PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 96, Number 1, January 1986

DIVISIBILITY PROPERTIES OF ADDITIVE BASES

MELVYN B. NATHANSON

ABSTRACT. Let $h \geqslant 2$. There exists an asymptotic basis A of order h such that $(a_1, \ldots, a_k) > 1$ for all $a_1, \ldots, a_k \in A$ if and only if $k < h$. If $k \geqslant h$, the sumset hA contains only composite numbers. For $h = k$, there exists a set A of nonnegative integers with $(a_1, \ldots, a_h) > 1$ for all $a_1, \ldots, a_h \in A$ such that for every prime p the sumset hA contains all sufficiently large multiples of p.

1. Introduction. Let A be a set of nonnegative integers. The *h-fold sum of A*, denoted hA, is the set consisting of all sums of h not necessarily distinct elements of A. If hA contains all sufficiently large integers, then A is an *asymptotic basis of order h*.

The set A has the property GCD(k) if the greatest common divisor of any k elements of A is strictly greater than 1. In this paper it is proved that there exists an asymptotic basis A of order h such that A satisfies GCD(k) if and only if $1 \leqslant k < h$. In particular, if A satisfies GCD(k) and $h \leqslant k$, then no prime can be represented as the sum of h elements of A. On the other hand, if $h \geqslant 2$, then there exists a set A satisfying GCD(h) such that for every prime p there exists a number $N(p)$ such that $np \in hA$ for every $n \geqslant N(p)$.

Notation. Let $[1, t]$ denote the interval of integers $1, 2, \ldots, t$. Let $|S|$ denote the cardinality of the finite set S. If $S \subseteq T$, then $T \setminus S$ denotes the relative complement of S in T. If A is a set of integers, then $A(x)$ denotes the number of positive elements of A not exceeding x. If $\mathbf{P}$ is the set of primes, then $\pi(x) = \mathbf{P}(x)$. The upper asymptotic density of the set A is $d_u(A) = \limsup_{x \to \infty} A(x)/x$. The asymptotic density of A is $d(A) = \lim_{x \to \infty} A(x)/x$, if the limit exists.

This paper originated in discussions with Gerald Myerson at the Conference on Analytic Number Theory at Oklahoma State University in June, 1984.

2. Results.

THEOREM 1. *Let $1 \leqslant k < h$. There exists an asymptotic basis A of order h such that $(a_1, a_2, \ldots, a_k) > 1$ for all $a_1, a_2, \ldots, a_k \in A$.*

PROOF. It suffices to consider only the case $h = k + 1$. Let $q_1, q_2, \ldots, q_{k+1}$ be pairwise relative prime integers greater than 1. Define $s_1, s_2, \ldots, s_{k+1}$ by $s_i =$

Received by the editors March 18, 1985.
1980 *Mathematics Subject Classification*. Primary 10L02, 10L05; Secondary 10J99, 05A05.
Key words and phrases. Density of sumsets, asymptotic bases, additive number theory, additive bases.

$\prod_{j=1, j\neq i}^{k+1} q_j$. Then

(1) $$(s_1, \ldots, s_{k+1}) = 1$$

and

(2) $$(s_1, \ldots, \hat{s}_j, \ldots, s_{k+1}) > 1$$

for $j = 1, \ldots, k+1$, where $(s_1, \ldots, \hat{s}_j, \ldots, s_{k+1}) > 1$ denotes the greatest common divisor of the k integers s_i for $i = 1, \ldots, k+1$, $i \neq j$.

Let $A = \{s_i u \mid u \geqslant 0, i = 1, \ldots, k+1\}$. It follows from (1) that the linear form $s_1u_1 + s_2u_2 + \cdots + s_{k+1}u_{k+1}$ represents all sufficiently large integers, and so A is an asymptotic basis of order $h = k+1$. Moreover, (2) implies that $(a_1, \ldots, a_k) > 1$ for all $a_1, \ldots, a_k \in A$. This proves the theorem.

REMARK. The preceding proof is based on the following combinatorial fact: Let $1 \leqslant s < t$ and $T = [1, t]$. Let $S_i \subseteq T$ and $|S_i| = s$ for $i = 1, \ldots, k$. If $k < t/(t-s)$, then $\bigcap_{i=1}^k S_i \neq \varnothing$. If $k \geqslant t/(t-s)$, then there exist sets $S_1, \ldots, S_k$ such that $\bigcap_{i=1}^k S_i = \varnothing$.

LEMMA. *Let $h \geqslant 2$. There exists a family $\mathscr{F}$ of finite sets of positive integers such that* (a) *the intersection of any h sets in $\mathscr{F}$ is nonempty, and* (b) *for any positive integer n there exist h sets in $\mathscr{F}$ whose intersection is exactly $\{n\}$.*

PROOF. Let $\mathbf{N} = M_1 \cup \cdots \cup M_h$ be a partition of the positive integers into h infinite sets M_i. Let $M_i = \{m_{ij}\}_{j=1}^{\infty}$. For $s = 1, \ldots, h$ and $t = 1, 2, 3, \ldots,$ define the family of finite sets F_{st} by

$$F_{st} = \{m_{ij} \mid i = 1, \ldots, h,\ i \neq s;\ j = 1, \ldots, t\} \cup \{m_{st}\}.$$

Then $|F_{st}| = (h-1)t + 1$.

Let $F_{s_i t_i} \in \mathscr{F}$ for $i = 1, \ldots, h$. If $\{s_1, s_2, \ldots, s_h\} = [1, h]$, choose $j \in [1, h]$ such that $t_j = \min\{t_1, t_2, \ldots, t_h\}$. Then

$$m_{s_j t_j} \in \bigcap_{i=1}^{h} F_{s_i t_i} \neq \varnothing.$$

If $\{s_1, \ldots, s_h\} \neq [1, h]$, choose $s^* \in [1, h]$ such that $s^* \neq s_i$ for $i = 1, \ldots, h$. Then

$$m_{s^* 1} \in \bigcap_{i=1}^{h} F_{s_i t_i} \neq \varnothing.$$

Thus, the intersection of every h element of $\mathscr{F}$ is nonempty. This proves (a).

Let $n \in \mathbf{N}$. Then $n = m_{st}$ for some unique $s \in [1, h]$ and $t \in \mathbf{N}$, and

$$F_{st} \cap \left(\bigcap_{\substack{i=1 \\ i \neq s}}^{h} F_{i, t+1} \right) = \{m_{st}\} = \{n\}.$$

This proves (b).

THEOREM 2. *Let $h \geqslant 2$. There exists a set A of nonnegative integers such that*
(i) $(a_1, \ldots, a_h) > 1$ *for all* $a_1, \ldots, a_h \in A$, *and*
(ii) *for every prime p there is an integer $N(p)$ such that $np \in hA$ for all $n \geqslant N(p)$.*

PROOF. Let $\mathscr{F}$ be a family of finite subsets of $\mathbf{N}$ that satisfies properties (a) and (b) of the Lemma. For $F \in \mathscr{F}$, define the integer $b(F)$ by $b(F) = \prod_{i \in F} p_i$, where p_i is the ith prime. Define the set A by

$$A = \{ b(F)u \mid u \geqslant 0,\ F \in \mathscr{F} \}.$$

Property (a) of the Lemma implies that $(b(F_1), b(F_2), \ldots, b(F_h)) > 1$ for every $F_1, F_2, \ldots, F_h \in \mathscr{F}$, and so (i) is satisfied. Property (b) of the Lemma implies that for every prime p there are sets $F_1, \ldots, F_h \in \mathscr{F}$ such that $\bigcap_{i=1}^h F_i = \{p\}$, and so $(b(F_1), \ldots, b(F_h)) = p$. It follows that the linear form $b(F_1)u_1 + \cdots + b(F_h)u_h$ represents all sufficiently large multiples of p, and so $np \in hA$ for all $n \geqslant N(p)$. This proves (ii).

THEOREM 3. *There exists a set A of nonnegative integers such that $(a_1, \ldots, a_h) > 1$ for all $a_1, \ldots, a_h \in A$ and hA has density* 1.

PROOF. Let A satisfy (i) and (ii) of Theorem 2. For any $t \in \mathbf{N}$, the sumset hA contains all sufficiently large multiples of the primes $p_1, \ldots, p_t$, and so there exists a constant c_t such that

$$(hA)(x) \geqslant x\left(1 - \prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right)\right) - c_t$$

for all x. The divergence of the series $\Sigma(1/p)$ implies that $(hA)(x) \geqslant (1-\varepsilon)x$ for every $\varepsilon > 0$ and $x \geqslant x(\varepsilon)$, and so $d(hA) = 1$.

THEOREM 4. *Let $2 \leqslant h < k$. If A is a set of nonnegative integers such that $(a_1, \ldots, a_k) > 1$ for all $a_1, \ldots, a_k \in A$, then the upper asymptotic density of the sumset hA is strictly less than* 1.

PROOF. Fix $a^* \in A$. Let $B^* = \{n \geqslant 0 \mid (n, a^*) > 1\}$. Then B^* has asymptotic density

$$d(B^*) = 1 - \prod_{p \mid a^*}\left(1 - \frac{1}{p}\right) < 1.$$

Let $n \in hA$. Then $n = a_1 + \cdots + a_h$ for some $a_1, \ldots, a_h \in A$. Since $k > h$, it follows that $(a_1, \ldots, a_h, a^*) = d > 1$, and so d divides n for some divisor $d > 1$ of a^*. Therefore, $hA \subseteq B^*$ and

$$d_u(hA) \leqslant d(B^*) < 1.$$

THEOREM 5. *Let $2 \leqslant h \leqslant k$. Let A be a set of nonnegative integers such that $(a_1, \ldots, a_k) > 1$ for all $a_1, \ldots, a_k \in A$. Then A is not an asymptotic basis of order h. In particular, if p is prime, then $p \notin hA$.*

PROOF. Let $n \in hA$. Then $n = a_1 + \cdots + a_h$ for some $a_1, \ldots, a_h \in A$, and $(a_1, \ldots, a_h) = d \geqslant 2$. Then

$$n = a_1 + \cdots + a_h = d\left(\frac{a_1}{d} + \cdots + \frac{a_h}{d}\right) = dd',$$

where $d' \geqslant h \geqslant 2$. Thus, $n \in hA$ implies that n is composite. This concludes the proof.

Note that Theorem 5 shows that Theroems 1 and 2 are best possible.

3. Open problems. 1. Let the set A of nonnegative integers satisfy GCD(h), and let $E = \mathbf{N} \setminus hA$. Theorem 5 shows that

$$E(x) \geqslant \pi(x) \sim x/\log x.$$

There exist sets A such that $E(x) \leqslant cx/\log\log x$. (For example, let $h = 2$ and $m_{1j} = 2j - 1$ and $m_{2j} = 2j$ in the Lemma, and construct A as in the proof of Theorem 2.) It is not known if there exists a set A satisfying GCD(h) such that $E(x)$ has order of magnitude $x/\log\log x$. Indeed, there is no example of a set A satisfying GCD(h) such that $\limsup E(x)\log x/x = \infty$, or even $E(x) \geqslant 2x/\log x$.

2. Let $2 \leqslant h < k$ and let $\varepsilon > 0$. Does there exist a set A satisfying GCD(k) such that $d(hA) > 1 - \varepsilon$?

3. Let A be a set of nonnegative integers with $(a_1, a_2) = 1$ for all a_1, $a_2 \in A$. Clearly, $A(x) \leqslant \pi(x)$ and A contains at most one even integer, hence the odd integers in $2A$ have density zero. If $\mathbf{P}$ is the set of primes, then $\{n \in \mathbf{N} \mid 2n \in 2\mathbf{P}\}$ has density 1. Is it possible to construct a set A satisfying $(a_1, a_2) = 1$ for all a_1, $a_2 \in A$ such that $2A$ contains all sufficiently large even integers?

DEPARTMENT OF MATHEMATICS, RUTGERS UNIVERSITY, NEWARK, NEW JERSEY 07102