Can. J. Math., Vol. XXVIII, No. 6, 1976, pp. 1280–1288

BOUNDS FOR A LINEAR DIOPHANTINE PROBLEM OF FROBENIUS, II

YEHOSHUA VITEK

1. Introduction. Let $A = \{a_0, a_1, \ldots, a_s\}$ be a set of relatively prime integers such that $0 < a_0 < a_1 < \ldots < a_s = n$. Let $\phi(A)$ denote the smallest integer such that, for $N \geqq \phi(A)$, the equation

$$a_0x_0 + a_1x_1 + \ldots + a_sx_s = N$$

should always have a solution in nonnegative integers.

For $s = 1$ it is well known that $\phi(a_0, a_1) = (a_0 - 1)(a_1 - 1)$ but for $s \geqq 2$ the problem of determining ϕ is difficult.

Schur [**1**] was the first to give an upper bound

(1) $\phi(A) \leqq (a_0 - 1)(a_s - 1).$

Lewin [**3**] proved that for $s \geqq 2$,

(2) $\phi(A) \leqq [\frac{1}{2}(n - 2)^2],$

where $[x]$ stands for the greatest integer $\leqq x$. This bound is sharp for $s = 2$ only, and Lewin conjectured that in general, $\phi(A) \leqq [(n - 2)(n - s)/s]$.

Support to Lewin's conjecture was given by Erdös and Graham, who proved [**2**].

(3) $\phi(A) \leqq 2[a_s/(s + 1)]a_{s-1} - a_s + 1 < 2n^2/(s + 1).$

In this paper we shall prove

THEOREM 1. *Let $a_0 < a_1 < \ldots < a_s = n$ be relatively prime positive integers such that $n \geqq s(s - 3)$. Then:*

(4) $\phi(a_0, \ldots, a_s) < n^2/s.$

The restriction, $n \geqq s(s - 3)$ is probably not essential. Yet, in Lewin's conjecture, n must be large enough with respect to s, since for example $\phi(2, 4, 5, 6, 7) = 4 > [(7 - 4)(7 - 2)/4]$.

Bound (4) is not the best possible one, but it cannot be improved beyond Lewin's conjecture since

$$\phi(n, n - 1, (s - 1)n/s, (s - 2)n/s, \ldots, n/s) = (n - 2)(n - s)/s.$$

There is one advantage of (1) over (2), (3), and (4). It considers the influence of a_0 which may be rather small and reduce $\phi(A)$ significantly.

Received January 9, 1976 and in revised form, June 18, 1976.

A step in this direction was done in [**6**]. It was proved there that if A contains at least two non-zero residues modulu a_0 then:

(5) $\phi(A) \leqq [a_0/2](a_s - 2)$.

The second purpose of this paper is to go further in this direction and to prove (using the notation $a|b$ for a divides b):

THEOREM 2. *Let $a_0 < a_1 < \ldots < a_s$ be relatively prime positive integers, having different residues* mod a_0. *If, for every divisor r of a_0 such that $r < s$ and $r \nmid s$, the number of residues* mod a_0/r *in $\{a_0, \ldots, a_s\}$ is not* $1 + [s/r]$, *then*

(6) $\phi(a_0, \ldots, a_s) \leqq [a_0 - 2 + s)/s](a_s - s)$.

This bound is achieved by the arithmetic sequence $a_0, a_0 + d, \ldots, a_0 + sd = a_s$, in case that $a_0 \equiv 1 \pmod{s}$ or $d = 1$, (see [**5**]).

Observe that the condition: "For every divisor r of a_0", etc., is always valid for $s = 2$, thus providing a shorter proof for Theorem 1 in [**6**]. Further, this condition is satisfied in "most" cases. Bound (6) is always valid if $a_0 \geqq \frac{2}{3}a_s$.

Finally we shall prove for $s = 3$

THEOREM 3. *Let $a_0 < a_1 < a_2 < a_3 = n$ be relatively prime positive integers. Then*

$$\phi(a_0, a_1, a_2, a_3) \leqq [(n - 2)(n - 3)/3].$$

2. Some lemmas. Let G be an abelian finite group, and let A, B be subsets of G. Let $|A|$ denote the cardinality of A, and $A + B$ denote the set $\{a + b | a \in A, b \in B\}$. Thus, $\sum^k A$ stands for $A + \ldots + A$, k times.

Then by a theorem of Mann, proved in [**4**], we have: If for every proper subgroup H of G, $|A + H| \geqq |A| + |H| - 1$, then for every subset B of G, for which $A + B \neq G$, we have $|A + B| \geqq |A| + |B| - 1$.

Henceforth, such a subset A, which satisfies $|A + H| \geqq |A| + |H| - 1$ for every proper subgroup H, will be said to satisfy *Mann's Condition*, or briefly *M.C.* Using induction we immediately obtain:

LEMMA 1. *Let G be an abelian finite group. Let A, A' be subsets such that $|A| = s + 1$, and A satisfies M.C. in G. Then*

$$|A' + \textstyle\sum^{l-1} A| \geqq \min\{|G|, |A| + (l - 1)s\}.$$

In particular, setting $A' = A$ we have $\sum^l A = G$, for $l = 1 + [(|G| - 2)/s]$.

Let q be a positive integer. Let J_q denote the group of residues modulo q, the members of which are the integers $\{0, 1, \ldots, q - 1\}$. Let E be a set of nonnegative integers. Then E_q denotes the set of residues mod q of the elements of E. Thus E_q is a subset of J_q and its elements are also integers. Hence $(E_q)_p$ has a meaning, where p is some positive integer. If $p|q$ then clearly $(E_q)_p = E_p$.

Let p be a positive integer. We denote the set of all nonnegative integral multiples of p by $\langle p \rangle$. With this notation, any subgroup of J_q is given by $\langle q/r \rangle_q = \{0, q/r, 2q/r, \ldots, (r-1)q/r\}$, where r is a divisor of q. (Saying divisor we always mean a proper one, neither 1 nor q.)

In terms of these notations, we now redefine $M.C.$ as follows: A subset E of J_q satisfies $M.C.$ if and only if $|E + \langle q/r \rangle_q| \geqq |E| + r - 1$, for every divisor r of q. Note that the $+$ operation in $E + \langle q/r \rangle_q$ is modulo q.

In the following Lemmas 2–6 we shall be concerned with a subset E of J_q such that $|E| = s + 1$, $0 \in E$ and $\gcd(q, E) = 1$. The notation $\gcd(q, E)$ stands for the greatest common divisor of the nonzero elements of $\{q\} \cup E$:

LEMMA 2. *Let r be a divisor of q. Then:*

(i) $|E + \langle q/r \rangle_q| = r|E_q/r|$

(ii) $|E + \langle q/r \rangle_q| < s + r$ *if and only if* $|E_{q/r}| \leqq 1 + (s-1)/r$.

Hence, E satisfies M.C. in J_q if and only if $|E_{q/r}| > 1 + (s-1)/r$, for every divisor r of q.

(iii) *If $|E_{q/r}| \leqq 1 + (s-1)/r$ then $r < s$, $r \nmid s$ and $|E_{q/r}| = 1 + [s/r]$.*

(iv) *E satisfies M.C. in J_q if and only if $|E_{q/r}| \neq 1 + [s/r]$ for every divisor r of q such that $r < s$, $r \nmid s$.*

Proof. (i) $E + \langle q/r \rangle_q$ is a union of cosets of the quotient group $J_q/\langle q/r \rangle_q$. This group is isomorphic to $J_{q/r}$ and each coset corresponds to a residue modulo q/r. Hence $|E + \langle q/r \rangle_q| = r|E_{q/r}|$.

(ii) Follows directly by (i).

(iii) If $r < s$ were not true, then we would have $|E_{q/r}| \leqq 1 + (s-1)/r < 2$. But then zero would be the only residue mod q/r in A, contradicting the assumption $\gcd(q, E) = 1$.

The two remaining arguments are due to the inequality: $|E + \langle q/r \rangle_q| \geqq |E| > s$. Together with (i) this implies $s/r < |E_{q/r}| \leqq 1 + (s-1)/r < 1 + s/r$. $|E_{q/r}|$ is an integer, hence $r \nmid s$ and $|E_{q/r}| = 1 + [s/r]$.

(iv) This is an immediate consequence of (ii) and (iii).

We shall study now (Lemmas 3–6) the subset E in case that it fails to satisfy $M.C.$ These lemmas are not necessary for the proof of Theorem 2.

LEMMA 3. *Let r be a divisor of q satisfying $|E + \langle q/r \rangle_q| < s + r$. By Lemma 2 we then have $|E_{q/r}| = 1 + [s/r]$. Define λ and μ by $\lambda = s - r[s/r]$ and $\mu + 1 = |E \cap \langle q/r \rangle|$. Then:*

(i) $1 \leqq \lambda \leqq \mu \leqq r - 1$.

(ii) *For each nonzero member of $E_{q/r}$, there are in E at least $r - \mu + \lambda$ elements, congruent to it* mod q/r.

Proof. Clearly, $\mu \leqq r - 1$ and by Lemma 2, $\lambda \geqq 1$. To prove the rest, denote $E_{q/r} = \{0, b_1, \ldots, b_{[s/r]}\}$. Let η_j be the number of elements of E that are congruent to b_j mod q/r. Then we have: $|E| = \mu + 1 + \sum_1^{[s/r]} \eta_j$. Setting $|E| = s + 1 = r[s/r] + \lambda + 1$ we obtain $\lambda + \sum_1^{[s/r]} (r - \eta_j) = \mu$. Since $\eta_j \leqq r$, this proves $\lambda \leqq \mu$ and $\eta_j \geqq r - \mu + \lambda$ and the proof is completed.

The result $\mu \geqq 1$, proved in Lemma 3, means that if $|E + \langle q/r\rangle_q| < s + r$ then E contains nonzero elements of $\langle q/r\rangle$. But we need more than that. Actually we need that the members of $E \cap \langle q/r\rangle$ should generate the whole subgroup $\langle q/r\rangle_q$. This happens if and only if $\gcd(q, E \cap \langle q/r\rangle) = q/r$.

LEMMA 4. *If E does not satisfy M.C. in J_q, then there is a divisor r of q such that*

(i) $|E_{q/r}| \leqq 1 + (s-1)/r$ *and* (ii) $\gcd(q, E \cap \langle q/r\rangle) = q/r$.

Proof. There is, by Lemma 2 (ii), some divisor ρ of q such that $|E_{q/\rho}| \leqq 1 + (s-1)/\rho$. Clearly, $\gcd(q, E \cap \langle q/\rho\rangle) = hq/\rho$ where h is some divisor of ρ. We denote $r = \rho/h$ and intend to prove that r satisfies arguments (i) and (ii).

We first claim that $|E_{q/r}| = |E_{hq/\rho}| \leqq 1 + h(|E_{q/\rho}| - 1)$. Indeed, there are at most h different elements in $E_{hq/\rho}$, having the same *nonzero* residue mod q/ρ, whereas those elements of E which divide q/ρ, divide hq/ρ too, and therefore contribute only one member to $E_{hq/\rho}$.

Now we obtain:

$$\begin{aligned}|E_{q/r}| &\leqq 1 + h(|E_{q/\rho}| - 1) \leqq 1 + (\rho/r)(1 + (s-1)/\rho - 1)\\ &= 1 + (s-1)/r,\end{aligned}$$

which proves (i). Since (ii) is obvious, the lemma is completed.

LEMMA 5. *Let $r\rho$ be a divisor of q satisfying:*

(i) $\gcd(q, E \cap \langle q/r\rangle) = q/r$ *and* (ii) $\gcd(q/r, E_{q/r} \cap \langle q/r\rho\rangle) = q/r\rho$,

Then

$$\gcd(q, E \cap \langle q/r\rho\rangle) = q/r\rho.$$

Proof. Let t be a divisor of $\gcd(q, E \cap \langle q/r\rho\rangle)$. Then $t|\gcd(q, E \cap \langle q/r\rangle)$, hence by (i) $t|(q/r)$. It follows that t divides any integer if and only if it divides its residue mod q/r. In particular, the assumption $t|(E \cap \langle q/r\rho\rangle)$ implies that $t|(E_{q/r} \cap q/r\rho)$ so that by (ii) we have $t|(q/r\rho)$. On the other hand

$$(q/r\rho)|\gcd(q, E \cap \langle q/r\rho\rangle), \quad \text{hence} \quad \gcd(q, E \cap \langle q/r\rho\rangle) = q/r\rho.$$

LEMMA 6. *Let r be a maximal divisor of q satisfying:*
(i) $|E_{q/r}| \leqq 1 + (s-1)/r$ *and* (ii) $\gcd(q, E \cap \langle q/r\rangle) = q/r$.
Then $E_{q/r}$, being a subset of $J_{q/r}$ satisfies M.C.

Proof. Suppose that the lemma is not true. Then, by applying Lemma 4 to $E_{q/r}$ we obtain for some divisor ρ of q/r:

(a) $|(E_{q/r})_{q/r\rho}| \leqq 1 + (|E_{q/r}| - 2)/\rho$,

and

(b) $\gcd(q/r, E_{q/r} \cap \langle q/r\rho\rangle) = q/r\rho$.

https://doi.org/10.4153/CJM-1976-127-0 Published online by Cambridge University Press

Note that the role of q in Lemma 4 is taken here by q/r, and that of r is taken by ρ. Thus, $|E_{q/r}| - 1$ comes here instead of s there.

We shall prove that r satisfies assumptions (i) and (ii) of the lemma, in contradiction to the maximality of r.

By (a) and (i) we have $|E_{q/r\rho}| \leqq 1 + (1 + (s-1)/r - 2)/\rho < 1 + (s-1)/r\rho$. On the other hand, assumption (ii) of this lemma, together with (b) imply, by Lemma 5, that $\gcd(q, E \cap \langle q/r\rho\rangle) = q/r\rho$.

LEMMA 7. *Let* $D = \{0, d_1, d_2, \ldots, d_\mu\}$ *be a subset of* J_r, *such that* $\gcd(r, D) = 1$. *Then* $\sum^{r-\mu} D = J_r$.

Proof. We argue that if $\sum^\alpha D \neq J_r$ then $\sum^\alpha D \neq \sum^{\alpha+1} D$. Indeed, $\sum^{\alpha+1} D = \sum^\alpha D \neq J_r$ implies that D is not a generating subset of J_r, in contradiction to the assumption $\gcd(r, D) = 1$. The lemma follows immediately.

LEMMA 8. *Let* $F = \{f_0, f_1, \ldots, f_t\}$ *be a set of positive integers such that* $\gcd(F) = 1$ *and* $q \in F$. *Let* X *be a set of nonnegative integers, all of them expressible as* $\sum_{i=0}^t \alpha_i f_i$, $\alpha_i > 0$, *such that* $X_q = J_q$. *Then*

$$\phi(F) \leqq \max X - q + 1.$$

Proof. Let y be an integer, $y \geqq \max X - q + 1$. By assumption, there is an integer $x \in X$ satisfying $x \equiv y \pmod q$. Since $y + q > \max X$, we have $x \leqq y$. Hence, $y = \beta q + x$, $\beta \geqq 0$ and since $x = \sum_0^s \alpha_i f_i$, the lemma follows.

3. Proof of the main theorems.

Theorem 1. Denote $\{a_0, \ldots, a_s\} = A$, and consider the subset A_n of J_n. The proof breaks down into two cases.

Case I. A_n satisfies *M.C.* in J_n. Applying Lemma 1, we deduce that $\sum^l A_n = J_n$, while $l = 1 + [(n-2)/s]$. Consequently the set

$$X = \{\textstyle\sum_{s=0}^{s-1} \alpha_i a_i | \sum_0^{s-1} \alpha_i \leqq 1 + [(n-2)/s], \alpha_i \geqq 0\}$$

satisfies $X_n = J_n$, and by Lemma 8 we obtain

$$\begin{aligned}\phi(a_0, \ldots, a_s) &\leqq \max X - n + 1 \\ &\leqq (1 + (n-2)/s)(n-1) - n + 1 < n^2/s.\end{aligned}$$

Case II. A_n does not satisfy *M.C.* Then, by Lemma 4 (setting $A_n = E$, $n = q$), there is a (maximal) divisor r of n such that

$$|A_{n/r}| \leqq 1 + (s-1)/r \quad \text{and} \quad \gcd(n, A_n \cap \langle n/r\rangle) = n/r.$$

We rearrange the members of A according to their residues mod n/r: $A = \{d_1 n/r,\ d_2 n/r \ldots d_\mu n/r, n\ |b_{11}, \ldots, b_{1\eta_1}|b_{21}, \ldots, b_{2\eta_2}|---|b_{\theta 1}, \ldots, b_{\theta\eta_\theta}\}$, so that $b_{j1} < b_{j2} < \ldots < b_{j\eta_j}$ for $1 \leqq j \leqq \theta$, and by Lemma 2, $\theta = [s/r] = (s-\lambda)/r$. The meaning of μ and λ here, is the same as in Lemma 4: $\lambda = s - r[s/r]$, $\mu + 1 = |A_n \cap \langle n/r\rangle|$.

Let B denote the subset $\{d_1n/r, \ldots, d_\mu n/r, n, b_{11}, b_{21}, \ldots, b_{\theta 1}\}$ of A. Our purpose is to establish $\phi(B) \leqq [n^2/s]$, for $n \geqq s(s-3)$.

Consider the two sets:

$$X = \left\{ \sum_1^\theta \beta_j b_{j1} \middle| \sum_1^\theta \beta_j \leqq 1 + [(n/r - 2)/\theta], \beta_j \geqq 0 \right\}$$

and

$$Y = \left\{ \sum_1^\mu \delta_i d_i n/r \middle| \sum_1^\mu \delta_i \leqq r - \mu, \delta_i \geqq 0 \right\}.$$

We argue that $X_{n/r} = J_{n/r}$ and $Y_n = \langle n/r \rangle_n$.

Indeed, by Lemma 6, $A_{n/r}$ satisfies $M.C.$ in $J_{n/r}$ and by Lemma 1 this implies that $\sum^l A_{n/r} = J_{n/r}$ while $l = 1 + [(n/r-2)/\theta]$. Since obviously $X_{n/r} = \sum^l A_{n/r}$, we have proved $X_{n/r} = J_{n/r}$.

To prove $Y_n = \langle n/r \rangle_n$, it is enough to prove that $\sum^{r-\mu} D = J_r$, where $D = \{0, d_1, \ldots, d_\mu\}$. But this is certainly true by Lemma 7, because $\gcd(r, D) = 1/(n/r) \gcd(n, A_n \cap \langle n/r \rangle) = 1$.

Next, since X represents all residues mod n/r and Y represents all multiples of n/r mod n, we gather that $X + Y$ represents all residues mod n. Applying Lemma 8, we find $\phi(B) \leqq \max X + \max Y - n + 1 = [1 + (n/r - 2)/\theta]$ $(\max_{1 \leqq j \leqq \theta} b_{j1}) + (r - \mu)(\max_{1 \leqq i \leqq \mu} d_i)n/r - n + 1$. Since $b_{jk} \leqq b_{j(k+1)} - n/r$ we have, by Lemma 3(ii), $b_{j1} \leqq (n-1) - (r - \mu + \lambda - 1)n/r = (\mu - \lambda + 1)n/r - 1$. On the other hand, $\max d_i \leqq r - 1$ and $\theta = (s - \lambda)/r$ so that

$$\begin{aligned}\phi(B) &\leqq (1 + (n-2r)/(s-\lambda))((\mu - \lambda + 1)n/r - 1) \\ &\quad + (r-\mu)(r-1)n/r - n + 1 \\ &< (1 + (n-2r)/(s-\lambda))(\mu - \lambda + 1)n/r \\ &\qquad + (r-\mu)(r-1)n/r - n = f(\lambda).\end{aligned}$$

Now, remember that by Lemma 4 and Lemma 2(iii), $1 \leqq \lambda \leqq \mu < r < s$, hence $f'(\lambda) = -(n/r)(1 + (n-2r)(s-\mu-1)/(s-\lambda)^2) < 0$. Thus, $f(\lambda)$ decreases and

$$\phi(B) < f(\lambda) \leqq f(1) = ((n-2r)\mu/(s-1) + (r-\mu)(r-2))n/r = g(\mu).$$

$g(\mu)$ is linear and $1 \leqq \mu \leqq r - 1$. It decreases if and only if

$$(n-2r)/(s-1) \leqq r - 2.$$

In this case, we have for $n \geqq s(s-3)$:

$$\begin{aligned}\phi(B) < g(1) &= ((n-2r)/(s-1) + (r-1)(r-2))n/r \\ &\leqq ((r-2) + (r-1)(r-2))n/r \\ &= (r-2)n \leqq (s-3)n \leqq n^2/s.\end{aligned}$$

Otherwise, $g(\mu)$ increases and $\phi < g(r-1) = ((n-2r)(r-1)/(s-1) + (r-2))n/r$.

There are two cases now to be considered. If $s/2 \leqq r \leqq s-1$ then

$$\phi(B) < \frac{(n-2r)n}{s-1} \cdot \frac{(r-1)}{r} + n < \frac{(n-2)n}{s-1} \cdot \frac{(s-1)}{s} + n = n^2/s.$$

Otherwise $r \leqq (s-1)/2$ and then:

$$\phi(B) < \frac{n^2}{s-1} \cdot \frac{r-1}{r} + \frac{r-2}{r} n \leqq \frac{n^2}{s-1} \cdot \frac{(s-1)/2-1}{(s-1)/2}$$
$$+ \frac{(s-1)/2-2}{(s-1)/2} n < \frac{n^2}{s-1} \cdot \frac{s-2}{s} + \frac{s-5}{s-1} n < \frac{n^2}{s},$$

where the last inequality holds for $n > s(s-5)$.

Since $\phi(A) \leqq \phi(B)$, the proof is completed.

Theorem 2. Let A denote the set $\{a_0, \ldots, a_s\}$ and $A' = \{a_0, \ldots, a_{s-u}\}$. By Lemma 2(iv), A_{a_0} satisfies $M.C.$ in J_{a_0}. Hence, by Lemma 1:

$$\left| A_{a_0}' + \sum^{l-1} A_{a_0} \right| \geqq \min\,(a_0, |A_{a_0}'| + (l-1)s) = \min\,(a_0, ls - u + 1).$$

We choose l, u such that $0 \leqq u < s$ and $a_0 = ls - u + 1$. Then

$$l = (a_0 - 1 + u)/s = [(a_0 - 2 + s)/s].$$

Now the set $X = A' + \sum^{l-1} A$ satisfies $X_{a_0} = J_{a_0}$, and $\max X = a_{s-u} + (l-1)a_s \leqq a_s - u + (l-1)a_s = la_s - u$. Hence, by Lemma 8,

$$\phi(a_0, \ldots, a_s) \leqq la_s - u - a_0 + 1 = a_s(a_0 - 1 + u)/s - (a_0 - 1 + u)$$
$$= ((a_0 - 1 + u)/s)(a_s - s) = [(a_0 - 2 + s)/s](a_s - s).$$

The proof is now completed.

The assumptions of Theorem 2 are easily checked. Yet there are certain cases in which these assumptions are automatically fulfilled. The case $s = 2$ has already been mentioned. Another interesting case is the following

COROLLARY. *Let $a_0 < a_1 < \ldots < a_s$ be relatively prime positive integers such that $a_0 \geqq \frac{2}{3}a_s$. Then:*

$$\phi(a_0, \ldots, a_s) \leqq [(a_0 - 2 + s)/s](s_s - s).$$

Proof. Let A denote the set $\{a_0, \ldots, a_s\}$. Clearly $|A_{a_0}| = |A| = s + 1$, thus satisfying the first assumption of Theorem 2. Using Lemma 3, we shall prove that A_{a_0} satisfies $M.C.$ in J_{a_0}.

Suppose that this is not true. Then we have r, μ, λ exactly as in Lemma 3. Then:

$$A = \{a_0, a_0 + d_1 a_0/r, \ldots, a_0 + d_\mu a_0/r, b_1, b_2, \ldots, b_{s-\mu}\},$$

where $b_1 < b_2 < \ldots < b_{s-\mu}$ are the non-multiples of a_0/r in A.

Applying Lemma 3 we have:

$$b_1 \leqq (a_s - r - \mu + \lambda - 1)a_0/r \leqq a_s - (r - \mu)a_0/r.$$

Since $a_0 \leqq b_1$ this implies $a_0 < a_s - (r - \mu)a_0/r$. On the other hand, clearly: $a_0 \leqq a_s - \mu a_0/r$. Summing these inequalities yields: $2a_0 < 2a_s - a_0$, hence $a_0 < \frac{2}{3}a_s$ which contradicts the assumptions.

Consequently, A_{a_0} satisfies $M.C.$, and by Theorem 2, the proof is completed.

Proof of Theorem 3. As before, $A = \{a_0, a_1, a_2, a_3\}$. The proof breaks down into 7 cases:

Case 1. $a_0 > n/2$ and A_{a_0} satisfies $M.C.$ in J_{a_0}. Then, by Theorem 2

$$\begin{aligned}\phi(A) &\leqq [(a_0 + 1)/3](a_3 - 3)\\ &\leqq [(n - 2)/3](n - 3) \leqq (n - 2)(n - 3)/3.\end{aligned}$$

Case 2. $a_0 > n/2$ and A_{a_0} does not satisfy $M.C.$ Then Lemma 2(iii) implies $r = 2$ and Lemma 3(i) implies $\lambda = \mu = 1$, where r, μ, λ are exactly as in Lemmas 2 and 3. Applying Lemma 3(ii), we find $A = \{a_0, 3a_0/2, b, b + a_0/2\}$. We argue that $\phi(A) \leqq \phi(a_0, 3a_0/2, b) \leqq a_0 + \phi(a_0/2, b)$.

Indeed, let x satisfy $x \geqq a_0 + \phi(a_0/2, b)$. Then $x = a_0 + \alpha(a_0/2) + \beta b = \alpha_1 a_0 + \alpha_2(3a_0/2) + \beta b$, where α_2 is 1 or 0, according to whether α is odd or even.

Now, observe that $\frac{1}{2}a_0 + b = n$, so that we have,

$$\begin{aligned}\phi(A) \leqq a_0 + (\tfrac{1}{2}a_0 - 1)(b - 1) &= (\tfrac{1}{2}a_0 - 1)(b + 1) + 2 < \tfrac{1}{2}a_0 b - 2\\ &= \tfrac{1}{2}a_0(n - \tfrac{1}{2}a_0) - 2 = f(a_0).\end{aligned}$$

$f(a_0)$ increases for $a_0 \leqq n$, but we have $a_0 \leqq \frac{2}{3}(n - 1)$, because $3a_0/2 \in A$. Hence,

$$\phi(A) < f(\tfrac{2}{3}(n - 1)) = 2/9(n - 1)^2 - 2 < (n - 2)(n - 3)/3,$$

for $n \geqq 6$.

Case 3. $a_0 = \frac{1}{2}n$. Then $|A_{a_0}| = 3$ and applying bound (5) (see introduction), we get for $n \geqq 5$:

$$\begin{aligned}\phi(A) &= \phi(a_0, a_1, a_2) \leqq [a_0/2](a_2 - 2)\\ &\leqq [n/4](n - 3) \leqq (n - 2)(n - 3)/3.\end{aligned}$$

Case 4. $\frac{1}{3}(n + 1) \leqq a_0 \leqq \frac{1}{2}(n - 1)$, and $|A_{a_0}| \geqq 3$. Then applying again bound (5) we have:

$$\phi(A) \leqq \tfrac{1}{4}(n - 1)(n - 2) \leqq (n - 2)(n - 3)/3, \quad \text{for } n \geqq 6.$$

Case 5. $\frac{1}{3}(n + 1) \leqq a_0 \leqq \frac{1}{2}(n - 1)$ and $|A_{a_0}| = 2$. Let a_0, b be the two generating members of A. Then the other two must belong to the set $\{2a_0, a_0 + b, 2b\}$. Hence, $b \leqq n - a_0$, therefore for $n \geqq 6$,

$$\begin{aligned}\phi(A) &= \phi(a_0, b) = (a_0 - 1)(b - 1)\\ &\leqq (a_0 - 1)(n - a_0 - 1) \leqq \tfrac{1}{4}(n - 2)^2 \leqq (n - 2)(n - 3)/3.\end{aligned}$$

Case 6. $a_0 = \frac{1}{3}n$. Then by Schur's bound (1), $\phi(A) = \phi(\frac{1}{3}n, a_1, a_2) \leqq (\frac{1}{3}(n-1))(n-2) = (n-2)(n-3)/3$.

Case 7. $a_0 \leqq \frac{1}{3}(n-1)$. Again by (1), $\phi(A) \leqq (\frac{1}{3}(n-1)-1)(n-1) < (n-2)(n-3)/3$.

To complete the proof it should be noted that the only set for $n = 5$ is $\{2, 3, 4, 5\}$ and $\phi(2, 3, 4, 5) = 2 = 2 \cdot 3/3$.

I should like to thank Professor M. Lewin for his help.

References

1. A. Brauer, *On a problem of partitions*, Amer. J. Math. *64* (1942), 299–312.

2. P. Erdös and R. L. Graham, *On a linear diophantine problem of Frobenius*, Acta Arith. *21* (1972), 399–408.

3. M. Lewin, *A bound for a solution of a linear diophantine problem*, J. London Math. Soc. *6* (1972), 61–69.

4. H. Mann, *An addition theorem for sets of elements of abelian groups*, Proc. Amer. Math. Soc. *4* (1953), 423.

5. J. B. Roberts, *Note on linear forms*, Proc. Amer. Math. Soc. *7* (1956), 465–469.

6. Y. Vitek, *Bounds for a linear diophantine problem of Frobenius*, J. London Math. Soc. (2) *10* (1975), 79–85.

Israel Institute of Technology,
Haifa, Israel