Problemen

| Problem Section

Edition 2010-4 We have received correct solutions from R. Kortram, Charles Delorme, Alex Heinis, Rik Bos, Rob van der Waall, Thijmen Krebs, Shai Como, José Nieto, Anton Schep, Paolo Perfetti, and Moubinool Omarjee.

Problem 2010-4/A Show that there are infinitely many prime numbers p for which there is a positive integer n with

$$2^{n^2+1} \equiv 3^n \pmod{p}.$$

Also, show that there are infinitely many prime numbers p for which there is no such n.

Solution We received a correct solution from R. Kortram, Charles Delorme, Alex Heinis, Rik Bos, Rob van der Waall and Thijmen Krebs. The book token goes to Rik Bos.
Let P be the set of primes that divide at least an element of the form $2^{n^2+1} - 3^n$ with n a positive integer. The set P is nonempty, because it contains 23, and we will prove that it has infinitely many elements.
Suppose, by contradiction, that P is a nonempty finite set of primes containing 23 and let n be $\prod_{p\in P}(p-1)$. Since n is greater than 1, the integer $2^{n^2+1} - 3^n$ has at least one prime factor q different from 2 and 3. Then, by Fermat's little theorem we get

$$2^{n^2+1} - 3^n \equiv 1 \bmod q,$$

contradicting the fact that q divides $2^{n^2+1} - 3^n$. Therefore, the set P contains infinitely many elements.
Let p be a prime such that $p \equiv 19 \bmod 24$. By quadratic reciprocity neither 2 nor 3 is a square modulo p. Since n^2+1 and n have different parity for every positive integer n, the congruence $2^{n^2+1} \equiv 3^n \bmod p$ has a square on one side and a non-square on the other one. Hence, it cannot hold and p is not contained in P. By Dirichlet's theorem on arithmetic progressions there are infinitely many primes congruent to 19 modulo 24. This proves the second part of the problem.

Problem 2010-4/B Let $f\colon \mathbb{R} \to \mathbb{R}$ be a continuous function that has a local minimum or maximum at every point of $\mathbb{R}$. Show that f is constant.

Solution We received a correct solution or reference from R. Kortram, Charles Delorme, Shai Como, José Nieto, Anton Schep, Alex Heinis, Paolo Perfetti, and Thijmen Krebs. The book token goes to Alex Heinis.
Indeed, the following result can be found in several places in the literature.

Proposition. *For any function $f\colon \mathbb{R} \to \mathbb{R}$, there are at most countably many $s \in \mathbb{R}$ for which f has a local extreme value s at some point in $\mathbb{R}$.*

Proof. Let S be the set of values $s \in \mathbb{R}$ for which f has a local maximum s at some point in $\mathbb{R}$. For each $s \in S$ we can choose rational numbers $a < b$ such that the absolute maximum of f on the interval (a, b) equals s. This yields an injective map $S \to \mathbb{Q} \times \mathbb{Q}$ sending s to (a, b), so S is countable. The same holds for the set of values of f at local minima.
Now let f be as given in the problem. If f is not constant, then by the intermediate value theorem f takes uncountably many values, contradicting the proposition.

Problem 2010-4/C Let $f\colon \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ be a function such that for all $a \in \mathbb{Q}$ the functions $x \mapsto f(a, x)$ and $x \mapsto f(x, a)$ are polynomial functions from $\mathbb{Q}$ to $\mathbb{Q}$. Is it true that f is given by a polynomial in two variables? What if we replace $\mathbb{Q}$ by $\mathbb{R}$?

Redactie:
Johan Bosman
Gabriele Dalla Torre
Ronald van Luijk
Lenny Taelman
Wouter Zomervrucht

Problemenrubriek NAW
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Oplossingen | Solutions

Solution This problem was solved by Alex Heinis, R.A. Kortram, José Nieto, Moubinool Omarjee, and Anton Schep. This solution is based on the one by José Nieto, who wins the book token. For the case $f\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}$ the answer is no. The following is a counterexample. Since $\mathbb{Q}$ is countable, there exists an enumeration $a_1, a_2, a_3, \ldots$ of $\mathbb{Q}$. Now define

$$f_n(x) = \prod_{i=1}^{n}(x - a_i)$$

for $n \geq 1$, and

$$f(x,y) = \sum_{n=1}^{\infty} f_n(x) f_n(y).$$

This is well-defined on $\mathbb{Q}\times\mathbb{Q}$, since $f_n(a_i)$ equals 0 for $n \geq i$. Furthermore, the specialisation

$$f(x,a_k) = f(a_k,x) = \sum_{n=1}^{k-1}\prod_{i=1}^{n}(a_k - a_i)(x - a_i)$$

is a polynomial in x of degree $k-1$, so f satisfies the conditions. If f were a polynomial in x and y, of a certain total degree d, then $f(x,a_{d+2})$ would be of degree at most d. Yet we have seen that $f(x,a_{d+2})$ has degree $d+1$. We conclude that f is not a polynomial.
Now suppose $f\colon \mathbb{R}\times\mathbb{R}\to\mathbb{R}$ is as stated. We will prove that in this case f is indeed given by a polynomial. The elements

$$p_n = x(x-1)\cdots(x-n+1), \qquad n \geq 0$$

form a linear basis of the polynomial ring $\mathbb{R}[x]$, so for all $a \in \mathbb{R}$ we can write $f(x,a)$ as a finite linear combination of the polynomials p_n. Hence there are functions $c_n : \mathbb{R}\to\mathbb{R}$ such that the equality

$$f(x,y) = \sum_{n=0}^{\infty} c_n(y) p_n(x) \tag{1}$$

holds for all $x, y \in \mathbb{R}$, while for each $a \in \mathbb{R}$, we have $c_n(a) = 0$ for all but finitely many n. The assumption that for each $r \geq 0$, the function

$$f(r,y) = \sum_{n=0}^{r} \frac{r!}{(r-n)!} c_n(y)$$

is a polynomial in y, shows by induction on n that $c_n(y)$ is a polynomial for each $n \geq 0$. We now claim that c_n is identically zero for almost all $n \geq 0$. Assume that there are infinitely many $n \geq 0$ such that the polynomial c_n is non-zero. Each of these polynomials has finitely many zeros, so together they have at most countably many. On the other hand, for all $a \in \mathbb{R}$ at least one (in fact infinitely many) of these non-zero polynomials has a zero at a, giving uncountably many zeros. This contradiction proves the claim, so (1) shows that f is itself a polynomial.
R.A. Kortram and Anton Schep refer to the article 'Some Analogues of Hartog's Theorem in an Algebraic Setting' by R.S. Palais, *American Journal of Mathematics*, Vol. 100. It contains a proof of the following, slightly more general fact: the statement of this problem holds for a field k if and only if k is finite or uncountable.