Problem

Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome. We will select the most elegant solutions for publication. For this, solutions should be received before **15 October 2019**. The solutions of the problems in this issue will appear in the next issue. Problem C, part b is a star exercise; we do not know a solution to this problem.

Problem A (proposed by Hendrik Lenstra)

Let $\tau : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ be the map such that $\tau(n)$ is the number of positive divisors of n for any $n \in \mathbb{Z}_{>0}$. Show that there are uncountably many maps $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that $f \circ f = \tau$.
Note: This is a follow-up to Problem A of the March 2018 edition.

Problem B (proposed by Daan van Gent)

Let X be a set and $* : X^2 \to X$ a binary operator satisfying the following properties:
1. $(\forall x \in X)\; x * x = x$;
2. $(\forall x,y,z \in X)\; (x*y)*z = (y*z)*x$.

Show that there exits an injective map $f : X \to 2^X$ that for all $x,y \in X$ satisfies $f(x*y) = f(x) \cap f(y)$.

Problem C (proposed by Onno Berrevoets)

a. Does there exist an infinite set $X \subset \mathbb{Z}_{>0}$ such that for all pairwise distinct $a,b,c \in X$ and all $n \in \mathbb{Z}_{>0}$ we have $\gcd(a^n + b^n, c) = 1$?

b.* Does there exist an infinite set $X \subset \mathbb{Z}_{>0}$ such that for all pairwise distinct $a,b,c,d \in X$ and all $n \in \mathbb{Z}_{>0}$ we have $\gcd(a^n + b^n + c^n, d) = 1$?

Edition 2019-2 We received solutions from Pieter de Groen, Marcel Roggeband, Rik Biel and Alex Heinis.

Problem 2019-2/A (proposed by Arthur Bik)

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathrm{SO}(3)$$

be a matrix not equal to the identity matrix. Prove: if the vector

$$\begin{pmatrix} (a_{23}+a_{32})^{-1} \\ (a_{13}+a_{31})^{-1} \\ (a_{12}+a_{21})^{-1} \end{pmatrix}$$

exists, then A is a rotation using this vector as axis.

Solution We received solutions from Pieter de Groen and Marcel Roggeband. The solution below is based on the solution by Marcel.
We write

$$v = \begin{pmatrix} (a_{23}+a_{32})^{-1} \\ (a_{13}+a_{31})^{-1} \\ (a_{12}+a_{21})^{-1} \end{pmatrix}.$$

Redactie: Onno Berrevoets, Rob Eggermont en Daan van Gent
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Since $A \in \mathrm{SO}(3)$, we know that A is a rotation matrix. Since v exists, we also know A is not the identity matrix. In particular, this means that A has a 1-dimensional eigenspace associated with eigenvalue 1 spanned by the rotation axis. It therefore suffices to show $Av = v$. Since A is orthogonal, the sum of squares of all entries in a row of A equals 1, and likewise the sum of squares of all entries in a column of A equals 1. Comparing the sum of squares of the first row and the first column of A gives us

$$a_{11}^2 + a_{12}^2 + a_{13}^2 = 1 = a_{11}^2 + a_{21}^2 + a_{31}^2,$$

and rearranging terms gives

$$a_{21}^2 - a_{12}^2 = a_{13}^2 - a_{31}^2.$$

Dividing by $a_{13} + a_{31}$ and by $a_{21} + a_{12}$ gives us

$$\frac{a_{21} - a_{12}}{a_{13} + a_{31}} = \frac{a_{13} - a_{31}}{a_{21} + a_{12}}.$$

We can re-arrange this to

$$\frac{a_{21}}{a_{13} + a_{31}} + \frac{a_{31}}{a_{21} + a_{12}} = \frac{a_{12}}{a_{13} + a_{31}} + \frac{a_{13}}{a_{21} + a_{12}}.$$

It follows that the first entry of Av and $A^T v$ are equal. Similar computations for the remaining rows and columns of A give us $Av = A^T v$. Since $A \in \mathrm{SO}(3)$, we have $A^T = A^{-1}$, so we find $A^2 v = v$. Likewise, we have $A^2(Av) = A(A^2 v) = Av$, so both v and Av are eigenvectors of A^2 with eigenvalue 1. If A^2 is not the identity matrix, it follows that v is the rotation axis of A^2. In this case, it is also the rotation axis of A, so we find $Av = v$. This leaves the case $A^2 = I$ (but $A \neq I$).

In the case $A^2 = I$, we find that A is a rotation around some vector of π radians. In particular, for any vector u in the plane of rotation, we find $(A + I)u = 0$. Moreover, $A + I$ fixes the rotation axis of A, so $A + I$ is a matrix of rank one with the rotation axis of A as its image. In particular, all columns of

$$\begin{pmatrix} a_{11}+1 & a_{12} & a_{13} \\ a_{21} & a_{22}+1 & a_{23} \\ a_{31} & a_{32} & a_{33}+1 \end{pmatrix}$$

are multiples of each other. Note that we also have $A^T = A$, so since v exists, we find that no off-diagonal entries are zero. Finally, we observe that in the first column of $A + I$, the ratio between the second and third entry equals the ratio between second and third entry of v (using $a_{12} = a_{21}$ and $a_{13} = a_{31}$), and in the second column of $A + I$, the ratio between the first and third entry equals the ratio between the first and third entry of v. Since there are no zeroes involved, we find that v lies in the image of $A + I$, and therefore A must be a rotation around v.

An alternative solution by Pieter de Groen uses the fact that A can be described by means of Euler–Rodrigues parameters.

Problem 2019-2/B (proposed by Onno Berrevoets)

1. Let $k \in \mathbb{Z}_{>0}$ and let $\mathcal{X} \subset 2^{\mathbb{Z}}$ be a subset such that for all distinct $A, B \in \mathcal{X}$ we have $\#(A \cap B) \leq k$. Prove that $\mathcal{X}$ is countable.
2. Does there exist an uncountable set $\mathcal{X} \subset 2^{\mathbb{Z}}$ such that for all distinct $A, B \in \mathcal{X}$ we have $\#(A \cap B) < \infty$?

Solution We received solutions from Rik Biel and Alex Heinis. The solution below is based on the solution by Alex.

For the first part of the problem, we replace $\mathbb{Z}$ by $\mathbb{N}$ without loss of generality. Since $\mathbb{N}$ only has countably many finite subsets, it suffices to show that $\mathcal{X}$ only contains countably many infinite sets. Without loss of generality, we assume that $\mathcal{X}$ contains no finite sets. Let S be the collection of subsets of $\mathbb{N}$ of cardinality $k+1$. Now define $f : \mathcal{X} \to S$ by mapping $A \in \mathcal{X}$ to the set consisting of its smallest $k+1$ elements. By the assumption that $A, B \in \mathcal{X}$ share at most k elements, the map f must be injective. Since S is countable, $\mathcal{X}$ must also be countable.

For the second part, the answer is yes. We replace $\mathbb{Z}$ by $\mathbb{N}^2$ without loss of generality. For $a > 0$, let $p_n = \lfloor na \rfloor$ for $n \in \mathbb{Z}_{>0}$. This defines a sequence $\frac{p_n}{n}$ that converges to a as $n \to \infty$. Note that for all n, we have $0 \le a - \frac{p_n}{n} < \frac{1}{n}$. Define $S_a := \{(p_1,1),(p_2,2),\dots\} \in 2^{\mathbb{N}^2}$. It is quickly verified that if $b \neq a$, the sets S_a and S_b share only finitely many elements, since if $|b-a| \ge \frac{1}{N}$, we find $\lfloor na \rfloor \neq \lfloor nb \rfloor$ for all $n \ge N$. This implies that for all $a,b > 0$ with $a \neq b$, the intersection $S_a \cap S_b$ is finite. In particular, the set $\mathcal{X} = \{S_a : a \in \mathbb{R}_{>0}\}$ is an uncountable set satisfying the desired properties.

Problem 2019-2/C (proposed by Onno Berrevoets)

Let $A : \mathbb{R}^2 \to \mathbb{R}$ be a continuous function such that for every $x,y,z \in \mathbb{R}$ we have

1. $A(x,y) = A(y,x)$,
2. $x \le y \Rightarrow A(x,y) \in [x,y]$,
3. $A(A(x,y),z) = A(x,A(y,z))$,
4. A is not the $\max$ and not the $\min$ function.

Prove that there exists an $a \in \mathbb{R}$ such that for all $x \in \mathbb{R}$ we have $A(x,a) = a$.

Solution For simplicity we write $x \oplus y := A(x,y)$ for all $x,y \in \mathbb{R}$. The binary operator $\oplus$ is then symmetric and associative by properties 1 and 3. We consider three subsets $X_<, X_0, X_>$ of $\mathbb{R}$ defined by

$$\begin{aligned} X_< &:= \{x \in \mathbb{R} \mid \exists y \in \mathbb{R} \mid x \oplus y < x\}, \\ X_0 &:= \{x \in \mathbb{R} \mid \forall y \in \mathbb{R} \mid x \oplus y = x\}, \\ X_> &:= \{x \in \mathbb{R} \mid \exists y \in \mathbb{R} \mid x \oplus y > x\}. \end{aligned}$$

Then it is clear that $X_< \cup X_0 \cup X_> = \mathbb{R}$. Moreover, $X_<$ and $X_>$ are open subsets of $\mathbb{R}$ by continuity of A. Since A is not the $\min$ function, it follows that there exist $x,y \in \mathbb{R}$ such that $x \le y$ and $x \oplus y > x$. Hence, $X_> \neq \varnothing$. It follows similarly from $A \neq \max$ that $X_< \neq \varnothing$. We will show that $X_> \cap X_< = \varnothing$, which yields the desired result $X_0 \neq \varnothing$ because of the connectedness of $\mathbb{R}$.

Suppose that $X_< \cap X_> \neq \varnothing$. We will derive a contradiction. Let $x \in X_< \cap X_>$. Let $y,z \in \mathbb{R}$ be such that $x \oplus y < x$ and $x \oplus z > x$. Without loss of generality we have $x \oplus y \oplus z \ge x$. We also have

$$x \oplus y \oplus y = x \oplus (y \oplus y) = x \oplus y < x.$$

The map $\zeta \mapsto x \oplus y \oplus \zeta$ is continuous since A is continuous, and by the intermediate value theorem we find that $x \oplus y \oplus w = x$ for some $w \in \mathbb{R}$. But now we arrive at a contradiction:

$$x > x \oplus y = (x \oplus y \oplus w) \oplus y = x \oplus (y \oplus y) \oplus w = x \oplus y \oplus w = x.$$

Therefore, $X_< \cap X_> = \varnothing$ and we conclude that $X_0 \neq \varnothing$.