Sidon sets

S.Berlov, K.Kokhas, K.Kuyumzhiyan

Problems

1 *Sidon sets in* $\mathbb{N}$

1.1. Prove that for a collection $\{a_1, a_2, \dots\}$ containing n different numbers the number of different sums of the form $a_i + a_j$, $i \leqslant j$, may be equal to any number from the interval $2n-1, C_{n+1}^2$.

1.2. The set of 20 positive integers has exactly 201 different pairwise sums (including sums of the form $a+a$). What is the minimal number of elements in the set of (positive) pairwise differences of these 20 numbers?

1.3. What is the maximal number of elements one can choose from the set $\{1, 2, \dots, 9\}$ such that all their pairwise sums $a_i + a_j$, $i < j$, would be different?

1.4. Does there exist a finite set of positive integers such that all its pairwise sums $a_i + a_j$, $i \leqslant j$, are different and this set of sums contains numbers M, $M+1$, …, $M+99$ for some $M \in \mathbb{N}$?

1.5. Does there exist a set of positive integers such that all its pairwise sums $a_i + a_j$, $i \leqslant j$, are different and this set of sums contains all numbers in the interval $\mathbb{N} \cap [M, +\infty)$ for some M?

A set A of integers is called a *Sidon set*, if the equation

$$x + y = u + v, \qquad x,\ y,\ u,\ v \in A$$

has trivial solution $\{x, y\} = \{u, v\}$ only. An analogous set of residues mod n is called a Sidon set in $\mathbb{Z}_n$. Let f_n denote the maximal possible number of elements of the Sidon set that is contained in $[1; n]$. The Sidon set $A \subset [1; n]$ is called *maximal*, if there is no Sidon set A' such that $A \subset A' \subset [1; n]$. Generally speaking, the number of elements in the maximal Sidon set can be very small with respect to f_n. Let m_n denote the minimal possible number of elements in the maximal Sidon set $A \subset [1; n]$. Finally, there exists the third point of view on extremal problems concerning Sidon sets. For an arbitrary infinite Sidon set A let $g_n = |A \cap [1; n]|$. How fast can the sequence g_n grow? It is evident that $g_n \leqslant f_n$. But the examples of "optimal" Sidon sets (see for example problem 2.7) has small intersections for different n. Therefore g_n must be much smaller than f_n.

We will deal with asymptotical inequalities. We say that the sequence a_n is asymptotically greater than b_n (and write $a_n \gtrsim b_n$) if for any $\varepsilon > 0$ and for sufficiently large n the inequality $a_n \geqslant (1-\varepsilon) b_n$ holds.

1.6. Prove that all the pairwise differences of Sidon set are different.

1.7. The set $\mathbb{N} \cap [1; 100]$ is split onto 7 subsets. Prove that at least one of them is not a Sidon set.

1.8. Prove that there exists a Sidon set $A \subset [1; 25\,000]$ such that $|A| = 100$.

1.9. A Sidon set A consists of m elements, B is an arbitrary set of n numbers, $A + B$ is a set of all sums $a + b$, where $a \in A$, $b \in B$. Prove that

$$|A + B| \geqslant \frac{m^2 n}{m + n - 1}.$$

1.10. Prove that $f_n \gtrsim \sqrt{n/2}$.

1.11. Prove that $f_n < \sqrt{2}\sqrt{n} + 1$.

1.12. Prove that $f_n < \sqrt{n} + \sqrt[4]{n} + 1$.

1.13. Prove that $f_n \gtrsim \sqrt{n}$.

1.14. Prove that $m_n \geqslant \sqrt[3]{n}$.

1.15. Prove that $m_n \leqslant C\sqrt[3]{n \log n}$.

1.16. Prove that there exists an infinite Sidon set A, such that $g_n \geqslant \sqrt[3]{n}$.

1.17. Prove that there exists (or construct) an infinite Sidon set, such that its sequence g_n grows faster than in the previous problem. The record growth now is $g_n \gtrsim n^{\sqrt{2}-1}$.

2 *Sidon sets in* $\mathbb{Z}_n$

2.1. Prove that there exists a Sidon set in $\mathbb{Z}_N$ that has at least $\sqrt[3]{N}$ elements.

2.2. Let $m, n \in \mathbb{N}$, $n \geqslant m/2$. Let $A \subset \mathbb{N} \cap [1;m]$, $|A| = n$. Prove that

$$(A + A) \bmod m = \{0, 1, \dots, m-1\}.$$

2.3. Let p be a prime number, and $\{a_1, a_2, \dots\}$ be a set of n different residues mod p. Prove that the number of different mod p pairwise sums $a_i + a_j$, $i \leqslant j$, is not less than $\min(p, 2n-1)$.

2.4. The set of integers in $[1; 2n]$ is split in two groups of n numbers each. Prove that the sets of pairwise sums mod $2n$ of each group coincide (the sets of pairwise sums contain the sums of the form $a + a$).

The optimal example of the "biggest" Sidon set in $\mathbb{Z}_n$ belongs to J. Singer. Two following problems describe this example. We need a prime number p for the construction. We choose $p = 5$.

2.5. Consider a formal element z, such that

$$z^3 + 3z + 2 = 0.$$

Due to this relation we can transform an arbitrary polynomial (with respect to the indeterminate z) to the polynomial of degree at most 2. Prove that the set of polynomials of the form $a + bz + cz^2$, where a, b, c are residues modulo 5, consists of the elements 0, z, z^2, z^3, z^4, $\dots$, z^{124}.

2.6. For each residue s (modulo 5) choose nonnegative integer k, such that $z^k = z + s$. Consider a set consisting of these 5 numbers and 0. Prove that this is an example of 6-element Sidon set in $\mathbb{Z}_{31}$.

2.7. Let p be a prime number. Prove that there exist $p-1$ nonegative integers d_1, d_2, $\dots$, d_{p-1}, such that all their pairwise sums $d_i + d_j$, $i \leqslant j$ are different mod $p(p-1)$.

2.8. Let p be a prime number. Prove that there exist p positive integers d_1, d_2, $\dots$, d_p, such that all their pairwise sums $d_i + d_j$, $i \leqslant j$, are different modulo $p^2 - 1$.

Solutions

1.1. This problem was offered at the Summer Conference in 2002.

Using mathematical induction, we shall prove that the number of diferent pairwise sums of the collection of n different integers may be any integer of the segment $[2n-1, C_{n+1}^2]$. Base $n = 2$ is trivial.

Step of induction. Suppose that the statement is true for $n = k$. Prove it for $n = k+1$. Let $a \in [2k-1, C_{k+1}^2]$. Consider 2 cases:

Case 1. $2k - 1 \leqslant a \leqslant 3k - 3$. The required set is $A = [1, k] \cup \{a - k + 2\}$. It's clear that the set of pairwise sums of the set A is $B = [3, a + 2]$ and the set B has a elements.

Case 2. $3k - 2 \leqslant a \leqslant C_{k+1}^2$. By the induction hypothesis there exists a collection A, such that the set of its pairwise sums has $a - k$ elements. Let $c > 2 \max A$, $B = A \cup \{c\}$. Then the set of pairwise sums of the collection B has a elements ($a - k$ sums of the initial collection and k sums with c).

1.2. Answer: 100. This problem was offered at the SPb olympiad-1996. Its author is S. Ivanov. We cite the solution from [1].

Suppose that the number of different differences is less than 100.

Write in an arbitrary order all the differences $a - b$, where a and b are arbitrary numbers from the collection, $a > b$. The number of these differences is equal to the number of pairs of 20 integers, i. e. 190. These differences have less than 100 different values, therefore during the process of writing at least 90 times the next difference coincides with one of the previous. So there exist more than 90 identities of the form $a - b = c - d$, where a, b, c and d are the numbers from the collection with $a > b$ and $c > d$. For each equality $a - b = c - d$ we put into correspondence an equality of sums: $a + d = b + c$. Then each equality $a + d = b + c$ corresponds to at most two identities with differences, exactly to those of the identities $a - b = c - d$, $b - a = d - c$, $a - c = b - d$ and $c - a = d - b$, which have positive terms.

We obtain more than 45 different identities with sums of more than 90 identities with differences (the identities are different if they cannot be transformed one into another by permutations of the left and right hand sides and by permutations of summands).

Prove that it leads to contradiction. Totally we have exactly 210 pairwise sums (190 sums with different summands and 20 sums where a number is summed with itself). Under given conditions they take 201 different values. I.e. they can be split into 201 groups so that in each group all the sums are equal, and in different groups the sums are different. Each group of k equal sums gives us $k(k-1)/2$ identities of the form $a+b=c+d$.

Hence the total number of identities between differences is equal to $\sum_{i=1}^{201} k_i(k_i-1)/2$, where $k_1, \ldots, k_{201}$ are the quantities of sums in groups. Notice that k_i are integers and $\sum k_i = 210$. It is easy to understand that this sum reaches its maximal value when all the values k_i but one are equal to 1. Indeed, if $k_i \geqslant k_j > 1$, then we can increase our sum by changing k_i and k_j to k_i+1 and k_j-1. It follows from the equality

$$\frac{(k_i+1)k_i}{2} + \frac{(k_j-1)(k_j-2)}{2} = \frac{k_i(k_i-1)}{2} + \frac{k_j(k_j-1)}{2} + k_i - k_j + 1.$$

But for $k_1 = \cdots = k_{200} = 1$ and $k_{201} = 10$ the sum $\sum_{i=1}^{201} k_i(k_i-1)/2$ is equal to 45. It means that the quantity of equalities in sums is not greater than 45. Contradiction.

Now we have to show an example of 20 integers that have 201 pairwise sums and 100 differences. Put $C = 10^{11}$ and consider a collection of integers $C + 10^k$ and $C - 10^k$, where $k = 1, \ldots, 10$. This collection has exactly 201 pairwise sums: $2C$, $2C \pm 2 \cdot 10^k$ and $2C \pm 10^k \pm 10^m$ $(k \neq m)$. Their differences are numbers $2 \cdot 10^k$ (10 values), $10^k - 10^m$ with $k > m$ (45 values) and $10^k - 10^m$ with $k > m$ (also 45 values), totally 100 different values.

1.3. This problem is taken from the Canadian olympiad-2002. Answer: 5 integers. Example: 1, 2, 3, 5, 8. If 6 integers are taken, they determine 15 pairwise sums. But all the pairwise sums can take 15 values: 3, 4, ..., 17. Notice that 3 and 17 may be got in the only way: $3 = 1 + 2$ and $17 = 8 + 9$. It means that 1, 2, 8 and 9 have to be chosen. But it is impossible because $1 + 9 = 2 + 8$.

1.4. This problem is from the 15th Ural Tournament of Young Mathematicians. Its author is S. Berlov. Answer: such a set exists.

Using induction by n we shall prove that there exists a Sidon set, containing n consequtive integers among its pairwise sums. Base is obvious. Step of induction: from $n-1$ to n. Take a Sidon set satisfying the induction hypothesis, let m be its maximal element. Let us add $2n$ to all its elements. It will remain a Sidon set, but all its pairwise sums will increase by $4m$, and they will still contain $n-1$ consecutive integers $2m+k$, $2m+k+1$, ..., $2m+k+n-2$. Now append two more integers — 1 and $2m+n-3$ — to our set. We've built a set, such that its pairwise sums contain n consecutive integers. It is a Sidon set, because all the shifted sums of the old set are different, pairwise sums containing 1 are less than all these sums and sums containing $2m+n-3$ are greater.

1.5. Answer: such a set does not exist. Let n be a sufficiently large integer and k be a number of elements of our set in the segment $[1; n]$. Then $k(k+1)/2 \geqslant n - \text{const}$, i.e. $k \gtrsim \sqrt{2n}$, which contradicts the estimation of the problem 1.12.

1.6. It's clear.

1.7. This is problem 4.7 from [3]. One of these sets contains at least 15 elements. They determine at least $15 \cdot 14/2 = 105$ (positive) differences. Hence there are two coinciding differences (all the differences are not greater than 99) and this set is not a Sidon set.

1.8. This problem of F.Petrov and D.Dzhukich was included in the IMO 2001 Shortlist. But 50 years before it was solved by P.Erdös.

Let $p = 101$. Consider the numbers $2kp + (k^2 \bmod p)$, $k = 1, \ldots, p$. Let us check that all their pairwise differences are different. Indeed, if

$$2kp + (k^2 \bmod p) + 2\ell p + (\ell^2 \bmod p) = 2mp + (m^2 \bmod p) + 2np + (n^2 \bmod p)\,,$$

then necessarily $k + \ell = m + n$, and $k^2 + \ell^2 \equiv m^2 + n^2 \pmod p$. Therefore $k + \ell \equiv m + n \pmod p$, $k\ell \equiv mn \pmod p$, and by Viete theorem $\{k, \ell\} = \{m, n\}$.

1.9. [10]. Let $\sigma(k)$ denote the number of solutions of the equation

$$a + b = k, \qquad a \in A,\ b \in B\,.$$

It is clear that $\sum_k \sigma(k) = |A| \cdot |B| = mn$. By the inequality between quadratic and arithmetic means we have

$$\sum_k \sigma(k)^2 \geqslant \frac{m^2 n^2}{|A+B|}\,. \tag{1}$$

The sum in the l.h.s. counts the number of 4-tuples a, $a' \in A$, b, $b' \in B$, such that $a + b = a' + b'$, or

$$a - a' = b' - b\,.$$

If $b = b'$ we have $a = a'$, and we obtain mn different solutions of the equation. For $b \neq b'$ at most one pair a, a' satisfies this equation due to the problem 1.6, and we obtain at most $n(n-1)$ solutions. Hence

$$\sum_k \sigma(k)^2 \leqslant n(n-1) + mn\,.$$

Combining with the inequality (1) we obtain a required inequality.

1.10. [6]. Similarly to the problem 1.8.

1.11. [6] Let $|A| = k$. The differences of the form $a - b$, $a > b$, $a, b \in A$ are different and belong to the interval $[1; n-1]$. The number of differences is $k(k-1)/2$. Therefore $k(k-1)/2 \leqslant n-1$, and $k \leqslant \sqrt{2n - \frac{7}{4}} + \frac{1}{2} < \sqrt{2n} + 1$.

1.12. We have two solution of this problem.

Solution 1 ([7]) . Let $1 \leqslant a_1 < a_2 < \cdots < a_r \leqslant n$ be given numbers. Then all the differences $a_i - a_j$ are different. We call the number $i - j$ an *order* of the difference $a_i - a_j$. All the differences of order q can be split into chains of the form

$$a_\alpha - a_\beta,\ a_\beta - a_\gamma,\ \ldots, \qquad \alpha - \beta = \beta - \gamma = \ldots = q\,.$$

The sum of all differences in every chain is less than n. Therefore the sum of all differences of order q is less than qn. Then the sum of all differences which order does not exceed m is less than $\frac{1}{2}m(m+1)n$.

The number of differences of order k equals $r - k$, because every such difference has a form $a_{i+k} - a_i$, where $1 \leqslant i \leqslant r - k$. Therefore the number of differences which order does not exceed m, $1 \leqslant m < r$, equals

$$mr - \frac{1}{2}m(m+1) = ms\,,$$

where $s = r - \frac{1}{2}(m+1)$. All these differences are pairwise different, hence their sum is not greater than $\frac{1}{2}ms(ms+1) > \frac{1}{2}m^2s^2$. So we have

$$\frac{1}{2}m^2s^2 < \frac{1}{2}m(m+1)n\,.$$

After cancelling m we have

$$s < \sqrt{1 + \frac{1}{m}}\,\sqrt{n} < \Big(1 + \frac{1}{2m}\Big)\sqrt{n}\,.$$

Therefore

$$r < \frac{1}{2}(m+1) + \Big(1 + \frac{1}{2m}\Big)\sqrt{n}\,.$$

Now choose $m = [\sqrt[4]{n}] + 1$, and we obtain required inequality.

Solution 2 ([10]). Let $A \subset [1, N]$ be a Sidon set consisting of m numbers and let $B = \{1, 2, \ldots, n\}$. Then $A + B \subset [2, N+n]$ and we have by the statement of the problem 1.9

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

Let $n = [m\sqrt{m}] - m + 1$:

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

Now solve this square inequality with respect to the variable m and we obtain

$$m \leqslant \sqrt{N} + \frac{1}{2} + \sqrt{\sqrt{N} + \frac{1}{4}} < \sqrt{N} + N^{1/4} + 1\,.$$

1.13. It follows from 2.7.

1.14. In order the set A to be maximal it is necessary that for any number $d \leqslant n$, $d \notin A$ we have one of the representations

$$\begin{aligned} d &= a + b - c, \quad \text{where } a \neq b \\ 2d &= a + b, \\ d &= 2a - c\,. \end{aligned}$$

where $a,\ b,\ c \in A$. The number of sums of the first type is at most $m_n^2(m_n-1)/2$, the number of sums of the second type is at most $m_n(m_n-1)/2$, the number of sums of the third type is at most $m_n(m_n-1)$. The number of numbers that we try to append to our set does not exceed the total number of sums. Therefore

$$n - m_n \leqslant \frac{m_n^2(m_n-1)}{2} + \frac{m_n(m_n-1)}{2} + m_n(m_n-1)\,.$$

If $m_n \geqslant 3$ then it easy to check that the r.h.s. of the last inequality is less than $m_n^3 - m_n$.

1.15. See [9].

1.16. You can take the sequence that is constructed by the greedy algorithm.

1.17. The record construction is described in [8].

2.1. Similarly to 1.14.

2.2. This is problem 4.5 from [3]. Let k be an arbitrary residue modulo m. Consider $2n$ numbers

$$a_1,\ a_2,\ \ldots, a_n,\ \ldots, k-a_1,\ k-a_2,\ \ldots,\ k-a_n\,.$$

First n of these numbers have different resudues modulo m by the problem statement, therefore the last n numbers have different residues too. But here we have $2n > m$ numbers, hence for some i and j we have $a_i \equiv k - a_j \pmod{m}$. Then $a_i + a_j \equiv k \pmod{m}$.

2.3. It follows from Cauchy–Davenport theorem: Let p be a prime number. Then for any two sets A and $B \subset \mathbb{Z}_p$ we have

$$|A+B| \geqslant \min\{p, |A|+|B|-1\}\,.$$

P r o o f of the theorem. The case $|A|+|B| > p$ is easy, we leave it to the reader. So let us suppose that $|A|+|B| \leqslant p$. Let for some sets A and B we have a reverse inequality

$$|A+B| \leqslant |A|+|B|-1\,. \tag{$*$}$$

Choose the pair of sets that have minimal value $|A+B|$, and between these pairs choose the pair for which the smaller set (w.l.o.g. A) contains minimal number of elements. We may suppose that $|A| \geqslant 2$.

Remark that if we will shift one of the set (for example if we will consider the set $A+c$ instead of A, where $c \in \mathbb{Z}_p$) then the set $A+B$ will also be shifted by c. Particularly, the number of elements in $A+B$ will not change.

Prove that there exists a shift of the set A such that $A \cap B \neq \varnothing$, and $A \not\subset B$. Suppose for any shift of the set A this is not the case, i.e. if the shifted set A intersects with B then it contains in B. Then consider a case of such intersection. Let $a,\ b \in A \cap B$ and $A \subset B$. Now shift the set A by $b-a$. The point a moves to b, and hence after the shift the sets will intersect. If we have $A \subset B$ again, then the point b belongs to both sets. Consider one more shift by $b-a$ and so on. If every time we will have that the shifted set A is a subset of B, then we will conclude that all the points

$$a,\ b,\ b+(b-a),\ b+2(b-a),\ b+3(b-a), \ldots$$

(arithmetic operations are modulo p) belong to the set B. This is impossible because the set of these points coincides with $\mathbb{Z}_p$.

So we can shift the set A in such a manner that the sets A and B would intersect and $A \not\subset B$. Remark that if $A_1 = A \cap B$ and $B_1 = A \cup B$ then $A_1 + B_1 \subset A + B$, i.e. $|A_1+B_1| \leqslant |A+B|$; moreover $|A_1|+|B_1| = |A|+|B|$. Thus the pair of sets A_1, B_1 satisfies the inequality ($*$). But $|A_1| < |A|$, in contradiction with the choise of A.

2.4. The problem is from the SPb olympiad – 1996, its author is S.Ivanov. We cite the solution from the book [2].

Dealing with residues modulo $2n$ we will always take $2n$ instead of 0.

Let the numbers a and b (possibly, equal) belong to the same group. It is sufficient to find two numbers in the second group such that their sum has the same residue modulo $2n$ as $(a+b)$. Split all the sets from 1 to $2n$ on pairs in the following manner. Let $c = (a+b)/2$. If c is integer then consider the following $n+1$ pairs (arithmetic operations modulo $2n$):

$$(c,c),\ (c-1,c+1),\ \ldots, (c-n+1, c+n-1),\ (c-n, c+n)\,.$$

The sum of numbers in each pair is congruent modulo $2n$ to $(a+b)$ and any two pairs do not intersect. One of these pairs is our initial pair

$$(a,b) = \Big(c + \frac{a-b}{2}, c - \frac{a-b}{2}\Big)\,.$$

We have n more pairs here and the first group of numbers contains $n-2$ more numbers except a and b, therefore one of pairs consists of two required numbers of the second group.

The case when c is not integer (a half of integer) is analogous.

2.5. Direct calculation shows that $z^{31}=3$.

2.6. Similarly to 2.8.

2.7. [10] Let g be a primitive root modulo p. For $i=1, 2, \ldots, p$ let a_i denote a solution of the system of equations

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

This is a required set of numbers. To prove this let us check that for every r the congruence

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

has at most one solution (i,j) up to a permutation. The congruence is equivalent to the system of two conguences

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

i.e.

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

Then the numbers $x_1 = g^i$, $x_2 = g^j$ satisfy the relations

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

and therefore are uniquely defined $\pmod{p}$. So the pair (i,j) is also uniquely defined.

2.8. [4]. Let c be a primitive root in F_{p^2}. We will denote the elements of F_p by $1, \ldots, (p-1), p$. For every i let d_i be a positive integer that satisfies the relation

$$c^{d_i} = c + i\,.$$

The set of numbers d_i is a required Sidon set. Indeed, let us suppose that $d_i + d_j = d_k + d_\ell \pmod{p^2-1}$. Then in F_{p^2} we have an equality $c^{d_i}c^{d_j} = c^{d_l}c^{d_\ell}$, i.e.

$$(c+i)(c+j) = (c+k)(c+\ell)$$

or

$$c(i+j-k-\ell) = k\ell - ij\,.$$

Since $c \notin F_p$ we conclude that $i+j-k-l=0$ and $k\ell - ij = 0$. But then $\{i,j\} = \{k,\ell\}$.

References

[1] *Berlov S., Ivanov S., Karpov D., Kokhas K., Petrov F., Khrabrov A.* Problems of St. Petersburg mathematical olympiad. 2000. St-Petersburg, 2000. [in Russian]

[2] *Berlov S., Ivanov S., Kokhas K.* St. Petersburg matematical olympiads. St.Petersburg.: Lan' Publ. House, 2003. [in Russian]

[3] *Konyagin S. V., Tonoyan G. A. et al.* Foreign mathematical olympiads. Moscow.: Nauka, 1987. [in Russian]

[4] *Bose R.C., Chowla S.* Theorems in the additive theory of numbers. // Comment. Math. Helv. 1962/63. Vol. 37. P. 141–147.

[5] *Katz N.H., Nao T.* A new bound on partial sum-sets and difference-sets, and applications to the Kakeya conjecture // arxiv.org

[6] *Kolountzakis M.* Problems in the additive number theory of general sets, I. Sets with didstinct sums. // http://www.math.uiuc.edu/˜ kolount/surveys.html

[7] *Lindsröm B.* An inequality for B_2-sequences. Journ. of Comb. Theory, V. 6. P. 211–212.

[8] *Ruzsa I.* An infinite Sidon sequence. // J. Number Theory. 1998. Vol. 68. P. 63–71.

[9] *Ruzsa I.* A small maximal Sidon set // Ramanujan J. 1998. Vol. 2. P. 55–58.

[10] *Ruzsa I.* Solving of linear equation in a set of integers, I. Acta Arithmetica. 1993. Vol. LXV. N. 3. P. 259–282.

[11] Singer J. A theorem in finite projective geometry and some applications to number theory // Trans. Amer. Math. Soc. 1938. Vol. 43 P. 377–385.