On a problem of Konyagin

by

TOMASZ ŁUCZAK and TOMASZ SCHOEN (Poznań)

1. Introduction. For a subset $A$ of an abelian group $G$ and $t \in G$, let $\nu(t) = \nu_A(t)$ count the number of ways we can represent $t$ as a sum of two elements from $A$, i.e.,

$$\nu(t) = |\{(a, b) \in A \times A : t = a + b\}|$$

(note that if $a \neq b$, then we view $t = a + b$ and $t = b + a$ as two different representations of $t$). We also set $\nu(A) = \min_{t \in A + A} \nu(t)$. Clearly, if $A$ is a finite subset of integers, then $\nu(A) = 1$, since for the element $s = 2 \max A$ we have $\nu(s) = 1$. On the other hand, for a finite subgroup $H$, we have $\nu(H) = |H|$. Is it possible that $\nu(A)$ is large also for sparse subsets $A$ of $\mathbb{Z}/p\mathbb{Z}$, i.e., are there sparse subsets of $\mathbb{Z}/p\mathbb{Z}$ which are “similar” to subgroups? Straus [6] constructed sparse subsets $A$ of $\mathbb{Z}/p\mathbb{Z}$, with $|A| = O(\log p)$, for which $\nu(A) = 2$ (see Section 3 below). Konyagin (see [3, Problem 5]) made the above “subgroup approximation problem” more specific and asked if there exist constants $\varepsilon, C > 0$ such that for every sufficiently large $p$ and each set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| < \sqrt{p}$, we have $\nu(A) \leq C|A|^{1-\varepsilon}$.

The goal of this note is to provide an upper bound for $\nu(A)$. Our main result, Theorem 1 below, gives a fair estimate of $\nu(A)$ for sparse sets $A \subseteq \mathbb{Z}/p\mathbb{Z}$. On the other hand, since our argument is based on Dirichlet’s approximation theorem, the upper bound for $\nu(A)$ we obtain is useful only for sets $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = p^{o(1)}$, so we are still far from settling Konyagin’s conjecture.

**Theorem 1.** Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$. If for some integer $d \geq 3$, and $K \geq 2^{d^2}$, we have

$$2^{2d+2}K^{2^{d+3}/d} \leq |A| \leq \frac{p^{2-d-1}K^{-3/d}}{2^{d+2}K},$$

then $\nu(A) < |A|/K$.

---

2000 Mathematics Subject Classification: Primary 11B34; Secondary 11B75.

Key words and phrases: sumsets, representation function.

The first and second authors partially supported by KBN grants 1 P03A 025 27 and 1 P03A 029 30, respectively.
Since the statement of Theorem 1 is somewhat technical, we state one of its consequences in a slightly more accessible form.

**Corollary.** For every $\varepsilon$, $0 < \varepsilon < 1$, there exists a constant $a_0$ such that for every $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with
\[ a_0 \leq |A| \leq 2^{(\log_2 p)^{1/5}}, \]
we have
\[ \nu(A) \leq |A|2^{-(1-\varepsilon)(\log_2 \log_2 |A|)^2}. \]

We also remark that results of Green and Ruzsa [2] imply that
\[ \nu(A) \leq \max\{1, |A|^{(\log_2 p)^{1/2 + o(1)}}\}, \]
for every $A \subseteq \mathbb{Z}/p\mathbb{Z}$, $|A| \leq \sqrt{p}$. For much sparser sets $A$ this fact follows immediately from Dirichlet’s approximation theorem and a “gap argument” used in the proof of Theorem 1 below. However, in the next section, we prove a result related to an additive lemma of Plünnecke and Ruzsa (Lemma 2) which leads to a better bound for $\nu(A)$. Then we give the proof of Theorem 1. Finally, in the last section, we supplement our results with an example of a sparse sets $A$ with (moderately) large $\nu(A)$.

2. **Proof of the main result.** Let us first recall the following result of Plünnecke and Ruzsa (see, for instance, Nathanson [4, Theorem 7.6]).

**Lemma 1.** Let $C$, $D$ be finite subsets of an abelian group. If $|C + D| \leq K|D|$, then for every $k \geq 1$,
\[ |kC| \leq K^k|D|. \]

Our first lemma states that if $\nu(A)$ is large, then we can find in $A$ dense subsets whose sumset is smaller than anticipated in Lemma 1. This result is somewhat similar to Lemma 2.7 of Green and Ruzsa [2] from which it follows that, basically, if $k \geq K$, then in (3) one can replace $K^k$ by $K^{k/\log_2 k}$. However, in the proof of Theorem 1, we use (3) with $k = 2^{\Theta(\sqrt{\log_2 K})}$, which is much smaller than $K$.

**Lemma 2.** Let $A$ be a finite subset of an abelian group and suppose that $\nu(A) \geq |A|/K$. Then, for each integer $d \geq 3$, there are subsets $A_1, \ldots, A_{2d}$ of $A$ such that $|A_j| \geq |A|/K$ for $j = 1, \ldots, 2d$, and
\[ |A_1 + \cdots + A_{2d}| \leq K^{2d+2/d-1}|A|. \]

**Proof.** Note that we can assume that
\[ |2^d A| > K^{2d+2/d-1}|A|, \]
since otherwise the assertion holds for $A_j = A$, $j = 1, \ldots, 2^d$. 


Let us consider the sequence of sumsets \( A, 2A, \ldots, 2^dA \), and for \( i \geq 1 \) set 
\[ \nu_i(t) = |\{(a, b) \in 2^{i-1}A \times 2^{i-1}A : t = a + b\}|. \]
We claim that for some \( i_0, 1 \leq i_0 \leq d \), we have
\[ \min_{t \in 2^iA} \nu_i(t) \leq K^{2^{i_0}/d-1}|A|. \]
Indeed, suppose that (5) does not hold, i.e., for every \( 1 \leq i \leq d \) we have
\[ \min_{t \in 2^iA} \nu_i(t) > K^{2^i/d-1}|A|. \]
We show that then, for \( 1 \leq i \leq d \),
\[ |2^iA| > K^{(d-i+4)2^i/d-1}|A|. \]
We prove (7) by a (backward) induction. For \( i = d \) the inequality (7) becomes (4). If (7) holds for \( i, 1 \leq i \leq d \), then, from (6) and the induction hypothesis,
\[ |2^{i-1}A|^2 = \sum_t \nu_t(t) > |2^iA|K^{2^i/d-1}|A| > K^{(d-(i-1)+4)2^i/d-2}|A|^2. \]
Thus, (7) holds for all \( i, 1 \leq i \leq d \). In particular, when \( i = 1 \), we have
\[ |2A| > K^{(d+3)/2-d-1}|A| = K^{1+6/d}|A|, \]
which contradicts the fact that
\[ |2A| \leq \nu(A) \leq K|A|. \]
Consequently, (5) holds, and for some \( i_0 \geq 1 \) and \( t_0 \in 2^{i_0}A \) we have
\[ \nu_{i_0}(t_0) \leq K^{2^{i_0}/d-1}|A|. \]
Take any two elements \( a, b \in 2^{i_0-1}A \) with \( t_0 = a + b \). Then \( a = a_1 + \cdots + a_{2^{i_0}-1} \) and \( b = b_1 + \cdots + b_{2^{i_0}-1} \) for some \( a_1, \ldots, a_{2^{i_0}-1}, b_1, \ldots, b_{2^{i_0}-1} \in A \). Set \( c_j = a_j + b_j, A_j = A \cap (c_j - A) \), and observe that \( |A_j| = \nu(c_j) \geq |A|/K \). Then
\[ t_0 = (a_1 + \cdots + a_{2^{i_0}-1}) + (b_1 + \cdots + b_{2^{i_0}-1}), \]
and for any choice of elements \( a_1 \in A_1, \ldots, a_{2^{i_0}-1} \in A_{2^{i_0}-1} \) we can find other elements \( b_1 \in A_1, \ldots, b_{2^{i_0}-1} \in A_{2^{i_0}-1} \) satisfying (8). Thus, there are at least \( |A_1 + \cdots + A_{2^{i_0}-1}| \) elements \( a \in 2^{i_0-1}A \) such that \( t_0 = a + b \) for some \( b \in 2^{i_0-1}A \), which yields
\[ |A_1 + \cdots + A_{2^{i_0}-1}| \leq \nu_{i_0}(t_0) \leq K^{2^{i_0}/d-1}|A|. \]
By Lemma 1 applied with \( C = A_1 + \cdots + A_{2^{i_0}-1-1}, D = A_{2^{i_0}-1} \), we get
\[ |kA_1 + \cdots + kA_{2^{i_0-1}-1}| \leq K^{k2^{i_0}/d-1}|A|. \]
In particular, for \( k = 2^{d-i_0+2}, \) we have
\[ |2^{d-i_0+2}A_1 + \cdots + 2^{d-i_0+2}A_{2^{i_0-1}-1}| \leq K^{2^{d+2}/d-1}|A|, \]
which completes the proof of Lemma 2.  \( \blacksquare \)
Our proof of Theorem 1 relies on the following consequence of Lemma 2.

**Lemma 3.** Let $d \geq 3$, $s = 2^d$, $K \geq 2^d$, and $A \subseteq \mathbb{Z}/p\mathbb{Z}$ be such that $|A| \geq 4s^2K^{8s/d}$, and $\nu(A) \geq |A|/K$. Then there exist subsets $R_1, \ldots, R_{2s-1}$ of $A$ with at most $\ell = \lfloor K^{3/d} \rfloor$ elements each, such that

$$|A \cap (R_1 + \cdots + R_s - R_{s+1} - \cdots - R_{2s-1})| > \frac{1}{4} K^{s/d} > 2K^2.$$  

**Proof.** Let $A_1, \ldots, A_s$ be the sets given by Lemma 2. We may and will assume that $|A_i| = |A|/K$ for all $i = 1, \ldots, s$. Denote by $r(t)$ the number of representations $t = a_1 + \cdots + a_s$, $a_i \in A_i$. Let $R_i$, $R_{s+i} \subseteq A_i$, $i = 1, \ldots, s$, be sets chosen independently at random from the family of all subsets of $A_i$ with $\ell$ elements. We denote by $U$ the set of $(2s - 1)$-tuples $(c_1, \ldots, c_{2s-1})$ such that $c_i \in R_i$, $i = 1, \ldots, 2s - 1$, all elements $c_i$ are different, and

$$c_1 + \cdots + c_s - c_{s+1} - \cdots - c_{2s-1} \in A_s \subseteq A.$$

Moreover, let $X = |U|$. In order to estimate the expectation of the random variable $X$ note that the number of solutions to

$$a_1 + \cdots + a_s = b_1 + \cdots + b_s, \quad a_i, b_i \in A_i,$$

is equal to $\sum_t r^2(t)$. By Lemma 2 and the Cauchy–Schwarz inequality we have

$$\sum_t r^2(t) \geq \frac{(\sum_t r(t))^2}{|A_1 + \cdots + A_s|} = \frac{|A|/K)^{2s}}{K^{4s/d-1}|A|} = K^{-4s/d} \left( \frac{|A|}{K} \right)^{2s-1}. $$

Furthermore, if we denote by $\overline{r}(a)$ the number of representations

$$a = a_1 + \cdots + a_s - a_{s+1} - \cdots - a_{2s-1}, \quad a_i, a_{i+s} \in A_i, \quad 1 \leq i \leq s,$$

such that $a_m \neq a_n$ for $1 \leq m < n \leq 2s - 1$, then (10) and the fact that $|A| \geq 4s^2K^{8s/d}$ imply that

$$\sum_{a \in A_s} \overline{r}(a) \geq \sum_t r^2(t) - \binom{2s - 1}{2} \left( \frac{|A|}{K} \right)^{2s-2} \geq \frac{1}{2} K^{-4s/d} \left( \frac{|A|}{K} \right)^{2s-1}. $$

Then

$$\mathbb{E}X = \sum_{a \in A_s} \overline{r}(a) \left( \frac{\ell K}{|A|} \right)^{2s-1} \geq \frac{1}{2} K^{-4s/d} \ell^{2s-1} > \frac{1}{2} K^{s/d} > 4K^2.$$

Now let $Y$ denote the number of pairs of distinct $(2s - 1)$-tuples $(c_1, \ldots, c_{2s-1}), (c_1', \ldots, c_{2s-1}')$ from $U$ such that

$$c_1 + \cdots + c_s - c_{s+1} - \cdots - c_{2s-1} = c_1' + \cdots + c_s' - c_{s+1}' - \cdots - c_{2s-1}'.$$ 

Then, for the expectation of $Y$, we have

$$\mathbb{E}Y \leq \sum_{a \in A_s} \overline{r}(a) \sum_{j=0}^{2s-3} \binom{2s-1}{j} \left( \frac{|A|}{K} \right)^{2s-2-j} \left( \frac{\ell K}{|A|/K} \right)^j \left( \frac{\ell}{2} \right)^{2s-1-j}.$$
Indeed, to estimate $EY$ we choose first the sum on the left hand side of (13) (so we sum over $a \in A_s$) and select the terms of the sum on the left hand side, which gives the factor of $\varpi(a)$. In order to bound the number of choices of the terms on the right hand side of (13), denote by $j$ the number of indices $i$, $i = 1, \ldots, 2s-1$, such that $c_i = c'_i$. The number of ways we can choose all but one $2s-1-j$ terms $c'_i$ which are different from $c_i$ is very crudely estimated by $((|A|/K)^{2s-1-j}$. Finally, the probability that a randomly chosen pair of distinct $(2s-1)$-tuples for which (13) holds is identical with the one we have just selected can be bounded from above by $(\ell K/A)^j$ (the probability of choosing $j$ elements which are the same on both sides) multiplied by $(\ell K/(|A|/K))^{2j-1-j}$ (the probability of choosing $2j-1-j$ pairs of different elements).

Thus, using (11) and the fact that $K \geq s^d$ and $|A| \geq 4s^2K^{8s/d}$, we get

$$EY \leq \sum_{a \in A_s} \varpi(a) \left( \ell K \right)^{2s-1} \left( \frac{|A|/K}{|A|/K-1} \right)^{2s-1} \frac{K}{|A|} \sum_{j=0}^{2s-3} \left( \frac{2s-1}{j} \right) \left( \frac{\ell K}{|A|} \right)^j \leq \exp \left( \frac{3sK}{|A|} \right) \frac{K (1+\ell)^{2s-1}}{|A|} E \leq 2e^{s/\ell} \frac{K \ell^{2s-1}}{|A|} E \leq \frac{E X}{2}.$$ 

Consequently, $E(X - Y) > \frac{1}{4} K^{s/d} > 2K^2$, and so there exists a choice of sets $R_1, \ldots, R_{2s-1}$ for which (9) holds.

**Proof of Theorem 1.** Let us recall that for $\alpha \in \mathbb{R},$

$$\|\alpha\| = \min_{n \in \mathbb{Z}} |\alpha - n|.$$ 

Let $R_1, \ldots, R_{2s-1}, s=2^d$, be the sets whose existence is ensured by Lemma 3, $R = \bigcup_i R_i$, and $F = A \cap (R_1 + \cdots + R_s - R_{s+1} - \cdots - R_{2s-1})$. Since $|R| \leq 2sK^{3/d}$, by Dirichlet’s approximation theorem there is $u, 1 \leq u \leq p$, such that for every $c \in R$, we have

$$\|uc/p\| \leq p^{-1/|R|} \leq p^{-1/(2sK^{3/d})}.$$ 

Thus, by (1), for every $a \in F, a = c_1 + \cdots + c_s - c_{s+1} - \cdots - c_{2s-1},$

$$\|ua/p\| \leq \|uc_1/p\| + \cdots + \|uc_{2s-1}/p\| \leq 2sp^{-1/(2sK^{3/d})} \leq 1/(2K|A|).$$

Since, obviously, for every $u \in \mathbb{Z}/p\mathbb{Z}$ and $B = \{u \cdot a : a \in A\}$, we have $|A| = |B|$ and $\nu(A) = \nu(B)$, without loss of generality we can assume that $u = 1$. Thus, for every $a \in F$, we have either

$$0 \leq a \leq \frac{p}{2K|A|},$$

or

$$p - \frac{p}{2K|A|} \leq a < p.$$
Let us suppose that for the set $F'$ of all elements of $F$ which satisfy (14) we have $|F'| \geq |F|/2 > K^2$ (the case when (15) holds more often than (14) can be dealt with by a similar argument).

Now let us make the following elementary observation. The set $A + A$ clearly contains a gap of length at least $p/|A + A| - 1 \geq p/(2K|A|)$. The existence of such a gap implies that there are at least $|A|/K$ gaps of at least the same length in the set $A$. Indeed, if $t \in A + A$ and

$$\{t + 1, \ldots, t + L\} \cap (A + A) = \emptyset,$$

then for every $a \in A$ such that $a + b = t$ we have

$$\{a + 1, \ldots, a + L\} \cap A = \emptyset.$$

Thus, let $H$ be the set of all $a \in A$ such that $\{a + 1, \ldots, a + 2d|A|\} \cap A = \emptyset$. Then

$$|A + A| \geq |H + F'| = |H||F'| > \frac{|A|}{K} K^2 = K|A|,$$

while

$$|A + A| \leq \frac{|A|^2}{\nu(A)} \leq K|A|.$$

This contradiction completes the proof of Theorem 1.

Proof of Corollary. We apply Theorem 1 with $d = \sqrt{1 - \varepsilon} \log_2 \log_2 |A|$ and $K = 2^d$, where, to simplify calculations, we assume that $\varepsilon$ is chosen in such a way that $d$ is an integer. Then

$$\log_2(2^{2d+2}K^{2d+3}/d) = 2d + 2 + d2^{d+3} \leq d2^d \leq \log_2 |A|,$$

provided $|A|$ is large enough, i.e., the left inequality in (1) holds. Moreover,

$$\log_2 \left( \frac{p^{2d-1}K^{-3/d}}{2d+2K} \right) = 2^{4d-1} \log_2 p - d - 2 - d^2 \geq \frac{\log_2 p}{2(\log_2 |A|)^{4\sqrt{1-\varepsilon}}} - 2(\log_2 |A|)^2 \geq \log_2 |A|,$$

so the right inequality in (1) holds as well. Consequently, $\nu(A) \leq |A|2^{-d^2}$ and the assertion follows.

Let us make a few comments on the proof of Theorem 1. Our argument is based on the fact that, using Dirichlet’s approximation theorem, we can “compress” the set $F$ so it can be put into large gaps which must exist in $A$. Basically the same proof would work if we could find in $A$ large subsets which depend on a small number of parameters as, for instance, dense subsets of long arithmetic progressions, or large cubes (i.e., the sets of the form $x + \{0, x_1\} + \cdots + \{0, x_d\}$ with many distinct sums). For example, for every set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A + A| \leq K|A|$, by Ruzsa’s theorem (see [5] or Lemma 7.4.
in [4]), we have $|A - A| \leq K^2|A|$. For such sets $A$ it was shown by Croot, Ruzsa, and Schoen (see Theorem 4 in [1]) that the set $A + A$ contains an arithmetic progression of length at least $L = \log_2 |A|/(4 \log_2 K)$. This result immediately implies that whenever $|A + A| \leq K|A|$ and $K^6|A| \leq p/\log_2 p$, we have

$$\nu(A) \leq |A|((\log_2 |A|)^{-1/5+o(1)}.$$  

Indeed, it is easy to observe that $\nu(A + A) \geq \nu(A) \geq |A|/K$ and from the Plünnecke–Ruzsa theorem it follows that $|4A| \leq K^4|A|$, so in any dilation of $4A$ there is a gap of size at least

$$\frac{p}{K^4|A| + 1} > \frac{\log_2 |A|}{4 \log_2 K},$$

which generates at least $|A|/K$ gaps of the same size in $2A$. On the other hand, every arithmetic progression of length $L$ can be compressed to the interval of the same length. Thus, we have

$$\frac{|A| \log_2 |A|}{K^4 |A|} \leq K^4 |A|$$

and (17) follows. This estimate is, of course, even weaker than the bound given in (2), but since the assumption $\nu(A) \geq |A|/K$ is stronger than $|A + A| \leq K|A|$, there is at least some hope that Konyagin’s conjecture can be shown using a similar technique. Such an approach looks even more promising if we observe that to improve bounds given by Theorem 1 it is enough to find a “large easily compressible subset” which shares a lot of elements with sets of type $A + A + A$, which are “much more structured” than $A$ itself. Indeed, if $\nu(A)$ is large, then the sets $A + A, A + A + A$, or, say, $8A$, are not much denser than $A$, and have large values of $\nu(\cdot)$ as well. Hence, one way to verify Konyagin’s conjecture would be, for instance, to show that if $\nu(A) \geq |A|^{1-\varepsilon}$, then the set $A + A + A + A$ shares a lot of elements with some large cube.

Finally, let us note that the elementary gap argument presented above shows that sets $A \subseteq \mathbb{Z}/p\mathbb{Z}$ for which $\nu(A) \geq |A|/K$ for small $K$, have rather special properties. For instance, each such set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ contains at least $|A|^2/K$ arithmetic progressions of length three (since for each $a \in A$ we have $\nu(2a) \geq |A|/K$) but no arithmetic progressions $P$ longer than $K^2$. Indeed, in this case we could transform $P$ into $v + u \cdot P = \{0, 1, \ldots, |P| - 1\}$, which would fit in into the gaps of $v + u \cdot A$, contradicting (16). In a similar way, $A + A$ cannot contain arithmetic progressions of length $K^4$, $A + A + A$ contains no arithmetic progressions of length $K^5$ and so on.

3. **Small sets $A$ with large $\nu(A)$**. In [6] Straus presented an example of a set $S \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $\nu(S) \geq 2$, and $|S| \geq \gamma_p \log_2 p$ for some constant
Since there are at least $\gamma_p \leq 2$ which tends to $2/\log_2 3$ as $p \to \infty$. In this section we show how to use this example to construct a sparse set $A$ with $\nu(A)$ larger than two.

We start with the following two observations.

**Lemma 4.** Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be non-empty sets and suppose that $|A| |B| < \sqrt{p}$. Then there exists $x_0 \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ such that $|A + x_0 B| = |A| |B|$.  

**Proof.** Let $\nu(x; t)$ denote the number of pairs $(a, b)$, $a \in A$, $b \in B$, so that $t$ can be represented as $t = a + bx$ with $a \in A$, $b \in B$. Then, clearly, $\nu^2(x; t)$ counts quadruplets $(a', b', a'', b'')$ such that $a' + b'x = a'' + b''x$, where $a', a'' \in A$ and $b', b'' \in B$. For fixed $a', a'' \in A$ and $b', b'' \in B$, we consider the number of $x$'s, where $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, for which

$$a' - a'' = (b' - b'')x. \tag{18}$$

Clearly, if $a \neq a'$ and $b \neq b'$, then (18) has one solution; if both $a' = a''$, $b' = b''$, then we have $p - 1$ such solutions; while when just one of the equalities $a = a'$, $b = b'$ holds, the equation (18) has no non-zero solutions at all. Thus, the total number of solutions to $a' + b'x = a'' + b''x$, where $a', a'' \in A$, $b', b'' \in B$ and $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, is equal to

$$\sum_{t} \sum_{x=1}^{p-1} \nu^2(x; t) = |A|(|A| - 1)|B|(|B| - 1) + (p - 1)|A| |B|. \quad \text{Hence, for some } x_0 \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\},$$

$$\sum_{t} \nu^2(x_0; t) \leq \frac{1}{p - 1} |A|(|A| - 1)|B|(|B| - 1) + |A| |B| < 1 + |A| |B|,$$

so that there are only trivial solutions to $a' + b'x_0 = a'' + b''x_0$. Consequently,

$$|A + x_0 B| = |A| |B|. \quad \blacksquare$$

**Lemma 5.** Let $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ be such that $|A + B| = |A| |B|$. Then, for $C = A + B$, we have $\nu(C) \geq \nu(A)\nu(B)$.  

**Proof.** Let $t \in C + C$, i.e., $t = c + c'$ for some $c, c' \in C$. Since $c = a + b$ and $c' = a' + b'$ for some $a, a' \in A$ and $b, b' \in B$, we have

$$c + c' = (a + b) + (a' + b') = (a + a') + (b + b').$$

Note that each representation $a + a' = a_1 + a_2$, $b + b' = b_1 + b_2$, where $a_1, a_2 \in A$, $b_1, b_2 \in B$, yields a different representation of $c + c'$. Indeed,

$$c + c' = (a + b) + (a' + b') = (a + a') + (b + b') = (a_1 + a_2) + (b_1 + b_2) = (a_1 + b_1) + (a_2 + b_2),$$

and from $|A + B| = |A| |B|$ it follows that all representations are distinct. Since there are at least $\nu(A) \nu(B)$ ways to write $a + a' = a_1 + a_2$, $b + b' = b_1 + b_2$, we get $\nu(C) \geq \nu(A)\nu(B). \quad \blacksquare$
Theorem 2. For every positive integer $Q < \log_2 p / (2 \log_2 (\gamma_p \log_2 p))$, where $\gamma_p$ is the constant given in Straus’ construction, there exists a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $|A| = (\gamma_p \log_2 p)^Q$ and $\nu(A) \geq 2^Q$.

Proof. Let $S$ be the set constructed by Straus. From Lemmas 4 and 5, it follows that for every $Q$ satisfying $|S|^Q < \sqrt{p}$ there is a set $A$ of the form $A = S + x_1 \cdot S + \cdots + x_{Q-1} \cdot S$, for some $x_1, \ldots, x_{Q-1} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, such that $|A| = |S|^Q$ and $\nu(A) \geq \nu(S)^Q \geq 2^Q$.  

References


Faculty of Mathematics and Computer Science
Adam Mickiewicz University
Umultowska 87
61-614 Poznań, Poland
E-mail: tomasz@amu.edu.pl
schoen@amu.edu.pl

Received on 1.3.2007
and in revised form on 7.5.2008 (5400)