ON SETS OF NATURAL NUMBERS WHOSE DIFFERENCE SET CONTAINS NO SQUARES

JÁNOS PINTZ, W. L. STEIGER AND ENDRE SZEMERÉDI

ABSTRACT

We show that if a sequence $\mathscr{A}$ of natural numbers has no pair of elements whose difference is a positive square, then the density of $\mathscr{A} \cap \{1, \ldots, n\}$ is $O(1/\log n)^{c_n})$, $c_n \to \infty$. This improves previous results which showed that the density converges to zero, but at a slower rate. We use a technique based on the method of Hardy and Littlewood together with a combinatorial result that is of independent interest. The approach may be useful for other problems in additive number theory.

1. *Introduction*

In this paper we study the density of strictly monotone increasing sequences of natural numbers whose difference set does not contain any positive square. If $\mathscr{A}$ is an increasing sequence of natural numbers, write $\mathscr{A}_n$ for $\mathscr{A} \cap \{1, \ldots, n\}$, $\sigma = |\mathscr{A}_n|$ for the cardinality, and $\mathrm{d}(\mathscr{A}_n) = \sigma/n$ for the density of $\mathscr{A}_n$. The asymptotic density of $\mathscr{A}$ is the limit, if it exists, of $\mathrm{d}(\mathscr{A}_n)$.

Earlier density results are due to Furstenberg [2] and to Sárközy [3, 4, 5]. They showed that if $\mathscr{A} - \mathscr{A}$ does not contain a positive square, it cannot have a positive density. In fact if $\mathrm{d}(\mathscr{A}) > 0$, then $\mathscr{A}_n - \mathscr{A}_n$ will have more than $c\sqrt{n}$ squares for infinitely many values of $n, c > 0$. Sárközy [4] later showed that if $\mathscr{A}_n - \mathscr{A}_n$ contains no positive squares then for large n, $\mathrm{d}(\mathscr{A}_n) = O((\log\log n)^{\frac{2}{3}}/(\log n)^{\frac{1}{3}})$. Our main result is the following.

THEOREM 1. *There exist positive constants c_0 and c_1 such that for any sequence $\mathscr{A}$, if $n > c_1$ and $\mathscr{A}_n - \mathscr{A}_n$ contains no positive squares, then*

$$\mathrm{d}(\mathscr{A}_n) \leqslant c_0/(\log n)^{(\log\log\log\log n)/12}. \tag{1}$$

The argument uses the method of Hardy and Littlewood (see [6], for example) together with a combinatorial construction in which, if $\mathscr{A}_n$ has a square-free difference set, we can find a more concentrated subset with the same property. This already allows us to infer that the density is $O((\log\log n)^{20}/\log n)$. Then we employ an iteration scheme in which, at each step, we find more values where the Fourier transform of the sequence is large. Parseval's identity applies to limit the density to the bound given in (1).

Received 24 March 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*) 11P55.

The research of the first author was partially supported by the Hungarian National Foundation for Scientific Research, grant 1811.

2. *Preliminaries*

Write $a \mid b$ if a divides b and $a \nmid b$ otherwise; write $[x]$ for the integer part of x. We begin by articulating some properties possessed by the trigonometric series used in the method. As usual $e(\alpha)$ means $e^{2\pi i\alpha}$ and

$$\frac{1}{n}\sum_{t=0}^{n-1} e(at/n) = \begin{cases} 1 & \text{if } n \mid a, \\ 0 & \text{if } n \nmid a. \end{cases} \tag{2}$$

Take n to be a large integer and write $L = \log n$ and $l = \log\log n$. To simplify notation, we write $\mathscr{A}$ for $\mathscr{A}_n$. Thus from now on given n, we denote by $\mathscr{A}$ the sequence $1 \leqslant a_1 < \ldots < a_\sigma \leqslant n$ of length $|\mathscr{A}| = \sigma \leqslant n$ and density $\gamma = \sigma/n \leqslant 1$.

A basic feature of the method is the Fourier transform of the characteristic function of $\mathscr{A}$,

$$F(\alpha) \equiv e(a_1\alpha) + \ldots + e(a_\sigma\alpha) \equiv \sum_{a_t \in \mathscr{A}} e(a_t\alpha). \tag{3}$$

The Parseval identity applied to F shows that

$$\sum_{t=0}^{n-1} |F(t/n)|^2 = \sigma n$$

and, if it is applied to the function

$$f(\alpha) = F(\alpha)/\sigma,$$

we see that

$$\sum_{t=0}^{n-1} |f(t/n)|^2 = n/\sigma = \gamma^{-1}. \tag{4}$$

Write $n_1 = \frac{1}{2}n$, and consider the following functions:

$$\left.\begin{aligned} &S(\alpha) = \sum_{g^2 \leqslant n_1} e(g^2\alpha)\,2g/\sqrt{n_1}, \qquad S(\alpha, m) = \sum_{g \leqslant m} e(g^2\alpha)\,2g, \\ &s(\alpha) = S(\alpha)/[\sqrt{n_1}]; \end{aligned}\right\} \tag{5}$$

all sums are over positive integers unless stated otherwise. Now S is a weighted Fourier transform for the squares less than n_1; weighting g^2 by $2g/\sqrt{n_1}$ makes the weighted squares in $[0, \sqrt{n_1}]$ uniform. We shall develop some bounds on S and s for certain α.

First, we consider the case where α is rational: $\alpha = a/q$, $(a,q) = 1$, $q \neq 1$. Define

$$B(a/q, m) = \sum_{g \leqslant m} e(g^2 a/q)$$

and $B_a(q) = B(a/q, q)$. If $m \leqslant q$, $B(a/q, m) \ll (q\log q)^{\frac{1}{2}}$ by [1, Lemma 3], where, as usual, if f and g are functions and g has only non-negative real values, $f \ll g$ means $|f| = O(g)$. From Abel's inequality,

$$S(a/q, m) \ll m \max\{B(a/q, j), j \leqslant m\} \ll m(q\log q)^{\frac{1}{2}}.$$

Therefore, if $q \geqslant \sqrt{n_1}$,

$$S(a/q) \ll (q\log q)^{\frac{1}{2}}. \tag{6}$$

Otherwise if $q < m$, write $m = hq + l$, $h \geqslant 1$. Using Abel's inequality and the previous estimate for $B(a/q, m)$ we obtain

$$\begin{aligned} S(a/q,m) &= \sum_{g \leqslant hq+l} e(g^2 a/q)\{2q[(g-1)/q] + 2g - 2q[(g-1)/q]\} \\ &= \sum_{j=0}^{h-1} 2jqB_a(q) + 2hqB(a/q,l) + O(hq(q\log q)^{\frac{1}{2}}) \\ &= h(h-1)\,qB_a(q) + O(hq(q\log q)^{\frac{1}{2}}) \\ &= (m+O(q))\,(m/q+O(1))\,B_a(q) + O(m(q\log q)^{\frac{1}{2}}) \\ &= B_a(q)\,m^2/q + O(m(q\log q)^{\frac{1}{2}}). \end{aligned}$$

This means that

$$\left.\begin{aligned} S(a/q) &= B_a(q)\sqrt{n_1}/q + O((q\log q)^{\frac{1}{2}}), \\ s(a/q) &= B_a(q)/q + O(((q\log q)/n)^{\frac{1}{2}}). \end{aligned}\right\} \tag{7}$$

Now we consider the case where α is a fixed distance η from a specific rational; namely, take $\alpha = a/q + \eta$, $(a,q) = 1$. Clearly

$$\begin{aligned} S(\alpha,m) &= \sum_{g \leqslant m} e(ag^2/q)\,2ge(g^2\eta) = \sum_{g \leqslant m} \{S(a/q,g) - S(a/q,g-1)\}\,e(g^2\eta) \\ &= \sum_{g \leqslant m} S(a/q,g)\{e(g^2\eta) - e(\eta(g+1)^2)\} + S(a/q,m)\,e(\eta(m+1)^2). \end{aligned}$$

Similarly we again use partial summation to calculate

$$\begin{aligned} B_a(q)\,S(\eta,m)/q = q^{-1}B_a(q) \sum_{g \leqslant m} g(g+1)\{e(g^2\eta) - e(\eta(g+1)^2)\} \\ + q^{-1}B_a(q)\,m(m+1)\,e(\eta(m+1)^2). \end{aligned}$$

If we subtract this equation from the preceding one and use the fact that

$$S(a/q,g) = g(g+1)\,B_a(q)/q + O(g(q\log q)^{\frac{1}{2}}),$$

we see that

$$\begin{aligned} S(\alpha,m) - B_a(q)\,S(\eta,m)/q &= O\left(m(q\log q)^{\frac{1}{2}}\left\{1 + \sum_{g=1}^{m} |e(g^2\eta) - e((g+1)^2\eta)|\right\}\right) \\ &= O(m(q\log q)^{\frac{1}{2}}(1 + |\eta|m^2)), \end{aligned}$$

which implies that

$$\left.\begin{aligned} S(\alpha) &= B_a(q)\,S(\eta)/q + O((q\log q)^{\frac{1}{2}}(1+|\eta|n)) \\ s(\alpha) &= B_a(q)\,s(\eta)/q + O(((q\log q)/n)^{\frac{1}{2}}(1+|\eta|n)). \end{aligned}\right\} \tag{8}$$

When $\eta = 0$, this result agrees with (7) because $S(0) = \sqrt{n_1}$.

We can say more if $\eta \neq 0$ is small. Suppose that $\eta = h/n$, $\frac{1}{10} < |h| < T$, h not necessarily an integer, T a large number that will be specified later. From (5),

$$\begin{aligned} s(\eta)[\sqrt{n_1}]/\sqrt{n_1} &= \frac{2}{n} \sum_{g^2 \leqslant \frac{1}{2}n} e(g^2h/n)\,2g \\ &= \frac{2}{n} \sum_{k=0}^{[\frac{1}{2}h]-1} \sum_{j=0}^{T-1} \sum e(g^2h/n)\,2g + \frac{2}{n} \sum_{n[\frac{1}{2}h]/h < g^2 \leqslant \frac{1}{2}n} e(g^2h/n)\,2g, \end{aligned} \tag{9}$$

where the third sum is over $\{g : n(k+j/T)/h < g^2 \leqslant n(k+(j+1)/T)/h\}$. Breaking up

the sum over g^2 in this way, g^2h/n is an integer plus j/T plus a small remainder and therefore the first term in (9), the triple sum, reduces to

$$\frac{2}{n}\sum_{k=0}^{[\frac{1}{2}h]-1}\sum_{j=0}^{T-1} e(j/T)\{\textstyle\sum 2g\}+O(n^{-1})\sum_{g^2\leqslant\frac{1}{2}n} 2g/T.$$

The last sum in (9) can be empty. It may be written as $O(I/h)$, where I is 1 if h is not an even integer, and 0 otherwise. Using the estimate

$$\sum_{g=\sqrt{A}}^{\sqrt{B}} 2g = \int_{\sqrt{A}}^{\sqrt{B}} 2t\,dt+O(\sqrt{B}) = B-A+O(\sqrt{B}),$$

we obtain

$$s(\eta) = \frac{2}{n}\sum_{k=0}^{[\frac{1}{2}h]-1}\sum_{j=0}^{T-1}\frac{ne(j/T)}{(hT)}+O(hT\sqrt{n}/n)+O(1/T)+O(I/h).$$

The inner sum is zero, in view of (2), so if we take $T=n^{\frac{1}{8}}$ it follows that

$$s(h/n) = \begin{cases} O(1/n^{\frac{1}{8}}) & \text{if } h \text{ is an even integer,} \\ O(1/|h|) & \text{if } h \text{ is not an even integer.} \end{cases} \tag{10}$$

REMARK. Davenport and Heilbronn [1] analysed the unweighted version of S in (5) and obtained results similar to the foregoing; for example (8) holds in both cases. However without weighting (10) would only give $s(h/n)=O(|h|^{-\frac{1}{2}})$, and this is not sufficient for our purposes later on.

We complete this section with a result that is basic in the proof of Theorem 1. Define

$$\tau(q,\eta) = \bigcup_{a\leqslant q:(a,q)=1}\left(\frac{a}{q}-\eta,\frac{a}{q}+\eta\right), \qquad C_\eta(q) = \sum_{\substack{0<t\leqslant n-1\\ t/n\in\tau(q,\eta)}} f^2(t/n).$$

An important ingredient is the property of $C_\eta(q)$ revealed in the following combinatorial result.

MAIN LEMMA. *Take q and η such that $q>1$ and $\eta^{-1}\leqslant\gamma n$, and write $D=[1/(q^2\eta L^2)]$. If $\mathscr{A}$ has density γ and $\mathscr{A}-\mathscr{A}$ has no positive squares, then we can construct a set $\mathscr{A}'\subset[1,D]$ with density $\mathrm{d}(\mathscr{A}')\geqslant(1+|C_\eta(q)|)(1+O(L^{-1}))\gamma$ and $\mathscr{A}'-\mathscr{A}'$ contains no positive square.*

Proof. Write $B=[L]D$. We start with the set $\mathscr{B}=\{b_\nu=q^2\nu: 1\leqslant\nu\leqslant B\}$ of multiples of q^2 and the shorter set $\mathscr{D}=\{b_\nu\in\mathscr{B}: 1\leqslant\nu\leqslant D\}$.

We count the number of solutions, J, of the congruence

$$a_i-a_j\equiv b_\nu-b_\mu(\mathrm{mod}\,n), \qquad a_i,a_j\in\mathscr{A},\ b_\nu,b_\mu\in\mathscr{B}, \tag{11}$$

using the function

$$g(\alpha) = B^{-1}\sum_{\nu=1}^{B} e(b_\nu\alpha).$$

If $|t/n-a/q|<\eta$, then $b_\nu t/n = aq\nu+O(Bq^2\eta)$, which implies that $e(b_\nu t/n)-1 = O(L^{-1})$. Therefore if $t/n\in\tau(q,\eta), g(t/n) = 1+O(L^{-1})$ and using (2) we obtain

$$J = (\sigma^2B^2/n)\sum_{t=0}^{n-1} f(t/n)\overline{f(t/n)}\,g(t/n)\overline{g(t/n)} \tag{12}$$

$$\geqslant (\sigma^2B^2/n)(1+|C_\eta(q)|)(1+O(L^{-1})).$$

We now approximate J in a different way. For fixed u, $0<u\leqslant n-(D-1)q^2$, define

$$\mathscr{A}(u) = \{a_i\in\mathscr{A}: a_i = u+jq^2, 0\leqslant j\leqslant D-1\}$$

and $\sigma(u) = |\mathscr{A}(u)|$. Then $\sigma(u)$ counts the number of a_i that belong to the shorter progression of length D, beginning at u, with difference q^2. It will turn out that the average over the u is more than γD. This means that $\mathscr{A}$ is more concentrated in some arithmetic progression of length $D<B$. The lemma is proved by transforming this progression back into $[1,D]$.

First we count the number of solutions, J', of

$$a_i-a_j = b_\nu-b_\mu = (\nu-\mu)q^2\leqslant (B-1)q^2, \qquad a_i,a_j\in\mathscr{A}, b_\nu,b_\mu\in\mathscr{B}. \tag{13}$$

The integers from 1 to n may be decomposed into residue classes mod q^2 and we group the consecutive elements in the same class into non-overlapping blocks of length D. For example, a typical block for the residue class $r(\mathrm{mod}\,q^2)$ is the progression

$$H(r,k) = \{r+kDq^2, r+(kD+1)q^2,\ldots, r+((k+1)D-1)q^2\}.$$

If a_i and a_j satisfy (13), they must be in the same class and cannot differ by more than Bq^2; more precisely $a_i\in\mathscr{A}(kDq^2+r)$ and $a_j\in\mathscr{A}(mDq^2+r)$ for some r, $1\leqslant r\leqslant q^2$, and $|k-m|\leqslant[L]$. Equivalently,

$$D(|k-m|-1)<|a_i-a_j|/q^2 = |\nu-\mu|<D(|k-m|+1),$$

so if a_i and a_j satisfy (13) then there are $B-|a_i-a_j|/q^2$ choices for the pair (ν,μ); as $|k-m|\leqslant[L]$ the number of pairs lies between $B\{1-(|k-m|+1)/[L]\}$ and $B\{1-(|k-m|-1)/[L]\}$.

This observation allows us to write

$$J' = \sum_{r=1}^{q^2}\sum_{k=0}^{n/(q^2D)}\sigma(q^2Dk+r)\sum_{h=-[L]}^{[L]}\sigma(q^2D(k+h)+r)\,B\left(1-\frac{|h|}{[L]}+O(L^{-1})\right).$$

The first sum is over all the residue classes for a_i and a_j. The second and third enumerate all the a_i, a_j pairs in class $r(\mathrm{mod}\,q^2)$ that are in adjacent big blocks. The last expression covers the ν,μ pairs. If we write $N = \max(\sigma(u), u\leqslant n)$ then

$$J'\leqslant\sigma NB\sum_{h=-[L]}^{[L]}\left(1-\frac{|h|}{[L]}+O(L^{-1})\right) = \sigma NB([L]+O(1)). \tag{14}$$

A quadruple that satisfies the congruence in (11) must either obey the equation in (13) or the relation

$$a_i-a_j = b_\nu-b_\mu\pm n.$$

Let J'' denote the number of solutions to the above equation. Consider the plus case. Then the b differ by one of the following values: $0, -q^2, -2q^2,\ldots, -(B-1)q^2$. This implies at most Bq^2 choices for a_i, then at most N choices for a_j, and finally at most B choices for the pair of b_i, a total of at most NB^2q^2 choices. Since the minus case is the same, J'' is no more than

$$2NB^2q^2\leqslant 2NB/(\eta L)\leqslant 2\sigma NB/L.$$

Combining this with (12) and (14),

$$\sigma^2 B^2 n^{-1}(1+|C_\eta(q)|)(1+O(L^{-1})) \leqslant J \leqslant \sigma N B[L](1+O(L^{-1})).$$

This implies the existence of a set $\mathscr{A}(u)$ of size $N = \sigma(u)$,

$$N \geqslant \sigma B/(n[L])(1+|C_\eta(q)|)(1+O(L^{-1})) = \gamma D(1+|C_\eta(q)|)(1+O(L^{-1})). \tag{15}$$

We map $\mathscr{A}(u)$ linearly into $[1, D]$ by $a_i' = 1+(a_i-u)/q^2$ and obtain the set

$$\mathscr{A}' = \{j+1 : u+jq^2 \in \mathscr{A}(u)\}.$$

If $\mathscr{A}'-\mathscr{A}'$ contains squares, say $j-k = m^2$, then $(u+(j-1)q^2)-(u+(k-1)q^2) = (mq)^2$, but this is forbidden. Finally, $\mathscr{A}'$ satisfies the lemma because, from (15), it has the asserted density.

The proof of Theorem 1 will be accomplished by induction on n. If n is the first large integer for which (1) fails then the Main Lemma applies to give an upper bound on $|C_\eta(q)|$.

COROLLARY A. *Suppose that $\mathscr{A}$ is a set of integers less than or equal to n and that $\mathscr{A}-\mathscr{A}$ contains no positive squares. If* (1) *is false but for all $m < n$ it is true, then $C_\eta(q) \ll l^3/L$ if $\eta \leqslant Q/n$ and $q \leqslant Q$ for any $Q \leqslant e^{2l}$.*

Proof. The assumptions guarantee that $D \geqslant n/Q^4 = n^{1-4\beta}$, where we write $\beta = \log Q/\log n$ and note that $\beta \leqslant 2l^2/L$. Therefore, for $1 \leqslant k \leqslant l$,

$$\log^k D \geqslant (1-4\beta)^k \log^k n \geqslant (\log^k n)/(1+5k\beta) \geqslant (\log^k n)/(1+10l^3/L). \tag{16}$$

Write $\log_1 \equiv \log$ and $\log_{i+1} \equiv \log(\log_i)$. An easy calculation shows that $\log_4 n - \log_4 D = O(4\beta/l \log l)$ so that

$$(\log n)^{(\log_4 n - \log_4 D)/12} < 1 + l^3/L. \tag{17}$$

If $|C_\eta(q)| \geqslant 13l^3/L$ then the induction hypothesis and the Main Lemma imply that

$$\gamma \leqslant \frac{(1+O(L^{-1}))\,\mathrm{d}(\mathscr{A}')}{1+|C_\eta|} \leqslant \frac{c_0}{(1+12l^3/L)(\log D)^{\log_4 D/12}}$$

$$\leqslant \frac{c_0(1+10l^3/L)}{(1+12l^3/L)(\log n)^{\log_4 D/12}} < \frac{c_0}{(\log n)^{\log_4 n/12}};$$

the last line is a consequence of (17) and then (16) with $k = \log_4 D/12$. This contradiction proves the corollary.

In the next section we show that the Main Lemma is already strong enough to imply a bound of $(\log\log n)^{20}/\log n$ on the density of any sequence whose difference set has no non-trivial squares. This finding may be iterated to give the bound stated in Theorem 1. The details appear in the subsequent sections.

3. *The starting step*

We write $\mathscr{A}_1$ for $\mathscr{A} \cap \{1, \ldots, [\frac{1}{2}n]\}$, $\mathscr{A}_2$ for $\mathscr{A} \cap \{1+[\frac{1}{2}n], \ldots, n\}$, and, for $i = 1, 2$,

$$F_i(\alpha) = \sum_{a \in \mathscr{A}_i} e(\alpha a), \qquad f_i(\alpha) = F_i(\alpha)/\sigma$$

where, as always, we write $\sigma = |\mathscr{A}|$. Using (2) it is easy to verify that

$$\frac{1}{n}\sum_{t=0}^{n-1} F(t/n)\overline{F_1(t/n)}\,\overline{S(t/n)} = \sum_{\mathscr{S}_1}\frac{2g}{\sqrt{n_1}}, \qquad \frac{1}{n}\sum_{t=0}^{n-1} F(t/n)\overline{F_2(t/n)}\,S(t/n) = \sum_{\mathscr{S}_2}\frac{2g}{\sqrt{n_1}}, \quad (18)$$

where $\mathscr{S}_1 = \{g \leqslant \sqrt{n_1} : g^2 = a_t - a_j, a_t \in \mathscr{A}, a_j \in \mathscr{A}_1\}$ and $\mathscr{S}_2 = \{g \leqslant \sqrt{n_1} : g^2 = a_j - a_t, a_t \in \mathscr{A}, a_j \in \mathscr{A}_2\}$. Assuming that $\mathscr{A} - \mathscr{A}$ contains no positive squares, both sums in (18) are zero and we have

$$\sum_{t=0}^{n-1} f(t/n) f_i(t/n)\, s(t/n) = 0$$

and

$$\sum_{t=1}^{n-1} |f(t/n) f_i(t/n)\, s(t/n)| \geqslant |f(0) f_i(0)\, s(0)|,$$

$i = 1, 2$. We may take $f_i(0) \geqslant \frac{1}{4}$. If not, $\mathrm{d}(\mathscr{A}_i) > \frac{4}{3}\gamma$ and, roughly speaking, if this situation were iterated, we would have a bound of $1/n^{1-\varepsilon}$ in (1). A precise argument would follow the proof of Corollary A. Because $f(0) = s(0) = 1$, we now have

$$\sum_{t=1}^{n-1} |f(t/n) f_i(t/n)\, s(t/n)| \gg 1, \qquad i = 1, 2. \quad (19)$$

Using (4) we see that it is permissible to neglect all t in (19) for which $|s(t/n)| \leqslant \gamma/100$; they contribute no more than

$$0.01\gamma\left\{\sum_{t=0}^{n-1}|f(t/n)|^2 \sum_{t=0}^{n-1}|f_i(t/n)|^2\right\}^{\frac{1}{2}} \leqslant 0.01\gamma\{(\gamma^{-1})^2)\}^{\frac{1}{2}} = \tfrac{1}{100}.$$

In an analogous way we can neglect those terms in (19) for which $|f(t/n)|$ or $|f_i(t/n)| \leqslant \gamma^{\frac{3}{2}}/L$, since their contribution is no more than

$$(\gamma^{\frac{3}{4}}/L^{\frac{1}{2}})\left(\sum_{t=0}^{n-1}|f(t/n)|^2\right)^{\frac{1}{2}}\left(\sum_{t=0}^{n-1}(|f_i(t/n)|^{\frac{1}{2}})^4\right)^{\frac{1}{4}}\left(\sum_{t=0}^{n-1}|s(t/n)|^4\right)^{\frac{1}{4}}$$

$$\ll (\gamma^{\frac{3}{4}}/L^{\frac{1}{2}})(\gamma^{-1})^{\frac{1}{2}}(\gamma^{-1})^{\frac{1}{4}}(n^2 L/[\sqrt{n_1}]^4)^{\frac{1}{4}} = O((\gamma^{\frac{3}{4}}/L^{\frac{1}{2}})(\gamma^{-\frac{3}{4}})(L^{\frac{1}{4}})) = O(L^{-\frac{1}{4}});$$

here we use

$$\frac{1}{n}\sum_{t=0}^{n-1}|S(t/n)|^4 = \frac{1}{n}\sum\prod_{i=1}^{4} 2g_i/[\sqrt{n_1}] \leqslant \frac{16}{n}\sum_{m=1}^{n} r^2(m) = O(L),$$

where $r(m) = \sum_{a^2+b^2=m} 1$, and the sum above runs over $g_1^2 + g_2^2 = g_3^2 + g_4^2, g_i^2 \leqslant n_1$.

Write $I(a, \delta)$ for $(a-\delta, a+\delta)$, the open interval of width δ centred at a. The above calculations and the bounds on s in (8) imply that we need only consider those t in (19) with $t/n \in I(b/k, Q/(kn)), k \leqslant Q$, for which $|f(t/n)|$ and $|f_i(t/n)|$ exceed Q^{-1}, where $Q \equiv e^{l^2}$. Therefore there must exist $K \leqslant Q$ and $U \leqslant Q$ such that

$$\sum_{K \leqslant k \leqslant 2K}\sum_{(b,k)=1}\sum |f(t/n)|\,|f_i(t/n)|\,|s(t/n)| \gg \frac{1}{l^4} \quad (20)$$

(the third sum is over $\{t : t/n \in I(b/k, Q/(kn)), U^{-1} \leqslant \max(|f(t/n)|, |f_i(t/n)|) \leqslant 2U^{-1}\}$). Again, using (8) and (10), for $1 < k < Q^2$ and $(b, k) = 1$,

$$\sum_{t/n \in I(b/k, Q^2/n)} |s(t/n)| \ll ((\log k)/k)^{\frac{1}{2}} \sum_{h=1}^{Q^2}\frac{1}{2h} \ll \left(\frac{l}{k^{\frac{1}{2}}}\right) l^2, \quad (21)$$

a statement that enables us to choose just one value of t/n from any interval

$I(b/k, Q/(kn))$. Combining (20) and (21), there must be at least P intervals $I(b/k, Q/(kn))$ with $1 \leqslant b \leqslant k, K \leqslant k \leqslant 2K$, each of which has at least one value of t/n with the relevant properties, and $P \gg U^2K^{\frac{1}{2}}/l^7$. The following result shows that values where $0 < |t| \ll Q^2$ may be neglected because their contribution to the sum in (19) is small.

LEMMA 2. *$f(t/n) \ll l^3/L$ if $t \ll Q^2$.*

Proof. Let $T = Q^2$. Then

$$\sigma^{-1}F(t/n) = \sigma^{-1}\sum_{a\in\mathscr{A}} e(at/n)$$

$$= \sigma^{-1}\sum_{i=0}^{t-1}\sum_{j=0}^{T-1}\sum_{\mathscr{A}_{ij}} e(at/n) = \sigma^{-1}\sum_{i=0}^{t-1}\sum_{j=0}^{T-1}\sum_{\mathscr{A}_{ij}} \{e(j/T)+O(T^{-1})\}$$

$$= \sigma^{-1}\sum_{i=0}^{t-1}\sum_{j=0}^{T-1} e(j/T)\left\{\frac{\sigma}{tT}+\sigma_{ij}\right\}+O(T^{-1});$$

$\mathscr{A}_{ij}$ is the set $\{a\in\mathscr{A}: nt^{-1}(i+j/T) < a \leqslant nt^{-1}(i+(j+1)/T)\}$ and $\sigma_{ij} = |\mathscr{A}_{ij}| - \sigma/(tT)$. As in the proof of Corollary A, $\sigma_{ij} \leqslant (13\sigma/(tT))(l^3/L)$ and since $\sum \sigma_{ij} = 0$,

$$\sum_{i=0}^{t-1}\sum_{j=0}^{T-1} |\sigma_{ij}| \ll \sigma l^3/L.$$

It now follows that

$$f(t/n) = \frac{1}{tT}\sum_{i=0}^{t-1}\sum_{j=0}^{T-1} e(j/T)+O(\sigma^{-1}\sigma l^3/L)+O(T^{-1}) = 0+O(l^3/L)+O(T^{-1}) = O(l^3/L).$$

Using $|f_i(t/n)| \leqslant 1$ and (10), we have the following simple consequence of Lemma 2.

COROLLARY 3.

$$\sum_{0<|t|\ll Q^2} |f(t/n)f_i(t/n)s(t/n)| \ll \frac{l^3}{L}\sum_{0<|t|\ll Q^2}\frac{1}{|t|} \ll \frac{l^5}{L}.$$

For any $\alpha\in[0,1]$ we can choose relatively prime integers a and $q, 1 \leqslant q \leqslant n/Q$, with $\alpha\in I(a/q, Q/(nq))$. Since $f = f_1+f_2$ we have either $U^{-1} \leqslant |f_i(t/n)| \leqslant 2U^{-1}$ for at least $\frac{1}{2}P$ values of t/n or $U^{-1} \leqslant |f(t/n)| \leqslant 2U^{-1}$ for at least $\frac{1}{2}P$ values. This establishes the following.

LEMMA 4. *There exists a set*

$$\mathscr{P} = \{t/n\in I(b/k, Q/(kn)), K < k \leqslant 2K, \text{ no two } t/n \text{ in the same interval}\},$$

such that for either $i = 1$ or $i = 2$, $|f_i(t/n)| \geqslant (2U)^{-1}$ for at least $\frac{1}{4}$ of the elements in $\mathscr{P}$ and $|\mathscr{P}|/U^2 \gg K^{\frac{1}{2}}/l^7$.

Now, a similar argument to the Main Lemma and Corollary A of Section 2 shows that Corollary A remains true if we replace f by f_1 or f_2 in the definition of $C_\eta(q)$. (First we show that if (1) fails for $\mathscr{A}$ but it is true for $m < n$ then $f_i(0) = (\frac{1}{2}\gamma)(1+O(l/L))$, $i = 1, 2$; afterwards, the proof of Corollary A runs as it stands.) Thus, with

Lemma 4 and the statement that $K^{\frac{1}{2}}/l^7 \ll |\mathscr{P}|/U^2 \leqslant Kl^3/l$, we see that $K \gg L^2/l^{20}$. As in (4) we apply Parseval's identity to f_t and obtain

$$\frac{L}{l^{17}} \ll \frac{K^{\frac{1}{2}}}{l^7} \ll \frac{|\mathscr{P}|}{U^2} \ll \sum_{t=0}^{n-1} |f_t(t/n)|^2 \ll \gamma^{-1},$$

which is clearly the same as $\gamma \ll (\log\log n)^{17}/\log n$. Although this bound is weaker than the statement in (1), it already improves the earlier density results. The next section shows how it may be successively improved to give the bound in (1) via an iteration scheme.

4. *The Iteration Lemma*

We just showed that

$$\sum_{t=0}^{n-1} |f_t(t/n)|^2 \geqslant \frac{L}{l^{17}} \tag{*}$$

by exhibiting a relatively sparse set $\mathscr{P}$ of values of t/n for which the sums of squares of Fourier coefficients exceed L/l^{17}; Parseval's identity immediately gives $\gamma \ll l^{17}/L$. Starting with $\mathscr{P}$ we shall perform an iteration step in which we produce a new set $\mathscr{R}$ with the property that

$$\sum_{r\in\mathscr{R}} |f_t(r)|^2 \geqslant \Big(\sum_{p\in\mathscr{P}} |f_t(p)|^2\Big) L^{\frac{1}{3}}. \tag{**}$$

Together with (*) this lowers the bound on γ by a factor of $L^{-\frac{1}{3}}$. The same procedure may now be applied to $\mathscr{R}$, etc., until after I steps, we shall have deduced the bound

$$\gamma \ll L^{-I/3}.$$

Finally, in the last section, we show that I may be as large as $(\log_4 n)/4$ and still it is valid to apply the iteration step. In this way we shall have (1). The exact details are given in the following.

ITERATION LEMMA. *Given numbers Q' and K, $Q < Q' < \frac{1}{8}Q^2$ and $K \gg L$, and $i = 1$ or 2, suppose that we have a set $\mathscr{P}$ of elements of the form $u/n \leqslant 1$ with $|u/n - b/k| \leqslant Q'/n$, $(b,k) = 1$, $0 < b < k$, $K \leqslant k \leqslant 2K$, $U^{-1} \leqslant |f_t(u/n)| \leqslant 2U^{-1}$, $\max(U,K) \leqslant Z \leqslant L^{\log l/100}$, and they have the property that at most one point $u/n \in \mathscr{P}$ is in any interval $I(b,k) = [b/k - Q'/n, b/k + Q'/n]$. Then there are numbers V and H, $H > L$ and another set $\mathscr{R}$ of numbers of the form $v/n \leqslant 1$ with $|v/n - c/h| \leqslant 7Q'/n$, $(c,h) = 1$, $0 < c < h$, $H \leqslant h \leqslant 2H$, $V^{-1} \leqslant |f_t(v/n)| \leqslant 2V^{-1}$, with $\max(V,H) \leqslant \gamma^{-4}Z^6L^5$ and there is at most one v/n in any interval $I'(c,h) = (c/h - 7Q'/n, c/h + 7Q'/n)$; if $\gamma \geqslant L^{-\log l/100}$ then also*

$$|\mathscr{R}|/V^2 \geqslant (|\mathscr{P}|/U^2) L^{\frac{1}{3}}. \tag{22}$$

Proof. We need only argue the case for $i = 1$, the other case being identical. Take $\alpha = u/n \in \mathscr{P}$. Since $\mathscr{A} - \mathscr{A}$ contains no positive squares,

$$\frac{1}{n}\sum_{t=0}^{n-1} F(t/n)\,\overline{F_1(\alpha + t/n)\,S(t/n)} = \sum e(-\alpha a_j)\frac{2g}{\sqrt{n_1}} = 0 \tag{23}$$

(the second sum is over $\{g^2 = a_t - a_j : a_t \in \mathscr{A}, a_j \in \mathscr{A}_1, g \leqslant \sqrt{n_1}\}$). Therefore, as in (19),

$$\sum_{t=1}^{n-1} |f(t/n) f_1(\alpha + t/n)\, s(t/n)| \geqslant |f_1(\alpha)| \geqslant U^{-1}. \tag{24}$$

For each $\alpha\in\mathscr{P}$ we shall identify a large set G'_α of values of t/n such that $|f_t(\alpha+t/n)|$ is large. We construct $\mathscr{R}$ from these sets. For each α we can choose a number a/q such that $\alpha\in I(a/q, Q/(qn)), q\leqslant n/Q$. Using Parseval's identity as in Section 3 we can neglect terms where

$$m_\alpha(t)=\min(|f(t/n)|,|f_1(\alpha+t/n)|,|s(t/n)|)<\gamma^{\frac{3}{2}}/(Z^2L)$$

and (24) will still remain true for the remaining terms, as long as we multiply the right-hand side by 0.99. We treat three cases.

I. First assume that for at least one per cent of the points $\alpha\in\mathscr{P}$ we have

$$\sum_{0<|t|<6Q'}|f(t/n)f_1(\alpha+t/n)s(t/n)|\geqslant\frac{|f_1(\alpha)|}{100}. \tag{25}$$

Then, similarly to Corollary 3,

$$\frac{|f_1(\alpha)|}{100}\leqslant\max(|f_1(\alpha+t/n)|,0<|t|<6Q')\sum_{0<|t|<6Q'}|f(t/n)s(t/n)|\ll|f_1(v/n)|\frac{l^5}{L},$$

the maximum being attained at the point $\alpha+u/n=v/n$. For these v/n we have $|v/n-b/k|\leqslant 7Q'/n$ so we can choose a subset $\mathscr{R}$ of cardinality $|\mathscr{R}|\gg|\mathscr{P}|/l^2$ such that $V^{-1}\leqslant|f_1(v/n)|<2V^{-1}$, $V\ll l^5U/L$; thus

$$|\mathscr{R}|/V^2\gg(|\mathscr{P}|/l^2)(L^2l^{-10}U^{-2})>|\mathscr{P}|U^{-2}L^{\frac{3}{2}}.$$

II. Next suppose that for at least one per cent of the points $\alpha\in\mathscr{P}$

$$\sum_{0\leqslant|t|<6Q'}|f(1-\alpha+t/n)f_1(t/n)s(1-\alpha+t/n)|\geqslant\frac{|f_1(\alpha)|}{100}\geqslant(100U)^{-1}. \tag{26}$$

Then, using $|f(\beta)|=|f(1-\beta)|$ and (21),

$$(100U)^{-1}\leqslant\max(|f(\alpha-t/n)|,0\leqslant t\leqslant 6Q')\sum_{u/n\in I(b/k,\,Q^2/n)}|s(u/n)|\leqslant|f(v/n)|\frac{l^3}{K^{\frac{1}{2}}},$$

where the maximum is attained at $\alpha-u/n=v/n$. Now if $|f_t(v/n)|\geqslant\frac{1}{2}|f(v/n)|$ for at least half of the points v/n we get the new system with $V\ll Ul^3/K^{\frac{1}{2}}$, $|\mathscr{R}|\gg|\mathscr{P}|/l^2$ and thus

$$|\mathscr{R}|/V^2\gg|\mathscr{P}|K/(U^2l^8)\geqslant(|\mathscr{P}|(U^2)(L/l^8).$$

III. The final case treats the set $\mathscr{P}_0$ of $\alpha\in\mathscr{P}$ for which both (25) and (26) fail to hold; clearly $|\mathscr{P}_0|\geqslant 0.98|\mathscr{P}|$. For any $\beta\in[0,1]$ we choose a/q with $q\leqslant n/(5Q')$, $(a,q)=1$, and such that $|\beta-a/q|\leqslant 5Q'/(qn)$. If $|\beta-a/q|=\eta$, with $1\leqslant q\leqslant Q^2$ and $Q'/n<\eta<5Q'/n$, then from (10) we know that $s(\beta)\ll(Q')^{-1}$.

Take $\alpha\in\mathscr{P}_0$ with $|\alpha-b/k|\leqslant Q'/n$ according to our condition. Then in (24) the remaining values t/n in the two intervals $I(0,5Q'/n)\equiv\{\beta:0<\beta\leqslant 5Q'/n$ or $1>\beta\geqslant 1-5Q'/n\}$ and $I(b/k,5Q'/n)$ may be neglected.

Taking $\alpha\in I(b/k,Q'/n)$ consider the set

$$G_\alpha=\{t/n\in[0,1):t/n\notin I(0,5Q'/n),\ t/n\notin I(b/k,5Q'/n),\ m_\alpha(t)\geqslant\gamma^{\frac{3}{2}}/(Z^2L)\}.$$

Then

$$\sum_{t/n\in G_\alpha}|f(t/n)f_1(\alpha+t/n)s(t/n)|\gg U^{-1}.$$

Write $X=\gamma^{-4}Z^5L^4$. If we have $t/n\in I(a/m,5Q'/(nm))$ for some $t/n\in G_\alpha$, then since $Q^2\geqslant Q'\geqslant Q>X$, (8) implies that $m<X$, using the bound on $m_\alpha(t)$.

Now for every α we can choose M, T, V as suitable positive powers of 2 in such a way that there exists a set $G'_\alpha \subset G_\alpha$ of values that satisfy $t/n \in I(a/m, 5Q'/(nm))$, $M \leqslant m \leqslant 2M$, $2 \leqslant T^{-1} \leqslant |f(t/n)| \leqslant 2T^{-1}$, $V^{-1} \leqslant |f_1(\alpha+t/n)| \leqslant 2V^{-1}$, and such that $\max(M, T, V) \leqslant X$, and

$$\sum_{t/n \in G'_\alpha} |f(t/n) f_1(\alpha+t/n)\, s(t/n)| \gg \frac{1}{U \log^3 X} \gg \frac{1}{U \log^3 Q} \gg \frac{1}{Ul^6}.$$

Also, using (21) we get a reduced set G''_α with at most one value of t/n from any interval $I(a/m, 5Q'/(nm))$ and

$$\sum_{t/n \in G''_\alpha} |f(t/n) f_1(\alpha+t/n)| \geqslant M^{\frac{1}{2}}/(Ul^9);$$

this says $|G''_\alpha| \geqslant M^{\frac{1}{2}} TV/(Ul^9)$.

If $\alpha + t/n$ could be equal to $\beta + u/n$ for many different values of α and β in $\mathscr{P}$ and $t/n \in G''_\alpha$, $u/n \in G''_\beta$, then it would be difficult to give a lower bound for the sum of squares of Fourier coefficients. We now show that no value of $\alpha + t/n$ can occur too frequently (Lemma A). Let $D_0 = \max(\tau(n), n \leqslant (2MK)^2)$, where τ is the divisor function. Fixing k, we let

$$\mathscr{B}(k) = \{b : \exists \alpha \in I(b/k, Q'/n), \alpha \in \mathscr{P}_0\}.$$

Clearly we can choose a pair of divisors of k, d_k and f_k, with $f_k | d_k | k$ (we put $e_k = d_k/f_k$), such that there is $\mathscr{B}'(k) \subset \mathscr{B}(k)$, $|\mathscr{B}'(k)| \geqslant |\mathscr{B}(k)|/D_0^2$ and for each $\alpha \in I(b/k, Q'/n), b \in \mathscr{B}'(k)$, there is a reduced set $G'''_\alpha \subset G''_\alpha$ with

$$|G'''_\alpha| \gg M^{\frac{1}{2}} TV/(D_0^2 Ul^9) \tag{27}$$

that satisfies the following property. If $t/n \in G'''_\alpha$, $t/n \in I(a/m, 5Q'/(mn))$ then $(k, m) = d_k$, and if we write $b/k + a/m$ as c/p, $(c, p) = 1$, then $c = (bm + ak)/(d_k f_k)$, where $p = km/(d_k f_k)$. Introducing the notation $m' = m/d_k$, $k' = k/d_k$, we have $b/k' + a/m = c/(k'm'e)$, with $(c, k'm'e) = 1$. Also $(b, k') = (a, m') = 1$ which implies that $(k'm', bm' + ak') = 1$. This means also that $(f_k, k') = (f_k, m') = 1$.

Consider now $\mathscr{P}_1 = \{\alpha \in \mathscr{P}_0 : \alpha \in I(b/k, Q'/(kn)), K \leqslant k \leqslant 2K, b \in \mathscr{B}'(k)\}$. Then clearly $|\mathscr{P}_1| \gg |\mathscr{P}|/D_0^2$. Suppose that $\mathscr{B}'(k)$ possesses $\beta(k)$ different values of b modulo (f_k). We can choose a set $\mathscr{K}$ of numbers k and the corresponding subset $\mathscr{P}_2 \subset \mathscr{P}_1$ of α values such that there exist integers D, E, F, B with $D \leqslant d_k \leqslant 2D$, $E \leqslant e_k \leqslant 2E$, $F \leqslant f_k \leqslant 2F$, $B \leqslant \beta(k) \leqslant 2B$, and $|\mathscr{P}_2| \gg |\mathscr{P}_1| l^6$. Denote the corresponding set of b/k by $\mathscr{P}_2^*$ and for $\alpha \in \mathscr{P}_2$, $\alpha \in I(b/k, Q'/n)$, consider the attached set $G^*(b/k)$ of rational numbers a/m, where $t/n \in G'''_\alpha$, $t/n \in I(a/m, 5Q'/(mn))$. It is easy to establish the following.

LEMMA A. *Given $a_0/m_0 \in G^*(b_0/k_0)$ and $b_0/k_0 \in \mathscr{P}_2^*$ suppose that we have $a/m \in G^*(b/k)$ and $b/k \in \mathscr{P}_2^*$. Then the number of quadruples (a, m, b, k) that satisfy the equation $a/m + b/k = a_0/m_0 + b_0/k_0$ is $\ll DBD_0^2$.*

Proof. There are at most D_0^2 choices for the triple (k', m', e) since $k'm'e = k'_0 m'_0 e_0$. Suppose that k', m' and e are fixed. Then there are at most $2F$ choices for f_k and this finally determines m and k. Now

$$bm' + ak' = cf_k = c_0 f_k,$$

so $bm' \equiv c_0 f_k \bmod (k')$. In view of $(k', m') = 1$, b is uniquely determined modulo k' and so we have at most $4BE$ choices for b.

The next result clarifies a connection between the many parameters that have been used. It provides the final step in establishing the asserted bound on $|\mathscr{R}|$.

LEMMA B. *Given* $k \in \mathscr{K}$,

$$BTVM^{\frac{1}{2}}/(D_0^2 Ul^9) \ll |\bigcup_{b \in \mathscr{B}'(k)} G^*(b/k)| \ll MT^2l^3/(LD).$$

Proof. The upper bound is a trivial consequence of the Main Lemma. For a fixed m there are $\ll T^2l^3/L$ different values of t/n in intervals of type $I(a/m, 5Q'/(mn))$ for which $|f(t/n)| \geqslant T^{-1}$. Since $(m,k) = d_k \geqslant D$ there are $\ll M/D$ choices for m.

To prove the lower bound, in view of (27) we need only show that if b_1 is not congruent to b_2 modulo (f_k), $b_i \in \mathscr{B}'(k)$, then $G^*(b_1/k)$ and $G^*(b_2/k)$ are disjoint, since we have at least B different values of b modulo (f_k). But if $a/m \in G^*(b_1/k) \cap G^*(b_2/k)$ then $b_1 m' + ak' \equiv b_2 m' + ak' \equiv 0 \bmod (f_k)$. This implies that $b_1 m' \equiv b_2 m' \bmod (f_k)$ and therefore $b_1 \equiv b_2 \bmod (f_k)$, because $(m', f_k) = 1$.

To complete the proof of the Iteration Lemma we have from Lemma A and (27) that there are

$$|\mathscr{R}| \gg (|\mathscr{P}_2| M^{\frac{1}{2}} TV/(D_0^2 Ul^9))/(DBD_0^2)$$

$$\gg |\mathscr{P}| M^{\frac{1}{2}} TV/(UDBD_0^4 l^{15})$$

different values of $a/m + b/k$, $a/m \in G^*(b/k)$, $b \in \mathscr{B}'(k)$, $k \in \mathscr{K}_2$, and therefore at least as many different values of $t/n + \alpha = v/n \in I(a/m + b/k, 6Q'/n)$ with $V^{-1} \leqslant |f_1(v/n)| \leqslant 2V^{-1}$; all intervals are disjoint.

Since Lemma B implies that

$$L/(D_0^2 l^{12} U) \ll M^{\frac{1}{2}} T/(BDV),$$

we see from the lower bound on $|\mathscr{R}|$ that

$$|\mathscr{R}| V^{-2} \gg (1/(D_0^4 l^{15}))(|\mathscr{P}|/U)(M^{\frac{1}{2}} T/(VDB)) \gg (L/(D_0^6 l^{27}))(|\mathscr{P}|/U^2) > L^{\frac{1}{3}} |\mathscr{P}|/U^2.$$

This will prove the Iteration Lemma. We use $\max(M, K) \ll L^{\log l/10}$ and thus, $D_0 \ll L^{\frac{1}{16}}$. From the construction of $e_k/h = a/m + b/k$, $(e_k, h) = 1$, it is clear that

$$MK/(DF) \ll h \ll MK/(DF) \ll \gamma^{-4} Z^6 L^4.$$

The relation $H > L$ follows by $Hl^3 L^{-1} \gg |\mathscr{R}| V^{-2} > L^{\frac{1}{3}} |\mathscr{P}| U^{-2} > L^{\frac{1}{3}} l^{-7}$, the same argument that was made for K in Section 3.

5. *Proof of the theorem*

In each iteration the parameter Z changes from Z to $Z' \leqslant Z^{10}$. After I iterations the initial Z is bounded by Z^{10^I}. As this quantity must also be at most $L^{\log l/100}$ if the iteration lemma is to be applied, the rapid growth of Z^{10^I} forces a fairly strict bound on I, the number of allowable iterations, as follows. The starting set satisfies $|\mathscr{P}|/U^2 > L/l^7$. If we can make $3I-2$ iteration steps we shall have

$$L^I \ll \sum_{t=0}^{n-1} |f_t^2(t/n)| < \sigma n/\sigma^2 = \gamma^{-1}; \tag{28}$$

that is, $\gamma \ll L^{-I}$. Suppose now that $\gamma \geqslant L^{-I}$.

We may also suppose that $K_0 < L^{3I}$, since otherwise $\mathscr{P}_0$ (cf. Section 3) leads

to $|\mathscr{P}_0|U_0^{-2} \gg K_0^{\frac{1}{2}}/l^r > L^l$. Again, from the starting step we may take $U_0 < L^{2l}$ since smaller values of f or f_t are neglected (cf. Section 3). Thus we may choose $Z_0 = L^{3l}$ as well, and so

$$\max(V, H) = \max(U_1, K_1) \leqslant \gamma^{-4} Z_0^6 L^5 \leqslant Z_0^{10}.$$

After $3l-2$ iteration steps we shall have $Z_{3l-2} \leqslant Z_0^{10^{3l-2}} \leqslant L^{10^{3l-2}}$. Now Z_{3l-2} will remain less than $L^{\log l/100}$ if we take

$$l = [\log\log l/(5\log 10)] \geqslant \log\log l/12.$$

Using this in (28) we arrive at the bound given (1).

REMARK. We have not violated the bounds on Q needed for the Iteration Lemma. After $3l-2$ steps we still have $Q_{3l-2} = Q6^{3l-2} < Q\log l < Qe^{t^2} = Q^2$.

References

1. H. DAVENPORT and H. HEILBRONN, 'On indefinite quadratic forms in five variables', *J. London Math. Soc.* 21 (1946) 185–193.
2. H. FURSTENBERG, 'Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions', *J. Analyse Math.* 31 (1977) 204–256.
3. A. SÁRKÖZY, 'On difference sets of integers I', *Acta Math. Acad. Sci. Hungar.* 31 (1978) 125–149.
4. A. SÁRKÖZY, 'On difference sets of integers II', *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* 21 (1978) 45–53.
5. A. SÁRKÖZY, 'On difference sets of integers III', *Acta Math. Acad. Sci. Hungar.* 31 (1978) 355–386.
6. R. C. VAUGHAN, *The Hardy–Littlewood method* (University Press, Cambridge, 1981).

Department of Mathematics
Rutgers University
USA

and
Mathematical Institute
Hungarian Academy of Sciences
Hungary

Department of Computer Science
Rutgers University
Busch Campus
New Brunswick
New Jersey 08903
USA

Department of Computer Science
Rutgers University
USA

and
Mathematical Institute
Hungarian Academy of Sciences
Hungary