Algebra

A1. Denote $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$ the set of all positive integers. Determine all functions $f : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ such that, for each positive integer n,

i) $\sum_{k=1}^{n} f(k)$ is a perfect square, and

ii) $f(n)$ divides n^3.

Albania

Solution. Induct on n to show that $f(n) = n^3$ for all positive integers n. It is readily checked that this f satisfies the conditions in the statement. The base case, $n = 1$, is clear.

Let $n \geqslant 2$ and assume that $f(m) = m^3$ for all positive integers $m < n$. Then $\sum_{k=1}^{n-1} f(k) = \frac{n^2(n-1)^2}{4}$, and reference to the first condition in the statement yields

$$f(n) = \sum_{k=1}^{n} f(k) - \sum_{k=1}^{n-1} f(k) = \left(\frac{n(n-1)}{2} + k\right)^2 - \frac{n^2(n-1)^2}{4} = k(n^2 - n + k),$$

for some positive integer k.

The divisibility condition in the statement implies $k(n^2 - n + k) \leqslant n^3$, which is equivalent to $(n - k)(n^2 + k) \geqslant 0$, showing that $k \leqslant n$.

On the other hand, $n^2 - n + k$ must also divide n^3. But, if $k < n$, then

$$n < \frac{n^3}{n^2 - 1} \leqslant \frac{n^3}{n^2 - n + k} \leqslant \frac{n^3}{n^2 - n + 1} < \frac{n^3 + 1}{n^2 - n + 1} = n + 1,$$

therefore $\frac{n^3}{n^2 - n + k}$ cannot be an integer.

Consequently, $k = n$, so $f(n) = n^3$. This completes induction and concludes the proof.

A2. If a, b, c are positive real numbers such that $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 3$, prove that

$$\frac{a+b+c-1}{\sqrt{2}} \geqslant \frac{\sqrt{a+\frac{b}{c}} + \sqrt{b+\frac{c}{a}} + \sqrt{c+\frac{a}{b}}}{3}$$

When does equality hold?

Albania

Solution. The inequality is equivalent to

$$12(a+b+c-1) \geqslant \sum_{\text{cyc}} 4\sqrt{2\left(a+\frac{b}{c}\right)}.$$

From AM-GM inequality we have

$$\sum_{cyc} 2\sqrt{2\left(a+\frac{b}{c}\right)} \leqslant \sum_{cyc}\left(2+a+\frac{b}{c}\right) = 6+a+b+c+\frac{a}{b}+\frac{b}{c}+\frac{c}{a}.$$

Again from AM-GM inequality we have

$$\frac{2a}{b}+\frac{2b}{c}+\frac{2c}{a} \geqslant 3\sqrt[3]{\frac{2a}{b}\cdot\frac{2b}{c}\cdot\frac{2c}{a}} = 3\sqrt[3]{8} = 6.$$

Hence,

$$\sum_{\text{cyc}} 2\sqrt{2\left(a+\frac{b}{c}\right)} \leqslant a+b+c+\frac{3a}{b}+\frac{3b}{c}+\frac{3c}{a}. \tag{1}$$

Again, from AM-GM inequality we have

$$\begin{aligned}\sum_{\text{cyc}} 2\sqrt{2\left(a+\frac{b}{c}\right)} = \sum_{\text{cyc}} 2\sqrt{\frac{2a}{c}\left(c+\frac{b}{a}\right)} &\leqslant \sum_{\text{cyc}}\left(\frac{2a}{c}+c+\frac{b}{a}\right) \\ &= a+b+c+\frac{3a}{c}+\frac{3b}{a}+\frac{3c}{b}.\end{aligned} \tag{2}$$

Adding (1) and (2) we get,

$$\sum_{\text{cyc}} 4\sqrt{2\left(a+\frac{b}{c}\right)} \leqslant 2(a+b+c)+3\left(\frac{a+b}{c}+\frac{b+c}{a}+\frac{c+a}{b}\right).$$

Now, using the asumption we have

$$\frac{a+b}{c}+\frac{b+c}{a}+\frac{c+a}{b} = (a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)-3 = 3(a+b+c-1).$$

Hence,

$$\sum_{\text{cyc}} 4\sqrt{2\left(a+\frac{b}{c}\right)} \leqslant 11(a+b+c)-9.$$

So, it is enough to prove

$$11(a+b+c)-9 \leqslant 12(a+b+c-1) \iff a+b+c \geqslant 3.$$

Last inequality is true since using $AM - HM$ and condition we have,

$$\frac{a+b+c}{3} \geqslant \frac{3}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} = 1 \Rightarrow a+b+c \geqslant 3.$$

It is known that equality in $AM - HM$ is achieved only when $a = b = c$ and, since $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} = 3$, $a = b = c = 1$. Clearly, for $a = b = c = 1$ equality holds.

A3. Let $P(x)$, $Q(x)$ be distinct polynomials of degree 2020 with non-zero coefficients. Suppose that they have r common real roots counting multiplicity and s common coefficients. Determine the maximum possible value of $r + s$.

Demetres Christofides, Cyprus

Solution. We claim that the maximum possible value is 3029.

The polynomials

$$P(x) = (x^2 - 1)^{1009}(x^2 + 1) \quad \text{and} \quad Q(x) = (x^2 - 1)^{1009}(x^2 + x + 1)$$

satisfy the conditions, have 2018 common roots, and have 1011 common coefficients (all coefficients of even powers). So $r + s \geqslant 3029$.

Suppose now that $P(x), Q(x)$ agree on the coefficients of $x^{2020}, x^{2019}, \ldots, x^{2021-k}$, disagree on the coefficient of x^{2020-k}, and agree on another $s - k$ coefficients. The common roots of $P(x), Q(x)$ are also non-zero roots of the polynomial $P(x) - Q(x)$ which has degree x^{2020-k}. (The condition on the non-zero coefficients guarantees that 0 is not a root of P and Q.) So $P(x) - Q(x)$ has at most $2020 - k$ real roots. On the other hand, $P(x) - Q(x)$ has exactly $s - k$ coefficients equal to zero. So by the following Lemma it has at most $2[(2020 - k) - (s - k)] = 4040 - 2s$ real non-zero roots. Averaging we get $r \leqslant \left\lfloor \dfrac{6060 - 2s - k}{2} \right\rfloor \leqslant 3030 - s$. Thus $r + s \leqslant 3030$. Furthermore, if equality occurs, we must have $k = 0$ and $r = 2020 - k = 4040 - 2s$. In other words, we must have $r = 2020$ and $s = 1010$. But if $r = 2020$, then $Q(x)$ is a multiple of $P(x)$ and since $P(x), Q(x)$ have non-zero coefficients, then $s = 0$, a contradiction. Therefore $r + s \leqslant 3029$ as required.

Lemma. Let f be a polynomial of degree n having exactly t coefficients equal to 0. Then f has at most $2(n - t)$ real non-zero roots.

Proof of Lemma. Since f has $n + 1 - t$ non-zero coefficients, by Descartes' rule of signs it has at most $n - t$ sign changes and therefore at most $n - t$ positive real roots. Similarly it has at most $n - t$ negative real roots.

Note. Counting the roots with multiplicity is not essential. We can demand 'r common distinct real roots' by changing the $(x^2 - 1)^{1009}$ in the example to

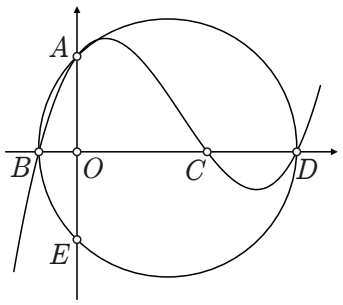
$$(x^2 - 1)(x^2 - 2) \cdots (x^2 - 1009).$$

A4. Let $P(x) = x^3 + ax^2 + bx + 1$ be a polynomial with real coefficients and three real roots ρ_1, ρ_2, ρ_3 such that $|\rho_1| < |\rho_2| < |\rho_3|$. Let A be the point where the graph of $P(x)$ intersects yy' and the points $B(\rho_1, 0)$, $C(\rho_2, 0)$, $D(\rho_3, 0)$. If the circumcircle of $\triangle ABD$ intersects yy' for a second time at E, find the minimum value of the length of the segment EC and the polynomials for which this is attained.

Brazitikos Silouanos, Greece

Solution. Let O be the origin. Since $P(0) = 1$, A is the point $(0, 1)$, so OA=1.

From Vieta's relations we have $\rho_1\rho_2\rho_3 = -1$, so $|\rho_1\rho_2\rho_3| = 1$. (1)



From the power of the point O we have

$$OB \cdot OD = OA \cdot OE \Rightarrow |\rho_1| \cdot |\rho_3| = 1 \cdot OE,$$

hence $OE = \frac{1}{|\rho_2|}$.

Finally, from Pythagoras' theorem we have

$$CE^2 = OE^2 + OC^2 = |\rho_2|^2 + \frac{1}{|\rho_2|^2} \geqslant 2,$$

hence $CE \geqslant \sqrt{2}$.

The equality holds for $|\rho_2| = 1 \iff \rho_2 = \pm 1$. In the first case we have the family

$$P(x) = (x-1)(x+a)\left(x - \frac{1}{a}\right),$$

while in the second case we have

$$P(x) = (x+1)(x-a)\left(x - \frac{1}{a}\right).$$

Combinatorics

C1. Let $s \geqslant 2$ and $n \geqslant k \geqslant 2$ be integes, and let $\mathcal{A}$ be a subset of $\{1, 2, \ldots, n\}^k$ of size at least $2sk^2n^{k-2}$ such that any two members of $\mathcal{A}$ share some entry. Prove that there are an integer $p \leqslant k$ and $s+2$ members A_1, A_2, $\ldots$, A_{s+2} of $\mathcal{A}$ such that A_i and A_j share the p-th entry alone, whenever $i \neq j$.

Miroslav Mironov, Bulgaria

Solution. Fix a member A of $\mathcal{A}$. Note that there are at most $\binom{k}{2}n^{k-2}$ k-tuples that share at least two entries with A. Indeed, there are n^{k-2} k-tuples sharing any two given entries. The bound now follows, since the two entries can be chosen in $\binom{k}{2}$ different ways.

Therefore, the number of members of $\mathcal{A}$ that share a single entry with A is at least

$$|\mathcal{A}| - \binom{k}{2}n^{k-2} \geqslant 2sk^2n^{k-2} - k^2n^{k-2} > sk^2n^{k-2}.$$

Letting $\mathcal{B}_p$ be the set of all members of $\mathcal{A}$ that share the p-th entry alone with A, the above estimate yields $\sum_{p=1}^{k} |\mathcal{B}_p| > sk^2n^{k-2}$, and hence $|\mathcal{B}_p| > skn^{k-2}$ for some p.

Let B be an arbitrary member of this $\mathcal{B}_p$. Then there are at most $(k-1)n^{k-2}$ k-tuples that share the p-th entry and some other entry with B. Now, let t be maximal with the property that there are B_1, B_2, $\ldots$, B_t in $\mathcal{B}_p$ such that any two B_i and B_j share the p-th entry alone for $i \neq j$. Hence any other member B' of $\mathcal{B}_p$ shares with some B_i at least one entry different from the p-th. Consequently, $|\mathcal{B}_p| \leqslant t(k-1)n^{k-2}$.

Finally, compare the two bounds for $|\mathcal{B}_p|$ to get $t > s$, and conclude that A, B_1, $\ldots$, B_t are $t+1 \geqslant s+2$ members of $\mathcal{A}$ every two of which share the p-th entry alone.

Remark. The argument in the solution shows that the conclusion holds under the less restrictive condition $|\mathcal{A}| > (s+1/2)k(k-1)n^{k-2}$.

C2. Let k be a positive integer. Determine the least integer $n \geqslant k+1$ for which the game below can be played indefinitely:

> Consider n boxes, labelled b_1, b_2, ..., b_n. For each index i, box b_i contains initially exactly i coins. At each step, the following three substeps are performed in order:
>
> **(1)** Choose $k+1$ boxes;
>
> **(2)** Of these $k+1$ boxes, choose k and remove at least half of the coins from each, and add to the remaining box, if labelled b_i, a number of i coins.
>
> **(3)** If one of the boxes is left empty, the game ends; otherwise, go to the next step.

Demetres Christofides, Cyprus

Solution. The required minimum is $n = 2^k + k - 1$.

In this case the game can be played indefinitely by choosing the last $k+1$ boxes, b_{2^k-1}, b_{2^k}, ..., b_{2^k+k-1}, at each step: At step r, if box b_{2^k+i-1} has exactly m_i coins, then $\lceil m_i/2 \rceil$ coins are removed from that box, unless $i \equiv r-1 \pmod{k+1}$, in which case $2^k + i - 1$ coins are added. Thus, after step r has been performed, box b_{2^k+i-1} contains exactly $\lfloor m_i/2 \rfloor$ coins, unless $i \equiv r-1 \pmod{k+1}$, in which case it contains exactly $m_i + 2^k + i - 1$ coins. This game goes on indefinitely, since each time a box is supplied, at least $2^k - 1$ coins are added, so it will then contain at least 2^k coins, good enough to survive the k steps to its next supply.

We now show that no smaller value of n works. So, let $n \leqslant 2^k + k - 2$ and suppose, if possible, that a game can be played indefinitely. Notice that a box currently containing exactly m coins survives at most $w = \lfloor \log_2 m \rfloor$ withdrawals; this w will be referred to as the *weight* of that box. The sum of the weigths of all boxes will referred to as the *total* weight. The argument hinges on the lemma below, proved at the end of the solution.

Lemma. *Performing a step does not increase the total weight. Moreover, supplying one of the first $2^k - 2$ boxes strictly decreases the total weight.*

Since the total weight cannot strictly decrease indefinitely, $n > 2^k - 2$, and from some stage on none of the first $2^k - 2$ boxes is ever supplied. Recall that each step involves a $(k+1)$-box choice. Since $n \leqslant 2^k + k - 2$, from that stage on, each step involves a withdrawal from at least one of the first $2^k - 2$ boxes. This cannot go on indefinitely, so the game must eventually come to an end, contradicting the assumption.

Consequently, a game that can be played indefinitely requires $n \geqslant 2^k + k - 1$.

Proof of the Lemma. Since a withdrawal from a box decreases its weight by at least 1, it is sufficient to show that supplying a box increases its weight by at most k; and if the latter is amongst the first $2^k - 2$ boxes, then its weight increases by at most $k-1$. Let the box to be supplied be b_i and let it currently contain exactly m_i coins, to proceed by case analysis:

If $m_i = 1$, the weight increases by $\lfloor \log_2(i+1) \rfloor \leqslant \lfloor \log_2(2^k + k - 1) \rfloor \leqslant \lfloor \log_2(2^{k+1} - 2) \rfloor \leqslant k$; and if, in addition, $i \leqslant 2^k - 2$, then the weight increases by $\lfloor \log_2(i+1) \rfloor \leqslant \lfloor \log_2(2^k - 1) \rfloor = k - 1$.

If $m_i = 2$, then the weight increases by $\lfloor \log_2(i+2) \rfloor - \lfloor \log_2 2 \rfloor \leqslant \lfloor \log_2(2^k + k) \rfloor - 1 \leqslant k - 1$.

If $m_i \geqslant 3$, then the weight increases by

$$\begin{aligned}\lfloor \log_2(i+m_i) \rfloor - \lfloor \log_2 m_i \rfloor &\leqslant \lfloor \log_2(i+m_i) - \log_2 m_i \rfloor + 1 \\ &\leqslant \left\lfloor \log_2 \left(1 + \frac{2^k + k - 2}{3}\right) \right\rfloor + 1 \leqslant k,\end{aligned}$$

since $1 + \frac{1}{3}(2^k + k - 2) = \frac{1}{3}(2^k + k + 1) < \frac{1}{3}(2^k + 2^{k+1}) = 2^k$.

Finally, let $i \leqslant 2^k - 2$ to consider the subcases $m_i = 3$ and $m_i \geqslant 4$. In the former subcase, the weight increases by

$$\lfloor \log_2(i+3) \rfloor - \lfloor \log_2 3 \rfloor \leqslant \lfloor \log_2(2^k + 1) \rfloor - 1 = k - 1,$$

and in the latter by

$$\begin{aligned}\lfloor \log_2(i+m_i) \rfloor - \lfloor \log_2 m_i \rfloor &\leqslant \lfloor \log_2(i+m_i) - \log_2 m_i \rfloor + 1 \\ &\leqslant \left\lfloor \log_2 \left(1 + \frac{2^k - 2}{4}\right) \right\rfloor + 1 \leqslant k - 1,\end{aligned}$$

since $1 + \frac{1}{4}(2^k - 2) = \frac{1}{4}(2^k + 2) < 2^{k-2} + 1$. This ends the proof and completes the solution.

C3. Odin and Evelyn are playing a game, Odin going first. There are initially $3k$ empty boxes, for some given positive integer k. On each player's turn, they can write a non-negative integer in an empty box, or erase a number in a box and replace it with a strictly smaller non-negative integer. However, Odin is only ever allowed to write odd numbers, and Evelyn is only allowed to write even numbers. The game ends when either one of the players cannot move, in which case the other player wins; or there are exactly k boxes with the number 0, in which case Evelyn wins if all other boxes contain the number 1, and Odin wins otherwise. Who has a winning strategy?

Agnijo Banerjee, United Kingdom

Solution. Evelyn has a winning strategy. Begin by noticing that any legal move by Odin involves writing an odd number n, so Evelyn is allowed to replace it with the even number $n-1$. In particular, the game cannot end because Evelyn is unable to move.

Evelyn's strategy is described in terms of the following valuation: Collect the numbers in all non-empty boxes to form $\mathbf{a} = (a_1, \ldots, a_\ell)$, where $\ell \leqslant 3k$, and define the *valuation* of $\mathbf{a}$ by

$$V(\mathbf{a}) = \textstyle\sum_{i=1}^{\ell} (-1/2)^{a_i}.$$

Notice that when Odin makes a move, the valuation strictly decreases; and when Evelyn makes a move, the valuation strictly increases.

Since the boxes are initially all empty, the game starts with a zero valuation, and after the first move (by Odin) the valuation is strictly negative. Evelyn's strategy consists in making the valuation at most zero after each of her moves. Consequently, after each legal move by Odin, the valuation is strictly negative.

To show that Evelyn can always achieve this, distinguish the two possible cases below.

Case 1: There is at least one empty box, and the current valuation is $-v$ for some strictly positive v. Then Evelyn should choose any even number n making $2^n v \geqslant 1$, and write n in an empty box.

Case 2: There are no empty boxes, so $3k$ numbers contributing to the evaluation. Then $V(\mathbf{a}) \equiv 0 \pmod 3$, since $(-1/2)^a \equiv 1 \pmod 3$. It is not possible that all numbers be zero, for otherwise the game would already have come to an end. Letting n be the largest entry of the current $\mathbf{a}$, it then follows that $V(\mathbf{a}) \leqslant -3/2^n$, since $V(\mathbf{a})$ is strictly negative and congruent to zero modulo 3.

If n is odd, respectively even, then replacing n by $n-1$, respectively $n-2$, increases the valuation by $3/2^n$. Consequently, in either case, Evelyn can make a move to yield a valuation that does not exceed zero.

To prove Evelyn's strategy winning, notice that she can ensure that the game ends either with Odin unable to move, or with k zeroes and a valuation $V(\mathbf{a}_{\text{end}}) \leqslant 0$. In the latter case, notice that the contribution of each non-zero number to the valuation is at least $-1/2$, so

$$V(\mathbf{a}_{\text{end}}) \geqslant k + \underbrace{(-1/2 - 1/2 - \cdots - 1/2)}_{2k} = 0,$$

forcing the non-zero numbers to be all equal to 1. Consequently, Evelyn's strategy is indeed winning.

C4. A *strategical video game* consists of a map of finitely many towns. In each town there are k directions, labelled from 1 through k. One of the towns is designated as *initial*, and one – as *terminal*. Starting from the initial town the hero of the game makes a finite sequence of *moves*. At each move the hero selects a direction from the current town. This determines the next town he visits and a certain positive amount of points he receives.

Two strategical video games are *equivalent* if for every sequence of directions the hero can reach the terminal town from the initial in one game, he can do so in the other game, and, in addition, he accumulates the same amount of points in both games.

For his birthday John receives two strategical video games – one with N towns and one with M towns. He claims they are equivalent. Marry is convinced they are not. Marry is right. Prove that she can provide a sequence of at most $N+M$ directions that shows the two games are indeed not equivalent.

Stefan Gerdjikov, Bulgaria

Solution 1. Without loss of generality we may assume that the set of directions is $D = \{1, 2, \ldots, k\}$. Let us enumerate the towns in the first game from 1 through N and the towns in the second game from $N+1$ through $N+M$. Without loss of generality we may assume that the initial and terminal towns in the first game are 1 and N, whereas in the second game these are – $N+1$ and $N+M$, respectively.

Next we consider a directed labelled graph $G = (V, \lambda)$ where $V = \{1, 2, \ldots, N+M\}$ and $\lambda : V \times D \to V \times \mathbb{N}$ maps a current town u and direction d to $\lambda(v, d) = (u, p)$, where u is the next town and p is the amount of points awarded for this move. In particular if $v \leqslant N$ if and only if $u \leqslant N$. For each vertex $v \in V$, we denote with $L_n(v) = L_{n,G}(v)$ the set of all pairs (s, p), where s is a sequence of directions of length less than or equal to n that leads from v to a terminal town and p is total amount of points awarded for this sequence. $L(v)$ is the union of all sets $L_n(v)$ for $n \in \mathbb{N} \cup \{0\}$. With this notion we want to prove that:

$$L(1) = L(N+1) \quad \text{if and only if} \quad L_n(1) = L_n(N+1) \quad \text{for all } n \leqslant N+M.$$

To this end, we first slightly modify the games by awarding the hero points he deserves as soon as possible. Formally, let:

$$c(v) = \min\{p \colon (s, p) \in L_{M+N}(v) \text{ for some } s\}.$$

Since the points are always positive, every cycle in G brings a positive amount of points. Therefore, $p' \geqslant c(v)$ for every n and every pair $(s', p') \in L_n(v)$. In particular, if $\lambda(v, d) = (u, p)$ then since the hero can win $p + c(u)$ points starting from v, we obtain $p + c(u) \geqslant c(v)$. Note that if $c(1) \neq c(N+1)$, then $L_{N+M}(1) = L_{N+M}(N)$ are vacuously distinct and we are done. Thus, we may assume that $c(1) = c(N+1)$.

Let $G' = (V, \lambda')$ be defined by $\lambda'(v, d) = (u, p + c(u) - c(v))$ whenever $\lambda(v, d) = (u, p)$. By the above argument every move in G' is awarded with non-negative amount of points. Furthermore, an easy inductive argument shows that $(s, p) \in L_n(v)$ if and only if $(s, p - c(v)) \in L'_n(v)$, where $L'_n(v) = L_{n,G'}(v)$. Hence $L_n(1) = L_n(N+1)$ if and only if $L'_n(1) = L'_n(N+1)$.

Assume that $L'(u) = L'(v)$ and consider an arbitrary direction d. If $(u', p') = \lambda(u, d)$ and $(v', q') = \lambda(v, d)$, we claim that $L'(u') = L'(v')$ and $p' = q'$. Indeed, let s be such a sequence of moves that $(s, c(u')) \in L(u')$. Hence $((d, s), p') \in L'(u)$. Since $L'(u) = L'(v)$

and there are no negative points along the arcs, we get $q' \leqslant p'$. Similarly, $p' \leqslant q'$ and therefore $p' = q'$. Now, it is easy to see that if $(s,p) \in L'(u')$ then $((d,s), p+p') \in L'(u) = L'(v)$ and therefore $(s,p) \in S(v)$ where we used that $p' = q'$. To reverse inclusion proceed similarly.

Finally, consider the equivalence relations $\equiv^{(n)}$ recursively defined below:

$$u \equiv^{(0)} v \text{ if and only if either } u, v \in \{N, M+N\} \text{ or } u, v \notin \{N, M+N\},$$
$$u \equiv^{(n+1)} v \text{ if and only if } u \equiv^{(n)} v, \text{ and } u' \equiv^{(n)} v' \text{ and } p' = q' \text{ for all } d \leqslant D,$$

where $(u', p') = \lambda'(u, d)$ and $(v', q') = \lambda'(v, d)$. Since $\equiv^{(n+1)}$ is contained in $\equiv^{(n)}$, and each equivalence relation has no more than $N + M$ classes, it follows that $\equiv^{(n)}$ and $\equiv^{(n+1)}$ coincide for some $n < N + M$. Therefore, for this particular n, an easy inductive argument shows that $\equiv^{(m)}$ and $\equiv^{(n)}$ are the same for all $m \geqslant n$. Hence if $u \equiv^{(n)} v$ an induction on the length of the sequence of moves reveals that $(s,p) \in L'(u)$ if and only if $(s,p) \in L'(v)$. Consequently, $L'(u) = L'(v)$.

This proves that if $L'(1) \neq L'(N+1)$, then $1 \not\equiv^{(n)} N+1$. Finally, we show that if $u \not\equiv^{(n)} v$, then $L_n(u) \neq L_n(v)$. This is obvious for $n = 0$ and $n = 1$. Assume that the statement holds for some n and all $u, v \in V$ and consider some $u \not\equiv^{(n+1)} v$. We need to prove that $L_{n+1}(u) \neq L_{n+1}(v)$. By the inductive hypothesis we may assume that $u \equiv^{(n)} v$. In particular, $u \equiv^{(1)} v$. Therefore, $\lambda'(u, d) = (u', p)$ for all $d \leqslant k$, and $\lambda'(v, d) = (v', q)$ implies that $p = q$. Therefore, the fact that $u \equiv^{(n+1)} v$ is due to some $d \leqslant k$ such that $u' \not\equiv^{(n)} v'$. By the inductive hypothesis $L'_n(u') \neq L'_n(v')$. It should now be clear that $L'_{n+1}(v) \neq L'_{n+1}(v')$.

Remarks. In fact, this is a straightforward implication of the minimisation algorithm for (sub)sequential transducers. It consists of two steps, each of which contains an interesting idea:

1. Pushing forward the costs – in this case, awarding the hero the maximum amount of points that he has already guaranteed. This is also related to potentials in weighted graphs, often used to accelerate the Minimum Cost Paths Problem. However, in this case the issue is not only of algorithmic flavour, but is conceptual.

2. The bisimulation and Nerode-Myhill relation that stabilises in at most $O(|Q|)$ steps.

Solution 2. One can also approach the problem from algebraic perspective. Again, consider the towns in the first and the second game as natural numbers from 1 through N, and from $N+1$ through $N+M$, respectively; initial and terminal towns – 1 and N in the first game; $N+1$ and $N+M$ – in the second.

For every direction d let A_d be the $(N+M) \times (N+M)$ matrix whose entries $a_d(i,j)$ are defined by

$$a_d(i,j) = \begin{cases} 2^p, & \text{if starting from town } i \text{ and following direction } d \\ & \text{the hero gets to town } j \text{ and is awarded } p \text{ points,} \\ 0, & \text{otherwise.} \end{cases}$$

With this notion, for any sequence of directions $\mathbf{d} = (d_1, d_2, \ldots, d_n)$ the (i,j) entry of the product matrix $A_{d_1} A_{d_2} \cdots A_{d_n}$ is 2^p if the hero, following the sequence $\mathbf{d}$ and starting from town i, arrives in town j and wins p points.

Let e_i be the standard unit vector in $\mathbb{R}^{N+M}$ whose i-th entry is 1 and the other entries are all 0. Write $s = e_1 - e_{N+1}$ and $f = e_N + e_{N+M}$.

Since there are no connections between towns in the two games, we have to prove that $s^T A f = 0$ for all $A = A_{d_1} \cdots A_{d_n}$ if and only if $s^T A f = 0$ for all $A = A_{d_1} \cdots A_{d_n}$ with $n \leqslant N + M$.

To prove this, let $V_0 = \{s\}$ and let $V_{n+1} = V_n \cup \{v^T A_d \colon v \in V_n \text{ and } d \leqslant k\}$. Clearly, each V_n spans a linear space of dimension at most $N + M$. Hence, $\dim \operatorname{span} V_n = \dim \operatorname{span} V_{n+1}$ for some $n < N+M$, and so every vector from V_{n+1} is a linear combination of vectors from V_n. A simple inductive argument then shows that the vectors in V_m are linear combinations of vectors from V_n for all $m \geqslant n$. In particular, if the vectors in V_n are all orthogonal to f, then so are the vectors in V_m for any $m \in \mathbb{N}$.

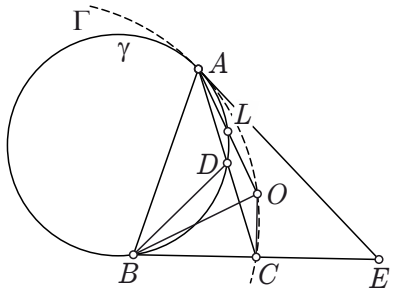
Remark. Both solutions have been provided by the author.

Geometry

G1. Let ABC be an isosceles triangle, $AB = AC$, let D be the midpoint of the side AC, and let γ be the vircumcircle of the triangle ABD. The tangent of γ at A crosses the line BC at E. Let O be the circumcentre of the triangle ABE. Prove that the midpoint of the segment AO lies on γ.

Sam Bealing, United Kingdom

Solution. Let Γ be the image of γ under the homothety of centre A and factor 2. Clearly, Γ is also tangent yo AE at A, and the conclusion is equivalent to Γ passing through O, which is the same as AE being tangent to the circle ACO.



Alternatively, but equivalently, this amounts to $\angle OAE = \angle OCA$. Write $\angle OAE = 90^\circ - \angle EBA$ and $\angle OCA = \angle OCB - \angle ACB = \angle OCB - \angle CBA = \angle OCB - \angle EBA$, to infer that the equality of the two angles is equivalent to C being the midpoint of the segment BE.

To prove the latter, it is sufficient to show that the triangles ABE and DBC are similar, for then $BE/BC = AB/CD = AC/CD = 2$ which implies that C is indeed the midpoint of the segment BE.

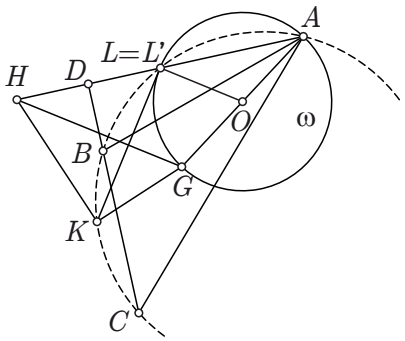
Finally, to prove the above similarity, write $\angle EBA = \angle CBA = \angle ACB = \angle DCB$ and $\angle BDC = \angle BAD + \angle DBA = \angle BAD + \angle DAE = \angle BAE$. This completes the proof.

G2. Let G, H be the centroid and orthocentre of $\triangle ABC$ which has an obtuse angle at $\angle B$. Let ω be the circle with diameter AG. ω intersects $\odot ABC$ again at $L \neq A$. The tangent to ω at L intersects $\odot ABC$ at $K \neq L$.

Given that $AG = GH$, prove $\angle HKG = 90^\circ$.

Sam Bealing, United Kingdom

Solution. Let L' be the midpoint of AH. Then we claim L' lies on $\odot ABC$.



Indeed, let D be the foot of the A-altitude on BC. Then:

$$AG = GH \Rightarrow \angle GL'A = 90^\circ \Rightarrow GL' \parallel BC \Rightarrow DL' = \frac{AL'}{2} = \frac{HL'}{2} \Rightarrow DL' = HD$$

where in the last step we have used that if M is the midpoint of BC, $AG : GM = 2 : 1$ and that $\angle B$ is obtuse so H, A lie on opposite sides of line BC. This means that L' is the reflection of H in BC, which is well-known to lie on $\odot ABC$. Also $AG = GH \Rightarrow \angle GL'A = 90^\circ$ so L' lies on ω and hence in fact $L \equiv L'$.

Let O be the midpoint of AG; then $OL \perp LK$. Homothety of factor 2 at A takes $OL \to HG$ so $HG \parallel OL$ and hence $LK \perp HG$. But the centre of $\odot ABC$ lies on HG so this means K is the reflection of L across line HG and hence as $\angle HLG = 90^\circ$ it follows $\angle HKG = 90^\circ$.

Remark. The midpoint of AH lies on the circumcircle of $\odot ABC$ iff $\angle A = 90^\circ$ or if:

$$a^4 + a^2(b^2 + c^2) - 2(b^2 - c^2)^2 = 0$$

The latter condition is exactly equivalent to $AG = GH$.

G3. Let ABC be a triangle. On the sides BC, CA, AB of the triangle, construct outwardly three squares with centres O_a, O_b, O_c respectively. Let ω be the circumcircle of $\triangle O_aO_bO_c$.

Given that A lies on ω, prove that the centre of ω lies on the perimeter of $\triangle ABC$.

Sam Bealing, United Kingdom

Solution. Let the vertices of the squares be AC_1C_2B, BA_1A_2C, CB_1B_2A.

Lemma: $BB_2 = CC_1$ and $BB_2 \perp CC_1$.

Proof: Notice that by rotating $\triangle AC_1C$ by 90° we get $\triangle ABB_2$ proving the lemma.

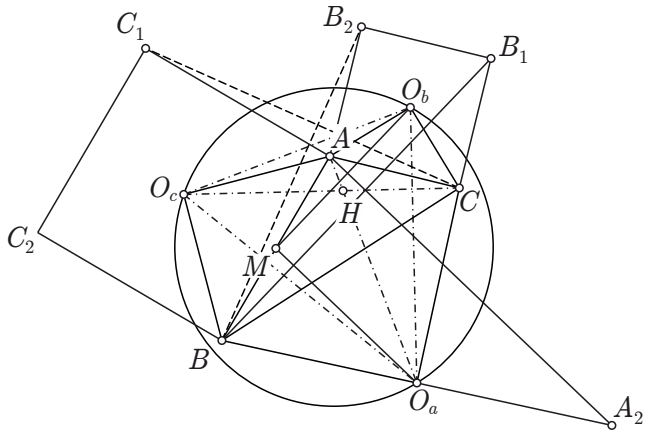
Claim: $AO_a \perp O_bO_c$

Proof: Let M be the midpoint of AB. By our lemma applied at vertex C we get $AA_2 = BB_1$ and they are perpendicular. By homothety of factor 2 at A and then B we get:

$$MO_b = \frac{1}{2}BB_1 = \frac{1}{2}AA_2 = MO_a \quad \text{and} \quad MO_b \parallel BB_1 \ , \ MO_a \parallel AA_2$$

Hence MO_a, MO_b are also perpendicular so in fact $\triangle O_bMO_a$ is an isosceles right triangle. This is also trivially the case for $\triangle AMO_c$. Now applying our lemma to $\triangle AMO_b$ at vertex M we get O_bO_c and AO_a are perpendicular which is exactly what we wanted.

Similarly we get $BO_b \perp O_aO_c$ and $CO_c \perp O_aO_b$ so lines AO_a, BO_b, CO_c concur at H, the orthocentre of $\triangle O_aO_bO_c$. As A lies on ω and on O_aH it follows A is the reflection of H in line O_bO_c.



Claim: $H = B$ or $H = C$

Proof: Assume not. By the previous observations we get $O_cH = O_cA = O_cB$. Hence as $O_cO_a \perp BH$ and $B \neq H$ this means B is the reflection of H in O_cO_a so B lies on ω.

Similarly, C lies on ω. But then we get:

$$\angle ACB = 180^\circ - \angle BO_cA = 90^\circ \quad \text{and} \quad \angle CBA = 180^\circ - \angle AO_bC = 90^\circ$$

so $\angle ACB + \angle CBA = 180^\circ$ which is absurd so in fact one of B, C is equal to H.

WLOG $B = H$. As A, H, O_a and C, H, O_c are collinear this means in fact B lies on these lines. Hence:

$$\angle AO_cC = \angle AO_cB = 90^\circ$$

Also $\angle AO_bC = 90^\circ$ hence C also lies on ω and ω in fact has diameter AC and so its circumcentre is the midpoint of AC which lies on the perimeter of $\triangle ABC$.

G4. Let $MAZN$ be an isosceles trapezium inscribed in a circle (c) with centre O. Assume that MN is a diameter of (c) and let B be the midpoint of AZ. Let (ε) be the perpendicular line on AZ passing through A. Let C be a point on (ε), let E be the point of intersection of CB with (c) and assume that AE is perpendicular to CB. Let D be the point of intersection of CZ with (c) and let F be the antidiametric point of D on (c). Let P be the point of intersection of FE and CZ. Assume that the tangents of (c) at the points M and Z meet the lines AZ and PA at the points K and T respectively. Prove that OK is perpendicular to TM.

Theoklitos Parayiou, Cyprus

Solution. We will first prove that PA is the tangent of (c) at A. Since $EDZA$ is cyclic, then $\angle EDC = \angle EAZ$. By the similarity of the triangles CAE and ABE we have $\angle EAZ = \angle EAB = \angle ACB$, so $\angle EDC = \angle EAZ$. Since $\angle FED = 90^\circ$, then

$$\angle EPD = 90^\circ - \angle EDC = 90^\circ - \angle ACB = \angle EAC$$

So the points E, A, C, P are concyclic. It follows that $\angle CPA = 90^\circ$, therefore the triangle APZ is right-angled. Since also B is the midpoint of AZ, then $PB = AB = BZ$.

We have

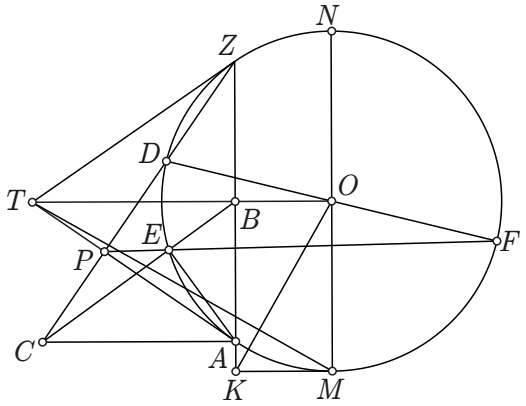
$$\angle BPE = \angle ABC - \angle BPZ = \angle ABC - \angle PZB$$

and

$$\angle PAE = \angle PCE = 90^\circ - \angle ACB - \angle CZA = \angle ABC - \angle CZA = \angle ABC - \angle PZB$$

Therefore $\angle BPE = \angle PAE$.

Since also $\angle EPD = \angle EAC = \angle EBA$, then $PEBZ$ is a cyclic quadrilateral and we get $\angle BPE = \angle EZB$. Therefore $\angle PAE = \angle EZB$, i.e. PA is the tangent of (c) at A.



Since AZ is parallel to MN then $TB \perp AZ$ and $TO \perp MN$.

The quadrilateral $KBOM$ is a rectangle. Consider the circumcircle of the rectangle and a tangent of this at K. Let X be a point on this tangent. So $XK \perp KO$. Since the triangle OBA and OTA are similar then $OA^2 = OT \cdot OB$. Since $OA = OM$ and $KM = OB$ we get $OM^2 = OT \cdot KM$ so $\frac{OT}{OM} = \frac{OM}{KM}$. Since also $\angle KMO = \angle TOM = 90^\circ$, the triangles TOM and OMK are similar. Therefore

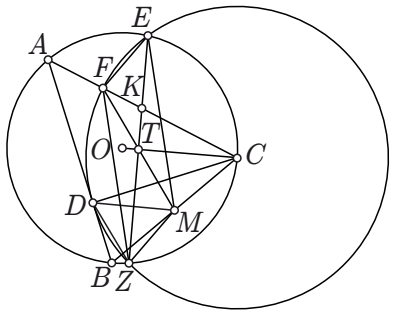
$$\angle MTO = \angle KOM = \angle XKM$$

Since KM is parallel to TO we have $\angle MTO = \angle KMT$. Therefore $\angle XKM = \angle KMT$. I.e. the tangent at point K is parallel to MT and since $XK \perp KO$ we get $OK \perp TM$.

G5. Let ABC be an isosceles triangle with $AB = AC$ and $\angle A = 45^\circ$. Its circumcircle (c) has center O, M is the midpoint of BC and D is the foot of the perpendicular from C to AB. With center C and radius CD we draw a circle which internally intersects AC at the point F and the circle (c) at the points Z and E, such that Z lies on the small arc $\overset{\frown}{BC}$ and E on the small arc $\overset{\frown}{AC}$. Prove that the lines ZE, CO, FM are concurrent.

Brazitikos Silouanos, Greece

Solution. Since ZE is the common chord of the two circles, the line of the centres CO is its perpendicular bisector. This means that CO passes through the midpoint of ZE, let it be T. Thus, it suffices to prove that FM passes through T. To this end, we will prove that $FZME$ is a parallelogram: we will precisely show that the segments FE and ZM are parallel and equal.



Let K be the intersection point of ZE and AC. Then K lies on the radical axis of the two circles, so it has equal powers to both circles. The power of the point K with respect to the one circle is $KA \cdot KC$, while the power to the other circle is $R^2 - KC^2 = CD^2 - KC^2$.

From the theorem of Pythagoras in triangle ADC we get $AC^2 = 2CD^2$. We set $KA = x, KC = y$, and combining all the above yields $xy = \frac{(x+y)^2}{2} - y^2$, hence $2xy = x^2 + y^2 + 2xy - y^2$, i.e. $x = y$.

This means that K is the midpoint of AC. Moreover, we have $\angle ADC = \angle AMC = 90^\circ$, so the points A, D, M, C are on the same circle – let it be (c_1) – and the center of this circle is K.

From the cyclic quadrilateral we have that $\angle DMB = 45^\circ$, but we have also that $\angle OCB = 45^\circ$, so the lines OC, DM are parallel, hence $KZ \perp DM$ and, since DM is a chord of the circle, $ZD = ZM$. (1)

The triangle CDF is isosceles and CO is bisector, so $CO \perp DF$, and this means that $ZE \parallel DF$. It follows that $DFEZ$ is an isosceles trapezium, so $DZ = FE$ (2), and from (1) and (2) we have that $ZM = FE$ (*).

From the isosceles trapezium we also have that $\angle FEZ = \angle DZE$ (3). Since ZK is an altitude in the isosceles triangle DZM, it will be also angle bisector, so $\angle DZE = \angle MZE$ (4).

From (3) and (4) we conclude that $\angle FEZ = \angle MZE$, so $FE \parallel ZM$ (**). From (*) and (**) we get that $FZME$ is a parallelogram, which is the desired result.

Number Theory

N1. Determine all positive integers n such that $\dfrac{a^2+n^2}{b^2-n^2}$ is a positive integer for some positive integers a and b.

Turkey

Solution. The required numbers are all even positive integers alone. Indeed, if n is even, then let $a = n^2/2 - 1$ and $b = n^2/2 + 1$, to check that $(a^2+n^2)/(b^2-n^2) = (n^4/4+1)/(n^4/4+1) = 1$.

Suppose now that such a and b exist for some positive odd integer n. Notice that we may and will assume $\gcd(n,a,b) = 1$. Note also that $n^2 \equiv 1 \pmod 4$. If b is odd, then b^2-n^2 is divisible by 4, and hence so is a^2+n^2. Since n is odd, a^2+1 is therefore divisible by 4, which is impossible. Thus, b must be even. Then $b^2-n^2 \equiv 3 \pmod 4$, so b^2-n^2 has a prime factor $p \equiv 3 \pmod 4$. Then a^2+n^2 is divisible by p, and it follows that so are both a and n, since $p \equiv 3 \pmod 4$. On the other hand, since n and b^2-n^2 are both divisible by p, so is b. Consequently, a, b and n are all divisible by p, contradicting the assumption $\gcd(n,a,b) = 1$.

N2. A number of N children are at a party, and they sit in a circle to play a game of Pass the Parcel. Because the host has no other form of entertainment, the parcel has infinitely many layers. On turn i, starting with $i = 1$, the following two things happen in order:

(1) The parcel is passed i^2 positions clockwise; and
(2) The child currently holding the parcel unwraps a layer and claims the prize inside.

For what values of N will every child receive a prize?

Patrick Winter, United Kingdom

Solution. Every child receives a prize if and only if $N = 2^a 3^b$ for some non-negative integers a and b. For convenience, say N is *good* if every child receives a prize.

Number the children $0, \ldots, N-1$ clockwise around the circle, child number 0 starting with the parcel. After n turns, the parcel will have been passed $1^2+2^2+\cdots+n^2 = n(n+1)(2n+1)/6$ places around the circle. For convenience, write $s_n = n(n+1)(2n+1)/6$. Thus, child m receives the parcel, and hence a prize, if and only if $m \equiv s_n \pmod N$ for some n, so N is good if and only if s_n assumes every possible value modulo N.

To rule out the case where N is divisible by a prime $p > 3$, it is sufficient to show that s_n misses some value modulo p. The latter follows from the fact that 6 has a multiplicative inverse modulo p, and $s_n \equiv 0 \pmod p$ if $n \equiv 0$ or $-1 \pmod p$, so s_n assumes at most $p-1$ values modulo p. Consequently, such an N is certainly not good.

We now show that each N of the form $2^a 3^b$ is good. We do this by showing that, if N is good, then so are both $2N$ and $3N$; since 1 is clearly good, this is sufficient to prove goodness of $2^a 3^b$ inductively on $a + b$.

To show that, if N is good, then so is $2N$, refer to goodness of the former to infer that, for each m modulo $2N$, there exists an n such that $s_n \equiv m$ or $m + N \pmod{2N}$. Clearly, only the case $s_n \equiv m + N \pmod{2N}$ is to be dealt with. In this case,

$$s_{n+6N} = s_n + (6n^2 + 6n + 1)N + 18(2n + 1)N^2 + 72N^3 \equiv s_n + N \equiv m \pmod{2N}.$$

Consequently, $2N$ is indeed good.

To show that, if N is good, then so is $3N$, refer again to goodness of the former to infer that, for each m modulo $3N$, there exists an n such that $s_n \equiv m$ or $m+N$ or $m+2N \pmod{3N}$. Clearly, only the last two cases are to be dealt with. In the former case,

$$s_{n+12N} = s_n + 2(6n^2 + 6n + 1)N + 72(2n + 1)N^2 + 2^6 3^2 N^3 \equiv s_n + 2N \equiv m \pmod{3N},$$

and in the latter,

$$s_{n+6N} = s_n + (6n^2 + 6n + 1)N + 18(2n + 1)N^2 + 72N^3 \equiv s_n + N \equiv m \pmod{3N}.$$

Consequently, $3N$ is indeed good.

N3. Given an integer $k \geqslant 2$, determine all functions f from the positive integers into themselves such that $f(x_1)! + f(x_2)! + \cdots + f(x_k)!$ is divisible by $x_1! + x_2! + \cdots + x_k!$ for all positive integers $x_1, x_2, \ldots, x_k$.

Albania

Solution. The identity is the only function satisfying the condition in the statement. Begin by letting the x's be all equal to n to infer that $f(n)!$ is divisible by $n!$, so $f(n) \geqslant n$ for all positive integers n.

Claim. *$f(p-1) = p-1$ for all but finitely many primes p.*

Assume the Claim for the moment to proceed as follows: Fix any positive integer n, and let p be a large enough prime, e. g., $p > f(n)! - n!$. Then let one of the x's be equal to 1 and the remaining $k-1$ be all equal to $p-1$, and use the Claim to infer that the number

$$(f(n)! - n!) + (n! + (k-1)(p-1)!) = f(n)! + (k-1)f(p-1)!$$

is divisible by $n! + (k-1)(p-1)!$, and hence so is $f(n)! - n!$. Since p is large enough, this forces $f(n)! = n!$, and since $f(n) \geqslant n$, it follows that $f(n) = n$, as desired.

Proof of the Claim. If k is even, let $p > f(1)!$, and let half of the x's be all equal to 1 and the other half be all equal to $p-1$, to infer that $f(p-1)! + f(1)!$ is divisible by $(p-1)!+1$. By Wilson's theorem, the latter is divisible by p, and hence so is the former. Since $p > f(1)!$, the number $f(1)!$ is not divisible by p, so $f(p-1)!$ is not divisible by p either, forcing $f(p-1) \leqslant p-1$. Recall now that $f(p-1) \geqslant p-1$, to conclude that $f(p-1) = p-1$.

If k is odd, let $p > f(2)! + \frac{1}{2}(k-3)f(1)!$, let $\frac{1}{2}(k+1)$ of the x's be all equal to $p-1$, let one of the x's be equal to 2, and let the remaining ones (if any) be all equal to 1, to infer that $\frac{1}{2}(k+1)f(p-1)! + f(2)! + \frac{1}{2}(k-3)f(1)!$ is divisible by $\frac{1}{2}(k+1)(p-1)! + 2 + \frac{1}{2}(k-3) = \frac{1}{2}(k+1)((p-1)!+1)$. By Wilson's theorem, the latter is divisible by p, and hence so is the former. Since $p > f(2)! + \frac{1}{2}(k-3)f(1)!$, the number $f(2)! + \frac{1}{2}(k-3)f(1)!$ is not divisible by p, so $\frac{1}{2}(k+1)f(p-1)!$ is not divisible by p either, forcing $f(p-1) \leqslant p-1$. Recall again that $f(p-1) \geqslant p-1$, to conclude that $f(p-1) = p-1$.

N4. Let $a_1 = 2$ and, for every positive integer n, let a_{n+1} be the smallest integer strictly greater than a_n that has more positive divisors than a_n has. Prove that $2a_{n+1} = 3a_n$ only for finitely many indices n.

Macedonia

Solution. Begin with a mere remark on the terms of the sequence under consideration.

Lemma 1. *Each a_n is minimal amongst all positive integers having the same number of positive divisors as a_n.*

Proof. Suppose, if possible, that for some n, some positive integer $b < a_n$ has as many positive divisors as a_n. Then $a_m < b \leqslant a_{m+1}$ for some $m < n$, and the definition of the sequence forces $b = a_{m+1}$. Since $b < a_n$, it follows that $m + 1 < n$, which is a contradiction, as a_{m+1} should have less positive divisors than a_n. □

Let $p_1 < p_2 < \cdots < p_n < \cdots$ be the strictly increasing sequence of prime numbers, and write canonical factorisations into primes in the form $N = \prod_{i \geqslant 1} p_i^{e_i}$, where $e_i \geqslant 0$ for all i, and $e_i = 0$ for all but finitely many indices i; in this notation, the number of positive divisors of N is $\tau(N) = \prod_{i \geqslant 1}(e_i + 1)$.

Lemma 2. *The exponents in the canonical factorisation of each a_n into primes form a non-strictly decreasing sequence.*

Proof. Indeed, if $e_i < e_j$ for some $i < j$ in the canonical decomposition of a_n into primes, then swapping the two exponents yields a smaller integer with the same number of positive divisors, contradicting Lemma 1. □

We are now in a position to prove the required result. For convenience, a term a_n satisfying $3a_n = 2a_{n+1}$ will be referred to as a *special* term of the sequence.

Suppose now, if possible, that the sequence has infinitely many special terms, so the latter form a strictly increasing, and hence unbounded, subsequence. To reach a contradiction, it is sufficient to show that:

(1) The exponents of the primes in the factorisation of special terms have a common upper bound e; and

(2) For all large enough primes p, no special term is divisible by p.

Refer to Lemma 2 to write $a_n = \prod_{i \geqslant 1} p_i^{e_i(n)}$, where $e_i(n) \geqslant e_{i+1}(n)$ for all i.

Statement **(2)** is a straightforward consequence of **(1)** and Lemma 1. Suppose, if possible, that some special term a_n is divisible by a prime $p_i > 2^{e+1}$, where e is the integer provided by **(1)**. Then $e \geqslant e_i(n) > 0$, so $2^{e_1(n)e_i(n)+e_i(n)} a_n / p_i^{e_i(n)}$ is a positive integer with the same number of positive divisors as a_n, but smaller than a_n. This contradicts Lemma 1. Consequently, no special term is divisible by a prime exceeding 2^{e+1}.

To prove **(1)**, it is sufficient to show that, as a_n runs through the special terms, the exponents $e_1(n)$ are bounded from above. Then, Lemma 2 shows that such an upper bound e suits all primes.

Consider a large enough special a_n. The condition $\tau(a_n) < \tau(a_{n+1})$ is then equivalent to $(e_1(n) + 1)(e_2(n) + 1) < e_1(n)(e_2(n) + 2)$. Alternatively, but equivalently, $e_1(n) \geqslant e_2(n) + 2$. The latter implies that a_n is divisible by 8, for either $e_1(n) \geqslant 3$ or a_n is a large enough power of 2.

Next, note that $9a_n/8$ is an integer strictly between a_n and a_{n+1}, so $\tau(9a_n/8) \leqslant \tau(a_n)$, which is equivalent to

$$(e_1(n) - 2)(e_2(n) + 3) \leqslant (e_1(n) + 1)(e_2(n) + 1),$$

so $2e_1(n) \leqslant 3e_2(n)+7$. This shows that a_n is divisible by 3, for otherwise, letting a_n run through the special terms, 3 would be an upper bound for all but finitely many $e_1(n)$, and the special terms would therefore form a bounded sequence.

Thus, $4a_n/3$ is another integer strictly between a_n and a_{n+1}. As before, $\tau(4a_n/3) \leqslant \tau(a_n)$. Alternatively, but equivalently,

$$(e_1(n) + 3)e_2(n) \leqslant (e_1(n) + 1)(e_2(n) + 1),$$

so $2e_2(n) - 1 \leqslant e_1(n)$. Combine this with the inequality in the previous paragraph to write $4e_2(n) - 2 \leqslant 2e_1(n) \leqslant 3e_2(n) + 7$ and infer that $e_2(n) \leqslant 9$. Consequently, $2e_1(n) \leqslant 3e_2(n) + 7 \leqslant 34$, showing that $e = 17$ is suitable for **(1)** to hold. This establishes **(1)** and completes the solution.

N5. Consider an integer $n \geqslant 2$ and an odd prime p. Let U be the set of all positive integers (strictly) less than p^n that are not divisible by p, and let N be the number of elements of U. Does there exist a permutation $a_1, a_2, \ldots, a_N$ of the numbers in U such that the sum $\sum_{k=1}^{N} a_k a_{k+1}$, where $a_{N+1} = a_1$, be divisible by p^{n-1}, but not by p^n ?

Alexander Ivanov, Bulgaria

Solution. The answer is in the affirmative. Letting $\equiv$ denote congruence modulo p^n throughout the argument, we will show that there exists a permutation $a_1, a_2, \ldots, a_N$ of the numbers in U such that $\sum_{k=1}^{N} a_k a_{k+1} \equiv p^{n-1}$.

Let $m = p^{n-1}-1$, so $N = p^{n-1}(p-1) = (m+1)(p-1)$, and write $U = \{u_1, u_2, \ldots, u_N\}$, where $u_k = k + \lfloor k/(p-1) \rfloor^*$, $k = 1, 2, \ldots, N$, and $\lfloor t \rfloor^*$ denotes the largest integer (strictly) less than the real number t.

That the u_k are pairwise distinct and they all lie in U follows from the fact that every k in the range 1, 2, …, N is uniquely expressible in the form $k = (p-1)j + i$ for some j in the range 0, 1, …, m and some i in the range 1, 2, …, $p-1$. Thus, $u_k = u_{(p-1)j+i} = pj + i$, so the u_k are indeed pairwise distinct and they all lie in U.

For k in the range 1, 2, …, $N-1$, notice that $u_{k+1} - u_k = 1$, unless k is divisible by $p-1$, in which case $u_{k+1} - u_k = 2$. Setting $u_{N+1} = u_1$, it is readily checked that $u_{N+1} - u_N = 2 - p^n \equiv 2$, so $u_{k+1} - u_k \equiv 2$ for all k divisible by $p-1$.

Letting now a_k be the multiplicative inverse of u_k modulo p^n, i. e., a_k is the unique member of U satisfying $a_k u_k \equiv 1$, we show that the a_k form the desired permutation of U.

To begin with, notice that $a_k a_{k+1} \equiv a_k - a_{k+1}$, unless k is divisible by $p-1$, in which case $a_k a_{k+1} \equiv \frac{1}{2}(a_k - a_{k+1})$. This is easily established by multiplying both sides of each congruence by $u_k u_{k+1}$, and noticing that $(a_k - a_{k+1}) u_k u_{k+1} \equiv u_{k+1} - u_k \equiv 1 \text{ or } 2$.

We are now in a position to evaluate the sum $S = \sum_{k=1}^{N} a_k a_{k+1}$ modulo p^n. Write

$$S = \sum_{k=1}^{N} a_k a_{k+1} = \sum_{j=0}^{m} \sum_{i=1}^{p-1} a_{(p-1)j+i}\, a_{(p-1)j+i+1},$$

and consider the inner sum for a fixed j in the range 0, 1, …, m:

$$\begin{aligned}
\sum_{i=1}^{p-1} a_{(p-1)j+i}\, a_{(p-1)j+i+1} &= \sum_{i=1}^{p-2} a_{(p-1)j+i}\, a_{(p-1)j+i+1} + a_{(p-1)j(j+1)} a_{(p-1)(j+1)+1} \\
&\equiv \sum_{i=1}^{p-2} \big(a_{(p-1)j+i} - a_{(p-1)j+i+1}\big) + \tfrac{1}{2}\big(a_{(p-1)j(j+1)} - a_{(p-1)(j+1)+1}\big) \\
&\equiv a_{(p-1)j+1} - a_{(p-1)(j+1)} + \tfrac{1}{2}\left(a_{(p-1)j(j+1)} - a_{(p-1)(j+1)+1}\right) \\
&\equiv a_{(p-1)j+1} - \tfrac{1}{2} a_{(p-1)j(j+1)} - \tfrac{1}{2} a_{(p-1)(j+1)+1}.
\end{aligned}$$

Hence

$$\begin{aligned} S &\equiv \sum_{j=0}^{m} a_{(p-1)j+1} - \frac{1}{2}\sum_{j=0}^{m} a_{(p-1)(j+1)} - \frac{1}{2}\sum_{j=0}^{m} a_{(p-1)(j+1)+1} \\ &\equiv \left(a_1 + \sum_{j=1}^{m} a_{(p-1)j+1}\right) - \frac{1}{2}\sum_{j=1}^{m+1} a_{(p-1)j} - \frac{1}{2}\left(\sum_{j=1}^{m} a_{(p-1)j+1} + a_{N+1}\right) \\ &\equiv \frac{1}{2}\sum_{j=1}^{m+1} a_{(p-1)j+1} - \frac{1}{2}\sum_{j=1}^{m+1} a_{(p-1)j}. \end{aligned}$$

Since $u_{(p-1)j+1} = pj + 1$, the $a_{(p-1)j+1}$ form a permutation of the $pj + 1$, therefore $\sum_{j=1}^{m+1} a_{(p-1)j+1} \equiv \sum_{j=1}^{m+1}(pj + 1)$. Similarly, $u_{(p-1)j} = pj - 1$, so the $a_{(p-1)j+1}$ form a permutation of the $pj - 1$, and hence $\sum_{j=1}^{m+1} a_{(p-1)j} \equiv \sum_{j=1}^{m+1}(pj - 1)$. Consequently,

$$S \equiv \frac{1}{2}\sum_{j=1}^{m+1} \big((pj + 1) - (pj - 1)\big) \equiv m + 1 \equiv p^{n-1},$$

as stated in the first paragraph. This completes the solution.

Remark. Multiplication modulo p^n makes U into the group of units of the ring $\mathbb{Z}_{p^n}$. Since p is odd, U is cyclic. Let g be a generator, i. e., a primitive root modulo p^n. In this setting, the sum in question is $S_{g,\alpha} \equiv \sum_{k=1}^{N} g^{\alpha_k + \alpha_{k+1}}$, where α is a permutation of 1, 2, …, N. The solution shows that $S_{g,\alpha} \equiv p^{n-1}$ for the permutation given by $a_k = g^{\alpha_k}$; for instance, if $n = 2$, $p = 5$ and $g = 2$, this permutation has disjoint cycle decomposition

$$(1\ 20\ 10\ 11)\,(2\ 19\ 9\ 4\ 18\ 3\ 13\ 16)\,(5\ 12\ 14\ 7\ 17\ 8\ 6\ 15).$$

Evaluating $S_{g,\alpha}$ is not an easy task, unless α exhibits particular features. Consider the identity permutation, in which case $S_{g,\mathrm{id}} \equiv 2g^3 \sum_{k=0}^{N/2-1} g^{2k}$, so $(g^2 - 1)S_{g,\mathrm{id}} \equiv 2g^3(g^N - 1) \equiv 0$. If $p > 3$ and g is a primitive root modulo p, then $S_{g,\mathrm{id}} \equiv 0$, so such a g is not a candidate. In particular, this rules out the standard choice for g modulo p^n as a primitive root modulo p such that $g^{p-1} - 1$ is not divisible by p^2. A good candidate for g ($p = 3$, inclusive) would be a primitive root modulo p^2 such that $g^2 - 1$ is divisible by p. In this case, $g^2 - 1$ is divisible by p but not by p^2, and $g^N - 1$ is divisible by p^n but not by p^{n+1}, so $S_{g,\mathrm{id}}$ satisfies the required condition. This is the case if $p = 3$: The primitive roots modulo 3^2 are 2 and 5, and the identity permutation works for both modulo 3^2. Unfortunately, no such g exists if $p = 5$: The primitive roots g modulo 5^2 are ± 2, ± 3 and ± 8, no $g^2 - 1$ is divisible by 5, so $S_{g,\mathrm{id}}$ is divisible by 5^2, showing the identity inadequate modulo 5^2.