Oplossingen

| Solutions

This time we do not have new problems, and the solutions of the problems in the September issue will appear in the next issue. Instead we have some additional solutions to the problems in the March and June issue. Fot these issues we missed some submissions by Thijmen Krebs and by Reinier Sorgdrager and Jim Wittebol. As an apology, we provide some of their approaches to a few problems that are different from the solutions posted before.

Thijmen Krebs provided a more direct solution to part b of problem A of the March 2020 problem section, which we would like to share. The problem was the following:

Problem 2020-1/A (proposed by Hendrik Lenstra)

For every positive integer n, we write $[n] := \{0,1,\ldots,n-1\}$. For every integer m, we let $T(m) := m(m+1)/2$ be the m-th triangular number. Let $\tau : [n] \to [n]$ be the map given by $m \mapsto T(m) \bmod n$.

a. For which n is τ a permutation?

b. For these n, determine the sign of τ as a function of n.

Solution to part b In part a, we showed that n has to be a power of 2. The case $n = 1$ is trivial, so suppose that $n \geq 2$ is a power of 2. Observe that for all $m \in [n/2]$, we have

$$\begin{aligned} T(n-1-m) &= (n-1-m)(n-m)/2 \\ &= (m+1-n)(m-n)/2 \\ &\equiv T(m) \pmod{n/2}. \end{aligned}$$

Recall that an inversion of a permutation π on $[n]$ is a pair $(i,j) \in [n]^2$ satisfying $i < j$ and $\pi(i) > \pi(j)$. We find that $(m, n-1-m)$ with $m \in [n/2]$ is an inversion precisely if $\tau(m) \geq n/2$, which is the case precisely if $T(m) - (T(m) \bmod n/2)$ is an odd multiple of $n/2$.

The number of inversions of this form modulo 2 is therefore

$$\frac{2}{n} \sum_{m \in [n/2]} T(m) - (T(m) \bmod n/2) = \frac{2}{n} \sum_{m \in [n/2]} T(m) - m = \frac{2}{n} \sum_{m \in [n/2]} T(m) = \left(\frac{n}{2} - 2\right)\left(\frac{n}{2} - 1\right)/6.$$

The first equality above uses that T induces a permutation mod $n/2$, the second uses that $\sum_{m \in [n/2]} m = T(n/2)$ and the third uses knowledge of the tetrahedral numbers (where in the case $n = 2$, we let $[0] = \emptyset$). Observe that $\left(\frac{n}{2} - 2\right)\left(\frac{n}{2} - 1\right)/6 \equiv T(n/2-2) \pmod 2$.

Switching all these inversions (a permutation of sign $(-1)^{T(n/2-2)}$) and applying τ afterwards gives us a permutation σ with the property $\sigma(m) \in [n/2]$ and $\sigma(n-m-1) = n/2 + \sigma(m)$ for all $m \in [n/2]$. If $i < n/2 \leq j$, then (i,j) is clearly not an inversion, and if $i,j \in [n/2]$ with $i < j$, then (i,j) is an inversion if and only if $(n-i-1, n-j-1)$ is not an inversion. In particular, σ has $\binom{n/2}{2} = T(n/2-1)$ inversions, so it has sign $(-1)^{T(n/2-1)}$. We have $T(n/2-2) + T(n/2-1) = (n-2)(n/2-1)/2 = (n/2-1)^2$, which is even precisely if $n = 2$. This means the sign of τ is even when $n = 2$ and odd for all higher powers of 2.

Thijmen also provided a more direct solution to Problem C of the March edition.

Problem 2020-1/C. (proposed by Hendrik Lenstra)

Let $n \geq 4$ be an integer and let A be an abelian group of order 2^n. Let σ be an automorphism of A such that the order of σ is a power of 2. Then the order of σ is at most 2^{n-2}.

Solution Denote $N = 2^n$, and let $G = \langle \sigma \rangle$ act on A. Since the length of each orbit divides the order of σ and the orbits partition A, those lengths divide N and the order of σ equals the length of a maximal orbit. As σ is an endomorphism, 0 is necessarily a fixed point, so orbits are at most of size $N/2$.

Suppose on the contrary that $|G \cdot x| = N/2$. Then all other orbits are strictly smaller. Let $B := A \backslash (G \cdot x)$, and note that $B = \{y \in A \mid \sigma^{N/4}(y) = y\}$. For $x, y \in B$, we find that $\sigma^{N/4}(y - x) = \sigma^{N/4}(y) - \sigma^{N/4}(z) = y - z$, hence B is a subgroup of A and we have $G \cdot x = x + B$. Let $y := \sigma(x) - x$ and let $s_k : B \to B$ be given by $s_k(z) = \sum_{i=0}^{k-1} \sigma^i(z)$. Then for all $k \in \mathbb{Z}_{\geq 0}$ we find (using a telescoping sum) that

$$\sigma^k(x) = x + s_k(y).$$

Redactie: Onno Berrevoets, Rob Eggermont en Daan van Gent

problems@nieuwarchief.nl

www.nieuwarchief.nl/problems

Oplossingen | Solutions

We show that B has exponent 2. Since $-x \in G\cdot x$, we have $-x = \sigma^j(x)$ for some $j \in \mathbb{Z}_{>0}$. Because $\sigma^{2j}(x) = x$, we find that $N/4 \mid j$. Observe that $\sigma^j(\sigma^k(x)) = -\sigma^k(x)$ for any k as well. Since $G\cdot x = x + B$, we can write any $z \in B$ as $x - \sigma^k(x)$ for some k. Since $\sigma^j(z) = z$, we find that $-z = -x + \sigma^k(x) = \sigma^j(z) = z$, so $2z$ has order at most 2, so B has exponent at most 2 (and exactly 2 since $|B| > 1$).

Consequently, if $|G\cdot y|$ divides $N/8$, then we find that $\sigma^{N/4}(x) = x + s_{N/4}(y) = x + 2s_{N/8}(y) = x$, a contradiction. So we must have $|G\cdot y| = N/4$.

By a similar argument to the one that showed $\sigma^k(x) = x + s_k(y)$, we now find that for $z := \sigma(y) - y \in B\backslash(G\cdot y)$, we have $\sigma^k(y) = y + s_k(z)$ for all $k \in \mathbb{Z}_{\geq 0}$. In particular, $|G\cdot z|$ divides $N/8$. But then

$$\begin{aligned}\sigma^{N/4}(x) &= x + \sum_{i=0}^{N/4} \sigma^i(y)\sigma^{N/4}(x) = x + \sum_{i=0}^{N/4-1} \sigma^i(y) = x + \sum_{i=0}^{N/4-1} y + s_i(z)\\ &= x + \sum_{i=0}^{N/8-1} 2y + s_i(z) + s_{N/8+i}(z) = x + \sum_{i=0}^{N/8-1} s_i(z) + (s_i(z) + \sigma^{N/8}(s_{N/8}(z)))\\ &= x + \sum_{i=0}^{N/8-1} s_{N/8}(z) = x + N/8 s_{N/8}(z) = x.\end{aligned}$$

Here, the last step uses that $N/8$ is even (and $s_{N/8}(z)$ has order 2), the only place we use that $n \geq 4$.

Reinier Sorgdrager and Jim Wittebol provided solutions to all exercises of the June 2020 problem section. Their solution to Problem B mentions an interesting property of square submatrices of Vandermonde matrices:

Problem 2020-2/B. (proposed by Onno Berrevoets)

Let $n \geq 1$ be an integer, and let $p_1, \ldots, p_{n-1}$ be pairwise distinct prime numbers. Suppose that $(v_1, \ldots, v_n)^\top \in \mathbb{Z}^n$ is a non-trivial element of the kernel of

$$\begin{pmatrix} 1^{p_1} & 2^{p_1} & \cdots & n^{p_1} \\ 1^{p_2} & 2^{p_2} & \cdots & n^{p_2} \\ \vdots & \vdots & \ddots & \vdots \\ 1^{p_{n-1}} & 2^{p_{n-1}} & \cdots & n^{p_{n-1}} \end{pmatrix}$$

Prove that

$$\max_k |v_k| \geq \frac{2}{n^2+n} \prod_{i=1}^{n-1} p_i.$$

Solution The matrix

$$M = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1^{p_1} & 2^{p_1} & \cdots & n^{p_1} \\ 1^{p_2} & 2^{p_2} & \cdots & n^{p_2} \\ \vdots & \vdots & \ddots & \vdots \\ 1^{p_{n-1}} & 2^{p_{n-1}} & \cdots & n^{p_{n-1}} \end{pmatrix}$$

is a square submatrix of a Vandermonde matrix with distinct positive eigenvalues. A property of such matrices is that they are invertible. Some details can be found on https://math.stackexchange.com/questions/1781867/.

The vector v is non-trivial, so it does not lie in the kernel of M. Hence $\sum_{k=1}^n kv_k \neq 0$. Reducing modulo p_i, we find that $p_i \mid \sum_{k=1}^n kv_k$ for all $i \in \{1, 2, \ldots, n-1\}$ and therefore

$$\binom{n+1}{2} \max_k |v_k| \geq \left| \sum_{k=1}^n kv_k \right| \geq \prod_{i=1}^{n-1} p_i.$$

Note from the editors: Since there are some details missing on proving this interesting property of square submatrices of Vandermonde matrices with distinct positive eigenvalues, we do not consider this a complete solution. Finding said details however is a good reason to look into Schur polynomials.