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 January 2020**. The solutions of the problems in this issue will appear in the next issue.

Problem A (proposed by Onno Berrevoets)

Let $F \in \mathbb{Z}[X]$ be a monic polynomial of degree 4. Let $A \subset \mathbb{Z}$ with $\#A \geq 5$ be such that for all $a \in A$ we have $2^{2019} \mid F(a)$. Prove that there exist distinct $a, a' \in A$ such that $a \equiv a' \bmod 2^{202}$.

Problem B (proposed by Jan Draisma)

Let $n \in \mathbb{Z}_{\geq 2}$ and let S be a non-empty subset of $\{1, 2, \ldots, n-1\}$.

1. Prove that there exists an n-th root of unity $z \in \mathbb{C}$ such that the real part of $\sum_{i \in S} z^i$ is smaller than or equal to $-\frac{1}{2}$.
2. Suppose that n is not a power of 2. Prove that the $-\frac{1}{2}$ in the previous part is optimal in the following sense: there exists a non-empty subset S of $\{1, 2, \ldots, n-1\}$ such that for all n-th roots of unity z, the real part of $\sum_{i \in S} z^i$ is at least $-\frac{1}{2}$.

Problem C (proposed by Onno Berrevoets)

Let $n \geq 1$ be an integer. Denote by S_n the permutation group on $\{1, \ldots, n\}$. An element $\sigma \in S_n$ is called *representable* if there exists a polynomial $f \in \mathbb{Z}[X]$ such that for all $x \in \{1, \ldots, n\}$ we have $\sigma(x) = f(x)$. What is the number of representable elements of S_n?

Edition 2019-3 We received solutions from Hans Samuels Brusse, Hans van Luipen and Thijmen Krebs.

Problem 2019-3/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.

Solution This solution is based on the solution by Thijmen Krebs.
We can construct uncountably many such maps f as follows. Let $S_1 \cup S_0$ be a partition of the odd primes with S_1 infinite, and let $g_1 : S_1 \to S_0$ be any surjection. Inductively on $i \geq 2$, let $S_i := \tau^{-1}(S_{i-2})$ and pick any surjection $g_i : S_i \to S_{i-1}$ such that for all $n \in S_{i-2}$, we have $g_i(\tau^{-1}(n)) = g_{i-1}^{-1}(n)$ (and in particular, $g_{i-1} \circ g_i = \tau|_{S_i}$). Note that such a surjection exists because $\tau^{-1}(n)$ is (countably) infinite for any $n \in \mathbb{Z}_{>1}$. For example, $\tau^{-1}(n)$ contains p^{n-1} for all primes p.
It is easy to verify that the S_i are disjoint. Moreover, $(S_i)_{i \geq 0}$ forms a partition of $\mathbb{Z}_{>2}$, since for all $n > 2$ we have $2 \leq \tau(n) < n$, meaning there is an $i > 0$ such that $\tau^i(n) = 2$ (which means either $n \in S_{2i-1}$ or $n \in S_{2i-2}$). We now define f by $f(1) = 1$, $f(n) = 2$ for $n \in \{2\} \cup S_0$, and $f(n) = g_i(n)$ for $n \in S_i$ with $i \geq 1$. This gives a well-defined map from $\mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$. We readily verify that $f^2(1) = 1 = \tau(1)$, $f^2(n) = 2 = \tau(n)$ for n prime, and $f^2(n) = g_{i-1}(g_i(n)) = \tau(n)$ for $n \in S_i$ with $i \geq 2$. Since there are uncountably many infinite subsets of the primes, the choice of S_1 is already sufficient to show there are uncountably many possible f satisfying $f \circ f = \tau$.

Redactie: Onno Berrevoets, Rob Eggermont en Daan van Gent

problems@nieuwarchief.nl

www.nieuwarchief.nl/problems

Problem 2019-3/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 $f(x*y) = f(x) \cap f(y)$.

Solution This solution is based on the solutions by Hans van Luipen and Hans Samuels Brusse.
We first prove that $*$ is commutative. We have

$$(x*y)*x = (y*x)*x = (x*x)*y = x*y.$$

Using this and the given properties of $*$, we find

$$x*y = (x*y)*(x*y) = (y*(x*y))*x = ((x*y)*x)*y = (x*y)*y = (y*y)*x = y*x,$$

so indeed $*$ is commutative. We can now also prove that $*$ is associative, since

$$(x*y)*z = (y*z)*x = x*(y*z)\,.$$

For $a \in X$, we define $f(a) = \bigcup_{x \in X} \{a*x\}$. If $c \in f(a) \cap f(b)$, there exist $x,y \in X$ such that $c = a*x = b*y$. This means

$$c = a*x = (a*a)*x = a*(a*x) = a*(b*y) = (a*b)*y = y*(a*b) \in f(a*b)\,.$$

Conversely, if $c \in f(a*b)$, there is $x \in X$ such that $c = (a*b)*x$, so $c = a*(b*x) \in f(a)$, and likewise, $c = (b*a)*x = b*(a*x) \in f(b)$, so we find $c \in f(a) \cap f(b)$. We conclude

$$f(a*b) = f(a) \cap f(b)\,.$$

It remains to show that f is injective. Suppose that $f(a) = f(b)$. Then there are $x,y \in X$ such that $b = a*x$ and $a = b*y$. Observe that

$$a*b = (b*y)*b = (b*b)*y = b*y = a,$$

and by a symmetrical argument, we conclude

$$a = a*b = b*a = b.$$

So f is injective, as was to be shown.

Problem 2019-3/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 $\gcd(a^n+b^n+c^n, d) = 1$?

Solution We received a solution to part a by Thijmen Krebs. Part b remains open.
Let X be the set of squares p^2 for each prime $p \equiv 3 \pmod 4$. We verify that $p^{2n}+q^{2n}$ is relatively prime to r^2 for any $n \in \mathbb{Z}_{>0}$. Indeed, if it were not, then we would have $p^{2n}+q^{2n} \equiv 0 \pmod r$. Since q is invertible modulo r, we can rewrite this as $(pq^{-1})^{2n} \equiv -1 \pmod r$. This would give a contradiction, since the left hand side is a square, but -1 is not a square modulo r if $r \equiv 3 \pmod 4$.