# Problems and results in additive number theory

par M. P. Erdös (Haifa)

In this lecture I will discuss several problems in additive number theory. They will not have much in common, except that they are all combinatorial in nature and that probability theory can be applied with advantage to most of them.

**1.** Let $a_1 < a_2 < \ldots$ be an infinite sequence of integers, denote by $f(n)$ the number of solutions of $n = a_i + a_j$ where $a_i + a_j$ counts twice if $i \neq j$ and once if $i = j$. Turán and I [1] proved that $f(n)$ can not be constant from a certain point on. Our proof though short and simple used lots of function theory (Fabry's gap theorem). But G. Dirac [2] observed that the theorem is trivial, since if $n = 2\,a_k$ $f(n)$ is odd (because of $n = a_k + a_k$), but if $n$ is not of this form then $f(n)$ is even. Dirac [2] observed that the definition of $f(n)$ can be modified in two ways. Define $f'(n)$ as the number of solutions of $n = a_i + a_j$ where all solutions count once and in $f''(n)$ only the solutions with $i \neq j$ are permitted. He and Newman [2] both proved that $f'(n)$ can not be constant from a certain point on, for if $f'(l+1) = f'(l+2) = \ldots$ we would evidenly have

$$\frac{1}{2}\left[\left(\sum z^{a_k}\right)^2 + \sum z^{2a_k}\right] = \sum_{n=0}^{\infty} f'(n)\, z^n$$

$$= \mathrm{P}_l(z) + a\frac{z^{l+1}}{1-z}, \quad [f'(l+1) = a], \qquad (1)$$

where $\mathrm{P}_l(z)$ is a polynomial of degree $\leqslant l$. If $z \longrightarrow -1$ on the real axis, the right side remains bounded, but the left side approaches infinity, since both terms on the left side are positive and the second tends to infinity. Thus (1) can not hold, which proves the theorem.

[1] *Journal London Math. Soc.*, **16** (1941), 212-215.
[2] *Ibid.*, **26** (1951), 312-313.

Dirac (2) also conjectured that $f''(n)$ can not be constant from a certain point on. This and considerably more was proved by Fuchs and myself (3). Turán and I (1) conjectured that if $f(n) > 0$ for all sufficiently large $n$ then $\limsup f(n) = \infty$. This conjecture has not yet been proved and seems very difficult. A still stronger conjecture would be that if $a_k < ck^2$ for all $k$, then $\limsup f(n) = \infty$. The best result we can prove (4) is that in this case $\lim\ \sup f(n) \geqslant 2$. Turán and I (1) further conjectured that

$$\sum_{k=1}^{n} f(k) = cn + o(1)$$

is impossible. Fuchs and I (3) proved this conjecture. In fact we showed that for $c > 0$

$$\sum_{k=1}^{n} f(k) = cn + o\left(\frac{n^{\frac{1}{4}}}{(\log n)^{\frac{1}{2}}}\right) \tag{2}$$

is impossible. The same holds for

$$\sum_{k=1}^{n} f'(k) \text{ and } \sum_{k=1}^{n} f''(k)\ .$$

If $a_k = k^2$ one comes to the problem of lattice points in the circle of radius $n^{\frac{1}{2}}$. Here Hardy and Landau (5) proved that

$$\sum_{k=1}^{n} f(k) = \pi(n) + o\left[(n \cdot \log n)^{\frac{1}{4}}\right] \tag{3}$$

does not hold. (3) is stronger than (2) by a factor $(\log n)^{\frac{3}{4}}$, but we proved out theorem for general sequences and not only for squares. Further our proof is very much simpler than that of Hardy and Landau, in fact we only use the Parseval equality.

One could have tried to prove the conjecture: $a_k < c \cdot k^2$ for all $k$ implies $\limsup f(n) = \infty$ by proving that if for all $k$, $a_k < ck^2$ then

$$\lim\sup \frac{1}{n} \sum_{k=1}^{n} f(k)^2 = \infty\,. \tag{4}$$

[3] Our paper will appear in the *Journal of the London Math. Soc.*

[4] *Ibid.* (1). The details of the proof are given by A. Stöhr, *Journal reine und angew. Math.*, **194** (1955), 132-133.

[5] Landau, *Zahlentheorie*, Vol. 2, 233-239.

Unfortunately (4) is false. In fact in a certain sense it is false for almost all sequences. Consider the space of all sequences of integers. We introduce a measure into this space as follows: Consider an infinite number of copies of the points 0 and 1. In the $n$-th copy $I_n$ the measure of 1 is $\alpha n^{-\frac{1}{2}}$ and of 0 is $1 - \alpha n^{-\frac{1}{2}}$. This defines in a well-known and obvious way a measure in the product space $\prod_{n=1}^{\infty} I_n$ (if for all $n$ the measure of both 0 and 1 is $\frac{1}{2}$, we obtain the Lebesgue measure on the interval $(0, 1)$). Thus we defined a measure in the space of sequences of 0-s and 1-s. Now we map a sequence of 0-s and 1-s into a sequence of integers by putting $n$ into our sequence if and only if the sequence of 0-s and 1-s cointains 1 at the $n$-th place. Thus we introduced a measure in the space of all sequences of integers. Speaking slightly imprecisely we can say that the probability of $n$ occurring in our sequence equals $\alpha n^{-\frac{1}{2}}$, or more precisely: The measure of the set of sequences where $n$ occurs equals $\alpha n^{-\frac{1}{2}}$. It is quite easy to show that for almost all sequences $a_1 < a_2 < \dots$ (i.e. except for a set of sequences of measure 0)

$$a_k = [1 + o(1)] \frac{k^2}{4\alpha^2}.$$

With somewhat more trouble I can prove that with probability 1 for every $r$

$$\sum_{n=1}^{X} [f(n)]^r = c_r X + o(X), \quad c_r = c_r(\alpha).$$

Thus (4) is false for almost all sequences. Similarly it can be shown that the density $d_l = d_l(\alpha)$ of integers with $f'(n) = l$ (or $f(n) = 2l$) exists and $\sum_{l > l_0} d_l(\alpha) \to 1$ as $\alpha \to \infty$ (for every $l_0$).

**2.** More than 20 years ago Sidon asked the question if there exists a sequence $a_1 < a_2 < \dots$ of integers for which $f(n) > 0$ for all sufficiently large $n$, but $\lim \frac{f(n)}{n^\varepsilon} = 0$ for all $\varepsilon > 0$. Using combinatorial and probabilistic arguments I [6] proved the existence of such a sequence, in fact I proved that there exists a sequence satisfying for $n > n_0$

$$0 < f(n) < c \log n. \tag{5}$$

I did not succeed in constructing such a sequence but proved that in a certain sense almost all sequences satisfy (5. A few days ago i noticed that this fact can be made more precise and that my original proof can be simplified and made more intuitive. Consider the space of all sequences of integers where the probability of $n$ occurring in our sequence equals $c_1\left(\frac{\log n}{n}\right)^{\frac{1}{2}}$ where $c_1 > \left(\frac{2}{\pi}\right)^{\frac{1}{2}}$. It is easy to see that for almost all sequences

$$a_k = [1 + o(1)]\,\frac{k^2}{4\,c^2 \log k}\ .$$

Now we prove that for almost all sequences $f(n) = 0$ holds only for a finite number of $n$-s (i.e. for almost all sequences $f(n) > 0$ for $n > n_0$). Denote by $\mathrm{E}_n$ the event that $f(n) = 0$ and by $\mathrm{P}(\mathrm{E}_n)$ we denote its probability. $\mathrm{E}_n^{(k)}$ denotes the event that $k$ and $n-k$ do not both occur in our sequence. Clearly $\mathrm{E}_n$ can occur only if all the $\mathrm{E}_n^{(k)}$ occur $1 \leqslant k < \frac{n}{2}$. The events $\mathrm{E}_n^{(k)}$, $1 = k < \frac{n}{2}$ are clearly independent. Thus

$$\mathrm{P}(\mathrm{E}_n) \leqslant \prod_{1 \leq k < \frac{n}{2}} \mathrm{P}(\mathrm{E}_n^{(k)}) = \prod_{1 \leq k < \frac{n}{2}} \left(1 - \frac{c_1^2\,[\log k \cdot \log (n-k)]^{\frac{1}{2}}}{[k\,(n-k)]^{\frac{1}{2}}}\right)$$

$$= \exp\left[-\left([1 + o\,(1)]\,c_1^2 \log n \sum_{1 \leq k < \frac{n}{2}} \frac{1}{[k\,(n-k)]^{\frac{1}{2}}}\right)\right]$$

$$= \exp\left(-[1 + o\,(1)]\,c_1^2 \log n \cdot \frac{\pi}{2}\right) < \frac{1}{n^{1+\varepsilon}}\ ,$$

or $\sum_{n=1}^{\infty} \mathrm{P}(\mathrm{E}_n) < \infty$. Thus by the Borel-Cantelli lemma the probability that $f(n) = 0$ holds infinitely often is $0$, which proves our assertion. It can be proved though with somewhat more trouble that if $c_1 < \left(\frac{2}{\pi}\right)^{\frac{1}{2}}$, then for almost all sequences $f(n) = 0$ holds infinitely often. By somewhat longer computation we can prove that if $c_1 > \left(\frac{2}{\pi}\right)^{\frac{1}{2}}$ then there exists a $c_2 = c_2(c_1) > 0$ so that for almost all sequences $f(n) > c_2 \log n$ holds for all but finitely many $n$.

[6] *Acta Sci. Math. Szeged*, **15** (1954), 255-259.

Next we outline the proof that for every $c_1 > 0$ there exists a $c_3 = c_3(c_1)$ so that with probability 1 for all but finitely many $n$ we have $f(n) < c_3 \log n$. To show this denote by $E_{n, c_3}$ the event that $f(n) > c_3 \log n$, and as before $E_n^{(k)}$ is the event that both $k$ and $n-k$ do not simultaneously occur in our sequence. Clearly $E_{n, c_3}$ holds only if $E_n^{(k)}$ fails to hold for at least $\frac{c_3}{2} \log n$ values of $k$. Now by standard but somewhat lengthy arguments of probability theory it follows that for sufficiently large $c_3 = c_3(c_1)$

$$P(E_{n, c_3}) < \frac{1}{n^{1+\varepsilon}} .$$

Thus by the Borel-Cantelli lemma it follows that with probability 1 $f(n) > c_3 \log n$ holds only for finitely many $n$. This completes the proof of (5). In fact we proved that a somewhat stronger result, namely that for almost all sequences and sufficiently large $n$

$$c_2 \log n < f(n) < c_3 \log n . \tag{6}$$

Using standard methods of probability theory it is not difficult to prove that for almost all sequences

$$f(n) = [1 + o(1)] \frac{c_1{}^2 \pi}{2} \log n \tag{7}$$

holds for all $n$, neglecting $a$ sequence of $n$-s having density 0. On the other hand the probability that (7) holds for all but a finite number of $n$ is 0. In fact I do not know whether there exists a sequence satisfying (7) for all $n$, i.e. if there exists a sequence with $\frac{f(n)}{\log n}$ tending to a limit $\neq 0$.

Let on the other hand $g(k)$ be an increasing function satisfying $\frac{g(k^2)}{g(k)} \to 1$ as $k \to \infty$. Consider the space of all sequences where the probability of $n$ occurring in our sequence equals $\frac{g(n)(\log n)^{\frac{1}{2}}}{n^{\frac{1}{2}}}$. Then for almost all sequences

$$f(n) = [1 + o(1)] \frac{\pi}{2} g(n)^2 \cdot \log n ,$$

holds for all but finitely many $n$. The proof follows by standard arguments of probability theory and will be omitted.

Consider again the space of all sequences of integers. Assume that the probability of $n$ occurring in our sequence equals $c\left(\frac{\log n}{n}\right)^{\frac{1}{k}}$ where $c$ is a sufficiently large constant. Denote by $f_k(n)$ the number of solutions of

$$n = a_{i_1} + a_{i_2} + \ldots + a_{i_k}\,.$$

Then for almost all sequences

$$c_1 \log n < f_k(n) < c_2 \log n\,, \quad c_1 = c_1(c), \quad c_2 = c_2(c) \qquad (8)$$

holds for all but finitely many $n$. The proof of (8) is similar but more complicated than that of (6) and will be omitted.

At present I can not decide the question whether a sequence $a_1 < a_2 < \ldots$ exists with $f_k(n) > 0$ for all $n > n_0$ and $f_k(n)/\log n \longrightarrow 0$ as $n \longrightarrow \infty$. In fact I can decide this for no $k \geqslant 2$.

**3.** Sidon called a sequence $a_1 < a_2 < \ldots$ a $B_2$ sequence if the sums $a_i + a_j$ are all different. Turán and I ([4]) proved that for every $B_2$ sequence $\limsup \frac{a_k}{k^2} = \infty$, but that there exists $B_2$ sequences with $\liminf \frac{a_k}{k^2} < \infty$. It is not difficult to construct a $B_2$ sequence for which $a_k < ck^3$ holds for all $k$, and it seems likely that for every $\varepsilon$ there exists a $B_2$ sequence for which $a_k < ck^{2+\varepsilon}$ holds for every $k$. Unfortunately probability theory does not seem to help with this problem. The best result I can obtain is that there exists a sequence satisfying $a_k < k^{2+\varepsilon}$ for which $f(n)$ is bounded.

**4.** Let $a_1 < a_2 < \ldots$ be any infinite sequence of integers. Straus and I conjectured that there always exists a sequence $b_1 < b_2 < \ldots$ of density 0, so that every sufficiently large integer is of the form $a_i + b_j$. Lorentz ([7]) proved this conjecture. In fact he showed that there exists such a sequence which satisfies for every $x$

$$B(x) < c \sum_{k=1}^{X} \frac{\log A(k)}{A(k)}\,, \qquad (9)$$

where $A(x)$ and $B(x)$ denotes the number of $a$-s, respectively $b$-s not exceeding $x$. Lorentz remarked that if the $a$-s are the primes then $B(x)$ can be chosen to be $< c(\log x)^3$. He asked me if this can be improved. I ([8]) showed by using com-

[7] *Proc. Amer. Math. Soc.*, **5** (1954), 838-841.

[8] *Ibid.*, **5** (1954), 847-853.

binatorial and probabilistic arguments that the sequence $b_1 < b_2 < \dots$ can be chosen so that $B(x) < c(\log x)^2$. Without changing the idea of the original proof we can make the connections with probability theory clearer. Let $c$ be a sufficiently large constant, and consider the space of all sequences of integers where the probability of $n$ occurring in our sequence equals $c\,\frac{\log n}{n}$. A simple probabilistic argument shows that

$$B(x) = [1 + 0(1)]\, 2\, c_1 (\log x)^2$$

for almost all sequences. Denote by $E_n$ the event that $n$ is not of the form $p + b$. Then it can be proved by methods similar to those used in my paper [8] that

$$P(E_n) < \frac{1}{n^{1+\varepsilon}} . \tag{10}$$

Thus from (10) and the Borel-Cantelli lemma it follows that for almost all sequences every sufficiently large integer is of the form $p + b$, which completes the proof of our assertion.

At present I can not decide if there exists a sequence $b_1 < b_2 < \dots$ satisfying $B(x)/(\log x)^2 \longrightarrow 0$ and such that every sufficiently large integer is of the form $p + b$. It is of course obvious from the prime number theorem that such a sequence must satisfy

$$\liminf\ B(x)\,\frac{\log x}{x} \geqslant 1 .$$

But perhaps even the proof of

$$\limsup\ B(x)\,\frac{\log x}{x} > 1$$

is not entirely trivial, at least I have not been able to prove it.

Several analogous problems can be stated. I only want to mention two of them. Let $b_1 < b_2 < \dots$ be an infinite sequence of integers, so that every integer is of the form $b + k^2$. Denote by $B(x)$ the number $b$-s not exceeding $x$. It is easy to see that

$$\limsup \frac{B(x)}{x^{\frac{1}{2}}} > 1$$

A simple example shows that $\limsup \frac{B(x)}{x^{\frac{1}{2}}}$ can be finite. To see this consider the integers

$$2^k \leqslant b \leqslant 2^k + 4{,}2^{\frac{2}{k}},\ k = 1, 2, \dots .$$

It is easy to see that in this case every integer is of the form $b+k^2$ and that $\limsup \frac{B(x)}{x^{\frac{1}{2}}}$ is finite. I can not determine the smallest possible value of $\limsup \frac{B(x)}{x^{\frac{1}{2}}}$. Clearly $B(x) \geqslant x^{\frac{1}{2}}$ holds, but I can not prove that $\liminf \frac{B(x)}{x^{\frac{1}{2}}} > 1$. Another question would be to estimate the smallest possible value of $t$ for which there exists a sequence

$$b_1^{(x)} < b_2^{(x)} < \ldots < b_t^{(x)}$$

so that every integer $n \leqslant x$ is of the form $b_c^{(x)} + k^2$. Clearly $t \geqslant x^{\frac{1}{2}}$.

Let $b_1 < b_2 < \ldots$ be an infinite sequence of integers with the property that every integer is of the form $2^k + b$. Clearly $B(x) \geqslant \frac{x \log 2}{\log x}$ but here I can not even prove that there exists a sequence with

$$\liminf B(x) \cdot \frac{\log x}{x} < \infty .$$

**5.** Let $a_1 < a_2 < \ldots$ be any sequence of integers. We define the asymptotic density $d_a$ of the sequence as $\liminf \frac{A(x)}{x}$, and its Schnirelmann density $d_s$ as the greatest lower bound of $\frac{A(x)}{x}$. Thus the asymptotic density of the integers $\geqslant 2$ is 1 and its Schnirelmann density is 0. The sum $A+B$ of the two sequences $a_1 < a_2 < \ldots$ and $b_1 < b_2 < \ldots$ is defined as the sequence consisting of the integers $\{a_i\}$, $\{b_j\}$, $\{a_i + b_j\}$. The well-known $\alpha + \beta$ theorem of Mann [9] states that if A and B have Schnirelmann densities $\alpha$ respectively $\beta$, then

$$d_s(A+B) \geqslant \min(1, \alpha+\beta) . \tag{11}$$

A sequence A is called by Khintchin an essential component if for every sequence B with $d_s(B) > 0$, $d_s(A+B) > d_s(B)$. By (11) every sequence of positive density is an essential component. (This can of course be proved without using (11).) Khintchin [10] proved that the squares are an essential component, thus giving an example of a sequence of density 0 which is an essential component. The sequence B

[9] *Annals of Math.*, **43** (1942), 523-527.
[10] *Math. Sbornik*, **40** (1933).

is called a basis of order $k$, if every integer is the sum of $k$ or fewer $b$-s. Let $d_s(A) = \alpha$ then I [11] proved that

$$d_s(A + B) \geqslant \alpha + \frac{\alpha(1-\alpha)}{2k}. \qquad (12)$$

Thus every base is an essential component. Several authors improved (12) in various ways [12]. I conjectured that

$$d_s(A + B) \geqslant \alpha + \frac{\alpha(1-\alpha)}{k}. \qquad (13)$$

The proof of (12) is based on the following lemma: If A is a sequence of density $\alpha$, then for every $n$ there exists an integer $k_n$ so that the number of distinct integers $N_n(A, A + k_n)$ not exceeding $n$ of the sequences A, $A + k_n$ satisfies

$$N_n(A, A + k_n) \geqslant \left(\alpha + \frac{\alpha(1-\alpha)}{2}\right) n. \qquad (14)$$

(13) would follow if instead of (14) one could prove

$$N_n(A, A + k_n) \geqslant [\alpha + \alpha(1-\alpha)]\, n. \qquad (15)$$

It is not difficult to show that (15) if true is certainly best possible i.e. $N_n(A, A + k_n) \geqslant [\alpha + \alpha(1-\alpha) + \varepsilon]\, n$ is false for all $\alpha$ and $n > n_0(\alpha, \varepsilon)$. In fact it follows by a simple probability argument that (15) is best possible for almost all sequences of density $\alpha$.

A somewhat similar question is the following one: Let $a_1, a_2, \ldots, a_{2n}$ be $2n$ integers in the interval $(1, 4n)$ and let $b_1, b_2, \ldots, b_{2n}$ be the other $2n$ integers of the same interval. Does there exist an integer $x$ so that the number of solutions of $a_i + x = b_j$ is at least $n$? If the $a$-s are the integers $n+1, n+2, \ldots, 3n$ we see immediately that the value $n$, if true is certainly best possible. It is quite easy to see that there exists an $x$ so that the number of solutions of $a_i + x = b_j$ is at least $\frac{n}{2}$. To see this we observe that the number of solutions of $a_i + y = b_j$ is $4n^2$ and that there are $8n$ possible choices of $y$ (i.e. $-4n \leqslant y \leqslant 4n$, $y \neq 0$). Thus for some $y_0$ there are at least $\frac{n}{2}$ $b$-s in $a_i + y_0$, as stated. Scherk improved $\frac{n}{2}$ to $n(2 - \sqrt{2})$, but up to now the conjecture on $n$ is neither proved nor disproved [13].

[11] *Acta arithm.*, **1** (1936), 197-200.

[12] For the litterature see the paper of Stöhr, *ibid.* [4], further a recent paper by Kasch, *Math. Zeitschrift*, 62 (1955), 368-387.

[13] This question is stated by P. Erdös, *Riveon Lematematika*, **9** (1955), 48.

Linnik [14] was the first to give an example of an essential component which is not a basis, Linnik's proof ot this fact was rather complicated. Recently Stöhr and Wirzing [15] gave a very simple proof of this result, in fact their sequence B has the property that it is not a basis but that if $d_s(\mathrm{A}) > 0$ then $d_a((\mathrm{A}+\mathrm{B}) = 1$. Linnik's example has the property that $\mathrm{N}_n(\mathrm{B}) < n^\varepsilon$ for every $\varepsilon > 0$ of $n > n_0(\varepsilon)$. This led me to the following conjecture: Let $n_1 < n_2 < \dots$ be an infinite sequence of integers satisfying $\frac{n_{k-1}}{n_k} > c > 1$, then our sequence can not be an essential component. I was so far unable to prove this conjecture. Denote by $p(k)$ the smallest value of $r$ for which $k = a_{i_1} n_{i_1} + n_{i_2} + \dots + n_{i_r}$. It seems likely that to every $\alpha$, $\varepsilon$ and $x > x_0(\alpha, \varepsilon)$ there exists an $r = r(\alpha, \varepsilon, x)$ so that the set of integers $k \leqslant x$ for which $p(k) \leqslant r$ have Schnirelmann density between $\alpha - \varepsilon$ and $\alpha$, and the Schnirelmann density of the integers $k \leqslant x$ for which $p(k) \leqslant r + 1$ is between $\alpha$ and $\alpha + \varepsilon$. This if true would prove our conjecture. (The Schnirelmann density of a finite sequence $a_1 < a_2 < \dots < a_k \leqslant x$ is defined as

$$\min_{1 \leq k \leq x} \frac{\mathrm{N}_k(\mathrm{A})}{k} \Big).$$

It would also be of interest to decide whether there exists a sequence $b_1 < b_2 < \dots$ which is not a basis and which has the following property: If $a_1 < a_2 < \dots$ is a sequence of density $\alpha$, then to every $n$ there exists a $b_i = b_i(n)$ so that

$$\mathrm{N}_n(\mathrm{A},\ \mathrm{A} + b_i) \geqslant n[\alpha + f(\alpha)]$$

where $f(\alpha) > 0$ for $0 < \alpha < 1$.

**6.** Some time ago Moser and I raised the following problem: What is the maximum number of integers $a_1 < a_2 < \dots < a_k \leqslant x$ so that all the $2^k - 1$ sums

$$a_{i_1} + a_{i_2} + \dots + a_{i_r}, \quad 1 \leqslant r \leqslant k, \quad \text{the } a\text{-s all distinct} \qquad (16)$$

are all different. In particular is it possible to give $k + 2$ such $a$-s not exceeding $2^k$. ($1, 2, \dots, 2^k$ shows that it is possible to give $k + 1$ such integers.) Denote by $g(x)$ the maximum value of $k$, thus $g(2^k) \geqslant k + 1$. All the sums (16) are less than $kx$. Thus

$$2^{g(x)} \leqslant x \cdot g(x)$$

or

$$g(x) < \frac{\log x}{\log 2} + [1 + o(1)] \frac{\log \log x}{\log 2}. \qquad (17)$$

[14] *Mat. Sbornik*, N. S. **10** (1942), 67-68.

[15] Will appear in the *Journal reine und angew. Math.*

Denote by $s_0, s_1, \ldots, s_{2^{g(x)}-1}$ all the sums (16) ($s_0$ is the empty sum and is 0). Moser and I observed that by putting $\sum_{i=1}^{g(x)} a_i = A$, we obtain

$$\sum_{i=0}^{2^{g(x)}-1} \left(s_i - \frac{A}{2}\right)^2 = 2^{g(x)-2} \sum_{i=1}^{g(x)} a_i^2 < 2^{g(x)-2} x^2 g(x) .$$

Thus the number of $i$-s for which

$$\left| s_i - \frac{A}{2} \right| \leqslant x g(x)^{\frac{1}{2}}$$

is greater than $2^{g(x)-1}$. Thus since all the sums (16) are different we have

$$2^{g(x)-1} < 2 x g(x)^{\frac{1}{2}} ,$$

or

$$g(x) < \frac{\log x}{\log 2} + [1 + o(1)] \frac{\log \log x}{2 \log 2} , \qquad (18)$$

which improves (17). At present we can not decide whether

$$g(x) = \frac{\log x}{\log 2} + O(1)$$

is true or not.