Introduction to Combinatorics
Solutions

Wojciech Nadara, class 4, 2020-03-19

1. Let x_i denote the chosen value in i-th vertex and S_i denote the set of values w. Fact that for every pair of adjacent vertices their values are different is equivalent to the fact that $P(x_1, \ldots, x_{2n}) = (x_1 - x_2)(x_2 - x_3) \ldots (x_{2n-1} - x_{2n})(x_{2n} - x_1))$ is nonzero. That polynomial has degree $2n$ and it can be easily verified that its coefficient next to $x_1 x_2 \ldots x_{2n}$ is 2 (which is nonzero). Moreover size of S_i is 2 what is bigger than degree of x_i in that monomial. Hence based on Combinatorial Nullstellensatz we can deduce that there exist $x_1 \in S_1, x_2 \in S_2, \ldots, x_{2n} \in S_{2n}$ such that $P(x_1, \ldots, x_{2n})$ is nonzero which is what we wanted.

2. Let us first deal with the case that $|A| + |B| > p$. We need to prove that $A + B = \mathbb{Z}_p$ then. Let $c \in \mathbb{Z}_p$. We can create p pairs $(0, c), (1, c-1), \ldots, (p-1, c-(p-1))$ so that sum of values within them is c (modulo p). Since $|A| + |B| > p$ we can easily conclude that for some of these pairs it is the case that its first element is in A and second is in B what proves our case (based on simple application of Dirichlet's pigeonhole principle).

   Let us now assume that $|A|+|B| \leq p$. We need to prove that $|A+B| \geq |A|+|B|-1$. Assume by contrary that $|A+B| \leq |A|+|B|-2$. For convenience let C denote arbitrary set so that $A+B \subseteq C$ and $|C| = |A|+|B|-2$. Now let us define polynomial $P(x, y) = \prod_{c \in C}(x+y-c)$. Based on the definition of $A+B$ and C we clearly see that for every $a \in A, b \in B$ we have $P(a, b) = 0$.

   Let us now inspect the coefficient of $x^{|A|-1}y^{|B|-1}$ in P. It is clearly equal $\binom{|A|+|B|-2}{|A|-1}$ which is nonzero modulo p. Since degree of P is $|A|+|B|-2$ (or when expressed a bit differently $(|A|-1)+(|B|-1)$), so assumptions of Combinatorial Nullstellensatz are fulfilled and based on it we conclude that there must exist $a \in A, b \in B$ such that $P(a, b) \neq 0$ which is a contradiction.

3. By taking remainders modulo p instead of set of $2p-1$ integers we can assume we are given a sequence $r_1, r_2, \ldots, r_{2p-1}$ so that $0 \leq r_1 \leq r_2 \leq \ldots \leq r_{2p-1} \leq p-1$. We would like to take advantage of Cauchy-Davenport and get p summands in total, so let us partition elements of that sequence into $p-1$ pairs $(r_1, r_p), (r_2, r_{p+1}), \ldots, (r_{p-1}, r_{2p-2})$ and a singleton (r_{2p-1}). If we take exactly one number from each of these pairs and r_{2p-1} we will indeed take p numbers in total. Before we use Cauchy-Davenport there is an important question — are elements within every pair distinct? Let us consider two cases.

   1) Let us assume that answer to that question is "no" which means there is some $c \in [p-1]$ such that $r_c = r_{c+p-1}$. However since we assumed that sequence r is sorted we can deduce that $r_c = r_{c+1} = r_{c+2} = \ldots = r_{c+p-1}$. These are p equal numbers and their sum is clearly disivible by p, so we are done in this case.

   2) Let us now assume that answer to that question is "yes" which means that if we treat elements of every pair as a set its size is 2. Let us denote $S_i = \{r_i, r_{i+p-1}$ and $R_0 = \{r_{2p-1}\}$. We will now incrementally add sets S_i to be able to have bigger and bigger set of remainders modulo p we are able to express as some sums. Let us define $R_i = R_{i-1} + S_i$ for every $i = 1, \ldots, p-1$ (we are working modulo p). By induction we argue that we are able to express all elements of R_i as sums of $i+1$ elements of sequence r (namely r_{2p-1} and one from pairs corresponding to sets $S_1, \ldots, S_i$). However by Cauchy-Davenport we know that $|R_i| \geq \min(p, |R_{i-1}| + |S_i| - 1) = \min(p, |R_{i-1}| + 1)$, so by induction we argue that $|R_i| \geq i+1$. Hence $|R_{p-1}| = p$, so $R_{p-1} = \{0, \ldots, p-1\}$, so in particular $0 \in R_{p-1}$ what proves that 0 is expressible as a sum of p elements of this sequence.

4. Let A be a $k \times k$ matrix such that $a_{ij} = x_i^{j-1}$. It is called Vandermonde's matrix and its determinant is $\prod_{1 \le i < j \le k} (x_i - x_j)$.

   We are now going to briefly describe why determinant of this matrix is given by that formula. Determinant of A is clearly a polynomial in variables $x_1, \ldots, x_n$ and its degree is $0+1+\ldots+k-1 = \binom{k}{2}$. Moreover whenever $x_i = x_j$ it has two equal rows, so this polynomial must be divisible by $(x_i - x_j)$. Hence we can conclude that $det(A) = \prod_{1 \le i < j \le k}(x_i - x_j) Q(x_1, \ldots, x_k)$, where Q is some polynomial. However degree of right hand side is $\binom{k}{2} + \deg Q$, so $\deg Q = 0$, so Q is just a real number. By comparing the coefficient next to $x_1^{k-1} x_2^{k-2} \ldots x_k^0$ on both sides we conclude that $Q \equiv 1$ (since this coefficient is 1 on both sides) what proves our assertion.

   Polynomial from the statement is actually square of this determinant. So instead of analyzing it, we analyze determinant of that matrix. Based on permutation formula for determinant we get that it is equal $\sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{i=1}^k a_{i,\sigma(i)} = \sum_{\sigma \in S_k} \operatorname{sgn}(\sigma) \prod_{i=1}^k x_i^{\sigma(i)-1}$, where S_k is the set of all permutations of $[k]$. If we want to get $x_1^{k-1} \ldots x_k^{k-1}$ in the square of this expression monomial $\prod_{i=1}^k x_i^{\sigma(i)-1}$ from first factor must be paired with $\prod_{i=1}^k x_i^{k-\sigma(i)} = \prod_{i=1}^k a_{i,k+1-\sigma(i)}$ from the second factor. Such monomial exists since if σ is a valid permutation of $[k]$ then τ where $\tau(i) = k+1-\sigma(i)$ is a valid permutation as well. Coefficient of the first monomial in first factor is $\operatorname{sgn} \sigma$, coefficient of the second monomial in second factor is $\operatorname{sgn} \tau$, so contribution of that pair of monomials to the result is $\operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau$. It turns out that $\operatorname{sgn} \tau = \operatorname{sgn} \sigma \cdot (-1)^{\lfloor \frac{k}{2} \rfloor}$ because σ^{-1} can be transformed to τ^{-1} by $\lfloor \frac{k}{2} \rfloor$ swaps of pairs of elements and every swap changes sign of the permutation (and $\operatorname{sgn} \sigma = \operatorname{sgn} \sigma^{-1}$). These swaps are swaps of elements on the pairs of positions $(i, k+1-i)$ for $i = 1, \ldots, \lfloor \frac{k}{2} \rfloor$. Because of that we conclude that $\operatorname{sgn} \sigma \cdot \operatorname{sgn} \tau = (-1)^{\lfloor \frac{k}{2} \rfloor}$ (so it doesn't depend on σ!). We now know that for every monomial from the first factor there is exactly one monomial from the second factor so that when multiplied they give nonzero contribution to the coefficient of monomial $x_1^{k-1} \ldots x_k^{k-1}$ and no matter what this monomial from first factor is, that contribution is $(-1)^{\lfloor \frac{k}{2} \rfloor}$. Since there are $k!$ monomials in whole expression for determinant, we conclude that answer to this problem is $(-1)^{\lfloor \frac{k}{2} \rfloor} k!$.

5. Let us consider following polynomial:

$$P(c_1, \ldots, c_k) = \prod_{1 \leq i < j \leq k} ((c_i - c_j)((c_i + a_i) - (c_j + a_j)))$$

in k variables $c_1, \ldots, c_k$ over $\mathbb{Z}_p$. It is clear that sequences $c_1, \ldots, c_k$ that are fulfilling conditions from problem statement are those that are not roots of this polynomial and such that $c_i \in \{b_1, \ldots, b_k\}$ (we can of course assume that $0 \leq b_i < p$). Degree of P is $k(k-1)$ which is the degree of monomial $c_1^{k-1} \cdot \ldots \cdot c_k^{k-1}$ as well. It is now clear that a_i terms in the expression for this polynomial don't have any influence on coefficient of this monomial since in order to reach maximum possible degree of a monomial we need to take either c_i or c_j from the factor $((c_i + a_i) - (c_j + a_j))$. After removing them this polynomial becomes $\prod_{1 \leq i < j \leq k} (c_i - c_j)^2$ which is the polynomial from previous exercise! Based on that exercise we know that coefficient next to this monomial is $(-1)^{\lfloor \frac{k}{2} \rfloor} k!$ which fortunately is not divisible by p (i.e. it is nonzero in $\mathbb{Z}_p$). Because of that we can apply Combinatorial Nullstellensatz for monomial $c_1^{k-1} \cdot \ldots \cdot c_k^{k-1}$ and sets $S_i = \{b_1, \ldots, b_k\}$ and conclude that there exists a point $(c_1, \ldots, c_k)$ such that $c_i \in S_i$ and $P(c_1, \ldots, c_k) \neq 0$ which is what we wanted to show.