JOURNAL OF NUMBER THEORY 4, 437–454 (1972)

Irregularity in Sifted Sequences

M. N. HUXLEY

Mathematical Institute, University of Oxford, Oxford, England

Communicated by K. F. Roth

Received September 14, 1970

K. F. Roth (*Acta Arith.* **9** (1964), 257–260) considered the distribution of a sequence $\mathcal{N}$ of distinct positive integers not exceeding N among the residue classes for each modulus not exceeding Q. He showed that a certain variance was $>\rho(1-\rho)\,Q^2N$, where ρ was the density of the sequence, implying that $\mathcal{N}$ is not too evenly distributed among the residue classes in all subintervals of $[1, N]$ unless ρ is almost 0 or 1. In this paper we consider a sifted sequence, one which is forbidden to enter certain residue classes, and enquire how evenly the sequence falls into the remaining residue classes for each modulus. Our main result shows that another variance lies between bounded multiples of $\rho(1-\rho)\,Q^2N/\Lambda$, where N/Λ is the Selberg upper bound for the number of members of $\mathcal{N}$ in $[1, N]$ and $\rho N/\Lambda$ is the actual number. The lower bound implies Roth's result in the unsifted case.

1. INTRODUCTION

In 1964 K. F. Roth [3] considered the distribution of an arbitrary sequence of integers among the residue classes to each modulus q not exceeding some bound Q, and showed that no sequence can be very well distributed unless either it or its complement is sparse. More precisely, he showed that a certain variance involving the integers of the sequence $\mathcal{N}$ not exceeding N was

$$\gg \rho(1-\rho)\,NQ^2,$$

where ρ is the density of $\mathcal{N}$ in $[1, N]$. In this paper we consider a sifted sequence $\mathcal{N}$, that is, one which for each prime p never meets any of a set $H(p)$ of $f(p)$ residue classes. The upper bound sieve tells us that (to within an error) term $\mathcal{N}$ can have at most $N\Lambda^{-1}$ members in any interval of length N, where Λ will be defined below as a function of Q and the numbers $f(p)$ for $p \leqslant Q$. The number of integers of $\mathcal{N}$ in $[1, N]$

is now $\rho N\Lambda^{-1}$, where ρ is bounded, and in Theorem 2 we show that a variance generalizing Roth's is

$$\gg \rho(1-\rho)\, NQ^2\Lambda^{-1}, \tag{1}$$

provided that the numbers $f(p)$ do not increase too rapidly with p (a sufficient condition for this is $f(p) \ll p^{\epsilon}$ for each $\epsilon > 0$), and if $Q = o(N^{1/2}(\log N)^{-1})$. In these inequalities the double inequality sign indicates an inequality with a suppressed absolute constant. The condition on Q was unnecessary in Roth's case. Theorem 2 is deduced from Theorem 1 in which we determine the asymptotic order of magnitude of a different variance. A simplified form of this variance occurs in Theorem 3, which takes only the distribution of $\mathcal{N}$ among residue classes into account, not that among subintervals of $[1, N]$. The variance of Theorem 1 has as asymptotic size the expression in (1), and that of Theorem 3 is bounded above by the same quantity diminished by Q^2.

To state the theorems we require the following notation. Lower case Roman letters denote integers; of these p will always denote a prime. Let

$$\kappa(n) = 1 \qquad \text{if} \quad 1 \leqslant n \leqslant N \quad \text{and} \quad n \in \mathcal{N},$$

$$\kappa(n) = 0 \qquad \text{otherwise},$$

so that $\kappa(n)$ is the characteristic function of $\mathcal{N}$. Let q be a positive integer. By the Chinese Remainder Theorem there is a set $H(q)$ of $f(q)$ residue classes mod q, where

$$f(q) = q \prod_{p \mid q} f(p)/p,$$

with the property $(h - n, q) = 1$ whenever $n \in \mathcal{N}$ and $h \in H(q)$, and a set $K(q)$ of $g(q)$ residue classes, where

$$g(q) = q \prod_{p \mid q} (1 - f(p)/p),$$

which cover the sequence $\mathcal{N}$. We set

$$\Lambda = \sum_{q \leqslant Q} \frac{\mu^2(q) f(q)}{g(q)}, \tag{2}$$

and put

$$E(A, B; b, q) = \sum_{\substack{m=A+1 \\ m \equiv b \pmod q}}^{B} \kappa(m) - \frac{\rho(B - A)\, \delta(b, q)}{\Lambda g(q)}, \tag{3}$$

where $\delta(b, q) = 1$ if $b \in K(q)$, 0 otherwise. We let

$$A_q(u) = \max(0, u - qX - 1), \tag{4}$$

$$B(u) = \min(N, u - 1), \tag{5}$$

where $X = [\frac{1}{2}Q]$. For real α we use the exponential sum notation $e(\alpha) = \exp 2\pi i\alpha$, $e_q(\alpha) = \exp 2\pi i\alpha/q$. We can now state the results.

THEOREM 1. *Let*

$$Z_q(A, B) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \Big| \sum_{b=1}^{q} E(A, B; b, q)\, e_q(ab) \Big|^2. \tag{6}$$

Then

$$\sum_{q \leqslant Q} \frac{1}{q^2} \sum_{u=2}^{N+qx} Z_q(A_q(u), B(u)) \tag{7}$$

lies between bounded multiples of

$$\rho(1 - \rho + o(1))\, NQ^2\Lambda^{-1}, \tag{8}$$

provided that

$$Q = o(N^{1/2}(\log N)^{-1}) \tag{9}$$

and the $f(p)$ grow slowly enough for

$$\sum_{q \leqslant Q} \frac{\mu^2(q) f(q)\, q}{g(q)} = o(Q\Lambda). \tag{10}$$

THEOREM 2. *Let*

$$V_q(A, B) = \sum_{b=1}^{q} | E(A, B); b, q |^2. \tag{11}$$

Then if (9) *and* (10) *hold we have*

$$\sum_{q \leqslant Q} \frac{1}{q} \sum_{u=2}^{N+qx} V_q(A_q(u), B(u)) \geqslant \pi^{-2}\rho(1 - \rho + o(1))\, NQ^2\Lambda^{-1}, \tag{12}$$

and the same lower bound holds for

$$Q \sum_{q \leqslant Q} V_q(0, N) + 4 \sum_{n=1}^{N} \sum_{q \leqslant Q} V_q(0, n)/q. \tag{13}$$

From H. L. Montgomery's form [2] of the upper bound sieve we deduce

THEOREM 3. *We have unconditionally*

$$\sum_{q \leqslant Q} Z_q(0, N) \leqslant \rho(1 - \rho + O(Q^2 N^{-1}))\, N\Lambda^{-1},$$

and

$$\sum_{\substack{q \leqslant Q \\ f(q) \neq 0}} f(q) \min_{p \mid q} \frac{p}{f(p)}\, V_q(0, N) \leqslant \rho(1 - \rho + O(Q^2 N^{-1}))\, N\Lambda^{-1}.$$

To interpret these results, we note that $Z_q(A_q(u), B(u))$ and $V_q(A_q(u), B(u))$ are sums over all arithmetic progresssions of X terms ending near u. Thus Theorem 2 assures us that there is a u for which the average square of the difference $E(A_q(u), B(u); b, q)$ between the expected number $\rho X\Lambda^{-1}$ and the actual number of members of $\mathcal{N}$ in the progression, taken over all these progressions, is of the same order as the expected number $\rho X\Lambda^{-1}$ itself, unless ρ is close to 1.

The failure of our method at $\rho = 1$ is intrinsic: if the Selberg upper bound could be attained, a number of arguments show that the sequence $\mathcal{N}$ must be extremely regular. In our notation below, $S(\alpha)$ would be very close to $\Lambda^{-1}U(\alpha)$, an exponential sum whose coefficients we shall show to be distributed evenly among residue classes. Our method is too closely tied to Selberg's to cast much light on the question as to whether the Selberg upper bound can be attained. It has been shown that it cannot be attained in certain cases when the interval is $[1, N]$ and the set $H(p)$ is defined in a way essentially independent of the prime p. Thus if $H(p)$ contains only the zero class for each prime p, $\mathcal{N}$ must be a subsequence of the primes, and by the prime number theorem $\rho \leqslant \frac{1}{2} + o(1)$.

The restriction (9) arises from a clumsy estimate of $V(\alpha)$ in Lemma 2. If $f(q) = 0$ when $q > 1$, which is Roth's unsifted case, then $V(\alpha) = 0$, and the condition (9) is unnecessary. On the other hand, we would be content with the condition $Q \ll N^{1/2}$. Condition (10) is fascinating; it arises both in Roth's original argument (as adapted to our problem) and in our variation of it. (10) may be there to protect the existence of the perfect squares, for which $f(p) = \frac{1}{2}(p - 1)$ and ρ is positive if we allow $Q \gg N^{1/2}$, but for which $V_q(0, N)$ is at most $g(q)$.

2. THE SELBERG COEFFICIENTS

Let

$$S(\alpha) = \sum_{n=1}^{N} \kappa(n)\, e(n\alpha). \tag{1}$$

We write

$$K(a, q) = \sum_{k \in K(q)} \frac{e_q(ak)}{g(q)} = \frac{\mu(q)}{g(q)} \sum_{h \in H(q)} e_q(ah). \tag{2}$$

It is easily verified that

$$| K(a, q)| \leqslant \mu^2(q) f(q)/g(q) \tag{3}$$

and

$$\sum_{(a,q)=1}^{q} | K(a, q)|^2 = \frac{\mu^2(q) f(q)}{g(q)}. \tag{4}$$

If the integers of $\mathcal{N}$ divide equally between the residue classes of the set $K(q)$ we should expect that for small real β

$$S(a/q + \beta) \sim MN^{-1}K(a, q) F(N, \beta), \tag{5}$$

where

$$M = S(0) = \sum_{n \leqslant N} \kappa(n) \tag{6}$$

and for any real β and positive integer U we write

$$F(U, \beta) = \sum_{n=1}^{U} e(n\beta). \tag{7}$$

Since

$$| F(U, \beta)| = \left| \frac{\sin \pi U\beta}{\sin \pi\beta} \right| \ll \frac{1}{\| \beta \|}, \tag{8}$$

where $\| \beta \|$ denotes the distance of the real number β from the nearest integer, the sum

$$U(\alpha) = \sum_{q \leqslant Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} K(a, q) F(N, \alpha - a/q) \tag{9}$$

will have the approximation property (5) near rational points a/q with $q \leqslant Q$. We shall use a/q to mean a rational point with $q \leqslant Q$, $1 \leqslant a \leqslant q$ and $(a, q) = 1$, that is, a member of the Farey sequence of order Q.

In order to work out the coefficient of $e(n\alpha)$ in (9) we consider for square free q the sum

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} \sum_{k\in K(q)} e_q(ak - an) = \sum_{k\in K(q)} \sum_{\substack{d\mid q\\ k\equiv n \pmod d}} d\mu\left(\frac{q}{d}\right)$$

$$= \sum_{\substack{d\mid q\\ n\in K(d)}} d\mu\left(\frac{q}{d}\right)\frac{g(q)}{g(d)}$$

$$= \mu(q)\, g(q) \prod_{\substack{p\mid q\\ n\in K(p)}} \left(1 - \frac{p}{g(p)}\right),$$

which it is convenient to invert as

$$f(q) \prod_{\substack{p\mid q\\ n\in H(p)}} \left(\frac{p}{f(p)} - 1\right) = f(q) \sum_{\substack{d\mid q\\ n\in H(d)}} \frac{\mu(d)\, d}{f(d)}.$$

The coefficient of $e(n\alpha)$ in (9) is now

$$\lambda(n) = \sum_{\substack{d\leqslant Q\\ n\in H(d)}} \frac{\mu(d)\, d}{f(d)} \sum_{\substack{q\equiv 0(d)\\ q\leqslant Q}} \frac{\mu^2(q) f(q)}{g(q)}, \tag{10}$$

the familiar Selberg upper sifting function. This method of constructing upper sifting functions will generalize to the situation where the $\kappa(n)$ are weights not necessarily 0 or 1, but we do not need this generality here. We recover Selberg's upper bound sieve from Cauchy's inequality:

$$\begin{aligned} M\Lambda &= \int_0^1 S(\alpha)\, U(-\alpha)\, d\alpha \\ &\leqslant \left(\int_0^1 |\, S(\alpha)|^2\, d\alpha\right)^{1/2} \left(\int_0^1 |\, U(\alpha)|^2\, d\alpha\right)^{1/2}. \end{aligned} \tag{11}$$

The first integral on the right is M, and we shall show in the next section that for small Q the second is

$$N\Lambda(1 + o(1)),$$

so that

$$M \leqslant N\Lambda^{-1}(1 + o(1)), \tag{12}$$

and when we write

$$M = \rho N \Lambda^{-1}$$

then ρ is bounded.

After our construction of the coefficient $\lambda(m)$ we expect that for any subinterval $[A, B]$ of $[1, N]$ when we write

$$\sum_{\substack{m=A+1 \\ m \equiv b (\mathrm{mod}\, r)}}^{B} \lambda(m) = \frac{(B - A)\, \delta(b, r)}{g(r)} + L(A, B; b, r), \tag{13}$$

where $\delta(b, r) = 0$ unless $b \in K(r)$, when it is 1, then $L(A, B; b, r)$ is of smaller order. In fact, we have

LEMMA 1. *If $r \leqslant Q$ then* (13) *holds with*

$$|L(A, B; b, r)| \leqslant E_1 = \sum_{q \leqslant Q} \frac{\mu^2(q) f(q) \sigma(q)}{g(q)}$$

where $\sigma(q)$ is the sum of the divisors of q.

Proof. We have

$$\sum_{\substack{m=A+1 \\ m \equiv b (\mathrm{mod}\, r)}}^{B} \lambda(m) = \sum_{d} \frac{\mu(d)\, d}{f(d)} \sum_{\substack{q \leqslant Q \\ q \equiv O(d)}} \frac{\mu^2(q) f(q)}{g(q)} \sum_{\substack{m=A+1 \\ m \in H(d) \\ m \equiv b (\mathrm{mod}\, r)}}^{B} 1.$$

We take first the sum over m. Over each complete system of residues mod$[d, r]$ it is zero unless $b \in H((d, r))$ when it is

$$f(d)/f((d, r)).$$

We can now write the sum required as

$$\sum_{d \leqslant Q} \frac{\mu(d)\, d}{f(d)} \sum_{\substack{q \equiv O(d) \\ q \leqslant Q}} \frac{\mu^2(q) f(q)}{g(q)} \left(\frac{(B - A)(d, r)}{dr} + O(1) \right) \frac{f(d)}{f((d, r))}$$

$$= \left(\frac{B - A}{r} \right) \sum_{d \leqslant Q} \frac{\mu(d)(d, r)}{f((d, r))} \sum_{\substack{q \equiv O(d) \\ q \leqslant Q}} \frac{\mu^2(q) f(q)}{g(q)}$$

$$+ O\left(\sum_{d \leqslant Q} d \sum_{\substack{q \equiv O(d) \\ q \leqslant Q}} \frac{\mu^2(q) f(q)}{g(q)} \right),$$

where the sum is taken over those d for which $b \in H((d, r))$. If q has any prime factor which does not divide r, the sum over d in the main term is 0. The coefficient of $(B - A)/r$ is then

$$\sum_{q|r} \frac{\mu^2(q) f(q)}{g(q)} \sum_{\substack{d|q \\ b \in H(d)}} \frac{\mu(d)\, d}{f(d)} = \sum_{\substack{d|q \\ b \in H(d)}} \frac{\mu(d)\, d}{f(d)} \cdot \frac{f(d) r}{dg(r)},$$

which is 0 unless $b \in K(r)$, when it is $r/g(r)$.

3. An Integral Involving $U(\alpha)$

Our object is to prove

Lemma 2. *We have*

$$\sum_{1 \leqslant m \leqslant N} \lambda^2(m) = N\Lambda(1 + o(1)) \tag{1}$$

provided that

$$Q = o(N^{1/2}/\log N). \tag{2}$$

Proof. We use the Hardy–Littlewood circle method. We divide the unit interval [0, 1] into arcs $I(a_r, q_r)$ corresponding to fractions a_r/q_r of the Farey sequence of order Q by

$$I(a_r, q_r) = \left[\frac{1}{2}\frac{a_{r-1}}{q_{r-1}} + \frac{1}{2}\frac{a_r}{q_r}, \frac{1}{2}\frac{a_r}{q_r} + \frac{1}{2}\frac{a_{r+1}}{q_{r+1}}\right], \tag{3}$$

with appropriate modifications at the ends of the interval [0, 1]. If $\alpha \in I(a, q)$ and b/r is any fraction of the Farey sequence of order Q we have

$$\| \alpha - b/r \| \geqslant \tfrac{1}{2} \| a/q - b/r \|, \tag{4}$$

the sign $\| \beta \|$ denoting the distance of the real number β from the nearest integer. The required sum in (1) is

$$\int_0^1 |U(\alpha)|^2 \, d\alpha. \tag{5}$$

For $\alpha \in I(a, q)$ we write

$$U(\alpha) = K(a, q) F(N, \alpha - a/q) + V(\alpha), \tag{6}$$

where

$$V(\alpha) = \sum_{b/r} K(b, r)\, F(N, \alpha - b/r), \tag{7}$$

the sum being over all Farey fractions b/r with $r \leqslant Q$ other than a/q itself. We shall treat $V(\alpha)$ as an error term.

Our main term is

$$\sum_{a/q} |K(a, q)|^2 \int_{I(a,q)} |F(N, \alpha - a/q)|^2\, d\alpha = \sum_{a/q} |K(a, q)|^2 (N + O(Q^2))$$
$$= (N + O(Q^2))\, \Lambda, \tag{8}$$

where we have used (2.4).

As for the error term, we need only consider

$$\int_0^1 |V(\alpha)|^2\, d\alpha, \tag{9}$$

since if this is $o(N\Lambda)$ then, by Cauchy's inequality, so is the integral arising from the cross product term when (6) is squared. By (7) and (4) if $\alpha \in I(a, q)$ we have

$$|V(\alpha)| \ll \sum_{b/r \neq a/q} \frac{|K(b, r)|}{\| a/q - b/r \|}, \tag{10}$$

the sum being over points b/r of the Farey sequence of order Q. Thus,

$$\int_0^1 |V(\alpha)|^2\, d\alpha \ll \sum_{b/r} |K(b, r)|^2 \sum_{a/q \neq b/r} \int_{I(a,q)} \frac{d\alpha}{\| a/q - b/r \|}$$
$$+ \sum_{b/r} |K(b, r)| \sum_{c/s \neq b/r} |K(c, s)|$$
$$\times \sum_{\substack{a/q \neq b/r \\ a/q \neq c/s}} \int_{I(a,q)} \frac{d\alpha}{\| a/q - b/r \|\, \| a/q - c/s \|}.$$

The integrals on the right come, respectively, to $\ll Qr$ and to $\ll \log Q / \| b/r - c/s \|$, so that

$$\int_0^1 |V(\alpha)|^2\, d\alpha$$
$$\ll \sum_{b/r} Qr\, |K(b, r)|^2 + \sum_{b/r} \log Q\, |K(b, r)|^2 \sum_{c/s \neq b/r} (\| b/r - c/s \|)^{-1}$$
$$\ll Q^2 \log^2 Q \sum_{b/r} |K(b, r)|^2 \ll Q^2 \Lambda \log^2 Q, \tag{11}$$

where we have used (2.3). Hence the integral (5) is equal to the right-hand side of (1) provided only that (2) holds.

We could also obtain (1) by using the series definition (2.5) of $\lambda(m)$; this gives

$$\sum_{1\leqslant m\leqslant N} \lambda^2(m) = N\Lambda + O(E_1^2); \tag{12}$$

this would give in place of (2) the condition

$$E_1 = o((N\Lambda)^{1/2}), \tag{13}$$

which is weaker than (2) only when $f(p)$ is usually less than 4.

4. The Analogue of Roth's Argument

Roth's argument is based on the inequality

$$\sum_{r\leqslant Q} |F(X, r\alpha)|^2 \geqslant 4X^2/\pi^2$$

(where $X = [\frac{1}{2}Q]$) valid for all $\alpha \in [0, 1]$. To simplify the estimations in the next section we use instead

$$G(\alpha) = \sum_{q\leqslant Q} \frac{1}{q^2} \sum_{\substack{a=1\\(a,q)=1}}^{q} |F(qX, \alpha - a/q)|^2. \tag{1}$$

For each α in [0, 1] there is a point a/q of the Farey sequence of order Q with $\alpha = a/q + \beta$, where $\|\beta\| \leqslant (Qq)^{-1}$. By (2.8) we have

$$|F(qX, \beta)| = \left|\frac{\sin \pi qX\beta}{\sin \pi\beta}\right| = qX \left|\frac{\sin \pi qX\beta}{\pi qX\beta}\right| \left|\frac{\pi\beta}{\sin \pi\beta}\right| \geqslant \frac{2qX}{\pi}$$

since $|\pi qX\beta| \leqslant \frac{1}{2}\pi$. Hence

$$G(\alpha) \geqslant 4X^2/\pi^2, \tag{2}$$

but unlike Roth's function, which can be as large as $\frac{1}{4}Q^3$, we have an inequality in the opposite direction for $G(\alpha)$. Suppose α lies between b/r and c/s in the Farey sequence of order Q. For the terms in (1) in b/r and c/s we use the upper bound X^2. Otherwise, if

$$\alpha < a/q \leqslant \alpha + \tfrac{1}{2} \qquad \text{(modulo 1)},$$

we have by (2.8)

$$|F(qX, \alpha - a/q)|^2 \leqslant \operatorname{cosec}^2 \pi(a/q - c/s)$$
$$\leqslant \frac{1}{4}\frac{q^2s^2}{(as - cq)^2}.$$

Now for each integer m the number of q between 1 and Q for which

$$as - cq = m$$

is at most $Q/s + 1$, and arguing similarly if $a/q < \alpha$ we have

$$G(\alpha) \leqslant 2X^2 + \frac{1}{4}\sum_{m=1}^{Q^2}\frac{s^2}{m^2}\left(\frac{Q}{s} + 1\right) + \frac{1}{4}\sum_{m=1}^{Q^2}\frac{r^2}{m^2}\left(\frac{Q}{r} + 1\right)$$
$$\leqslant \left(\frac{1}{2} + \frac{\pi^2}{6}\right)Q^2 \leqslant 2Q^2. \tag{3}$$

This is the property of $G(\alpha)$ that makes the estimations in the next section very much easier.

Let

$$T(\alpha) = S(\alpha) - \rho\Lambda^{-1}U(\alpha)$$
$$= \sum_{n=1}^{N}(\kappa(n) - \rho\Lambda^{-1}\lambda(n)). \tag{4}$$

Then in the notation of Theorem 1

$$T(\alpha)\,F(qX, \alpha - a/q)$$
$$= \sum_{u=2}^{N+\sigma X} e(u\alpha) \sum_{m=A_q(u)+1}^{B(u)} (\kappa(m) - \rho\Lambda^{-1}\lambda(m))\, e_q(am - au)$$
$$= \sum_{u=2}^{N+qX} e_q(-au)\, e(u\alpha) \sum_{b=1}^{q} J(A_q(u), B(u); b, q)\, e_q(ab),$$

where

$$J(A, B; b, q) = \sum_{\substack{m=A+1 \\ m \equiv b \pmod q}}^{B} (\kappa(m) - \rho\Lambda^{-1}\lambda(m)). \tag{5}$$

Hence

$$\int_0^1 G(\alpha)\,|T(\alpha)|^2\,d\alpha = \sum_{q \leqslant Q}\frac{1}{q^2}\sum_{\substack{a=1 \\ (a,q)=1}}^{q}\sum_{u=2}^{N+qX}\left|\sum_{b=1}^{q} J(A_q(u), B(u); b, q)\, e_q(ab)\right|^2. \tag{6}$$

The left-hand side of (6) can be estimated: apart from the scaling factor $\rho\Lambda^{-1}$, $T(\alpha)$ differs from $U(\alpha)$ in that ρ in M terms has been replaced by $\rho - 1$ (since $\lambda(n) = \Lambda$ if $m \in \mathcal{N}$). By Lemma 2 we have

$$\int_0^1 |T(\alpha)|^2 \, d\alpha = \rho^2\Lambda^{-2} \int_0^1 |U(\alpha)|^2 \, d\alpha - M(\rho^2 - (\rho - 1)^2)$$
$$= \rho(1 - \rho + o(1)) \, N\Lambda^{-1}, \tag{7}$$

provided that (3.2) holds. We have unconditionally

$$\int_0^1 |U(\alpha)|^2 \, d\alpha \geqslant \Lambda M,$$

and so

$$\int_0^1 |T(\alpha)|^2 \, d\alpha \geqslant \rho(1 - \rho)^2 \, N\Lambda^{-1},$$

but we shall need to assume (3.2) later in the argument. If (3.2) holds, the expression in (6) lies between bounded multiples of

$$\rho(1 - \rho + o(1)) \, NQ^2\Lambda^{-1}. \tag{8}$$

To obtain Theorem 1 we must replace $J(A, B; b, r)$ in (6) by $E(A, B; b, r)$.

5. Proof of Theorem 1

We shall find an upper estimate for the integral

$$\int_0^1 G(\alpha) \, |U(\alpha)|^2 \, d\alpha \tag{1}$$

with an error term

$$o(NQ^2\Lambda). \tag{2}$$

We divide $[0, 1]$ into arcs $I(a, q)$ given by (3.3) and use (3.6) to distinguish between a main term and an error term $V(\alpha)$ in the expansion of $U(\alpha)$. A major arc term in (1) is

$$\int_{I(a,q)} q^{-2} \, |F(qX, \alpha - a/q)|^2 \, |K(a, q)|^2 \, |F(N, \alpha - a/q)|^2 \, d\alpha$$
$$\leqslant q^{-2} \, |K(a, q)|^2 \int_0^1 |F(qX, \beta)|^2 \, |F(N, \beta)|^2 \, d\beta,$$

and the integral from 0 to 1 is

$$\leqslant (N + qX)\, q^2X^2.$$

Using (2.4) to sum over arcs a/q we see that the major arcs contribute

$$\leqslant (N + Q^2)\, X^2\Lambda. \tag{3}$$

A minor arc term is

$$|\, K(a, q)|^2\, r^{-2} \int_{I(a,q)} |\, F(N, \alpha - a/q)|^2\, |\, F(rX, \alpha - b/r)|^2\, d\alpha$$

with $r \neq q$ or $b/r \neq a/q$. By (3.4) we may take out the second factor in the integrand at its maximum

$$\ll \left\| \frac{ar - bq}{qr} \right\|^{-2}$$

so that the whole integral is

$$\ll |\, K(a, q)|^2\, r^{-2} \left\| \frac{ar - bq}{qr} \right\|^{-2} N. \tag{4}$$

Now the number of pairs (b, r) with $r \leqslant Q$ for which $ar - bq$ takes a given value is $\ll Q/q$, so that when we sum (4) over points b/r other than a/q we have

$$\ll |\, K(a, q)|^2\, NqQ,$$

which sums over Farey points a/q to

$$\ll NQE_2\,,$$

where

$$E_2 = \sum_{q \leqslant Q} \frac{\mu^2(q)\, f(q)\, q}{g(q)} \tag{5}$$

and the minor arcs term satisfies (2) provided that

$$E_2 = o(Q\Lambda). \tag{6}$$

As in the proof of Lemma 2 it suffices to show that the term in $|\, V(\alpha)|^2$ satisfies (2) for the cross-product term to do so also. But now from (3.11) and (4.3) it is immediate that

$$\int_0^1 G(\alpha)\, |\, V(\alpha)|^2\, d\alpha \ll Q^4\Lambda \log^2 Q, \tag{7}$$

and so (2) is satisfied if (3.2) holds. Under the assumption of (3.2) and (6) we have now

$$\int_0^1 G(\alpha) \mid V(\alpha)|^2 \, d\alpha \leqslant NX^2\Lambda(1 + o(1)). \tag{8}$$

The integral (1) can be evaluated by the method of Section 4 also; we have

$$U(\alpha) F(qX, \alpha - a/q)$$

$$= \sum_{u=2}^{N+qX} e(u\alpha) \sum_{m=A_q(u)+1}^{B(u)} \lambda(m) e_q(am - au)$$

$$= \sum_{u=2}^{N+qX} e(u\alpha) \sum_{b=1}^{q} \left\{ \frac{(A_q(u) - B(u)) \delta(b, q)}{g(q)} + L(A_q(u), B(u); b, r) \right\} e_q(ab),$$

where $A_q(u)$, $B(u)$ are as before and $L(A, B; b, q)$ was defined in (2.13). The term in $F(qX, \alpha - a/q)$ therefore contributes to the integral (1)

$$q^{-2} \sum_{u=2}^{N+qX} (B(u) - A_q(u))^2 \mid K(a, q)|^2$$

$$+ 2 \operatorname{Re} \sum_{u=2}^{N+qX} q^{-2}(B(u) - A_q(u)) K(a, q) \sum_{b=1}^{q} L(A_q(u), B(u); b, q) e_q(-ab)$$

$$+ q^{-2} \sum_{u=2}^{N+qX} \left| \sum_{b=1}^{q} L(A_q(u), B(u); b, q) e_q(ab) \right|^2. \tag{9}$$

We estimate the middle term by Lemma 1 and partial summation over u. It is

$$\ll q^{-2} \mid K(a, q)|^2 \sum_{b=1}^{q} qQE_1 \ll \frac{\mu^2(q) f(q) QE_1}{g(q)},$$

where we have used (2.3). Using (1.2) to sum over all Farey points a/q we have

$$\int_0^1 G(\alpha) \mid U(\alpha)|^2 \, d\alpha = (N + O(Q^2)) X^2\Lambda$$

$$+ \sum_{q \leqslant Q} \frac{1}{q^2} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{u=2}^{N+qX} \left| \sum_{b=1}^{q} L(A_q(u), B(u); b, q) e_q(ab) \right|^2 + O(QE_1E_2). \tag{10}$$

Comparing (10) with (8), we see that

$$\sum_{q\leqslant Q}\frac{1}{q^2}\sum_{\substack{a=1\\(a,q)=1}}^{q}\sum_{u=2}^{N+qX}\mathbf{1}\left|\sum_{b=1}^{q}L(A_q(u),B(u);b,q)\,e_q(ab)\right|^2=o(NQ^2\Lambda) \quad (11)$$

provided (3.2) and (6) hold.

When we substitute

$$J(A,B;b,q)=E(A,B;b,q)-\rho\Lambda^{-1}L(A,B;b,q)$$

into (4.6) the term in $|L(A,B;b,q)|^2$ will be

$$o(\rho^2NQ^2\Lambda^{-1})$$

provided (3.2) holds, and so the cross-product term will be

$$o(\rho NQ^2\Lambda^{-1}).$$

Hence we have proved Theorem 1.

6. A Quadratic Form

For fixed square free q we consider the positive semidefinite quadratic form $\mathscr{F}_q$ in $g(q)$ variables indexed by the classes k of $K(q)$

$$\begin{aligned}\mathscr{F}_q(\mathbf{x})&=\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|\sum_{k\in K(q)}e_q(ak)\,x_k\right|\\&=\sum_{k\in K(q)}\sum_{l\in K(q)}x_kx_l\sum_{\substack{d\mid q\\d\mid(k-l)}}d\mu\left(\frac{q}{d}\right).\end{aligned} \quad (1)$$

By factorizing the appropriate determinant we see that the eigenvalues of this form are the numbers $qd^{-1}f(d)$ for d dividing q, each occurring

$$\prod_{p\mid q/d}(g(p)-1)$$

times. The eigenvector corresponding to the eigenvalue $f(q)$ is therefore unique and can be found by inspection: under a suitable normalization it has $x_k=1$ for each k. The other eigenvectors therefore lie in the subspace

$$\sum x_k=0. \quad (2)$$

We have now

$$f(q) \sum x_k^2 \leqslant \mathscr{F}_q(\mathbf{x}) \leqslant q \sum x_k^2, \tag{3}$$

and if (2) is satisfied then we can replace $f(q)$ in this inequality by the second smallest eigenvalue.

Now

$$Z_q(A, B) = \mathscr{F}_q(\mathbf{x}) \tag{4}$$

with

$$x_k = E(A, B; k, q), \tag{5}$$

so that we have

$$Z_q(A, B) \leqslant q \sum_{k \in K(q)} x_k^2 = q V_q(A, B), \tag{6}$$

and so Theorem 1 implies Theorem 2.

7. An Upper Bound

So far we have used Selberg's form of the upper bound sieve. H. L. Montgomery's form [1] is easily adapted to give an upper bound for a variance. We sketch Montgomery's result. Let q be square free. Since if $n \in \mathscr{N}$ then $(h - n, q) = 1$ for each h in $H(q)$, we have

$$\begin{aligned} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S\left(\frac{a}{q}\right) e_q(-ah) &= \sum_{n=1}^{N} \kappa(n) \sum_{\substack{a=1 \\ (a,q)=1}}^{q} e_q(an - ah), \\ &= \mu(q)\, M. \end{aligned}$$

Hence

$$\mu(q) f(q)\, M = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} S\left(\frac{a}{q}\right) \sum_{h \in H(q)} e_q(ah),$$

and Cauchy's inequality gives

$$\mu^2(q) f^2(q)\, M^2 \leqslant \Big(\sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right) \right|^2 \Big) \Big(\sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{h \in H(q)} e_q(-ah) \right|^2 \Big).$$

By (2.2) and (2.3) we have

$$\sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{h \in H(q)} e_q(ah) \right|^2 = \mu^2(q) f(q)\, g(q),$$

so that

$$\frac{\mu^2(q)f(q)}{g(q)} M^2 \leqslant \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right)\right|^2, \tag{1}$$

and if we sum over q, we have

$$M^2\Lambda \leqslant \sum_{q\leqslant Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right)\right|^2.$$

The best upper bounds for this sum known to the author are (from [1], except (2) which is folklore)

$$(N + \tfrac{2}{3}\sqrt{3}\, Q^2 + 3)\, M \qquad \text{if} \quad N \geqslant Q^2, \tag{2}$$

$$(Q^2 + 27N^3Q^{-4})\, M \qquad \text{if} \quad Q^2 \geqslant N, \tag{3}$$

$$2\max(N, Q^2)\, M \text{ in any case,} \tag{4}$$

so that

$$M \leqslant (N + O(Q^2))\, \Lambda^{-1}, \tag{5}$$

which we may compare with (2.11), valid provided (3.2) holds. What interests us here is that the difference of the two sides of (1) is a positive semidefinite form in the $g(q)$ variables

$$x_k = L(0, N; k, q) \tag{6}$$

corresponding to the classes k of $K(q)$.

In fact, it is the form $\mathscr{F}_q(\mathbf{x})$ of the last section, and we have the further condition

$$\sum_{k\in K(q)} x_k = 0,$$

so that

$$f(q) \min_{p|q} \frac{p}{f(p)} \sum_{k\in K(q)} x_k^2 \leqslant \mathscr{F}_q(\mathbf{x}) \leqslant q \sum_{k\in K(q)} x_k^2.$$

Hence we have

$$\sum_{q\leqslant Q} f(q) \min_{p|q} \frac{p}{f(p)} V_q(0, N) \leqslant Z_q(0, N)$$

$$\leqslant \rho N\Lambda^{-1}(1 + O(Q^2N^{-1})) - \rho^2 N\Lambda^{-1},$$

which gives Theorem 3.

REFERENCES

1. E. BOMBIERI AND H. DAVENPORT, Some inequalities involving trigonometric polynomials, *Ann. Scuola Norm. Sup. Pisa* **13** (1969), 223–241.
2. H. L. MONTGOMERY, A note on the large sieve, *J. London Math. Soc.* **43** (1968), 93–98.
3. K. F. ROTH, Remark concerning integer sequences, *Acta Arith.* **9** (1964), 257–260.