JOURNAL OF NUMBER THEORY 27, 196–205 (1987)

Subset Sums

N. ALON*

Bell Communications Research, 435 South Street Morristown, New Jersey 07960, and Department of Mathematics, Tel Aviv University, Tel Aviv, Israel

Communicated by R. L. Graham

Received September 8, 1986

Suppose $\varepsilon > 0$ and $k > 1$. We show that if $n > n_0(k, \varepsilon)$ and $A \subseteq Z_n$ satisfies $|A| > ((1/k) + \varepsilon)n$ then there is a subset $B \subseteq A$ such that $0 < |B| \leqslant k$ and $\sum_{b \in B} b = 0$ (in Z_n). The case $k = 3$ solves a problem of Stalley and another problem of Erdös and Graham. For an integer $m > 0$, let snd(m) denote the smallest integer that does not divide m. We prove that for every $\varepsilon > 0$ there is a constant $c = c(\varepsilon) > 1$, such that for every $n > 0$ and every m, $n^{1+\varepsilon} \leqslant m \leqslant n^2/\log^2 n$ every set $A \subseteq \{1, 2, \ldots, n\}$ of cardinality $|A| > c \cdot n/\text{snd}(m)$ contains a subset $B \subseteq A$ so that $\sum_{b \in B} b = m$. This is best possible, up to the constant c. In particular it implies that for every n there is an m such that every set $A \subseteq \{1, \ldots, n\}$ of cardinality $|A| > cn/\log n$ contains a subset $B \subseteq A$ so that $\sum_{b \in B} b = m$, thus settling a problem of Erdös and Graham.

1. INTRODUCTION

Let n be a positive integer and put $N = \{1, 2, \ldots, n\}$. For $m \geqslant 1$ let $f(n, m)$ denote the maximum cardinality of a set $A \subseteq N$ that contains no subset $B \subseteq A$ so that $\sum_{b \in B} b = m$. Here we first show that

$$f(n, 2n) = (\tfrac{1}{3} + o(1)) \cdot n \tag{1.1}$$

(as $n \to \infty$). This settles a problem of Erdös and Graham [E]. To establish (1.1) we prove the following result about subset sums in the abelian group Z_n.

THEOREM 1.1. *For every fixed $\varepsilon > 0$ and $k > 1$, if $n > n_0(k, \varepsilon)$ and $A \subseteq Z_n$ satisfies $|A| > ((1/k) + \varepsilon) \cdot n$ then there is a subset $B \subseteq A$ such that $0 < |B| \leqslant k$ and $\sum_{b \in B} b = 0$.*

The case $k = 3$ of this theorem solves a problem of Stalley [S]. Clearly

* Research supported in part by Allon Fellowship and by B. de Rothschild grant.

0022-314X/87 $3.00

$f(n, m) = n$ for $m > 1 + 2 + \cdots + n = \binom{n+1}{2}$. Erdös and Graham [E] observed that

$$f(n, m) \geqslant (\tfrac{1}{2} + o(1)) \cdot n/\log n \tag{1.2}$$

for all n, m. Indeed, by the preceding remark we can assume that $m \leqslant \binom{n+1}{2}$. By the prime number theorem there is a number q, $1 \leqslant q \leqslant (2 + o(1)) \cdot \log n$ which does not divide m. Put $A = \{i \in N: q \mid i\}$. Clearly $|A| \geqslant (\frac{1}{2} + o(1))n/\log n$ and there is no $B \subseteq A$ so that $\sum_{b \in B} b = m$. This establishes (1.2). In this paper we show that (1.2) is best possible, up to the constant $\frac{1}{2}$. In fact, we prove a more general result, that determines the asymptotic behavior of $f(n, m)$ for every pair (n, m) where, say, $n^{1.01} \leqslant m \leqslant n^2/\log n$. For $m \geqslant 1$ let $\mathrm{snd}(m)$ denote the smallest non divisor of m, i.e., $\mathrm{snd}(m) = \min\{l : l \geqslant 1, l \nmid m\}$. Clearly $f(n, m) \geqslant \lfloor n/\mathrm{snd}(m) \rfloor$ for all n, m. Indeed, the set A of all multiples of $\mathrm{snd}(m)$ in N has cardinality $\lfloor n/\mathrm{snd}(m) \rfloor$ and contains no subset B the sum of whose elements is m. The following theorem shows that this obvious lower bound is, in fact, close to the real order of magnitude of $f(n, m)$.

THEOREM 1.2. *For every fixed $\varepsilon > 0$ there exists a constant $c = c(\varepsilon) \geqslant 1$ such that for every n and every m that satisfies*

$$n^{1+\varepsilon} \leqslant m \leqslant n^2/\log^2 n \tag{1.3}$$

the inequality

$$\lfloor n/\mathrm{snd}(m) \rfloor \leqslant f(n, m) \leqslant c \cdot n/\mathrm{snd}(m) \tag{1.4}$$

holds.

Note that the upper bound in (1.4) does not hold for very large m (since for every $m \geqslant n^2$ $f(n, m) = n$), and does not hold for very small m (since for every $m \leqslant n/2$, $f(n, m) \geqslant n/2$). Thus some restriction of the form (1.3) on the size of m is necessary.

As a special case of Theorem 1.2 observe that if $m = l \cdot n$, where l is the least common multiple of $2, 3, \ldots, \frac{1}{2}\log n$, then, by the prime number theorem, $l = e^{(1/2)\log n(1+o(1))}$ and thus, for sufficiently large n, m satisfies (1.3) for any $\varepsilon < \frac{1}{2}$. Hence, by Theorem 1.2

$$f(n, m) = O(n/\log n).$$

Our paper is organized as follows. In Section 2 we prove Theorem 1.1. Our proof uses some extremal graph theory, the classical theorem of Roth [R] about the maximum cardinality of a subset of N that contains no three term arithmetic progression, and a theorem of Scherk [Sch] on

abelian groups. In Section 3 we prove Theorem 1.2 by combining the Cauchey–Davenport theorem and some of the methods of Erdös and Heilbronn [EH] and of Olson [O], with the well known results of Vinogradov [V] concerning Goldbach conjecture. The final Section 4 contains several related results and open problems.

2. Subset Sums in Z_n.

Let $r_3(n)$ denote the maximum cardinality of a subset $A \subseteq N = \{1, 2, \ldots, n\}$ that contains no arithmetic progression of three terms. More than 30 years ago, K. F. Roth [R] (see also [GRS]) proved the following.

Lemma 2.1. $r_3(n) \leqslant O(n/\log\log n)$.

There are some improvements of this estimate (see [H]), but for our purpose here this result suffices.

Next we need the following result of Scherk [Sch].

Lemma 2.2. *Let B and C be two subsets of an abelian group. Suppose $0 \in B \cap C$ and suppose that if $0 = b + c$, where $b \in B$ and $c \in C$ then $b = c = 0$. Then $|B + C| \geqslant |B| + |C| - 1$.*

Corollary 2.3. *Let A be a subset of an abelian group G of order n, and suppose $|A| \geqslant n/k$. Then there is an integer r, $1 \leqslant r \leqslant k$ and a sequence $a_1, a_2, \ldots, a_r$ of r not necessarily distinct elements of A such that $\sum_{i=1}^{r} a_i = 0$.*

Proof. Suppose this is false. For each $i \leqslant k$ let $A(i)$ denote the set of all elements $g \in G$ such that $g = a_1 + a_2 + \cdots + a_r$ for some $1 \leqslant r \leqslant i$ and some not necessarily distinct elements $a_1, a_2, \ldots, a_r$ of A. We claim that $|A(i)| \geqslant i \cdot |A|$ for all $i \leqslant k$. Indeed, this is obvious for $i = 1$. Assume it holds for some $i < k$. Put $B = A(i) \cup \{0\}$ and $C = A \cup \{0\}$. Notice that by our assumption $0 \notin A(i)$ and hence $|B| = |A(i)| + 1$, $|C| = |A| + 1$. Also, if $0 = b + c$ for some $b \in B$ and $c \in C$ then $b = c = 0$, since otherwise $0 \in A(i+1)$, contradicting the assumption. By Lemma 2.2 $|B + C| \geqslant |B| + |C| - 1 = |A(i)| + |A| + 1$. Since $B + C = A(i+1) \cup \{0\}$ we conclude that $|A(i+1)| \geqslant (i+1)\,|A|$, as claimed. In particular, we obtain $|A(k)| \geqslant k\,|A| \geqslant n$ and hence $A(k) = G$. Thus $0 \in A(k)$, a contradiction. This completes the proof of the corollary. ∎

The next lemma follows easily from the known estimates for Turán numbers for hypergraphs, (see [De]). A slightly weaker version of it can be proved by some standard probabilistic arguments.

LEMMA 2.4. *Let H be a 3-uniform hypergraph with m vertices and at most $l \cdot m$ edges. Then H contains an independent set of size at least $m/(1+\sqrt{3l})$, i.e., a set of at least $m/(1+\sqrt{3l})$ vertices that contains no edge.*

The next proposition and Lemma 2.1 imply Theorem 1.1.

PROPOSITION 2.5. *Let A be a subset of Z_n of cardinality $|A| \geq (n/k) + (1+\sqrt{3(k-2)})\, r_3(n)$. Then there is a subset $B \subseteq A$ of cardinality $1 \leq |B| \leq k$ such that $\sum_{b \in B} b = 0$ (in Z_n).*

Proof. It is convenient to first consider the elements of A as integers in $N = \{1, 2, \ldots, n\}$ rather than residues modulo n. Call an element $a \in A$ *good* if it is the midterm of at least $k-1$ distinct 3 term arithmetic progressions of elements of A. Otherwise, call it *bad*. Let C be the set of all bad members of A. We claim that $|C| \leq (1+\sqrt{3(k-2)})\, r_3(n)$. Indeed, suppose this is false. Let H be the three uniform hypergraph whose vertices are all elements of C. A triple $\{c_1, c_2, c_3\}$ is an edge if c_1, c_2, c_3 form a 3 term arithmetic progression. By the definition of C, no member of C is the middle term of more than $k-2$ such progressions and hence the number of edges of H is at most $(k-2) \cdot |C|$. By Lemma 2.4, H contains an independent set of size at least $|C|/(1+\sqrt{3(k-2)}) > r_3(n)$. However, this set corresponds to a subset of cardinality greater than $r_3(n)$ which contains no 3-term arithmetic progression. This contradicts the definition of $r_3(n)$, and thus $|C| \leq (1+\sqrt{3(k-2)})\, r_3(n)$, as claimed.

Let $\bar{A} = A \setminus C$ be the set of all good members of A. By assumption $|\bar{A}| \geq n/k$. Hence, by Corollary 2.3 there are $a_1, \ldots, a_s \in \bar{A}$ such that

$$\sum_{i=1}^{s} \alpha_i a_i \equiv 0 \pmod{n}, \quad \alpha_i \geq 1, \qquad \sum_{i=1}^{s} \alpha_i \leq k, \quad s \geq 1. \tag{2.1}$$

Among all the choices for $s, a_1, \ldots, a_s, \alpha_1, \ldots, \alpha_s$ that satisfy (2.1) choose one for which $x = \max \alpha_i$ is minimum and is obtained the minimum possible number of times. To complete the proof we must show that for this choice $\max \alpha_i = 1$. Suppose this is false and assume, without loss of generality, that $\alpha_1 = \max \alpha_i \geq 2$. However, a_1 is a good member of A, and thus there are $k-1$ pairs (c_1^i, c_2^i) $1 \leq i \leq k-1$ of elements of A such that $2a_1 = c_1^i + c_2^i$ for all $1 \leq i \leq k-1$. Clearly all these pairs are pairwise disjoint. Since $\sum_{i=1}^{s} \alpha_i = k$ and $\alpha_1 \geq 2$ we conclude that $s-1 \leq k-2$ and hence there is an i, $1 \leq i \leq k-1$ such that $\{c_1^i, c_2^i\} \cap \{a_2, \ldots, a_{s-1}\} = \varnothing$. Hence $(\alpha_1 - 2)\, a_1 + \alpha_2\, a_2 + \cdots + \alpha_s\, a_s + c_1^i + c_2^i = 0 \pmod{n}$ contradicting the choice of $s, a_1, \ldots, a_s$ $\alpha_1, \ldots, \alpha_s$. Thus $\alpha_i = 1$ for all $1 \leq i \leq s$, and the assertion of Proposition 2.5 follows. ∎

As mentioned above, Proposition 2.5 and Lemma 2.1 imply Theorem 1.1

(and, in fact, a slightly stronger statement). We conclude this section by showing how to deduce from Theorem 1.1 that $f(n, 2n) = (\frac{1}{3} + o(1)) \cdot n$.

COROLLARY 2.6. *The maximum cardinality of a subset* $A \subseteq N = \{1, 2, \ldots, n\}$ *such that there is no* $B \subseteq A$ *with* $\sum_{b \in B} b = 2n$ *is* $(\frac{1}{3} + o(1)) \cdot n$. *More precisely, for all* $n \geq 2$,

$$\lceil n/3 \rceil + 1 \leq f(n, 2n) < \frac{n}{3} + 3 + (1 + \sqrt{3})\, r_3(n).$$

Proof. The set $A = \{i \in N: i \geq \lfloor 2n/3 \rfloor\}$ has cardinality $\lceil n/3 \rceil + 1$ and clearly there is no $B \subseteq A$ with $\sum_{b \in B} b = 2n$. To prove the upper bound, suppose $A \subseteq N$ has cardinality $|A| \geq (n/3) + 3 + (1 + \sqrt{3})\, r_3(n)$. By Proposition 2.5, there is a subset $B_1 \subseteq A$, $1 \leq |B_1| \leq 3$ with $\sum_{b \in B} b \equiv 0 \pmod{n}$. Since $|B_1| \leq 3$, the sum $\sum_{b \in B_1} b$ is either n or $2n$. If it is $2n$ we take $B = B_1$. If it is n we apply Proposition 2.5 to $A \setminus B_1$ to get another subset $B_2 \subseteq A \setminus B_1$ with $|B_2| \leq 3$ and $\sum_{b \in B_2} b = n$. Then for $B = B_1 \cup B_2$ we have $\sum_{b \in B} b = 2n$. This completes the proof. ∎

3. FORBIDDING ONE SUM

In this section we prove Theorem 1.2. To this end we need several lemmas. For an abelian group G, an element $a \in G$ and a subset $B \subseteq G$, define $f_B(a) = |(a + b) \cap \bar{B}|$. This function was introduced by Erdös and Heilbronn in [EH]. Olson [O] proved the following simple but useful lemma.

LEMMA 3.1. (i) $f_B(\sum_{i=1}^{s} a_i) \leq \sum_{i=1}^{s} f_B(a_i)$.

(ii) *If* $E \subseteq G$, *then*

$$\sum_{e \in E} f_B(e) \geq |B| \cdot (|E| - |B|).$$

The next lemma is the well known Cauchy–Davenport theorem (see [Da]).

LEMMA 3.2. *If* p *is a prime and* $A, B \subseteq Z_p$ *then* $|A + B| \geq \min\{p, |A| + |B| - 1\}$.

LEMMA 3.3. *If* p *is a prime,* $k > 0$ *an integer and* $A \subseteq Z_p$ *satisfies* $|A| \geq (2p/k) + 8k$ *then for every* $g \in Z_p$ *there is a subset* $B \subseteq A$ *of cardinality* $|B| \leq 8k - 2$ *so that* $\sum_{b \in B} b = g$. *In particular, there are at most* $8k - 2$ *distinct elements of* A *whose sum is* 0.

Proof. Let $C_1 \subseteq A$ be an arbitrary subset of A of cardinality $p/4k < |C_1| \leqslant (p/4k) + 1$. For a set $F \subseteq G$, let F^* denote the set of all subset-sums of F, i.e., $F^* = \{\sum_{f \in F'} f : F' \subseteq F\}$. We claim that for every i, $0 \leqslant i \leqslant 4k-2$ there are i distinct elements $b_1, b_2, \ldots, b_i \in A \setminus C_1$ such that

$$|\{b_1, b_2, \ldots, b_i\}^* + C_1| > \frac{i+2}{2} \cdot \frac{p}{4k}. \tag{3.1}$$

This certainly holds for $i = 0$. Assuming it holds for $i < 4k-2$ we prove it for $i+1$. Put $D = A \setminus (C_1 \cup \{b_1, b_2, \ldots, b_i\})$. Clearly $|D| \geqslant (p/k) + 1$. By Lemma 3.2 the sum of $\lfloor (i+2)/2 \rfloor$ copies of D satisfies

$$|D + D + \cdots + D| \geqslant \min\left(p, \left\lfloor \frac{i+2}{2} \right\rfloor \cdot \frac{p}{k}\right) \geqslant \frac{i+2}{2}\left(\frac{p}{2k} + 1\right).$$

Let B be a subset of $\{b_1, \ldots, b_i\}^* + C_1$ of cardinality greater than $((i+2)/2 \cdot (p/4k)$ but not greater than half the cardinality of the above sum $D + D + \cdots + D$, and let E be a subset of $D + D + \cdots + D$ of cardinality $2|B|$. By Lemma 3.1(ii) $\sum_{e \in E} f_B(e) \geqslant |B| \cdot (|E| - |B|)$ and thus there is an $e \in E$ such that $f_B(e) \geqslant |B| \cdot (|E| - |B|)/|E| = |B|/2$. By definition, $e = d_1 + d_2 + \cdots + d_{\lfloor (i+2)/2 \rfloor}$ for some $d_1, d_2, \ldots, d_{\lfloor (i+2)/2 \rfloor} \in D$. Hence, by Lemma 3.1(i) $f_B(d_j) \geqslant |B|/(i+2)$ for at least one d_j. Define $b_{i+1} = d_j$. Observe that

$$\{b_1, \ldots, b_{i+1}\}^* + C_1 \supseteq B \cup (b_{i+1} + B),$$

and hence

$$\begin{aligned} |\{b_1, \ldots, b_{i+1}\}^* + C_1| &\geqslant |B| + f_B(d_j) \geqslant |B|\left(1 + \frac{1}{i+2}\right) \\ &> \frac{i+2}{2} \cdot \frac{p}{4k}\left(1 + \frac{1}{i+2}\right) = \frac{i+3}{2} \cdot \frac{p}{4k}. \end{aligned}$$

Therefore (3.1) holds for all $i \leqslant 4k-2$ and in particular, there is a subset $B_1 \subseteq A \setminus C_1$ of cardinality $|B_1| = 4k-2$ such that

$$|B_1^* + C_1| > p/2. \tag{3.2}$$

Now let $C_2 \subseteq A \setminus (C_1 \cup B_1)$ be any subset of cardinality $p/4k < |C_2| \leqslant (p/4k) + 1$. Repeating the argument above one can show that there is a set $B_2 \subseteq A \setminus (C_1 \cup B_1 \cup C_2)$, $|B_2| = 4k-2$, such that

$$|B_2^* + C_2| > p/2. \tag{3.3}$$

Let $g \in Z_p$ be an arbitrary element. By (3.2) and (3.3) the two sets $B_1^* + C_1$ and $g - (B_2^* + C_2)$ have a nonempty intersection. Therefore, there are $c_1 \in C_1$, $c_2 \in C_2$, $B_1' \subseteq B_1$ and $B_2' \subseteq B_2$ such that

$$c_1 + c_2 + \sum_{b \in B_1' \cup B_2'} b = g.$$

Define $B = B_1' \cup B_2' \cup \{C_1, C_2\}$. Clearly $|B| \leqslant 8k-2$ and $\sum_{b \in B} b = g$. This completes the proof of the lemma. ▮

LEMMA 3.4. *Suppose $n \geqslant 1$ and let p be a prime, $n \leqslant p \leqslant 3n$. Let k be an integer and let l denote the least common multiple of $2, 3, \ldots, 8k-2$. Then, every set $A \subseteq N = \{1, 2, \ldots, n\}$ of cardinality $|A| \geqslant (6n/k) + (8k)^2 l$ contains a subset B of cardinality $|B| \leqslant 8kl$ such that $\sum_{b \in B} b = l \cdot p$.*

Proof. Since $|A| \geqslant (2p/k) + 8k$ there is, by Lemma 3.3, a subset $B_1 \subseteq A$ of cardinality $|B_1| \leqslant 8k-2$ such that $\sum_{b \in B_1} b = 0 \pmod p$. Put $\sum_{b \in B_1} b = l_1 \cdot p$ and observe that $l_1 \leqslant 8k-2$. Suppose we have already defined, for some $i < 8kl$, i pairwise disjoint subsets $B_1, \ldots, B_i$ of A, each of cardinality at most $8k-2$, such that for every $1 \leqslant j \leqslant i$, $\sum_{b \in B_j} b = l_j \cdot p$, where $1 \leqslant l_j \leqslant 8k-2$ is an integer. Put $\bar{A} = A \setminus (\bigcup_{j=1}^{i} B_j)$ and observe that $|A| \geqslant (2p/k) + 8k$. Hence, by Lemma 3.3, there is a subset $B_{i+1} \subseteq A \setminus \bigcup_{j=1}^{i} B_j$, so that $\sum_{b \in B_{i+1}} b = l_{i+1} \cdot p$ where $l_{i+1} \leqslant 8k-2$. It follows that A contains $8kl$ pairwise disjoint subsets $B_1, \ldots, B_{8kl}$ such that $\sum_{b \in B_j} b = l_j \cdot p$, where $1 \leqslant l_j \leqslant 8k-2$. By the Pigeonhole principle there is some i, $1 \leqslant i \leqslant 8k-2$ so that at least l/i of the l_j's equal i. Let B be the union of l/i of the corresponding B_j's. Then $|B| \leqslant (8k-2) \cdot l/i \leqslant 8kl$ and $\sum_{b \in B} b = l \cdot p$, as needed. ▮

The well known conjecture of Goldbach asserts that any even integer greater than 2 is the sum of two primes. Vinogradov [V] (see also [Da2]) proved that there is an n_0 so that every odd integer greater than n_0 is a sum of three primes. His proof can be easily modified to show that these primes can be chosen in the range, e.g., $(0.3n, 0.35n)$. This is stated in the following lemma, whose proof is an easy modification of the one given in [Da2] to Vinogradov's theorem.

LEMMA 3.5. *For $n > n_0$, every odd integer in the range $(4n, 8n)$ is a sum of three primes p_1, p_2, p_3, where $n \leqslant p_i \leqslant 3n$. Thus every integer $m > 16n$ is a sum of at most m/n primes, each greater or equal than n and smaller or equal than $3n$.*

PROPOSITION 3.6. *There exists an n_0, such that for every $n > n_0$ and every m, if $s = \mathrm{snd}(m)$, $8k-2 < s$, l is the least common multiple of $2, 3, \ldots, 8k-2$ and $m/l > 16n$, then any set $A \subseteq N = \{1, \ldots, n\}$ that satisfies $|A| \geqslant (6n/k) + (8k)^2 l + (m/n) \cdot 8k$ contains a subset $B \subseteq A$ so that $\sum_{b \in B} b = m$.*

Proof. By definition $l \mid m$. Since $m/l > 16n$, by Lemma 3.5 there exists a sequence $(p_1, p_2, \ldots, p_s)$ of primes, where $s \leqslant m/l \cdot n$, $n \leqslant p_i \leqslant 3n$ and $\sum_{i=1}^{s} p_i = m/l$. By repeated application of Lemma 3.4 we obtain s pairwise disjoint subsets $B_1, \ldots, B_s$ of A, where $\sum_{b \in B_i} b = l \cdot p_i$ for $1 \leqslant i \leqslant s$. Define $B = B_1 \cup \cdots \cup B_s$. Then $B \subseteq A$ and $\sum_{b \in B} b = m$, as needed.

Proof of Theorem 1.2. The lower bound $f(n, m) \geqslant \lfloor n/\mathrm{snd}(m) \rfloor$ is trivial. It clearly suffices to prove the upper bound for $n > n_1$, where $n_1 = n_1(\varepsilon)$ is any constant, since the constant $c(\varepsilon)$ can be adjusted to give the result for $n \leqslant n_1$. Suppose $n^{1+\varepsilon} \leqslant m \leqslant n^2/\log^2 n$ and put $s = \mathrm{snd}(m)$. By the prime number theorem $s \leqslant (2 + o(1)) \cdot \log n$. If $s < 8$ there is nothing to prove. Otherwise, define $k = \min(\lfloor s/8 \rfloor, \varepsilon \log n/16)$ and note that $8k - 2 < s$ and that $k \geqslant d(\varepsilon) \cdot s$ for some $d(\varepsilon) > 0$. Let l be the least common multiple of $2, 3, \ldots, 8k-2$. Then $l = e^{(8k-2)(1+o(1))} \leqslant n^{(\varepsilon/2)(1+o(1))} < \frac{1}{16} n^{\varepsilon}$ for sufficiently large n. Hence $m/l > 16n$. By Proposition 3.6 for $n > n_0$,

$$f(n, m) < \frac{6n}{k} + (8k)^2 \cdot l + \frac{m}{n} \cdot 8k$$

$$\leqslant \frac{n}{d(\varepsilon) \cdot s} + O(\log^2 n \cdot n^{\varepsilon}) + O\left(\frac{n}{\log n}\right) = O\left(\frac{n}{s}\right).$$

This completes the proof. ∎

4. Related Results and Open Problems

For $n \geqslant 1$ and a set M of integers, let $f(n, M)$ denote the maximum cardinality of a set $A \subseteq N$ that contains no subset $B \subseteq A$ such that $\sum_{b \in B} b \in M$. Clearly if $M = \{m\}$ then $f(n, M)$ coincides with our previous function $f(n, m)$.

Let M_1 denote the set of all powers of two. Clearly $f(3n, M_1) \geqslant n$, as shown by the set of all multiples of 3 up to $3n$. Erdös and Freud (see [E]) asked whether $f(3n, M_1) = n$ for all $n \geqslant 1$. At the moment we are unable to settle this problem. We can show, however, that $f(3n, M_1)$ is not far from n.

Proposition 4.1. *The maximum cardinality of a subset* $A \subseteq N = \{1, 2, \ldots, n\}$ *such that there is no* $B \subseteq A$ *whose sum of elements is a power of* 2 *is* $(\frac{1}{3} + o(1)) \cdot n$. *More precisely, for every* $n > 1$,

$$\lfloor n/3 \rfloor \leqslant f(n, M_1) < \frac{n}{3} + 13\sqrt{n} + (1 + \sqrt{3})\, r_3([n + 2\sqrt{n}]).$$

Proof. The lower bound is given by $A = \{i \in N : 3 \mid i\}$. To prove the upper bound, suppose $A \subseteq N$ has cardinality $|A| \geqslant (n/3) + 13\sqrt{n} + (1 + \sqrt{3})\, r_3([n + 2\sqrt{n}])$. We first claim that there is a sequence $a_1, \ldots, a_s$ of $s \leqslant 2\sqrt{n}$ not necessarily distinct integers, where $n \leqslant a_i \leqslant n + 2\sqrt{n}$ and

$\sum_{i=1}^{s} a_i$ is a power of two. Indeed one can easily check that every integer m that satisfies $n^{3/2} \leqslant m \leqslant 2n^{3/2}$ is a sum of s integers $a_1, \ldots, a_s$, where $\lfloor \sqrt{n} \rfloor \leqslant s \leqslant 2\sqrt{n}$ and $n \leqslant a_i \leqslant n + 2\sqrt{n}$. Clearly there is an m in this range which is a power of 2. By repeated application of Proposition 2.5 (or Corollary 2.6), we conclude that there are s pairwise disjoint subsets $B_1, B_2, \ldots, B_s$ of A, where $|B_i| \leqslant 6$ and $\sum_{b \in B_i} b = 2a_i$. Indeed, suppose $B_1, \ldots, B_i$ have already been defined for some $i < s$. Put $\bar{A} = A \setminus (\bigcup_{j=1}^{i} B_j)$ and observe that $|\bar{A}| \geqslant (a_{i+1}/3) + 3 + (1 + \sqrt{3}) r_3(a_{i+1})$. Hence, by Proposition 2.5 there are two pairwise disjoint subsets B'_{i+1} and B''_{i+1} of $\bar{A}$ such that $|B'_{i+1}| \leqslant 3$, $|B''_{i+1}| \leqslant 3$ and $\sum_{b \in B'_{i+1}} b \equiv 0 \pmod{a_{i+1}}$ $\sum_{b \in B''_{i+1}} b \equiv 0 \pmod{a_{i+1}}$. As in the proof of Corollary 2.6 we conclude that either B'_{i+1} or B''_{i+1} or $B'_{i+1} \cup B''_{i+1}$ can be chosen as B_{i+1}. Therefore the sets $B_1, \ldots, B_s$ with the desired properties exist. Now put $B = B_1 \cup \cdots \cup B_s$ and observe that $B \subseteq A$ $\sum_{b \in B} b$ is a power of 2. This completes the proof. ∎

Let M_2 denote the set of all square free numbers. Clearly $f(4n, M_2) \geqslant n$, as shown by the set of all multiples of 4 up to $4n$. Erdös and Freud [E] asked whether $f(4n, M_2) = n$ for all $n \geqslant 1$. Again, our methods here do not resolve this question but suffice to show that $f(4n, M_2) = (1 + o(1)) \cdot n$.

PROPOSITION 4.2. *The maximum cardinality of a subset $A \subseteq N$ such that there is no $B \subseteq A$ whose sum of elements is square free is $(\frac{1}{4} + o(1)) \cdot n$. More precisely*

$$\lfloor n/4 \rfloor \leqslant f(n, M_2) < \frac{n}{4} + (1 + \sqrt{6}) r_3([n + 16\sqrt{n}]) + 4\sqrt{n}.$$

Proof. The lower bound is given by $A = \{i \in N : 4 \mid i\}$. To prove the upper bound suppose $A \subseteq N$ has cardinality

$$|A| \geqslant \frac{n}{4} + (1 + \sqrt{6}) r_3([n + 16\sqrt{n}]) + 4\sqrt{n}.$$

We claim that there is a square free number m, $n \leqslant m \leqslant n + 16\sqrt{n}$ such that $2 \nmid m$ and $3 \nmid m$. Indeed, the number of elements in this range that are divisible by either 2 or 3 is smaller than $4 + 16\sqrt{n}\,\frac{2}{3}$. In addition, the number of elements in this range divisible by p^2 for some prime p, $3 < p \leqslant \sqrt{n + 16\sqrt{n}}$ is smaller than $1 + (1/p^2) \cdot 16\sqrt{n}$. One can easily check that

$$4 + 16\sqrt{n}\,\frac{2}{3} + \sum_{\substack{3 < p \leqslant \sqrt{n + 16\sqrt{n}} \\ p \text{ prime}}} \left(1 + \frac{1}{p^2} 16\sqrt{n}\right) < 16\sqrt{n}$$

and hence there is an m with the desired properties. Consider the elements of A as residues modulo m. By assumption $|A| \geqslant (m/4) + (1 + \sqrt{6}) r_3(m)$. Hence, by Proposition 2.5, there is a subset $B \subseteq A$ of cardinality $|B| \leqslant 4$

such that $\sum_{b\in B} b \equiv 0 \pmod m$. Since $|B| \leqslant 4$ we conclude that over the integers $\sum_{b\in B} b \in \{m, 2m, 3m\}$. However, by the choice of m each of these numbers is square free. This completes the proof. ∎

Let M_3 denote the set of all squares. Erdös [E] showed that $f(n, M_3) \geqslant (1+o(1))\cdot 2^{1/3}\cdot n^{1/3}$. An immediate consequence of Theorem 1.2 is that $f(n, M_3) = O(n/\log n)$. At the moment we are unable to improve this upper bound, but we suspect that the lower bound is closer to the truth.

We conclude this paper with the following conjecture, which is a strengthening of Theorem 1.2.

CONJECTURE 4.3. *If* $n^{1.1} \leqslant m \leqslant n^{1.9}$ *then*

$$f(n, m) = (1+o(1))\cdot n/\mathrm{snd}(m)$$

as $n \to \infty$.

ACKNOWLEDGMENT

I would like to thank A. M. Odlyzko for fruitful discussions.

Note added in proof. Conjecture 4.3 has been recently proved for $m \leqslant n^{3/2}$ by Lipkin and for $m \geqslant n^{5/3+\varepsilon}$ in [AF]. Related results appear in [EF]. Theorem 1.1 can be proved for every finite Abelian group of odd order by replacing Lemma 2.1 by the main result of [FGR].

REFERENCES

[Da] H. DAVENPORT, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[Da2] H. DAVENPORT, "Multiplicative Number Theory," 2nd ed., Chap. 26, revised by H. L. Montgomery, Springer-Verlag, Berlin, 1980.

[De] D. DECAEN, Extensions of a theorem of Moon and Moser on complete graphs, *Ars Combin.* **16** (1983), 5–10.

[E] P. ERDÖS, Some problems and results on combinatorial number theory, *in* "Proc. 1st China Conference in Combinatorics, 1986," to appear.

[EH] P. ERDÖS AND H. HEILBRONN, On the addition of residue classes mod p, *Acta Arith.* **9** (1964), 149–159.

[GRS] R. L. GRAHAM, B. L. ROTHSCHILD, AND J. H. SPENCER, "Ramsey Theory," Wiley, New York, 1980.

[H] D. R. HEATH-BROWN, Integer sets containing no arithmetic progressions, preprint, 1986.

[O] J. E. OLSON, An addition theorem modulo p, *J. Combin. Theory* **5** (1968), 45–52.

[R] K. ROTH, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.

[Sch] P. SCHERK, *Amer. Math. Monthly* **62** (1955), 46–47.

[S] R. STALLEY, Private communication from D. Richman.

[V] I. M. VINOGRADOV, *Mat. Sb. (N.S.)* **44** (1937), 179–195.

[AF] N. ALON AND G. FRIEMAN, On sums of subsets of a set of integers, preprint (1987).

[EF] P. ERDÖS AND G. FRIEMAN, On two additive problems, preprint (1987).

[FGR] P. FRANKL, R. L. GRAHAM AND V. RÖDL, On subsets of Abelian groups with no 3-term arithmetic progression, preprint (1986).