ISSN 0001-4346, Mathematical Notes, 2020, Vol. 107, No. 2, pp. 238–246. © Pleiades Publishing, Ltd., 2020.
Russian Text © The Author(s), 2020, published in Matematicheskie Zametki, 2020, Vol. 107, No. 2, pp. 210–220.

Chromatic Numbers of Some Distance Graphs

D. A. Zakharov[1*]

[1] *National Research University Higher School of Economics, Moscow, 101000 Russia*

Received August 5, 2016; in final form, August 30, 2018; accepted September 04, 2019

Abstract—For positive integers $n > r > s$, $G(n, r, s)$ is the graph whose vertices are the r-element subsets of an n-element set, two subsets being adjacent if their intersection contains exactly s elements. We study the chromatic numbers of this family of graphs. In particular, the exact value of the chromatic number of $G(n, 3, 2)$ is found for infinitely many n. We also improve the best known upper bounds for chromatic numbers for many values of the parameters r and s and for all sufficiently large n.

DOI: 10.1134/S000143462001023X

Keywords: *chromatic number, distance graph, upper bound.*

1. INTRODUCTION AND STATEMENT OF RESULTS

We set $\mathcal{R}_n = \{0, 1, \dots, n-1\}$ and consider the graph

$$G(n, r, s) = (V, E), \qquad V = \{v \subset \mathcal{R}_n : |v| = r\}, \quad E = \{(v, u) : |v \cap u| = s\}.$$

This graph plays an important role in problems of coding theory (see [1]), Ramsey theory (see [2] and [3]), and combinatorial geometry (see [4]–[14]). It is in connection with the last problems that this graph is interpreted as a distance graph. The *chromatic number* of this graph, that is, the least number $\chi(G(n, r, s))$ of colors needed to color all vertices of the graph in such a way that the endvertices of each edge have distinct colors, is of particular importance. Detailed surveys of all currently known estimates can be found in [15] and [16]. In particular, it has earlier been proved that

$$n \geq \chi(G(n, r, r-1)) \geq n - r + 1. \tag{1}$$

We have been able to prove the estimate (1) in the general case in a substantially simpler way than in [15]. We have also been able to improve this estimate in quite a few cases. Further, for $r = 3$ and $s = 2$, we have found an infinite sequence of values of n for which the chromatic number can be calculated exactly. This is the first nontrivial case of this kind, except the case of the graphs $G(n, 3, 1)$, in which the exact value of the chromatic number was found for all $n = 2^k$ (see [17]). Below we give the corresponding statements.

Theorem 1. *Let $p > 3$ be a prime. If the congruence $-1 \equiv 2^r \pmod p$ fails for any r, then $\chi(G(n, 3, 2)) \leq n - 2$ for $n = p + 2$ and $\chi(G(n, 3, 2)) \leq n - 1$ for $n = p + 1$.*

We prove Theorem 1 in Sec. 2, and in Sec. 3, we explain why the assumptions of the theorem are satisfied for infinitely many primes p.

Theorem 2. *The following assertions hold.*

(A) *For any n and r,*

$$n \geq \chi(G(n, r, r-1)) \geq n - r + 1$$

if $n - r$ is even and

$$n \geq \chi(G(n, r, r-1)) \geq n - r + 2$$

if $n - r$ is odd.

(B) *The estimate $\chi(G(n, r, r-1)) \geq n - r + 2$ holds for $n = rk - 1$, r being prime.*

*E-mail: s18b1_zakharov@179.ru

For $r = 3$, it follows from Theorem 2 that

$$\chi(G(n,3,2)) \geq n-1, \qquad n \equiv 0,2,4,5 \pmod{6}.$$

Thus, the value of $\chi(G(n,3,2))$ has been found for infinitely many n. We prove Theorem 2 in Sec. 4.

For $r < 2s+1$, the best known estimate of $\chi(G(n,r,s))$ was given by the inequality (see [15])

$$\chi(G(n,r,s)) \leq (1+o(1))n^{r-s}\frac{r!}{s!\,((r-s)!)^2}\,. \tag{2}$$

We have been able to improve the estimate (2) in some domain of parameters; namely, we prove the following result in Sec. 5.

Theorem 3. *Let n be a prime. Then*

$$\chi(G(n,r,s)) \leq n^{r-s}.$$

We will prove this theorem in two ways, using additive combinatorics and without it.

Note that Theorem 3 holds for any r and s. At the same time, Theorem 3 readily implies an asymptotic statement that does not use n being prime but slightly restricts the parameters r and s; namely,

$$\chi(G(n,r,s)) \leq (1+o(1))n^{r-s}$$

for r and s such that the asymptotics

$$\left(1+\frac{1}{n^{0.475}}\right)^{r-s} \sim 1$$

holds as $n \to \infty$, which is equivalent to $r-s = o(n^{0.475})$. The point is that Baker, Harman, and Pintz [18] proved the existence of a constant c such that there always exists a prime between x and $x + cx^{0.525}$. Using this result, we obtain

$$\begin{aligned}\chi(G(n,r,s)) &\leq \chi(G(n',r,s)) \leq (n+cn^{0.525})^{r-s}\\ &= n^{r-s}\left(1+\frac{c}{n^{0.475}}\right)^{r-s} = (1+o(1))n^{r-s},\end{aligned}$$

where n' is a prime between n and $n + cn^{0.475}$. Using the Riemann hypothesis, one can replace the index 0.475 with $0.5 + o(1)$ (see [19]), and there is a belief that actually there always exist primes even on intervals of the form $[x, x + c\ln^2 x]$. Of course, all of this potentially weakens the restrictions imposed on r and s.

Theorem 3 improves the previous result (2), for example, in the case where $d = r-s < \sqrt{s}$ and $s \geq 2$. Indeed,

$$\frac{r!}{s!\,(d!)^2} \geq \frac{s^d}{d^{2d}} > 1.$$

Finally, it is possible to strengthen Theorem 3 in a number of cases. The following theorem holds, which we prove in Sec. 6.

Theorem 4. *Let $n = 2p$, let p be prime, and let $r-s$ be odd. Then*

$$\chi(G(n,r,s)) \leq \frac{n^{r-s}}{2^{r-s-1}}\,.$$

2. PROOF OF THEOREM 1

2.1. Construction of the Coloring

Note at once that it suffices to consider the case of $n = p + 2$. Indeed, to construct the desired $(n-1)$-coloring of $G(n, 3, 2)$, it suffices to take an $(n-1)$-coloring of $G(n+1, 3, 2)$ and remove all vertices (triples of elements) passing through some chosen element.

Thus, let us construct some coloring of vertices of our graph. We single out the elements $n-1$ and $n-2$ and divide the set of vertices of $G(n, 3, 2)$ into four subsets:

- V_0 is the set of vertices that do not meet $n-1$ and $n-2$;
- V_2 is the set of vertices meeting $n-1$ and $n-2$;
- W_1 is the set of vertices that meet $n-2$ and do not meet $n-1$;
- W_2 is the set of vertices that meet $n-1$ and do not meet $n-2$.

To each vertex $x = (x_1, x_2, x_3) \in V_0$ we assign the color

$$\chi(x) = x_1 + x_2 + x_3 \pmod{p},$$

and to each vertex $x = (x_1, n-1, n-2) \in V_2$ we assign the color

$$\chi(x) = 3x_1 \pmod{p}.$$

To color the sets W_1 and W_2, we use the following lemma, which we prove in Sec. 2.3.

Lemma 1. *Let $\binom{\mathcal{R}_p}{2}$ be the set of all pairs of elements of $\mathcal{R}_p = \mathcal{R}_{n-2}$. Then there exist functions $f_1,\ f_2\colon \binom{\mathcal{R}_p}{2} \to \mathcal{R}_p$ such that*

(1) $f_i(x, y) \in \{x, y\}$;

(2) $f_1(x, y) \neq f_2(x, y)$;

(3) *there exists no pair x, y such that*

$$f_i(x, y) = x, \qquad f_i\left(\frac{x+y}{2}, x\right) = \frac{x+y}{2}$$

for some $i \in \{1, 2\}$. (Here the division is in $\mathbb{Z}_p$; that is, one takes the corresponding residue in the set $\{0, \dots, p-1\}$.)

Now to each vertex

$$x = (x_1, x_2, m) \in W_i, \qquad m \in \{n-1, n-2\},$$

we assign the color

$$\chi(x) = x_1 + x_2 + f_i(x_1, x_2) \pmod{p}.$$

Obviously, we have constructed a p-coloring, $p = n-2$, of all vertices of our graph. In the next section, we prove that this coloring is proper; i.e., two arbitrary vertices (triples of elements) having exactly two common elements (forming an edge) have distinct colors.

2.2. Proof that the Coloring Is Proper

Take two arbitrary adjacent vertices

$$x = (x_1, x_2, x_3), \qquad y = (x_1, x_2, x_4)$$

and consider the following cases.

Case 1. Let $x, y \in V_0$. Then, obviously,

$$\chi(x) \equiv x_1 + x_2 + x_3 \not\equiv x_1 + x_2 + x_4 \equiv \chi(y) \pmod p.$$

Case 2. Let $x, y \in V_2$. Then

$$\chi(x) \equiv 3x_3 \not\equiv 3x_4 \equiv \chi(y) \pmod p,$$

because, by assumption, p is a prime greater than three; i.e., $p \nmid 3$.

Case 3. Let $x \in V_0$ and $y \in V_2$. This case is obviously impossible.

Case 4. Let $x \in W_i$ and $y \in V_2$. In what follows, without loss of generality, we assume that $i = 2$. Then we can assume that $x_1 = n - 1$ and $x_4 = n - 2$, whence

$$\chi(x) - \chi(y) \equiv x_2 + x_3 + f_2(x_2, x_3) - 3x_2 \equiv x_3 + f_2(x_2, x_3) - 2x_2 \pmod p.$$

If $f_2(x_2, x_3) = x_2$, then

$$\chi(x) - \chi(y) \equiv x_3 - x_2 \not\equiv 0 \pmod p,$$

and if $f_2(x_2, x_3) = x_3$, then

$$\chi(x) - \chi(y) \equiv 2x_3 - 2x_2 \not\equiv 0 \pmod p,$$

because $p = n - 2$ is odd.

Case 5. Let $x \in W_2$ and $y \in V_0$. We can assume that $x_3 = n - 1$. We have

$$\chi(x) - \chi(y) \equiv x_1 + x_2 + f_i(x_1, x_2) - x_1 - x_2 - x_4 \equiv f_i(x_1, x_2) - x_4 \not\equiv 0 \pmod p$$

by property 1 in Lemma 1.

Case 6. Let $x \in W_1$ and $y \in W_2$. Then $x_3 = n - 2$, $x_4 = n - 1$, and, therefore,

$$\chi(x) - \chi(y) \equiv f_1(x_1, x_2) - f_2(x_1, x_2) \not\equiv 0 \pmod p$$

by property 2 in Lemma 1.

Case 7. Let $x, y \in W_i$. We can assume that $i = 1$, i.e., that $x_1 = n - 2$. We can write

$$\begin{aligned} \chi(x) - \chi(y) &\equiv x_2 + x_3 + f_i(x_2, x_3) - x_2 - x_4 - f_i(x_2, x_4) \\ &\equiv x_3 + f_i(x_2, x_3) - x_4 - f_i(x_2, x_4) \pmod p. \end{aligned}$$

Consider the following subcases.

Subcase 7.1. If $f_i(x_2, x_3) = f_i(x_2, x_4) = x_2$, then

$$x_3 + f_i(x_2, x_3) - x_4 - f_i(x_2, x_4) \equiv x_3 - x_4 \not\equiv 0 \pmod p.$$

Subcase 7.2. If $f_i(x_2, x_3) = x_3$ and $f_i(x_2, x_4) = x_4$, then

$$x_3 + f_i(x_2, x_3) - x_4 - f_i(x_2, x_4) \equiv 2x_3 - 2x_4 \not\equiv 0 \pmod p.$$

Subcase 7.3. If $f_i(x_2, x_3) = x_2$ and $f_i(x_2, x_4) = x_4$, then

$$x_3 + f_i(x_2, x_3) - x_4 - f_i(x_2, x_4) \equiv x_3 + x_2 - 2x_4 \pmod p.$$

Assume that $x_3 + x_2 \equiv 2x_4 \pmod p$. We have $x_4 = (x_2 + x_3)/2$. But then we obtain

$$f_i(x_2, x_3) = x_2, \qquad f_i\left(x_2, \frac{x_2 + x_3}{2}\right) = \frac{x_2 + x_3}{2}\,,$$

which contradicts property 3 in Lemma 1. Therefore, $\chi(x) - \chi(y) \not\equiv 0 \pmod p$.

The last case of $f_i(x_2, x_3) = x_3$ and $f_i(x_2, x_4) = x_2$ can be analyzed in a similar way.

Thus, we have analyzed all cases, and the coloring is proper.

2.3. Proof of Lemma 1

For each pair of distinct i and j, we construct the following cyclic sequences (which will be referred to as *circles*) in $\mathbb{Z}_p$:

$$C(i,j) = \left(j_m \;\middle|\; j_0 = j,\ j_m \equiv \frac{j_{m-1}+i}{2} \pmod p \right).$$

For example, for $p = 7$, we have the circle

$$C(1,5) = C(1,3) = C(1,2) = (2,5,3) = (3,2,5) = (5,3,2).$$

Lemma 2. *The length $|C(i,j)|$ of the circle $C(i,j)$ is equal to the order k of the number 2 in $\mathbb{Z}_p$.*

Proof. Note that $j_m \equiv (j + (2^m - 1)i)/2^m \pmod p$. This can readily be verified by induction: $j_0 = j \equiv (j + (2^0 - 1)i)/2^0$ and

$$j_m \equiv \frac{j_{m-1}+i}{2} \equiv \frac{(j + (2^{m-1}-1)i)/2^{m-1} + i}{2} \equiv \frac{j + (2^m - 1)i}{2^m} \pmod p. \tag{3}$$

But then

$$j_k \equiv \frac{j + (2^k - 1)i}{2^k} \equiv i + \frac{j-i}{2^k} \equiv i + j - i \equiv j_0 \pmod p.$$

If we assume that $j_m \equiv j_0 \pmod p$ for $m < k$, then

$$2^m (j_0 - i) \equiv j_0 - i \pmod p,$$
$$(2^m - 1)(j_0 - i) \equiv 0 \pmod p,$$

which is not true for prime p. The proof of the lemma is complete. □

We construct a graph $G = (V, E)$ of circles as follows: its vertices are all circles $C(i,j)$, and its edges are the pairs of circles $C(i,j)$ and $C(j,i)$. It is the *cyclic sequences* which we connect: for example, for $p = 7$, the circles $C(1,2)$, $C(1,3)$, and $C(1,5)$ represent the same vertex of the graph, which is hence connected to each of the vertices

$$C(2,1) = C(2,5) = \cdots, \qquad C(3,1) = \cdots, \qquad C(5,1) = \cdots,$$

etc.

Lemma 3. $\chi(G) = 2$.

Proof. Suppose that G contains a cycle of odd length l,

$$C(i_1, i_2), \quad C(i_2, i_3), \quad \ldots, \quad C(i_{l-1}, i_l), \quad C(i_l, i_1).$$

It is clear that the existence of an edge is equivalent to the inclusion $i_{m-1} \in C(i_m, i_{m+1})$. By (3),

$$i_{m-1} \equiv \frac{i_{m+1} + (2^{s_m} - 1)i_m}{2^{s_m}} \pmod p,$$
$$-2^{s_m}(i_m - i_{m-1}) \equiv i_{m+1} - i_m \pmod p$$

for some s_m. Let $d_m \equiv i_m - i_{m-1} \pmod p$. Then the last equation can be rewritten as

$$d_{m+1} \equiv -2^{s_m} d_m \pmod p.$$

Applying this formula l times, we obtain

$$d_l \equiv -2^{s_{l-1}} d_{l-1} \equiv (-1)^2 2^{s_{l-1}+s_{l-2}} d_{l-2} \equiv \cdots$$
$$\equiv (-1)^{l-1} 2^{s_{l-1}+s_{l-2}+\cdots+s_1} d_1 \equiv (-1)^l 2^{s_1+\cdots+s_l} d_l.$$

Therefore,

$$d_l(2^S + 1) \equiv 0 \pmod p$$

for some S, which is impossible by the assumptions of the theorem. The proof of the lemma is complete. □

We are now in a position to complete the proof of Lemma 1, i.e., to construct functions with the three properties in the statement of the lemma. Namely, we color all the circles in two colors, $\mathcal{M}_1$ and $\mathcal{M}_2$, being the sets of circles of the first and the second color, respectively. We set

- $f_1(i,j) = i$ and $f_2(i,j) = j$ if $C(i,j) \in \mathcal{M}_1$;
- $f_1(i,j) = j$ and $f_2(i,j) = i$ if $C(i,j) \in \mathcal{M}_2$.

Since the coloring is proper, it follows that the functions are well defined; namely, $f_i(x,y) = f_i(y,x)$. Thus, properties 1 and 2 are satisfied automatically. Let us prove property 3. Let there exist x and y such that

$$f_i(x,y) = x, \qquad f_i\left(\frac{x+y}{2}, x\right) = \frac{x+y}{2}.$$

Then

$$C(x,y) \in \mathcal{M}_i, \qquad C\left(\frac{x+y}{2}, x\right) \in \mathcal{M}_i,$$

and hence

$$C\left(x, \frac{x+y}{2}\right) \in \mathcal{M}_{3-i},$$

but it is clear that $C(x,y) = C(x,(x+y)/2)$. We arrive at a contradiction, and the proof of the lemma is complete. $\square$

3. PROOF THAT THERE EXIST INFINITELY MANY PRIMES IN THEOREM 1

Let us prove that the condition $-1 \not\equiv 2^r \pmod p$ is satisfied by all primes of the form $p = 8k-1$, which are infinitely many by the classical Dirichlet theorem. Note that not only these primes satisfy the condition. For example, the number 73 satisfies the condition as well.

Let d be the order of 2 modulo $p = 8k-1$, and let $\left(\frac{a}{p}\right)$ denote the Legendre symbol (see [20]). It is well known that (see [20])

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^{(64k^2-16k+1-1)/8} = 1.$$

Therefore, 2 is a quadratic residue in $\mathbb{Z}_p$. Consequently, $2^{(p-1)/2} \equiv 1 \pmod p$, and it follows that $d \mid (p-1)/2 = 4k-1$; i.e., d is odd.

Assume that l is the smallest positive integer such that $2^l \equiv -1 \pmod p$. Then $d \mid 2l$, but d is odd, which implies that $d \mid l$ and hence $2^l \equiv 1 \pmod p$. This contradiction completes the proof.

4. PROOF OF THEOREM 2

First, we establish the inequality $\chi(G(n,r,r-1)) \le n$. To each vertex $x = (x_1,\dots,x_r)$, we assign the color

$$\chi(x) = x_1 + \dots + x_r \pmod n.$$

Then the difference of the colors of two adjacent vertices $x = (x_1,\dots,x_r)$ and $y = (x_2,\dots,x_{r+1})$ is $\chi(x) - \chi(y) \equiv x_1 - x_{r+1} \not\equiv 0 \pmod n$.

Let us proceed to the lower bounds in (A). Let W be an independent set in $G(n,r,r-1)$. Then we fix $r-2$ elements $a_1,\dots,a_{r-2}$. It is clear that they are contained in at most $[(n-r+2)/2]$ elements of W, and each set in W contains $\binom{r}{r-2}$ sets of cardinality $r-2$, whence it follows that

$$|W| \le \frac{[(n-r+2)/2]\binom{n}{r-2}}{\binom{r}{2}};$$

i.e.,

$$\chi(G(n,r,r-1)) \geq \frac{|V(n,r,r-1)|}{\alpha(G(n,r,r-1))} \geq \frac{\binom{n}{r}\binom{r}{2}}{[(n-r+2)/2]\binom{n}{r-2}} = \frac{(n-r+2)(n-r+1)}{2[(n-r+2)/2]}.$$

Considering the two cases of the parity of the difference, we obtain assertion (A) of the theorem.

Finally, let $n = rk-1$, and let r be prime. Assume that the vertices $G(n,r,r-1)$ are painted with $n-r+1$ colors. Then all colors occur in every maximal clique. All in all, there are $\binom{n}{r-1}$ maximal cliques, and each vertex is contained in r cliques. It follows that there are $\binom{n}{r-1}/r$ vertices of each color, but since r is prime and $n = rk-1$, we see that this number is noninteger, which is a contradiction.

The proof of the theorem is complete.

5. PROOF OF THEOREM 3

5.1. First Proof

Let n be prime, and let $h = r-s$. Then by the Bose–Chowla theorem (see [21]) there exist numbers $a_0, \dots, a_{n-1} \in \mathbb{Z}_{n^h-1}$ such that all sums of h numbers in this set are pairwise distinct.

Now we construct a coloring as follows: if $x = (x_1, \dots, x_r)$ is a vertex, then

$$\chi(x) = a_{x_1} + \dots + a_{x_r} \pmod{n^h-1}.$$

It is clear that the total number of colors does not exceed n^h. Let us verify that this coloring is proper. Indeed, if two vertices

$$x = (x_1, \dots, x_s, y_1, \dots, y_{r-s}), \qquad y = (x_1, \dots, x_s, z_1, \dots, z_{r-s})$$

form an edge, then

$$\chi(x) - \chi(y) \equiv a_{y_1} + \dots + a_{y_h} - (a_{z_1} + \dots + a_{z_h}) \not\equiv 0 \pmod{n^h-1}$$

by the definition of a_i.

The proof of the theorem is complete. □

Note that each color in this coloring consists of sets whose intersections have cardinalities not only different from s but strictly less than s. This allows us to expect a further strengthening of the result.

We also note that one can take not only primes but also powers of primes in the Bose–Chowla theorem. However, this has little effect on the generality of the result (cf. the remarks about the distribution density of primes in the positive integers after the statement of the theorem).

5.2. Second Proof

Let again n be a prime, and let $h = r-s$. The colors will be vectors in $\mathbb{Z}_n^h$. Namely, let $x = (x_1, \dots, x_r)$. Then we define the ith coordinate of its color as the sum of all products of i coordinates of x modulo n. Assume that the coloring is not proper, i.e., there exist vertices $x = (x_1, \dots, x_h, z_1, \dots, z_s)$ and $y = (y_1, \dots, y_h, z_1, \dots, z_s)$ of the same color. We set

$$\mathbb{X} = \{x_1, \dots, x_h\}, \qquad \mathbb{Y} = \{y_1, \dots, y_h\}, \qquad \mathbb{W} = \{z_1, \dots, z_s\},$$

and

$$\sigma_i(\mathbb{M}) = \sum_{S \subset \mathbb{M},\, |S|=i} \prod_{t \in S} t, \qquad \mathbb{M} \in \{\mathbb{X}, \mathbb{Y}, \mathbb{W}\}.$$

Now we shall prove by induction that

$$\sigma_i(\mathbb{X}) \equiv \sigma_i(\mathbb{Y}) \pmod{n}$$

for any $i \in \{1, \dots, h\}$.

Base of induction. For $i = 1$, the condition that the vertices x and y have the same color means that

$$\sum_{i=1}^{h} x_i + \sum_{i=1}^{s} z_i \equiv \sum_{i=1}^{h} y_i + \sum_{i=1}^{s} z_i \pmod n;$$

i.e., $\sigma_1(\mathbb{X}) \equiv \sigma_1(\mathbb{Y}) \pmod n$, as desired.

Inductive step. Let the statement be true for all $i_0 < i$. If we consider the sums of terms with i factors in each of them, then the terms that are products of elements of the set $\mathbb{W}$ alone cancel out immediately. In turn, the sums of terms each of which includes exactly $j < i$ factors in $\mathbb{W}$ will be represented as $\sigma_{ij}(\mathbb{M})\sigma_j(\mathbb{W})$, where $\mathbb{M} \in \{\mathbb{X}, \mathbb{Y}\}$. Thus, by the induction assumption, these sums cancel out as well, which means that all terms except those in which there are no elements of the set $\mathbb{W}$ cancel out. We see that

$$\sigma_i(\mathbb{X}) \equiv \sigma_i(\mathbb{Y}) \pmod n.$$

The inductive step is complete.

Thus, we see that the sets $\mathbb{X}$ and $\mathbb{Y}$, each of which has cardinality h, satisfy the congruences

$$\begin{aligned} &\sigma_1(\mathbb{X}) \equiv \sigma_1(\mathbb{Y}) \pmod n, \\ &\sigma_2(\mathbb{X}) \equiv \sigma_2(\mathbb{Y}) \pmod n, \\ &\dots\dots\dots\dots\dots\dots\dots \\ &\sigma_h(\mathbb{X}) \equiv \sigma_h(\mathbb{Y}) \pmod n. \end{aligned}$$

Consider the polynomials with root sets $\mathbb{X}$ and $\mathbb{Y}$. By the Vieta theorem, their coefficients coincide, which means that the polynomials are equal as functions, that is, have the same roots, and so $\mathbb{X} = \mathbb{Y}$. At this point, we have used the fact that the root set $\pmod n$ of the polynomial $(x - x_1) \cdots (x - x_h)$ is $\{x_1, \dots, x_h\}$, which is only true for prime n.

We have arrived at a contradiction; the proof of the theorem is complete. □

6. PROOF OF THEOREM 4

Let us define the graph $G(n, r, s)$ on the set $\mathcal{R} = \mathcal{R}_p \times \{0, 1\}$. Then, for each vertex

$$\overline{x} = \{\overline{x}_1, \dots, \overline{x}_r\}, \qquad \overline{x}_i = (x_i, \alpha_i),$$

we set

$$X = \{x_1, \dots, x_r\}, \qquad \alpha = (\alpha_1, \dots, \alpha_r)$$

and define the color

$$\chi(\overline{x}) = (\sigma_1^p(X), \dots, \sigma_{r-s}^p(X), \sigma_1^2(\alpha)),$$

where σ_i^p is the function in Sec. 5.2 and the new superscript indicates that all congruences are modulo p. It is clear that, in this way, we use at most $2p^{r-s} = n^{r-s}/2^{r-s-1}$ colors.

Assume that there exist adjacent vertices $\overline{x}$ and $\overline{y}$ of the same color. Then, as in the second proof of Theorem 3, we set

$$\overline{x} = \{\overline{x}_1, \dots, \overline{x}_{r-s}, \overline{z}_1, \dots, \overline{z}_s\}, \qquad \overline{y} = \{\overline{y}_1, \dots, \overline{y}_{r-s}, \overline{z}_1, \dots, \overline{z}_s\},$$

where

$$\overline{x}_i = (x_i, \alpha_i), \qquad \overline{y}_i = (y_i, \beta_i), \qquad \overline{z}_i = (z_i, \gamma_i),$$
$$\mathbb{X} = \{x_1, \dots, x_{r-s}\}, \qquad \mathbb{Y} = \{y_1, \dots, y_{r-s}\}.$$

The second proof of Theorem 3 obviously implies that $\mathbb{X} = \mathbb{Y}$. We can assume that $x_i = y_i$ for each i. Since $\overline{x} \cap \overline{y} = \{\overline{z}_1, \dots, \overline{z}_s\}$, it follows that $\overline{x}_i \neq \overline{y}_i$ for all i. This means that one always has $\alpha_i + \beta_i = 1$. Consequently,

$$\alpha_1 + \dots + \alpha_{r-s} + \beta_1 + \dots + \beta_{r-s} \equiv r - s \equiv 1 \pmod 2;$$

i.e., these sums are not congruent modulo 2, but then

$$\alpha_1 + \dots + \alpha_{r-s} + \gamma_1 + \dots + \gamma_s \not\equiv \beta_1 + \dots + \beta_{r-s} + \gamma_1 + \dots + \gamma_s \pmod 2,$$

which contradicts $\overline{x}$ and $\overline{y}$ being of the same color.

We have arrived at a contradiction, and the proof of the theorem is complete. □

REFERENCES

1. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I* (North-Holland Publ., Amsterdam, 1977).
2. Z. Nagy, "A certain constructive estimate of the Ramsey number," Mat. Lapok **23**, 301–302 (1972).
3. P. Frankl and R. Wilson, "Intersection theorems with geometric consequences," Combinatorica **1** (4), 357–368 (1981).
4. A. M. Raigorodskii, "Cliques and cycles in distance graphs and graphs of diameters," in *Discrete Geometry and Algebraic Combinatorics*, *Contemp. Math.* (Amer. Math. Soc., Providence, RI, 2014), Vol. 625, pp. 93–109.
5. A. M. Raigorodskii, "Coloring Distance Graphs and Graphs of Diameters," in *Thirty Essays on Geometric Graph Theory* (Springer, New York, 2013), pp. 429–460.
6. B. Bollobás, B. P. Narayanan, and A. M. Raigorodskii, "On the stability of the Erdős–Ko–Rado theorem," J. Combin. Theory Ser. A **137**, 64–78 (2016).
7. A. V. Bobu, A. E. Kupriyanov, and A. M. Raigorodskii, "Asymptotic study of the maximum number of edges in a uniform hypergraph with one forbidden intersection," Mat. Zametki **207** (5), 17–42 (2016) [Math. Notes **207** (5), 652–677 (2016)].
8. A. M. Raigorodskii, "Combinatorial geometry and coding theory," Fund. Inform. **145** (3), 359–369 (2016).
9. A. V. Bobu, A. E. Kupriyanov, and A. M. Raigorodskii, "On the maximal number of edges in a uniform hypergraph with one forbidden intersection," Dokl. Akad. Nauk **463** (1), 11–13 (2015) [Dokl. Math. **92** (1), 401–403 (2015)].
10. A. V. Bobu, A. E. Kupriyanov, and A. M. Raigorodskii, "On the number of edges of a uniform hypergraph with a range of allowed intersections," Problemy Peredachi Informatsii **53** (4), 16–42 (2017) [Probl. Inform. Transm. **53** (4), 319–342 (2017)].
11. A. V. Bobu, A. E. Kupriyanov, and A. M. Raigorodskii, "On the number of edges in a uniform hypergraph with a range of permitted intersections," Dokl. Akad. Nauk **475** (4), 365–368 (2017) [Dokl. Math. **96** (1), 354–357 (2017)].
12. R. I. Prosanov, A. A. Sagdeev, and A. M. Raigorodskii, "Improvements of the Frankl–Rödl theorem and geometric consequences," Dokl. Akad. Nauk **475** (2), 137–139 (2017) [Dokl. Math. **96** (1), 336–338 (2017)].
13. D. Cherkashin, A. Kulikov and A. Raigorodskii, "On the chromatic numbers of small-dimensional Euclidean spaces," Discrete Appl. Math. **243**, 125–131 (2018).
14. L. I. Bogolyubskii, A. S. Gusev, M. M. Pyaderkin, and A. M. Raigorodskii, "Independence numbers and chromatic numbers of the random subgraphs of some distance graphs," Mat. Sb. **206** (10), 3–36 (2015) [Sb. Math. **206** (10), 1340–1374 (2015)].
15. A. V. Bobu, O. A. Kostina, and A. E. Kupriyanov, ""Independence numbers and chromatic numbers of some distance graphs," Problemy Peredachi Informatsii **51** (2), 86–98 (2015) [Probl. Inform. Transm. **51** (2), 165–176 (2015)].
16. M. M. Pyaderkin, "Independence numbers of random subgraphs of distance graphs," Mat. Zametki **99** (4), 564–573 (2016) [Math. Notes **99** (4), 556–563 (2016)].
17. J. Balogh, A. Kostochka, and A. Raigorodskii, "Coloring some finite sets in $\mathbb{R}^n$," Discuss. Math. Graph Theory **33** (1), 25–31 (2013).
18. R. C. Baker, G. Harman, and J. Pintz, "The difference between consecutive primes. II," Proc. London Math. Soc. (3) **83** (3), 532–562 (2001).
19. H. Cramèr, "Some theorems concerning prime numbers," Ark. Mat., Astron. Fys. **15** (5) (1921).
20. I. M. Vinogradov, *Foundations of Number Theory* ("Regular and Chaotic Dynamics," Moscow–Izhevsk, 2003) [in Russian].
21. R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," Comment. Math. Helv. **37**, 141–147 (1962).