Problemen

| Problem Section

Edition 2020-1 We received solutions from Hendrik Reuvers and Jaap Spies. The solution deadline was supposed to be 15 April rather than 15 March. We apologize for the mistake, and thank Jaap Spies and Hendrik Reuvers for pointing it out. Since there were a few questions about the deadline: We try to accept solutions that arrive (shortly) after the deadline as well. In Problem 2020-1/A there was a small typo in part b; the letter T should have been τ. We thank Henry Ricardo for paying attention.

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 We received a partial solution from Hendrik Reuvers.

For part a, we prove that τ is a permutation if and only if n is a power of 2.

Suppose n is not a power of 2, say $n = n_1 n_2$ with n_1 odd and n_2 a power of 2. Suppose that $n_1 > 1$. We find $0 \le m_1 < m_2 \le n-1$ with $\tau(m_1) = \tau(m_2)$. If $2n_2 \ge n_1 + 1$, let $m_1 = (2n_2 - n_1 - 1)/2$ and $m_2 = (2n_2 + n_1 - 1)/2$. Otherwise, we have $2n_2 \le n_1 - 1$, and we let $m_1 = (n_1 - 1 - 2n_2)/2$ and $m_2 = (2n_2 + n_1 - 1)/2$. In both cases, we find $0 \le m_1 < m_2 \le n-1$ and $\tau(m_1) = \tau(m_2)$. So n must be a power of 2.

Conversely, suppose that n is a power of 2, and suppose that $m(m+1)/2 = m'(m'+1)/2 \bmod n$ with $m, m' \in [n]$. Since 2 is not invertible $\bmod n$, this is the case if and only if $m(m+1) = m'(m'+1) \bmod 2n$. We can reduce this to $(m-m')(m+m'+1) = 0 \bmod 2n$. Since precisely one of $m-m'$ and $m+m'+1$ is even, we find that either $m = m' \bmod 2n$ or $m + m' + 1 = 0 \bmod 2n$. This second case is not possible since $0 < m + m' + 1 < 2n$, hence $m = m' \bmod 2n$, and in particular $m = m'$. This shows that τ is injective and hence a permutation.

The answer to part b is that τ has sign 1 if $n = 1$ or $n = 2$ (can be verified immediately), and sign -1 if $n = 2^k$ with $k \ge 2$.

Suppose that $n = 2^k$ with $k \ge 2$. Define $s : [n] \to [n]$ by $s(2x) = x$ and $s(2x+1) = n - x - 1$ for $x \in [n/2]$. Observe that for $x \in [n]$, we have $\tau[x] = s(x)(1 + 2s(x)) \bmod n$. We first show that s is an even permutation of $[n]$. It is clear that $s(x)$ is a permutation. For $1 \le i \le n-2$, we let s_i be the permutation of $[n]$ obtained by fixing $0, \ldots, i-1$ and mapping x to $n - 1 + i - x$ otherwise. Observe that $s_{i+1} \circ s_i$ fixes $0, \ldots, i-1$, maps $n-1$ to i, and maps x to $x+1$ otherwise. This is an even permutation if i is odd. We readily verify that $s_{n-2} \circ s_{n-1} \circ \cdots \circ s_1 \circ s = \mathrm{id}_{[n]}$. From this, we conclude that s is an even permutation.

To show that τ is an odd permutation, it now suffices to show that $\tau \circ s^{-1}$ is an odd permutation. Since $\tau(x) = s(x)(1 + 2s(x))$, we find that $\tau \circ s^{-1}(x) = x + 2x^2 \bmod n$ for all $x \in [n]$. The following lemma then finishes the proof.

Lemma. *Let $f(X) = aX^2 + bX + c \in \mathbb{Z}[X]$ be a polynomial and suppose that a is even and b is odd. Let $n \ge 4$ be a power of 2. Then the map $f_n : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $x \mapsto f(x)$ is a permutation and has sign*

$$\epsilon(f_n) = a + b + 2c \bmod 4,$$

where we identify the group of signs $\{\pm 1\}$ with the subgroup of order 2 in $\mathbb{Z}/4\mathbb{Z}$.

Proof. We prove this by induction on n. First note that for $n = 2$ the sign of such a polynomial permutation is 1 if and only if c is even.

We first prove the base case $n = 4$. We can verify that the translation $X \mapsto X + c$ has sign $1 + 2c$, so we may assume without loss of generality that $c = 0$. Now 0 and 2 are fixed elements of f_4. Moreover, we have that $1 \mapsto 1 \bmod 4$ if and only if $a + b \equiv 1 \bmod 4$ (and $1 \mapsto 3$ otherwise), and $3 \mapsto 3 \bmod 4$ if and only if $a + b \equiv 1 \bmod 4$ (and $3 \mapsto 1$ otherwise).

Now let $N > 4$ be a power of 2 and assume that the lemma is true for all $n < N$. Again, we may assume that $c = 0$. Indeed, the translation $X \mapsto X + 1$ is simply an N-cycle and hence an odd permutation; all other translations are simply repeated applications of this translation.

Redactie: Onno Berrevoets, Rob Eggermont en Daan van Gent

problems@nieuwarchief.nl

www.nieuwarchief.nl/problems

Oplossingen | Solutions

The sets $2\mathbb{Z}$ and $2\mathbb{Z}+1$ are invariant sets of the polynomial function f. Consider the polynomials $g(X) := f(2X)/2 \in \mathbb{Q}[X]$ and $h(X) := (f(2X+1)-1)/2 \in \mathbb{Q}[X]$. Then

$$g(X) = 2aX^2 + bX,\ h(X) = 2aX^2 + (2a+b)X + \tfrac{a+b-1}{2}.$$

We see that $g(X), h(X) \in \mathbb{Z}[X]$ both satisfy the posed conditions of the lemma on f. Therefore, they respectively induce permutations $g_{N/2}, h_{N/2} : \mathbb{Z}/(N/2)\mathbb{Z} \to \mathbb{Z}/(N/2)\mathbb{Z}$. Notice that $g_{N/2}$ and $h_{N/2}$ have the same sign as the permutation of f_N on the set $\{\overline{0}, \overline{2}, \ldots, \overline{N-2}\} \subset \mathbb{Z}/N\mathbb{Z}$ (even classes) and $\{\overline{1}, \overline{3}, \ldots, \overline{N-1}\}$ (odd classes) respectively. Hence, we find that $\epsilon(f_N) = \epsilon(g_{N/2})\epsilon(h_{N/2})$. By applying the induction hypothesis on $g_{N/2}$ and $h_{N/2}$ we see that

$$\begin{aligned}\epsilon(g_{N/2})\epsilon(h_{N/2}) &= (2a+b)\cdot(2a+(2a+b)+(a+b-1)) \\ &\equiv b(a+1) \equiv a+b \bmod 4.\end{aligned}$$

This proves that $\epsilon(f_N) = a+b \bmod 4$. This concludes the proof of the lemma. We conclude that τ has odd sign if $n = 2^k$ with $k \geq 2$.

Thijmen Krebs provided a more direct solution to part b of this problem:

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.

Problem 2020-1/B (proposed by Onno Berrevoets)

Let G be a finite group of order n. A map $f : G \to \mathbb{R}$ is called a near-homomorphism if for all $x, y \in G$, we have $|f(xy) - f(x) - f(y)| \leq 1$.

a. Show that for every near-homomorphism f from $G \to \mathbb{R}$, we have $\operatorname{diam}(f[G]) := \sup_{x,y\in G} |f(x) - f(y)| \leq 2 - 2/n$.

b. Show that if G is cyclic, then there exists a near-homomorphism $f : G \to \mathbb{R}$ with $\operatorname{diam}(f[G]) = 2 - 2/n$.

Solution We received a partial solution from Hendrik Reuvers.

For part a, let f be a near-homomorphism from G to $\mathbb{R}$, and let $a, b \in G$ with $f(b) - f(a) = \operatorname{diam}(f[G]) =: D$. For all $x \in G$, we have

Oplossingen | Solutions

$$f(bx)-f(ax)=(f(bx)-f(b)-f(x))-(f(ax)-f(a)-f(x))+f(b)-f(a)$$
$$\geq -2+f(b)-f(a)=D-2.$$

Summing over x, we find

$$0=\sum_{x\in G} f(bx)-f(ax)=f(b)-f(a)+\sum_{x\in G\setminus\{1\}} f(bx)-f(ax)$$
$$\geq D+(n-1)*(D-2)=nD-2(n-1).$$

This reduces to $D\leq 2-2/n$ as required.
For part b, if G is cyclic with generator g, the function $f:G\to\mathbb{R}$ given by $f(g^k):=(2k-n)/n$ for $k\in\{0,1,\ldots,n-1\}$ is a near-homomorphism satisfying the requirements.

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 Hendrik Reuvers and Jaap Spies submitted partial solutions. The current solution was provided by Hendrik Lenstra.
Consider the subring of $\mathrm{End}(A)$ generated by $\epsilon=\sigma-1$. This subring is commutative. Note that both 2 and ϵ are nilpotent, the latter because $\epsilon^{2^k}\equiv\sigma^{2^k}-1\equiv 0 \bmod 2$ for k sufficiently large. This means that the ideal $m=(2,\epsilon)$ satisfies $m^k=0$ for k sufficiently large. Let k be minimal such that $m^k=0$. Then the chain of subgroups m^iA is strictly descending for $i=0,\ldots,k$. In particular, A/m^iA has order at least 2^i for $i\leq k$. Moreover, we find $k\leq n$, meaning $m^n=0$.
We first prove that $A/(2\epsilon(2-\epsilon)A)$ has order at least 2^4. Since $2\epsilon(2-\epsilon)\in m^3$, this is obvious if A/m^3A has order at least 2^4. So suppose that the latter only has order 2^3. Then we also find A/m^iA has order 2^i for $i=1,2,3$. For $r\in\{2,\epsilon,2-\epsilon\}$, consider the group homomorphism $f_r:A/mA\to mA/m^2A$ (both of these are groups of order 2) sending $a+mA$ to $ra+m^2A$. Because $f_2-f_\epsilon=f_{2-\epsilon}$, these three cannot all be isomorphisms, so at least one of the three is 0. For this r, we find $rA\subseteq m^2A$, and multiplying with the other two gives us $2\epsilon(2-\epsilon)A\subseteq m^4A$, so we find that $A/(2\epsilon(2-\epsilon)A)$ has order at least 2^4.
Finally, we use this to prove that $\sigma^{2^{n-2}}-1=0$. The former equals $(1+\epsilon)^{2^{n-2}}-1$. We use Newton's binomium to expand $(1+\epsilon)^{2^{n-2}}$. Note that if $i=2^ku$ with u odd, then the number of factors 2 in $\binom{2^{n-2}}{i}$ equals $n-2-k$ if $0<i<2^{n-2}$. This tells us that all terms with $i>2$ in the expansion of $(1+\epsilon)^{2^{n-2}}$ lie in m^n and hence equal 0. It follows that

$$(1+\epsilon)^{2^{n-2}}-1=2^{n-2}\epsilon+2^{n-3}(2^{n-2}-1)\epsilon^2$$
$$=2^{n-2}\epsilon-2^{n-3}2\epsilon^2$$
$$=2^{n-4}2\epsilon(2-\epsilon).$$

Above, we showed that $2\epsilon(2-\epsilon)A$ has order at most 2^{n-4}. We find that $2^{n-4}2\epsilon(2-\epsilon)A=0$, from which we conclude $\sigma^{2^{n-2}}-1=0$.

Thijmen provided a more direct solution to this problem.

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 $B:=A\setminus(G\cdot x)$, 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

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

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 $n \geq 4$.