PROBLEMS AND RESULTS ON MINIMAL BASES IN ADDITIVE NUMBER THEORY

Paul Erdős
Mathematical Institute
Hungarian Academy of Sciences
Budapest, Hungary

and

Melvyn B. Nathanson
Office of the Provost and
Vice President for Academic Affairs
Lehman College (CUNY)
Bronx, New York 10468

The central problem in additive number theory is as follows: Let A be a set of nonnegative integers. Describe the set of integers that can be written as the sum of h elements of A, with repetitions allowed. This <u>sumset</u> is denoted by hA. If hA is the set of all nonnegative integers, then A is called a <u>basis of order h</u>. If hA contains all sufficiently large integers, then A is called an <u>asymptotic basis of order h</u>. Most of classical additive number theory is the study of sumsets hA, where A is the set of squares (Lagrange's theorem), or the k-th powers (Waring's problem), or the polygonal numbers (Gauss's theorem for triangular numbers or Cauchy's theorem for polygonal numbers of any order), or the primes (Goldbach's conjecture). Shnirel'man [14] created a new field of research in additive number theory when he discovered a simple criterion that implies that a set A of nonnegative integers is a basis of order h for some h. Much recent work in additive number theory concerns general properties of additive bases of finite order. In this paper we discuss some unsolved problems about bases.

Let A be a set of nonnegative integers. Let A(x) denote the number of positive elements of A not exceeding x. The function A(x) is called the counting function of the set A. If lim A(x)/x exists, then it is called the asymptotic density of A, denoted d(A). In particular, if lim A(x)/x = 0, then A has asymptotic density 0. The lower asymptotic density of A, denoted $d_L(A)$, is defined by $d_L(A)$ = lim inf A(x)/x, and the upper asymptotic density, denoted $d_U(A)$, is defined by $d_U(A)$ = lim sup A(x)/x.

There are many examples of asymptotic bases A of order h with density zero. An easy combinatorial argument will show that the counting function of an asymptotic basis A of order h must grow at least as fast as $x^{1/h}$. Let A be an asymptotic basis of order h. Then there is an integer N such that n belongs to hA for all n greater than N. If $N < n \leq x$ and $n = a_1+a_2+\ldots+a_h$, where each a_i belongs to A, then $0 \leq a_i \leq n \leq x$ for i = 1, 2,..., h, and so the number of such a_i is at most A(x)+1. The number of formal expressions of the form $a_1 + \ldots + a_h$ with a_i belonging to A and $0 \leq a_i \leq x$ is at most $(A(x)+1)^h$, and these expressions represent every integer n such that $N < n \leq x$. It follows that $(A(x)+1)^h > x-N-1$. This simple argument proves the following.

LEMMA. If A is an asymptotic basis of order h, then

$$\liminf A(x)/x^{1/h} \geq 1.$$

As a consequence of this result, it is natural to ask if there exist asymptotic bases A of order h such that A(x) has order of magnitude $x^{1/h}$.

DEFINITION. An asymptotic basis A of order h is thin if there is a constant $c > 0$ such that $A(x) < cx^{1/h}$ for all x sufficiently large.

Thin bases exist. The first examples were constructed by Chatrovsky [2], Raikov [13], and Stöhr [15]. Cassels [1] obtained a more precise version of this result. For every $h \geq 2$ he constructed a family of asymptotic bases A of order h such that if $A = \{a_n\}$, then $a_n = cn^h + O(n^{h-1})$ for some $c > 0$.

It is a difficult open problem to determine if the classical bases in additive number theory contain subsets that are thin asymptotic bases. Consider the set Q of squares. Lagrange proved that every positive integer is the sum of four squares, that is, Q is a basis of order 4. However, $Q(x) \sim x^{1/2}$. Erdős and Nathanson [6] proved that for every $\varepsilon > 0$ there is a subset A of the squares Q such that $3A = 3Q$, $4A = 4Q$ and $A(x) \sim cx^{(1/3)+\varepsilon}$ for some $c > 0$. Since the set 3Q of sums of three squares has positive density, this result (except for the $\varepsilon > 0$) is best possible. We conjectured that for any $\varepsilon > 0$ there exists a subset A of the squares such that $4A = 4Q$ (that is, A is a basis of order 4) and $A(x) \sim cx^{(1/4)+\varepsilon}$ for some $c > 0$. In his doctoral dissertation at Mainz, Zöllner [17] has proved this conjecture. Is it possible to drop the $\varepsilon > 0$ in Zöllner's result? That is, does there exist a set A of squares such that A is a basis of order 4 and $A(x) \sim cx^{1/4}$ for some $c > 0$? This problem may be very difficult.

It is important to note that Erdős and Nathanson and Zöllner prove their theorems by using probabilistic methods. It is an open problem to construct explicit sets of squares that satisfy the conclusions of these two theorems.

Nathanson [12] has investigated similar questions for Waring's problem, that is, for sums of k-th powers. In particular, he proved that for any $s > s_0$ there is a set A of integers of density zero such that every nonnegative integer can be represented in the form $n = a_1^k + \ldots + a_s^k$, where $a_1, \ldots, a_s$ belong to A. Wirsing (unpublished) has considered similar questions for sums of three primes in connection with Vinogradov's theorem.

Let A be a set of nonnegative integers, and let $h \geq 2$. Denote by $r_h(n)$ the number of solutions of the equation $n=a_1+...+a_h$ with $a_1 \leq ... \leq a_h$ and $a_1,..., a_h$ belonging to A. Clearly, A is an asymptotic basis of order h if and only if $\liminf r_h(n) > 0$. Erdős and Turán [9] conjectured that if $\liminf r_2(n) > 0$, then $\limsup r_2(n) = \infty$. This remains a major unsolved problem in the study of additive bases. In general, if $h \geq 2$ and $\liminf r_h(n) > 0$, is it true that $\limsup r_h(n) = \infty$?

A second open problem is as follows: The sequence A is called a B_2 sequence if every integer has at most one representation in the form $n = a_1 + a_2$ with a_1, a_2 in A and $a_1 \leq a_2$. Does there exist a B_2 sequence that is an asymptotic basis of order 3?

A key role in additive number theory is played by the concept of minimality.

DEFINITION. An asymptotic basis A of order h is <u>minimal</u> if no proper subset of A is an asymptotic basis of order h. This means that for every number a in the set A there must be infinitely many integers n all of whose representations as a sum of h elements of A include the number a as a summand.

Stöhr [16] introduced this definition of minimality. Using a nonconstructive argument, Härtter [10] proved the existence of uncountably many minimal asymptotic bases of order h for every $h \geq 2$. Nathanson [11] independently rediscovered the notion of minimal asymptotic basis. His hope (unfulfilled) was that an asymptotic basis of order 2 that was both thin and minimal might provide a counterexample to the Erdős-Turán conjecture. Let A be the set of all strictly positive integers that can be written either as a sum of distinct even powers of 2 or as a sum of distinct odd powers of 2. Nathanson [11] showed that A is a minimal asymptotic basis of order 2 and also that A is thin.

Moreover, A is minimal in the following strongest possible sense: For every integer a in A, let E<a> denote the set of integers in the sum set hA that are destroyed by the removal of a from A. Then $E\langle a\rangle(x) > c_1 x^{1/2} > c_2 A(x)$ for positive constants c_1 and c_2 and all sufficiently large x.

Not every asymptotic basis A of order h contains a minimal basis of order h. A trivial example of this phenomenon is the set consisting of 1 together with all nonnegative multiples of h. Nathanson [11] constructed the first nontrivial example of an asymptotic basis of order 2, no subset of which is minimal. Erdős and Nathanson [3] constructed a family of asymptotic bases A of order 2 with the property that, for every subset S of A, the set A\S is an asymptotic basis of order 2 if and only if S is finite. Since there is no maximal finite subset of the infinite set A, it follows that A does not contain a minimal asymptotic basis of order 2.

Let $h \geq 3$. It is an open problem to construct an asymptotic basis A of order h such that, for any subset S of A, the set A\S is an asymptotic basis of order h if and only if S is finite.

There is a class of related open problems. For example, does there exist an asymptotic basis A of order h such that, for any subset S of A, the set A\S is an asymptotic basis of order h if $S(x) < c \log x$, but not if $S(x) > c(\log x)^2$? A more extreme problem: Does there exist an asymptotic basis A of order h such that A\S is still an asymptotic basis if $S(x) < c \log\log x$, but not if $S(x) > cx$? These problems seem difficult.

It is obvious that if A is a minimal asymptotic basis of order 2, then $r_2(n) = 1$ for infinitely many n. The reason is the following: For every a in A there are infinitely many positive integers n such that if $n = a_i + a_j$, then $a_i = a$ or $a_j = a$. Thus,

$r_2(n) = 1$. In a previous paper [5] we asserted incorrectly that if A is a minimal asymptotic basis of order $h \geq 3$, then $r_h(n) = 1$ for infinitely many n. Certainly, for every a in A there are infinitely many n that do not belong to the sumset $h(A\backslash\{a\})$, and each representation of such an n in hA is of the form $n = a_1+...+a_{h-1}+a$. It is possible, however, to have more than one representation of n-a as a sum of h-1 elements of $A\backslash\{a\}$, and so it may happen that $r_h(n) \geq 2$ for all n sufficiently large. Indeed, the Erdős-Rényi probability method [8] may lead to a proof of the existence of a minimal basis of order $h \geq 3$ such that $r_h(n) \geq 2$ for all large n, or even such that $r_h(n)$ tends to infinity. An explicit construction of such bases (if they exist) would be extremely interesting.

Let A be a set of nonnegative integers such that $d_L(A) > 0$ and $d_U(A) < 1$. Suppose there exists a positive real number c such that if n is sufficiently large and n is in 2A, that is, if $r_2(n) \geq 1$, then $r_2(n) > cn$. Do there exist sets X and Y such that $(A\backslash X) \cup Y$ is a minimal asymptotic basis of order 2?

Erdős and Nathanson [4] proved that if $c > 1/\log(4/3)$ and if A is an asymptotic basis of order 2 such that $r_2(n) > c \log n$ for all sufficiently large n, then A contains a minimal asymptotic basis of order 2. This result suggests the following three open problems.

First, if A is an asymptotic basis of order 2 such that $r_2(n) > c \log n$ for <u>some</u> $c > 0$ and all large n, then does A contain a minimal asymptotic basis of order 2? This should be true, but we have no idea how to prove it.

Second, let A be an asymptotic basis of order 2 such that $r_2(n)$ tends to infinity. Does A contain a minimal asymptotic basis of order 2? This problem seems to be very difficult. In the opposite direction, we have recently constructed for every K an asymptotic basis A of order 2 such that $r_2(n) > K$ for all n sufficiently large, but A does not contain a minimal asymptotic basis of order 2.

Third, let $h \geq 3$. Does there exist a function $u_h(n)$ tending to infinity such that if A is an asymptotic basis of order h with $r_h(n) > u_h(n)$ for all sufficiently large n, then A contains a minimal asymptotic basis of order h?

Let A be an asymptotic basis of order 2. For any integer n we define the solution set $S_2(n)$ as the set of all a in A such that n-a is also in A. Using the probability method, we proved [7] that for "almost all" sets A of nonnegative integers, the set A is an asymptotic basis of order 2, and, for all but finitely many pairs of distinct integers m and n, the intersection of the sets $S_2(m)$ and $S_2(n)$ contains at most 5 elements. We do not know if the following generalization to bases of order $h \geq 3$ is true. Define the solution set $S_h(n)$ as the set of all a in A such that n-a is in (h-1)A. Is there a probability measure on the space of all sets of nonnegative integers such that, for some K = K(h), almost all sets A have the following two properties: First, A is an asymptotic basis of order h, and, second, for all but finitely many pairs of distinct integers m, n, the intersection of the solution sets $S_h(m)$ and $S_h(n)$ contains at most K elements.

We conclude with three more problems about minimal bases.

Cassels [1] constructed for each $h \geq 2$ a class of bases $A = (a_n)$ of order h such that $a_n = cn^h + O(n^{h-1})$. Does there exist a minimal asymptotic basis of order h that satisfies this growth condition?

Lagrange proved that every natural number is the sum of four squares. Does there exist a subset of the squares that is a minimal asymptotic basis of order four?

Finally, let A be an asymptotic basis of order h, and let $E\langle a\rangle = hA \setminus h(A\setminus\{a\})$ be the set of integers all of whose representations in hA are destroyed by the removal of a from A. If A is minimal, then $E\langle A\rangle$ is infinite for every a in A. Does there exist an asymptotic basis A with the stronger property that the upper asymptotic densities $d_U(E\langle a\rangle)$ are positive for every a in A? Indeed, we cannot disprove the existence of an asymptotic basis A of order h such that the lower asymptotic densities $d_L(E\langle a\rangle)$ are positive for all a in A.

The problems and results described in this paper represent only a small sample of the open problems that lie in the intersection of classical and combinatorial additive number theory.

REFERENCES

1. J. W. S. Cassels, Über Basen der natürlichen Zahlenreihe, Abh. Math. Sem. Univ. Hamburg. 21 (1957), 247-257.

2. L. Chatrovsky, Sur les bases minimales de la suite des nombres naturels (Russian), Izv. Akad. Nauk SSSR Ser. Mat. 4 (1940), 335-340.

3. P. Erdős and M. B. Nathanson, Oscillations of bases for the natural numbers, Proc. Amer. Math. Soc. 53 (1957), 253-258.

4. P. Erdős and M. B. Nathanson, Systems of distinct representatives and minimal bases in additive number theory, in: M. B. Nathanson (ed.), Number Theory, Carbondale 1979, Lecture Notes in Mathematics, vol. 751, Springer-Verlag, Heidelberg, 1979, pp. 89-107.

5. P. Erdős and M. B. Nathanson, Minimal asymptotic bases for the natural numbers, J. Number Theory 12 (1980), 154-159.

6. P. Erdős and M. B. Nathanson, Lagrange's theorem and thin subsequences of squares, in: J. Gani and V. K. Rohatgi (eds.), Contributions to Probability, Academic Press, New York, 1981, pp. 3-9.

7. P. Erdős and M. B. Nathanson, Independence of solution sets in additive number theory, in: G.-C. Rota (ed.), Probability, Statistical Mechanics, and Number Theory, Academic Press, 1986, pp. 97-105.

8. P. Erdős and A. Rényi, Additive properties of random quences of positive integers, Acta Arith. 6 (1960), 83-110.

9. P. Erdős and P. Turán, On a problem of Sidon in additive mber theory, and some related problems, J. London Math. Soc. 16 941), 212-215; Addendum (by P. Erdős) ibid. 19 (1944), 208.

10. E. Härtter, Ein Beitrag zur Theorie der Minimalbasen, J. ine Angew. Math. 196 (1956), 170-204.

11. M. B. Nathanson, Minimal bases and maximal nonbases in ditive number theory, J. Number Theory 6 (1974), 324-333.

12. M. B. Nathanson, Waring's problem for sets of density zero, : M. I. Knopp (ed.), Number Theory, Philadelphia 1980, Lecture tes in Mathematics, vol. 899, Springer-Verlag, Heidelberg, 1981, . 301-310.

13. D. Raikov, Über die Basen der natürlichen Zahlenreihe, Mat. or. N.S. 2 (44) (1937), 595-597.

14. L. G. Shnirel'man, Über additive Eigenschaften von Zahlen, th. Ann. 107 (1933), 649-690.

15. A. Stöhr, Eine Basis h-ter Ordnung für die Menge aller türlichen Zahlen, Math. Zeit. 42 (1937), 739-743.

16. A. Stöhr, Gelöste und ungelöste Fragen über Basen der türlichen Zahlenreihe I,II, J. Reine Angew. Math. 194 (1955), -65, 111-140.

17. J. Zöllner, Der Vier-Quadrate-Satz und ein Problem von Erdős d Nathanson, Dissertation, Johannes Gutenberg-Universität, Mainz, 84.