IMC 2012, Blagoevgrad, Bulgaria
Day 1, July 28, 2012

Problem 1. For every positive integer n, let $p(n)$ denote the number of ways to express n as a sum of positive integers. For instance, $p(4) = 5$ because

$$4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.$$

Also define $p(0) = 1$.

Prove that $p(n) - p(n-1)$ is the number of ways to express n as a sum of integers each of which is strictly greater than 1.

(Proposed by Fedor Duzhin, Nanyang Technological University)

Solution 1. The statement is true for $n = 1$, because $p(0) = p(1) = 1$ and the only partition of 1 contains the term 1. In the rest of the solution we assume $n \geq 2$.

Let $\mathcal{P}_n = \{(a_1, \ldots, a_k) : k \in \mathbb{N},\ a_1 \geq \ldots \geq a_k,\ a_1 + \ldots + a_k = n\}$ be the set of partitions of n, and let $\mathcal{Q}_n = \{(a_1, \ldots, a_k) \in \mathcal{P}_n : a_k = 1\}$ the set of those partitions of n that contain the term 1. The set of those partitions of n that do not contain 1 as a term, is $\mathcal{P}_n \setminus \mathcal{Q}_n$. We have to prove that $|P_n \setminus \mathcal{Q}_n| = |\mathcal{P}_n| - |\mathcal{P}_{n-1}|$.

Define the map $\varphi \colon \mathcal{P}_{n-1} \to \mathcal{Q}_n$ as

$$\varphi(a_1, \ldots, a_k) = (a_1, \ldots, a_k, 1).$$

This is a partition of n containing 1 as a term (so indeed $\varphi(a_1, \ldots, a_k) \in \mathcal{Q}_n$). Moreover, each partition $(a_1, \ldots, a_k, 1) \in \mathcal{Q}_n$ uniquely determines $(a_1, \ldots, a_k)$. Therefore the map φ is a bijection between the sets $\mathcal{P}_{n-1}$ and $\mathcal{Q}_n$. Then $|\mathcal{P}_{n-1}| = |\mathcal{Q}_n|$. Since $\mathcal{Q}_n \subset \mathcal{P}_n$,

$$|\mathcal{P}_n \setminus \mathcal{Q}_n| = |\mathcal{P}_n| - |\mathcal{Q}_n| = |\mathcal{P}_n| - |\mathcal{P}_{n-1}| = p(n) - p(n-1).$$

Solution 2 (outline). Denote by $q(n)$ the number of partitions of n not containing 1 as term ($q(0) = 1$ as the only partition of 0 is the empty sum), and define the generating functions

$$F(x) = \sum_{n=0}^{\infty} p(n)x^n \quad \text{and} \quad G(x) = \sum_{n=0}^{\infty} q(n)x^n.$$

Since $q(n) \leq p(n) < 2^n$, these series converge in some interval, say for $|x| < \frac{1}{2}$, and the values uniquely determine the coefficients.

According to Euler's argument, we have

$$F(x) = \sum_{n=0}^{\infty} p(n)x^n = \prod_{k=1}^{\infty}(1 + x^k + x^{2k} + \ldots) = \prod_{k=1}^{\infty} \frac{1}{1 - x^k}$$

and

$$G(x) = \sum_{n=0}^{\infty} q(n)x^n = \prod_{k=2}^{\infty}(1 + x^k + x^{2k} + \ldots) = \prod_{k=2}^{\infty} \frac{1}{1 - x^k}.$$

Then $G(x) = (1-x)F(x)$. Comparing the coefficient of x^n in this identity we get $q(n) = p(n) - p(n-1)$.

Problem 2. Let n be a fixed positive integer. Determine the smallest possible rank of an $n \times n$ matrix that has zeros along the main diagonal and strictly positive real numbers off the main diagonal.

(Proposed by Ilya Bogdanov and Grigoriy Chelnokov, MIPT, Moscow)

Solution. For $n = 1$ the only matrix is (0) with rank 0. For $n = 2$ the determinant of such a matrix is negative, so the rank is 2. We show that for all $n \geq 3$ the minimal rank is 3.

Notice that the first three rows are linearly independent. Suppose that some linear combination of them, with coefficients c_1, c_2, c_3, vanishes. Observe that from the first column one deduces that c_2 and c_3 either have opposite signs or both zero. The same applies to the pairs (c_1, c_2) and (c_1, c_3). Hence they all must be zero.

It remains to give an example of a matrix of rank (at most) 3. For example, the matrix

$$\begin{pmatrix} 0^2 & 1^2 & 2^2 & \dots & (n-1)^2 \\ (-1)^2 & 0^2 & 1^2 & \dots & (n-2)^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (-n+1)^2 & (-n+2)^2 & (-n+3)^2 & \dots & 0^2 \end{pmatrix} = \Big((i-j)^2\Big)_{i,j=1}^{n} =$$

$$= \begin{pmatrix} 1^2 \\ 2^2 \\ \vdots \\ n^2 \end{pmatrix} (1, 1, \dots, 1) - 2 \begin{pmatrix} 1 \\ 2 \\ \vdots \\ n \end{pmatrix} (1, 2, \dots, n) + \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} (1^2, 2^2, \dots, n^2)$$

is the sum of three matrices of rank 1, so its rank cannot exceed 3.

Problem 3. Given an integer $n > 1$, let S_n be the group of permutations of the numbers $1, 2, \dots, n$. Two players, A and B, play the following game. Taking turns, they select elements (one element at a time) from the group S_n. It is forbidden to select an element that has already been selected. The game ends when the selected elements generate the whole group S_n. The player who made the last move loses the game. The first move is made by A. Which player has a winning strategy?

(Proposed by Fedor Petrov, St. Petersburg State University)

Solution. Player A can win for $n = 2$ (by selecting the identity) and for $n = 3$ (selecting a 3-cycle).

We prove that B has a winning strategy for $n \geq 4$. Consider the moment when all permitted moves lose immediately, and let H be the subgroup generated by the elements selected by the players. Choosing another element from H would not lose immediately, so all elements of H must have been selected. Since H and any other element generate S_n, H must be a maximal subgroup in S_n.

If $|H|$ is even, then the next player is A, so B wins. Denote by n_i the order of the subgroup generated by the first i selected elements; then $n_1 | n_2 | n_3 | \dots$. We show that B can achieve that n_2 is even and $n_2 < n!$; then $|H|$ will be even and A will be forced to make the final – losing – move.

Denote by g the element chosen by A on his first move. If the order n_1 of g is even, then B may choose the identical permutation id and he will have $n_2 = n_1$ even and $n_2 = n_1 < n!$.

If n_1 is odd, then g is a product of disjoint odd cycles, so it is an even permutation. Then B can chose the permutation $h = (1, 2)(3, 4)$ which is another even permutation. Since g and h are elements of the alternating group A_n, they cannot generate the whole S_n. Since the order of h is 2, B achieves $2 | n_2$.

Remark. If $n \geq 4$, all subgrups of odd order are subgroups of A_n which has even order. Hence, all maximal subgroups have even order and B is never forced to lose.

Problem 4. Let $f \colon \mathbb{R} \to \mathbb{R}$ be a continuously differentiable function that satisfies $f'(t) > f(f(t))$ for all $t \in \mathbb{R}$. Prove that $f(f(f(t))) \leq 0$ for all $t \geq 0$.

(Proposed by Tomáš Bárta, Charles University, Prague)

Solution.

Lemma 1. Either $\lim_{t\to+\infty} f(t)$ does not exist or $\lim_{t\to+\infty} f(t) \neq +\infty$.

Proof. Assume that the limit is $+\infty$. Then there exists $T_1 > 0$ such that for all $t > T_1$ we have $f(t) > 2$. There exists $T_2 > 0$ such that $f(t) > T_1$ for all $t > T_2$. Hence, $f'(t) > f(f(t)) > 2$ for $t > T_2$. Hence, there exists T_3 such that $f(t) > t$ for $t > T_3$. Then $f'(t) > f(f(t)) > f(t)$, $f'(t)/f(t) > 1$, after integration $\ln f(t) - \ln T_3 > t - T_3$, i.e. $f(t) > T_3 e^{t-T_3}$ for all $t > T_3$. Then $f'(t) > f(f(t)) > T_3 e^{f(t)-T_3}$ and $f'(t)e^{-f(t)} > T_3 e^{-T_3}$. Integrating from T_3 to t yields $e^{-f(T_3)} - e^{-f(t)} > (t-T_3)T_3 e^{-T_3}$. The right-hand side tends to infinity, but the left-hand side is bounded from above, a contradiction. □

Lemma 2. For all $t > 0$ we have $f(t) < t$.

Proof. By Lemma 1, there are some positive real numbers t with $f(t) < t$. Hence, if the statement is false then there is some $t_0 > 0$ with $f(t_0) = t_0$.

Case I: There exist some value $t \geq t_0$ with $f(t) < t_0$. Let $T = \inf\{t \geq t_0 : f(t) < t_0\}$. By the continuity of f, $f(T) = t_0$. Then $f'(T) > f(f(T)) = f(t_0) = t_0 > 0$. This implies $f > f(T) = t_0$ in a right neighbourhood, contradicting the definition of T.

Case II: $f(t) \geq t_0$ for all $t \geq t_0$. Now we have $f'(t) > f(f(t)) \geq t_0 > 0$. So, f' has a positive lower bound over (t_0, ∞), which contradicts Lemma 1. □

Lemma 3. (a) If $f(s_1) > 0$ and $f(s_2) \geq s_1$, then $f(s) > s_1$ for all $s > s_2$.

(b) In particular, if $s_1 \leq 0$ and $f(s_1) > 0$, then $f(s) > s_1$ for all $s > s_1$.

Proof. Suppose that there are values $s > s_2$ with $f(s) \leq s_1$ and let $S = \inf\{s > s_2 : \ f(s) \leq s_1\}$. By the continuity we have $f(S) = s_1$. Similarly to Lemma 2, we have $f'(S) > f(f(S)) = f(s_1) > 0$. If $S > s_2$ then in a left neighbourhood of S we have $f < s_1$, contradicting the definition of S. Otherwise, if $S = s_2$ then we have $f > s_1$ in a right neighbourhood of s_2, contradiction again.

Part (b) follows if we take $s_2 = s_1$. □

With the help of these lemmas the proof goes as follows. Assume for contradiction that there exists some $t_0 > 0$ with $f(f(f(t_0))) > 0$. Let $t_1 = f(t_0)$, $t_2 = f(t_1)$ and $t_3 = f(t_2) > 0$. We show that $0 < t_3 < t_2 < t_1 < t_0$. By lemma 2 it is sufficient to prove that t_1 and t_2 are positive. If $t_1 < 0$, then $f(t_1) \leq 0$ (if $f(t_1) > 0$ then taking $s_1 = t_1$ in Lemma 3(b) yields $f(t_0) > t_1$, contradiction). If $t_1 = 0$ then $f(t_1) \leq 0$ by lemma 2 and the continuity of f. Hence, if $t_1 \leq 0$, then also $t_2 \leq 0$. If $t_2 = 0$ then $f(t_2) \leq 0$ by lemma 2 and the continuity of f (contradiction, $f(t_2) = t_3 > 0$). If $t_2 < 0$, then by lemma 3(b), $f(t_0) > t_2$, so $t_1 > t_2$. Applying lemma 3(a) we obtain $f(t_1) > t_2$, contradiction. We have proved $0 < t_3 < t_2 < t_1 < t_0$.

By lemma 3(a) ($f(t_1) > 0$, $f(t_0) \geq t_1$) we have $f(t) > t_1$ for all $t > t_0$ and similarly $f(t) > t_2$ for all $t > t_1$. It follows that for $t > t_0$ we have $f'(t) > f(f(t)) > t_2 > 0$. Hence, $\lim_{t\to+\infty} f(t) = +\infty$, which is a contradiction. This contradiction proves that $f(f(f(t))) \leq 0$ for all $t > 0$. For $t = 0$ the inequality follows from the continuity of f.

Problem 5. Let a be a rational number and let n be a positive integer. Prove that the polynomial $X^{2^n}(X+a)^{2^n} + 1$ is irreducible in the ring $\mathbb{Q}[X]$ of polynomials with rational coefficients.

(Proposed by Vincent Jugé, École Polytechnique, Paris)

Solution. First let us consider the case $a = 0$. The roots of $X^{2^{n+1}} + 1$ are exactly all primitive roots of unity of order 2^{n+2}, namely $e^{2\pi i \frac{k}{2^{n+2}}}$ for odd $k = 1, 3, 5, \ldots, 2^{n+2} - 1$. It is a cyclotomic polynomial, hence irreducible in $\mathbb{Q}[X]$.

Let now $a \neq 0$ and suppose that the polynomial in the question is reducible. Substituting $X = Y - \frac{a}{2}$ we get a polynomial $(Y - \frac{a}{2})^{2^n}(Y + \frac{a}{2})^{2^n} + 1 = (Y^2 - \frac{a^2}{4})^{2^n} + 1$. It is again a cyclotomic polynomial in the variable $Z = Y^2 - \frac{a^2}{4}$, and therefore it is not divisible by any polynomial in Y^2 with rational coefficients. Let us write this polynomial as the product of irreducible monic polynomials in Y with appropriate multiplicities, i.e.

$$\left(Y^2 - \frac{a^2}{4}\right)^{2^n} + 1 = \prod_{i=1}^{r} f_i(Y)^{m_i} \qquad f_i \text{ monic, irreducible, all different.}$$

Since the left-hand side is a polynomial in Y^2 we must have $\prod_i f_i(Y)^{m_i} = \prod_i f_i(-Y)^{m_i}$. By the above argument non of the f_i is a polynomial in Y^2, i.e. $f_i(-Y) \neq f_i(Y)$. Therefore for every i there is $i' \neq i$ such that $f_i(-Y) = \pm f_{i'}(Y)$. In particular r is even and irreducible factors f_i split into pairs. Let us renumber them so that $f_1, \ldots, f_{\frac{r}{2}}$ belong to different pairs and we have $f_{i+\frac{r}{2}}(-Y) = \pm f_i(Y)$. Consider the polynomial $f(Y) = \prod_{i=1}^{r/2} f_i(Y)^{m_i}$. This polynomial is monic of degree 2^n and $(Y^2 - \frac{a^2}{4})^{2^n} + 1 = f(Y)f(-Y)$. Let us write $f(Y) = Y^{2^n} + \cdots + b$ where $b \in \mathbb{Q}$ is the constant term, i.e. $b = f(0)$. Comparing constant terms we then get $\left(\frac{a}{2}\right)^{2^{n+1}} + 1 = b^2$. Denote $c = \left(\frac{a}{2}\right)^{2^{n-1}}$. This is a nonzero rational number and we have $c^4 + 1 = b^2$.

It remains to show that there are no rational solutions $c, b \in \mathbb{Q}$ to the equation $c^4+1 = b^2$ with $c \neq 0$ which will contradict our assumption that the polynomial under consideration is reducible. Suppose there is a solution. Without loss of generality we can assume that $c, b > 0$. Write $c = \frac{u}{v}$ with u and v coprime positive integers. Then $u^4 + v^4 = (bv^2)^2$. Let us denote $w = bv^2$, this must be a positive integer too since u, v are positive integers. Let us show that the set $\mathcal{T} = \{(u, v, w) \in \mathbb{N}^3 \mid u^4 + v^4 = w^2 \text{ and } u, v, w \geq 1\}$ is empty. Suppose the contrary and consider some triple $(u, v, w) \in \mathcal{T}$ such that w is minimal. Without loss of generality, we may assume that u is odd. (u^2, v^2, w) is a primitive Pythagorean triple and thus there exist relatively prime integers $d > e \geq 1$ such that $u^2 = d^2 - e^2$, $v^2 = 2de$ and $w = d^2 + e^2$. In particular, considering the equation $u^2 = d^2 - e^2$ in $\mathbb{Z}/4\mathbb{Z}$ proves that d is odd and e is even. Therefore, we can write $d = f^2$ and $e = 2g^2$. Moreover, since $u^2 + e^2 = d^2$, (u, e, d) is also a primitive Pythagorean triple: there exist relatively prime integers $h > i \geq 1$ such that $u = h^2 - i^2$, $e = 2hi = 2g^2$ and $d = h^2 + i^2$. Once again, we can write $h = k^2$ and $i = l^2$, so that we obtain the relation $f^2 = d = h^2 + i^2 = k^4 + l^4$ and $(k, l, f) \in \mathcal{T}$. Then, the inequality $w > d^2 = f^4 \geq f$ contradicts the minimality of w.

Remark 1. One can also use Galois theory arguments in order to solve this question. Let us denote the polynomial in the question by $P(X) = X^{2^n}(X + a)^{2^n} + 1$ and we will also need the cyclotomic polynomial $T(X) = X^{2^n} + 1$. As we already said, when $a = 0$ then $P(X)$ is itself cyclotomic and hence irreducible. Let now $a \neq 0$ and x be any complex root of $P(x) = 0$. Then $\zeta = x(x+a)$ satisfies $T(\zeta) = 0$, hence it is a primitive root of unity of order 2^{n+1}. The field $\mathbb{Q}[x]$ is then an extension of $\mathbb{Q}[\zeta]$. The latter field is cyclotomic and its degree over $\mathbb{Q}$ is $\dim_{\mathbb{Q}}\big(\mathbb{Q}[\zeta]\big) = 2^n$. Since the polynomial in the question has degree 2^{n+1} we see that it is reducible if and only if the above mentioned extension is trivial, i.e. $\mathbb{Q}[x] = \mathbb{Q}[\zeta]$. For the sake of contradiction we will now assume that this is indeed the case. Let $S(X)$ be the minimal polynomial of x over $\mathbb{Q}$. The degree of S is then 2^n and we can number its roots by odd numbers in the set $I = \{1, 3, \ldots, 2^{n+1} - 1\}$ so that $S(X) = \prod_{k\in I}(X - x_k)$ and $x_k(x_k + a) = \zeta^k$ because Galois automorphisms of $\mathbb{Q}[\zeta]$ map ζ to $\zeta^k, k \in I$. Then one has

$$S(X)S(-a - X) = \prod_{k\in I}(X - x_k)(-a - X - x_k) = (-1)^{|I|}\prod_{k\in I}\Big(X(X + a) - \zeta^k\Big) = T\big(X(X + a)\big) = P(X)\,.$$

In particular $P(-\frac{a}{2}) = S(-\frac{a}{2})^2$, i.e. $\left(\frac{a}{2}\right)^{2^{n+1}}+1 = \left(\left(\frac{a}{2}\right)^{2^n}+1\right)^2$. Therefore the rational numbers $c = \left(\frac{a}{2}\right)^{2^{n-1}} \neq 0$ and $b = \left(\frac{a}{2}\right)^{2^n} + 1$ satisfy $c^4 + 1 = b^2$ which is a contradiction as it was shown in the first proof.

Remark 2. It is well-known that the Diophantine equation $x^4 + y^4 = z^2$ has only trivial solutions (i.e. with $x = 0$ or $y = 0$). This implies immediately that $c^4 + 1 = b^2$ has no rational solution with nonzero c.