Special Classes of Shifted k-dimensional Vectors Modulo a Prime

Borbély József, Csala-Takács Éva

Óbudai Egyetem, Székesfehérvár, Hungary

borbely.jozsef@amk.uni-obuda.hu

csala.takacs@amk.uni-obuda.hu

***Abstract*— In this paper we will discuss a problem concerning vectors with integer coordinates modulo a prime number. We will proceed from a problem that was set in the Kürschák competition in 2018, and we will give a strong generalization of it. We will also formulate some open questions.**

I. INTRODUCTION

There are a lot of standard linear algebraic questions, how many vectors one can choose in the k-dimensional plane, if one expects some prescribed properties to be fulfilled But one can also ask similar questions with some number theoretical restrictions. In this paper we will discuss the generalization of a Kürschák problem. Throughout the whole paper k will denote a positive integer, and k will denote a prime number.

II. A KÜRSCHÁK PROBLEM FROM 2018 AND ITS GENERALIZATION

We formulate the second problem of the Kürschák competition as a theorem:

Theorem 1: *Let p be an odd prime number, and let* $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ *be distinct three-dimensional vectors with integer coordinates, whose lengths equal p. If for every 1≤i<j≤n there exists an integer t such that 0<t<p and all the coordinates of the vector* $\boldsymbol{v_i}$*-t*$\boldsymbol{v_j}$ *are divisible by p, then n (which is the number of the vectors) is at most 6.*

We will prove a generalization of this problem in every finite dimensional case.

We formulate the generalization as a theorem:

Theorem 2: *Let p be an odd prime number, and let k be a positive integer, and let* $\boldsymbol{v_1}, \boldsymbol{v_2}, \ldots, \boldsymbol{v_n}$ *be distinct k-dimensional vectors with integer coordinates, whose lengths equal p. If for every 1≤i<j≤n there exists an integer t such that 0<t<p and all the coordinates of the vector* $\boldsymbol{v_i}$*-t*$\boldsymbol{v_j}$ *are divisible by p, then n (which is the number of the vectors) is at most 2k.*

Obviously, Theorem 2 is a generalization of Theorem 1. The result of Theorem 1 follows from the one of Theorem 2, if we consider the case k=3.

It is easy to see that in Theorem 2 the two parameters p and k can be chosen independently from each other.

The condition $\mathbf{v_i}$-t$\mathbf{v_j}$ being divisible by p means, that the vectors $\boldsymbol{v_j}$ and $\boldsymbol{v_i}$ are in some sense multiples of each other (in the sense of calculating modulo p).

Before proving Theorem 2, we need some lemmas and some definitions.

III. THE CAUCHY-SCHWARZ INEQUALITY

Lemma 1: *Let k be a positive integer. For any k-dimensional vectors **u** and **v** holds the inequality*

$$|\boldsymbol{uv}| \leq |\boldsymbol{u}||\boldsymbol{v}|$$

Lemma 1 is called the Cauchy-Schwarz inequality. In other words we can say, that for any vectors **u**=(u_1, u_2, ..., u_k) and **v**=(v_1, v_2, ..., v_k) with real coordinates holds the inequality

$$|u_1v_1+u_2v_2+\ldots+u_kv_k| \leq$$

$$\leq \sqrt{u_1{}^2+u_2{}^2+\cdots+u_k{}^2} \cdot \sqrt{v_1{}^2+v_2{}^2+\cdots+v_k{}^2}$$

Equality occurs in the Cauchy-Schwarz inequality if and only if the vectors **u** and **v** are multiples of each other, i.e. there exists a real number r such that one of the equalities r**u**=**v** or r**v**=**u** holds.

Now we will define linear dependence and independence.

IV. LINEAR DEPENDENCE AND INDEPENDENCE

One of the most important terms in linear algebra is the one of linear independence. We will define linear independence and dependence to be able to prove Theorem 2.

Definition : *Let V be a vector space over the field F. The vectors $\boldsymbol{v_1}$, $\boldsymbol{v_2}$, ..., $\boldsymbol{v_k}$ form a linearly independent system of vectors, if for the elements t_1, t_2, ..., t_k of F the equality $t_1\boldsymbol{v_1}$+$t_2\boldsymbol{v_2}$+...+ $t_k\boldsymbol{v_k}$= $\boldsymbol{0}$ implies that t_1=t_2=...= t_k=0. If a system of vectors is not linearly independent, we call it linearly dependent.*

We will use also the following well-known theorem:

Theorem 3: If the vectors $\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_n}$ with *k coordinates from a vector space over the field F are linearly independent, then n≤k.*

In order to have a more simple formulation we will use the (standard) terminology that the vectors **u**=(u_1, u_2, ..., u_k) and **v**=(v_1, v_2, ..., v_k) are perpendicular if and only if

u_1v_1+u_2v_2+...+u_kv_k = $\mathbf{uv} = \mathbf{0}$.

We need another lemma:

Lemma 2: *If the nonzero vectors $\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_k}$ of a vector space over the field F are pairwise perpendicular, then they form a linearly independent system of vectors in this space.*

Proof of Lemma 2:

Let t_1, t_2, ..., t_k elements of F such that

$t_1\mathbf{v_1}$+$t_2\mathbf{v_2}$+...+ $t_k\mathbf{v_k}$= $\mathbf{0}$

holds. Let us multiply this equality by $\boldsymbol{v_1}$, then we get that

$t_1\mathbf{v_1}\mathbf{v_1}$ = 0.

$\mathbf{v_1}\neq \mathbf{0}$, therefore t_1 = 0. A similar argumentation shows that

t_1=t_2=...= t_k=0, thus the vectors are linearly independent **QED**.

Now we are able to prove Theorem 2.

V. PROOF OF OUR MAIN THEOREM

Let **u**=(u_1, u_2, ..., u_k) and **v**=(v_1, v_2, ..., v_k) be distinct k-dimensional vectors with integer coordinates and with length p. Suppose that there is an integer t such that 0<t<p and all the coordinates of the vector **u**-t**v** are divisible by p. That means that all the numbers u_i-tv_i are divisible by p. Thus the sum

$(u_1 - \mathrm{t}v_1)^2$+$(u_2 - \mathrm{t}v_2)^2$+...+$(u_k - \mathrm{t}v_k)^2$

is divisible by p^2.

Now, using the condition, that |u|=p and|v|=p we have

$(u_1 - \mathrm{t}v_1)^2$+$(u_2 - \mathrm{t}v_2)^2$+...+$(u_k - \mathrm{t}v_k)^2$=

=${u_1}^2$+${u_2}^2$+ ... ${u_k}^2$+ $t^2({v_1}^2 + {v_2}^2 + \dots {v_k}^2)$-

-2t$(u_1v_1 + u_2v_2 + \dots + u_kv_k)$ =

= p^2 + t^2p^2 + -2t$(u_1v_1 + u_2v_2 + \dots + u_kv_k)$.

The number $p^2 + t^2p^2$ is divisible by p^2, therefore

2t$(u_1v_1 + u_2v_2 + \dots + u_kv_k)$ must be divisible by p^2 as well.

The numbers 2t and p are coprimes because p is odd and 0<t<p. That means that the number

$$u_1v_1 + u_2v_2 + \dots + u_kv_k$$

is divisible by p^2.

Now we will use the Cauchy-Schwarz inequality.

We know that

$|u_1v_1$+u_2v_2+...+$u_kv_k|$≤

$\leq\sqrt{{u_1}^2 + {u_2}^2 + \cdots + {u_k}^2}\cdot\sqrt{{v_1}^2 + {v_2}^2 + \cdots + {v_k}^2}$.

The right hand side of the inequality equals p^2, because the length of the vectors u and v is p. Thus the expression

u_1v_1+u_2v_2+...+u_kv_k

is divisible by p^2 and its absolute value cannot be greater than p^2. So we have two possibilities:

Case 1:

$|u_1v_1+u_2v_2+...+u_kv_k|=0$

Case 2:

$|u_1v_1+u_2v_2+...+u_kv_k|= p^2$.

In Case 1 the vectors u and v are perpendicular, in Case 2 there must be a real number r such that one of the equalities r**u=v** or r**v=u** holds. **u** and **v** are different vectors, their length is the same, and for some real number r one of the equalities r**u=v** or r**v=u** holds, therefore in Case 2 we get **u** = - **v**.

Thus if we have the vectors distinct $\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}$ k-dimensional vectors, which corespond to the conditions of Theorem 2, then for every 1≤i<j≤ one of the following conditions holds:

Condition 1: $\boldsymbol{v_i}$ and $\boldsymbol{v_j}$ are perpendicular

Condition 2: $\boldsymbol{v_i}+\boldsymbol{v_j} = \mathbf{0}$

We will show that in this case n ≤ 2k.

Let us choose a linearly independent subset of the set $\{\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}\}$ with the maximal number of elements, let this subset be $\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}$. Due to Theorem 3 the inequality j ≤ k holds.

Let **v** be an element of the set

H = $\{\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}\} \setminus \{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}$.

If the vector **v** was perpendicular to all the elements in the set $\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}$, then the set $\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}, \mathbf{v}\}$ would be a linearly independent set of vectors, but that would contradict to the maximality of the subset

$\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}$.

Therefore for every element **v** of H there is a **v*** vector in the set $\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}$ such that **v+v*=0**. Because for every vector **v** in the whole vector space there is exactly one vector **v*** such that **v+v*=0**, this implies that

$|H| \leq |\{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}| = j \leq k$.

Thus we have

$n = |\{\mathbf{v_1}, \mathbf{v_2}, \dots, \mathbf{v_n}\}| = |H \cup \{\mathbf{w_1}, \mathbf{w_2}, \dots, \mathbf{w_j}\}| \leq$

$\leq k + k = 2k$, as desired.

Thus we proved of the statement of Theorem 2 **QED**.

VI. SOME QUESTIONS CONCERNING THEOREM 2

Naturally arises the question whether one can choose exactly 2k vectors with the prescribed conditions. The answer is yes. Let us take the following vectors:

$\boldsymbol{g_1}$=(p, 0, 0, ..., 0, 0)

$\boldsymbol{g_2}$=(0, p, 0, ..., 0, 0)

...

...

...

$\boldsymbol{g_k}$=(0, 0, 0, ..., 0, - p)

$\boldsymbol{f_1}$=(- p, 0, 0, ..., 0, 0)

$\boldsymbol{f_2}$=(0, - p, 0, ..., 0, 0)

...

...

...

$\boldsymbol{f_k}$=(0, 0, 0, ..., 0, - p)

It is easy to see that for every 1 ≤ j ≤k the equality

$\boldsymbol{g_j} = -\boldsymbol{f_j}$ and $|\boldsymbol{g_j}| = |\boldsymbol{f_j}|$ = p hold,

and for every 1 ≤ i , j ≤k we have

$\boldsymbol{g_j}\boldsymbol{f_j}$=0.

That means that the estimate is tight.

But as one could notice in our construction we have only vectors whose (k-1) coordinates are zeros.

If k=2z is an even number and p is a prime number that can be written as a sum of two squares, i.e.

p = $a^2 + b^2$ for some integers a and b, then let us define our vectors in the following way:

$\boldsymbol{q_1}$=(a, b, 0, 0, 0, 0, ... 0, 0, 0, 0)

$\boldsymbol{q_2}$=(0, 0, a, b, 0, 0,...., 0, 0, 0, 0)

...

...

...

$\boldsymbol{q_z}$=(0, 0, 0, ..., 0, 0, 0, 0, a, b),

$\boldsymbol{q_{z+1}}$=(b, -a, 0, 0, 0, 0, ... 0, 0, 0, 0)

$\boldsymbol{q_{z+2}}$=(0, 0, b, -a, 0, 0,...., 0, 0, 0, 0)

...

...

...

$\boldsymbol{q_{2z}}$=(0, 0, 0, ..., 0, 0, 0, 0, b, -a), and let us take $\boldsymbol{q_{2z+j}} = - \boldsymbol{q_j}$ for every $1 \leq j \leq 2z$.

It is easy to see that this construction is also appropriate.

But generally one can ask, whether one can find constructions with vectors which does not contain zero as a coordinate? If yes, then for which prime numbers p is it possible to do it?

Another way to generalize the problem would be omitting the condition that p is a prime number. In this case we would have to consider a lot more diviibility relations (see our proof).

A third way to investigate this problem would be to extend (or modify) the condition concerning the lengths of our vectors.

The generalizations above would be very difficult and interesting, and probably one should use deep number theoretical tools to handle them.

References

[1] Freud, Számelmélet, Nemzeti Tankönyvkiadó, 2006.

[2] Kuros, Felsőbb Algebra, Tankönyvkiadó vállalat, 1968.