References

[1] J. Galambos, *The ergodic properties of the denominators in the Oppenheim expansion of real numbers into infinite series of rationals*, Quart. J. Math. Oxford (2), 21 (1970), pp. 177–191.

[2] A. Oppenheim, *On the representation of real numbers by products of rational numbers*, Quart. J. Math. Oxford (2), 4 (1953), pp. 303–307.

[3] O. Perron, *Irrationalzahlen*, 2nd ed., New York 1948.

Received on 20. 8. 1971 (187)

ACTA ARITHMETICA
XXI (1972)

On a linear diophantine problem of Frobenius

by

P. Erdös (Budapest) and R. L. Graham (Murray Hill, N. J.)

Introduction. Given integers $0 < a_1 < \ldots < a_n$ with $\gcd(a_1, \ldots, a_n) = 1$, it is well-known that the equation $N = \sum_{k=1}^{n} x_k a_k$ has a solution in non-negative integers x_k provided N is sufficiently large. Following [9], we let $G(a_1, \ldots, a_n)$ denote the greatest integer N for which the preceding equation has no such solution.

The problem of determining $G(a_1, \ldots, a_n)$, or at least obtaining non-trivial estimates, was first raised by G. Frobenius (cf. [2]) and has been the subject of numerous papers (e.g., cf. [1], [2], [3], [4], [7], [8], [9], [11], [12], [13]). It is known that:

$$G(a_1, a_2) = (a_1-1)(a_2-1)-1 \quad ([2], [11]);$$

$$G(a_1, \ldots, a_n) \leqslant (a_1-1)(a_n-1)-1 \quad ([2], [4]);$$

$$G(a_1, \ldots, a_n) \leqslant \sum_{k=1}^{n-1} a_{k+1} d_k/d_{k+1}$$

where $d_k = \gcd(a_1, \ldots, a_k)$ ([2]). The exact value of G is also known for the case in which the a_k form an arithmetic progression ([1], [13]).

In this paper, we obtain the bound

$$G(a_1, \ldots, a_n) \leqslant 2a_{n-1}\left[\frac{a_n}{n}\right] - a_n,$$

which in many cases is superior to previous bounds and which will be seen to be within a constant factor of the best possible bound. We also consider several related extremal problems and obtain an exact solution in the case that $a_n - 2n$ is small compared to $n^{1/2}$.

A general bound. As before, we consider integers $0 < a_1 < \ldots < a_n$ with $\gcd(a_1, \ldots, a_n) = 1$.

Theorem 1.

$$G(a_1, \ldots, a_n) \leqslant 2a_{n-1}\left[\frac{a_n}{n}\right] - a_n. \tag{1}$$

Proof. Let g denote a_n, let m denote $\left[\frac{a_n}{n}\right]$ and let A denote the set $\{0, a_1, \ldots, a_{n-1}\}$ of residues modulo g. Consider the sum

$$\mathscr{C} = \underbrace{A + \ldots + A}_{m} = \{b_1 + \ldots + b_m:\ b_k \in A\} \pmod{g}.$$

By a strong theorem of Kneser ([10]; cf. also [6], p. 57), there exists a (minimal) divisor g' of g such that

$$\mathscr{C} = \underbrace{A^{(g')} + \ldots + A^{(g')}}_{m} \pmod{g}$$

where

$$A^{(g')} = \{a + rg':\ 0 \leqslant r < g/g',\ a \in A\} \pmod{g}$$

and such that

$$\frac{|\mathscr{C}|}{g} \geqslant \frac{mn}{g} - \frac{m-1}{g'}. \tag{2}$$

Assume $\mathscr{C}$ does not contain a complete system of residues modulo g. Since $\gcd(a_1, \ldots, a_{n-1}, g) = 1$ then $A^{(g')}$ must consist of more than one congruence class mod g'. By the theorem of Kneser and the minimality of g', it follows that $\mathscr{C}$ must contain at least $m+1$ distinct residue classes mod g'; thus

$$\frac{|\mathscr{C}|}{g} \geqslant \frac{m+1}{g'}. \tag{3}$$

Note that $g \geqslant n$ and $m = [g/n]$ imply

$$m+1 > \frac{1}{2}\left(\frac{m-1}{\frac{mn}{g} - \frac{1}{2}}\right). \tag{4}$$

Suppose now that $|\mathscr{C}| \leqslant \frac{1}{2}g$. By (2) and (4) we have

$$\frac{mn}{g} - \frac{m-1}{g'} \leqslant \frac{1}{2}, \qquad g' \leqslant \frac{m-1}{\frac{mn}{g} - \frac{1}{2}} < 2(m+1).$$

Hence, by (3),

$$\frac{|\mathscr{C}|}{g} \geqslant \frac{m+1}{g'} > \frac{m+1}{2(m+1)} = \frac{1}{2}$$

which is a contradiction.

We may therefore assume $|\mathscr{C}| > \frac{1}{2}g$. But in this case it is easily seen that $\mathscr{C} + \mathscr{C}$ contains a complete residue system mod g. It follows that the least possible integer not representable in the form

$$x_1 b_1 + \ldots + x_{2m} b_{2m} + xg$$

with $x_k \geqslant 0$, $x \geqslant 0$, $b_k \in A$, is given by

$$2m \cdot \max_{a \in A}(a) - g = 2a_{n-1}\left[\frac{a_n}{n}\right] - a_n.$$

This proves the theorem.

Note that in the case that $n = 2$ and a_2 is odd we have

$$G(a_1, a_2) \leqslant 2a_1\left[\frac{a_2}{2}\right] - a_2 = a_1 a_2 - a_1 - a_2$$

which is best possible.

An extremal problem. The question of the estimation of G naturally suggests the following extremal problem. For integers n and t, define $g(n, t)$ by

$$g(n, t) = \max_{a_i} G(a_1, \ldots, a_n)$$

where the max is taken over all a_i satisfying

$$0 < a_1 < \ldots < a_n \leqslant t, \qquad \gcd(a_1, \ldots, a_n) = 1. \tag{5}$$

By Theorem 1 the following result is immediate.

Corollary. $g(n, t) < 2t^2/n$.

On the other hand, it is not hard to see that for the set $\{x, 2x, \ldots \ldots, (n-1)x, x^*\}$ with $x = [t/(n-1)]$ and $x^* = (n-1)[t/(n-1)] - 1$,

$$g(n, t) \geqslant G(x, \ldots, x^*) \geqslant \frac{t^2}{n-1} - 5t \quad \text{for} \quad n \geqslant 2.$$

Thus, $g(n, t)$ is bounded below by essentially t^2/n.

Of course, for $n = 2$, the exact value of g is given by $g(2, t) = (t-1)(t-2) - 1$. It appears that

$$g(3, t) = \left[\frac{(t-2)^2}{2}\right] - 1,$$

with the sets $\{t/2, t-1, t\}$ or $\{t-2, t-1, t\}$ for t even and $\{(t-1)/2, t-1, t\}$ for t odd achieving this bound. However, this has not yet been established. It follows from the Corollary that $g(n, cn) < 2c^2 n$ and $g(n, n^2) < 2n^3$; again, the truth probably differs from these estimates by a factor of $1/2$ for large n.

Determination of $g(n, 2n+k)$. The remainder of the paper will be concerned with the determination of $g(n, 2n+k)$ for n large compared to k. It follows easily from density considerations that $g(n, 2n+k) = 2n+2k-1$ for $k \leqslant -1$ (cf. [12]). It was shown in [5] that $g(n, 2n) = 2n+1$ and $g(n, 2n+1) = 2n+3$. It was also proved in [5] that for k fixed $g(n, 2n+k) = 2n+h(k)$ for some function h of k provided n is sufficiently large. The exact value of $h(k)$ is given by the next result.

THEOREM 2. *For k fixed, if n is sufficiently large then*

$$g(n, k) = \begin{cases} 2n+2k-1 & \text{for } k \leqslant -1, \\ 2n+1 & \text{for } k = 0, \\ 2n+4k-1 & \text{for } k \geqslant 1 \text{ and } n-k \equiv 1 \pmod 3, \\ 2n+4k+1 & \text{for } k \geqslant 1 \text{ and } n-k \not\equiv 1 \pmod 3. \end{cases}$$

Proof. By previous remarks we may restrict ourselves to $k \geqslant 2$. Assume for a fixed integer $K \geqslant 2$ the theorem holds for all $k < K$. Let $A = \{a_1, \ldots, a_n\}$ be a set satisfying (5) with $k = K$ and n large (to be specified later). We first establish

$$(6) \qquad g(n, k) \leqslant \begin{cases} 2n+4K-1 & \text{if} \quad n-K \equiv 1 \pmod 3, \\ 2n+4K+1 & \text{if} \quad n-K \not\equiv 1 \pmod 3. \end{cases}$$

Let $S(A)$ denote the set of sums $\{\sum_{i=0}^{n} x_i a_i \colon x_i \geqslant 0\}$ we are considering and let $G(A)$ abbreviate $G(a_1, \ldots, a_n)$. Note that if there exists an x, $1 \leqslant x \leqslant 2n+K$, with $x \in S(A)$, $x \notin A$, then the set $A' = A \cup \{x\}$ satisfies

$$0 < a'_1 < \ldots < a'_{n+1} = 2n+K = 2(n+1)+K-2.$$

By the induction hypothesis

$$G(A) = G(A') \leqslant 2(n+1)+4(K-2)+1 = 2n+4K-5 < 2n+4K-1$$

so that (6) certainly holds in this case. Hence, we may assume A and $S(A)$ agree below $2n+K$.

Next, suppose $2n+K+1 \in S(A)$. Then for $A' = A \cup \{2n+K+1\}$ we have

$$0 < a'_1 < \ldots < a'_{n+1} = 2n+K+1 = 2(n+1)+K-1$$

so that by the induction hypothesis

$$G(A) = G(A') \leqslant 2(n+1)+4(K-1)+1 = 2n+4K-1$$

and (6) holds in this case. Hence, we may assume

$$2n+K+1 \notin S(A).$$

Now, suppose $2n+K+2 \in S(A)$, $2n+K+3 \in S(A)$. For $A' = A \cup \{2n+K+2, 2n+K+3\}$ we have

$$0 < a'_1 < \ldots < a'_{n+2} = 2n+K+3 = 2(n+2)+K-1.$$

By the induction hypothesis

$$G(A) = G(A') \leqslant \begin{cases} 2(n+2)+4(K-1)-1 & \text{if } (n+2)-(K-1) \equiv 1 \pmod 3, \\ 2(n+2)+4(K-1)+1 & \text{if } (n+2)-(K-1) \not\equiv 1 \pmod 3 \end{cases}$$

$$= \begin{cases} 2n+4K-1 & \text{if } n-k \equiv 1 \pmod 3, \\ 2n+4K+1 & \text{if } n-k \not\equiv 1 \pmod 3, \end{cases}$$

so that (6) holds in this case. Hence we may assume that either

$$2n+K+2 \notin S(A) \quad \text{or} \quad 2n+K+3 \notin S(A).$$

There are two cases:

(I) Suppose $a_1 \leqslant 3K$. If at least $3K$ consecutive integers belong to A then by successively adding a_1 to these integers, we infer that $G(A) < 2n+K$ and (6) holds in this case. Therefore, we may assume that A does not contain $3K$ consecutive integers.

Since we have assumed $2n+K+1 \notin S(A)$ then for all i, $1 \leqslant i \leqslant 2n+K$, either $i \notin A$ or $2n+K+1-i \notin A$. Thus, for exactly $\left[\frac{K+1}{2}\right]$ values of j we have $j \notin A$ and $n+K+1-j \notin A$. For a given integer $f(K)$, if n is sufficiently large then for some $t \leqslant \left[\frac{K+1}{2}\right] f(K)$, each of the integers $t+i$, $1 \leqslant i \leqslant f(K)$, satisfies either

$$t+i \in A \quad \text{or} \quad 2n+K+1-(t+i) \in A.$$

Consequently, for some t', $t+1 \leqslant t' \leqslant t+3K$, we have

$$2n+K-t'+1 \in A.$$

There are several possibilities:

(i) Suppose $2n+K-t' \in A$. If $t'+2 \in A$ then we would have $2n+K-t'+2$, $2n+K-t'+3 \in S(A)$ which contradicts our assumptions on A. We may therefore assume

$$2n+K-t'-1 \in A.$$

But now consider $t'+3$. If $t'+3 \in A$ then as before we find $2n+K-t'+2$, $2n+K-t'+3 \in S(A)$ which is a contradiction. Hence, we must have

$$2n+K-t'-2 \in A.$$

We can continue this argument to conclude that

$$2n+K-t'-s\in A \quad \text{for} \quad 0\leqslant s\leqslant 3K-1,$$

provided $f(K)\geqslant 6K$ and n is sufficiently large. But this is a sequence of $3K$ consecutive integers in A and since this contradicts our assumption on A, then case (i) is impossible.

(ii) Suppose $2n+K-t'\notin A$. Then we have

$$t'+1\in A.$$

If we now have $t'+2\in A$ then as before $2n+K-t'+2,\ 2n+K-t'+3\in S(A)$ which is a contradiction. Therefore, we may assume $t'+2\notin A$, i.e.,

$$2n+K-t'-1\in A.$$

Now, by using the same arguments as in (i) we can argue that $t'+3$, $2n+K-t'-3, \ldots, t'+2r+1,\ 2n+K-t'-2r-1\in A$ for $2r<f(K)-3K$ if n is sufficiently large. In particular we have

$$t'+2j+1\in A, \quad 0\leqslant j<\tfrac{1}{2}(f(K)-3K)$$

where $t'\leqslant\left[\frac{K+1}{2}\right]f(K)+3K$. Since $a_1\leqslant 3K$ then by successively adding $2a_1$ to the integers $t'+2j+1$, we see that all integers x of the form $x=t'+2s+1$, $s\geqslant 0$, belong to $S(A)$ provided

$$6K\leqslant f(K)-3K.$$

Of course if $t'\equiv 0 \pmod 2$, then by adding $t'+1\in A$ to the integers $t'+2s+1$, $s\geqslant 0$, we see that all integers $\geqslant 2\left[\frac{K+1}{2}\right]f(K)+6K+2$ belong to $S(A)$. For n sufficiently large, this certainly implies (6). We may therefore assume

$$t'\equiv 1 \pmod 2$$

and consequently all even integers $\geqslant t'+1$ belong to $S(A)$. In fact, is it clear that if $x\in A$ is an odd integer and $x\leqslant 2n+K-(t'+1)$ then all odd integers $\geqslant 2n+K$ (and hence all integers $\geqslant 2n+K$) belong to $S(A)$. Thus, we may assume that

$$x\in A, \quad x \text{ odd } \Rightarrow x>2n-\left[\frac{K+1}{2}\right]f(K)-2K.$$

Further, if K is odd then $2n+K+1$ is even and therefore belongs to $S(A)$ for n sufficiently large. This contradicts our assumption on A and we may assume K is even.

Now, let u be the largest integer such that $2n+K-2u+1\in A$. Since K is even it follows that

$$u<\frac{1}{2}\left(\left[\frac{K+1}{2}\right]f(K)+3K+1\right).$$

Consider the $K+1$ integers $2u+2j$, $1\leqslant j\leqslant K+1$. By the definition of u none of the integers $2n+K-(2u+2j)+1$ belongs to A. Since there are at most $\left[\frac{K+1}{2}\right]=\frac{K}{2}$ of these integers for which both $2u+2j\notin A$ and $2n+K-(2u+2j)+1\notin A$ then we see that at least $K+1-\frac{K}{2}=\frac{K}{2}+1$ of them belong to A, say,

$$2u+2j_1, \ldots, 2u+2j_t\in A, \quad t\geqslant K/2+1.$$

Forming the sums

$$(2n+K-2u+1)+(2u+2j_i), \quad i=1,2,\ldots,t,$$

we obtain at least $K/2+1$ sums $2n+K+2j_i+1$ which are $\geqslant 2n+K+3$ and $\leqslant 2n+3K+3$ and which belong to $S(A)$. But all the even integers $2n+K+2r$, $1\leqslant r\leqslant K+1$, also belong to $S(A)$. Hence, $S(A)$ contains at least $n+(K/2+1)+K+1$ integers which are less than or equal to $2n+3K+3$ and we can find a subset $A'\subseteq S(A)$ with

$$0<a_1'<\ldots<a'_{n+3K/2+2}=2n+3K+3-d,$$

for some integer $d\geqslant 0$. Since

$$(2n+3K+3-d)-(2+3K/2+2)\leqslant -1$$

then by the induction hypothesis we conclude that all integers $\geqslant 2n+3K+3-d$ belong to $S(A)$. If $d\geqslant 1$ then in fact all integers $\geqslant 2n+3K+2$ belong to $S(A)$; if $d=0$ then since $2n+3K+2$ is even then we still have all integers $\geqslant 2n+3K+2\in S(A)$. Thus,

$$G(A)\leqslant 2n+3K+1.$$

But for $K\geqslant 2$, $4K-1\geqslant 3K+1$ so that

$$G(A)\leqslant 2n+4K-1$$

and (6) holds in this case. This concludes case (I).

(II) Suppose $a_1>3K$. There are two cases:

(i) Suppose $a_1>n+\left[\frac{K+1}{2}\right]$. Thus, exactly $\left[\frac{K+1}{2}\right]$ of the integers which are $>n+\left[\frac{K+1}{2}\right]$ and $<2n+K$ are missing from A. This implies that for some i, $1 \leqslant i \leqslant \left[\frac{K+1}{2}\right]+1$, both $n+2\left[\frac{K+1}{2}\right]+1+i \in A$ and $n+2\left[\frac{K+1}{2}\right]+2-i \in A$, i.e., $2n+4\left[\frac{K+1}{2}\right]+3 \in S(A)$. Of course, the same argument can be repeated for $2n+4\left[\frac{K+1}{2}\right]+4$, etc., so that for n sufficiently large, $2n+4\left[\frac{K+1}{2}\right]+j+2 \in S(A)$ for $1 \leqslant j \leqslant 4\left[\frac{K+1}{2}\right]+3$. Hence $S(A)$ contains a subset A' with

$$0 < a'_1 < \ldots < a'_{n+4\left[\frac{K+1}{2}\right]+3} = 2n+8\left[\frac{K+1}{2}\right]+5-d$$

for some $d \geqslant 0$. Since

$$2\left(n+4\left[\frac{K+1}{2}\right]+3\right) > 2n+8\left[\frac{K+1}{2}\right]+5-d$$

then by the induction hypothesis all integers $> 2n+8\left[\frac{K+1}{2}\right]+5$ belong to $S(A)$. But since $2n+4\left[\frac{K+1}{2}\right]+j+2 \in S(A)$ for $1 \leqslant j \leqslant 4\left[\frac{K+1}{2}\right]+3$ then all integers $> 2n+4\left[\frac{K+1}{2}\right]+2$ belong to $S(A)$. However, $4\left[\frac{K+1}{2}\right]+2 < 4K-1$ for $K \geqslant 2$ so that (6) holds in this case.

(ii) Suppose $a_1 \leqslant n+\left[\frac{K+1}{2}\right]$. Consider the $3K-1$ integers $2n+K-a_1+i+1$, $1 \leqslant i \leqslant 3K-1$. Since a_1 is the least element of A then at least $3K-1-\left[\frac{K+1}{2}\right]$ of these integers must belong to A. Adding a_1 to each of them gives at least $3K-1-\left[\frac{K+1}{2}\right]$ integers in $S(A)$ which are $> 2n+K$ and $\leqslant 2n+4K$. Thus, $S(A)$ contains a subset A' with

$$0 < a'_1 < \ldots < a'_{n+3K-1-\left[\frac{K+1}{2}\right]} = 2n+4K-d$$

for some $d \geqslant 0$.

For $K \geqslant 4$,

$$2\left(n+3K-1-\left[\frac{K+1}{2}\right]\right) > 2n+4K-d$$

so that by the induction hypothesis

$$G(A) \leqslant G(A') \leqslant 2n+4K-1$$

and (6) holds. Hence, we may assume $K \leqslant 3$. There are two cases.

Suppose $K = 2$. If $2n-a_1+j \in A$, $4 \leqslant j \leqslant 6$, then $2n+j \in S(A)$, $4 \leqslant j \leqslant 6$. Thus $S(A)$ contains a subset A' with

$$0 < a'_1 < \ldots < a'_{n+3} = 2n+6$$

and by the induction hypothesis

$$G(A) \leqslant G(A') \leqslant 2n+7$$

so that (6) holds in this case.

If at least one of $2n-a_1+j$, $4 \leqslant j \leqslant 6$, is missing from A, then in fact, exactly one of $2n-a_1+j$, $4 \leqslant j \leqslant 6$, is missing from A, and all of $2n-a_1+j \in A$, $1 \leqslant j \leqslant 9$. Hence, $2n+j \in S(A)$, $7 \leqslant j \leqslant 9$, and $S(A)$ contains a subset A' with

$$0 < a'_1 < \ldots < a'_{n+5} \leqslant 2n+9.$$

By the induction hypothesis

$$G(A') \leqslant 2n+8$$

and since $2n+7$, $2n+8 \in S(A)$ then

$$G(A) \leqslant 2n+6$$

which satisfies (6) in this case.

The case $K = 3$ is similar and will be omitted. It can be checked that the condition that n be sufficiently large in the preceding arguments is satisfied, for example, by taking $n > 20K^2$.

This concludes case (II) and (6) is proved.

We next exhibit specific sets A which satisfy (6) with equality for n arbitrarily large. There are three cases.

(i) $n-K \equiv 1 \pmod 3$. Write $n = 3m+K+1$ and let

$$A = \bigcup_{i=1}^{2m+K} \{3i\} \cup \bigcup_{j=1}^{m+1} \{3m+3K+5-3j\}.$$

The least element of $S(A)$ which is $\equiv 1 \pmod 3$ is $2(3m+3K+2) = 6m+6K+4$ so that

$$2n+4K-1 = 6m+6K+1 \notin S(A).$$

Therefore $0 < a_1 < \ldots < a_n = 2n+K$ and $G(A) \geqslant 2n+4K-1$.

(ii) $n-K \equiv 2 \pmod 3$. Write $n = 3m+K+2$ and let

$$A = \bigcup_{i=1}^{2m+K+1} \{3i\} \cup \bigcup_{j=1}^{m+1} \{3m+3K+7-3j\}.$$

(iii) $n-K \equiv 0 \pmod 3$. Write $n = 3m+K$ and let

$$A = \bigcup_{i=1}^{2m+K} \{3i\} \cup \bigcup_{j=1}^{m} \{6m+3K+2-3j\}.$$

It is easy to see in (ii) and (iii) that A satisfies (5) and $G(A) \geqslant 2n+4K+1$.

The examples in (i), (ii) and (iii) together with (6) establish the theorem for $k = K$. This completes the induction step and the theorem is proved.

Acknowledgment. The authors wish to thank E. G. Straus for important suggestions in the proof of Theorem 1.

Added in proof: The conjecture $g(3, t) = \left[\frac{(t-2)^2}{2}\right] - 1$ has recently been settled in the affirmative by M. Lewin (personal communication).

References

[1] P. T. Bateman, *Remark on a recent note on linear forms*, Amer. Math. Monthly 65 (1958), pp. 517–518.
[2] Alfred Brauer, *On a problem of partitions*, Amer. J. Math. 64 (1942), pp. 299–312.
[3] — and B. M. Seelbinder, *On a problem of partitions, II*, Amer. J. Math. 76 (1954), pp. 343–346.
[4] — and J. E. Shockley, *On a problem of Frobenius*, J. Reine Angew. Math. 211 (1962), pp. 215–220.
[5] P. Erdös, *Problem P–84*, Can. Math. Bull. 14 (1971), pp. 275–277.
[6] H. Halberstam and K. F. Roth, *Sequences I*, London 1966.
[7] B. R. Heap and M. S. Lynn, *A graph theoretic algorithm for the solution of a linear diophantine equation*, Numerische Math. 6 (1964), pp. 346–354.
[8] — — *On a linear diophantine problem of Frobenius: an improved algorithm*, Numerische Math. 7 (1965), pp. 226–231.
[9] S. M. Johnson, *A linear diophantine problem*, Can. J. Math. 12 (1960), pp. 390–398.
[10] M. Kneser, *Abschätzungen der asymptotischen Dichte von Summenmengen*, Math. Zeitschr. 58 (1953), pp. 459–484.
[11] N. S. Mendelsohn, *A linear diophantine equation with applications to nonnegative matrices*, Ann. N. Y. Acad. Sci. 175 art. 1 (1970), pp. 287–294.
[12] M. Nagata and H. Matsumura, Sûgaku 13 (1961–62), p. 161; Math. Rev. 25 no. 3 #2386 (1963).

HUNGARIAN ACADEMY OF SCIENCES
Budapest, Hungary
BELL TELEPHONE LABORATORIES, INCORPORATED
Murray Hill, New Jersey

Received on 25. 8. 1971 (220)

ACTA ARITHMETICA
XXI (1972)

Remarks on some new applications of the dispersion method

by

B. M. Bredihin (Leningrad) and Yu. V. Linnik

Dispersion method as expounded in the works [1] and [2] can be applied to proving a general result on the equation

$$n = \frac{\nu_1\varphi_1 - \nu_2\varphi_2}{\nu_1 - \nu_2}$$

for large n's; ν_i, φ_i being rather general system of numbers the equation is solvable, and a *lower estimate of the asymptotic* can be obtained. The particular cases are:

The equation:

$$n = \frac{p_1 p - p_1' p'}{p_1 - p_1'} \tag{A}$$

with p, p', p_1, p_1' primes, $p \leqslant n, p_1, p_1' \leqslant (\ln n)^a$; $a > e$ has the number of solutions:

$$Q_A(n) \geqslant (\ln a)(\ln a - 1)\frac{n}{\ln n} + O\left(\frac{n}{\ln n \ln\ln n}\right).$$

The equation:

$$2 = \frac{p_1 p - p_1' p'}{p_1 - p_1'} \tag{B}$$

with p, p', p_1, p_1' as above, $n \to \infty$ has the number of solutions:

$$Q_B(n) \geqslant \ln a(\ln a - 1)\frac{n}{\ln n} + O\left(\frac{n}{\ln n \ln\ln n}\right).$$

The equation:

$$n = \frac{p_1^r p - p_1'^r p'}{p_1^r - p_1'^r} \tag{C}$$