A note on additive bases of integers

By I. Z. RUZSA,*) (Budapest) and S. TURJÁNYI (Debrecen)

1. Introduction

As usual, if A and B are sets of integers, we write

$$A \pm B = \{a \pm b\colon\ a \in A,\ b \in B\}$$

and we apply kA to denote $A+A+\dots+A$ (k times). We use $A(x), B(x), \dots$ to denote the number of elements of $A, B, \dots$ below x, and $A_k(x), \dots$ for the number of elements of kA below x.

A set of natural numbers is a *basis* of order h if every sufficiently large integer is the sum of at most h elements of A. (From our point of view it makes no difference whether we require all the integers to be in hA or we permit a finite number of exceptions.) P. ERDŐS and R. L. GRAHAM (1980) conjectured that if A is a basis and $A(x)= =o(x)$, then $A_2(x)/A(x)\to\infty$. One of the authors disproved this (TURJÁNYI (1981)) by constructing for every $k\geqq 4$ a basis of order k such that

$$\liminf A_2(x)/A(x) < \infty.$$

In section 2 we generalize this counterexample. In section 3 we present a modified form of the Erdős—Graham conjecture that has more chance to be true and in the remainder of the paper we prove a partial result.

2. An example

Here we prove our

Theorem 1. *For every* $h\geqq 3$ *there exists a basis* A *of order* h *such that* $A(x)= =o(x)$ *and* $\liminf A_{h-1}(x)/A(x)<\infty$.

PROOF. Let B be a basis of order h satisfying $B(x)=o(x^{1/h})$ (cf. e.g. OSTMANN (1969) or HALBERSTAM—ROTH (1966)). Let d_n be a sufficiently quickly increasing

*) Paper finished when author was visiting the University of Ulm with a stipendium of the A. v. Humboldt-Stiftung.

sequence and

$$d_n' = d_n - d_n^r;$$

the number $r \in (0, 1)$ and the necessary rate of increase of d_n will be specified later.

We put

$$A = B \cup \bigcup_{n=1}^{\infty} [d_n', d_n]$$

where by $[a, b]$ now we mean the set of integers between the limits a and b. Clearly

$$A(d_n) \geqq d_n^r. \tag{1}$$

We estimate $A_{h-1}(d_n)$ from above. Obviously

$$A_{h-1}(d_n) \leqq d_n^r + A_{h-1}(d_n') \leqq d_n^r + (A(d_n'))^{h-1} \leqq d_n^r + (d_{n-1} + B(d_n))^{h-1} \ll d_n^r$$

assuming

$$d_n > d_{n-1}^{(h-1)/r}$$

and $r > 1 - 1/h$. Choosing r and d_n according to these requirements we obtain the desired example.

3. A more probable conjecture

Observe that in the previous example the following happened: $A(x)$ grew suddenly in a short interval, but the sum of two numbers near to x being near to $2x$, $A_2(x)$ began to grow only much later. This motivates the

Conjecture 1. If A is a basis and $A(x) = o(x)$, then $A_2(2x)/A(x) \to \infty$. We prove something more modest.

Theorem 2. *If A is a basis and $A(x) = o(x)$, then $A_3(3x)/A(x) \to \infty$.*

We shall deduce Theorem 2 from

Theorem 3. *If X is any finite set of integers, $|X| = n$ and $|3X| = sn$, then for every k we have $|kX| \leqq s^k n$.*

In a similar way we could deduce Conjecture 1 from

Conjecture 2. If X is any finite set of integers, $|X| = n$ and $|2X| = sn$, then for every k

$$|kX| \leqq f(s, k) n,$$

with a number $f(s, k)$ depending only on c and k.

Probably Conjecture 2 and hence Conjecture 1 can be deduced from Freiman's deep main theorem (1966) with

$$f(s, k) = \exp cks.$$

We do not pursue this further since we think that the real order of $f(s, k)$ is something like s^{ck}.

4. Proof of Theorem 3

This is based on the following inequality of Ruzsa (1976): for arbitrary sets X, Y, Z of integers we have

$$|X||Y-Z| \leqq |X-Y||X-Z|. \tag{2}$$

Write

$$|kX-lX| = q(k, l)|X|, \quad q(3, 0) = s,$$

and substitute $Y=-(X+X)$, $Z=kX-lX$ into (2). We obtain

$$q(k, l+2) \leqq sq(k+1, l). \tag{3}$$

Choosing $k=2$, $l=0$ we obtain

$$q(2, 2) \leqq s^2. \tag{4}$$

Now we prove

$$q(k, l) \leqq s^{k+l} \tag{5}$$

for all k, l. Suppose this is wrong; consider a counterexample to (5) with the minimal $k+l$. If $l \geqq 2$, then we have by (3)

$$q(k, l) \leqq sq(k+1, l-2) \leqq s^{k+l}.$$

The same argument works if $k \geqq 2$ (since $q(k, l)=q(l, k)$). Finally if $k<2$ and $1<2$, then (5) follows from (4).

Theorem 3 is just the case $l=0$ of (5).

5. Proof of Theorem 2

Consider the set $X=A\cap[1, x]$. Clearly

$$|X| = A(x), \quad |3X| \leqq A_3(3x),$$

and if A is a basis of order h, then

$$|hX| \geqq x-c$$

with a constant c depending on X but independent of x. Theorem 3 yields

$$x-c \leqq |hX| \leqq \left(\frac{|3X|}{|X|}\right)^h |X| \leqq A(x)\left(\frac{A_3(3x)}{A(x)}\right)^h,$$

hence

$$\frac{A_3(3x)}{A(x)} \geqq \left(\frac{x-c}{A(x)}\right) \to \infty, \quad \text{qu.e.d.}$$

References

P. ERDŐS, R. L. GRAHAM, On bases with an exact order, *Acta Arithmetica* **37** (1980), 201—207.
G. A. FREIMAN (1966), The foundations of the structural theory of addition of sets, *Kazan (In Russian;* Enlish translation in the AMS Translations of math. monograps ser.)
H. HALBERSTAM, K. F. ROTH (1966), Sequences, vol. 1, *Oxford Univ. Press.*
H. H. OSTMANN (1969), Additive Zahlentheorie, *Springer-Verlag, Berlin.*
I. Z. RUZSA (1976), On the cardinality of $A+A$ and $A-A$, *Coll. Math. Soc. Bolyai* **18**. Combinatorics, *Keszthely*.
S. TURJÁNYI (1981), A note on basis sequences, *Coll. Math. Soc. Bolyai*, Number Theory, *Budapest*.

(Received November 28, 1983.)

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST

MATHEMATICAL INSTITUTE OF THE
"KOSSUTH LAJOS" UNIVERSITY, DEBRECEN