COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 8 (4) 1988 297—306

ON SUMS OF SUBSETS OF A SET OF INTEGERS

N. ALON* and G. FREIMAN

Received July 1, 1987

For $r\geqq 2$ let $p(n,r)$ denote the maximum cardinality of a subset A of $N=\{1,2,\ldots,n\}$ such that there are no $B\subset A$ and an integer y with $\sum_{b\in B} b=y^r$. It is shown that for any $\varepsilon>0$ and $n>n(\varepsilon)$, $(1+o(1))2^{1/(r+1)}n^{(r-1)/(r+1)}\leqq p(n,r)\leqq n^{\varepsilon+2/3}$ for all $r\leqq 5$, and that for every fixed $r\geqq 6$, $p(n,r)=(1+o(1))\cdot 2^{1/(r+1)}n^{(r-1)/(r+1)}$ as $n\to\infty$. Let $f(n,m)$ denote the maximum cardinality of a subset A of N such that there is no $B\subset A$ the sum of whose elements is m. It is proved that for $3n^{5/3+\varepsilon}\leqq m\leqq n^2/20\log^2 n$ and $n>n(\varepsilon)$, $f(n,m)=\lfloor n/s\rfloor+s-2$, where s is the smallest integer that does not divide m. A special case of this result establishes a conjecture of Erdős and Graham.

Introduction

Let n be an integer and define $N=\{1,2,\ldots,n\}$. For a set $A\subset N$, let A^* denote the set of all sums of subsets of A, i.e. $A^*=\left\{\sum_{b\in B} b\colon\ B\subseteq A\right\}$. There are several recent and less recent problems and results, that assert that if $|A|$ is large enough, then A^* must contain some numbers of prescribed type. See [5], [3], [1], [2], [4]. In particular, Erdős [3] has recently asked for the maximum cardinality $p(n,2)$ of a subset A of N such that A^* contains no squares. He observed that

$$p(n,2)\geqq (1+o(1))2^{1/3}n^{1/3} \tag{1.1}$$

and in [1] it is noticed that $p(n,2)\leqq c_2 n/\log n$. This is considerably improved in [4], where it is shown that for every $\varepsilon>0$,

$$p(n,2)\leqq c_3 n^{3/4+\varepsilon}, \tag{1.2}$$

provided $n>n_0(\varepsilon)$. Here and throughout this paper, the numbers $c_1, c_2, c_3, \ldots$, always denote some absolute positive constants. In this paper we further improve (1.2) and show that for every $\varepsilon>0$

$$p(n,2)\leqq n^{2/3+\varepsilon}; \tag{1.3}$$

provided $n>n_1(\varepsilon)$. More generally, for $r\geqq 2$ let $p(n,r)$ denote the maximum cardinality of a subset A of N such that there is no r-th power of an integer in A^*. An easy

* Research supported in part by Allon Fellowship, by a Bat-Sheva de Rothschild Grant and by the Fund for Basic Research administered by the Israel Academy of Sciences.
AMS subject classification (1980): 10 A 50, 10 B 35, 10 J 10.

generalization of (1.1) shows that

$$p(n,r) \geqq (1+o(1)) \cdot 2^{1/(r+1)} \cdot n^{(r-1)/(r+1)} \tag{1.4}$$

for every fixed $r \geqq 2$. Indeed, let p be the smallest prime such that the sum of the elements in the set $A=\{a \in N\colon p|a\}$ is less than p^r. One can easily check that $p=(1+o(1))2^{-1/(r+1)} \cdot n^{2/(r+1)}$, and hence $|A| \geqq (1+o(1))2^{1/(r+1)} \cdot n^{(r-1)/(r+1)}$. As each member of A^* is divisible by p and is smaller than p^r (1.4) follows. The following result shows that (1.4) is sharp for every $r \geqq 6$.

Proposition 1.1.
(i) *For every fixed* $r \geqq 6$

$$p(n,r) = (1+o(1))2^{1/(r+1)} n^{(r-1)/(r+1)}. \tag{1.5}$$

(ii) *For every* $2 \leqq r \leqq 5$, $\varepsilon > 0$ *and* $n > n_0(\varepsilon)$

$$(1+o(1))2^{1/(r+1)} n^{(r-1)/(r+1)} \leqq p(n,r) \leqq n^{2/3+\varepsilon}.$$

An estimate similar to (1.5), but only for $r \geqq 10$, is proved in [4].

For $m \geqq 1$, let $f(n,m)$ denote the maximum cardinality of a set $A \subseteq N$ such that $m \notin A^*$. Let $snd(m)$ denote the smallest integer that does not divide m. Clearly $f(n,m) \geqq \lfloor n/snd(m) \rfloor$. Indeed, the set of all multiples of $snd(m)$ in N has cardinality $\lfloor n/snd(m) \rfloor$ and contains no subset the sum of whose elements is m. In [1] it is shown that for every $n^{1+\varepsilon} < m < n^2/\log^2 n$, $f(n,m) \leqq c(\varepsilon) \cdot \lfloor n/snd(m) \rfloor$. It is conjectured in [1] that in fact in this range $f(n,m) = (1+o(1)) \cdot n/snd(m)$. This is proved in [4] for $n \log n < m < n^{3/2}$. The following theorem, that determines $f(n,m)$ precisely for $3n^{5/3+\varepsilon} < m < n^2/20 \log^2 n$, and $n > n_0(\varepsilon)$ establishes the conjecture for this range of m.

Theorem 1.2. *For every* $\varepsilon > 0$, $n > n(\varepsilon)$ *and every* m *satisfying*

$$3n^{5/3+\varepsilon} < m < n^2/20 \log^2 n,$$

$$f(n,m) = \left\lfloor \frac{n}{snd(m)} \right\rfloor + snd(m) - 2.$$

An easy consequence of this Theorem is that for every n there is an m such that $f(n,m) = (1/2+o(1))n/\log n$: simply take as m the least common multiple of all integers smaller than s, where s is the largest integer so that this common multiple is still at most $n^2/20 \log^2 n$. By the prime number theorem this gives $s = (2+o(1))\log n$, and hence $f(n,m) = (1/2+o(1))n/\log n$. This verifies a conjecture of Erdős and Graham [3], who observed that $f(n,m) \geqq (1/2+o(1))n/\log n$ for all n, m.

The estimates (1.3) and (1.5), together with the proof of Theorem 1.2 follow from the following, somewhat technical, result.

Proposition 1.3. *Let* $A = \{a_1, a_2, \ldots, a_x\}$ *be a subset of cardinality* x *of* $N = \{1, 2, \ldots, n\}$. *Define* $S_A = 1/2 \sum_{i=1}^{x} a_i$ *and* $B_A = 1/2 \sqrt{\sum_{i=1}^{x} a_i^2}$. *Suppose that* $x > n^{2/3+\varepsilon}$, *where* $\varepsilon > 0$ *and* $n > n_0(\varepsilon)$ *and suppose, further, that*

$$|\{i | a_i \equiv 0 \pmod q\}| \leqq x - n^{2/3} \quad \textit{for all} \quad q \geqq 2. \tag{1.6}$$

Then every integer M *satisfying*

$$|M - S_A| \leqq B_A \tag{1.7}$$

belongs to A^*. *Moreover; the number of representations of* M *as a sum* $\sum_{i=1}^{x} \varepsilon_i a_i$ *with* $\varepsilon_i \in \{0, 1\}$ *is*

$$(1.8) \qquad (1+o(1))\cdot\frac{2^x}{\sqrt{2\pi B_A^2}}\, e^{\frac{-(M-S_A)^2}{2B_A^2}}$$

The proof of Proposition 1.3 is analytic, and is given in Section 2. In Section 3 we apply this proposition to derive the upper estimates (1.3) and (1.5) (and to prove Proposition 1.1). In Section 4 we prove Theorem 1.2 and Section 5 contains some concluding remarks.

2 The Proof of Proposition 1.3

Let ε be a fixed positive number, and suppose that n is sufficiently large, $x > n^{2/3+\varepsilon}$ and that $A=\{a_1, a_2, \dots, a_x\}$ is a subset of cardinality x of $N=\{1, 2, \dots, n\}$ satisfying (1.6). For $1 \leqq j \leqq x$ define $\varphi_j(\alpha)=1/2(1+e^{2\pi i\alpha a_j})$ and $\varphi(\alpha)=\prod_{j=1}^{x}\varphi_j(\alpha)$. For an integer M define $J_M=2^x\int_0^1 \varphi(\alpha)e^{-2\pi i\alpha M}\,d\alpha$. Clearly, J_M is simply the number of solutions of the equation $\sum_{i=1}^{x}\varepsilon_i a_i=M$ with $\varepsilon_i\in\{0, 1\}$. Put $F_M(\alpha)=\varphi(\alpha)e^{-2\pi i\alpha M}$ and $L=[n^{1+\varepsilon}]$. Since $F_M(\alpha)$ has period 1, $J_M=2^x\int_{-1/L}^{1-1/L} F_M(\alpha)d\alpha$. Split the interval $[-1/L, 1-1/L]$ into the major arc $I_1=[-1/L, 1/L]$ and the minor arc $I_2=[1/L, 1-1/L]$. In order to prove Proposition 1.3 it clearly suffices to prove that for every M that satisfies (1.7):

$$(2.1) \qquad |F_M(\alpha)| \leqq \frac{1}{n^3} \quad \text{for all} \quad \alpha\in I_2$$

and

$$(2.2) \qquad \int_{I_1} F_M(\alpha)\,d\alpha = (1+o(1))\cdot\frac{1}{\sqrt{2\pi B_A^2}}\, e^{\frac{-(M-S_A)^2}{2B_A^2}}$$

hold.

We first establish (2.1). As is well known, every real α has a representation $\alpha=p/q+z$ where $(p, q)=1$, $0<q<L$ and $|z|<1/qL$. For $\alpha\in I_2=[1/L, 1-1/L]$ it is obvious that in this representation $q\geqq 2$. Clearly $\varphi_j(\alpha)=1/2\left(1+e^{2\pi i\left(\frac{pa_j}{q}+za_j\right)}\right)$ and $|za_j|<n/(qL)<1/2q$. For $0\leqq s<q$, let m_s denote the number of j, $1\leqq j\leqq x$ that satisfy $pa_j\equiv s \pmod q$. We consider three possible cases, according to the value of q. In our estimates we use the trivial fact that $|\varphi_j(\alpha)|\leqq 1$ and the easy inequality $(1/2)|1+e^{2\pi iy}|\leqq e^{-\pi y^2}$ which hold for all $0\leqq y\leqq 1/2$. As before, $c_1, c_2, c_3, \dots$, always denote absolute positive constants and whenever needed we assume that n is sufficiently large

Case 1. $q>n$.

In this case $m_s \leqq 1$ for all s and hence, clearly

$$|\varphi(\alpha)| \leqq \prod_{s=1}^{\left\lfloor\frac{x-1}{2}\right\rfloor} \frac{1}{2}\left|1+e^{2\pi i\frac{s-1/2}{q}}\right| \cdot \prod_{s=-\left\lfloor\frac{x-1}{2}\right\rfloor}^{-1} \frac{1}{2}\left|1+e^{2\pi i\frac{s+1/2}{q}}\right| \leqq$$

$$\leqq \prod_{s=1}^{\left\lfloor\frac{x}{2}\right\rfloor-2} e^{-c_1\frac{s^2}{q^2}} \leqq e^{-c_2\frac{x^3}{q^2}} \leqq e^{-c_2\frac{n^{2+3\varepsilon}}{L^2}} \leqq e^{-c_2 n^{\varepsilon}} \ll \frac{1}{n^3}.$$

Case 2. $q < 10n/x (< 10n^{1/3-\varepsilon})$.

Since A satisfies (1.6) we conclude that $\sum_{s\neq 0} m_s \geqq n^{2/3}$. Hence

$$|\varphi(\alpha)| \leqq \left(\frac{1}{2}\left|1+e^{2\pi i\frac{1}{2q}}\right|\right)^{n^{2/3}} \leqq e^{-c_3\frac{n^{2/3}}{q^2}} \leqq e^{-c_4 n^{2\varepsilon}} \ll \frac{1}{n^3}.$$

Case 3. $10n/x \leqq q \leqq n$.

In this case $m_s \leqq \lceil n/q \rceil \leqq 2n/q$ for all s and hence

$$|\varphi(\alpha)| \leqq \prod_{s=1}^{\frac{xq}{4n}} \left(\frac{1}{2}\left|1+e^{2\pi i\frac{(s-1/2)}{q}}\right|\right)^{2n/q} \leqq e^{-c_5\frac{x^3q^3}{n^3q^2}\cdot\frac{n}{q}} = e^{-c_5\frac{x^3}{n^2}} \leqq e^{-c_5 n^{3\varepsilon}} \ll 1/n^3.$$

Since $|F_M(\alpha)| = |\varphi(\alpha)|$ this completes the proof of (2.1).

Next we prove (2.2). Put $S = S_A = (1/2)\sum_{i=1}^{x} a_i$ and $B = B_A = (1/2)\sqrt{\sum_{i=1}^{x} a_i^2}$ and $M = S+m$. By (1.7) $|m| \leqq B$. Notice that $B^2 \geqq 1/4 \sum_{i=1}^{x} i^2 \geqq c_6 x^3 \geqq c_6 n^{2+3\varepsilon}$ and hence $B \geqq c_7 n^{1+(3/2)\varepsilon}$. Since $L = \lceil n^{1+\varepsilon} \rceil$ we conclude that for $b = 10\sqrt{\log n}/B$, $b \leqq 1/L$ holds. Define $J_1 = [-b, b]$, $J_2 = [-1/L, -b]$, $J_3 = [b, 1/L]$ and $G_i = \int_{J_i} F_M(\alpha)\,d\alpha$ $(1 \leqq i \leqq 3)$. Clearly $\int_{I_1} F_M(\alpha)\,d\alpha = G_1+G_2+G_3$. For every $\alpha \in I_1 = [-1/L, 1/L]$, $|\alpha a_j| \leqq 1/n^{\varepsilon}$ holds. By the Taylor expansion formula, for every j, $1 \leqq j \leqq x$,

$$\varphi_j(\alpha)\cdot e^{-2\pi i\alpha\frac{a_j}{2}} = e^{-\frac{\pi^2}{2}\alpha^2 a_j^2 + o\left(\frac{\alpha^2 a_j^2}{l^{2\varepsilon}}\right)}$$

and hence

$$F_M(\alpha) = \left(\prod_{j=1}^{x} (\varphi_j(\alpha) e^{-2\pi i\alpha\frac{a_j}{2}})\right)\cdot e^{-2\pi i\alpha m} = e^{-2\pi^2\alpha^2B^2 - 2\pi i\alpha m + o\left(\frac{\alpha^2B^2}{l^{2\varepsilon}}\right)}.$$

If $|\alpha| \geqq b = 10\sqrt{\log n}/B$ then

$$|F_M(\alpha)| \leqq e^{-2\pi^2\alpha^2B^2(1+o(1))} \leqq \frac{1}{n^{200\pi^2(1+o(1))}} \ll \frac{1}{n^3}.$$

Hence $|G_2+G_3| \ll 1/n^3$. Similarly, since $\int_{|\alpha|\geqq b} e^{-2\pi^2\alpha^2B^2(1+o(1))} \ll 1/n^3$ we conclude that

$$\int_{I_1} F_M(\alpha)\,d\alpha = G_1 + o\left(\frac{1}{n^3}\right) \leqq \int_{-\infty}^{\infty} e^{-2\pi^2\alpha^2B^2 - 2\pi i\alpha m}\cdot\left(1+o(1)\right).$$

However, as is well known (see, e.g., [6]),

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-\frac{1}{2}t^2+itu}\,dt = e^{-\frac{1}{2}u^2}.$$

Substituting $t=2\pi\alpha B$ and $u=m/B$ we obtain that

$$\int_{I_1} F_M(\alpha)\,d\alpha = (1+o(1))\cdot\frac{1}{\sqrt{2\pi B^2}}\,e^{-\frac{m^2}{2B^2}}.$$

This establishes (2.2) and completes the proof of Proposition 1.3. ∎

3 Forbidding *r*-th powers

In this section we prove Proposition 1.1. We start with the following simple consequences of Proposition 1.3.

Lemma 3.1. *Let A be a subset of cardinality x of $N=\{1, 2, ..., n\}$ and let S_A denote half the sum of its elements. Suppose that $x>n^{2/3+\varepsilon}$, where $\varepsilon>0$ and $n>n(\varepsilon)$ and suppose, further, that*

$$|\{a\in A \mid a \equiv 0 \pmod q\}| \leqq x-\frac{x}{2\log n} \quad \text{for all} \quad q \geqq 2. \tag{3.1}$$

Then every integer M satisfying

$$\left(1-\frac{1}{4\log n}\right)S_A \leqq M \leqq S_A \tag{3.2}$$

belongs to A^*.

Proof. Suppose $A=\{a_1, a_2, ..., a_x\}$ where $1\leqq a_1<a_2<...<a_x\leqq n$. For every integer j, $\lfloor(1-1/(4\log n))x\rfloor\leqq j\leqq x$, define $A_j=\{a_1, ..., a_j\}$. Thus, in particular, $A_x=A$. Define $S_j=(1/2)\sum_{i=1}^{j} a_i$ and $B_j=(1/2)\sqrt{\sum_{i=1}^{j} a_i^2}$. Clearly $S_x\geqq S_{x-1}\geqq ...$ and $B_x\geqq B_{x-1}\geqq ....$ It is also easy to check that for the smallest j $(j=\lfloor(1-1/(4\log n))x\rfloor)$, $S_j\leqq(1-1/(4\log n))\cdot S_x$, and that every B_{j+1} is bigger than the difference between S_j and S_{j+1}. Since each A_j is obtained from A by deleting less than $[x/(4\log n)]$ elements, (3.1) implies that for each j

$$|\{a\in A_j \mid a \equiv 0 \pmod q\}| \leqq x-\frac{x}{2\log n} \leqq |A_j|-n^{2/3} \quad \text{for all} \quad q \geqq 2.$$

Hence one can apply Proposition 1.3 to each A_j and conclude that every integer M satisfying (3.2) belongs to A^*. This completes the proof. ∎

Lemma 3.2. *Suppose $\varepsilon>0$, $n>n(\varepsilon)$ and suppose A is a subset of cardinality x of N, where $x>2n^{2/3+\varepsilon}$. Then there exist an integer k, $1\leqq k\leqq 2n/x$ and a subset $B=\{b_1, ..., b_r\}$ of cardinality $r\geqq x/2$ of A satisfying the following:*

(i) *$b_i = kd_i$ for all $1 \leqq i \leqq r$, where $d_1, \ldots, d_r$ are integers, and*

(ii) *If $S = 1/2 \sum_{i=1}^{r} d_i$ then every integer K satisfying $\bigl(1 - 1/(4\log n)\bigr) S \leqq K \leqq S$ belongs to $\{d_1, d_2, \ldots, d_r\}^*$, (and hence $k \cdot K$ belongs to A^*).*

Proof. If A satisfies (3.1) then the assertion follows immediately from Lemma 3.1 (simply take $k=1, B=A$). Otherwise, choose a number q, for which (3.1) is violated and define

$$A_1 = \{a \in A \mid a \equiv 0 \pmod{q_1}\}, \quad \bar{A}_1 = \left\{\frac{a}{q_1} \,\Big|\, a \in A_1\right\}.$$

If $\bar{A}_1$ satisfies (3.1), then Lemma 3.1 gives the desired result with $k=q_1$, $B=A_1$. Otherwise choose a number q_2 for which (3.1) is violated and define

$$A_2 = \{a \in A_1 \mid a \equiv 0 \pmod{q_1 q_2}\}, \quad \bar{A}_2 = \left\{\frac{a}{q_1 q_2} \,\Big|\, a \in A_2\right\}.$$

Here, again, if A_2 satisfies (3.1), the desired result with $k=q_1q_2$ and $B=A_2$ follows. Else, we repeat the same process. Clearly, this process must stop after at most $\log n$ steps. Since in each step the new set A_{i+1} is of cardinality

$$|A_{i+1}| \geqq |A_i| - \frac{|A_i|}{2\log n} \geqq |A_i| - \frac{x}{2\log n}$$

we must stop with a set B of cardinality $r \geqq x/2$, and since all elements in this set are distinct and divisible by k, $k \leqq 2n/x$. This completes the proof. ∎

An immediate consequence of the last Lemma is the following.

Lemma 3.3. Suppose $\varepsilon > 0$, $n > n(\varepsilon)$, $x > 2n^{2/3+\varepsilon}$ *and* $A \subset N$, $|A| = x$. *Then there is an integer k, $k < 2n/x$ and a number $S \geqq x^2/16$ such that every integer M which satisfies*

$$k \mid M \quad \text{and} \quad \left(1 - \frac{1}{4\log n}\right) kS \leqq M \leqq kS \tag{3.3}$$

belongs to A^*.

Proof of Proposition 1.1, part (ii). In view of inequality (1.4) it suffices to prove the upper bound. Suppose $\varepsilon > 0$, $n > n(\varepsilon)$, $x > n^{2/3+\varepsilon}$ and $A \subset N$, $|A| = x$. We claim that there are integers y_2, y_3, y_4 and y_5 such that

$$\{y_2^2, y_3^3, y_4^4, y_5^5\} \subset A^* \tag{3.4}$$

(and hence $p(n, r) \leqq n^{2/3+\varepsilon}$ for all $2 \leqq r \leqq 5$, $n > n(\varepsilon)$).

Indeed, by Lemma 3.3 (with $\varepsilon' < \varepsilon$), there is an integer $k \leqq 2n^{1/3-\varepsilon}$ and a number $S \geqq (1/16) n^{4/3+2\varepsilon}$ such that every integer M that satisfies (3.3) belongs to A^*. One can easily check that since $S > \Omega(k^4 \cdot n^{6\varepsilon})$ there are integers z_2, z_3, z_4, z_5 such that

$$\{z_2^2 \cdot k, z_3^3 \cdot k^2, z_4^4 \cdot k^3, z_5^5 \cdot k^4\} \subseteq \left\{ y \,\Big|\, \left(1 - \frac{1}{4\log n}\right) S \leqq y \leqq S \right\}.$$

The numbers $y_i = z_i k$ $(2 \leqq i \leqq 5)$ satisfy (3.4) and complete the proof. ∎

Lemma 3.4. *Suppose $\varepsilon > 0$, $n > n(\varepsilon)$, and let A be a subset of cardinality x of N, where $x > 3n^{2/3+\varepsilon}\log n$. Then there exist a subset $G=\{g_1, \dots, g_t\}$ of cardinality t of A, and an integer q satisfying the following:*

(i) $t \geqq x - n^{2/3}$

(ii) $q \leqq n/t$

(iii) *Each g_i is divisible by q.*

(iv) *If $S=\sum_{i=1}^{t} g_i$ then every integer M, which is divisible by q and satisfies*

$$\frac{n^{2/3+\varepsilon}}{t}\cdot S + n^{4/3}\log n \leqq M \leqq S - \frac{n^{2/3+\varepsilon}}{t}\cdot S - n^{4/3}\log n$$

belongs to $G^* \subset A^*$.

Proof. By applying Lemma 3.2 (with $\varepsilon' < \varepsilon$) to the set of $n^{2/3+\varepsilon}$ smallest elements of A, we obtain a subset $B=B_1$ of cardinality $\Omega(n^{2/3})$ of A and an integer $k=k_1 \leqq n^{1/3}$, so that each element of B_1 is divisible by k and B_1^* contains a long arithmetic progression of multiples of k (containing at least $\Omega(n^{4/3+2\varepsilon}/\log n) \geqq \Omega(n^{4/3})$ numbers). Suppose that

$$|\{a \in A \mid a \not\equiv 0 \pmod k\}| \geqq k^2. \tag{3.5}$$

Then there is an i, $i \not\equiv 0 (\text{mod } k)$ such that $|\{a \in A | a \equiv i (\text{mod } k)\}| \geqq k$. Let $a_1, \dots, a_k$ be k distinct members of A, each congruent to i modulo $k=k_1$. Define $B_2 = B_1 \cup \cup \{a_1, \dots, a_{k_1}\}$, $k=k_2=g.c.d.(k_1, i)$. One can check that each element of B_2 is divisible by $k=k_2$ and that B_2^* contains an arithmetic progression of at least $\Omega(n^{4/3})$ multiples of $k=k_2$. If (3.5) still holds (for the new k) we continue the same process. Clearly it must stop after at most log n steps (as each k_i is a proper divisor of the previous one). When the process stops we have a set B of at most $n^{2/3+\varepsilon}+n^{1/3}\log n$ elements. Each element of B is divisible by k. Moreover, all but at most $k^2 \leqq n^{2/3}$ of the elements of A are divisible by k. Also, B^* contains an arithmetic progression of $\Omega(n^{4/3})$ terms of multiples of k. Define $q=k$ and $G=\{a \in A | a \equiv 0 (\text{mod } k)\}$, $t=|G|$. Then $t \geqq x-n^{2/3}$ and clearly $t \leqq n/q$ as all members of G are distinct. By adding to B^* all elements in $G \setminus B$, one by one, we conclude that G^* contains every multiple of $k=q$ whose distance from 0 and from $\sum_{g \in G} g$ is greater than $\sum_{b \in B} b$. However, clearly

$$\sum_{b \in B} b \leqq \frac{n^{2/3+\varepsilon}}{t}\cdot S + n^{4/3}\log n,$$

where the first term is a bound on the sum of the $n^{2/3+\varepsilon}$ smallest elements of A, and the second is a bound on the sum of the other elements added to B during the process described above. Thus G, t and q satisfy (i)—(iv), as needed. ∎

Proof of Proposition 1.1, part (1). In view inequality (1.4) it suffices to prove the upper bound. Fix $r \geqq 6$ and $\delta > 0$ and suppose A is a subset of cardinality $x \geqq (1+\delta)\cdot \cdot 2^{1/(r+1)} n^{(r-1)/(r+1)}$ of N. We must show that there is an integer y such that $y^r \in A^*$. Apply Lemma 3.4 to A to get G, t and q satisfying (i)—(iv).

Consider two possible cases.

Case 1.

$$q^r \geqq \frac{n^{2/3+\varepsilon}}{t}\cdot S + n^{4/3}\log n.$$

In this case, we claim that $q^r \in G^* \subseteq A^*$. Indeed

$$S = \sum_{i=1}^{t} g_i \geqq q(1+2+\ldots+t) > \frac{qt^2}{2} \geqq \frac{q(x-n^{2/3})^2}{2} = (1+o(1))\frac{qx^2}{2}.$$

Since $q \leqq n/t = (1+o(1))\,n/x$ and $x \geqq (1+\delta)2^{1/(r+1)}n^{(r-1)/(r+1)}$ one easily checks that

$$q^r \leqq S - \frac{n^{2/3+\varepsilon}}{t}S - n^{4/3}\log n = (1+o(1))S$$

and hence $q^r \in G^*$, by (iv). (Recall that $r \geqq 6$ and hence $x \geqq t \geqq \Omega(n^{5/7})$).

Case 2.

$$q^r \leqq \frac{n^{2/3+\varepsilon}}{t}S + n^{4/3}\log n.$$

In this case

$$q^r < \frac{2n^{2/3+\varepsilon}}{t}\cdot S$$

(as $S > t^2/2$ and $t = \Omega(n^{5/7})$). Hence

$$\frac{S}{q^r} > \frac{t}{2n^{2/3+\varepsilon}} = \Omega\,(n^{5/7-2/3-\varepsilon}).$$

Thus, the arithmetic progression of multiples M of q in the range described in Lemma 3.4, (iv) contains $\Omega(n^{1/21-\varepsilon})$ multiples of q^r, and the ratio between the largest and the smallest is (much) greater than 2. This implies that one of these multiples is of the form $q^r z^r$ for some integer z and hence $G^* \subset A^*$ constains an r-th power in this case, too. This completes the proof of the Proposition. ∎

4. Forbidding One Sum

In this section we prove Theorem 1.2 staed in Section 1. For convenience, we split the proof into a few lemmas.

Lemma 4.1. *For every sufficiently large n and every $m \leqq n^2$,*

$$f(n, m) \geqq \left\lfloor \frac{n}{snd(m)} \right\rfloor + snd(m) - 2.$$

Proof. Put $s = snd(m)$ and suppose $m \equiv i (\bmod s)$. Clearly $1 \leqq i \leqq s-1$ and $s \leqq 3\log n$. Let A_1 be the set of all $\lfloor n/s \rfloor$ multiples of s in $N \equiv \{1, 2, \ldots, n\}$. Let A_2 be a set of $i-1$ distinct members of N, each congruent to 1 modulo s, and let A_3 be a set of $s-i-1$ distinct members of N, each congruent to -1 modulo s. (Clearly, such A_2 and A_3 exist, as n is sufficiently large and $s \leqq 3\log n$). Define $A = A_1 \cup A_2 \cup A_3$. Clearly $|A| = \lfloor n/s \rfloor + s - 2$. To complete the proof it suffices to check that $m \notin A^*$. However, this is obvious, since no element of A^* is congruent to i modulo s. ∎

Lemma 4.2. *Let $s=p^k$ be a prime power, and let $a_1, a_2, \ldots, a_{s-1}$ be a sequence of $s-1$ (not necessarily distinct) non zero elements of the cyclic group Z_s. Then for every i, $1\leqq i\leqq p-1$ there are $\varepsilon_1, \ldots, \varepsilon_{s-1}\in\{0, 1\}$ such that in Z_s $\sum_{i=1}^{s-1}\varepsilon_i a_i=ip^{k-1}$.*

Proof. For every j, $1\leqq j\leqq s-1$, define $B_j=\left\{\sum_{i=1}^{j}\varepsilon_i a_i|\varepsilon_i\in\{0, 1\}\right\}$. Clearly $B_1= =|\{0, a_1\}|=2$, and $B_j\subseteq B_{j+1}$. We claim that if $B_j=B_{j+1}$ for some $j<s-1$, then B_j contains the cyclic subgroup of Z_s generated by a_{j+1}. Indeed, if $B_j=B_{j+1}$ then $a_{j+1}\in B_j$ and for every $b\in B_j$ the element $b+a_{j+1}$ belongs to $B_{j+1}=B_j$ as well, establishing the claim. Since the elements $\{ip^{k-1}|1\leqq i\leqq p-1\}$ belong to every subgroup of Z_s, the desired result follows in case $B_j=B_{j+1}$ for some j. Otherwise $2=|B_1|<|B_2|<\ldots<|B_{s-1}|\leqq s$ and hence $|B_{s-1}|=s$, i.e., $B_s=Z_s$ and every element of Z_s is a sum $\sum_{i=1}^{s-1}\varepsilon_i a_i$ for some $\varepsilon_i\in\{0, 1\}$. This completes the proof. ∎

Lemma 4.3. *Suppose $\varepsilon>0$, $n>n(\varepsilon)$, $s\leqq 3\log n$ and $A\subseteq N$ is a set of cardinality $|A|\geqq[n/s]$. Then there is an integer q, $q\leqq s$ such that every integer m satisfying*

$$n^{5/3+\varepsilon}\leqq m\leqq n^2/20\log^2 n$$

and $m\equiv 0(\bmod q)$ belongs to A^*, and is, in fact, in $\{a\in A|a\equiv 0(\bmod q)\}^*$.

Proof. Apply Lemma 3.4 to A to get G, t and q satisfying the conclusions of the Lemma. Clearly here

$$t\geqq\frac{n}{s}-n^{2/3}>\frac{n}{s+1}.$$

Hence $q\leqq s$. Also $S\geqq 1+\ldots+[n/2]>n^2/19\log^2 n$ and

$$\frac{n^{2/3+\varepsilon}}{t}\cdot S+n^{4/3}\log n\leqq 2n^{5/3+\varepsilon}.$$

Hence the result follows from Lemma 3.4. ∎

Proof of Theorem 1.2. Put $s=snd(m)$ and suppose $A\subset N$, $|A|\geqq[n/s]+s-1$. In view of Lemma 4.1 it suffices to show that $m\in A^*$. Since $m\leqq n^2/(20\log^2 n)$, $s\leqq 3\log n$ (for sufficiently large n). By Lemma 4.3 there is an integer k, $k\leqq s$ so that every number congruent to 0 modulo k in the range $[2n^{5/3+\varepsilon}\cdot(n^2/20\log^2 n)]$ is in A^*. If $k<s$, then $k|m$, as s is the smallest non-divisor of m, and hence $m\in A^*$, as needed. It remains to check the case $k=s$. Clearly $s=p^k$ is a prime power and $m\equiv ip^{k-1}\cdot\cdot(\bmod s)$ for some $1\leqq i\leqq p-1$. Also, since $|A|\geqq[n/s]+s-1$ there are $s-1$ distinct elements $a_1, \ldots, a_{s-1}$ in A such that $a_i\not\equiv 0(\bmod s)$. By Lemma 4.2 there are $\varepsilon_i\in\{0, 1\}$ such that $m'=m-\sum_{i=1}^{s-1}\varepsilon_i a_i\equiv 0(\bmod s)$. As $m'\in\{a\in A|a\equiv 0(\bmod s)\}^*$ since $2n^{5/3+\varepsilon}\leqq m'\leqq n^2/(20\log^2 n)$ and $m'\equiv 0(\bmod k)$, we conclude that $m\in A^*$. This completes the proof. ∎

5. Concluding Remarks

Proposition 1.3 can be used to prove various other results, besides the estimates given in Proposition 1.1 and the proof of Theorem 1.2. For example, it can be used to prove the following two results of Erdős and Freiman [2], conjectured by Erdős and Freud [3]. (One can easily check that both results follow, up to an additive error of 2, from Theorem 1.2).

Proposition 5.1 (see [2]). *If* $n=3x-3$ *is sufficiently large, then for any subset* A *of cardinality* x *of* $N=\{1, 2, ..., n\}$, A^* *contains a power of* 2.

Proposition 5.2 (see [2]). *If* $n>n_0$, $n=4x-4$ *and* A *is a subset of* $\{1, 2, ..., n\}$ *of cardinality* x, *then* A^* *contains a square free number.*

As the proofs of both Propositions are quite similar to that of Theorem 1.2, we omit the details.

It seems that the lower bound given for $p(n, r)$ in (1.4) is closer to the truth than the upper bound given in Propositions 1.1. In fact, we believe that $p(n, r)=$ $=(1+o(1))2^{1/(r+1)}n^{(r-1)/(r+1)}$ for every fixed $r\geqq 2$, as n tends to infinity. The most difficult case of this equality seems to be $r=2$.

References

[1] N. Alon, Subset sums, *J. Number Theory*, **27** (1987), 196—205.
[2] P. Erdős and G. Freiman, On two additive problems, *J. Number Theory, to appear.*
[3] P. Erdős, Some problems and results on combinatorial number theory, *Proc. First China Conference in Combinatorics* **(1986)**, *to appear.*
[4] E. Lipkin, On representation of r-powers by subset sums, *Acta Arithmetica, submitted.*
[5] J. Olson, An additive theorem modulo p, *J. Combinatorial Theory* **5** (1968), 45—52.
[6] E. C. Titchmarsh, *Introduction to the theory of Fourier integrals*, Oxford at the Clarendon Press, London, 1948, p. 177.

Noga Alon

School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv
Israel

Gregory Freiman

School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv
Israel