ACTA ARITHMETICA
LXV.3 (1993)

Solving a linear equation in a set of integers I

by

Imre Z. Ruzsa (Budapest)

1. Introduction. The following three problems of combinatorial number theory are discussed in numerous works.

1) A set is called *sum-free* if no sum of two elements equals a third. It is well known that at most $[(N+1)/2]$ numbers can be selected from the first N natural numbers to form a sum-free set, and one of the extremal sets is the set of odd numbers.

2) Let $r(N)$ denote the maximal number of integers that can be selected from $\{1,\dots,N\}$ without including any three-term arithmetical progression. It is known that

$$Ne^{-\beta\sqrt{\log N}} \ll r(N) \ll N(\log N)^{-\alpha}$$

with certain positive constants α and β. Here the lower bound is due to Behrend (1946), the upper bound to Heath-Brown (1987) and Szemerédi (1990), while an earlier weaker bound was given by Roth (1953).

3) A *Sidon set* is a set of integers with the property that all sums of pairs are different, that is, the equation $x+y=u+v$ has no solution in this set, *except* the trivial solutions given by $x=u$, $y=v$ and $x=v$, $y=u$. The maximal cardinality $s(N)$ of a Sidon set $\mathcal{A}\subset[1,N]$ satisfies

$$\sqrt{N}-c_1N^{5/22} < s(N) < \sqrt{N}+c_2N^{1/4}$$

with positive constants c_1, c_2. These bounds are essentially due to Erdős and Turán; the exponent in the lower bound depends on estimates of the difference between consecutive primes, and the improvement over Erdős and Turán's bound is due to improved results on primes.

The common feature of these problems is that they are related to a linear equation; in case 1), $x+y=z$, in case 2), $x+y=2z$, in case 3), $x+y=u+v$. We try to consider this sort of problem for general linear

Supported by Hungarian National Foundation for Scientific Research, Grant No. 1901, and CNRS Laboratoire de Mathématiques Discrètes, Marseille.

equations, and we try to understand why the answers behave so differently in these cases. Our efforts are only partially successful; at least, we formulate the most important general questions and some conjectures, and study some further equations.

Let $(a_i)_{1\le i\le k}$ and b be integers. We try to solve the equation

$$a_1x_1 + \ldots + a_kx_k = b \tag{1.1}$$

with $x_1, \ldots, x_k$ in a set of integers.

Some of these equations have "trivial" solutions that need to be excluded from the consideration; for arithmetical progressions, they were collections of three identical numbers, in Sidon's problem, collections where (u, v) is a permutation of (x, y). In general, we define trivial solutions as follows.

1.1. Definition. Assume that the integers $x_1, \ldots, x_k$ form a solution of equation (1.1), and there are l different among them. Let

$$\{1, \ldots, k\} = \mathcal{T}_1 \cup \ldots \cup \mathcal{T}_l$$

be the partition of the set of subscripts into disjoint nonempty parts $\mathcal{T}_j$ such that $x_i = x_j$ if and only if $i, j \in \mathcal{T}_\nu$ for some ν. We call this solution *trivial* if

$$\sum_{i\in\mathcal{T}_\nu} a_i = 0, \qquad \nu = 1, \ldots, l\,,$$

and *nontrivial* otherwise.

Clearly trivial solutions exist only if $b = 0$ and

$$s = a_1 + \ldots + a_k = 0\,.$$

If $b = 0$ and $s = 0$, then a collection of k identical numbers always forms a trivial solution, while a solution with k distinct numbers is always nontrivial.

1.2. Definition. Let

$$r(N) = \max\{|\mathcal{A}| : \mathcal{A} \subset [1, N]\}$$

over sets $\mathcal{A}$ such that equation (1.1) has no nontrivial solution with $x_i \in \mathcal{A}$, and let $R(N)$ be the analogous maximum over sets such that equation (1.1) has no solution with distinct integers $x_i \in \mathcal{A}$.

In case of the equation $x + y = 2z$ (three-term arithmetical progression), obviously $r(N) = R(N)$. For the equation $x + y = u + v$ (Sidon sets) we shall see that $r(N) \sim R(N)$. We shall also meet equations for which these quantities behave very differently (Section 3).

We shall try to find estimates for the quantities $r(N)$ and $R(N)$ for certain classes of equations. We shall also consider the problem of infinite sets without a solution.

In connection with equation (1.1) we saw that the vanishing of the constant term b and the sum of the coefficients $s = a_1 + \ldots + a_k = 0$ affects the

existence of trivial solutions. They also affect the behaviour of $r(N)$. The following result is known.

1.3. THEOREM. *If* $b = s = 0$, *then*

$$r(N) \le R(N) = o(N)\,. \tag{1.2}$$

On the other hand, if $b \neq 0$ *or* $s \neq 0$, *then* $r(N) > \lambda N$ *with some* $\lambda > 0$ *for all* N *large enough.*

(1.2) can be proved with Roth's method, and it also follows immediately from the famous theorem of Szemerédi (1975) on arithmetical progressions. One can also adapt the methods of Heath-Brown (1987) and Szemerédi (1990) to obtain

$$r(N) \le R(N) \ll N(\log N)^{-\alpha} \tag{1.3}$$

with a positive constant α depending on the coefficients $a_1, \dots, a_k$. The fact that $r(N) \gg N$ if $b \neq 0$ or $s \neq 0$ is stated by Komlós, Sulyok and Szemerédi (1975), and was probably known long before that.

The condition $b = 0$ is equivalent to homogeneity or multiplication invariance (if $x_1, \dots, x_k$ is a solution, so is $tx_1, \dots, tx_k$), while the other means translation invariance (if $x_1, \dots, x_k$ is a solution, so is $x_1 + t, \dots, x_k + t$). This double invariance also plays an important role in the study of $r(N)$. For short we shall call equations with $b = s = 0$ *invariant*, and those with $b \neq 0$ or $s \neq 0$ *noninvariant*.

Noninvariant equations have drawn little attention so far. The estimate $r(N) \gg N$ is easy, but there remain many nontrivial unsolved problems. We shall consider noninvariant equations in the second part, and devote the first part to invariant equations.

Notation. Sets of integers will be denoted by script letters. If a letter, say $\mathcal{A}$, denotes a set, the corresponding Roman letter is used to denote its counting function without any further explanation, so that

$$A(N) = |\mathcal{A} \cap [1, N]|\,.$$

2. Lower bounds. Recall that we consider the equation

$$a_1x_1 + \ldots + a_kx_k = 0 \tag{2.1}$$

under the assumption that $a_1 + \ldots + a_k = 0$.

The simplest method for finding lower estimates is the greedy algorithm, which leads to the following result.

2.1. THEOREM. *There is an infinite sequence* $1 = u_1 < u_2 < \ldots$ *of integers such that*

$$u_n \le kn^{k-1} \tag{2.2}$$

and equation (2.1) *has no nontrivial solution in the set* $\mathcal{A} = \{u_1, u_2, \ldots\}$. *In particular*, *we have*

$$R(N) \ge r(N) \ge k^{-1/(k-1)} N^{1/(k-1)} . \tag{2.3}$$

The proof would be completely obvious if we only wanted the bound for $R(N)$. The possibility of equal ones among the variables and the existence of trivial solutions add some complications, so we include a proof.

P r o o f. We put $u_1 = 1$ and define u_n recursively. Given $u_1, \ldots, u_{n-1}$, let u_n be the smallest positive integer satisfying

$$u_n \ne -\Big(\sum_{i\in\mathcal{S}} a_i\Big)^{-1} \sum_{1\le i\le k, i\notin\mathcal{S}} a_i x_i \tag{2.4}$$

for every set $\mathcal{S} \subset \{1, \ldots, k\}$ of subscripts such that $\sum_{i\in\mathcal{S}} a_i \ne 0$ and every choice of $x_i \in \{u_1, \ldots, u_{n-1}\}$ for $i \notin \mathcal{S}$. For a fixed $\mathcal{S}$ with $|\mathcal{S}| = j$ this excludes $(n-1)^{k-j}$ numbers, thus the total number of excluded integers is at most

$$\sum_{j=1}^{k-1} \binom{k}{j} (n-1)^{k-j} = n^k - (n-1)^k - 1 < kn^{k-1} .$$

Consequently, we can extend our set by an integer $u_n \le kn^{k-1}$. This will automatically be different from $u_1, \ldots, u_{n-1}$, since putting $x_i = u_j$ for all $i \notin \mathcal{S}$ in (2.4) we get $u_n \ne u_j$. It will also satisfy $u_n > u_{n-1}$ by the minimal choice of u_{n-1}.

We show that (2.1) has no nontrivial solution in the set $\{u_1, \ldots, u_n\}$. We use induction. The statement is obviously true for $n = 1$. We establish it for n assuming its validity for $n-1$. Suppose that there is a solution, and let $\mathcal{S}$ denote the set of those subscripts for which $x_i = u_n$. If $\sum_{i\in\mathcal{S}} a_i \ne 0$, this contradicts to (2.4). If $\sum_{i\in\mathcal{S}} a_i = 0$, then by replacing each occurrence of u_n by u_1 we get another nontrivial solution, which contradicts the induction hypothesis. ∎

The greedy algorithm probably never gives the correct order of magnitude. In the cases when the size of $r(N)$ is known, it is always much higher, at least of order $N^{2/k}$.

The same order of magnitude (up to a constant) can be achieved by a random construction.

Behrend's method that gave the sharp lower bound for three-term arithmetical progressions does not work for every equation but it can be extended to a class.

2.2. Definition. We say that an equation $a_1x_1 + \ldots + a_kx_k = 0$ is of *type* (l, m) if l coefficients are positive and m are negative $(l + m = k)$.

We consider type $(l,1)$. We can rearrange such an equation as

$$a_1x_1+\ldots+a_lx_l=by \qquad (a_1+\ldots+a_l=b)\,. \tag{2.5}$$

2.3. THEOREM. *Let $a_1,\ldots,a_l$ and b be positive integers. There is a positive constant β, depending on b and l, such that for the equation* (2.5) *the estimate*

$$r(N)\gg Ne^{-\beta\sqrt{\log N}} \tag{2.6}$$

holds.

We suppress the proof, which requires only a minimal modification of Behrend's (1946) argument.

3. Symmetric equations. For certain equations a simple combinatorial argument yields better estimates than Roth's method.

3.1. DEFINITION. We call an equation *symmetric* if the number of unknowns is even, say $k=2l$, and the coefficients can be arranged into pairs of type $a,-a$.

Sidon's equation is a typical example.

A symmetric equation can be rearranged as

$$a_1x_1+\ldots+a_lx_l=a_1x_{l+1}+\ldots+a_lx_{2l} \tag{3.1}$$

(so $a_{l+i}=-a_i$ for $1\le i\le l$).

3.2. THEOREM. *Let $l\ge 2$, and let $a_1,\ldots,a_l$ be positive integers. For the symmetric equation* (3.1) *we have*

$$r(N)=O(N^{1/l})\,, \tag{3.2}$$

$$R(N)=O(N^{1/2})\,. \tag{3.3}$$

Proof. Let $\mathcal{A}\subset[1,N]$ be any set, and write $|\mathcal{A}|=M$. For an integer n let $t(n)$ denote the number of solutions of the equation

$$a_1x_1+\ldots+a_lx_l=n, \qquad x_i\in\mathcal{A}\,.$$

Write $S=a_1+\ldots+a_l$. We have

$$\sum_{n\le SN}t(n)=M^l\,.$$

The number $\sum t(n)^2$ is equal to the total number of solutions of equation (3.1) with $x_i\in\mathcal{A}$, including the trivial ones. The inequality of the arithmetic and square mean yields

$$\sum t(n)^2\ge\frac{M^{2l}}{SN}\,. \tag{3.4}$$

Now we estimate the number of trivial solutions. In a trivial solution there is a partition of the set $\{1,\dots,2l\}$ of subscripts into sets $\mathcal{T}_1,\dots,\mathcal{T}_m$ such that

$$\sum_{i\in\mathcal{T}_j} a_i = 0\,,$$

and x_i is constant for $i\in\mathcal{T}_j$. Each $\mathcal{T}_j$ must have at least two elements, hence $m\le l$. At most M^m solutions belong to a fixed partition, hence the total number of trivial solutions is at most PM^l, where P is the number of partitions. If the set $\mathcal{A}$ is such that (3.1) has only trivial solutions, then (3.4) yields

$$\frac{M^{2l}}{SN} \le PSN\,,$$

that is, $M\le(\sqrt{P}SN)^{1/l}$, which proves (3.2).

Next we estimate the number of solutions where not all x_i are distinct. Consider those for which $x_i=x_j$ for certain subscripts $1\le i<j\le 2l$. Let m be a subscript different from i and j. Equation (3.1) uniquely determines x_m in terms of the other x_ν, $\nu\ne j,m$, and consequently it has at most M^{2l-2} solutions. Taking into account the $\binom{k}{2}$ possible choices of i and j, the number of solutions with at least one repeated value of the variables is at most

$$\binom{k}{2}M^{2l-2}\,.$$

For a set $\mathcal{A}$ in which there is no solution of (3.1) with distinct x_i we obtain

$$\frac{M^{2l}}{SN} \le \binom{k}{2}M^{2l-2}\,,$$

and this implies (3.3). ∎

The bounds of (3.2) and (3.3) are of different order of magnitude if $l\ge 3$. We show that in general it is impossible to replace the exponent $1/2$ of (3.3) by any smaller number.

3.3. Theorem. *For every $l\ge 3$ and $\varepsilon>0$ there are positive integers $a_1,\dots,a_l$ such that for the equation* (3.1) *we have*

$$R(N) \gg N^{1/2-\varepsilon}\,. \tag{3.5}$$

Proof. We consider the equation

$$x_1 + d(x_2+\dots+x_l) = x_{l+1} + d(x_{l+2}+\dots+x_{2l})\,. \tag{3.6}$$

Put $m=d^2l$, and let $\mathcal{A}$ consist of those numbers $n\le N$ whose development in base m contains only the digits $0,1,\dots,d-1$. We show that (3.6) has no solution with different elements of $\mathcal{A}$. Consider any solution of (3.6) in $\mathcal{A}$,

say

$$x_i = \sum \alpha_{ij} m^j \,.$$

The choice of m is sufficiently large to guarantee that in both sides of (3.6), multiplication by d and addition of the terms can be performed in base m without carry, hence the corresponding equation must hold for each digit:

$$\alpha_{1j} + d(\alpha_{2j} + \ldots + \alpha_{lj}) = \alpha_{l+1,j} + d(\alpha_{l+2,j} + \ldots + \alpha_{2l,j}) \,.$$

This implies that $\alpha_{1j} \equiv \alpha_{l+1,j} \pmod{d}$, and consequently $\alpha_{1j} = \alpha_{l+1,j}$ for all j, that is, $x_1 = x_{l+1}$.

The number of such integers up to N is $\gg N^\delta$, where

$$\delta = \frac{\log d}{\log m} = \frac{\log d}{2\log d + \log l} > \frac{1}{2} - \varepsilon$$

if $d > l^{1/\varepsilon}$. ∎

3.4. Problem. Given a symmetric equation (3.1), is there always a constant $c > 0$ (depending on the coefficients) such that

$$R(N) \ll N^{1/2-c} \,?$$

Theorem 3.2 can be applied to deduce a bound for certain nonsymmetric equations.

Consider the equation

$$a_1 x_1 + \ldots + a_k x_k = 0 \,. \tag{3.7}$$

3.5. Definition. By the *genus* of equation (3.7) we mean the largest number m such that there is a partition

$$\{1, \ldots, k\} = \mathcal{T}_1 \cup \ldots \cup \mathcal{T}_m$$

of the set of subscripts into m disjoint nonempty sets $\mathcal{T}_j$ such that

$$\sum_{i \in \mathcal{T}_j} a_i = 0$$

for every j.

3.6. Theorem. *For any equation of genus m we have*

$$r(N) \ll N^{1/m} \,. \tag{3.8}$$

Proof. For each $1 \le j \le m$ select an $i(j) \in \mathcal{T}_j$ and let $b_j = a_{i(j)}$. We consider the auxiliary equation

$$b_1 y_1 + \ldots + b_m y_m = b_1 y_{m+1} + \ldots + b_m y_{2m} \,. \tag{3.9}$$

From any solution of (3.9) we can make a solution of (3.7) by setting $x_{i(j)} = y_j$ and $x_i = y_{m+j}$ for $i \in \mathcal{T}_j$, $i \ne i(j)$. We claim that nontrivial

solutions of (3.9) turn into nontrivial solutions. Indeed, for every integer n we have (by putting $b_{m+j} = -b_j$)

$$\sum_{x_i=n} a_i = \sum_{y_j=n} b_j\,,$$

and a choice of n for which the right side does not vanish proves the nontriviality of the solution (x_i). Now an application of Theorem 3.2 to equation (3.9) completes the proof. ∎

4. Sidon sets. A set $\mathcal{A}$ of integers is called a *Sidon set* if the equation $x+y = u+v$ with $x, y, u, v \in \mathcal{A}$ can hold only trivially, that is, either $x = u$, $y = v$ or $x = v$, $y = u$.

The equation $x + y = u + v$ can be rearranged to $x - u = v - y$. This form gives the following useful equivalent condition. For an integer n let $\delta(n)$ denote the number of solutions of $n = x - y$, $x, y \in \mathcal{A}$. The set $\mathcal{A}$ is a Sidon set if and only if $\delta(n) \le 1$ for every $n \ne 0$.

This is a symmetric equation, thus the estimate $O(\sqrt{N})$ for the cardinality of a Sidon set follows from Theorem 3.2. Here more precise estimates are available.

4.1. Theorem. *A Sidon set $\mathcal{A} \subset [1, N]$ always satisfies*

$$|\mathcal{A}| \le N^{1/2} + N^{1/4} + 1\,. \tag{4.1}$$

The first proof of this result is due to Erdős–Turán (1941) and can be found in Halberstam–Roth (1966). Another proof was given by Lindström (1969). Both proofs are based on the idea of counting "small" differences $a - a'$. We give a third proof, where the same idea is somewhat hidden. We shall deduce (4.1) from a property which is perhaps of an independent interest.

4.2. Theorem. *Let $\mathcal{A}$, $\mathcal{B}$ be nonempty finite sets of integers, $|\mathcal{A}| = m$, $|\mathcal{B}| = n$. Assume that $\mathcal{A}$ is a Sidon set. Then*

$$|\mathcal{A} + \mathcal{B}| \ge \frac{m^2 n}{m + n - 1}\,. \tag{4.2}$$

Proof. For any integer u let $\sigma(u)$ denote the number of solutions of $u = a + b$, $a \in \mathcal{A}$, $b \in \mathcal{B}$. We have obviously

$$\sum \sigma(u) = |\mathcal{A}||\mathcal{B}| = mn\,,$$

hence the inequality of the arithmetic and square mean yields

$$\sum \sigma(u)^2 \ge \frac{m^2 n^2}{|\mathcal{A} + \mathcal{B}|}\,. \tag{4.3}$$

The sum $\sum \sigma(u)^2$ counts those quadruples a, a', b, b' that satisfy $a, a' \in \mathcal{A}$, $b, b' \in \mathcal{B}$, $a + b = a' + b'$, which can be rearranged as

$$a - a' = b' - b\,. \tag{4.4}$$

For a pair $b \neq b'$ there can be at most one pair a, a' that satisfies (4.4). This gives at most $n(n-1)$ solutions, besides which we have the mn trivial solutions $a = a'$, $b = b'$. Consequently,

$$\sum \sigma(u)^2 \leq n(n-1) + mn\,;$$

comparing this and (4.3) we obtain (4.2). ∎

Proof of Theorem 4.1. Assume that $\mathcal{A} \subset [1, N]$ is a Sidon set, $|\mathcal{A}| = m$, and apply Theorem 4.2 to the set $\mathcal{B} = \{1, \dots, n\}$. Since $\mathcal{A} + \mathcal{B} \subset [2, N + n]$, we have

$$N + n - 1 \geq |\mathcal{A} + \mathcal{B}| \geq \frac{m^2 n}{m + n - 1}\,.$$

This gives a lower estimate of N which depends on n. The optimal value is around $m\sqrt{m} - m$. By putting $n = [m\sqrt{m}\,] - m + 1$ we obtain

$$N \geq \frac{m^2(m\sqrt{m} - m)}{m\sqrt{m}} - m\sqrt{m} + m = m^2 - 2m\sqrt{m} + m = (m - \sqrt{m})^2\,.$$

This yields a quadratic inequality for $\sqrt{m}$, from which we obtain

$$m \leq \sqrt{N} + \tfrac{1}{2} + \sqrt{\sqrt{N} + \tfrac{1}{4}} < \sqrt{N} + N^{1/4} + 1\,. \;\blacksquare$$

4.3. Theorem. *For infinitely many values of N there are Sidon sets $\mathcal{A} \subset [1, N]$ with*

$$|\mathcal{A}| \geq N^{1/2}\,. \tag{4.5}$$

Proofs of (4.5) are based on constructions of Sidon sets modulo m for certain values of m, that is, sets of residues such that $x + y \equiv u + v \pmod m$ can only hold trivially among elements of the set. The known constructions are: $p + 1$ residues modulo $p^2 + p + 1$ (Singer 1938), and p residues modulo $p^2 - 1$ (Bose 1942), where p is a power of a prime. (Proofs of these results and further information can be found in Halberstam–Roth (1966).) Both constructions are based on properties of finite fields.

We present a similar construction, which, however, applies only the existence of a primitive root modulo a prime.

4.4. Theorem. *Let p be a prime. There is a collection $a_1, \dots, a_{p-1}$ of $p - 1$ integers such that the sums $a_i + a_j$ are all different modulo $p(p-1)$.*

It is easy to see by counting the differences $a_i - a_j$ that there cannot be p such numbers.

Proof. Let g be a primitive root modulo p. For $i = 1, \dots, p-1$, let a_i be the solution of the congruences

$$a_i \equiv i \pmod{p-1}, \qquad a_i \equiv g^i \pmod{p}.$$

Our aim is to show that for arbitrary r the congruence

$$a_i + a_j \equiv r \pmod{p(p-1)} \tag{4.6}$$

has at most one solution in i, j (up to permutation).

(4.6) is equivalent to the system of two congruences

$$a_i + a_j \equiv r \pmod{p-1}, \qquad a_i + a_j \equiv r \pmod{p},$$

that is,

$$i + j \equiv r \pmod{p-1}, \qquad g^i + g^j \equiv r \pmod{p}.$$

The integers $x_1 = g^i$, $x_2 = g^j$ satisfy

$$x_1 + x_2 \equiv r \pmod{p}, \qquad x_1 x_2 \equiv g^r \pmod{p}, \tag{4.7}$$

and consequently $(x - x_1)(x - x_2)$ is the factorization of the polynomial $x^2 - rx + g^r$ modulo p. From the uniqueness of factorization we infer the uniqueness of i, j up to a permutation. ∎

Theorem 4.1 estimates $r(N)$ for Sidon's equation. With a small modification of the argument a slightly weaker estimate can be given for $R(N)$.

4.5. Definition. We call $\mathcal{A}$ a *weak Sidon set* if the equation $x+y = u+v$ has no solution with four distinct elements of $\mathcal{A}$.

4.6. Theorem. *A weak Sidon set $\mathcal{A} \subset [1, N]$ satisfies*

$$|\mathcal{A}| \le N^{1/2} + 4N^{1/4} + 11. \tag{4.8}$$

4.7. Theorem. *Let $\mathcal{A}$, $\mathcal{B}$ be nonempty finite sets of integers, $|\mathcal{A}| = m$, $|\mathcal{B}| = n$. Assume that $\mathcal{A}$ is a weak Sidon set. Then*

$$|\mathcal{A} + \mathcal{B}| \ge \frac{m^2 n}{3m + n - 1}. \tag{4.9}$$

Proof. Let $\mathcal{A}$ be a weak Sidon set. We claim that $\delta(u) \le 2$ for every $u \ne 0$, and there are at most $2m$ values of u such that $\delta(u) = 2$.

Indeed, take any $u > 0$ with $\delta(u) > 1$, and let w be the smallest element of $\mathcal{A}$ for which $w - u \in \mathcal{A}$. Take any other solution of $u = x - y$, $x, y \in \mathcal{A}$. Since the four numbers $w, w - u, x, y = x - u$ cannot be all distinct, by the minimality of w we have $y = w$. Thus there is at most one further solution, which shows $\delta(u) \le 2$, and if there is one, then the two solutions have a common element w. For any u with $\delta(u) = 2$ let $w(u)$ be this common element.

We claim that the numbers $w(u)$ are all distinct for $u > 0$. Indeed, assume that $w(u) = w(v) = w$, $u > v > 0$. Then

$$(w+u)+(w-u) = (w+v)+(w-v)$$

is a solution of the forbidden equation with four distinct elements of $\mathcal{A}$.

We have assigned distinct elements $w(u)$ of $\mathcal{A}$ to each $u > 0$ with $\delta(u) = 2$, thus there are at most m such numbers. By the symmetry $\delta(u) = \delta(-u)$ there are altogether at most $2m$ such numbers.

Let $u_1, \dots, u_k$, $k \le 2m$, be the nonzero numbers such that $\delta(u_i) = 2$. Following the argument of the proof of Theorem 4.2 we obtain

$$\sum \sigma(u)^2 \le n(n-1) + mn + \sum_{b-b'=u_i} 1\,.$$

Each u_i has at most n representations in the form $b-b'$, hence the last term is at most $kn \le 2mn$, and we have

$$\sum \sigma(u)^2 \le n(n-1) + 3mn\,.$$

The proof can be completed like that of Theorem 4.2, and the deduction of Theorem 4.6 goes along the same lines as for Theorem 4.1. ∎

5. A generalization of Sidon's equation. In this section we consider the equation

$$x_1 + x_2 + \dots + x_l = y_1 + y_2 + \dots + y_l\,. \tag{5.1}$$

A sequence in which (5.1) has no nontrivial solution is often called a B_l-sequence. The case $l = 2$ is the class of Sidon sets.

From Theorem 3.2 we know that $r(N) \ll N^{1/l}$. The special nature of equation (5.1) permits us to obtain this result by an easy counting argument. Let $\mathcal{A} \subset [1, N]$ be a solution-free set, $|\mathcal{A}| = r(N) = m$. Let us form all sums of l terms of $\mathcal{A}$, repetitions allowed. The number of these sums (order disregarded) is $\binom{n+l-1}{l}$. These sums are different integers, all less than lN. This yields

$$\frac{m^l}{l!} \le \binom{m+l-1}{l} \le lN\,,$$

and consequently

$$r(N) = m \le (ll!)^{1/l} N^{1/l}\,. \tag{5.2}$$

On the other hand, it is known that

$$r(N) \ge (1 + o(1)) N^{1/l} \tag{5.3}$$

(Bose–Chowla (1962–63), see also Halberstam–Roth (1966), Chapter II). It is undecided whether the limit

$$\lim r(N) N^{-1/l}$$

exists, except in the case $l = 2$.

This argument does not work for $R(N)$, and the general results of Section 3 give only $R(N) \ll \sqrt{N}$. We show that an $O(N^{1/l})$ estimate can be deduced for $R(N)$, albeit in a more complicated way.

5.1. Theorem. *For equation* (5.1) *we have*

$$R(N) \le (1+o(1))l^{2-1/l}N^{1/l}\,. \tag{5.4}$$

Proof. Take a set $\mathcal{A} \subset [1,N]$, $|\mathcal{A}| = M = R(N)$, in which (5.1) has no solution with $2l$ distinct integers. For positive integers j and n let $\sigma_j(n)$ denote the number of solutions of

$$n = x_1 + \ldots + x_j, \qquad x_j \in \mathcal{A}\,, \tag{5.5}$$

and let $s_j(n)$ be the number of solutions of (5.5) with the restriction that $x_1, \ldots, x_j$ are all distinct.

We write $e(t) = e^{2\pi i t}$ and we introduce the generating function

$$f(t) = \sum_{a\in\mathcal{A}} e(at)\,.$$

We have

$$f(t)^j = \sum \sigma_j(n) e(nt)\,,$$

and consequently Parseval's formula yields

$$M_j = \int_0^1 |f(t)|^{2j}\,dt = \sum_n \sigma_j(n)^2\,.$$

In particular, we have $M_1 = M$.

Consider the sum $\sum s_l(n)^2$. It counts the number of solutions of (5.1) under the restriction that $x_1, \ldots, x_l$ are distinct, $y_1, \ldots, y_l$ are distinct, but $x_i = y_j$ is allowed. By the assumption on $\mathcal{A}$ we know that some coincidence $x_i = y_j$ must indeed occur. If we fix i, j and the value of $x_i = y_j$, then equation (5.1) reduces to the corresponding equation with $l-1$ variables. The number of solutions of this equation is $\sum s_{l-1}(n)^2$. Taking into account the l possible choices of i, j and the M possibilities of x_i we find that

$$\sum s_l(n)^2 \le l^2 M \sum s_{l-1}(n)^2 \le l^2 M M_{l-1}\,. \tag{5.6}$$

Now we estimate the square mean of $\sigma_l(n) - s_l(n)$. This quantity is the number of those solutions of (5.5) in which $x_i = x_j$ holds for some $i \ne j$. For fixed i and j this is equal to the number of solutions of

$$n = 2x_1 + x_2 + \ldots + x_{l-1}\,,$$

which we shall denote by $q(n)$. We conclude that

$$\sigma_l(n) - s_l(n) \le \binom{l}{2} q(n)\,. \tag{5.7}$$

We have

$$\sum q(n)e(nt) = f(2t)f(t)^{l-2}\,,$$

and consequently, by applying Parseval's identity and Hölder's inequality we obtain

$$\begin{aligned}\sum |q(n)|^2 &= \int_0^1 |f(2t)|^2|f(t)|^{2l-4}\,dt\\ &\le \Big(\int_0^1 |f(2t)|^{2l-2}\,dt\Big)^{1/(l-1)}\Big(\int_0^1 |f(t)|^{2l-2}\,dt\Big)^{1-1/(l-1)}\\ &= M_{l-1}^{1/(l-1)}M_{l-1}^{1-1/(l-1)} = M_{l-1}\,.\end{aligned}$$

(5.7) and this inequality imply

$$\sum(\sigma_l(n) - s_l(n))^2 \le l^4 M_{l-1}\,. \tag{5.8}$$

From (5.6) and (5.8) we infer, using the triangle inequality,

$$\begin{aligned}M_l &\le (\sqrt{l^2 M M_{l-1}} + \sqrt{l^4 M_{l-1}})^2\\ &= l^2 M_{l-1}(\sqrt{M} + l)^2 \le (1+o(1))l^2 M_{l-1}M\,.\end{aligned} \tag{5.9}$$

These moments of the function f are also connected by a general property that can be deduced from Hölder's inequality, namely, for an arbitary function f the moments $\int |f|^\alpha$ form a logarithmically convex function of α. In particular, we have

$$M_{l-1} \le M_l^{(l-2)/(l-1)} M^{1/(l-1)}\,. \tag{5.10}$$

(To deduce (5.10), one can apply Hölder's inequality for $f^{2/(l-1)}$ and $f^{l(l-2)/(l-1)}$, with the exponents $l-1$ and $(l-1)/(l-2)$, respectively.)

By multiplying (5.9) and (5.10) and raising to the $(l-1)$th power we obtain

$$M_l \le (1+o(1))l^{2l-2}M^l\,. \tag{5.11}$$

A lower estimate of M_l was given in Section 3; (3.4) yields

$$M_l \ge \frac{M^{2l}}{lN}\,. \tag{5.12}$$

(5.11) and (5.12) imply

$$M \le (1+o(1))l^{2-1/l}N^{1/l}\,,$$

which was to be proved. ∎

6. A supermultiplicativity property. In the previous estimates of $r(N)$ and $R(N)$ they were often compared to a power of N. We could determine the optimal exponents only for a few equations. It is perhaps

more surprising that even the *existence* of optimal exponents, that is, of numbers γ and Γ with the property that

$$N^{\gamma-\varepsilon} \ll r(N) \ll N^{\gamma+\varepsilon}, \qquad N^{\Gamma-\varepsilon} \ll R(N) \ll N^{\Gamma+\varepsilon}$$

is uncertain. In other words, we ask the following.

6.1. Problem. Do the limits

$$\gamma = \lim \frac{\log r(N)}{\log N}, \qquad \Gamma = \lim \frac{\log R(N)}{\log N}$$

exist?

The only possibility to establish the existence of such a limit in the case when we are unable to find its value via estimates of $r(N)$ is to find a connection between values of $r(N)$ for different values of N. We are able to do this for a class of equations.

We consider an equation

$$a_1 x_1 + \ldots + a_k x_k = 0\,. \tag{6.1}$$

The condition will be connected with the partitions

$$\{1, \ldots, k\} = \mathcal{T}_1 \cup \ldots \cup \mathcal{T}_l \tag{6.2}$$

such that

$$\sum_{i \in \mathcal{T}_j} a_i = 0, \qquad j = 1, \ldots, l. \tag{6.3}$$

6.2. Definition. We call equation (6.1) *primitive* if there is a finest one among the partitions (6.2) satisfying (6.3); in other words, there is a partition such that any subset $\mathcal{T}$ of subscripts such that $\sum_{i \in \mathcal{T}} a_i = 0$ is the union of certain sets $\mathcal{T}_j$.

Write

$$S = \sum |a_i|\,.$$

6.3. Theorem. *If equation* (6.1) *is primitive, then for any integers* n_1, n_2 *we have*

$$r(Sn_1n_2) \geq r(n_1)r(n_2)\,. \tag{6.4}$$

Proof. Take maximal solution-free sets $\mathcal{A}_i \subset [1, n_i]$ and consider the set

$$\mathcal{A} = \{u + Sn_1 v : u \in \mathcal{A}_1,\ v \in \mathcal{A}_2\}\,. \tag{6.5}$$

We show that equation (6.1) has only trivial solutions in $\mathcal{A}$. Indeed, assume that the numbers

$$x_i = u_i + Sn_1 v_i$$

form a solution. (6.1) implies the congruence

$$\sum a_i u_i \equiv 0 \pmod{Sn_1}\,.$$

Since the absolute value of the left side is less than Sn_1, we infer that $\sum a_i u_i = 0$, hence also $\sum a_i v_i = 0$. These solutions must be trivial, that is, u_i and v_i are constant for $i \in \mathcal{T}_j$, thus the solution x_i is trivial as well. ∎

6.4. Remark. A typical case when this argument does not work is Sidon's equation. In a set of type (6.5) we find solutions of the equation $x + y = u + v$ as soon as both sets $\mathcal{A}_i$ have at least two elements:

$$(u_1 + Snv_1) + (u_2 + Snv_2) = (u_1 + Snv_2) + (u_2 + Snv_1)\,.$$

6.5. Theorem. *For a primitive equation the limit*

$$\gamma = \lim \frac{\log r(N)}{\log N}$$

exists.

Proof. An iteration of (6.4) yields

$$r(S^{k-1}n^k) \geq r(n)^k\,.$$

Take any $N > n$. With the choice

$$k = \left[\frac{\log N}{\log Sn}\right]$$

we have $N \geq (Sn)^k$, hence $r(N) \geq r(n)^k$, or

$$\frac{\log r(N)}{\log N} \geq \left(\frac{\log N}{\log Sn} - 1\right)\frac{\log r(n)}{\log N}\,.$$

As $N \to \infty$, this implies

$$\gamma_- = \liminf \frac{\log r(N)}{\log N} \geq \frac{\log r(n)}{\log Sn} \geq \frac{\log r(n)}{\log n} - \frac{\log S}{\log n}\,.$$

Since this holds for every n, we have

$$\gamma_- \geq \limsup \frac{\log r(n)}{\log n} - \frac{\log S}{\log n} = \limsup \frac{\log r(n)}{\log n}\,,$$

which is possible only if the upper and lower limits are equal. ∎

7. Equations in four variables. Any equation in three variables is of type (2, 1), hence it satisfies

$$Ne^{-\beta\sqrt{\log N}} \ll r(N) = R(N) \ll N(\log N)^{-\alpha} \tag{7.1}$$

with certain positive constants α, β depending on the coefficients. Equations in four variables show a more varied picture. In Section 4 we studied a particular case, Sidon's equation, and had $r(N) \sim \sqrt{N}$. The lower estimate $R(N) \gg N^{1/3}$ follows from Theorem 2.1. This can be improved in the following way.

7.1. Theorem. *For an invariant equation in four variables, the limits*

$$\gamma = \lim \frac{\log r(N)}{\log N}, \qquad \Gamma = \lim \frac{\log R(N)}{\log N}$$

exist and

$$1/2 \le \gamma = \Gamma\,.$$

At first we show that $r(N)$ and $R(N)$ are not very different.

7.2. Theorem. *For an invariant equation in four variables we have*

$$r(N) \gg R(N)e^{-\beta\sqrt{\log N}} \tag{7.2}$$

with some positive constant β, depending on the coefficients.

Proof. Write the equation as

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = 0\,. \tag{7.3}$$

Take a set $\mathcal{A} \subset [1, N]$, $|\mathcal{A}| = R(N)$, in which equation (7.3) has no solution with four distinct numbers. Any solution must satisfy $x_i = x_j$ with some $1 \le i < j \le 4$. If $a_i = -a_j$, this is a trivial solution. If $a_i \ne -a_j$, then by replacing x_j by x_i we get an equation in three variables. Thus, any nontrivial solution in $\mathcal{A}$ induces a solution to one of at most six equations in three variables, say

$$b_{j1}y_1 + b_{j2}y_2 + b_{j3}y_3 = 0, \qquad j = 1, \dots, J,\ J \le 6\,. \tag{7.4}$$

For each j let $\mathcal{B}_j \subset [1, N]$ be a set of integers in which equation (7.4) has no solution in distinct integers and

$$|\mathcal{B}_j| \gg Ne^{-\beta_j\sqrt{\log N}}\,;$$

such sets exist by Theorem 2.3. By an averaging argument we can find a set

$$\mathcal{A}' = \mathcal{A} \cap \bigcap(\mathcal{B}_j + t_j), \qquad |\mathcal{A}'| \gg |\mathcal{A}|e^{-\beta\sqrt{\log N}}\,,$$

which implies

$$r(N) \ge |\mathcal{A}'| \gg Ne^{-\beta\sqrt{\log N}}\,. \ \blacksquare$$

Next we estimate $R(N)$. For equations of type $(3, 1)$ we have the same lower estimate as stated in (7.1) for type $(2, 1)$. The other possibility is type (2, 2). We can write an equation of type (2, 2) in the form

$$aX + bY = cU + dV, \qquad a, b, c, d > 0,\ \ a + b = c + d\,. \tag{7.5}$$

7.3. Theorem. *For the equation* (7.5) *we have*

$$r(N) \gg \sqrt{N} \tag{7.6}$$

if abcd is not a square and

$$r(N) \gg \sqrt{N} e^{-\beta\sqrt{\log N}} \tag{7.7}$$

with a positive constant β, depending on the coefficients, if abcd is a square.

P r o o f. Write $a+b=S$. Take a prime $p>S$, and let $\mathcal{B}$ consist of the numbers

$$1 + x + Spx', \qquad 0 \le x, x' < p,\ x' \equiv x^2 \pmod{p}\,. \tag{7.8}$$

Clearly $|\mathcal{B}| = p$ and $\mathcal{B} \subset [1, Sp^2]$. We are going to study solutions of (7.5) in $\mathcal{B}$. Equation (7.5) reduces to

$$(ax + by - cu - dv) + Sp(ax' + by' - cu' - dv') = 0\,.$$

This yields $ax+by \equiv cu+dv \pmod{Sp}$. Since both sides of this congruence are in the interval $[0, Sp)$, they must be equal. We conclude that

$$ax + by = cu + dv\,, \tag{7.9}$$

and consequently

$$ax' + by' = cu' + dv'\,,$$

which in turn yields

$$ax^2 + by^2 \equiv cu^2 + dv^2 \pmod{p}\,. \tag{7.10}$$

The square of (7.9) is

$$a^2x^2 + 2abxy + b^2y^2 = c^2u^2 + 2cduv + d^2v^2\,, \tag{7.11}$$

while multiplying (7.10) by the equality $a+b=c+d$ we obtain

$$a^2x^2 + ab(x^2+y^2) + b^2y^2 \equiv c^2u^2 + cd(u^2+v^2) + d^2v^2 \pmod{p}\,. \tag{7.12}$$

By subtracting (7.11) from (7.12) we get

$$ab(x-y)^2 \equiv cd(u-v)^2 \pmod{p}\,. \tag{7.13}$$

If $x \equiv y \pmod{p}$, then (7.13) yields $u \equiv v$. Since x, y, u, v are all in $[0,p)$, these congruences imply $x=y$, $u=v$. A substitution into (7.9) now shows that $x=y=u=v$, and we are dealing with a trivial solution. Consequently, if this is a nontrivial solution, then $x-y \not\equiv 0 \pmod{p}$ and (7.13) is possible only if $abcd$ is a quadratic residue modulo p.

If $abcd$ is not a square, then we can choose a residue q modulo $8abcd$ so that $(q, 8abcd) = 1$ and $abcd$ is a quadratic nonresidue for every prime $p \equiv q \pmod{8abcd}$. Indeed, the theorem of quadratic reciprocity and the theorem on the quadratic character of 2 show that the Jacobi symbol $\left(\frac{abcd}{p}\right)$ depends only on the residue of p modulo $8abcd$ and both values ± 1 are possible (in fact, they occur with the same frequency). By the prime number theorem

for arithmetic progressions we can find such a prime p in the interval

$$\sqrt{\frac{N}{2S}} < p < \sqrt{\frac{N}{S}} \tag{7.14}$$

for large N. For such a prime we have $\mathcal{B} \subset [1, N]$, and consequently

$$r(N) \geq |\mathcal{B}| = p \geq \sqrt{\frac{N}{2S}}$$

for $N > N_0$.

If $abcd = t^2$ with an integer $t > 0$, then we can rewrite (7.13) as

$$t^2(x-y)^2 \equiv (cd)^2(u-v)^2 \pmod{p},$$

that is,

$$t(x-y) \equiv \pm cd(u-v) \pmod{p}.$$

If the + sign is valid, then this and (7.9) lead to

$$cSu \equiv (ac+t)x + (bc-t)y, \qquad dSv \equiv (ad-t)x + (bd+t)y. \tag{7.15}$$

If the − sign holds, then we obtain

$$cSu \equiv (ac-t)x + (bc+t)y, \qquad dSv \equiv (ad+t)x + (bd-t)y. \tag{7.16}$$

Let $\mathcal{B}'$ consist of those elements of $\mathcal{B}$ in whose representation (7.8) the condition $x < \varepsilon p$ holds, where

$$\varepsilon = \frac{1}{2S^2 + 2t}.$$

For a solution of (7.5) among elements of $\mathcal{B}'$ in both sides of the congruences in (7.15) and (7.16) there are numbers $< p$ in absolute value, hence the congruences turn into equalities:

$$cSu = (ac+t)x + (bc-t)y, \qquad dSv = (ad-t)x + (bd+t)y, \tag{7.17}$$

or

$$cSu = (ac-t)x + (bc+t)y, \qquad dSv = (ad+t)x + (bd-t)y. \tag{7.18}$$

The plan is to select a subset $\mathcal{B}'' \subset \mathcal{B}'$ in which neither system of equations has a nontrivial solution. Consider equations (7.17). Assume first that $bc \neq t$. Then the first equation of (7.17) is an equation in three variables, and there is a set $\mathcal{C}_1 \subset [1, \varepsilon p]$ such that this equation has no solution in $\mathcal{C}_1$ and

$$|\mathcal{C}_1| \gg pe^{-c\sqrt{\log p}}$$

(Theorem 2.3). If $bc = t$, then taking into account the equalities $abcd = t^2$ and $a + b = c + d$ we easily infer that $b = d$ and $a = c$. In this case the equations of (7.17) reduce to $u = x$, $v = y$ and they induce trivial solutions (recall the just stated equalities between coefficients), so we can take $\mathcal{C}_1 = [1, \varepsilon p] \cap \mathbb{N}$. Similarly we construct a set $\mathcal{C}_2$ for the equations (7.18).

By an averaging argument we can find a set $\mathcal{C}$ in the form $\mathcal{C} = \mathcal{C}_1 \cap (\mathcal{C}_2 + t)$ satisfying

$$|\mathcal{C}| \gg pe^{-c'\sqrt{\log p}}\,.$$

The set $\mathcal{B}''$ of integers, induced by formula (7.8) for $x \in \mathcal{C}$, satisfies

$$|\mathcal{B}''| = |\mathcal{C}| \gg pe^{-c\sqrt{\log p}}\,.$$

Equation (7.5) has only trivial solutions in $\mathcal{B}''$ and by choosing a prime satisfying (7.14) we obtain

$$r(N) \geq |\mathcal{B}''| \gg \sqrt{N}e^{-\beta\sqrt{\log N}}$$

as claimed. ∎

7.4. Remark. For Sidon's equation, the equations in (7.17) and (7.18) reduce to $u = x$, $v = y$ or $u = y$, $v = x$, so instead of the last argument we can simply set $\mathcal{B}'' = \mathcal{B}'$ and obtain $r(N) \gg \sqrt{N}$ although $abcd = 1$ is a square. This construction is due to P. Erdős and appeared in Stöhr (1955) (if one intends to handle only Sidon sets and not general equations, many details of the proof become superfluous). Although constructions based on finite fields or the one given in Section 9 yield sharper estimates, this construction has certain applications where it cannot be replaced by the other ones. Also, the other constructions do not seem to admit such a generalization to arbitrary equations as this one.

Now we can easily deduce Theorem 7.1.

Proof of Theorem 7.1. For primitive equations (Definition 6.2) the existence of γ follows from Theorem 6.5. The only nonprimitive equation in four variables is (a constant multiple of) Sidon's equation, for which $\gamma = 1/2$ by Theorem 4.1. Now Theorem 7.2 implies the existence of Γ and the equality $\gamma = \Gamma$, and Theorem 7.3 implies $\gamma \geq 1/2$. ∎

For equations of type $(3,1)$ Theorem 2.3 yields $\gamma = 1$, for equations of genus 2 (these must be symmetric) Theorems 3.2 and 7.3 give $\gamma = 1/2$. For equations of genus 1 and type $(2,2)$, the value of γ is unknown. We show that for this class of equations there is no universal nontrivial upper bound for γ.

7.5. Theorem. *For every $\varepsilon > 0$ there is an equation of type $(2,2)$ and genus 1 such that $\gamma > 1 - \varepsilon$.*

Proof. We take an integer $d \geq 2$ and consider the equation

$$(d+1)x + y = (d-1)u + 3v\,. \tag{7.19}$$

Let $\mathcal{B} \subset [0, d/3)$ be a set of integers such that $0 \in \mathcal{B}$ and the auxiliary equation

$$x + y + u = 3v \tag{7.20}$$

has no nontrivial solution in $\mathcal{B}$. Let $\mathcal{A}$ consist of those integers whose representation in base d contains only digits belonging to $\mathcal{B}$. We show that equation (7.19) has no nontrivial solution in $\mathcal{A}$.

Assume that x, y, u, v form a nontrivial solution of (7.19) and develop them in base d : $x = \sum x_i d^i$, etc. Let j be the least i for which x_i, y_i, u_i, v_i are not all equal. (7.19) yields

$$(d+1)x_j d^j + y_j d^j \equiv (d-1)u_j d^j + 3v_j d^j \pmod{d^{j+1}},$$

that is,

$$x_j + y_j + u_j \equiv 3v_j \pmod{d}. \tag{7.21}$$

Since $x_j, \dots, v_j$ are all in $[0, d/3)$, the congruence in (7.21) must be an equality. By definition of the set $\mathcal{B}$ this implies that they are equal, a contradiction.

By an obvious calculation we find

$$A(N) \gg N^{\log|\mathcal{B}|/\log d},$$

hence

$$\gamma \geq \frac{\log|\mathcal{B}|}{\log d}.$$

Equation (7.14) is of type $(3, 1)$, hence by Theorem 7.2 we have $\max|\mathcal{B}| \gg d\exp(-\beta\sqrt{\log d})$ with some constant β, and for sufficiently large d we can achieve $|\mathcal{B}| > d^{1-\varepsilon}$ and thus $\gamma > 1 - \varepsilon$. ∎

8. Finite and infinite sets. Besides estimating the size of finite sets, one can also ask how dense an infinite set can be without containing a solution of the equation

$$a_1 x_1 + \ldots + a_k x_k = 0. \tag{8.1}$$

Such a set $\mathcal{A}$ satisfies $A(N) \leq r(N)$ for every N. It is a difficult, and in general unsolved problem whether there is an infinite solution-free set $\mathcal{A}$ such that $A(N)$ is not much less than $r(N)$ for all, or at least for infinitely many values of N. Moser (1953) modified Behrend's construction to find an infinite set $\mathcal{A}$ that contains no three-term arithmetical progression and satisfies

$$A(N) \gg Ne^{-\beta\sqrt{\log N}}.$$

First we show that this can be done for every equation of genus 1. (The genus of an equation was defined in Definition 3.5.)

8.1. THEOREM. *Assume that equation* (8.1) *is of genus* 1.

(a) *There is an infinite set* $\mathcal{A}$ *of positive integers such that* (8.1) *has no nontrivial solution in* $\mathcal{A}$ *and*

$$A(N) \gg r(N)$$

for every N.

(b) *There is an infinite set* $\mathcal{A}$ *of positive integers such that* (8.1) *has no solution in* $\mathcal{A}$ *with* k *different numbers and*

$$A(N) \gg R(N)$$

for every N.

Proof. Write $S = \sum |a_i|$ and put $m = S+1$. For every integer i choose a set $\mathcal{A}_i$ such that

$$\mathcal{A}_i \subset ((m-1)m^{i-1}, m^i], \qquad |\mathcal{A}_i| = r(m^{i-1})$$

and equation (8.1) has no nontrivial solution in $\mathcal{A}_i$. Let $\mathcal{A} = \bigcup \mathcal{A}_i$.

We show that there is no solution in $\mathcal{A}$. Suppose that $x_1, \dots, x_k$ form a solution. Let j be the maximal number for which $\mathcal{A}_j$ contains any x_i. Let $\mathcal{S}$ be the set of those i for which $x_i \in \mathcal{A}_j$, and $\mathcal{T} = \{1, \dots, k\} \setminus \mathcal{S}$. We have

$$\Big| \sum_{i \in \mathcal{T}} a_i x_i \Big| \le m^{j-1} \sum_{i \in \mathcal{T}} |a_i|$$

and

$$\Big| \sum_{i \in \mathcal{S}} a_i (x_i - m^j) \Big| \le m^{j-1} \sum_{i \in \mathcal{S}} |a_i| \,.$$

Adding these inequalities we obtain

$$\Big| \sum_{i=1}^{k} a_i x_i - m^j \sum_{i \in \mathcal{S}} a_i \Big| \le S m^{j-1} \,. \tag{8.2}$$

If the numbers x_i form a solution, then the first term on the left side vanishes and (8.2) yields

$$\Big| \sum_{i \in \mathcal{S}} a_i \Big| \le S/m < 1 \,.$$

On the other hand, the a_i's are integers, and consequently $\sum_{i \in \mathcal{S}} a_i = 0$. Since the equation is of genus 1, we have $\mathcal{T} = \emptyset$, that is, $x_i \in \mathcal{A}_j$ for all i, which contradicts the choice of the set $\mathcal{A}_j$.

We estimate $A(N)$. Assume that $m^j \le N < m^{j+1}$. Then

$$A(N) \ge |\mathcal{A}_j| = r(m^{j-1}) \ge \frac{1}{m^2} r(m^{j+1}) \ge \frac{1}{m^2} r(N) \,.$$

(In the second step we used the inequality $r(uv) \le u r(v)$, which can be shown by cutting an interval of length uv into u equal pieces.)

This concludes the proof of case (a). Case (b) is completely analogous. ∎

There are equations for which the analog of Theorem 8.1 fails. For Sidon's equation we know that $r(N) \sim \sqrt{N}$ (Section 4), while Erdős proved that an infinite Sidon set $\mathcal{A}$ cannot satisfy $A(N) \gg \sqrt{N}$. He even proved that

$$\liminf A(N) \Big/ \sqrt{\frac{N}{\log N}} < \infty \tag{8.3}$$

(see Stöhr (1955), Halberstam–Roth (1966), Ch. II, §3)). We now present a weaker result which *may* hold for every equation, albeit we are able to prove it only for a subclass.

8.2. Theorem. *Assume that equation* (8.1) *is primitive. There is an infinite set $\mathcal{A}$ of positive integers such that* (8.1) *has no nontrivial solution in $\mathcal{A}$ and*

$$A(N) = r(N)N^{o(1)}\,. \tag{8.4}$$

This corresponds to part (a) of Theorem 8.1. We do not know any such extension of part (b).

Proof. We already know (Theorem 6.5) that the limit

$$\gamma = \lim \frac{\log r(N)}{\log N}$$

exists. Our task is to construct an infinite set $\mathcal{A}$ satisfying

$$A(N) = N^{\gamma + o(1)}\,.$$

We represent the integers in changing base system with the numbers $m_i = S(i+1)$ as bases:

$$n = \alpha_0 + \alpha_1 m_0 + \alpha_2 m_0 m_1 + \ldots, \qquad 0 \le \alpha_i \le m_i - 1\,. \tag{8.5}$$

For each i let $\mathcal{B}_i \subset [0, i]$ be a set of integers in which equation (8.1) has no solution, $0 \in \mathcal{B}_i$ and $|\mathcal{B}_i| = r(i+1)$. Such a set can be obtained from a set $\mathcal{B}_i' \subset [1, i+1]$ by translating it by its first element. Now we define the set $\mathcal{A}$ as the collection of all integers n in whose decomposition (8.5) all the digits α_i satisfy $\alpha_i \in \mathcal{B}_i$.

The fact that (8.1) has no nontrivial solution in $\mathcal{A}$ can be shown like in the proof of Theorem 6.3.

We estimate $A(N)$. Let

$$m_0 m_1 \ldots m_k \le N < m_0 m_1 \ldots m_k m_{k+1}\,.$$

For such an N we have

$$A(N) \ge |\mathcal{B}_0||\mathcal{B}_1| \ldots |\mathcal{B}_k|\,.$$

For every $\varepsilon > 0$ we have

$$|\mathcal{B}_i| = r(i+1) \ge (i+1)^{\gamma - \varepsilon} \ge m_i^{\gamma - 2\varepsilon}$$

if $i > i_0 = i_0(\varepsilon)$. We also know that

$$m_{k+1} = S(k+2) < (k!)^{\varepsilon} < (m_1 \dots m_k)^{\varepsilon}$$

for $k > k_0$. Consequently,

$$A(N) \geq \prod_{i=i_0}^{k} m_i^{\gamma-2\varepsilon} \geq N^{\gamma-2\varepsilon} m_{k+1}^{-\gamma} \prod_{i<i_0} m_i^{-\gamma} \geq N^{\gamma-4\varepsilon}$$

if N is so large that also the inequality

$$\prod_{i<i_0} m_i < N^{\varepsilon}$$

is satisfied.

We proved that $A(N) \geq N^{\gamma-4\varepsilon}$ holds for every positive ε if N is sufficiently large. Since $A(N) \leq r(N) \leq N^{\gamma+\varepsilon}$ holds by the definition of γ, (8.4) is established. ∎

Sidon's equation $x + y = u + v$ is nonprimitive, of genus 2, thus neither result of this section applies; we mentioned (see (8.3)), that the first does not hold. The second may hold (Erdős conjectures it does), but much less is known. The greedy algorithm, described in Section 2, guarantees the existence of a Sidon set satisfying

$$A(N) \geq 4^{-1/3} N^{1/3}\,.$$

By exploiting the special form of this equation, the constant is easily improved to $\sqrt{2}$, and for a long time nothing better was known. Ajtai, Komlós and Szemerédi (1981) found the following improvement.

8.3. Theorem. *There is an infinite Sidon set $\mathcal{A}$ satisfying*

$$A(N) \gg (N \log N)^{1/3}\,. \tag{8.6}$$

9. Concluding remarks. We defined three properties of invariant equations, type, genus and primitivity, which are connected with the behaviour of $r(N)$ and $R(N)$. Probably the most important is the genus. All our estimates are compatible with the following possibility (there is too little positive support to call it a conjecture):

$$\gamma = 1/\text{genus} \tag{9.1}$$

for every equation.

At the moment we do not even know the existence of γ and Γ. For an easier formulation of the following problems, however, let us pretend that they exist (the problems can be easily reformulated with lower and upper limits if this assumption is dropped).

The simplest equation for which we do not know the value of γ is $x+3y = 2u + 2v$; I do not know anything more than $\gamma \geq 1/2$ by Theorem 7.1.

By Theorem 7.1 we know that $\gamma = \Gamma$ if k, the number of variables, is at most 4, and Theorems 3.2–3.3 show that $\gamma < \Gamma$ is possible with $k = 6$. Can $\gamma < \Gamma$ happen for $k = 5$?

If (9.1) holds, then we have $\gamma \geq 1/[k/2]$ for every equation. The only unconditional result for $k \geq 5$ is $\gamma \geq 1/(k-1)$ by Theorem 2.1. Could one find an improvement of this inequality (say, $\gamma \geq 2/k$)?

Acknowledgements. I am greatly indebted to Professor Vera T. Sós; the main stimulation for this research came from her problems and remarks. I also profited much from discussions with Professor R. Freud.

References

M. Ajtai, J. Komlós and E. Szemerédi (1981), *A dense infinite Sidon sequence*, European J. Combin. 2, 1–11.

F. A. Behrend (1946), *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U.S.A. 32, 331–333.

R. C. Bose (1942), *An affine analogue of Singer's theorem*, J. Indian Math. Soc. 6, 1–15.

R. C. Bose and S. Chowla (1962–63), *Theorems in the additive theory of numbers*, Comment. Math. Helv. 37, 141–147.

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

H. Halberstam and K. F. Roth (1966), *Sequences*, Clarendon, London (2nd ed. Springer, New York, 1983).

D. R. Heath-Brown (1987), *Integer sets containing no arithmetic progression*, J. London Math. Soc. 35, 385–394.

J. Komlós, M. Sulyok and E. Szemerédi (1975), *Linear problems in combinatorial number theory*, Acta Math. Hungar. 26, 113–121.

B. Lindström (1969), *An inequality for B_2-sequences*, J. Combin. Theory 6, 211–212.

L. Moser (1953), *On non-averaging sets of integers*, Canadian J. Math. 5, 245–252.

K. F. Roth (1953), *On certain sets of integers*, J. London Math. Soc. 28, 104–109.

J. Singer (1938), *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43, 377–385.

A. Stöhr (1955), *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe*, J. Reine Angew. Math. 194, 40–65, 111–140.

E. Szemerédi (1975), *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 27, 199–245.

E. Szemerédi (1990), *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. 56, 155–158.

MATHEMATICAL INSTITUTE
HUNGARIAN ACADEMY OF SCIENCES
BUDAPEST, PF. 127
H-1364 HUNGARY
E-mail: H1140RUZ@ELLA.HU

Received on 21.1.1993
and in revised form on 25.6.1993 (2371)