

On bases with an exact order

by

P. ERDÖS (Budapest) and R. L. GRAHAM (Murray Hill, N. J.)

Introduction. A set A of nonnegative integers is said to be an (*asymptotic*) *basis of order r* if every sufficiently large integer can be expressed as a sum of at most r integers taken from A (where repetition is allowed) and r is the least integer with this property. In this case we write $\text{ord}(A) = r$. A basis A is said to have *exact order s* if every sufficiently large integer is the sum of *exactly* s elements taken from A (again, allowing repetition) where s is the least integer with this property. We indicate this by writing $\text{ord}^*(A) = s$.

It is easy to find examples of bases A which do not have an exact order, e.g., the set of positive odd integers. Of course, if $0 \in A$ and $\text{ord}(A) = r$ then $\text{ord}^*(A) = r$ as well. However, it is not difficult to construct examples of bases A for which

$$\text{ord}^*(A) > \text{ord}(A).$$

For example, the set B defined by

$$B = \bigcup_{k=0}^{\infty} I_k$$

where

$$I_k = \{x: 2^{2k} + 1 \leq x \leq 2^{2k+1}\}$$

has

$$\text{ord}(B) = 2 \quad \text{and} \quad \text{ord}^*(B) = 3.$$

In this note we characterize those bases A which have an exact order. It turns out that the only bases which do not have an exact order are those whose elements fail to satisfy a simple modular condition. We also estimate to within a constant factor the largest value $\text{ord}^*(A)$ can attain given that $\text{ord}(A) = r$. (The reader may consult [1] for a survey of results on bases.)

Bases with an exact order

THEOREM 1. *A basis $A = \{a_1, a_2, \dots\}$ has an exact order if and only if*

$$(*) \quad \text{g.c.d.}\{a_{k+1} - a_k : k = 1, 2, \dots\} = 1.$$

Proof. (Necessity). Suppose for some s that $\text{ord}^*(A) = s$ and assume $(*)$ does not hold, i.e.,

$$\text{g.c.d.}\{a_{k+1} - a_k : k = 1, 2, \dots\} = d > 1.$$

Thus, for all k ,

$$a_{k+1} \equiv a_k \pmod{d}.$$

Therefore, the sum of any s integers taken from A is always congruent to sa_1 modulo d which contradicts the assumption that $\text{ord}^*(A) = s$.

(Sufficiency). Denote $\text{ord}(A)$ by r and assume $(*)$ holds. Let mA denote the set

$$\{x_1 + x_2 + \dots + x_m : x_k \in A\}.$$

FACT. For some n ,

$$nA \cap (n+1)A \neq \emptyset.$$

Proof of Fact. It follows from $(*)$ that for some t ,

$$\text{g.c.d.}\{a_{k+1} - a_k : 1 \leq k \leq t\} = 1.$$

Thus, for suitable integers c_k we have

$$(1) \quad \sum_{k=1}^t c_k (a_{k+1} - a_k) = 1.$$

Define p_k and q_k by

$$p_k = \begin{cases} a_{k+1} & \text{if } c_k \geq 0, \\ a_k & \text{if } c_k < 0, \end{cases} \quad q_k = \begin{cases} a_k & \text{if } c_k \geq 0, \\ a_{k+1} & \text{if } c_k < 0. \end{cases}$$

Then (1) can be rewritten as

$$\sum_{k=1}^t |c_k| (p_k - q_k) = 1,$$

i.e.,

$$(2) \quad \sum_{k=1}^t |c_k| p_k = 1 + \sum_{k=1}^t |c_k| q_k.$$

Now consider the integer

$$M = \sum_{k=1}^t |c_k| p_k q_k.$$

Since

$$(3) \quad M = \sum_{k=1}^t \sum_{i=1}^{|c_k|p_k} q_k \in \left(\sum_{k=1}^t |c_k|p_k \right) A$$

and also

$$(4) \quad M = \sum_{k=1}^t \sum_{j=1}^{|c_k|q_k} p_k \in \left(\sum_{k=1}^t |c_k|q_k \right) A,$$

the Fact follows from (2) by taking

$$n = \sum_{k=1}^t |c_k|q_k.$$

It follows immediately from (2), (3) and (4) that

$$2M = M + M \in 2nA \cap (2n+1)A \cap (2n+2)A$$

and, more generally, that for any $w \geq 1$,

$$(5) \quad wM \in \bigcap_{k=0}^w (wn+k)A.$$

However, by hypothesis, every sufficiently large integer x belongs to $\bigcup_{i=1}^r iA$. Thus, from (5) with $w = r-1$, we have

$$(6) \quad x + (r-1)M \in ((r-1)n+r)A$$

for all sufficiently large x . This shows that A has an exact order and in fact, that

$$\text{ord}^*(A) \leq (r-1)n+r.$$

This proves Theorem 1. ■

Comparing $\text{ord}(A)$ and $\text{ord}^*(A)$. Define the function $g: \mathbf{Z}^+ \rightarrow \mathbf{Z}^+$ as follows:

$$g(r) \equiv \max \{ \text{ord}^*(A) : \text{ord}(A) = r \text{ and } A \text{ satisfies } (*) \}.$$

A crude analysis of the proof of Theorem 1 shows that $g(r)$ exists and, for example, $g(r) < cr^4$ for a suitable constant c . The following result sharpens this estimate considerably.

THEOREM 2. For all r ,

$$(7) \quad \frac{1}{4}(1+o(1))r^2 \leq g(r) \leq \frac{5}{4}(1+o(1))r^2.$$

Proof. We first prove the upper bound. Assume $\text{ord}(A) = r$. Thus, all sufficiently large x satisfy

$$(8) \quad x \in \bigcup_{k=1}^r kA.$$

From (8) it follows that for any t ,

$$(9) \quad tx \in \bigcup_{k=1}^r tkA$$

for x sufficiently large.

It also follows from (8) that for some m and some c , $1 \leq c \leq r$,

$$(10) \quad m \in cA \cap (r+1)A.$$

Thus, letting

$$\bar{d} = r+1 - c$$

we have

$$2m \in 2cA \cap (2c + \bar{d})A \cap (2c + 2\bar{d})A$$

and, more generally,

$$(11) \quad um \in \bigcap_{i=0}^u (uc + i\bar{d})A,$$

a special case being

$$(12) \quad u\bar{d}m \in \bigcap_{i=0}^{u\bar{d}} (u\bar{d}c + i\bar{d})A.$$

Setting $t = \bar{d}$ in (9), we obtain

$$(13) \quad \bar{d}x \in \bigcup_{k=1}^r \bar{d}kA$$

for all sufficiently large x . Therefore,

$$(14) \quad \bar{d}x + u\bar{d}m \in (\bar{d}r + u\bar{d}c)A$$

for all sufficiently large x provided

$$(15) \quad u\bar{d} \geq r-1$$

since for each $\bar{d}x \in \bar{d}kA$, $1 \leq k \leq r$, we also have $u\bar{d}m \in (u\bar{d}c + (r-k)\bar{d})A$. In other words, if (15) holds then all sufficiently large multiples of \bar{d} belong to $(r + uc)\bar{d}A$.

Our next task is to find a number $w = o(r^2)$ so that wA contains a complete residue system mod \bar{d} . Let $\bar{A} = \{l_1, \dots, l_s\}$ denote the set of distinct residues modulo \bar{d} which occur in A . Since A satisfies (*) by hypothesis, we can assume that a_i and l_i are labelled so that $a_i \equiv l_i \pmod{\bar{d}}$ and, for some t ,

$$(16) \quad G_1 > G_2 > \dots > G_t = 1$$

where

$$G_i \equiv \text{g.c.d.} \{l_2 - l_1, l_3 - l_2, \dots, l_{i+1} - l_i\}.$$

Since G_{i+1} divides G_i for all i , it follows at once that

$$(17) \quad t \leq \frac{\log s}{\log 2} \leq \frac{\log d}{\log 2} \leq \frac{\log r}{\log 2}.$$

Thus, for any $z \pmod d$ there exist integers $c_k = c_k(z)$ with $0 \leq c_k < d$ so that

$$(18) \quad \sum_{k=1}^t c_k(l_{k+1} - l_k) \equiv \sum_{k=1}^t c_k(a_{k+1} - a_k) \equiv z \pmod d.$$

It follows from (18) that all residue classes modulo d are in $(t+1)dA$.

Finally, using this together with (14), we see that (provided (15) holds) all sufficiently large integers belong to $d(r+uc+t+1)A$. To satisfy

(15) it is enough to take $u = \left\lceil \frac{r-1}{d} \right\rceil$.

An easy calculation (using (17)) shows that the maximum value the coefficient $d\left(r+c\left\lceil \frac{r-1}{d} \right\rceil+t+1\right)$ achieves is $(1+o(1))r^2$. Thus,

$$g(r) \leq \frac{5}{4}(1+o(1))r^2$$

which is the upper bound of (7).

To obtain the lower bound of (7), consider the following set $A_r(m)$ defined by

$$A_r(m) \equiv \{x > 0 : x \equiv i \pmod n \text{ for some } i, rm \leq i \leq (r+2)m\}$$

where $n = rm(r/2+2)$ and we assume r is even. Reduced modulo n , $A_r(m)$ is simply the interval of residues $\{rm, rm+1, \dots, rm+2m\}$.

On one hand, since

$$\frac{r}{2}(rm+2m) = \frac{r^2m}{2} + rm = \left(\frac{r}{2} + 1\right)rm$$

and

$$r(rm+2m) = n + \frac{1}{2}r(rm)$$

then all residues modulo n belong to

$$\frac{1}{2}rA_r(m) \cup (r/2+1)A_r(m) \cup \dots \cup rA_r(m)$$

and consequently

$$(19) \quad \text{ord}(A_r(m)) \leq r.$$

On the other hand, for any k , $kA_r(m)$ reduced modulo n forms an interval of length $2mk+1$. Therefore,

$$(20) \quad \text{ord}^*(A_r(m)) \geq \frac{n-1}{2m} = \frac{r^2}{4} + r - \frac{1}{2m}.$$

Taking m large, it follows from (19) and (20) that

$$g(r) \geq \frac{1}{4}(1+o(1))r^2$$

which is the lower bound of (7). This completes the proof of Theorem 2. ■

Concluding remarks. We mention here several questions related to the preceding results which we were unable to settle.

1. Show that $\lim_{r \rightarrow \infty} \frac{g(r)}{r^2}$ exists, and, if possible, determine its value.

To obtain the exact value of $g(r)$ seems very difficult. It can be shown that $g(2) = 4$. However, at present we do not even know the value of $g(3)$. (It is at least 7.)

2. For a set A , let $A_n(x)$ denote $|mA \cap \{1, \dots, x\}|$. If A is a basis and $A_1(x) = o(x)$ is it true that $\lim_{x \rightarrow \infty} \frac{A_2(x)}{A_1(x)} = \infty$?

3. By the *restricted order* of A , denoted by $\text{ord}_R(A)$, we mean the least integer t (if it exists) such that every sufficiently large integer is the sum of at most t *distinct* summands taken from A . As pointed out by Bateman, for $h \geq 3$ the set $A_h = \{x > 0: x \equiv 1 \pmod{h}\}$ has $\text{ord}(A) = h$ but has no restricted order. However, Kelly [2] has shown that $\text{ord}(A) = 2$ implies $\text{ord}_R(A) \leq 4$ and conjectures that, in fact, $\text{ord}_R(A) \leq 3$ is true.

(i) What are necessary and sufficient conditions on a basis A to have a restricted order?

(ii) Is there a function $f(r)$ such that if $\text{ord}(A) = r$ and $\text{ord}_R(A)$ exists then $\text{ord}_R(A) \leq f(r)$?

(iii) What are necessary and sufficient conditions that $\text{ord}(A) = \text{ord}_R(A)$? Even for sequences of polynomial values, the situation is not clear. For example, for the set $S_1 = \{n^2, n \geq 1\}$, $\text{ord}(S_1) = 4$ (by Lagrange's theorem): and $\text{ord}_R(S_1) = 5$ (by Pall [3]), whereas for the set $S_2 = \{(n^2 + n)/2: n \geq 1\}$,

$$\text{ord}(S_2) = \text{ord}_R(S_2) = 3.$$

(iv) Is it true that if for some r , $\text{ord}(A - F) = r$ for all finite sets F , then $\text{ord}_R(A)$ exists? What if we just assume $\text{ord}(A - F)$ exists for all finite F ?

4. Let $n \times A$ denote the set $\{a_{i_1} + \dots + a_{i_n}: a_{i_k} \text{ are distinct elements of } A\}$. Is it true that if $\text{ord}(A) = r$ then $r \times A$ has positive (lower) density?

If sA has positive upper density then $s \times A$ must also have positive upper density?

5. Given k and m , when does there exist a set $A \subseteq \mathbf{Z}_m$ so that $A, 2A, \dots, kA$ form a disjoint cover of \mathbf{Z}_m ? For example, for $k = 2$, $m = 3t - 1$, the set $A = \{t, t+1, \dots, 2t-1\}$ works.

Of course, many of the preceding questions could be formulated for $\text{ord}_R^*(A)$ (defined in the obvious way). However, we leave these for a later paper (IWL).

References

- [1] H. Halberstam and K. Roth, *Sequences*, Vol. 1, Clarendon Press, Oxford 1966.
- [2] John B. Kelly, *Restricted bases*, Amer. Journ. Math. 79 (1957), pp. 258-264.
- [3] G. Pall, *On sums of squares*, Amer. Math. Monthly 40 (1933), pp. 10-18.

MATHEMATICS INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
Budapest, Hungary
BELL LABORATORIES
Murray Hill, New Jersey, U.S.A.

Received on 11. 8. 1977

(979)
