ACTA ARITHMETICA
XXIV (1973)

On cosine polynomials corresponding to sets of integers

by

K. F. Roth (London)

To Professor C. L. Siegel on his 75th birthday

§ 1. Introduction. Let

$$\mathcal{N} = \{n_1, n_2, \ldots, n_N\} \tag{1.1}$$

be a (non-empty) set of N distinct natural numbers. Write

$$E(\alpha) = \sum_{j=1}^{N} e(n_j\alpha), \tag{1.2}$$

with the usual notation

$$e(\beta) = e^{2\pi i\beta},$$

and also write

$$C(\alpha) = \tfrac{1}{2}\{E(\alpha)+E(-\alpha)\} = \sum_{j=1}^{N} \cos 2\pi n_j\alpha. \tag{1.3}$$

We define

$$A(\mathcal{N}) = \int_0^1 |E(\alpha)|\,d\alpha, \tag{1.4}$$

$$L(\mathcal{N}) = \inf_{0\leqslant\alpha\leqslant 1} C(\alpha). \tag{1.5}$$

Littlewood [5] conjectured that (1)

$$A(\mathcal{N}) \gg \log N;$$

this estimate, if true, would be best possible (as is easily seen by considering the case when the elements of (1.1) are consecutive members of an arithmetic progression).

(1) In all relations in which the $\gg$ notation is used, the implicit constant is absolute and N is supposed to be large. (But this latter assumption is not made elsewhere.)

But even the problem of establishing any lower bound for $A(\mathcal{N})$, depending only on N and tending to infinity with N, proved highly resistant. Nothing of this kind was known until Paul Cohen [3] devised a remarkable method with which he proved

$$A(\mathcal{N}) \gg \{(\log N)/(\log\log N)\}^{1/8}. \tag{1.6}$$

That estimate, however, did not exploit his method to the full, for his proof of (1.6) included a combinatorial lemma (see [3], Lemma 4) which was not the most effective possible of its kind.

In [4] Davenport replaced this result by his elegant, and essentially best possible, Lemmas 3 and 5 (which in combination correspond to a refinement of Cohen's Lemma 4). The substitution of this improved version of [3] Lemma 4 in Paul Cohen's method automatically yields

$$A(\mathcal{N}) \gg \{(\log N)/(\log\log N)\}^{1/4}. \tag{1.7}$$

In fact Davenport proved (1.7) with the constant here implicit in the $\gg$ notation equal to $\frac{1}{8}$ (where N is large in this context). Another point of interest in Davenport's paper is that he achieved a surprisingly simple exposition of Paul Cohen's method by defining explicitly certain coefficients whose existence (2) Paul Cohen had established indirectly by an appeal to the Hahn–Banach theorem. (See [3], Lemma 3, Corollary).

In connection with a problem concerning zeta functions, N. C. Ankeny and S. Chowla [1] conjectured that $|L(\mathcal{N})|$ was bounded below by a function of N tending to infinity with N. This conjecture also remained unproved until Paul Cohen obtained his above mentioned result, despite the fact that here nothing better than

$$\operatorname*{Inf}_{|\mathcal{N}|=N} |L(\mathcal{N})| \ll N^{1/2}$$

(where the infimum is taken over all sets (1.1) having N elements) is known in the opposite direction.

Lower bounds for $|L(\mathcal{N})|$ are implicit in (1.6) and (1.7) because there is the following simple relationship (see [6]) between the problems of Littlewood and Ankeny–Chowla. Since

$$\int_0^1 |C(\alpha)|\,d\alpha = \int_0^1 \{|C(\alpha)| - C(\alpha)\}\,d\alpha \leqslant 2\,|L(\mathcal{N})|$$

and

$$|C(\alpha)| = \tfrac{1}{2}\,|\{E(-\alpha) + E(\alpha)\}\,e(m\alpha)|,$$

(2) Paul Cohen proved that there exist exponential sums of prescribed structure having certain desired properties. After explicit choice of coefficients in the exponential sums of this structure, Davenport was able to verify the properties directly.

(where the integer m may be chosen to be large), we have

$$|L(\mathcal{N})| \geqslant \tfrac{1}{4}A(\mathcal{N}_1), \tag{1.8}$$

where $\mathcal{N}_1$ is a set of $2N$ distinct natural numbers. Thus (1.7) immediately yields (3)

$$|L(\mathcal{N})| \gg \{(\log N)/(\log\log N)\}^{1/4}. \tag{1.9}$$

In the present paper we prove, by a method fundamentally different from that of Paul Cohen, the stronger estimate

$$|L(\mathcal{N})| \gg \{(\log N)/(\log\log N)\}^{1/2}. \tag{1.10}$$

We shall obtain our result in the following more explicit form.

THEOREM. *Let N be a natural number and let $n_1, n_2, \ldots, n_N$ be any set of N distinct natural numbers. Write*

$$L = \inf_{0\leqslant\alpha\leqslant 1} \sum_{j=1}^{N} \cos 2\pi n_j\alpha, \tag{1.11}$$

and define the natural number M by

$$M = -[2L]. \tag{1.12}$$

Then we have

$$(8M)^{16M^2} > N. \tag{1.13}$$

We remark that whilst Paul Cohen's method applies equally to sums of type

$$\sum_{j=1}^{N} c_j e(n_j\alpha),$$

whenever

$$|c_j| \geqslant 1 \quad (j = 1, 2, \ldots, N),$$

we have not established any corresponding generalization of the above theorem. We make use of the fact that the coefficients of $\cos 2\pi n_j\alpha$ are all equal (for $j = 1, 2, \ldots, N$) and our method (at least in its present form) appears to admit only slight relaxations of this condition.

Our method is not applicable to Littlewood's problem.

For results depending on the rates of growth of infinite sequences, see [8], [2]; and for results concerning special sequences, see [7].

§ 2. Notation.

Lower case Roman type. The letter k may be used to represent any *integer*, but all other small Latin letters denote *natural numbers* (except where they are used to denote functions, or coefficients in exponential sums).

(3) [6] contains a more explicit form of this result.

Script capital type. We reserve script capitals (without superfixes) for non-empty *finite subsets of the set of all natural numbers*.

Operations on sets of integers. In the definitions below $\boldsymbol{U}$, $\boldsymbol{V}$ denote subsets of the set of all integers, and λ, μ denote real numbers.

We write

$$\lambda\boldsymbol{U}+\mu = \{\lambda k+\mu;\ k\in\boldsymbol{U}\}.$$

We define

$$\boldsymbol{U}+\boldsymbol{V} = \{k;\ \exists k_1\in\boldsymbol{U},\ \exists k_2\in\boldsymbol{V}|\ k = k_1+k_2\};$$

In other words, $\boldsymbol{U}+\boldsymbol{V}$ consists of all the distinct integers k representable in the form

$$k = k_1+k_2 \qquad (k_1\in\boldsymbol{U},\ k_2\in\boldsymbol{V}).$$

We define $\boldsymbol{U}-\boldsymbol{V}$ by

$$\boldsymbol{U}-\boldsymbol{V} = \boldsymbol{U}+(-1)\boldsymbol{V}.$$

The meanings of $\lambda\mathscr{U}+\mu$, $\mathscr{U}+\mathscr{V}$, $\mathscr{U}-\mathscr{V}$ (where, as always, script letters have the meaning prescribed above) arise as special cases of the above definitions. Needless to say, $\mathscr{U}+\mathscr{U}$ and $2\mathscr{U}$ have completely different meanings.

Sets $\overline{\mathscr{S}}$ and $\mathscr{S}^*$. We denote by $\overline{\mathscr{S}}$ the *complement of $\mathscr{S}$ with respect to the set of natural numbers.*

We define the set $\mathscr{S}^*$ by

$$\mathscr{S}^* = (\mathscr{S})\cup(-\mathscr{S}); \tag{2.1}$$

so that $\mathscr{S}^*$ consists of *the elements of $\mathscr{S}$ together with their reflections in* 0. This definition will be much applied throughout.

Symmetry. We shall say that $\mathscr{S}$ is *symmetric* if there exists a number τ such that

$$\mathscr{S} = \tau+(-\tau+\mathscr{S})^*, \tag{2.2}$$

and we shall refer to τ as the *centre of symmetry*. This terminology is clearly appropriate, since (2.2) asserts that $\mathscr{S}$ is identical to its reflection in τ.

Cardinality. We use $|\mathfrak{S}|$ to denote the *number of elements* of a finite set $\mathfrak{S}$. In particular, we have

$$|\mathscr{N}| = N, \qquad |\mathscr{N}^*| = 2N, \tag{2.3}$$

where $\mathscr{N}$ is the set (1.1)

Cosine polynomials. We define

$$C(\mathscr{U};\alpha) = \sum_{u\in\mathscr{U}}\cos 2\pi u\alpha, \tag{2.4}$$

so that in particular,

$$C(\alpha) = C(\mathscr{N};\alpha). \tag{2.5}$$

We note that $C(2\mathscr{U};\alpha) = C(\mathscr{U};2\alpha)$, so that (for the purpose of proving (1.13)) we may assume

$$\mathscr{N} \text{ contains only even integers.} \tag{2.6}$$

§ 3. Simple lemmas involving exponential sums. We write

$$F(\alpha) = M+2C(\alpha) = M+\sum_{k\in\mathscr{N}^*}e(k\alpha), \tag{3.1}$$

where M is defined by (1.11), (1.12), and note that

$$F(\alpha)\geqslant 0 \quad \text{for all real } \alpha. \tag{3.2}$$

We use g to denote functions of type

$$g(\alpha) = \sum_{j\in\mathscr{J}}c_j e(j\alpha), \tag{3.3}$$

and introduce the notation

$$(g_1,g_2) = \int_0^1 g_1(\alpha)\overline{g_2(\alpha)}F(\alpha)\,d\alpha,$$

$$\|g\|^2 = (g,g).$$

To each $\mathscr{U}$ we associate the function $g = \varphi[\mathscr{U}]$, on the interval $0\leqslant\alpha\leqslant 1$, defined by

$$g(\alpha) = \varphi[\mathscr{U}](\alpha) = \sum_{u\in\mathscr{U}}e(u\alpha). \tag{3.4}$$

Lemma 1 below results from applying Schwarz's inequality to

$$\int_0^1 \{g(\alpha)(F(\alpha))^{1/2}\}\,(F(\alpha))^{1/2}\,d\alpha.$$

Lemmas 2 and 3 are trivial, and Lemma 4 is an immediate consequence of them.

Lemma 1. *If g is given by* (3.3), *then*

$$\|g\|^2\geqslant M^{-1}\Big|\sum_{j\in\mathscr{N}\cap\mathscr{J}}c_j\Big|^2.$$

Lemma 2. *We have for every $\mathscr{U}$,*

$$\|\varphi[\mathscr{U}]\|^2 = M|\mathscr{U}|+\sum_{k\in\mathscr{N}^*}r(\mathscr{U};k), \tag{3.5}$$

where $r(\mathscr{U};k)$ denotes the number of solutions u', u'' of

$$u'-u'' = k \qquad (u'\in\mathscr{U},\ u''\in\mathscr{U}). \tag{3.6}$$

COROLLARY.

$$\|\varphi[\mathscr{U}]\|^2 \leqslant (M-1)|\mathscr{U}| + |\mathscr{U}|^2.$$

LEMMA 3. *If $\mathscr{V}$, $\mathscr{W}$ satisfy $\mathscr{V}-\mathscr{W} \subset \mathscr{N}$, then*

$$(\varphi[\mathscr{V}], \varphi[\mathscr{W}]) = (\varphi[\mathscr{W}], \varphi[\mathscr{V}]) = |\mathscr{V}| \cdot |\mathscr{W}|.$$

LEMMA 4. *If $\mathscr{V}-\mathscr{W} \subset \mathscr{N}$ and $|\mathscr{V}| = |\mathscr{W}|$, then*

$$\|\varphi[\mathscr{V}] - \varphi[\mathscr{W}]\|^2 < 2M|\mathscr{V}|.$$

Proof. This follows at once from Lemma 2 Corollary and Lemma 3, in view of the identity

$$\|g_1 - g_2\|^2 = \|g_1\|^2 - (g_1, g_2) - (g_2, g_1) + \|g_2\|^2.$$

§ 4. The two basic lemmas. The results of the previous section are required for the sole purpose of establishing the following two lemmas, upon which all the remaining work will be based.

LEMMA 5. *Suppose that $\mathscr{U} \subset \mathscr{N}$ and $|\mathscr{U}| \geqslant 2M^2$. Denote by $r(k) = r(\mathscr{U}; k)$ the number of solutions u', u'' of* (3.6). *Then*

$$\sum_{k \in \mathscr{N}^*} r(k) \geqslant (2M)^{-1}|\mathscr{U}|^2. \tag{4.1}$$

Proof. Applying Lemma 1 with $g = \varphi[\mathscr{U}]$, we obtain (in view of (3.5))

$$M|\mathscr{U}| + \sum_{k \in \mathscr{N}^*} r(k) \geqslant M^{-1}|\mathscr{U}|^2.$$

Since $M \leqslant \frac{1}{2}M^{-1}|\mathscr{U}|$, this yields (4.1).

LEMMA 6. *Suppose $\mathscr{V} \subset \overline{\mathscr{N}}$, $\mathscr{W} \subset \mathscr{N}$, $\mathscr{V}-\mathscr{W} \subset \mathscr{N}$ and $|\mathscr{V}| = |\mathscr{W}|$. Then $|\mathscr{V}| < 2M^2$.*

Proof. On applying Lemma 1 with $c_j = 1$ or -1 according as j lies in $\mathscr{V}$ or $\mathscr{W}$, we obtain

$$\|\varphi[\mathscr{V}] - \varphi[\mathscr{W}]\|^2 \geqslant M^{-1}|\mathscr{V}|^2.$$

Hence Lemma 4 yields $2M|\mathscr{V}| > M^{-1}|\mathscr{V}|^2$, which is equivalent to the result asserted.

§ 5. Structure of the proof of (1.13). The two basic lemmas in the previous section are of course a consequence of the relationship between M and $\mathscr{N}$ inherent in (1.11) and (1.12). The deduction of (1.13) from these lemmas will however be independent of this relationship; we shall make no further reference to the definition of the natural number M. In this sense the remainder of the work will be independent of the original problem.

In this section we deduce (1.13) from Lemmas A and B below; these lemmas will in turn be deduced from the two basic lemmas in the final sections. But first we introduce a further concept.

Paradoxical sets. The set $\mathscr{A}$ will be said to be *paradoxical* if it has the following three properties.

(i) $\mathscr{A}$ is symmetric with centre of symmetry in $\overline{\mathscr{A}}$ (so that, in particular, the centre of symmetry is a natural number).

(ii) $|\mathscr{A}| \geqslant 10M^4$.

(iii) Corresponding to every subset $\mathscr{B}$ of $\mathscr{A}$, with $|\mathscr{B}| \leqslant 2M^2+1$, there corresponds a set $\mathscr{S} = \mathscr{S}(\mathscr{B})$ such that $|\mathscr{S}^*| = 2M^2$ and $\mathscr{B} + \mathscr{S}^* \subset \mathscr{N}$.

LEMMA A. *Suppose that*

$$(2^3M)^{2^t} < N^{1/4}. \tag{5.1}$$

Then there exist d, $\mathscr{X}$, $\mathscr{T}$ such that

$$|\mathscr{T}^*| = 2^t, \tag{5.2}$$

$$|\mathscr{X}^*| \geqslant 10M^4, \tag{5.3}$$

$$d + \mathscr{X}^* + \mathscr{T}^* \subset \mathscr{N} \tag{5.4}$$

(*so that, in particular $d + \mathscr{X}^*$ contains only positive integers*).

We remark that if

$$2^t \geqslant 2M^2, \tag{5.5}$$

then we can select a subset $\mathscr{S}^*$ of $\mathscr{T}^*$ having exactly $2M^2$ elements. In this case the conditions (5.2), (5.3), (5.4) imply that the set $d + \mathscr{X}^*$ is paradoxical (indeed, for condition (iii), we can choose the same set $\mathscr{S}$ for all $\mathscr{B}$, which is not possible for general paradoxical sets).

COROLLARY TO LEMMA A. *If there exists a natural number t satisfying both* (5.1) *and* (5.5), *then there exists a paradoxical set.*

LEMMA B. *If the set $\mathscr{A}_1$ is paradoxical and c is the centre of symmetry of $\mathscr{A}_1$, then the set $\mathscr{A}_2 = c + \mathscr{A}_1$ is also paradoxical.*

Repeated application of Lemma B shows that the sets $\mathscr{A}_{m+1} = 2^{m-1}c + \mathscr{A}_m$ are paradoxical for all natural numbers m. But this leads to a contradiction for large m; for condition (iii) implies that the centre of symmetry of a paradoxical set is less than the greatest element of the set $\mathscr{N}$.

COROLLARY TO LEMMA B. *Paradoxical sets cannot exist.*

It is clear that the two corollaries above are inconsistent if there exists a natural number t satisfying both (5.1) and (5.5). But if (1.13) were false, the t defined by

$$2M^2 \leqslant 2^t < 4M^2$$

would be such a number. Thus Lemmas A and B together imply (1.13).

§ 6. Proof of Lemma A.

LEMMA 7. *Suppose* $\mathscr{U} \subset \mathscr{N}$ *and that*

$$|\mathscr{U}| \geqslant \max(2M^2, 4MN^{1/2}). \tag{6.1}$$

Then there exist l, $\mathscr{X}$ *such that*

$$l + \mathscr{X}^* \subset \mathscr{U}, \quad |\mathscr{X}^*| \geqslant 2^{-4}N^{-1}M^{-2}|\mathscr{U}|^2. \tag{6.2}$$

Proof. Let $R(k) = R(\mathscr{U}; k)$ denote the number of solutions of

$$u' + u'' = k \quad (u' \in \mathscr{U}, u'' \in \mathscr{U}). \tag{6.3}$$

Since the relation $u_1' + u_1'' = u_2' + u_2''$ can be rewritten in the form $u_1' - u_2'' = u_2' - u_1''$, we have

$$\sum_{k=2}^{\infty} R^2(k) = \sum_{k=-\infty}^{\infty} r^2(k) \geqslant \sum_{k \in \mathscr{N}^*} r^2(k),$$

where $r(k)$ is the function featuring in Lemma 5. But, by (4.1) and Cauchy's inequality,

$$2N \sum_{k \in \mathscr{N}^*} r^2(k) \geqslant \{(2M)^{-1}|\mathscr{U}|^2\}^2.$$

Hence

$$2^{-3}N^{-1}M^{-2}|\mathscr{U}|^4 \leqslant \sum_{k=2}^{\infty} R^2(k) \leqslant |\mathscr{U}|^2 \max_k R(k),$$

in view of

$$\sum_{k=2}^{\infty} R(k) = |\mathscr{U}|^2.$$

Since $\mathscr{N}$ and hence $\mathscr{U}$ contains only *even* integers (see (2.6)), it follows that there exists $k_0 = 2l$ such that

$$R(2l) \geqslant 2^{-3}N^{-1}M^{-2}|\mathscr{U}|^2 \geqslant 2(2^{-5}N^{-1}M^{-2}|\mathscr{U}|^2) + 1.$$

For this l, the number of solutions of

$$u' + u'' = 2l, \quad u' > u'' \tag{6.4}$$

is at least $2^{-5}N^{-1}M^{-2}|\mathscr{U}|^2$. Let $\mathscr{Y}$ be the set of all those elements u' of $\mathscr{U}$ to which there corresponds an element u'' satisfying (6.4), and write $\mathscr{X} = -l + \mathscr{Y}$. The l, $\mathscr{X}$ thus constructed obviously satisfy (6.2).

In the following lemma $\mathfrak{S}^*$ denotes a non-empty finite set of integers, satisfying $-\mathfrak{S}^* = \mathfrak{S}^*$; but we *admit* the possibility $0 \in \mathfrak{S}^*$ (and have avoided using a script letter for this reason).

LEMMA 8. *Suppose* p, $\mathscr{U}$, $\mathfrak{S}^*$ *are such that*

$$\mathscr{U} \subset \mathscr{N}, \quad |\mathscr{U}| \geqslant \max(2M^2, 2^3M|\mathfrak{S}^*|^2), \tag{6.5}$$

$$(p-1) + \mathscr{U} + \mathfrak{S}^* \subset \mathscr{N}. \tag{6.6}$$

Then there exist q, $\mathscr{V}$, $\mathscr{T}^*$, *with* $\mathscr{T}^* = 2|\mathfrak{S}^*|$, *such that*

$$\mathscr{V} \subset \mathscr{N}, \quad |\mathscr{V}| > (2^3NM)^{-1}|\mathscr{U}|^2, \tag{6.7}$$

$$(q-1) + \mathscr{V} + \mathscr{T}^* \subset \mathscr{N}. \tag{6.8}$$

Proof. Let $\mathscr{N}_1$ consist of all those elements of $\mathscr{N}$ which do not lie in the set $\mathfrak{S}^* - \mathfrak{S}^*$, and let $r(k) = r(\mathscr{U}; k)$ be the function featuring in Lemma 5. Since $|\mathfrak{S}^* - \mathfrak{S}^*| \leqslant |\mathfrak{S}^*|^2$ and $r(k) \leqslant |\mathscr{U}|$ always, we have by (6.5) and (4.1) (noting that $r(-k) = r(k)$)

$$\sum_{k \in \mathscr{N}_1} r(k) \geqslant (2^2M)^{-1}|\mathscr{U}|^2 - |\mathfrak{S}^*|^2|\mathscr{U}| \geqslant (2^3M)^{-1}|\mathscr{U}|^2.$$

Since $\mathscr{N}_1$ contains only even integers (see (2.6)), it follows that there exists h such that $2h \notin \mathfrak{S}^* - \mathfrak{S}^*$ and

$$r(2h) \geqslant (2^3NM)^{-1}|\mathscr{U}|^2. \tag{6.9}$$

We take

$$\mathscr{T}^* = (-h - \mathfrak{S}^*) \cup (h + \mathfrak{S}^*) = (-h + \mathfrak{S}^*) \cup (h + \mathfrak{S}^*);$$

and note that the requirement $|\mathscr{T}^*| = 2|\mathfrak{S}^*|$ is satisfied because $2h$ is not an element of $\mathfrak{S}^* - \mathfrak{S}^*$.

Let $\mathscr{V}$ consist of those elements u'' of $\mathscr{U}$ to which there correspond elements u' satisfying (3.6) with $k = 2h$. Then, in view of (6.9),

$$\mathscr{V} \subset \mathscr{U}, \quad 2h + \mathscr{V} \subset \mathscr{U}; \quad |\mathscr{V}| \geqslant (2^3NM)^{-1}|\mathscr{U}|^2.$$

Hence, on chosing $q = p + h$, all the assertions of the lemma are justified.

Completion of the proof of Lemma A. We write

$$m_k = (2^3M)^{2^k} \quad (k = 0, 1, 2, \ldots), \tag{6.10}$$

so that

$$m_0 = 2^3M, \quad m_{k+1} = m_k^2 \quad (k = 0, 1, 2, \ldots).$$

Since the natural number t satisfies (5.1), we have

$$(2^3M)^2 \leqslant m_t < N^{1/4}. \tag{6.11}$$

For each $k = 0, 1, \ldots, t$, we shall construct the entities

$$p_k, \quad \mathscr{V}_k, \quad \mathfrak{S}_k^*, \tag{6.12}$$

to satisfy

$$|\mathfrak{S}_k^*| = 2^k, \tag{6.13}$$

$$\mathscr{V}_k \subset \mathscr{N}, \quad |\mathscr{V}_k| \geqslant 2^3 N M m_k^{-1}, \tag{6.14}$$

$$(p_k - 1) + \mathscr{V}_k + \mathfrak{S}_k^* \subset \mathscr{N}. \tag{6.15}$$

We remark that (6.13), (6.14) automatically ensure that

$$|\mathscr{V}_k| \geqslant 2^3 M^2 |\mathfrak{S}_k^*|^2; \tag{6.16}$$

for

$$2^3 M^2 (2^k)^2 \leqslant M m_k \leqslant M m_t < M N^{1/4},$$

whilst

$$2^3 N M m_k^{-1} > M N m_t^{-1} > M N^{3/4}.$$

We choose

$$p_0 = 1, \quad \mathscr{V}_0 = \mathscr{N}, \quad \mathfrak{S}_0^* = \{0\} \tag{6.17}$$

(where $\{0\}$ consists of the single element 0), and note that this choice satisfies the requirements (6.13), (6.14), (6.15) for $k = 0$.

Now suppose that for a given k, satisfying $0 \leqslant k < t$, the entities (6.12) have already been constructed. We apply Lemma 8 with

$$p = p_k, \quad \mathscr{U} = \mathscr{V}_k, \quad \mathfrak{S}^* = \mathfrak{S}_k^*; \tag{6.18}$$

the first assertion of (6.14) together with (6.15) and (6.16) ensure that the premises of the lemma are satisfied. We use the resulting q, $\mathscr{V}$, $\mathscr{T}$ to define

$$p_{k+1} = q, \quad \mathscr{V}_{k+1} = \mathscr{V}, \quad \mathfrak{S}_{k+1}^* = \mathscr{T}^*. \tag{6.19}$$

Since

$$(2^3 N M)^{-1} \{2^3 N M m_k^{-1}\}^2 = 2^3 N M m_{k+1}^{-1},$$

the properties of q, $\mathscr{V}$, $\mathscr{T}$ (as stated in Lemma 8) ensure that, with the choice (6.19), the relations (6.13), (6.14), (6.15) remain valid when k is replaced by $k+1$. This inductive step enables us (starting from (6.17)) to make the successive choices for (6.12) up to $k = t$.

We now apply Lemma 7 with $\mathscr{U} = \mathscr{V}_t$; this choice is admissible in view of

$$\max(2M^2, 4MN^{1/2}) \leqslant \max(m_t, 4MN^{1/2}) \leqslant 4MN^{1/2},$$

$$|\mathscr{V}_t| \geqslant 2^3 N M m_t^{-1} > 8 M N^{3/4}.$$

On writing

$$d = (p_t - 1) + l, \quad \mathscr{T}^* = \mathfrak{S}_t^*,$$

the l, $\mathscr{X}^*$ resulting in this application of Lemma 7 provide the d, $\mathscr{X}^*$ which, together with $\mathscr{T}^*$, have all the properties asserted in Lemma A; for

$$2^{-4} N^{-1} M^{-2} |\mathscr{V}_t|^2 \geqslant 2^2 N m_t^{-2} > 4 m_t^2 \geqslant 4 (2^3 M)^4,$$

so that the condition $|\mathscr{X}^*| \geqslant 10 M^4$ is satisfied.

§ 7. Proof of Lemma B. We recall that a paradoxical set $\mathscr{A}$ has the properties (i), (ii), (iii) stated in § 5.

LEMMA 9. *Let $\mathscr{A}$ be paradoxical and let a_0 be an element of $\mathscr{A}$. Then at most $2M^2 - 1$ of the elements of $a_0 + \mathscr{A}$ lie in $\overline{\mathscr{N}}$.*

Proof. Suppose that the conclusion of the lemma is false. Then there exists a subset $\mathscr{E}$ of $\mathscr{A}$ such that

$$|\mathscr{E}| = 2M^2, \quad a_0 + \mathscr{E} \subset \overline{\mathscr{N}}. \tag{7.1}$$

Applying the property (iii) of paradoxical sets, with

$$\mathscr{B} = \{a_0\} \cup \mathscr{E},$$

(where $\{a_0\}$ consists of the single element a_0), we obtain an $\mathscr{S}$ such that

$$|\mathscr{S}^*| = 2M^2, \quad a_0 + \mathscr{S}^* \subset \mathscr{N}, \quad \mathscr{E} + \mathscr{S}^* \subset \mathscr{N}. \tag{7.2}$$

But now, since

$$(a_0 + \mathscr{E}) - (a_0 + \mathscr{S}^*) = \mathscr{E} - \mathscr{S}^* = \mathscr{E} + \mathscr{S}^*,$$

the relations (7.1), (7.2) contradict Lemma 6 with $\mathscr{V} = a_0 + \mathscr{E}$, $\mathscr{W} = a_0 + \mathscr{S}^*$.

Completion of the proof of Lemma B. The properties (i) and (ii) of the paradoxical set $\mathscr{A}_1$ are invariant under the translation c. Thus it suffices to demonstrate that given a subset $\mathscr{B}$ of $c + \mathscr{A}_1$, with $|\mathscr{B}| \leqslant 2M^2 + 1$, we can construct a set $\mathscr{S}^*$ such that $|\mathscr{S}^*| = 2M^2$ and $\mathscr{B} + \mathscr{S}^* \subset \mathscr{N}$. Let

$$c + a^{(\nu)} \quad (\nu = 1, 2, \ldots, |\mathscr{B}|)$$

be the elements of the given set $\mathscr{B}$.

Since c is the centre of symmetry of $\mathscr{A}_1$ (and $\mathscr{A}_1$ has property (ii)), we can write

$$\mathscr{A}_1 = c + \mathscr{X}^*, \quad \text{where} \quad |\mathscr{X}^*| \geqslant 10 M^4.$$

For each ν, we apply Lemma 9 with $\mathscr{A} = \mathscr{A}_1$, $a_0 = a^{(\nu)}$. This tells us that at most $2M^2 - 1$ elements of the set

$$a^{(\nu)} + \mathscr{A}_1 = (c + a^{(\nu)}) + \mathscr{X}^*$$

lie in $\overline{\mathscr{N}}$; thus the set

$$(\mathscr{X}^*) \cap (-c - a^{(\nu)} + \overline{\mathscr{N}}) \tag{7.3}$$

contains at most $2M^2 - 1$ elements. Taking $\mathscr{E}_\nu^*$ to be the union of the set (7.3) and its reflection in 0, we have $|\mathscr{E}_\nu^*| \leqslant 2(2M^2 - 1)$ for each ν, and hence (since $|\mathscr{B}| \leqslant 2M^2 + 1$)

$$|\mathscr{X}^*| - \sum_\nu |\mathscr{E}_\nu^*| \geqslant 10 M^4 - 2(4M^4 - 1) > 2M^2.$$

We can therefore select a subset $\mathscr{S}^*$ of $\mathscr{X}^*$, satisfying $|\mathscr{S}^*| = 2M^2$ and containing no elements of any of the sets

$$-c-a^{(\nu)}+\overline{\mathscr{N}} \quad (\nu = 1, 2, \ldots, |\mathscr{B}|).$$

This last property is equivalent to the desired condition $\mathscr{B}+\mathscr{S}^* \subset \mathscr{N}$.

References

[1] S. Chowla, *The Riemann zeta and allied functions*, Bull. American Math. Soc. 58 (1952), pp. 287–305.

[2] — *Some applications of a method of A. Selberg*, J. Reine Angew. Math. 217 (1965), pp. 128–132.

[3] Paul J. Cohen, *On a conjecture of Littlewood and idempotent measures*, American J. Math. 82 (1960), pp. 191–212.

[4] H. Davenport, *On a theorem of P. J. Cohen*, Mathematika 7 (1960), pp. 93–97.

[5] G. H. Hardy and J. E. Littlewood, *A new proof of a theorem on rearrangements*, J. London Math. Soc. 23 (1948), pp. 163–168.

[6] Uchiyama, née Katayama, Miyoko; Uchiyama, Saburô, *On the cosine problem*, Proc. Japan Acad. 36 (1960), pp. 475–479.

[7] Uchiyama, Saburô, *À propos d'un problème de M. J. E. Littlewood*, C. R. Acad. Sci. Paris 260 (1965), pp. 2675–2678.

[8] R. Salem, *On a problem of Littlewood*, American J. Math. 77 (1955), pp. 535–540.

IMPERIAL COLLEGE
London, S.W. 7

Received on 25. 6. 1972 (305)

ACTA ARITHMETICA
XXIV (1973)

On gaps between numbers with a large prime factor

by

K. Ramachandra and T. N. Shorey (Bombay)

In honour of Professor C. L. Siegel on his 75th birthday

§ 1. Introduction. Let k be a fixed natural number and $n_1, n_2, n_3, \ldots$ all the natural numbers (in the increasing order) which have at least one prime factor exceeding k. It is easy to see that

$$f(k) = \max_{i=1,2,\ldots} (n_{i+1}-n_i)$$

is finite. P. Erdös was the first to give the estimate $f(k) = O\left(\frac{k}{\log k}\right)$ ([3]) which goes beyond the trivial estimate $f(k) = O(k)$. (The problem of the O-constant here was also difficult and a non-trivial value for the O-constant was obtained by Sylvester and Schur independently. See [2].) His argument gives that the upper limit of $f(k)\left(\frac{k}{\log k}\right)^{-1}$ as k tends to infinity does not exceed 3. Even the lowering of this constant 3 seemed difficult and Erdös remarked in [3] that the proof of $f(k) < \pi(k)$ for all large k would prove to be considerably difficult (it is now known by Tijdeman's result to be mentioned immediately). The first author of the present paper reduced 3 to 1 in [5]. Further he made some partial progress in the direction of reducing this constant to $\frac{1}{2}$, in [6]. A part of the proof in [6] depended on an adaptation of the Roth–Halberstam method (see [3] of [6]), and an ingeneous adaptation of this method was made by Tijdeman [11] who reduced 1 to $\frac{1}{2}$. The other part of [6] depended on Baker's methods and in this paper we develop this method and use the results of [5] and [7] to prove the following

Main Theorem. *We have*

$$f(k) = O\left(\frac{k}{\log k}\left(\frac{\log\log\log\log k}{\log\log\log k}\right)^{1/2}\right)$$

where the O-constant is computable (but it is tedious to do so).