PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 72, Number 1, October 1978

REPRESENTATION FUNCTIONS OF SEQUENCES IN ADDITIVE NUMBER THEORY

MELVYN B. NATHANSON[1]

ABSTRACT. Let $\mathcal{A}$ be a set of nonnegative integers, and let $r_2^{\mathcal{A}}(n)$ denote the number of representations of n in the form $n = a_i + a_j$ with $a_i, a_j \in \mathcal{A}$. The set $\mathcal{A}$ is periodic if $a \in \mathcal{A}$ implies $a + m \in \mathcal{A}$ for some $m \geqslant 1$ and all $a > N$. It is proved that if $\mathcal{A}$ is not periodic, then for every set $\mathcal{B} \neq \mathcal{A}$ there exist infinitely many n such that $r_2^{\mathcal{A}}(n) \neq r_2^{\mathcal{B}}(n)$. Moreover, all pairs of periodic sets $\mathcal{A}$ and $\mathcal{B}$ are constructed that satisfy $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all but finitely many n.

Let $\mathcal{A}$ be a set of nonnegative integers. Let $r_h^{\mathcal{A}}(n)$ denote the number of representations of n as a sum of h elements of $\mathcal{A}$. If $f_{\mathcal{A}}(z) = \sum_{a\in\mathcal{A}} z^a$ is the generating function for $\mathcal{A}$, then $f_{\mathcal{A}}(z)^h = \sum_{n=0}^{\infty} r_h^{\mathcal{A}}(n)z^n$. Let $r^{\mathcal{A}}(n)$ denote the number of representations of n as a sum of an arbitrary number of elements of $\mathcal{A}$. If $0 \notin \mathcal{A}$, then $r^{\mathcal{A}}(n) = \sum_{h=1}^{\infty} r_h^{\mathcal{A}}(n)$ is finite for all n. Representation functions have been studied by various authors [1]–[7].

In this note I consider the question: To what extent do the sequences $r_h^{\mathcal{A}}(n)$ and $r^{\mathcal{A}}(n)$ determine the set $\mathcal{A}$? I shall prove that if $\mathcal{A}$ and $\mathcal{B}$ are sets of nonnegative integers such that $r_h^{\mathcal{A}}(n) = r_h^{\mathcal{B}}(n)$ for some $h \geqslant 1$ and all $n \geqslant 0$, or if $r^{\mathcal{A}}(n) = r^{\mathcal{B}}(n)$ for all $n \geqslant 0$, then $\mathcal{A} = \mathcal{B}$. However, there do exist sets $\mathcal{A}$ and $\mathcal{B}$ such that $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all sufficiently large n, but $\mathcal{A} \neq \mathcal{B}$. All such pairs of sets $\mathcal{A}$ and $\mathcal{B}$ will be constructed explicitly. An infinite set $\mathcal{A}$ of integers is called periodic if there exist integers $m \geqslant 1$ and N such that $a \in \mathcal{A}$ implies $a + m \in \mathcal{A}$ for all $a > N$. It will be shown that if the set $\mathcal{A}$ is not periodic, then for every set $\mathcal{B} \neq \mathcal{A}$ we must have $r_2^{\mathcal{A}}(n) \neq r_2^{\mathcal{B}}(n)$ for infinitely many n.

THEOREM 1. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of nonnegative integers, and let $r_h^{\mathcal{A}}(n)$ and $r_h^{\mathcal{B}}(n)$ denote the number of representations of n as a sum of h elements of $\mathcal{A}$ and $\mathcal{B}$, respectively. If $r_h^{\mathcal{A}}(n) = r_h^{\mathcal{B}}(n)$ for all $n \geqslant 0$, then $\mathcal{A} = \mathcal{B}$.*

PROOF. If $r_h^{\mathcal{A}}(n) = r_h^{\mathcal{B}}(n)$ for all $n \geqslant 0$, then

$$0 = \sum_{n=0}^{\infty} r_h^{\mathcal{A}}(n)z^n - \sum_{n=0}^{\infty} r_h^{\mathcal{B}}(n)z^n = f_{\mathcal{A}}(z)^h - f_{\mathcal{B}}(z)^h$$

$$= (f_{\mathcal{A}}(z) - f_{\mathcal{B}}(z))\left(f_{\mathcal{A}}(z)^{h-1} + f_{\mathcal{A}}(z)^{h-2} f_{\mathcal{B}}(z) + \cdots + f_{\mathcal{B}}(z)^{h-1}\right).$$

Received by the editors February 14, 1977.

AMS (MOS) subject classifications (1970). Primary 10L15, 10L05, 10J99.

Key words and phrases. Representation functions, addition of sequences, sum sets.

[1]This paper was written in July, 1976, at the Institute for Advanced Study, Princeton, New Jersey. The author wishes to thank the Institute for its hospitality.

But $f_{\mathcal{A}}(z)^{h-1} + \cdots + f_{\mathcal{B}}(z)^{h-1}$ is a nonzero power series with nonnegative coefficients, and so $f_{\mathcal{A}}(z) - f_{\mathcal{B}}(z) = 0$, that is, $\mathcal{A} = \mathcal{B}$. □

THEOREM 2. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of positive integers, and let $r^{\mathcal{A}}(n)$ and $r^{\mathcal{B}}(n)$ denote the number of representations of n as a sum of an arbitrary number of elements of $\mathcal{A}$ and $\mathcal{B}$, respectively. If $r^{\mathcal{A}}(n) = r^{\mathcal{B}}(n)$ for all $n \geqslant 1$, then $\mathcal{A} = \mathcal{B}$.*

PROOF. Let $r^{\mathcal{A}}(0) = r_0^{\mathcal{A}}(0) = 1$ and let $r_0^{\mathcal{A}}(n) = 0$ for all $n \geqslant 1$. Clearly,

$$r^{\mathcal{A}}(n) = \sum_{h=0}^{\infty} r_h^{\mathcal{A}}(n) \quad \text{for all } n \geqslant 0.$$

Therefore,

$$\sum_{n=0}^{\infty} r^{\mathcal{A}}(n)z^n = \sum_{n=0}^{\infty}\sum_{h=0}^{\infty} r_h^{\mathcal{A}}(n)z^n = \sum_{h=0}^{\infty}\sum_{n=0}^{\infty} r_h^{\mathcal{A}}(n)z^n$$
$$= \sum_{h=0}^{\infty} f_{\mathcal{A}}(z)^h = \frac{1}{1 - f_{\mathcal{A}}(z)}.$$

Consequently, if $r^{\mathcal{A}}(n) = r^{\mathcal{B}}(n)$ for all $n \geqslant 0$, then $(1 - f_{\mathcal{A}}(z))^{-1} = (1 - f_{\mathcal{B}}(z))^{-1}$, and so $\mathcal{A} = \mathcal{B}$. □

THEOREM 3. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of positive integers, and let $p^{\mathcal{A}}(n)$ and $p^{\mathcal{B}}(n)$ denote the number of representations of n as the sum of an arbitrary number of elements of $\mathcal{A}$ and $\mathcal{B}$, respectively, where representations differing only in the arrangement of their summands are not counted separately. If $p^{\mathcal{A}}(n) = p^{\mathcal{B}}(n)$ for all $n \geqslant 1$, then $\mathcal{A} = \mathcal{B}$.*

PROOF. Let $p^{\mathcal{A}}(0) = p^{\mathcal{B}}(0) = 1$. The generating function for $p^{\mathcal{A}}(n)$ has the form

$$\sum_{n=0}^{\infty} p^{\mathcal{A}}(n)z^n = \prod_{a\in\mathcal{A}}\sum_{k=0}^{\infty} z^{ak} = \prod_{a\in\mathcal{A}} \frac{1}{1 - z^a}.$$

If $p^{\mathcal{A}}(n) = p^{\mathcal{B}}(n)$ for all $n \geqslant 1$, then $\prod_{a\in\mathcal{A}}(1 - z^a) = \prod_{b\in\mathcal{B}}(1 - z^b)$, and so $\mathcal{A} = \mathcal{B}$. □

If $\mathcal{A}$ and $\mathcal{B}$ are sets of nonnegative integers such that $r_h^{\mathcal{A}}(n) = r_h^{\mathcal{B}}(n)$ for some $h \geqslant 1$ and all sufficiently large n, then it does not follow that $\mathcal{A} = \mathcal{B}$. For example, $r_1^{\mathcal{A}}(n) = 1$ if $n \in \mathcal{A}$ and $r_1^{\mathcal{A}}(n) = 0$ if $n \notin \mathcal{A}$, and so $r_1^{\mathcal{A}}(n) = r_1^{\mathcal{B}}(n)$ for all sufficiently large n if and only if $\mathcal{A}$ and $\mathcal{B}$ eventually coincide. If $\mathcal{A} = \{n \geqslant 1\}$ and $\mathcal{B} = \{0\} \cup \{n \geqslant 2\}$, then $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all $n \geqslant 3$, but $\mathcal{A} \neq \mathcal{B}$. This construction can be generalized in the following way.

Let A, B, and T be finite sets of integers. If each residue class modulo m contains exactly the same number of elements of A as elements of B, then we write $A \equiv B \pmod m$. If the number of solutions of the congruence $a + t \equiv$

$n \pmod m$ with $a \in A$, $t \in T$, equals the number of solutions of the congruence $b + t \equiv n \pmod m$ with $b \in B$, $t \in T$, for each residue class n modulo m, then we write $A + T \equiv B + T \pmod m$.

Let A, B, and T be finite sets of integers with $A \cup B \subset \{0, 1, 2, \ldots, N\}$ and $T \subset \{0, 1, \ldots, m - 1\}$ such that $A + T \equiv B + T \pmod m$ for some $m \geqslant 1$. Define the periodic set $\mathcal{C}$ by

$$\mathcal{C} = \{c > N | c \equiv t \pmod m \text{ for some } t \in T\}.$$

Let $\mathcal{A} = A \cup \mathcal{C}$ and $\mathcal{B} = B \cup \mathcal{C}$. If $A \neq B$, then $\mathcal{A} \neq \mathcal{B}$. We shall prove that $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all $n > 2N$.

Let $s^A(n)$ (resp. $s^B(n)$) denote the number of representations of n in the form $n = a + c$ with $a \in A$, $c \in \mathcal{C}$ (resp. $n = b + c$ with $b \in B$, $c \in \mathcal{C}$). If $a_1, a_2 \in A$, then $a_1 \leqslant N$ and $a_2 \leqslant N$, hence $a_1 + a_2 \leqslant 2N$. Consequently, if $n > 2N$ then the only representations of n as a sum of two elements of $\mathcal{A} = A \cup \mathcal{C}$ are of the form $a + c$, $c + a$, and $c + c'$, where $a \in A$ and $c, c' \in \mathcal{C}$. Since $A \cap \mathcal{C} = \varnothing$, this implies that $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{C}}(n) + 2s^A(n)$. Similarly, $r_2^{\mathcal{B}}(n) = r_2^{\mathcal{C}}(n) + 2s^B(n)$.

Therefore, $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ if and only if $s^A(n) = s^B(n)$.

But if $n > 2N$, then $s^A(n)$ is exactly the number of solutions of the congruence $n \equiv a + t \pmod m$ with $a \in A$, $t \in T$. For if $n \equiv a + t \pmod m$, then $n - a \equiv t \pmod m$ and $n - a > 2N - a \geqslant N$, hence $n - a = c \in \mathcal{C}$, and $n = a + (n - a) = a + c$. Conversely, if $n = a + c$ with $a \in A$, $c \in \mathcal{C}$, then $c = n - a > 2N - a \geqslant N$, and so $c \equiv t \pmod m$ for some $t \in T$, and $n \equiv a + t \pmod m$.

Similarly, $s^B(n)$ is the number of solutions of the congruence $n \equiv b + t \pmod m$ with $b \in B$, $t \in T$. Since $A + T \equiv B + T \pmod m$, this implies that $s^A(n) = s^B(n)$, and so $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all $n > 2N$. The following theorem shows that this construction produces *all* pairs of sets $\mathcal{A}$ and $\mathcal{B}$ such that $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all sufficiently large n.

Theorem 4. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of nonnegative integers such that $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all sufficiently large n. Then there exist finite sets A, B, and T with $A \cup B \subset \{0, 1, \ldots, N\}$ and $T \subset \{0, 1, \ldots, m - 1\}$ such that $A + T \equiv B + T \pmod m$, and $\mathcal{A} = A \cup \mathcal{C}$ and $\mathcal{B} = B \cup \mathcal{C}$, where $\mathcal{C} = \{c > N | c \equiv t \pmod m$ for some $t \in T\}$.*

Proof. To every representation $2n = a_i + a_j$ with $a_i, a_j \in \mathcal{A}$ and $a_i \neq a_j$ corresponds a second representation $2n = a_j + a_i$. Therefore, $r_2^{\mathcal{A}}(2n)$ is odd if and only if $n \in \mathcal{A}$. Similarly, $n \in \mathcal{B}$ if and only if $r_2^{\mathcal{B}}(n)$ is odd. If $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for all $n > N_0$, then for all $n > N_0$ we have $n \in \mathcal{A}$ if and only if $n \in \mathcal{B}$. Let $f_{\mathcal{A}}(z) = \sum_{a \in \mathcal{A}} z^a$ and $f_{\mathcal{B}}(z) = \sum_{b \in \mathcal{B}} z^b$. Then $f_{\mathcal{A}}(z) - f_{\mathcal{B}}(z) = Q(z)$ is a polynomial of degree at most N_0, and $f_{\mathcal{A}}(z) + f_{\mathcal{B}}(z)$ is a power series such that, for $n > N_0$, the coefficient of z^n is either 0 (if $n \notin \mathcal{A} \cup \mathcal{B}$) or 2 (if $n \in \mathcal{A} \cap \mathcal{B}$). Then

$$Q(z)(f_{\mathcal{A}}(z) + f_{\mathcal{B}}(z)) = (f_{\mathcal{A}}(z) - f_{\mathcal{B}}(z))(f_{\mathcal{A}}(z) + f_{\mathcal{B}}(z))$$
$$= f_{\mathcal{A}}(z)^2 - f_{\mathcal{B}}(z)^2 = \sum_{n=0}^{\infty} (r_2^{\mathcal{A}}(n) - r_2^{\mathcal{B}}(n))z^n$$
$$= \sum_{n=0}^{N_0} (r_2^{\mathcal{A}}(n) - r_2^{\mathcal{B}}(n))z^n = P(z),$$

where $P(z)$ is a polynomial of degree at most N_0. Therefore, $f_{\mathcal{A}}(z) + f_{\mathcal{B}}(z) = P(z)/Q(z)$ is a rational function, and so the sequence of coefficients of the power series $f_{\mathcal{A}}(z) + f_{\mathcal{B}}(z)$ eventually satisfies a linear recurrence relation. These coefficients are eventually either 0 or 2. But a sequence defined by a linear recurrence on a finite set must be eventually periodic. This implies that for some modulus $m \geqslant 1$ there exists a set $T \subset \{0, 1, 2, \ldots, m - 1\}$ and an integer $N > N_0$ such that, for all $n > N$, we have $n \in \mathcal{A} \cap \mathcal{B}$ if and only if $n \equiv t \pmod{m}$ for some $t \in T$.

Let

$$A = \{a \leqslant N | a \in \mathcal{A}\}, \quad B = \{b \leqslant N | b \in \mathcal{B}\},$$

and

$$\mathcal{C} = \{c > N | c \in \mathcal{A} \cap \mathcal{B}\} = \{c > N | c \equiv t \pmod{m} \text{ for some } t \in T\}.$$

Then $\mathcal{A} = A \cup \mathcal{C}$ and $\mathcal{B} = B \cup \mathcal{C}$.

If $n > 2N$, then $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{C}}(n) + 2s^A(n)$ and $r_2^{\mathcal{B}}(n) = r_2^{\mathcal{C}}(n) + 2s^B(n)$, where $s^A(n)$ (resp. $s^B(n)$) is the number of representations of n in the form $n = a + c$ with $a \in A$, $c \in \mathcal{C}$ (resp. $n = b + c$ with $b \in B$, $c \in \mathcal{C}$). Since $r_2^{\mathcal{A}}(n) = r_2^{\mathcal{B}}(n)$ for $n > 2N$, it follows that $s^A(n) = s^B(n)$. But $s^A(n)$ (resp. $s^B(n)$) is also the number of solutions of the congruence $n \equiv a + t \pmod{m}$ with $a \in A$, $t \in T$ (resp. $n \equiv b + t \pmod{m}$ with $b \in B$, $t \in T$). Therefore, $A + T \equiv B + T \pmod{m}$. □

Corollary. *If the set $\mathcal{A}$ of nonnegative integers is not eventually periodic, then for every set $\mathcal{B} \neq \mathcal{A}$ we have $r_2^{\mathcal{A}}(n) \neq r_2^{\mathcal{B}}(n)$ for infinitely many n.*

Remarks. The converse of this corollary is false. If $\mathcal{A}$ is the sequence of all nonnegative integers, then $r_2^{\mathcal{A}}(n) = n + 1$ for all $n \geqslant 0$. If $\mathcal{B} \neq \mathcal{A}$, then $r_2^{\mathcal{B}}(n) \leqslant n$ for all sufficiently large n. But the sequence $\mathcal{A}$ is periodic with period 1.

It is an open problem to determine those sets $\mathcal{A}$ and $\mathcal{B}$ such that $r_h^{\mathcal{A}}(n) = r_h^{\mathcal{B}}(n)$ for some $h \geqslant 3$ and all sufficiently large n.

The following problem arises from Theorem 4. Let A, B, and T be finite nonempty sets of nonnegative integers with $T \subset \{0, 1, 2, \ldots, m - 1\}$ for some $m \geqslant 1$ such that $A + T \equiv B + T \pmod{m}$. Assume the modulus m is "reduced" in the sense that there does not exist a divisor m_1 of m and a set $T_1 \subset \{0, 1, \ldots, m_1 - 1\}$ such that $T = \{t \in \{0, 1, \ldots, m - 1\} | t \equiv t_1 \pmod{m_1}$ for some $t_1 \in T_1\}$. Does this imply that $A \equiv B \pmod{m}$? This is obviously true if $m = 1$. The following result proves this is also true if the modulus m is prime.

THEOREM 5. *Let p be a prime number, and let A, B, T be finite, nonempty sets of nonnegative integers with $T \subset \{0, 1, \ldots, p-1\}$. If $T = \{0, 1, \ldots, p-1\}$, then $A + T \equiv B + T \pmod p$ if and only if $|A| = |B|$. If $T \subsetneq \{0, 1, \ldots, p-1\}$, then $A + T \equiv B + T \pmod p$ if and only if $A \equiv B \pmod p$.*

PROOF. If $T = \{0, 1, \ldots, p-1\}$, then the number of solutions of the congruence $a + t \equiv n \pmod p$ with $a \in A$, $t \in T$ (resp. $b + t \equiv n \pmod p$ with $b \in B$, $t \in T$) is exactly $|A|$ (resp. $|B|$) for all n. Therefore, $A + T \equiv B + T \pmod p$ if and only if $|A| = |B|$.

Suppose that $T \subsetneq \{0, 1, \ldots, p-1\}$. Write $f_A(z) = \sum_{a \in A} z^a$, $f_B(z) = \sum_{b \in B} z^b$, and $f_T(z) = \sum_{t \in T} z^t$. If $A + T \equiv B + T \pmod p$, then

$$f_A(z) f_T(z) \equiv f_B(z) f_T(z) \pmod{z^p - 1},$$

that is, $z^p - 1$ divides $(f_A(z) - f_B(z)) f_T(z)$. The cyclotomic polynomial $z^p - 1$ is the product of two irreducible factors

$$z^p - 1 = (z-1)(1 + z + z^2 + \cdots + z^{p-1}).$$

The degree of $f_T(z)$ is at most $p - 1$, and so, if $1 + z + \cdots + z^{p-1}$ divides $f_T(z)$, then $f_T(z) = 1 + z + \cdots + z^{p-1}$ and $T = \{0, 1, \ldots, p-1\}$, which is false. Therefore, $1 + z + \cdots + z^{p-1}$ divides $f_A(z) - f_B(z)$. If $z - 1$ divides $f_T(z)$, then $f_T(z) = (z-1)g(z)$ for some polynomial $g(z)$. But this implies that $f_T(1) = 0$. However, since $f_T(z) = \sum_{t \in T} z^t$, it follows that $f_T(1) = |T| \neq 0$ since $T \neq \varnothing$. Therefore, $z - 1$ also divides $f_A(z) - f_B(z)$. Consequently, $z^p - 1$ divides $f_A(z) - f_B(z)$. But this means precisely that $A \equiv B \pmod p$. □

COROLLARY. *Let p be a prime, and let A, B, and T be nonempty, proper subsets of $\{0, 1, \ldots, p-1\}$. If $A + T \equiv B + T \pmod p$, then $A = B$.*

REFERENCES

1. A. O. L. Atkin, *On pseudo-squares*, Proc. London Math. Soc. (3) **14** (1965), 22–27.

2. P. T. Bateman, E. E. Kohlbecker and J. P. Tull, *On a theorem of Erdős and Fuchs in additive number theory*, Proc. Amer. Math. Soc. **14** (1963), 278–284.

3. P. Erdös and W. H. J. Fuchs, *On a problem of additive number theory*, J. London Math. Soc. **31** (1956), 67–73.

4. P. Erdős, B. Gordon, L. A. Rubel and E. G. Straus, *Tauberian theorems for sum sets*, Acta Arith. **9** (1964), 177–189.

5. P. Erdös and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. **6** (1960), 83–110.

6. P. Erdös and P. Turán, *On a problem of Sidon in additive number theory, and on some related problems*, J. London Math. Soc. **16** (1941), 212–215.

7. R. C. Vaughan, *On the addition of sequences of integers*, J. Number Theory **4** (1972), 1–16.

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901