Problemen

| Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome.
For each problem, the most elegant correct solution will be rewarded with a book token worth € 20. At times there will be a Star Problem, to which the proposer does not know any solution. For the first correct solution sent in within one year there is a prize of € 100.
When proposing a problem, please either include a complete solution or indicate that it is intended as a Star Problem. Electronic submissions of problems and solutions are preferred (problems@nieuwarchief.nl).
The deadline for solutions to the problems in this edition is 1 June 2013.

Problem A (folklore)

Consider a regular n-gon $P_1P_2\dots P_n$, and draw $n-3$ diagonals such that there are no intersection points in the interior. The polygon is now divided into $n-2$ triangles. Let t_i be the number of such triangles that have a vertex at P_i. Show that

$$t_1 - \cfrac{1}{t_2 - \cfrac{1}{\dots - \cfrac{1}{t_{n-1}}}} = 0.$$

Problem B (MSRI Emissary)

You are allowed to transform positive integers n in the following way. Write n in base 2. Write plus signs between the bits at will (at most one per position), and then perform the indicated additions of binary numbers. For example, $123_{10} = 1111011$ can get + signs after the second, third and fifth bits to become $11+1+10+11 = 9_{10}$; or it can get + signs between all the bits to become $1+1+1+1+0+1+1 = 6_{10}$; and so on.
Prove that it is possible to reduce arbitrary positive integers to 1 in a bounded number of steps. That is, there is a constant C such that for any n there is a sequence of at most C transformations that starts with n and ends at 1.

Problem C (proposed by Jinbi Jin)

Let R be a commutative ring with 1. Consider the set

$$S = \left\{(i,j) \in R^2 : i^2 = i, j^2 = j, ij = 0\right\}.$$

Show that the cardinality of S is a power of 3 if S is finite.

Rectification. In Problem C of the previous issue (2012-4), the circles A, B, and C should not have collinear centres.

Redactie:
Johan Bosman
Gabriele Dalla Torre
Christophe Debry
Jinbi Jin
Ronald van Luijk
Marco Streng
Wouter Zomervrucht

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

Edition 2012-3 We received solutions from Hao Chen (Seattle), Pieter de Groen (Brussels), Alex Heinis (Hoofddorp), Richard Kraaij (Delft), Thijmen Krebs (Nootdorp) and Traian Viteam (Montevideo).

Problem 2012-3/A Let $(X_n)_{n\geq 1}$ be a sequence of independent random variables with values in $\mathbb{R}_{\geq 0}$ satisfying $P(X_i > t) = (1+t)^{-1}$ for all i and all $t \geq 0$. Let $(c_n)_{n\geq 1}$ be a sequence of positive real integers. Show that the sequence $(c_nX_n)_{n\geq 1}$ is bounded with probability 1 if and only if the series $\sum_{n=1}^{\infty} c_n$ converges.

Solution We received solutions from Pieter de Groen, Alex Heinis, Richard Kraaij and Thijmen Krebs. The book token goes to Richard Kraaij. The following solution is based on that of Richard Kraaij.

Lemma 1. *Let $B \in \mathbb{R}_{>0}$, and let $(c_n)_{n\geq 1}$ be a sequence of positive real numbers. Then the series $\sum_{n=1}^{\infty}(1+B/c_n)^{-1}$ converges if and only if the series $\sum_{n=1}^{\infty} c_n$ converges.*

Proof. First suppose that $\sum_{n=1}^{\infty} c_n$ converges. For all n, we have $(1+B/c_n)^{-1} < c_n/B$, so $\sum_{n=1}^{\infty}(1+B/c_n)^{-1}$ converges as well.
Now suppose that $\sum_{n=1}^{\infty}(1+B/c_n)^{-1}$ converges. Note that if n is such that $c_n > B$, then we have $\frac{1}{2} < (1+B/c_n)^{-1}$. Hence there are only finitely many such n.
For the n such that $c_n \leq B$, we have $(2B)^{-1}c_n < (1+B/c_n)^{-1}$. As $c_n \leq B$ holds for all but finitely many n, it follows that $\sum_{n=1}^{\infty} c_n$ converges as well. □

First assume that $\sum_{n=1}^{\infty} c_n$ converges. Fix a real number $B > 0$. Then by Lemma 1, $\sum_{n=1}^{\infty}(1+B/c_n)^{-1}$ converges. So let $\epsilon > 0$, and let N be such that $\sum_{n=N}^{\infty}(1+B/c_n)^{-1} < \epsilon$. Let P denote the probability that $c_iX_i > B$ for infinitely many i, and let P' denote the probability that $c_iX_i > B$ for at least one $i \geq N$. Then

$$P \leq P' \leq \sum_{i=N}^{\infty} P(c_iX_i > B) = \sum_{i=N}^{\infty}(1+B/c_n)^{-1} < \epsilon.$$

So $P < \epsilon$ for all $\epsilon > 0$, so $P = 0$. We deduce that with probability 1, there are only finitely many i such that $c_iX_i > B$, i.e. $(c_nX_n)_{n\geq 1}$ is bounded.
Now assume that $(c_nX_n)_{n\geq 1}$ is bounded with probability 1. For $B > 0$, let P_B denote the probability that for all i, we have $c_iX_i \leq B$. Our assumption then implies that $\lim_{B\to\infty} P_B = 1$, hence we may assume that there exists a $B > 0$ such that $P_B > 0$. Then for all $N > 0$ we have, using that the random variables are independent, and that $1 + x < e^x$ for all $x \neq 0$,

$$\begin{aligned} 0 < P_B \leq \prod_{n=1}^{N} P(c_nX_n \leq B) &= \prod_{n=1}^{N}(1-(1+B/c_n)^{-1}) \\ &< \prod_{n=1}^{N} e^{-(1+B/c_n)^{-1}} = e^{-\sum_{n=1}^{N}(1+B/c_n)^{-1}}. \end{aligned}$$

Hence $-\log(P_B) > \sum_{n=1}^{N}(1+B/c_n)^{-1}$, for all N, so the series $\sum_{n=1}^{\infty}(1+B/c_n)^{-1}$ is bounded and therefore convergent, as its terms are positive. By Lemma 1, it follows that $\sum_{n=1}^{\infty} c_n$ converges as well.

Problem 2012-3/B Determine all pairs (a, b) of positive integers such that there are only finitely many positive integers n for which n^2 divides $a^n + b^n$.

Solution We received solutions from Hao Chen, Alex Heinis, Thijmen Krebs and Traian Viteam. The book token goes to Thijmen Krebs. The following solution is based on those of Alex Heinis and Thijmen Krebs.
We call a pair (a, b) *valid* if a and b are positive integers satisfying the given condition. A pair (a, b) of positive integers that is not valid is called *invalid*. We will show that a pair (a, b) is valid if and only if either $a + b = 3$, or a and b are odd and $a + b = 2^k$ for some k. For any prime p and any nonzero rational number x, we denote the valuation of x at p by $v_p(x)$, so if $x = p^r \cdot \frac{a}{b}$ with r, a, b integers and $p \nmid ab$, then $v_p(x) = r$.

Lemma 1. *Suppose a, b, n are positive integers with $n > 1$ and $n^2 | a^n + b^n$. Then the smallest prime divisor p of n divides $a + b$.*

Proof. The exponent n is coprime with the order $p - 1$ of the group $\mathbb{F}_p^*$, which is either 1 or even, so there is an odd integer m with $nm \equiv 1 \pmod{p-1}$. Hence, the equality $\bar{a}^n = -\bar{b}^n$ in $\mathbb{F}_p^*$ implies $\bar{a} = \bar{a}^{nm} = (-\bar{b}^n)^m = -\bar{b}$, so $\bar{a} + \bar{b} = 0$ in $\mathbb{F}_p$. □

Lemma 2. *Suppose $a, b \geq 1$ are coprime, p is prime with $p|a+b$, and $n > 0$ is odd. Then $v_p(a^n + b^n) = v_p(a+b) + v_p(n)$.*

Proof. Set $s = v_p(a+b) \geq 1$. Suppose $q > 2$ is prime and set $\epsilon = v_p(q) \in \{0, 1\}$. Modulo $p^{s+1+\epsilon}$ we have

$$a^q + b^q = a^q + \left((a+b) - a\right)^q = \sum_{k=1}^{q} \binom{q}{k} (-a)^{q-k} (a+b)^k \equiv q a^{q-1}(a+b),$$

so the lemma follows for $n = q$ from $v_p(a) = 0$. For general n we write $n = q_1 q_2 \ldots q_r$ and use the result for prime exponent repeatedly. □

Suppose $n > 3$ and $n^2 | 1 + 2^n$. Then n is odd and Lemma 1 shows that 3 divides n. The same lemma, applied to $a = 1, b = 2^3$, and $n/3$, shows that the smallest prime divisor of $n/3$ divides $a + b = 9$, so $v_3(n) \geq 2$. This contradicts the inequality

$$2v_3(n) = v_3(n^2) \leq v_3(1 + 2^n) = v_3(1+2) + v_3(n) = 1 + v_3(n)$$

coming from Lemma 2, so the pairs $(a, b) = (1, 2)$ and $(a, b) = (2, 1)$ are valid.
Suppose $a, b > 0$ are odd and $a + b = 2^k$ for some k. Suppose $n > 1$ and $n^2 | a^n + b^n$. Then n is even by Lemma 1, but this contradicts the fact that $4 \nmid a^n + b^n$ for a, b odd and n even. Therefore, the pair (a, b) is valid.
To show that the remaining pairs are invalid, first note that for $a, b > 0$ with greatest common divisor $d > 1$, we have $d^{2k} | a^{d^k} + b^{d^k}$ for every k, so (a, b) is invalid.
Finally, we assume $a, b > 0$ are coprime and $a + b > 4$ is not a power of 2. Without loss of generality we assume $b \geq a$ and hence $b \geq 3$. Set $k = v_2(a+b)$. Then we have $v_2(a^n + b^n) = k$ for any odd n by Lemma 2 if $k > 0$; the same holds trivially if $k = 0$. Since $a + b$ is not a power of 2, we have $a + b \geq 3 \cdot 2^k$. Assuming $n > 0$ is odd and $n^2 | a^n + b^n$, we will construct an odd $m > n$ with $m^2 | a^m + b^m$. From $3^n > 2n^2$ we find

$$a^n + b^n \geq b^n \geq \frac{b}{3} \cdot 3^n > \frac{2b}{3} n^2 \geq \frac{a+b}{3} n^2 \geq 2^k n^2.$$

Hence the integer $(a^n + b^n)/(2^k n^2)$ is odd and bigger than 1, so there is a prime $p > 2$ with $v_p(a^n+b^n) \geq v_p(n^2)+1$. From Lemma 2, applied to a^n, b^n, and p, we conclude $v_p(a^{np}+b^{np}) \geq v_p(n^2)+2$, so for $m = np$ we find $m^2 | a^m + b^m$. Starting with $n = 1$, this allows us to construct an infinite number of odd n such that $n^2 | a^n + b^n$. We conclude that the pair (a, b) is invalid, which finishes the proof.

Problem 2012-3/C Let $f \in \mathbb{Z}[X]$ be a monic polynomial, and let R be the ring $\mathbb{Z}[X]/(f)$. Let U be the set of all $u \in R$ satisfying $u^2 = 1$. Show that U has a ring structure with the following properties: the zero element is 1, the identity element is -1, the sum of two elements in U is their product in R, and the product $*$ in U is such that for all u, v, s, t in U the identity $u * v = s * t$ holds in U if and only if

$$(1-u)(1-v) = (1-s)(1-t)$$

holds in R.

Solution We received no correct solutions to this problem.
Since f is monic, the additive group structure of R is just $\mathbb{Z}^d$, where d is the degree of f, so multiplication by 2 on R is injective and for every element $b \in R$, there is at most one element $a \in R$ with $2a = b$.
We start by showing that if such a product $*$ on U exists, then it is uniquely determined. By choosing $s = u * v$ and $t = -1$ in

$$u * v = s * t \iff (1-u)(1-v) = (1-s)(1-t),$$

we find $(1-u)(1-v) = 2(1 - u * v)$, so $u * v = 1 - a$ for the unique element $a \in R$ with $2a = (1-u)(1-v)$, if such a exists.

Oplossingen | Solutions

The crux of the problem is to prove for all $u, v \in U$ that $(1-u)(1-v)$ is divisible by 2 in R. Note, however, that the element $1-u$ is not necessarily divisible by 2, as we can see from the counterexample $f = X^2 - 1$ and $u = (X \mod f)$.

Given any pair of elements $u, v \in U$, to show 2 divides $(1-u)(1-v)$, it suffices to prove that $(1-\overline{u})(1-\overline{v})$ is zero in $R/2R \cong \mathbb{F}_2[X]/(\overline{f})$, where the bar denotes reduction by 2. Let $\overline{f} = \prod_{i=1}^{s} g_i^{e_i}$ be the factorization of $\overline{f} \in \mathbb{F}_2[X]$. Then the Chinese Remainder Theorem yields

$$R/2R \cong \mathbb{F}_2[X]/(\overline{f}) \cong \prod_{i=1}^{s} \mathbb{F}_2[X]/(g_i^{e_i}).$$

Let $u \in U$ and $1 \le i \le s$. Let $p \in \mathbb{F}_2[x]$ represent $1-\overline{u} \in \mathbb{F}_2[x]/(\overline{f})$. Let $\operatorname{ord}_{g_i}(p)$ denote the number of factors of g_i in p. Then p reduces to 0 in $\mathbb{F}_2[X]/(g_i^{e_i})$ if and only if $\operatorname{ord}_{g_i}(p) \ge e_i$. Note that $(1-\overline{u})^2 = 2(1-\overline{u}) = 0$ in $\mathbb{F}_2[X]/(\overline{f})$, so $\operatorname{ord}_{g_i}(p) \ge e_i/2$. Similarly, for $v \in U$, let $q \in \mathbb{F}_2[x]$ represent $1-\overline{v}$. Then $\operatorname{ord}_{g_i}(q) \ge e_i/2$, so pq reduces to 0 in $\mathbb{F}_2[X]/(g_i^{e_i})$. This holds for all $1 \le i \le s$, so pq reduces to 0 in $\mathbb{F}_2[x]/(\overline{f})$, which means $(1-\overline{u})(1-\overline{v}) = 0$. This finishes the proof that there exists an $a \in R$ with $2a = (1-u)(1-v)$. One checks directly that $u * v = 1 - a$ satisfies $(u * v)^2 = 1$, so that indeed $u * v \in U$.

The proof could now be finished with an easy and completely straightforward verification of the ring axioms for $(U, \cdot, *)$. Instead, we finish by sketching two slightly faster alternatives to this verification.

One method is to note that every $u \in U$ gives rise to an idempotent $(1-u)/2 \in \mathbb{Q}[X]/(f)$, and that this embeds $(U, \cdot, *)$ into the *ring of idempotents* of $\mathbb{Q}[X]/(f)$ (which has its own special ring operations).

Alternatively, write $f = \prod h_i^{s_i}$ with irreducible $h_i \in \mathbb{Z}[X]$, and use the injective ring homomorphism $R \to \prod \mathbb{Z}[X]/(h_i^{s_i})$ to embed U into the product of the analogs U_i in the rings $\mathbb{Z}[X]/(h_i^{s_i})$. This reduces the verification to the case where f is a power of an irreducible polynomial. In that case we have $U_i = \{\pm 1\}$, which with the given operations is easily seen to be a ring isomorphic to $\mathbb{F}_2$.