v} \right) < 1, \quad (6.2)$$

$$(\log v) \left(\frac{2}{15} + \frac{11}{2v} \right) < 1, \quad (6.3)$$

$$(\log v) \left(\frac{96}{1001} + \frac{35}{v} \right) < 1. \quad (6.4)$$

We now show that if $1 < v \leq 20,000$, then at least one of these does hold. Let

$$f(v; \alpha, \beta) = (\log v)(\alpha + \beta v^{-1}).$$

A simple calculation reveals that $f'(v; \frac{1}{4}, \frac{3}{2}) > 0$ for all $v > 1$, so that if $1 \leq v \leq 20$, then

$$f(v; \frac{1}{4}, \frac{3}{2}) \leq f(20; \frac{1}{4}, \frac{3}{2}) < 1.$$

To treat the remaining cases we observe that

$$f'(v; \alpha, \beta) = \beta v^{-2}(\alpha \beta^{-1} + 1 - \log v).$$

Clearly $\alpha \beta^{-1} + 1 = \log v$ has at most two solutions, the lesser of which is the only local maximum of f . For $f(v; \frac{1}{8}, 3)$ this smaller solution lies in $[e, 12]$, for $f(v; \frac{2}{15}, \frac{11}{2})$ in $[e, 4]$, and for $f(v; \frac{96}{1001}, 35)$ in $[e, 3]$. Thus f has no local maximum in the intervals we shall consider. When $18 \leq v \leq 270$ we have

$$f(v; \frac{1}{8}, 3) \leq \max(f(18; \frac{1}{8}, 3), f(270; \frac{1}{8}, 3)) < 1,$$

when $42 \leq v \leq 1000$

$$f(v; \frac{2}{15}, \frac{11}{2}) \leq \max(f(42; \frac{2}{15}, \frac{11}{2}), f(1000; \frac{2}{15}, \frac{11}{2})) < 1,$$

and when $700 \leq v \leq 20,000$

$$f(v; \frac{96}{1001}, 35) \leq \max(f(700; \frac{96}{1001}, 35), f(20,000; \frac{96}{1001}, 35)) < 1.$$

Hence (6.1) holds if $1 \leq v \leq 20$, (6.2) if $18 \leq v \leq 270$, (6.3) if $42 \leq v \leq 1000$, and (6.4) if $700 \leq v \leq 20000$. This establishes the inequality $E < F$ throughout the range $k < y \leq 20000k$.

7. *Proof of Corollary 2.* Rosser and Schoenfeld [21] have shown that

$$\frac{N}{\log N} < \pi(N)$$

when $N \geq 17$. Hence, by (1.12),

$$\pi(M + N) - \pi(M) \leq 2\pi(N)$$

for $N \geq 17$. It remains only to deal with the range $1 < N \leq 17$. If $M = 1$, then

$$\pi(M + N) - \pi(M) = \pi(N + 1) \leq 2\pi(N),$$

and if $M \geq 2$, then

$$\pi(M + N) - \pi(M) \leq \frac{1}{2}(N + 1)$$

since all the primes in the range are odd. We now remark that $\frac{1}{2}(N + 1) \leq 2\pi(N)$ for $2 \leq N \leq 17$, and we are finished. An alternative treatment of the range $1 \leq N \leq 17$ is contained in the work of Schinzel and Sierpiński [23] and Schinzel [22], where it is shown that if $1 < \min(M, N) \leq 146$, then

$$\pi(M + N) \leq \pi(M) + \pi(N).$$

8. *Proof of Theorem 3.* We assume throughout this section that N is large. Let $z = (\frac{2}{3}N)^{\frac{1}{2}}$ and $P = \prod_{p \leq z} p$. We use (2.6) with $M = 0$, $a_n = \Lambda(n)$ if $(n, P) = 1$ and $a_n = 0$ if $(n, P) > 1$. By the prime theorem number, the right hand side of

(2.6) is

$$\sum_{\substack{n=1 \\ (n, P)=1}}^N \Lambda(n)^2 = N \log N - N + o(N) < N \log N - \frac{1}{2}N$$

for large N . Bombieri and Davenport [2] have shown that if $q \leq z$, then

$$\sum_{\chi} |\tau(\chi)|^2 \left| \sum_{n=1}^N a_n \chi(n) \right|^2 = \phi(q) \sum_{a=1}^q \left| S\left(\frac{a}{q}\right) \right|^2.$$

We now see from (2.6) that

$$\sum_{q \leq z} (1 + qz^{-1})^{-1} \phi(q)^{-1} \sum_{\chi} |\tau(\chi)|^2 \left| \sum_{n=1}^N a_n \chi(n) \right|^2 \leq N^2 \log N - \frac{1}{2}N^2. \quad (8.1)$$

We next group together those characters χ which are induced by the same primitive character χ^* . Clearly $\sum a_n \chi(n) = \sum a_n \chi^*(n)$, and if χ is to the modulus q and χ^* is to the modulus q^* , then q^* divides q , say $q^* r = q$. It is well known (see for instance Davenport [4, p. 148]) that $|\tau(\chi)|^2 = q^*$ if r is square free and $(r, q^*) = 1$, and otherwise $|\tau(\chi)|^2 = 0$. Thus the left hand side of (8.1) becomes

$$\sum_{q^* \leq z} \frac{q^*}{\phi(q^*)} \left(\sum_{\substack{r \leq z/q^* \\ (r, q^*)=1}} \mu(r)^2 \phi(r)^{-1} (1 + rq^*/z)^{-1} \right) \sum_{\chi}^* \left| \sum_{n=1}^N a_n \chi(n) \right|^2.$$

From Lemmas 3 and 8 we see that the sum in parenthesis is

$$> \frac{\phi(q^*)}{q^*} \left(\log \frac{z}{q^*} + 0.361 \right) > \frac{\phi(q^*)}{q^*} \log \frac{N^{\frac{1}{2}}}{q^*}$$

provided that $q^* \leq \frac{1}{100}z$. Since $W = \frac{1}{200}N^{\frac{1}{2}} < \frac{1}{100}z$ we are able to assert that

$$\sum_{q \leq W} \left(\log \frac{N^{\frac{1}{2}}}{q} \right) \sum_{\chi}^* \left| \sum_{n=1}^N a_n \chi(n) \right|^2 < N^2 \log N - \frac{1}{2}N^2. \quad (8.2)$$

It remains to consider those n with $(P, n) > 1$. Gallagher [6] has shown that

$$\sum_{\chi}^* \left| \sum_{n=1}^N c_n \chi(n) \right|^2 \leq \sum_{a=1}^q \left| \sum_{n=1}^N c_n e(an/q) \right|^2.$$

Thus from (2.6) it follows that

$$\begin{aligned} \sum_{q \leq W} \left(\log \frac{N^{\frac{1}{2}}}{q} \right) \sum_{\chi}^* \left| \sum_{\substack{n=1 \\ (n, P)=1}}^N \Lambda(n) \chi(n) \right|^2 &\ll N(\log N) \sum_{\substack{n=1 \\ (n, P)=1}}^N \Lambda(n)^2 \\ &\ll N \log N \sum_{p \leq N^{\frac{1}{2}}} (\log p)^2 \left[\frac{\log N}{\log p} \right]. \end{aligned}$$

Hence

$$\sum_{q \leq W} \log \left(\frac{N^{\frac{1}{2}}}{q} \right) \sum_z^* \left| \sum_{\substack{n=1 \\ (n, P) > 1}}^N \Lambda(n) \chi(n) \right|^2 \ll N^{\frac{1}{2}} (\log N)^2. \quad (8.3)$$

We use Minkowski's inequality to combine (8.2) and (8.3); we find that

$$\sum_{q \leq W} \left(\log \frac{N^{\frac{1}{2}}}{q} \right) \sum_z^* |\psi(N, \chi)|^2 \leq (N(\log N - \tfrac{1}{2})^{\frac{1}{2}} + O(N^{\frac{1}{2}} \log N))^2.$$

For large N this upper bound is $< N^2 \log N$, as required.

References

1. E. Bombieri, "A note on the large sieve", *Acta Arith.*, 18 (1971), 401–404.
2. ——— and H. Davenport, "On the large sieve method", *Abh. aus Zahlentheorie und Analysis Zur Erinnerung an Edmund Landau*, Deut. Verlag Wiss., Berlin, 1968, 11–22.
3. ——— and ———, "Some inequalities involving trigonometrical polynomials", *Ann. Scuola Norm. Sup. Pisa*, 23 (1969), 223–241.
4. H. Davenport, *Multiplicative number theory* (Markham, Chicago, 1967).
5. P. D. T. A. Elliott, "Some remarks concerning the large sieve type", *Acta Arith.*, 18 (1971), 405–422.
6. P. X. Gallagher, "The large sieve", *Mathematika*, 14 (1967), 14–20.
7. G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities* (University Press, Cambridge, 1934).
8. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fourth edition (Clarendon Press, Oxford, 1964).
9. E. Hellinger and O. Toeplitz, "Grundlagen für eine Theorie der unendlichen Matrizen", *Math. Ann.*, 69 (1910), 289–330.
10. D. Hensley and I. Richards, "On the incompatibility of two conjectures concerning primes", *Proc. Symposia Pure Math.*, 24 (1973), 123–128.
11. N. I. Klimov, "Almost prime numbers", *Uspehi Mat. Nauk*, 16 (3), (99) (1961), 181–188. See *Amer. Math. Soc. Transl.*, (92) 46 (1965), 48–56.
12. I. Kobayashi, "Remarks on the large sieve method", *Proc. Japan–United States Seminar on Number Theory*, 1971, 3 pp.
13. J. H. van Lint and H.-E. Richert, "On primes in arithmetic progressions", *Acta Arith.*, 11 (1965), 209–216.
14. K. R. Matthews, "On an inequality of Davenport and Halberstam", *J. London Math. Soc.*, (2) 4 (1972), 638–642.
15. ———, "On a bilinear form associated with the large sieve", *J. London Math. Soc.*, (2) 5 (1972), 567–570.
16. ———, "Hermitian forms and the large and small sieves", *J. Number Theory*, 5 (1973), 16–23.
17. Ming-Chit Liu, "On a result of Davenport and Halberstam", *J. Number Theory*, 1 (1969), 385–389.
18. H. L. Montgomery, "A note on the large sieve", *J. London Math. Soc.*, 43 (1968), 93–98.
19. ———, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, 227 (Springer-Verlag, 1971).
20. ——— and R. C. Vaughan, "Hilbert's inequality", *J. London Math. Soc.* (to appear).
21. J. B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.*, 6 (1962), 64–94.
22. A. Schinzel, "Remarks on the paper 'Sur certaines hypothèses concernant les nombres premiers'", *Acta Arith.*, 7 (1961), 1–8.
23. ——— and W. Sierpiński, "Sur certaines hypothèses concernant les nombres premiers", *Acta Arith.*, 4 (1958), 185–208.

- 24. A. Selberg, "On elementary methods in prime number theory and their limitations", *Den 11-te Skand. Mat.-Kongress*, Trondhjem, 1949, 13–22.
- 25. ———, "The general sieve-method and its place in prime number theory", *Proc. Intern. Congr. Math.*, Cambridge, Mass., 1950, 1, 286–292.
- 26. S. Uchiyama, "A note on the sieve method of A. Selberg", *J. Fac. Sci. Hokkaido Univ.*, (1) 16 (1962), 189–192.
- 27. D. R. Ward, "Some series involving Euler's function", *J. London Math. Soc.*, 2 (1927), 210–214.

The University of Michigan,
Ann Arbor, Michigan, U.S.A.
Imperial College,
London.

10H30: *NUMBER THEORY; Multiplicative
theory; Sieves.*

Received on the 17th of July, 1973.