Problemen

| Problem Section

Edition 2017-4 We received solutions from Math Dicker (Hoensbroek), Hendrik Reuvers (Maastricht) and Sep Thijssen (Lent). The book tokens go to Hendrik Reuvers for problem A and Math Dicker for problem C.

Problem 2017-4/A

Consider two identical bags of stones, all having integral weights. No two weights in a bag are the same. Suppose that the stones from these two bags are divided into proper subsets of equal cardinality and equal total weight. No two weights in a subset are the same. Is it then possible to readjust this division such that each subset contains stones from the same bag?

Solution Solved by Hendrik Reuvers and Sep Thijssen in the same way. No, this is not always possible. If one bag has weights $\{1,2,3,4,5,6\}$ and the other bag has weights $\{1',2',3',4',5',6'\}$ then it is possible to divide the weights into

$$\{1,3,4,6\},\{2',3',4',5'\},\{2,5,1',6'\}$$

Clearly, this division cannot be readjusted such that each subset contains stones of the same color, since six is not divisible by four. This solves the problem.
However, it is possible to divide the bag $\{1,2,3,4,5,6\}$ into subsets of equal weight and cardinality in another way, namely $\{1,6\},\{2,5\},\{3,4\}$. The NAW problem section is understaffed and overworked and runs the risk of coming to a full stop. This is why problems are not always stated accurately. The problem gets harder if we alter the last sentence: is it then possible to divide each single bag into proper subsets of equal weight? Again, it turns out that this is not always possible, but the simplest example that we know has cardinality fifteen.

Problem 2017-4/B

Let $H_1,\ldots,H_k$ be k planes in $\mathbb{R}^3$. Prove that the unit ball contains an open ball of radius $\frac{1}{k+1}$ which does not intersect any of the planes.

Solution We need to find a point p that has distance $\geq 1/(k+1)$ to the planes such that $\|p\| \leq k/(k+1)$. In other words, we need to show that the sets

$$P_i = \{x \in \mathbb{R}^3 : d(x,H_i) < 1/(k+1)\}$$

do not cover the ball of diameter $k/(k+1)$. Such a set P_i is called a *plank*. Our planks are open. Tarski proved that closed planks can only cover the unit ball if their widths add up to 2 or more. The widths of our planks add up to $2k/(k+1)$. If we make these planks a wee bit less wide then they cannot cover the ball of radius $k/(k+1)$. For every $d < 1/(k+1)$ there is a point of distance $\geq d$ to the planes. By compactness, there is a p that has distance $\geq 1/(k+1)$ to the planes.
To prove his result, Tarski used the well-known but remarkable fact that the area of the intersection of a plank and a sphere is constant, as long as both faces of the plank intersect the sphere. If the widths of the planks do not add up to two, we can stack them around the equator without reaching out to the poles. Therefore these planks will never cover the ball's surface, no matter where you put them.
What if we replace the ball by an oval? If a boiled egg has unit width, can you slice it into pieces with total width less than one? This is called Tarski's plank problem, raised by Tarski in 1932 and solved by Bang in 1951. The plank problem has a way of turning up in number theory. Problem B is Lemma 4.1 in a recent paper by Akiyama and Caalim on beta-expansions and the plank problem, see arxiv:1509.04785v2. Surprisingly, the plank problem is more difficult for cubes. Is it possible to find a cube of size $1/(k+1)$ inside the unit cube and outside the k planes? Davenport conjectured that such a cube exists in one of his works on simultaneous Diophantine approximation. It is equivalent to a conjecture by Bang at the end of his 1951 paper and remains unsolved.

Redacteur: Rob Eggermont
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Oplossingen | Solutions

Problem 2017-4/C (proposed by Hendrik Lenstra)

Suppose that a, b, n, m are integers, and that m, n are positive, such that $a^n \equiv b^n \equiv -1 \bmod m$. Prove there exists an integer c such that $ab \equiv c^2 \bmod m$. Also provide a fast method to compute such a c which works even if the prime factors of m are unknown.

Solution Solved by Math Dicker and Hendrik Reuvers, although their method to compute c is not as efficient as the method below.

If n is odd, then we may take $c = (ab)^{(n+1)/2}$ and we are done. We may assume that n is even. In particular, -1 is a square modulo m. Since -1 is not a square modulo 4, either m is odd or m is even and $m/2$ is odd. In the latter case, we can reduce the problem to odd m by the Chinese Remainder Theorem. We may assume that m is odd.

By the Chinese Remainder Theorem ab is a square modulo m if and only if it is a square modulo p^k for all p^k that divide m. The group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic for odd primes and therefore so is its subgroup $S = \{x : x^{2n} \equiv 1 \bmod p^k\}$. An element of S is a square if and only if $x^n \equiv 1 \bmod p^k$. It follows that ab is a square in S, and hence modulo m.

We have to provide a fast method to compute c if the prime factors of m are unknown. Observe that if at any point we find $y^2 \equiv 1 \bmod m$ for a certain integer y with $y \not\equiv \pm 1 \bmod m$, then this allows us to factor $m = \gcd(y+1, m) \cdot \gcd(y-1, m)$. These two factors are relatively prime since m is odd and $y+1, y-1$ can only have 2 as a common divisor. By the Chinese Remainder Theorem, it suffices to find roots of ab modulo $\gcd(y+1, m)$ and modulo $\gcd(y-1, m)$.

We write $n = u2^v$ and we let $c_0 = (ab)^{(u+1)/2}$. Then $c_0^2 \equiv (ab)y_0$ with $y_0 \equiv (ab)^u$. In particular $y_0^{2^v} \equiv 1$. If $y_0 \equiv 1$ then we are done. If not, let $w \geq 0$ be the maximal integer such that $y_0^{2^w} \not\equiv 1$. If $y_0^{2^w} \not\equiv -1$, then we can factor m as described above. If $y_0^{2^w} \equiv -1$ then we replace c_0 by $c_1 = c_0 a^{u2^{v-w-1}}$ and y_0 by $y_1 = y_0 a^{u2^{v-w}}$. It follows that $y_1^{2^w} \equiv 1$. Repeat iteratively. Since the minimal l required to get $y_k^{2^l} \equiv 1$ strictly shrinks in each step, eventually we will either find $y_k \equiv 1$ and $c_k^2 \equiv ab$ or we can factor m.