<table>
<thead>
<tr>
<th>Status</th>
<th>Rapid Code</th>
<th>Branch Name</th>
<th>Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pending</td>
<td>IND</td>
<td>Math</td>
<td>7/13/2009 8:30:46 AM</td>
</tr>
</tbody>
</table>

**CALL #:** QA 1 .Ac82

**LOCATION:** IND :: Math :: MATH PER

**TYPE:** Article  CC:CCL

**JOURNAL TITLE:** Acta mathematica Academiae Scientiarum Hungaricae


**IND CATALOG TITLE:** Acta mathematica Academiae Scientiarum Hungaricae.

**ARTICLE TITLE:** On difference sets of sequences of integers

**ARTICLE AUTHOR:** Sarkozy

**VOLUME:** 31

**ISSUE:**

**MONTH:**

**YEAR:** 1977

**PAGES:** 125-

**ISSN:** 0001-5954

**OCLC #:**

**CROSS REFERENCE ID:** 414855

**VERIFIED:**

**BORROWER:** UMC :: Main Library

**PATRON:** Gasarch, William

**PATRON ID:** -

**PATRON ADDRESS:** -

**PATRON PHONE:** -

**PATRON FAX:** -

**PATRON E-MAIL:** -

**PATRON DEPT:** -

**PATRON STATUS:** -

**PATRON NOTES:** -

This material may be protected by copyright law (Title 17 U.S. Code)
System Date/Time: 7/13/2009 8:46:04 AM MST
ON DIFFERENCE SETS OF SEQUENCES OF INTEGERS. I

By
A. SÁRKÖZY (Budapest)

1. A set of integers \( u_1, u_2, \ldots \) will be called an \( S \)-set if its difference set does not contain the square of a positive integer; in other words, if \( u_n - u_m = x^2 \) (where \( x, y, z \) are integers) implies that \( x = y, z = 0 \). Let \( A(x) \) denote the greatest number of integers that can be selected from \( 1, 2, \ldots, x \) to form an \( S \)-set and let us write

\[
a(x) = \frac{A(x)}{x}.
\]

L. Lovász conjectured that

\[
a(x) = o(1)
\]

(oral communication). The aim of this paper is to prove the following sharper form of (1):

THEOREM.

\[
a(x) = O\left(\frac{(\log \log x)^{\frac{1}{2}}}{(\log x)^{\frac{1}{3}}}\right).
\]

(We remark that (1) has been proved independently also by H. Fürstenberg: his proof is unpublished yet.)

To prove this theorem, we are going to use that version of the Hardy-Littlewood method which has been elaborated by K. F. Roth in [2] and [3].

Throughout this paper, we use the following notations:

We denote the distance of the real number \( x \) from the nearest integer by \( \lfloor x \rfloor \), i.e. \( \lfloor x \rfloor = \min \{ x - \lfloor x \rfloor, \lfloor x \rfloor + 1 - x \} \). We write \( e(x) = e^{2\pi i x} \) where \( x \) is real. \( L_b, L_3, \ldots \), \( X_b, X_3, \ldots \) denote absolute constants. If \( a, b \) are real numbers and \( b > 0 \), then we define the symbol \( \min \{ a, \frac{b}{0} \} \) by

\[
\min \{ a, \frac{b}{0} \} = a.
\]

Finally, if \( g(x_1, x_2, \ldots, x_n) \equiv f(x_1, x_2, \ldots, x_n) \) then we write

\[
g(x_1, x_2, \ldots, x_n) = \theta(f(x_1, x_2, \ldots, x_n)).
\]

2. Following Roth's method, we are going to deduce a functional inequality for the function \( a(x) \).
Let $N$ be a large integer and let us write $M = \lceil \sqrt{N} \rceil$. Let

$$T(z) = \sum_{z=1}^{M} e(z^2 z) = \sum_{z=1}^{M} e(z^2 z).$$

Let $u_1, u_2, \ldots, u_{A(N)}$ be a maximal $\mathcal{A}$-set selected from $1, 2, \ldots, N$ and let

$$F(z) = \sum_{z=1}^{A(N)} e(u_z z).$$

We are going to investigate the integral

$$(4) \quad E = \int_0^1 |F(z)|^2 T(z) \, dz.$$

Obviously,

$$(5) \quad E = \int_0^1 F(z) F(-z) T(z) \, dz =$$

$$= \int_0^1 \sum_{z=1}^{A(N)} e(u_z z) \sum_{z=1}^{A(N)} e(-u_z z) \sum_{z=1}^{M} e(z^2 z) \, dz = \sum_{u_z, u_{z+\sqrt{z+1}}} \delta = 0$$

since $u_1, u_2, \ldots, u_{A(N)}$ is an $\mathcal{A}$-set.

On the other hand, we shall estimate this integral by using the Hardy—Littlewood method. For this purpose, we need some estimates for the functions $T(z)$ and $F(z)$.

3. In this section, we estimate the function $T(z)$.

**Lemma 1.** If $a, b$ are integers such that $a \leq b$, and $\beta$ is an arbitrary real number then

$$\left| \sum_{k=a}^{b} e(k \beta) \right| \leq \min \left\{ b-a+1, \frac{1}{2 \| \beta \|} \right\}.$$

(For $\| \beta \| = 0$, the right hand side is defined by (3).)

**Proof.** Obviously,

$$\left| \sum_{k=a}^{b} e(k \beta) \right| \leq \sum_{k=a}^{b} 1 = b-a+1$$

for all $a, b, \beta$ (where $a \leq b$).

Furthermore, for $\| \beta \| \neq 0$,

$$\left| \sum_{k=a}^{b} e(k \beta) \right| = \frac{1-e((b-a+1) \beta)}{1-e(\beta)} \leq \frac{2}{|1-e(\beta)|} =$$

$$= \frac{2}{|e(-\beta/2) - e(\beta/2)|} = \frac{1}{\sin \pi \| \beta \|} = \frac{1}{\sin \pi \| \beta \|} \leq \frac{2}{\pi \| \beta \|} = \frac{1}{\| \beta \|}$$

which proves Lemma 1.
Lemma 2. Let $p, q$ be integers and $\alpha, \gamma$ real numbers such that $q > 1$, $(p, q) = 1$ and

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Then

$$\sum_{x=0}^{q-1} \min \left\{ q, \frac{1}{\|y + ax\|} \right\} < 8q \log q.$$

This lemma is identical to Theorem 44 in [1], p. 26.

Lemma 3. Let $p, q$ be integers and $\alpha, \gamma, P$ real numbers such that $q > 1$, $(p, q) = 1$, and

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Then

$$\sum_{x=0}^{q-1} \min \left\{ p, \frac{1}{\|y + ax\|} \right\} = 8P + 8q \log q.$$

Proof. For $q = 1$, (7) holds trivially (by $P \geq 1$).

For $q > 1$, the left hand side of (7) can be rewritten in the following way:

$$\sum_{x=0}^{q-1} \min \left\{ p, \frac{1}{\|y + ax\|} \right\} =$$

$$= \sum_{0 \leq x \leq q-1} \min \left\{ p, \frac{1}{\|y + ax\|} \right\} + \sum_{0 \leq x \leq q-1} \min \left\{ p, \frac{1}{\|y + ax\|} \right\} \leq$$

$$\leq \sum_{0 \leq x \leq q-1} \frac{1}{\|y + ax\|} \leq \sum_{0 \leq x \leq q-1} \frac{1}{q} = \frac{P}{q} \sum_{x=0}^{q-1} \min \left\{ q, \frac{1}{\|y + ax\|} \right\} \leq$$

$$\leq P \sum_{0 \leq x \leq q-1} \frac{1}{q} \sum_{x=0}^{q-1} \min \left\{ q, \frac{1}{\|y + ax\|} \right\} \leq$$

$$= P \sum_{0 \leq x \leq q-1} \frac{1}{q} \sum_{x=0}^{q-1} \min \left\{ q, \frac{1}{\|y + ax\|} \right\} =$$

We are going to show that

$$\sum_{0 \leq x \leq q-1} \frac{1}{q} \sum_{x=0}^{q-1} \frac{1}{\|y + ax\|} \leq 8.$$

Let us assume indirectly that the left hand side of this inequality is $\geq 9$. This indirect assumption implies the existence of integers $x_1, x_2, x_3, x_4, x_5$ such that

$$\|y + ax_i\| < \frac{1}{q} \quad (for \quad i = 1, \ldots, 5)$$

Acta Mathematica Academiae Scientiarum Hungaricae 51, 1978
and which all lie either in the interval \([0, \frac{q-1}{2}]\) or in \([\frac{q-1}{2}, q-1]\); in either case

\[
0 < |x_i - x_j| < \frac{q}{2} \quad \text{(for } 1 \leq i \neq j < 5). \tag{11}
\]

By (10), there exist integers \(y_i\) and real numbers \(\theta_i\) such that

\[
\gamma + \alpha x_i = y_i + \frac{\theta_i}{q} \quad \text{(for } i = 1, \ldots, 5) \tag{12}
\]

and

\[-1 < \theta_i < 1 \quad \text{(for } i = 1, \ldots, 5). \tag{13}\]

Using the matchbox principle, we obtain the existence of indices \(\mu, \nu\) such that \(1 \leq \mu < \nu \leq 5\) and

\[
|\theta_\mu - \theta_\nu| < \frac{1}{2q}. \tag{14}
\]

Writing \(i = \mu\) and \(\nu\) in (12), respectively, and subtracting the equalities obtained in this way, we obtain that

\[
\alpha(x_\mu - x_\nu) = y_\mu - y_\nu + \frac{\theta_\mu - \theta_\nu}{q}. \tag{15}
\]

Hence

\[
\|\alpha(x_\mu - x_\nu)\| \leq \frac{\theta_\mu - \theta_\nu}{q} < \frac{1}{2q} \tag{16}
\]

(by (13)).

On the other hand, we obtain with respect to (6) and (11) that

\[
\|\alpha(x_\mu - x_\nu)\| = \left\| \frac{p}{q} (x_\mu - x_\nu) + \left( \alpha - \frac{p}{q} \right) (x_\mu - x_\nu) \right\| \leq \left\| \frac{p(x_\mu - x_\nu)}{q} \right\| + \left| \alpha - \frac{p}{q} \right| |x_\mu - x_\nu| > \frac{1}{q} - \frac{1}{q^2} \cdot \frac{q}{2} = \frac{1}{2q}
\]

in contradiction with (14), which proves (9).

(8), (9) and Lemma 2 yield (7) and Lemma 3 is proved.

**Lemma 4.** Let \(N, p, q\) be integers and \(\alpha\) a real number such that \(N \equiv 1, q \equiv 1, (p, q) = 1\) and

\[
|\alpha - \frac{p}{q}| \leq \frac{1}{q^2}. \tag{17}
\]

Then

\[
|T(\alpha)| = \left| \sum_{k=1}^{M} e(k^2 \alpha) \right| < 7 \left( \frac{M}{q^{1/2}} + (M \log q)^{1/2} + (q \log q)^{1/2} \right) \tag{18}
\]

(where \(M = \left\lfloor \sqrt{N} \right\rfloor \)).
PROOF.

\[ |T(\alpha)|^2 = T(\alpha)T(-\alpha) = \sum_{x=1}^{M} \sum_{y=1}^{M} e((x^2 - y^2)\alpha) = \]

\[ = \sum_{x=1}^{M} \sum_{y=1}^{M} e((x - y)(x + y)\alpha) = \sum_{u=1-M}^{M} \min_{y=\max{(1-u,1)}}^{M} e(u(u+2y)\alpha) \equiv \]

\[ \equiv \sum_{u=1-M}^{M-1} \left| \sum_{y=\max{(1-u,1)}}^{M} e(u(u+2y)\alpha) \right| = \sum_{u=1-M}^{M-1} \left| \sum_{y=\max{(1-u,1)}}^{M} e(2uy\alpha) \right|. \]

To estimate the inner sum, we apply Lemma 1 with \( \beta = 2\alpha, \ a = \max{(1-u,1)}, \ b = \min{(M, M-u)}. \) Then obviously,

\[ b - a = \min{(M, M-u)} - \max{(1-u,1)} \leq M - 1, \]

thus Lemma 1 yields that

\[ |T(\alpha)|^2 \equiv \sum_{u=1-M}^{M-1} \min{(M-1)+1, \ \frac{1}{2\|2\alpha\|}} = \]

\[ = \frac{1}{2} \sum_{u=1-M}^{M-1} \min{(2M, \ \frac{1}{\|2\alpha\|})} \equiv \frac{1}{2} \sum_{u=1-M}^{M-1} \min{(2M, \ \frac{1}{\|2\alpha\|})} \equiv \]

\[ \equiv \frac{1}{2} \sum_{j=0}^{\frac{M-4}{4}} \min{(2M, \ \frac{1}{\|2\alpha\|})}. \]

The inner sum can be estimated by using Lemma 3 with \( \gamma = (2 - 2M + jq)\alpha, \ P = 2M. \) We obtain that

\[ |T(\alpha)|^2 \equiv \frac{1}{2} \sum_{j=0}^{\frac{M-4}{4}} (16M + 8q \log q) = \]

\[ = \frac{1}{2} \left( \frac{4M-4}{q} + 1 \right) (16M + 8q \log q) = \left( \frac{4M}{q} + 1 \right) (8M + 4q \log q) = \]

\[ = 32 \frac{M^2}{q} + 8M + 16M \log q + 4q \log q. \]

For \( q = 1, \)

\[ M \equiv \frac{M}{q} = \frac{M^2}{q}, \]

while for \( q \geq 2 \)

\[ M < M \log 4 = 2M \log 2 \equiv 2M \log q. \]

Hence

\[ M \equiv \frac{M}{q} + 2M \log q. \]
Thus we obtain from (16) that
\[
\lvert T(x) \rvert^2 < 32 \frac{M^2}{q} + 8 \left( \frac{M^2}{q} + 2M \log q \right) + 16M \log q + 4q \log q =
\]
\[
= 40 \frac{M^2}{q} + 32M \log q + 4q \log q < 49 \left( \frac{M^2}{q} + M \log q + q \log q \right).
\]

With respect to the inequality
\[(a^2 + b^2 + c^2)^{1/2} \leq a + b + c \quad (\text{where } a, b, c \equiv 0),\]
this yields (15) which proves Lemma 4.

**Lemma 5.** Let \( N, p, q \) be integers and \( x \) a real number such that \((p, q) = 1,\)
\[
N \equiv 3,
\]
\[
1 \equiv q \equiv N^{1/2}/\log N
\]
and
\[
\left\lvert x - \frac{p}{q} \right\rvert < \frac{1}{q^2}.
\]
Then
\[
\lvert T(x) \rvert < 21 \left( \frac{N}{q} \right)^{1/2}.
\]

**Proof.** Applying Lemma 4, we obtain with respect to (17) and (18) that
\[
\lvert T(x) \rvert < 7 \left( \frac{M}{q^{1/2}} + (M \log q)^{1/2} + (q \log q)^{1/2} \right) \equiv
\]
\[
\equiv 7 \left( \left( \frac{N}{q} \right)^{1/2} + N^{1/4}(\log q)^{1/2} + (q \log q)^{1/2} \right) =
\]
\[
= 7 \left( \frac{N}{q} \right)^{1/2} + N^{1/4}(\log N)^{1/2} + (N^{1/2} \log N)^{1/2}
\]
\[
= 7 \left( \frac{N}{q} \right)^{1/2} + 2 \left( \frac{\log N}{N^{1/2}} \right)^{1/2} \equiv 7 \left( \frac{N}{q} \right)^{1/2} - 3 = 21 \left( \frac{N}{q} \right)^{1/2}.
\]

**Lemma 6.** Let \( N, p, q \) be integers and \( x, \beta \) real numbers such that
\[
N \equiv 9,
\]
\[
(p, q) = 1,
\]
\[
1 \equiv q \equiv \sqrt{N},
\]
\[
x = \frac{p}{q} + \beta
\]
and
\[ \frac{\log N}{N} \leq |\beta| < \frac{1}{2q\sqrt[4]{N}}. \]

Then
\[ |T(\alpha)| < 30 \left( \frac{\log N}{q|\beta|} \right)^{1/2}. \]

Proof. Let
\[ Q = \left[ \frac{1}{q|\beta|} \right] + 1. \]

Then obviously,
\[ Q > \frac{1}{q|\beta|}, \]

hence
\[ |\beta| > \frac{1}{qQ}. \]

By (24),
\[ \frac{1}{q|\beta|} > \sqrt[4]{N}. \]

Thus
\[ Q = \left[ \frac{1}{q|\beta|} \right] + 1 \approx \frac{1}{q|\beta|} + \sqrt[4]{N} = \frac{1}{q|\beta|} + \frac{1}{q|\beta|} = \frac{2}{q|\beta|}. \]

By Dirichlet's theorem, there exist integers \( r, s \) such that
\[ (r, s) = 1, \]
\[ 1 \leq s \leq Q \]
and
\[ \left| \alpha - \frac{r}{s} \right| < \frac{1}{sQ}. \]

(31) and (32) imply that also
\[ \left| \alpha - \frac{r}{s} \right| < \frac{1}{s^2}. \]

holds. Thus we may apply Lemma 4 with \( \frac{L}{s} \) in place of \( \frac{P}{q} \). We obtain that
\[ |T(\alpha)| \leq 7 \left( \frac{M}{s^{3/2}} + (M \log s)^{1/2} + (s \log s)^{1/2} \right) \leq \]
\[ \equiv 7 \left( \left( \frac{N}{s} \right)^{1/2} + N^{1/4}(\log s)^{1/2} + (s \log s)^{1/2} \right). \]

To deduce (25) from this inequality, we have to estimate \( s \) in terms of \( q|\beta| \) and \( N \), respectively.
By (29) and (31),

\[ s \equiv \Omega \equiv \frac{2}{q|\beta|} \]

hence with respect to (20) and (24),

\[ s \leq \frac{2}{q|\beta|} \leq \frac{2}{|\beta|} \leq \frac{2}{\log N} < N. \]

Thus (33) implies that

\[ |T(\alpha)| < 7 \left( \left( \frac{N}{s} \right)^{3/\gamma} + (N^{1/4} + s^{1/2})(\log N)^{1/2} \right). \]

We are going to show that

\[ \frac{p}{q} \neq \frac{r}{s}. \]

Let us assume indirectly that

\[ \frac{p}{q} = \frac{r}{s}. \]

By \( q \equiv 1, s \equiv 1, \) (21) and (30), this implies also \( q = s. \) Thus in view of (23), (27) and (32)

\[ \left| \frac{p}{q} - \frac{r}{s} \right| = \left| \left( \frac{p}{q} - \alpha \right) + \left( \alpha - \frac{r}{s} \right) \right| \leq \left| \alpha - \frac{p}{q} \right| + \left| \alpha - \frac{r}{s} \right| = \]

\[ = |\beta| - \left| \alpha - \frac{r}{s} \right| > \frac{1}{qQ} + \frac{1}{sQ} = 0 \]

in contradiction with (37), which proves (36).

(36) implies that

\[ \left| \frac{p}{q} - \frac{r}{s} \right| = \left| \frac{ps - qr}{qs} \right| \leq \frac{1}{qs}. \]

On the other hand, with respect to (22), (23), (24), (26) and (32),

\[ \left| \frac{p}{q} - \frac{r}{s} \right| = \left| \left( \frac{p}{q} - \alpha \right) + \left( \alpha - \frac{r}{s} \right) \right| \leq \left| \alpha - \frac{p}{q} \right| + \left| \alpha - \frac{r}{s} \right| = \]

\[ = |\beta| + \left| \alpha - \frac{r}{s} \right| < |\beta| + \frac{1}{sQ} < |\beta| + \frac{q |\beta|}{s} \leq |\beta| + \frac{1}{2sQ} \leq \frac{|\beta| + 1}{2s}. \]

(38) and (39) yield that

\[ \frac{1}{qs} \leq |\beta| + \frac{1}{2sq}. \]

Thus by (24),

\[ s \equiv \frac{1}{2q|\beta|} > \sqrt{N}. \]
In view of (28), (34) and (40), we obtain from (35) that
\[ |T(\alpha)| < 7 \left( \frac{N^{1/2}}{s} + 2s^{1/2} (\log N)^{1/2} \right) = 7s^{1/2} (\log N)^{1/2} \left( \frac{N^{1/2}}{s (\log N)^{1/2}} + 2 \right) \leq \]
\[ \leq 7s^{1/2} (\log N)^{1/2} (1 + 2) = 21s^{1/2} (\log N)^{1/2} \leq 21 \left( \frac{2}{q_{\beta}} \right)^{1/2} (\log N)^{1/2} = 30 \left( \frac{\log N}{q_{\beta}} \right)^{1/2} \]
and Lemma 6 is proved.

**Lemma 7.** Let \( N, p, q \) be integers, \( R, Q, \alpha \) real numbers such that \( N \equiv 1, (p, q) = 1 \),

\[ 1 \equiv R \equiv q \equiv Q, \]

\[ \sqrt{N} \equiv Q \equiv N \]
and

\[ \left| \frac{s - p}{q} \right| < \frac{1}{Q^2} \]
Then

\[ |T(\alpha)| < 7 \left( \frac{N^{1/2}}{R} + 14 (Q \log N)^{1/2} \right). \]

**Proof.** (41) and (43) imply also

\[ \left| \frac{s - p}{q} \right| < \frac{1}{Q^2}. \]
Thus with respect to (41) and (42), Lemma 4 yields that

\[ |T(\alpha)| < 7 \left( \frac{N^{1/2}}{Q^{1/2}} + (N^{1/2} \log q)^{1/2} + (q \log q)^{1/2} \right) \equiv \]
\[ \equiv 7 \left( \frac{N^{1/2}}{R} + (Q \log N)^{1/2} + (Q \log N)^{1/2} \right) \]
which proves (44).

4. In this section, we estimate the function \( F(\alpha) \) by using Roth's method. Lemmas 8 and 9 follow trivially from the definitions of the functions \( A(\alpha) \) and \( a(\alpha) \).

**Lemma 8.** If \( x, y \) are positive integers such that \( x \equiv y \) then \( A(x) = A(y) \).

**Lemma 9.** For any positive integer \( x \),

\[ \frac{1}{x} \equiv a(x) \equiv 1. \]

For any integer \( b \) and positive integers \( q, x \), let \( A_{b, q}(x) \) denote the greatest number of integers that can be selected from \( b + q, b + 2q, \ldots, b + qx \) to form an \( \alpha \)-set.

*Acta Mathematica Academiae Scientiarum Hungaricae* 31, 1976
LEMMA 10. For any integer $b$ and positive integers $q, x$,

$$A_{b, q}(x) = A(x).$$

PROOF. This follows trivially from the fact that the numbers $b + u_1 q^a, b + u_2 q^a, \ldots, b + u_k q^a$ form an $A$-set if and only if also the numbers $u_1, u_2, \ldots, u_k$ do.

LEMMA 11. For any positive integers $x$ and $y$, we have

(45) $A(x + y) \equiv A(x) + A(y)$,

(46) $A(xy) \equiv xA(y)$,

(47) $a(xy) \equiv a(y)$,

(48) $a(x) \equiv \left(1 + \frac{y}{x}\right)a(y)$.

PROOF. Applying Lemma 10 with $b = y$, $q = 1$, we obtain that the greatest number of integers that can be selected from $y + 1, y + 2, \ldots, y + x$ to form an $A$-set is $A(x)$. (45) follows easily from this fact.

(46) is a consequence of (45).

(47) can be obtained from (46) by dividing by $xy$.

Finally, by Lemma 8 and (46),

$$A(x) \equiv A \left( \left\lceil \frac{x}{y} \right\rceil + 1 \right) \equiv \left( \left\lceil \frac{x}{y} \right\rceil + 1 \right) A(y) \equiv \left( \frac{x}{y} + 1 \right) A(y).$$

Dividing by $x$, we obtain (48).

LEMMA 12. Let $q, t, N$ be positive integers, $p$ integer, $\alpha, \beta$ real numbers such that

$$a = \frac{p}{q} = \beta.$$

Let

$$F_1(x) = \frac{a(t)}{q^2} \left( \sum_{j=1}^{q^2} e\left( \frac{sp}{q} \right) \sum_{j=1}^{N} e(bj) \right),$$

so that if $(p, q) = 1$ then

$$F_1(x) = \begin{cases} a(t) \sum_{j=1}^{N} e(j\alpha) & \text{for } q = 1 \\
0 & \text{for } q > 1 \end{cases}$$

(50) (where $(p, q) = 1$).

Then

$$|F(x) - F_1(x)| \leq (a(t) - a(N))N + 2a(t)qt^2(1 + \pi \beta |N) = H(t, N, q, \beta).$$

PROOF. We are going to show at first that

(51) $F(x) = \frac{1}{tq^2} \sum_{r=1}^{q^2} \sum_{j=1}^{N} \sum_{s+tq^2 \equiv u \equiv 1 (mod q^2)} e(uxu) + \theta(a(t)qt^2)$.

Let us investigate the coefficient of $e(uxu)$ on the right hand side.
If $tq^3 \equiv u_k \equiv N$ then we account $e(ux_k)$ exactly $tq^2$ times, namely for the following values of $j$:

$$j = u_k - tq^2 + 1, \quad u_k - tq^2 + 2, \ldots, u_k.$$ 

Thus the coefficient of $e(ux_k)$ is

$$tq^2 \cdot \frac{1}{tq^2} = 1$$

in this case (and its coefficient is the same on the left hand side).

If

$$1 \equiv u_k \equiv tq^2$$

then we account $e(ux_k)$ on the right of (52) for $j = 1, 2, \ldots, u_k$, thus its coefficient is

$$(0 \equiv) u_k \cdot \frac{1}{tq^2} = tq^2 \cdot \frac{1}{tq^2} = 1$$

on the right and 1 on the left of (52). The numbers $u_k$ satisfying (53) form an $\mathcal{A}$-set thus in view of (46) in Lemma 11, their number is

$$\equiv A(tq^3) \equiv A(t)(q^2) = a(t) tq^2.$$ 

These facts yield that, in fact, the error term in (52) is $\theta(a(t) tq^2)$.

The term $e(ux_k)$ in the inner sum in (52) can be rewritten in the following way:

$$e(ux_k) = e\left(\frac{p\beta}{q} u_k\right) = e\left(\frac{p\beta u_k}{q}\right) e(\beta u_k) =$$

$$= e\left(\frac{p\beta}{q}\right) e(\beta) e(\beta(u_k - j)) = e\left(\frac{p\beta}{q}\right) e(\beta)(1 + \theta(2\pi |\beta(u_k - j)|)) =$$

$$= e\left(\frac{p\beta}{q}\right) e(\beta) + \theta(2\pi |\beta(u_k - j)|) = e\left(\frac{p\beta}{q}\right) e(\beta) + \theta(2\pi |\beta| tq^2)$$

since $|u_k - j| < tq^2$ in the inner sum, and

$$|e(\gamma) - 1| = |e(\gamma/2) - e(-\gamma/2)| = |2 \sin \pi \gamma| \equiv 2 |\pi \gamma| = 2 \pi |\gamma|$$

for any real number $\gamma$.

Thus the inner sum in (52) can be estimated in the following way:

$$\sum_{j\equiv u_k \equiv j + tq^3 \pmod{q^2}} e(ux_k) = \sum_{j\equiv u_k \equiv j + tq^3 \pmod{q^2}} e\left(\frac{p\beta}{q}\right) e(\beta) + \theta(2\pi |\beta| tq^2)$$

$$= e\left(\frac{p\beta}{q}\right) e(\beta) + \theta(2\pi |\beta| tq^2) \sum_{j\equiv u_k \equiv j + tq^3 \pmod{q^2}} 1.$$ 

Let us define the integer $v$ by

$$v = j \equiv v + q^3, \quad v \equiv s \pmod{q^2}.$$
Then by Lemma 10,
\[ \sum_{\frac{j}{n} \equiv \frac{a}{q} \pmod{q}} 1 \equiv \mathcal{A}_{n, q}^2(t) = A(t) = a(t) t. \]
Thus if we define \( D(j, t, q, s) \) by
\[ \sum_{j \equiv \frac{a}{q} \pmod{q}} 1 = a(t) t - D(j, t, q, s) \]
then \( D(j, t, q, s) \equiv 0 \). Putting this into (54):
\[ \sum_{\frac{j}{n} \equiv \frac{a}{q} \pmod{q}} e(\pi \beta) = \left( e\left( \frac{P_0}{q} \right) e(\beta) + o(2\pi |\beta| t q^2) \right) (a(t) t - D(j, t, q, s)) = \]
\[ = e\left( \frac{P_0}{q} \right) e(\beta) (a(t) t - D(j, t, q, s)) + o(2\pi |\beta| a(t) t^2 q^2). \]
Thus (52) yields that
\[ F(\alpha) = \frac{1}{t q^2} \sum_{j=1}^{q} \sum_{\beta=1}^{N} \left[ e\left( \frac{P_0}{q} \right) e(\beta) (a(t) t - D(j, t, q, s)) + o(2\pi |\beta| a(t) t^2 q^2) \right] + \]
\[ + o(a(t) t q^2) = \frac{a(t)}{q^2} \sum_{j=1}^{q} e\left( \frac{P_0}{q} \right) e(\beta) - \frac{1}{t q^2} \sum_{j=1}^{q} e\left( \frac{P_0}{q} \right) e(\beta) D(j, t, q, s) + \]
\[ + o\left( \frac{1}{t q^2} \cdot q^2 \cdot N \cdot 2\pi |\beta| a(t) t^2 q^2 \right) + o(a(t) t q^2) = \]
\[ = F_1(\alpha) - \frac{1}{t q^2} \sum_{j=1}^{q} e\left( \frac{P_0}{q} \right) e(\beta) D(j, t, q, s) + o(2\pi |\beta| N a(t) t q^2) + o(a(t) t q^2). \]
Putting here \( \alpha = \beta = p = 0 \), we obtain that
\[ A(N) = a(t) \cdot N - \frac{1}{t q^2} \sum_{j=1}^{q} N \sum_{\beta=1}^{N} D(j, t, q, s) + o(a(t) t q^2). \]
Hence
\[ (56) \quad \frac{1}{t q^2} \sum_{j=1}^{q} N \sum_{\beta=1}^{N} D(j, t, q, s) = a(t) \cdot N - A(N) + a(t) t q^2 = \]
\[ = (a(t) - a(N)) N + a(t) t q^2. \]
With respect to (56), (55) yields that
\[ |F(\alpha) - F_1(\alpha)| \leq \frac{1}{t q^2} \sum_{j=1}^{q} N \sum_{\beta=1}^{N} D(j, t, q, s) + 2\pi |\beta| N a(t) t q^2 + a(t) t q^2 \equiv \]
\[ \equiv (a(t) - a(N)) N + a(t) t q^2 + 2\pi |\beta| N a(t) t q^2 + a(t) t q^2 = \]
\[ = (a(t) - a(N)) + 2a(t) t q^2 (1 + \pi |\beta| N) \]
which proves Lemma 12.
5. In this section, we are going to deduce a functional inequality for the function \( a(x) \), by investigating the integral \( E \) defined in Section 2. This inequality will contain four parameters: \( t, N, R, Q \) whose values will be fixed later.

**Lemma 13.** Let \( t, N \) be positive integers, \( R, Q \) real numbers such that

\[
N \equiv a^t,
\]

\[
t/N,
\]

\[
l \equiv R \equiv N^{1/2} \log N,
\]

\[
2N^{1/8} \ll Q \ll \frac{N}{\log N}.
\]

Then

\[
a^t(t)N^{3/2} \ll 1260 a(t)(a(t) - a(N))N^{3/2} \log \log N +
+ 12600 a^t(t) t N (\log N)^{1/2} Q^{-1/2} +
+ 120(a(t) - a(N))^2(7N^{1/2} R^{1/2} \log N + 20N^2(\log N)^{1/2} Q^{-1/2} R) +
+ 26000 a^t(t) t^2(2N^{1/2} R^{1/2} \log N) R^{1/2} + 2N R^{1/2} Q^{-1/2} R^3 +
+ 140 a(t) N^{3/8} R^{-1/2} + 2NQ^{1/8}(\log N)^{1/2}).
\]

**Proof.** Let us write

\[G(a) = a(t) \sum_{j=1}^N e(ja)\]

Then

\[
E = \int_0^1 |F(a)|^2 T(a) \, da = \int_0^1 |G(a)|^2 T(a) \, da + \int_0^1 (|F(a)|^2 - |G(a)|^2) T(a) \, da
\]

where \( E = 0 \) by (5). Hence

\[
\int_0^1 |G(a)|^2 T(a) \, da = - \int_0^1 (|F(a)|^2 - G(a)|^2) T(a) \, da.
\]

Here,

\[
\int_0^1 |G(a)|^2 T(a) \, da = \int_0^1 \left( a(t) \sum_{j=1}^N e(ja) \right) \left( a(t) \sum_{k=1}^N e(-ka) \right) \left( \sum_{z=1}^{[\sqrt{N}]} e(z^2a) \right) \, da =
\]

\[
a^t(t) \int_0^1 \sum_{1 \leq j,k \leq N} e((j-k)^2a) \, da = a^t(t) \sum_{j=1}^{N/2} 1.
\]

If

\[
l \equiv z^2 \equiv \frac{N}{2} - 1, \quad z > 0,
\]

\[
l \equiv j \equiv \frac{N}{2} + 1
\]

then the numbers $j, k = j + z^2$, $z$ satisfy the conditions
\[ j - k + z^2 = 0, \quad 1 \leq j, k \leq N, \quad 1 \leq z \leq \sqrt{N} \]
since
\[ k = j + z^2 = \left( \frac{N}{2} + 1 \right) + \left( \frac{N}{2} - 1 \right) = N. \]

By (57), the number of the positive integers $z$ satisfying (64) is at least
\[
\left\lfloor \frac{N}{2} - 1 \right\rfloor \geq \left\lceil \frac{\sqrt{N}}{2} \right\rceil \geq \frac{\sqrt{N}}{2} - 1 \leq \frac{\sqrt{N}}{2} - \frac{\sqrt{N}}{4} = \frac{\sqrt{N}}{4}
\]
while (65) holds for $\left\lfloor \frac{N}{2} \right\rfloor + 1 > \frac{N}{2}$ integers $j$. Thus (63) yields that
\[
\int_0^1 |G(z)|^2 T(z) \, d\alpha = a^2(i) \sum_{j-k+z^2=0 \atop 1 \leq j, k \leq N} 1 > a^2(i) \cdot \frac{\sqrt{N}}{4} \cdot \frac{N}{2} = \frac{1}{8} a^2(i) N^{3/2}. \tag{66}
\]

To complete the proof of (61), we have to give an upper estimate for the right hand side of (62).

For $q = 1, 2, \ldots, [Q]$ and $p = 0, 1, \ldots, q - 1$, let
\[
I_{p,q} = \left( \frac{p}{q}, \frac{1}{pQ}, \frac{p + 1}{q} Q \right)
\]
and let $S$ denote the set of those real numbers $\alpha$ for which
\[-\frac{1}{Q} < \alpha \leq 1 - \frac{1}{Q} \]
holds and
\[
\alpha \notin I_{p,q} \quad \text{for} \quad 1 \leq q \leq R, \quad 0 \leq p \leq q - 1, \quad (p, q) = 1. \tag{67}
\]
Then
\[
\int_0^1 (|F(\alpha)|^2 - |G(\alpha)|^2) T(\alpha) \, d\alpha =
\]
\[
= \int_{-1/\sqrt{Q}}^{1-1/\sqrt{Q}} (|F(\alpha)|^2 - |G(\alpha)|^2) T(\alpha) \, d\alpha \leq \int_{-1/\sqrt{Q}}^{1/\sqrt{Q}} ||F(\alpha)||^2 - ||G(\alpha)||^2 ||T(\alpha)|| \, d\alpha +
\]
\[
+ \sum_{q=1}^{[Q]} \sum_{p=0}^{q-1} \int_{I_{p,q}} ||F(\alpha)||^2 - ||G(\alpha)||^2 ||T(\alpha)|| \, d\alpha +
\]
\[
+ \int_{\mathbb{R}} ||F(\alpha)||^2 - ||G(\alpha)||^2 ||T(\alpha)|| \, d\alpha = E_1 + E_2 + E_3. \tag{68}
\]

Let us estimate the term $E_1$ at first.

\textit{Acta Mathematica Academiae Scientiarum Hungaricae} 21, 1970
For any complex numbers \( u, v \), we have
\[
\begin{align*}
|u|^2 - |v|^2 &= |u - (u - v)| = |u - v|(|u| + |v|) = |u - v|(|u - v| + |v|) \\
&= |u - v|(|u - v| + 2 |v|) = |u - v|^2 + 2 |u - v||v|.
\end{align*}
\]
Furthermore, applying Lemma 12 with \( p = 0 \), \( q = 1 \), \( \alpha = \beta \), we have \( F_1(\alpha) = G(\alpha) \) there, thus we obtain that
\[
|F(x) - G(x)| \leq H(t, N, 1, \alpha).
\]
(69) and (70) yield that
\[
(71) \quad E_1 = \int_{-1/2}^{1/2} \left| |F(x)|^2 - |G(x)|^2 \right| |T(\alpha)| \, dx \leq
\]
\[
= \frac{1}{1/2} \int_{-1/2}^{1/2} |F(x) - G(x)|^2 |T(\alpha)| \, dx + 2 \int_{-1/2}^{1/2} |F(x) - G(x)| |G(x)| |T(\alpha)| \, dx \leq
\]
\[
\leq \frac{1}{1/2} \frac{H(t, N, 1, \alpha)}{|T(\alpha)|} \, dx + 2 \int_{-1/2}^{1/2} H(t, N, 1, \alpha) |G(x)| \, dx = E'_1 + 2E'_1.
\]
(71) will be estimated simultaneously with \( E_1 \); here we estimate only \( E'_1 \).

The function \( |G(x)| \) can be estimated by using Lemma 1. Furthermore, for \( |x| \equiv \log N/N \), we use the trivial inequality
\[
(72) \quad |T(\alpha)| = \left| \sum_{i=1}^{M} e(z^2 \alpha) \right| \leq \sum_{i=1}^{M} 1 = M \leq N^{1/2},
\]
while for \( \log N/N < |x| \equiv 1/2 \) (\( < 1/2 \sqrt{N} \), by (60)), we apply Lemma 6. In this way, we obtain that
\[
(73) \quad E'_1 = \int_{|x| \leq 1/N} \left\{ (a(t) - a(N))N + 2a(t) \right\} \left( 1 + \frac{1}{N} \right) \, dx + \frac{1}{2} a(t) \left( a(t) - a(N) \right) N^{1/2} \, dx + \int_{-1/N < x < 1/N} \left( \frac{a(t) - a(N)}{N} + 2a(t) \right) x \, dx \
+ \int_{\log N/N < |x| \leq 1/2} \left\{ (a(t) - a(N))N + 2a(t) \right\} \left( 1 + \pi \right) \, dx \leq \frac{1}{2} \left( a(t) - a(N) \right) N^{1/2} + 2a(t) \cdot 5 \cdot N^{3/2} + \frac{1}{2} a(t) \left( a(t) - a(N) \right) N^{3/2} \int_{1/N < |x| < 1/2} \frac{1}{\log N/N} \, dx + \frac{1}{2}) a(t) \left( a(t) - a(N) \right) N^{1/2} \int_{1/2 < |x| < 1/2} \frac{1}{\log N/N} \, dx \leq \frac{1}{2} \left( a(t) - a(N) \right) N^{1/2} + 2 \cdot \frac{1}{N} \cdot a^2(t) \cdot 5 \cdot N^{3/2} + \frac{1}{2} a(t) \left( a(t) - a(N) \right) N^{1/2} \int_{1/N < |x| < 1/2} \frac{1}{\log N/N} \, dx + \frac{1}{2} a(t) \left( a(t) - a(N) \right) N^{1/2} \int_{1/2 < |x| < 1/2} \frac{1}{\log N/N} \, dx.
\]
Here
\[
\int_{\log N \leq x \leq \log N^{1/2}} \frac{1}{|x|^{1/2}} \, dx = 2 \log \log N, \\
\int_{\log N^{1/2} \leq |x| \leq 1} \frac{1}{|x|^{1/2}} \, dx = 2 \cdot 2 \left( \frac{\log N}{N} \right)^{-1/2} = 4 \left( \frac{N}{\log N} \right)^{1/2}
\]
and
\[
\int_{\log N^{1/2} \leq |x| \leq 1} \frac{1}{|x|^{1/2}} \, dx = 2 \int_{0}^{1/\sqrt{2}} \frac{1}{x^{1/2}} \, dx = 2 \cdot 2 \left( \frac{1}{Q} \right)^{1/2} = \frac{4}{Q^{1/2}}.
\]
Thus with respect to (57), (60) and \( a(t) \equiv a(N) \) (by (47) and (58)),
\[
E''_1 \leq 2a(t)(a(t) - a(N))N^{3/2} + 20a^3(t)N^{3/2} + \\
+ a(t)(a(t) - a(N))N^{3/2} \log \log N + 10a^3(t)\log N + \\
+ 60a(t)(a(t) - a(N))N^{3/2} + 600a^3(t)\log N^2 Q^{-1/2} = \\
\leq 63a(t)(a(t) - a(N))N^{3/2} \log \log N + 30a^3(t)\log N \leq 630a^3(t)\log N^2 Q^{-1/2}.
\]

Now we are going to estimate \( E'_1 + E_2 \).
If \( 2 \equiv q \equiv Q, 1 \equiv p \equiv q - 1 \) then \( x \in I_{p,q} \) implies that
\[
\|x\| = \frac{1}{q} - \frac{1}{qQ} = \frac{1}{q} - \frac{1}{2q} = \frac{1}{2q}.
\]
Thus for \( 2 \equiv q \equiv Q, 1 \equiv p \equiv q - 1 \) and \( (p, q) = 1 \), Lemmas 1 and 12 (where \( F_1(x) = 0 \) in this case) and the trivial inequality (72) yield that
\[
\int_{I_{p,q}} |F(x)|^2 - |G(x)|^2 |T(x)| \, dx \leq \int_{I_{p,q}} |F(x)|^2 |T(x)| \, dx + \int_{I_{p,q}} |G(x)|^2 |T(x)| \, dx \leq \\
= \int_{I_{p,q}} |F(x)|^2 |T(x)| \, dx + \int_{I_{p,q}} a^2(t) \frac{1}{2q} N^{1/2} \, dx = \\
= \int_{I_{p,q}} H^2(t, N, q, \beta) \left| \beta \frac{p}{q} + \beta \right| \, d\beta + a^2(t) N^{1/2}.
\]
Hence
\[
E'_1 + E_2 \leq \int_{I_{p,q}} H^2(t, N, 1, \alpha) |T(x)| \, dx + \\
\leq \sum_{q=1}^{\infty} \sum_{(p, q) = 1} \left\{ \int_{-1/q}^{-1/2q} H^2(t, N, q, \beta) \left| \beta \frac{p}{q} + \beta \right| \, d\beta + a^2(t) N^{1/2} \right\}. \\
\leq \sum_{q=1}^{\infty} \sum_{(p, q) = 1} \left\{ \int_{-1/q}^{-1/2q} H^2(t, N, q, \beta) \left| \beta \frac{p}{q} + \beta \right| \, d\beta + a^2(t) R^2 N^{1/2}. \\
\]
To estimate $T\left(\frac{p}{q} + \beta\right)$, we use Lemmas 5 and 6 for $|\beta| \leq \log N/N$ and $\log N/N < |\beta| \leq \frac{1}{qQ}$, respectively. We obtain with respect to (57), (59) and (60) that (for $q \leq R$, $(p, q) = 1$)

$$
\int_{-\frac{1}{qQ}}^{+\frac{1}{qQ}} H^2(t, N, q, \beta) \left| T\left(\frac{p}{q} + \beta\right) \right| d\beta =
$$

$$
= \int_{|\beta| \leq \log N/N} \{2(a(t) - a(N))^2 N^2 + 16a^2(t) t^2 q^4 (1 + \pi^2 N^2)\} \left(\frac{N}{q}\right)^{1/2} d\beta +
$$

$$
= \int_{|\beta| > \log N/N} \{2(a(t) - a(N))^2 N^2 + 16a^2(t) t^2 q^4 (1 + \pi^2 N^2)\} \left(\frac{\log N}{q |\beta|}\right)^{1/2} d\beta <
$$

$$
< 2 \frac{\log N}{N} \{2(a(t) - a(N))^2 N^2 + 16a^2(t) t^2 q^4 \left(1 + \pi^2 \frac{\log N}{N^2} N^2\right)\} \left(\frac{N}{q}\right)^{1/2} +
$$

$$
+ 60(a(t) - a(N))^2 N^3 \left(\log N\right)^{1/2} q^{-1/2} \int_{\log N/N < |\beta| \leq \frac{1}{qQ}} |\beta|^{-1/2} d\beta +
$$

$$
= 480a^2(t) t^2 q^4 \cdot 11 \beta^2 N^2 \left(\frac{\log N}{q |\beta|}\right)^{1/2} d\beta <
$$

$$
< 84(a(t) - a(N))^2 N^{3/2} \log N \cdot q^{-1/2} + 32 \cdot \log N \cdot \log N \cdot a^2(t) t^2 q^7 N^2 \cdot 11 \cdot \log N \cdot 21 +
$$

$$
+ 120(a(t) - a(N))^2 N^2 \left(\log N\right)^{1/2} q^{-1/2} \int_{\beta < \frac{1}{qQ}} \beta^{-1/2} d\beta +
$$

$$
+ 10560a^2(t) t^2 q^7 N^2 \left(\log N\right)^{1/2} \int_{0}^{\frac{1}{qQ}} \beta^{1/2} d\beta =
$$

$$
= 84(a(t) - a(N))^2 N^{3/2} \log N \cdot q^{-1/2} + 7392a^2(t) t^2 N^{-1/2} \left(\log N\right)^2 q^{7/2} +
$$

$$
+ 120(a(t) - a(N))^2 N^2 \left(\log N\right)^{1/2} q^{-1/2} \cdot 2(qQ)^{-1/2} +
$$

$$
+ 10560a^2(t) t^2 q^{7/2} N^2 \left(\log N\right)^{1/2} \cdot \frac{7}{5} (qQ)^{-3/2} =
$$

$$
= (a(t) - a(N))^2 \{84 N^{3/2} \log N \cdot q^{-1/2} + 240 N^2 \left(\log N\right)^{1/2} (qQ)^{-1/2} q^{-1}\} +
$$

$$
+ a^2(t) t^2 \left(7392 N^{-1/2} \left(\log N\right)^2 q^{7/2} + 4224 N^2 \left(\log N\right)^{1/2} (qQ)^{-3/2} q\right)
$$

since

$$(x+y)^2 = 2x^2 + 2y^2$$

for any real numbers \(x, y\). Thus (75) yields with respect to (57) and (59) that

\[ E_1 + E_2 \leq \sum_{a=1}^{g-1} \left\{ (a(t) - a(N))^2 (84N^{3/2} \log N \cdot q^{3/2} + 240N^2 \log N)^{1/2} Q^{-1/2} q^{-1} \right\} + \frac{a^2(t)}{4} (7392N^{-1/2} (\log N)^2 q^{3/2} + 224N \log N)^{1/2} Q^{-1/2} q^{-1} \] 

\[ + \frac{a^2(t)}{4} (7392N^{-1/2} (\log N)^2 q^{3/2} + 224N \log N)^{1/2} Q^{-1/2} q^{-1} \] 

\[ < \sum_{a=1}^{g-1} \left( (a(t) - a(N))^2 (84N^{3/2} \log N \cdot q^{3/2} + 240N^2 \log N)^{1/2} Q^{-1/2} q^{-1} \right) + \frac{a^2(t)}{4} (7392N^{-1/2} (\log N)^2 q^{3/2} + 224N \log N)^{1/2} Q^{-1/2} q^{-1} \] 

\[ \leq \left( (a(t) - a(N))^2 (84N^{3/2} R^{3/2} \log N + 240N^2 \log N)^{1/2} Q^{-1/2} q^{-1} \right) + \frac{a^2(t)}{64} (7392N^{-1/2} (\log N)^2 R^{3/2} + 224N \log N)^{1/2} Q^{-1/2} q^{-1} \] 

Finally, in order to estimate \(E_1\), we use Lemma 7. Namely, if \( \alpha \in S \) then there exist integers \(p, q\) such that

\[ 1 \equiv q \equiv \alpha \pmod{\alpha}, \quad 0 \equiv p \equiv q-1, \quad (p, q) = 1 \]

and

\[ \left| \frac{\alpha - p}{q} \right| \leq \frac{1}{qQ}; \]

by (67), \( q \) satisfies also \( R < q \). Thus (41) and (43) in Lemma 7 hold (and also (42) holds by (60)). Hence, Lemma 7 yields that

\[ \sup_{\alpha \in S} \left| T(\alpha) \right| \leq \left( \frac{N}{R} \right)^{1/2} + 14Q \log N; \]

Thus we obtain applying Parseval's formula that

\[ E_2 = \int_S \left| |F(\alpha)|^2 - |G(\alpha)|^2 \right| |T(\alpha)| \, d\alpha \leq \]

\[ \sup_{\alpha \in S} \left| T(\alpha) \right| \left( \int_S |F(\alpha)|^2 \, d\alpha + \int_S |G(\alpha)|^2 \, d\alpha \right) < \]

\[ \left( 7N^{3/2} R^{-1/2} + 14Q^{3/2} (\log N)^{1/2} \right) \left( \int_S |F(\alpha)|^2 \, d\alpha + \int_S |G(\alpha)|^2 \, d\alpha \right) = \]

\[ = \left( 7N^{3/2} R^{-1/2} + 14Q^{3/2} (\log N)^{1/2} \right) (A(N) + a^2(t) N) = \]

\[ = \left( 7N^{3/2} R^{-1/2} + 14Q^{3/2} (\log N)^{1/2} \right) (a(N) N + a^2(t) N) \leq \]

\[ \leq \left( 7N^{3/2} R^{-1/2} + 14Q^{3/2} (\log N)^{1/2} \right) (a(t) N + a(t) N) = \]

\[ = a(t) \left( 14N^{3/2} R^{-1/2} + 28Q^{3/2} (\log N)^{1/2} \right) \]

by Lemma 9 and since \( a(N) \equiv a(t) \) by (47) in Lemma 11 and (58).
Collecting the results (62), (66), (68), (71), (74), (76) and (77) together, we obtain that
\[
\frac{1}{8} a^2(t) N^{3/2} \leq \int_8^1 |G(x)|^2 T(x) \, dx \leq E_1 + E_2 + E_3 \leq \\
\leq (E'_1 + 2E'_2) + E_2 + E_3 = 2E'_2 + (E'_1 + E_2) + E_3 < \\
< 126a(t)(a(t) - a(N)) N^{2/3} \log \log N + 1260a^2(t) tN(\log N)^{1/2} Q^{-1/2} + \\
+ (a(t) - a(N))^2 \{84N^{2/3} R^{2/3} \log N + 240N^2 (\log N)^{1/2} Q^{-1/2} R\} + \\
+ a^2(t) t^2 \{7392N^{-1/2} (\log N)^2 R^{1/2} + 4224N^2 (\log N)^{1/2} Q^{-5/8} R^2\} + \\
+ \frac{1}{64} a^2(t) N^{3/2} + a(t) \{4N^{2/3} R^{-3/2} + 28NQ^{1/2} (\log N)^{1/2}\}.
\]
Subtracting \(\frac{1}{64} a^2(t) N^{3/2}\) and then multiplying by \(\left(1 - \frac{1}{64}\right)^{-1} = \left(\frac{7}{64}\right)^{-1} = 7 \times 64 = 10\),
we obtain that
\[
a^2(t) N^{3/2} < 1260\alpha(t)(a(t) - a(N))^{2/3} \log \log N + 12600a^2(t) tN(\log N)^{1/2} Q^{-1/2} + \\
+ 120(a(t) - a(N))^2 \{7N^{2/3} R^{2/3} \log N + 20N^2 (\log N)^{1/2} Q^{-1/2} R\} + \\
+ 26000a^2(t) t^2 \{3N^{-1/2} (\log N)^2 R^{1/2} + 2N^2 (\log N)^{1/2} Q^{-5/8} R^2\} + \\
+ 140a(t) \{N^{3/2} R^{-1/2} + 2NQ^{1/2} (\log N)^{1/2}\}
\]
which proves Lemma 13.

6. In this section, we are going to simplify the functional inequality given in Lemma 13. It can be shown that we obtain the best possible estimate for \(a(x)\) in the case when the order of magnitude of the product \(QR\) is \(N/\log N\); thus we choose
\[
R = \frac{N}{Q}, \quad \frac{1}{\log N}.
\]
Furthermore, we put
\[
r = \frac{N}{t}, \quad s = \frac{N}{Q}.
\]
Then
\[
R = \frac{s}{\log N}.
\]
The inequalities (59) and (60) can be rewritten in form
\[
1 \leq \frac{s}{\log N} \leq \frac{N^{1/2}}{\log N},
\]
(78)

and
\[ 2N^{1/2} \leq \frac{N}{s} \leq \frac{N}{\log N}, \]
\[ \frac{1}{2} N^{1/2} \leq s \leq \log N, \]
(79)
respectively. (79) implies (78) thus it suffices to assume that (79) holds.

Finally, if we divide (61) by \( N^{1/2} \) then we obtain that
\[
a^2(t) < 1260a(t)(a(t)-a(N)) \log \log N + 12600a(t)r^{-1}s^{1/2}(\log N)^{1/2} +
+ 120(a(t)-a(N))^2(3s^{1/2}(\log N)^{-1/2} + 2s^{1/2}(\log N)^{-1/2}) +
+ 26000a(t)r^{-2}(3s^{1/2}(\log N)^{-1/2} + 2s^{1/2}(\log N)^{-1/2}) +
+ 140a(t)(s^{-1/2}(\log N)^{1/2} + 2s^{-1/2}(\log N)^{1/2}) <
< 1260a(t)(a(t)-a(N)) \log \log N +
+ 130000a(t)(r^{-1}s^{1/2}(\log N)^{1/2} + r^{-2}s^{1/2}(\log N)^{-1/2}) +
+ 3240(a(t)-a(N))^2s^{1/2}(\log N)^{-1/2} + 420a(t)s^{-1/2}(\log N)^{1/2}.
\]
Thus we have proved the following

**Lemma 14.** Let \( t, N, r \) be positive integers; \( s \) a real number such that
(80) \( N \equiv e^s \),
(81) \( N = \frac{r}{s} \),
(82) \( \log N \leq s \leq \frac{1}{2} N^{1/2} \).

Then
(83) \( a^2(t) < 1260a(t)(a(t)-a(N)) \log \log N +
+ 130000a(t)(r^{-1}s^{1/2}(\log N)^{1/2} + r^{-2}s^{1/2}(\log N)^{-1/2}) +
+ 3240(a(t)-a(N))^2s^{1/2}(\log N)^{-1/2} + 420a(t)s^{-1/2}(\log N)^{1/2} \).

7. In this section, we are going to complete the proof of our theorem by showing that the functional inequality given in Lemma 14 implies (2).

Let us put
\[ \phi(x) = \frac{(\log \log x)^{3/2}}{(\log x)^{1/2}} \]
for \( x \geq 3 \). Furthermore, for \( L = 3, 4, \ldots, \) let us define the sequence \( B(L) = \{b_1, b_2, \ldots\} \) by the following recursion: let \( b_1 = L \), and for \( k = 1, 2, \ldots, \) let
\[ b_{k+1} = b_k \left[ 4 \cdot 10^{2x}(\phi(b_k))^{-1/2}(\log b_k)^{3/2} \right]. \]

Obviously, \( (\phi(x))^{-1} + \infty \) as \( x \to +\infty \). Thus there exists a real number \( X_0 \).
such that \((\varphi(x))^{-1} > 1\) for \(x \in X_b\). Let us put \(L_1 = \max \{X_b, 3\}\). Then we obtain (by straight induction) that for \(L \equiv L_1\),

\[
\frac{b_{k+1}}{b_k} = \left[4 \cdot 10^{22} (\varphi(b_k))^{-11/2} (\log b_k)^{3/2}\right] \geq \left[4 \cdot 10^{22} \cdot 1 \cdot 1\right] = 4 \cdot 10^{22} > 1.
\]

Hence

\[
L = b_1 = b_2 < b_3 < \ldots \quad (\text{for } L \equiv L_1).
\]

We are going to show (by straight induction, using Lemma 14) that if \(L\) is large enough then for \(k = 1, 2, \ldots\),

\[
a(b_k) \equiv \frac{1}{\varphi(L)} \varphi(b_k).
\]

For \(k = 1\), the right hand side of (86) is

\[
\frac{1}{\varphi(L)} \varphi(b_k) = \frac{1}{\varphi(L)} \varphi(b_k) = \frac{1}{\varphi(L)} \varphi(L) = 1
\]

thus in this case, (86) holds trivially by Lemma 9.

Let us suppose now that (86) holds for some positive integer \(k\). We have to show that this implies also

\[
a(b_{k+1}) \equiv \frac{1}{\varphi(L)} \varphi(b_{k+1}).
\]

Let us suppose indirectly that

\[
a(b_{k+1}) > \frac{1}{\varphi(L)} \varphi(b_{k+1}).
\]

By the construction of the sequence \(\mathcal{B}(L)\),

\[
b_k / b_{k+1}.
\]

Hence,

\[
a(b_k) \equiv a(b_{k+1})
\]

by (47) in Lemma 11.

We are going to show that for sufficiently large \(L\), Lemma 14 is applicable with \(i = b_k\), \(N = b_{k+1}\),

\[
r = N/t = b_{k+1} / b_k = \left[4 \cdot 10^{22} (\varphi(b_k))^{-11/2} (\log b_k)^{3/2}\right],
\]

\[
s = 5 \cdot 10^6 (\varphi(b_k))^{-2} \log b_{k+1} = 5 \cdot 10^6 (\varphi(b))^{-2} \log N.
\]

Then by (85),

\[
N \gg t \gg L \quad (\text{for } L \equiv L_1).
\]

Thus (89) holds for \(L \equiv \max \{x^*, L_1\}\).

(81) holds by the definitions of \(N, t, r\) and \(\mathcal{B}(L)\).

By Lemma 9,

\[
s = 5 \cdot 10^6 (\varphi(b_k))^{-2} \log N \gg 5 \cdot 10^6 \log N \gg \log N.
\]
Finally, we have to prove that
\[ s < \frac{1}{2} N^{1/2}. \]

With respect to (84), (88) and (89),

\[ s = 5 \cdot 10^6 (a(b_k))^{-2} \log b_{k+1} \equiv \]
\[ \leq 5 \cdot 10^6 (\varphi(b_k))^{-2} \log b_{k+1} = 5 \cdot 10^6 \left( \frac{1}{\varphi(L)} \right)^{-2} \log b_{k+1} \equiv \]
\[ \leq 5 \cdot 10^6 (\varphi(b_k))^{-2} \log b_{k+1} = 5 \cdot 10^6 (\varphi(N))^{-1/2} \log N = 5 \cdot 10^6 \frac{\log N^{1/3}}{(\log \log N)^{1/3}} \]

for \( L \equiv L_1 \equiv X_0 \). Thus it suffices to show that
\[ 5 \cdot 10^6 \frac{\log N^{1/3}}{(\log \log N)^{1/3}} < \frac{1}{2} N^{1/2}. \]

But this holds trivially for large \( N \), i.e. for \( L \equiv L_2 \) (in view of (91)).

Thus Lemma 14 is applicable and it yields that (83) holds. To deduce a contradiction from (83), we have to estimate \( r \) and \( a(t) - a(N) \) in terms of \( a(t) \) and \( N \).

Obviously,
\[ r = \frac{N}{t} = \frac{b_{k+1}}{b_k} = \left[ 4 \cdot 10^{25} (\varphi(b_k))^{-1/2} (\log b_k)^{3/2} \right] = \]
\[ = \left[ 4 \cdot 10^{25} (\varphi(t))^{-1/2} (\log t)^{3/2} \right] = \left[ 4 \cdot 10^{25} \left( \frac{\log \log t}{(\log \log t)^{1/3}} \right)^{-1/2} (\log t)^{1/2} \right] = \]
\[ \leq \left[ 4 \cdot 10^{25} \frac{(\log t)^{10/3}}{(\log \log t)^{1/3}} \right] \leq 4 \cdot 10^{25} \frac{(\log t)^{10/3}}{(\log \log t)^{1/3}} \]

and with respect to (84),

\[ r = \frac{N}{t} = \left[ 4 \cdot 10^{25} \frac{(\log t)^{10/3}}{(\log \log t)^{1/3}} \right] \geq 2 \cdot 10^{25} \frac{(\log t)^{10/3}}{(\log \log t)^{1/3}} \quad \text{(for } L \equiv L_3 \text{)}.

In view of (91), (93) and (94) imply that for \( L \leq L_3 \),

\[ (0 < r) \log r = \log N - \log t = \]
\[ = \frac{10}{3} \log \log t + (1) \cdot \log (4 \cdot 10^{25}) + (11/3) \log \log \log t \approx \]
\[ < 4 \log \log t \quad \text{(for } L \leq L_3 \text{)} \]

hence for \( L \equiv L_3 \),

\[ \log t = \log N - 4 \log \log t > \log N - 4 \log \log N > \]
\[ > \frac{1}{2} \log N \quad \text{(for } L \equiv L_3 \text{)} \]

*Acta Mathematica Academiae Scientiarum Hungaricae 31, 1976*
and for $L \equiv L_4$,

(97) \[ \log \log t > \log \left( \frac{1}{2} \log N \right) = \log \log N - \log 2 > \frac{1}{2} \log \log N \quad \text{(for } L \equiv L_4). \]

(86), (88), (91), (95), (96) and (97) yield that for $L \equiv L_4$,

(98) \[ a(t) - a(N) = a(t) \left( 1 - \frac{a(N)}{a(t)} \right) < a(t) \left( 1 - \frac{(\varphi(L))^{-1} \varphi(N)}{(\varphi(L))^{-1} \varphi(t)} \right) = \]

\[ = a(t) \frac{\varphi(t) - \varphi(N)}{\varphi(t)} = a(t) \frac{(\log t)^{1/3}}{\log \log t^{2/3}} \left( \frac{\log \log N^{1/3} - (\log t)^{1/3}}{(\log t)^{1/3} - (\log N)^{1/3}} \right) < \]

\[ < a(t) \frac{2(log t)^{1/3}}{log \log N^{1/3} + (log N log t)^{1/3} + (log t)^{1/3}} = \]

\[ = 2a(t) \frac{\log N - \log t}{(\log N)^{1/3} + (\log N log t)^{1/3} + (\log t)^{1/3}} < \]

\[ < 2a(t) \frac{4 \log \log t}{(\log N)^{1/3} - 3 (\log t)^{1/3}} < \frac{8}{3} a(t) \frac{\log \log N}{(\log N)^{1/3} \left( \frac{1}{2} \log N \right)^{2/3}} < \]

\[ < 6a(t) \frac{\log \log N}{\log N}. \]

By (88), (90), (91), (92), (94), (96) and (98), (83) implies that for $L \equiv L_7$,

\[ a^2(t) < 1260 a(t) - 6a(t) \frac{\log \log N}{\log N} \cdot \log \log N + \]

\[ + 130000 a^2(t) \left( 2 - 10^{-2b} \frac{(\log \log t)^{1/3}}{(\log t)^{1/3}} \left( 5 \cdot 10^a \frac{(\log N)^{1/3}}{(\log \log N)^{1/3}} \right)^{1/3} \cdot (\log N)^{1/3} + \right. \]

\[ \left. + \left( 2 - 10^{-2b} \frac{(\log \log t)^{1/3}}{(\log t)^{1/3}} \right)^2 \left( 5 \cdot 10^a \frac{(\log N)^{1/3}}{(\log \log N)^{1/3}} \right)^{1/3} \cdot (\log N)^{-1/3} \right) + \]

\[ + 3240 \left( 6a(t) \frac{\log \log N}{\log N} \right)^2 \left( 5 \cdot 10^a (a(t))^{-1/2} \log N^{1/3} \cdot (\log N)^{1/3} \right) + \]

\[ - 420 a(t) (5 \cdot 10^a (a(t))^{-1/2} \log N)^{-1/3} \cdot (\log N)^{1/3} = \frac{7560 (\log \log N)^2}{\log N} a^4(t) + \]

\[ + 130 \cdot 10^a a^2(t)^2 \left( 2 - 10^{-2b} \frac{(\log \log N)^{1/3}}{(\log \log N)^{1/3}} \cdot 3 \cdot 10^a \frac{(\log N)^{1/3}}{(\log \log N)^{1/3}} \right) + \]

\[ \ldots \]

\[ \ldots \]

\[ \ldots \]
\[ + 2^{-2} \cdot 10^{-44} \cdot \left( \frac{\log \log N}{\log N} \right)^{3/2} \cdot 5^{1/2} \cdot 5^2 \cdot 10^{20} \left( \frac{\log N}{\log N} \right)^{2/3} \leq \]

\[ + 4 \cdot 10^2 \cdot 36 \cdot a^2(t) \left( \frac{\log \log N^2}{\log N^2} \right) \cdot 125^{1/2} \cdot 10^8 (a(t))^{-8} \log N + \]

\[ + (21^2 \cdot 2^2 \cdot 10^4 / 500 \cdot 2^2 \cdot 10^4 \cdot 25)^{1/3} a^2(t) \leq \]

\[ \leq \frac{1}{10} a^2(t) + a^2(t) \left\{ 130 \cdot 10^{-10} \cdot 27^{1/2} \cdot 3 \cdot \left( \frac{\log \log N^2}{\log N^2} \right) + 130 \cdot 10^{-9} \cdot 2^{-2} \cdot 27 \cdot 3 \cdot 5^8 \right\} \leq \]

\[ + 1 + 44 \cdot 10^2 \cdot 12 a^2(t) \left( \frac{\log \log N^2}{\log N} \right) \left( \frac{1}{\varphi(L)} \frac{\varphi(N)}{N} \right)^{-3} + \left( \frac{441}{500} \cdot \frac{1}{25} \right)^{1/3} a^2(t) \leq \]

\[ \leq \frac{1}{10} a^2(t) + a^2(t) \left\{ \frac{1}{10} + 390 \cdot 10^{-3} \right\} + 2 \cdot 10^{15} a^2(t) \varphi^3(L) + \frac{1}{5} a^2(t) \leq \]

\[ \leq \frac{1}{10} a^2(t) + a^2(t) \left( \frac{1}{10} + \frac{2}{5} \right) + \frac{1}{5} a^2(t) + \frac{1}{5} a^2(t) = 2 a^2(t) \leq \]

provided that

\[ 2 \cdot 10^{15} \varphi^3(L) \leq \frac{1}{5}, \quad \varphi(L) \leq 10^{-10/3} \]

but this holds for \( L \approx L_k \).

Thus for large \( L \), the indirect assumption (88) leads to the contradiction \( a^2(t) \leq a^2(t) \), which proves (86).

Finally, if \( x \) is a positive integer satisfying \( x \approx b_k = L \), then there exists a positive integer \( k \) such that \( b_k \leq x < b_{k+1} \). By (48) in Lemma 11, (86) implies that

\[ a(x) \leq \left( \frac{1 + b_k}{x} \right) a(b_k) \leq 2 \cdot \frac{1}{\varphi(L)} \varphi(b_k) \leq \]

\[ \leq 2 \cdot \frac{1}{\varphi(L)} \left( \frac{\log \log b_k}{\log b_k} \right)^{1/3} \leq 2 \cdot \frac{1}{\varphi(L)} \left( \frac{\log \log x}{\log x} \right)^{1/3}. \]

With respect to (96),

\[ \log b_k \geq \frac{1}{2} \log b_{k+1} \geq \frac{1}{2} \log x. \]

Thus we obtain from (99) that

\[ a(x) \leq 2 \cdot \frac{1}{\varphi(L)} \left( \frac{\log \log x}{\log x} \right)^{1/3} \leq \frac{4}{\varphi(L)} \left( \frac{\log \log x}{\log x} \right)^{1/3} \quad \text{for} \quad x \leq L \]

which completes the proof of our theorem.
We remark that $L$ can be chosen as the least positive integer $L$ satisfying $L \equiv \{a, b, L_2, \ldots, L_8\}$. All the constants $L_3, L_2, \ldots, L_8$ are explicitly computable thus also the constants in (100) are explicitly computable.

8. In Part II of this series, we will give a lower estimate for $a(x)$.

References


Received January 12, 1977

Mathematical Institute
Of the Hungarian Academy of Sciences

Acta Mathematica Academiae Scientiarum Hungaricae 31, 1978