49th International Mathematical Olympiad

July, 10-22 2008

Madrid, Spain

SHORT LIST

WITH SOLUTIONS

49$^{\text{th}}$ International Mathematical Olympiad

Spain 2008

Shortlisted Problems with Solutions

Contents

Contributing Countries & Problem Selection Committee **5**

Algebra **7**

Problem A1 . . . 7
Problem A2 . . . 9
Problem A3 . . . 11
Problem A4 . . . 12
Problem A5 . . . 14
Problem A6 . . . 15
Problem A7 . . . 17

Combinatorics **21**

Problem C1 . . . 21
Problem C2 . . . 23
Problem C3 . . . 24
Problem C4 . . . 25
Problem C5 . . . 26
Problem C6 . . . 27

Geometry **29**

Problem G1 . . . 29
Problem G2 . . . 31
Problem G3 . . . 32
Problem G4 . . . 34
Problem G5 . . . 36
Problem G6 . . . 37
Problem G7 . . . 40

Number Theory **43**

Problem N1 . . . 43
Problem N2 . . . 45
Problem N3 . . . 46
Problem N4 . . . 47
Problem N5 . . . 49
Problem N6 . . . 50

Contributing Countries

Australia, Austria, Belgium, Bulgaria, Canada, Colombia, Croatia, Czech Republic, Estonia, France, Germany, Greece, Hong Kong, India, Iran, Ireland, Japan, Korea (North), Korea (South), Lithuania, Luxembourg, Mexico, Moldova, Netherlands, Pakistan, Peru, Poland, Romania, Russia, Serbia, Slovakia, South Africa, Sweden, Ukraine, United Kingdom, United States of America

Problem Selection Committee

Vicente Muñoz Velázquez
Juan Manuel Conde Calero
Géza Kós
Marcin Kuczma
Daniel Lasaosa Medarde
Ignasi Mundet i Riera
Svetoslav Savchev

Algebra

A1. Find all functions $f\colon (0,\infty) \to (0,\infty)$ such that

$$\frac{f(p)^2+f(q)^2}{f(r^2)+f(s^2)} = \frac{p^2+q^2}{r^2+s^2}$$

for all $p,q,r,s>0$ with $pq=rs$.

Solution. Let f satisfy the given condition. Setting $p=q=r=s=1$ yields $f(1)^2=f(1)$ and hence $f(1)=1$. Now take any $x>0$ and set $p=x$, $q=1$, $r=s=\sqrt{x}$ to obtain

$$\frac{f(x)^2+1}{2f(x)} = \frac{x^2+1}{2x}\,.$$

This recasts into

$$\begin{gathered} xf(x)^2+x = x^2f(x)+f(x), \\ \big(xf(x)-1\big)\big(f(x)-x\big)=0. \end{gathered}$$

And thus,

$$\text{for every } \ x>0, \quad \text{either } \ f(x)=x \ \text{ or } \ f(x)=\frac{1}{x}\,. \tag{1}$$

Obviously, if

$$f(x)=x \quad \text{for all } x>0 \qquad \text{or} \qquad f(x)=\frac{1}{x} \quad \text{for all } x>0 \tag{2}$$

then the condition of the problem is satisfied. We show that actually these two functions are the only solutions.

So let us assume that there exists a function f satisfying the requirement, other than those in (2). Then $f(a)\neq a$ and $f(b)\neq 1/b$ for some $a,b>0$. By (1), these values must be $f(a)=1/a$, $f(b)=b$. Applying now the equation with $p=a$, $q=b$, $r=s=\sqrt{ab}$ we obtain $(a^{-2}+b^2)/2f(ab)=(a^2+b^2)/2ab$; equivalently,

$$f(ab)=\frac{ab(a^{-2}+b^2)}{a^2+b^2}\,. \tag{3}$$

We know however (see (1)) that $f(ab)$ must be either ab or $1/ab$. If $f(ab)=ab$ then by (3) $a^{-2}+b^2=a^2+b^2$, so that $a=1$. But, as $f(1)=1$, this contradicts the relation $f(a)\neq a$. Likewise, if $f(ab)=1/ab$ then (3) gives $a^2b^2(a^{-2}+b^2)=a^2+b^2$, whence $b=1$, in contradiction to $f(b)\neq 1/b$. Thus indeed the functions listed in (2) are the only two solutions.

Comment. The equation has as many as four variables with only one constraint $pq = rs$, leaving three degrees of freedom and providing a lot of information. Various substitutions force various useful properties of the function searched. We sketch one more method to reach conclusion (1); certainly there are many others.

Noticing that $f(1) = 1$ and setting, first, $p = q = 1$, $r = \sqrt{x}$, $s = 1/\sqrt{x}$, and then $p = x$, $q = 1/x$, $r = s = 1$, we obtain two relations, holding for every $x > 0$,

$$f(x) + f\left(\frac{1}{x}\right) = x + \frac{1}{x} \qquad \text{and} \qquad f(x)^2 + f\left(\frac{1}{x}\right)^2 = x^2 + \frac{1}{x^2}\,. \tag{4}$$

Squaring the first and subtracting the second gives $2f(x)f(1/x) = 2$. Subtracting this from the second relation of (4) leads to

$$\left(f(x) - f\left(\frac{1}{x}\right)\right)^2 = \left(x - \frac{1}{x}\right)^2 \qquad \text{or} \qquad f(x) - f\left(\frac{1}{x}\right) = \pm\left(x - \frac{1}{x}\right).$$

The last two alternatives combined with the first equation of (4) imply the two alternatives of (1).

A2. (a) Prove the inequality

$$\frac{x^2}{(x-1)^2}+\frac{y^2}{(y-1)^2}+\frac{z^2}{(z-1)^2}\geq 1$$

for real numbers $x, y, z \neq 1$ satisfying the condition $xyz=1$.

(b) Show that there are infinitely many triples of rational numbers x, y, z for which this inequality turns into equality.

Solution 1. (a) We start with the substitution

$$\frac{x}{x-1}=a, \qquad \frac{y}{y-1}=b, \qquad \frac{z}{z-1}=c, \qquad \text{i.e.,} \qquad x=\frac{a}{a-1}, \qquad y=\frac{b}{b-1}, \qquad z=\frac{c}{c-1}.$$

The inequality to be proved reads $a^2+b^2+c^2 \geq 1$. The new variables are subject to the constraints $a, b, c \neq 1$ and the following one coming from the condition $xyz=1$,

$$(a-1)(b-1)(c-1)=abc.$$

This is successively equivalent to

$$\begin{aligned} a+b+c-1 &= ab+bc+ca, \\ 2(a+b+c-1) &= (a+b+c)^2-(a^2+b^2+c^2), \\ a^2+b^2+c^2-2 &= (a+b+c)^2-2(a+b+c), \\ a^2+b^2+c^2-1 &= (a+b+c-1)^2. \end{aligned}$$

Thus indeed $a^2+b^2+c^2 \geq 1$, as desired.

(b) From the equation $a^2+b^2+c^2-1=(a+b+c-1)^2$ we see that the proposed inequality becomes an equality if and only if both sums $a^2+b^2+c^2$ and $a+b+c$ have value 1. The first of them is equal to $(a+b+c)^2-2(ab+bc+ca)$. So the instances of equality are described by the system of two equations

$$a+b+c=1, \qquad ab+bc+ca=0$$

plus the constraint $a, b, c \neq 1$. Elimination of c leads to $a^2+ab+b^2=a+b$, which we regard as a quadratic equation in b,

$$b^2+(a-1)b+a(a-1)=0,$$

with discriminant

$$\Delta=(a-1)^2-4a(a-1)=(1-a)(1+3a).$$

We are looking for rational triples (a, b, c); it will suffice to have a rational such that $1-a$ and $1+3a$ are both squares of rational numbers (then Δ will be so too). Set $a=k/m$. We want $m-k$ and $m+3k$ to be squares of integers. This is achieved for instance by taking $m=k^2-k+1$ (clearly nonzero); then $m-k=(k-1)^2$, $m+3k=(k+1)^2$. Note that distinct integers k yield distinct values of $a=k/m$.

And thus, if k is any integer and $m=k^2-k+1$, $a=k/m$ then $\Delta=(k^2-1)^2/m^2$ and the quadratic equation has rational roots $b=(m-k \pm k^2 \mp 1)/(2m)$. Choose e.g. the larger root,

$$b=\frac{m-k+k^2-1}{2m}=\frac{m+(m-2)}{2m}=\frac{m-1}{m}.$$

Computing c from $a+b+c=1$ then gives $c=(1-k)/m$. The condition $a,b,c\neq 1$ eliminates only $k=0$ and $k=1$. Thus, as k varies over integers greater than 1, we obtain an infinite family of rational triples (a,b,c)—and coming back to the original variables ($x=a/(a-1)$ etc.)—an infinite family of rational triples (x,y,z) with the needed property. (A short calculation shows that the resulting triples are $x=-k/(k-1)^2$, $y=k-k^2$, $z=(k-1)/k^2$; but the proof was complete without listing them.)

Comment 1. There are many possible variations in handling the equation system $a^2+b^2+c^2=1$, $a+b+c=1$ $(a,b,c\neq 1)$ which of course describes a circle in the (a,b,c)-space (with three points excluded), and finding infinitely many rational points on it.

Also the initial substitution $x=a/(a-1)$ (etc.) can be successfully replaced by other similar substitutions, e.g. $x=1-1/\alpha$ (etc.); or $x=x'-1$ (etc.); or $1-yz=u$ (etc.)—eventually reducing the inequality to $(\cdots)^2\geq 0$, the expression in the parentheses depending on the actual substitution.

Depending on the method chosen, one arrives at various sequences of rational triples (x,y,z) as needed; let us produce just one more such example: $x=(2r-2)/(r+1)^2$, $y=(2r+2)/(r-1)^2$, $z=(r^2-1)/4$ where r can be any rational number different from 1 or -1.

Solution 2 (an outline)**.** (a) Without changing variables, just setting $z=1/xy$ and clearing fractions, the proposed inequality takes the form

$$(xy-1)^2\big(x^2(y-1)^2+y^2(x-1)^2\big)+(x-1)^2(y-1)^2\geq (x-1)^2(y-1)^2(xy-1)^2.$$

With the notation $p=x+y$, $q=xy$ this becomes, after lengthy routine manipulation and a lot of cancellation

$$q^4-6q^3+2pq^2+9q^2-6pq+p^2\geq 0.$$

It is not hard to notice that the expression on the left is just $(q^2-3q+p)^2$, hence nonnegative.

(Without introducing p and q, one is of course led with some more work to the same expression, just written in terms of x and y; but then it is not that easy to see that it is a square.)

(b) To have equality, one needs $q^2-3q+p=0$. Note that x and y are the roots of the quadratic trinomial (in a formal variable t): t^2-pt+q. When $q^2-3q+p=0$, the discriminant equals

$$\delta=p^2-4q=(3q-q^2)^2-4q=q(q-1)^2(q-4).$$

Now it suffices to have both q and $q-4$ squares of rational numbers (then $p=3q-q^2$ and $\sqrt{\delta}$ are also rational, and so are the roots of the trinomial). On setting $q=(n/m)^2=4+(l/m)^2$ the requirement becomes $4m^2+l^2=n^2$ (with l,m,n being integers). This is just the Pythagorean equation, known to have infinitely many integer solutions.

Comment 2. Part (a) alone might also be considered as a possible contest problem (in the category of easy problems).

A3. Let $S \subseteq \mathbb{R}$ be a set of real numbers. We say that a pair (f, g) of functions from S into S is a *Spanish Couple* on S, if they satisfy the following conditions:

(i) Both functions are strictly increasing, i.e. $f(x) < f(y)$ and $g(x) < g(y)$ for all $x, y \in S$ with $x < y$;

(ii) The inequality $f(g(g(x))) < g(f(x))$ holds for all $x \in S$.

Decide whether there exists a Spanish Couple

(a) on the set $S = \mathbb{N}$ of positive integers;

(b) on the set $S = \{a - 1/b : \ a, b \in \mathbb{N}\}$.

Solution. We show that the answer is NO for part (a), and YES for part (b).

(a) Throughout the solution, we will use the notation $g_k(x) = \overbrace{g(g(\ldots g}^{k}(x)\ldots))$, including $g_0(x) = x$ as well.

Suppose that there exists a Spanish Couple (f, g) on the set $\mathbb{N}$. From property (i) we have $f(x) \geq x$ and $g(x) \geq x$ for all $x \in \mathbb{N}$.

We claim that $g_k(x) \leq f(x)$ for all $k \geq 0$ and all positive integers x. The proof is done by induction on k. We already have the base case $k = 0$ since $x \leq f(x)$. For the induction step from k to $k + 1$, apply the induction hypothesis on $g_2(x)$ instead of x, then apply (ii):

$$g(g_{k+1}(x)) = g_k\big(g_2(x)\big) \leq f\big(g_2(x)\big) < g(f(x)).$$

Since g is increasing, it follows that $g_{k+1}(x) < f(x)$. The claim is proven.

If $g(x) = x$ for all $x \in \mathbb{N}$ then $f(g(g(x))) = f(x) = g(f(x))$, and we have a contradiction with (ii). Therefore one can choose an $x_0 \in S$ for which $x_0 < g(x_0)$. Now consider the sequence $x_0, x_1, \ldots$ where $x_k = g_k(x_0)$. The sequence is increasing. Indeed, we have $x_0 < g(x_0) = x_1$, and $x_k < x_{k+1}$ implies $x_{k+1} = g(x_k) < g(x_{k+1}) = x_{k+2}$.

Hence, we obtain a strictly increasing sequence $x_0 < x_1 < \ldots$ of positive integers which on the other hand has an upper bound, namely $f(x_0)$. This cannot happen in the set $\mathbb{N}$ of positive integers, thus no Spanish Couple exists on $\mathbb{N}$.

(b) We present a Spanish Couple on the set $S = \{a - 1/b : \ a, b \in \mathbb{N}\}$.

Let

$$\begin{aligned} f(a - 1/b) &= a + 1 - 1/b, \\ g(a - 1/b) &= a - 1/(b + 3^a). \end{aligned}$$

These functions are clearly increasing. Condition (ii) holds, since

$$f(g(g(a - 1/b))) = (a + 1) - 1/(b + 2 \cdot 3^a) < (a + 1) - 1/(b + 3^{a+1}) = g(f(a - 1/b)).$$

Comment. Another example of a Spanish couple is $f(a - 1/b) = 3a - 1/b$, $g(a - 1/b) = a - 1/(a+b)$. More generally, postulating $f(a - 1/b) = h(a) - 1/b$, $g(a - 1/b) = a - 1/G(a, b)$ with h increasing and G increasing in both variables, we get that $f \circ g \circ g < g \circ f$ holds if $G\big(a, G(a, b)\big) < G\big(h(a), b\big)$. A search just among linear functions $h(a) = Ca$, $G(a, b) = Aa + Bb$ results in finding that any integers $A > 0$, $C > 2$ and $B = 1$ produce a Spanish couple (in the example above, $A = 1$, $C = 3$). The proposer's example results from taking $h(a) = a + 1$, $G(a, b) = 3^a + b$.

A4. For an integer m, denote by $t(m)$ the unique number in $\{1, 2, 3\}$ such that $m + t(m)$ is a multiple of 3. A function $f : \mathbb{Z} \to \mathbb{Z}$ satisfies $f(-1) = 0$, $f(0) = 1$, $f(1) = -1$ and

$$f(2^n + m) = f(2^n - t(m)) - f(m) \quad \text{for all integers } m, n \geq 0 \text{ with } 2^n > m.$$

Prove that $f(3p) \geq 0$ holds for all integers $p \geq 0$.

Solution. The given conditions determine f uniquely on the positive integers. The signs of $f(1), f(2), \ldots$ seem to change quite erratically. However values of the form $f(2^n - t(m))$ are sufficient to compute directly any functional value. Indeed, let $n > 0$ have base 2 representation $n = 2^{a_0} + 2^{a_1} + \cdots + 2^{a_k}$, $a_0 > a_1 > \cdots > a_k \geq 0$, and let $n_j = 2^{a_j} + 2^{a_{j-1}} + \cdots + 2^{a_k}$, $j = 0, \ldots, k$. Repeated applications of the recurrence show that $f(n)$ is an alternating sum of the quantities $f(2^{a_j} - t(n_{j+1}))$ plus $(-1)^{k+1}$. (The exact formula is not needed for our proof.)

So we focus attention on the values $f(2^n - 1)$, $f(2^n - 2)$ and $f(2^n - 3)$. Six cases arise; more specifically,

$$t(2^{2k}-3) = 2,\ t(2^{2k}-2) = 1,\ t(2^{2k}-1) = 3,\ t(2^{2k+1}-3) = 1,\ t(2^{2k+1}-2) = 3,\ t(2^{2k+1}-1) = 2.$$

Claim. For all integers $k \geq 0$ the following equalities hold:

$$\begin{array}{lll} f(2^{2k+1} - 3) = 0, & f(2^{2k+1} - 2) = 3^k, & f(2^{2k+1} - 1) = -3^k, \\ f(2^{2k+2} - 3) = -3^k, & f(2^{2k+2} - 2) = -3^k, & f(2^{2k+2} - 1) = 2 \cdot 3^k. \end{array}$$

Proof. By induction on k. The base $k = 0$ comes down to checking that $f(2) = -1$ and $f(3) = 2$; the given values $f(-1) = 0$, $f(0) = 1$, $f(1) = -1$ are also needed. Suppose the claim holds for $k - 1$. For $f(2^{2k+1} - t(m))$, the recurrence formula and the induction hypothesis yield

$$\begin{aligned} f(2^{2k+1} - 3) &= f(2^{2k} + (2^{2k} - 3)) = f(2^{2k} - 2) - f(2^{2k} - 3) = -3^{k-1} + 3^{k-1} = 0, \\ f(2^{2k+1} - 2) &= f(2^{2k} + (2^{2k} - 2)) = f(2^{2k} - 1) - f(2^{2k} - 2) = 2 \cdot 3^{k-1} + 3^{k-1} = 3^k, \\ f(2^{2k+1} - 1) &= f(2^{2k} + (2^{2k} - 1)) = f(2^{2k} - 3) - f(2^{2k} - 1) = -3^{k-1} - 2 \cdot 3^{k-1} = -3^k. \end{aligned}$$

For $f(2^{2k+2} - t(m))$ we use the three equalities just established:

$$\begin{aligned} f(2^{2k+2} - 3) &= f(2^{2k+1} + (2^{2k+1} - 3)) = f(2^{2k+1} - 1) - f(2^{2k+1} - 3) = -3^k - 0 = -3^k, \\ f(2^{2k+2} - 2) &= f(2^{2k+1} + (2^{2k+1} - 2)) = f(2^{2k+1} - 3) - f(2^{2k} - 2) = 0 - 3^k = -3^k, \\ f(2^{2k+2} - 1) &= f(2^{2k+1} + (2^{2k+1} - 1)) = f(2^{2k+1} - 2) - f(2^{2k+1} - 1) = 3^k + 3^k = 2 \cdot 3^k. \end{aligned}$$

The claim follows.

A closer look at the six cases shows that $f(2^n - t(m)) \geq 3^{(n-1)/2}$ if $2^n - t(m)$ is divisible by 3, and $f(2^n - t(m)) \leq 0$ otherwise. On the other hand, note that $2^n - t(m)$ is divisible by 3 if and only if $2^n + m$ is. Therefore, for all nonnegative integers m and n,

(i) $f(2^n - t(m)) \geq 3^{(n-1)/2}$ if $2^n + m$ is divisible by 3;

(ii) $f(2^n - t(m)) \leq 0$ if $2^n + m$ is not divisible by 3.

One more (direct) consequence of the claim is that $|f(2^n - t(m))| \leq \frac{2}{3} \cdot 3^{n/2}$ for all $m, n \geq 0$.

The last inequality enables us to find an upper bound for $|f(m)|$ for m less than a given power of 2. We prove by induction on n that $|f(m)| \leq 3^{n/2}$ holds true for all integers $m, n \geq 0$ with $2^n > m$.

The base $n = 0$ is clear as $f(0) = 1$. For the inductive step from n to $n+1$, let m and n satisfy $2^{n+1} > m$. If $m < 2^n$, we are done by the inductive hypothesis. If $m \geq 2^n$ then $m = 2^n + k$ where $2^n > k \geq 0$. Now, by $|f(2^n - t(k))| \leq \frac{2}{3} \cdot 3^{n/2}$ and the inductive assumption,

$$|f(m)| = |f(2^n - t(k)) - f(k)| \leq |f(2^n - t(k))| + |f(k)| \leq \frac{2}{3} \cdot 3^{n/2} + 3^{n/2} < 3^{(n+1)/2}.$$

The induction is complete.

We proceed to prove that $f(3p) \geq 0$ for all integers $p \geq 0$. Since $3p$ is not a power of 2, its binary expansion contains at least two summands. Hence one can write $3p = 2^a + 2^b + c$ where $a > b$ and $2^b > c \geq 0$. Applying the recurrence formula twice yields

$$f(3p) = f(2^a + 2^b + c) = f(2^a - t(2^b + c)) - f(2^b - t(c)) + f(c).$$

Since $2^a + 2^b + c$ is divisible by 3, we have $f(2^a - t(2^b + c)) \geq 3^{(a-1)/2}$ by (i). Since $2^b + c$ is not divisible by 3, we have $f(2^b - t(c)) \leq 0$ by (ii). Finally $|f(c)| \leq 3^{b/2}$ as $2^b > c \geq 0$, so that $f(c) \geq -3^{b/2}$. Therefore $f(3p) \geq 3^{(a-1)/2} - 3^{b/2}$ which is nonnegative because $a > b$.

A5. Let a, b, c, d be positive real numbers such that

$$abcd = 1 \quad \text{and} \quad a+b+c+d > \frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}.$$

Prove that

$$a+b+c+d < \frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}.$$

Solution. We show that if $abcd = 1$, the sum $a+b+c+d$ cannot exceed a certain weighted mean of the expressions $\frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}$ and $\frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}$.

By applying the AM-GM inequality to the numbers $\frac{a}{b}$, $\frac{a}{b}$, $\frac{b}{c}$ and $\frac{a}{d}$, we obtain

$$a = \sqrt[4]{\frac{a^4}{abcd}} = \sqrt[4]{\frac{a}{b}\cdot\frac{a}{b}\cdot\frac{b}{c}\cdot\frac{a}{d}} \le \frac{1}{4}\left(\frac{a}{b}+\frac{a}{b}+\frac{b}{c}+\frac{a}{d}\right).$$

Analogously,

$$b \le \frac{1}{4}\left(\frac{b}{c}+\frac{b}{c}+\frac{c}{d}+\frac{b}{a}\right), \quad c \le \frac{1}{4}\left(\frac{c}{d}+\frac{c}{d}+\frac{d}{a}+\frac{c}{b}\right) \quad \text{and} \quad d \le \frac{1}{4}\left(\frac{d}{a}+\frac{d}{a}+\frac{a}{b}+\frac{d}{c}\right).$$

Summing up these estimates yields

$$a+b+c+d \le \frac{3}{4}\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}\right)+\frac{1}{4}\left(\frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}\right).$$

In particular, if $a+b+c+d > \frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}$ then $a+b+c+d < \frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}$.

Comment. The estimate in the above solution was obtained by applying the AM-GM inequality to each column of the 4×4 array

$$\begin{array}{cccc} a/b & b/c & c/d & d/a \\ a/b & b/c & c/d & d/a \\ b/c & c/d & d/a & a/b \\ a/d & b/a & c/b & d/c \end{array}$$

and adding up the resulting inequalities. The same table yields a stronger bound: If $a, b, c, d > 0$ and $abcd = 1$ then

$$\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}\right)^3\left(\frac{b}{a}+\frac{c}{b}+\frac{d}{c}+\frac{a}{d}\right) \ge (a+b+c+d)^4.$$

It suffices to apply Hölder's inequality to the sequences in the four rows, with weights $1/4$:

$$\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}\right)^{1/4}\left(\frac{a}{b}+\frac{b}{c}+\frac{c}{d}+\frac{d}{a}\right)^{1/4}\left(\frac{b}{c}+\frac{c}{d}+\frac{d}{a}+\frac{a}{b}\right)^{1/4}\left(\frac{a}{d}+\frac{b}{a}+\frac{c}{b}+\frac{d}{c}\right)^{1/4}$$
$$\ge \left(\frac{aaba}{bbcd}\right)^{1/4}+\left(\frac{bbcb}{ccda}\right)^{1/4}+\left(\frac{ccdc}{ddab}\right)^{1/4}+\left(\frac{ddad}{aabc}\right)^{1/4} = a+b+c+d.$$

A6. Let $f\colon \mathbb{R} \to \mathbb{N}$ be a function which satisfies

$$f\left(x+\frac{1}{f(y)}\right)=f\left(y+\frac{1}{f(x)}\right) \qquad \text{for all } x,y\in\mathbb{R}. \tag{1}$$

Prove that there is a positive integer which is not a value of f.

Solution. Suppose that the statement is false and $f(\mathbb{R})=\mathbb{N}$. We prove several properties of the function f in order to reach a contradiction.

To start with, observe that one can assume $f(0)=1$. Indeed, let $a\in\mathbb{R}$ be such that $f(a)=1$, and consider the function $g(x)=f(x+a)$. By substituting $x+a$ and $y+a$ for x and y in (1), we have

$$g\left(x+\frac{1}{g(y)}\right)=f\left(x+a+\frac{1}{f(y+a)}\right)=f\left(y+a+\frac{1}{f(x+a)}\right)=g\left(y+\frac{1}{g(x)}\right).$$

So g satisfies the functional equation (1), with the additional property $g(0)=1$. Also, g and f have the same set of values: $g(\mathbb{R})=f(\mathbb{R})=\mathbb{N}$. Henceforth we assume $f(0)=1$.

Claim 1. For an arbitrary fixed $c\in\mathbb{R}$ we have $\left\{f\left(c+\frac{1}{n}\right) : n\in\mathbb{N}\right\}=\mathbb{N}$.

Proof. Equation (1) and $f(\mathbb{R})=\mathbb{N}$ imply

$$f(\mathbb{R})=\left\{f\left(x+\frac{1}{f(c)}\right) : x\in\mathbb{R}\right\}=\left\{f\left(c+\frac{1}{f(x)}\right) : x\in\mathbb{R}\right\}\subset\left\{f\left(c+\frac{1}{n}\right) : n\in\mathbb{N}\right\}\subset f(\mathbb{R}).$$

The claim follows.

We will use Claim 1 in the special cases $c=0$ and $c=1/3$:

$$\left\{f\left(\frac{1}{n}\right) : n\in\mathbb{N}\right\}=\left\{f\left(\frac{1}{3}+\frac{1}{n}\right) : n\in\mathbb{N}\right\}=\mathbb{N}. \tag{2}$$

Claim 2. If $f(u)=f(v)$ for some $u,v\in\mathbb{R}$ then $f(u+q)=f(v+q)$ for all nonnegative rational q. Furthermore, if $f(q)=1$ for some nonnegative rational q then $f(kq)=1$ for all $k\in\mathbb{N}$.

Proof. For all $x\in\mathbb{R}$ we have by (1)

$$f\left(u+\frac{1}{f(x)}\right)=f\left(x+\frac{1}{f(u)}\right)=f\left(x+\frac{1}{f(v)}\right)=f\left(v+\frac{1}{f(x)}\right).$$

Since $f(x)$ attains all positive integer values, this yields $f(u+1/n)=f(v+1/n)$ for all $n\in\mathbb{N}$. Let $q=k/n$ be a positive rational number. Then k repetitions of the last step yield

$$f(u+q)=f\left(u+\frac{k}{n}\right)=f\left(v+\frac{k}{n}\right)=f(v+q).$$

Now let $f(q)=1$ for some nonnegative rational q, and let $k\in\mathbb{N}$. As $f(0)=1$, the previous conclusion yields successively $f(q)=f(2q), f(2q)=f(3q),\ldots, f\left((k-1)q\right)=f(kq)$, as needed.

Claim 3. The equality $f(q)=f(q+1)$ holds for all nonnegative rational q.

Proof. Let m be a positive integer such that $f(1/m)=1$. Such an m exists by (2). Applying the second statement of Claim 2 with $q=1/m$ and $k=m$ yields $f(1)=1$.

Given that $f(0)=f(1)=1$, the first statement of Claim 2 implies $f(q)=f(q+1)$ for all nonnegative rational q.

Claim 4. The equality $f\left(\frac{1}{n}\right) = n$ holds for every $n \in \mathbb{N}$.

Proof. For a nonnegative rational q we set $x = q$, $y = 0$ in (1) and use Claim 3 to obtain

$$f\left(\frac{1}{f(q)}\right) = f\left(q + \frac{1}{f(0)}\right) = f(q+1) = f(q).$$

By (2), for each $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that $f(1/k) = n$. Applying the last equation with $q = 1/k$, we have

$$n = f\left(\frac{1}{k}\right) = f\left(\frac{1}{f(1/k)}\right) = f\left(\frac{1}{n}\right).$$

Now we are ready to obtain a contradiction. Let $n \in \mathbb{N}$ be such that $f(1/3 + 1/n) = 1$. Such an n exists by (2). Let $1/3 + 1/n = s/t$, where $s, t \in \mathbb{N}$ are coprime. Observe that $t > 1$ as $1/3 + 1/n$ is not an integer. Choose $k, l \in \mathbb{N}$ so that that $ks - lt = 1$.

Because $f(0) = f(s/t) = 1$, Claim 2 implies $f(ks/t) = 1$. Now $f(ks/t) = f(1/t + l)$; on the other hand $f(1/t + l) = f(1/t)$ by l successive applications of Claim 3. Finally, $f(1/t) = t$ by Claim 4, leading to the impossible $t = 1$. The solution is complete.

A7. Prove that for any four positive real numbers a, b, c, d the inequality

$$\frac{(a-b)(a-c)}{a+b+c}+\frac{(b-c)(b-d)}{b+c+d}+\frac{(c-d)(c-a)}{c+d+a}+\frac{(d-a)(d-b)}{d+a+b} \geq 0$$

holds. Determine all cases of equality.

Solution 1. Denote the four terms by

$$A=\frac{(a-b)(a-c)}{a+b+c}, \quad B=\frac{(b-c)(b-d)}{b+c+d}, \quad C=\frac{(c-d)(c-a)}{c+d+a}, \quad D=\frac{(d-a)(d-b)}{d+a+b}.$$

The expression $2A$ splits into two summands as follows,

$$2A = A' + A'' \qquad \text{where} \qquad A'=\frac{(a-c)^2}{a+b+c}, \qquad A''=\frac{(a-c)(a-2b+c)}{a+b+c};$$

this is easily verified. We analogously represent $2B = B' + B''$, $2C = C' + C''$, $2B = D' + D''$ and examine each of the sums $A' + B' + C' + D'$ and $A'' + B'' + C'' + D''$ separately.

Write $s = a + b + c + d$; the denominators become $s - d$, $s - a$, $s - b$, $s - c$. By the Cauchy-Schwarz inequality,

$$\begin{aligned}&\left(\frac{|a-c|}{\sqrt{s-d}}\cdot\sqrt{s-d}+\frac{|b-d|}{\sqrt{s-a}}\cdot\sqrt{s-a}+\frac{|c-a|}{\sqrt{s-b}}\cdot\sqrt{s-b}+\frac{|d-b|}{\sqrt{s-c}}\cdot\sqrt{s-c}\right)^2\\ &\qquad\leq\left(\frac{(a-c)^2}{s-d}+\frac{(b-d)^2}{s-a}+\frac{(c-a)^2}{s-b}+\frac{(d-b)^2}{s-c}\right)\big(4s-s\big)=3s\big(A'+B'+C'+D'\big).\end{aligned}$$

Hence

$$A'+B'+C'+D' \geq \frac{\big(2|a-c|+2|b-d|\big)^2}{3s} \geq \frac{16\cdot|a-c|\cdot|b-d|}{3s}. \tag{1}$$

Next we estimate the absolute value of the other sum. We couple A'' with C'' to obtain

$$\begin{aligned}A''+C'' &= \frac{(a-c)(a+c-2b)}{s-d}+\frac{(c-a)(c+a-2d)}{s-b}\\ &= \frac{(a-c)(a+c-2b)(s-b)+(c-a)(c+a-2d)(s-d)}{(s-d)(s-b)}\\ &= \frac{(a-c)\big(-2b(s-b)-b(a+c)+2d(s-d)+d(a+c)\big)}{s(a+c)+bd}\\ &= \frac{3(a-c)(d-b)(a+c)}{M}, \qquad \text{with} \qquad M=s(a+c)+bd.\end{aligned}$$

Hence by cyclic shift

$$B''+D''=\frac{3(b-d)(a-c)(b+d)}{N}, \qquad \text{with} \qquad N=s(b+d)+ca.$$

Thus

$$A''+B''+C''+D''=3(a-c)(b-d)\left(\frac{b+d}{N}-\frac{a+c}{M}\right)=\frac{3(a-c)(b-d)W}{MN} \tag{2}$$

where

$$W=(b+d)M-(a+c)N=bd(b+d)-ac(a+c). \tag{3}$$

Note that

$$MN > \big(ac(a+c) + bd(b+d)\big)s \geq |W| \cdot s. \tag{4}$$

Now (2) and (4) yield

$$|A'' + B'' + C'' + D''| \leq \frac{3 \cdot |a-c| \cdot |b-d|}{s}. \tag{5}$$

Combined with (1) this results in

$$\begin{aligned} 2(A+B+C+D) &= (A'+B'+C'+D') + (A''+B''+C''+D'') \\ &\geq \frac{16 \cdot |a-c| \cdot |b-d|}{3s} - \frac{3 \cdot |a-c| \cdot |b-d|}{s} = \frac{7 \cdot |a-c| \cdot |b-d|}{3(a+b+c+d)} \geq 0. \end{aligned}$$

This is the required inequality. From the last line we see that equality can be achieved only if either $a = c$ or $b = d$. Since we also need equality in (1), this implies that actually $a = c$ and $b = d$ must hold simultaneously, which is obviously also a sufficient condition.

Solution 2. We keep the notations A, B, C, D, s, and also M, N, W from the preceding solution; the definitions of M, N, W and relations (3), (4) in that solution did not depend on the foregoing considerations. Starting from

$$2A = \frac{(a-c)^2 + 3(a+c)(a-c)}{a+b+c} - 2a + 2c,$$

we get

$$\begin{aligned} 2(A+C) &= (a-c)^2\left(\frac{1}{s-d} + \frac{1}{s-b}\right) + 3(a+c)(a-c)\left(\frac{1}{s-d} - \frac{1}{s-b}\right) \\ &= (a-c)^2\,\frac{2s-b-d}{M} + 3(a+c)(a-c) \cdot \frac{d-b}{M} = \frac{p(a-c)^2 - 3(a+c)(a-c)(b-d)}{M} \end{aligned}$$

where $p = 2s - b - d = s + a + c$. Similarly, writing $q = s + b + d$ we have

$$2(B+D) = \frac{q(b-d)^2 - 3(b+d)(b-d)(c-a)}{N};$$

specific grouping of terms in the numerators has its aim. Note that $pq > 2s^2$. By adding the fractions expressing $2(A+C)$ and $2(B+D)$,

$$2(A+B+C+D) = \frac{p(a-c)^2}{M} + \frac{3(a-c)(b-d)W}{MN} + \frac{q(b-d)^2}{N}$$

with W defined by (3).

Substitution $x = (a-c)/M$, $y = (b-d)/N$ brings the required inequality to the form

$$2(A+B+C+D) = Mpx^2 + 3Wxy + Nqy^2 \geq 0. \tag{6}$$

It will be enough to verify that the discriminant $\Delta = 9W^2 - 4MNpq$ of the quadratic trinomial $Mpt^2 + 3Wt + Nq$ is negative; on setting $t = x/y$ one then gets (6). The first inequality in (4) together with $pq > 2s^2$ imply $4MNpq > 8s^3\big(ac(a+c) + bd(b+d)\big)$. Since

$$(a+c)s^3 > (a+c)^4 \geq 4ac(a+c)^2 \quad \text{and likewise} \quad (b+d)s^3 > 4bd(b+d)^2,$$

the estimate continues as follows,

$$4MNpq > 8\big(4(ac)^2(a+c)^2 + 4(bd)^2(b+d)^2\big) > 32\big(bd(b+d) - ac(a+c)\big)^2 = 32W^2 \geq 9W^2.$$

Thus indeed $\Delta < 0$. The desired inequality (6) hence results. It becomes an equality if and only if $x = y = 0$; equivalently, if and only if $a = c$ and simultaneously $b = d$.

Comment. The two solutions presented above do not differ significantly; large portions overlap. The properties of the number W turn out to be crucial in both approaches. The Cauchy-Schwarz inequality, applied in the first solution, is avoided in the second, which requires no knowledge beyond quadratic trinomials.

The estimates in the proof of $\Delta < 0$ in the second solution seem to be very wasteful. However, they come close to sharp when the terms in one of the pairs (a, c), (b, d) are equal and much bigger than those in the other pair.

In attempts to prove the inequality by just considering the six cases of arrangement of the numbers a, b, c, d on the real line, one soon discovers that the cases which create real trouble are precisely those in which a and c are both greater or both smaller than b and d.

Solution 3.

$$(a-b)(a-c)(a+b+d)(a+c+d)(b+c+d) =$$
$$= \Big((a-b)(a+b+d)\Big)\Big((a-c)(a+c+d)\Big)(b+c+d) =$$
$$= (a^2+ad-b^2-bd)(a^2+ad-c^2-cd)(b+c+d) =$$
$$= \big(a^4+2a^3d-a^2b^2-a^2bd-a^2c^2-a^2cd+a^2d^2-ab^2d-abd^2-ac^2d-acd^2+b^2c^2+b^2cd+bc^2d+bcd^2\big)(b+c+d) =$$
$$= a^4b+a^4c+a^4d+(b^3c^2+a^2d^3)-a^2c^3+(2a^3d^2-b^3a^2+c^3b^2)+$$
$$+(b^3cd-c^3da-d^3ab)+(2a^3bd+c^3db-d^3ac)+(2a^3cd-b^3da+d^3bc)$$
$$+(-a^2b^2c+3b^2c^2d-2ac^2d^2)+(-2a^2b^2d+2bc^2d^2)+(-a^2bc^2-2a^2c^2d-2ab^2d^2+2b^2cd^2)+$$
$$+(-2a^2bcd-ab^2cd-abc^2d-2abcd^2)$$

Introducing the notation $S_{xyzw} = \sum\limits_{cyc} a^x b^y c^z d^w$, one can write

$$\sum_{cyc}(a-b)(a-c)(a+b+d)(a+c+d)(b+c+d) =$$
$$= S_{4100}+S_{4010}+S_{4001}+2S_{3200}-S_{3020}+2S_{3002}-S_{3110}+2S_{3101}+2S_{3011}-3S_{2120}-6S_{2111} =$$
$$+\left(S_{4100}+S_{4001}+\frac{1}{2}S_{3110}+\frac{1}{2}S_{3011}-3S_{2120}\right)+$$
$$+\left(S_{4010}-S_{3020}-\frac{3}{2}S_{3110}+\frac{3}{2}S_{3011}+\frac{9}{16}S_{2210}+\frac{9}{16}S_{2201}-\frac{9}{8}S_{2111}\right)+$$
$$+\frac{9}{16}\Big(S_{3200}-S_{2210}-S_{2201}+S_{3002}\Big)+\frac{23}{16}\Big(S_{3200}-2S_{3101}+S_{3002}\Big)+\frac{39}{8}\Big(S_{3101}-S_{2111}\Big),$$

where the expressions

$$S_{4100}+S_{4001}+\frac{1}{2}S_{3110}+\frac{1}{2}S_{3011}-3S_{2120} = \sum_{cyc}\left(a^4b+bc^4+\frac{1}{2}a^3bc+\frac{1}{2}abc^3-3a^2bc^2\right),$$

$$S_{4010}-S_{3020}-\frac{3}{2}S_{3110}+\frac{3}{2}S_{3011}+\frac{9}{16}S_{2210}+\frac{9}{16}S_{2201}-\frac{9}{8}S_{2111} = \sum_{cyc}a^2c\left(a-c-\frac{3}{4}b+\frac{3}{4}d\right)^2,$$

$$S_{3200}-S_{2210}-S_{2201}+S_{3002} = \sum_{cyc}b^2(a^3-a^2c-ac^2+c^3) = \sum_{cyc}b^2(a+c)(a-c)^2,$$

$$S_{3200}-2S_{3101}+S_{3002} = \sum_{cyc}a^3(b-d)^2 \qquad \text{and} \qquad S_{3101}-S_{2111} = \frac{1}{3}\sum_{cyc}bd(2a^3+c^3-3a^2c)$$

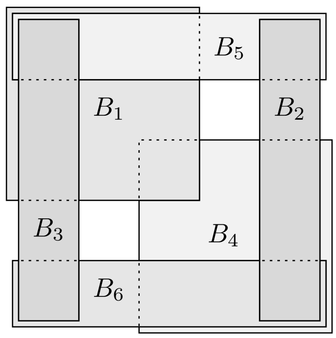
are all nonnegative.

Combinatorics

C1. In the plane we consider rectangles whose sides are parallel to the coordinate axes and have positive length. Such a rectangle will be called a *box*. Two boxes *intersect* if they have a common point in their interior or on their boundary.

Find the largest n for which there exist n boxes $B_1, \ldots, B_n$ such that B_i and B_j intersect if and only if $i \not\equiv j \pm 1 \pmod{n}$.

Solution. The maximum number of such boxes is 6. One example is shown in the figure.



Now we show that 6 is the maximum. Suppose that boxes $B_1, \ldots, B_n$ satisfy the condition. Let the closed intervals I_k and J_k be the projections of B_k onto the x- and y-axis, for $1 \leq k \leq n$.

If B_i and B_j intersect, with a common point (x, y), then $x \in I_i \cap I_j$ and $y \in J_i \cap J_j$. So the intersections $I_i \cap I_j$ and $J_i \cap J_j$ are nonempty. Conversely, if $x \in I_i \cap I_j$ and $y \in J_i \cap J_j$ for some real numbers x, y, then (x, y) is a common point of B_i and B_j. Putting it around, B_i and B_j are disjoint if and only if their projections on at least one coordinate axis are disjoint.

For brevity we call two boxes or intervals adjacent if their indices differ by 1 modulo n, and nonadjacent otherwise.

The adjacent boxes B_k and B_{k+1} do not intersect for each $k = 1, \ldots, n$. Hence (I_k, I_{k+1}) or (J_k, J_{k+1}) is a pair of disjoint intervals, $1 \leq k \leq n$. So there are at least n pairs of disjoint intervals among $(I_1, I_2), \ldots, (I_{n-1}, I_n), (I_n, I_1); (J_1, J_2), \ldots, (J_{n-1}, J_n), (J_n, J_1)$.

Next, every two nonadjacent boxes intersect, hence their projections on both axes intersect, too. Then the claim below shows that at most 3 pairs among $(I_1, I_2), \ldots, (I_{n-1}, I_n), (I_n, I_1)$ are disjoint, and the same holds for $(J_1, J_2), \ldots, (J_{n-1}, J_n), (J_n, J_1)$. Consequently $n \leq 3 + 3 = 6$, as stated. Thus we are left with the claim and its justification.

Claim. Let $\Delta_1, \Delta_2, \ldots, \Delta_n$ be intervals on a straight line such that every two nonadjacent intervals intersect. Then Δ_k and Δ_{k+1} are disjoint for at most three values of $k = 1, \ldots, n$.

Proof. Denote $\Delta_k = [a_k, b_k]$, $1 \leq k \leq n$. Let $\alpha = \max(a_1, \ldots, a_n)$ be the rightmost among the left endpoints of $\Delta_1, \ldots, \Delta_n$, and let $\beta = \min(b_1, \ldots, b_n)$ be the leftmost among their right endpoints. Assume that $\alpha = a_2$ without loss of generality.

If $\alpha \leq \beta$ then $a_i \leq \alpha \leq \beta \leq b_i$ for all i. Every Δ_i contains α, and thus no disjoint pair (Δ_i, Δ_{i+1}) exists.

If $\beta < \alpha$ then $\beta = b_i$ for some i such that $a_i < b_i = \beta < \alpha = a_2 < b_2$, hence Δ_2 and Δ_i are disjoint. Now Δ_2 intersects all remaining intervals except possibly Δ_1 and Δ_3, so Δ_2 and Δ_i can be disjoint only if $i = 1$ or $i = 3$. Suppose by symmetry that $i = 3$; then $\beta = b_3$. Since each of the intervals $\Delta_4, \ldots, \Delta_n$ intersects Δ_2, we have $a_i \leq \alpha \leq b_i$ for $i = 4, \ldots, n$. Therefore $\alpha \in \Delta_4 \cap \ldots \cap \Delta_n$, in particular $\Delta_4 \cap \ldots \cap \Delta_n \neq \emptyset$. Similarly, $\Delta_5, \ldots, \Delta_n, \Delta_1$ all intersect Δ_3, so that $\Delta_5 \cap \ldots \cap \Delta_n \cap \Delta_1 \neq \emptyset$ as $\beta \in \Delta_5 \cap \ldots \cap \Delta_n \cap \Delta_1$. This leaves (Δ_1, Δ_2), (Δ_2, Δ_3) and (Δ_3, Δ_4) as the only candidates for disjoint interval pairs, as desired.

Comment. The problem is a two-dimensional version of the original proposal which is included below. The extreme shortage of easy and appropriate submissions forced the Problem Selection Committee to shortlist a simplified variant. The same one-dimensional Claim is used in both versions.

Original proposal. We consider parallelepipeds in three-dimensional space, with edges parallel to the coordinate axes and of positive length. Such a parallelepiped will be called a *box*. Two boxes *intersect* if they have a common point in their interior or on their boundary.

Find the largest n for which there exist n boxes $B_1, \ldots, B_n$ such that B_i and B_j intersect if and only if $i \not\equiv j \pm 1 \pmod{n}$.

The maximum number of such boxes is 9. Suppose that boxes $B_1, \ldots, B_n$ satisfy the condition. Let the closed intervals I_k, J_k and K_k be the projections of box B_k onto the x-, y- and z-axis, respectively, for $1 \leq k \leq n$. As before, B_i and B_j are disjoint if and only if their projections on at least one coordinate axis are disjoint.

We call again two boxes or intervals adjacent if their indices differ by 1 modulo n, and nonadjacent otherwise.

The adjacent boxes B_i and B_{i+1} do not intersect for each $i = 1, \ldots, n$. Hence at least one of the pairs (I_i, I_{i+1}), (J_i, J_{i+1}) and (K_i, K_{i+1}) is a pair of disjoint intervals. So there are at least n pairs of disjoint intervals among $(I_i, I_{i+1}), (J_i, J_{i+1}), (K_i, K_{i+1})$, $1 \leq i \leq n$.

Next, every two nonadjacent boxes intersect, hence their projections on the three axes intersect, too. Referring to the Claim in the solution of the two-dimensional version, we cocnclude that at most 3 pairs among $(I_1, I_2), \ldots, (I_{n-1}, I_n), (I_n, I_1)$ are disjoint; the same holds for $(J_1, J_2), \ldots, (J_{n-1}, J_n), (J_n, J_1)$ and $(K_1, K_2), \ldots, (K_{n-1}, K_n), (K_n, K_1)$. Consequently $n \leq 3 + 3 + 3 = 9$, as stated.

For $n = 9$, the desired system of boxes exists. Consider the intervals in the following table:

i	I_i	J_i	K_i
1	$[1,4]$	$[1,6]$	$[3,6]$
2	$[5,6]$	$[1,6]$	$[1,6]$
3	$[1,2]$	$[1,6]$	$[1,6]$
4	$[3,6]$	$[1,4]$	$[1,6]$
5	$[1,6]$	$[5,6]$	$[1,6]$
6	$[1,6]$	$[1,2]$	$[1,6]$
7	$[1,6]$	$[3,6]$	$[1,4]$
8	$[1,6]$	$[1,6]$	$[5,6]$
9	$[1,6]$	$[1,6]$	$[1,2]$

We have $I_1 \cap I_2 = I_2 \cap I_3 = I_3 \cap I_4 = \emptyset$, $J_4 \cap J_5 = J_5 \cap J_6 = J_6 \cap J_7 = \emptyset$, and finally $K_7 \cap K_8 = K_8 \cap K_9 = K_9 \cap K_1 = \emptyset$. The intervals in each column intersect in all other cases. It follows that the boxes $B_i = I_i \times J_i \times K_i$, $i = 1, \ldots, 9$, have the stated property.

C2. For every positive integer n determine the number of permutations $(a_1, a_2, \dots, a_n)$ of the set $\{1, 2, \dots, n\}$ with the following property:

$$2(a_1 + a_2 + \cdots + a_k) \quad \text{is divisible by } k \quad \text{for } k = 1, 2, \dots, n.$$

Solution. For each n let F_n be the number of permutations of $\{1, 2, \dots, n\}$ with the required property; call them *nice*. For $n = 1, 2, 3$ every permutation is nice, so $F_1 = 1$, $F_2 = 2$, $F_3 = 6$.

Take an $n > 3$ and consider any nice permutation $(a_1, a_2, \dots, a_n)$ of $\{1, 2, \dots, n\}$. Then $n - 1$ must be a divisor of the number

$$\begin{aligned} 2(a_1 + a_2 + \cdots + a_{n-1}) &= 2\big((1 + 2 + \cdots + n) - a_n\big) \\ &= n(n+1) - 2a_n = (n+2)(n-1) + (2 - 2a_n). \end{aligned}$$

So $2a_n - 2$ must be divisible by $n - 1$, hence equal to 0 or $n - 1$ or $2n - 2$. This means that

$$a_n = 1 \qquad \text{or} \qquad a_n = \frac{n+1}{2} \qquad \text{or} \qquad a_n = n.$$

Suppose that $a_n = (n+1)/2$. Since the permutation is nice, taking $k = n - 2$ we get that $n - 2$ has to be a divisor of

$$\begin{aligned} 2(a_1 + a_2 + \cdots + a_{n-2}) &= 2\big((1 + 2 + \cdots + n) - a_n - a_{n-1}\big) \\ &= n(n+1) - (n+1) - 2a_{n-1} = (n+2)(n-2) + (3 - 2a_{n-1}). \end{aligned}$$

So $2a_{n-1} - 3$ should be divisible by $n - 2$, hence equal to 0 or $n - 2$ or $2n - 4$. Obviously 0 and $2n - 4$ are excluded because $2a_{n-1} - 3$ is odd. The remaining possibility ($2a_{n-1} - 3 = n - 2$) leads to $a_{n-1} = (n+1)/2 = a_n$, which also cannot hold. This eliminates $(n+1)/2$ as a possible value of a_n. Consequently $a_n = 1$ or $a_n = n$.

If $a_n = n$ then $(a_1, a_2, \dots, a_{n-1})$ is a nice permutation of $\{1, 2, \dots, n-1\}$. There are F_{n-1} such permutations. Attaching n to any one of them at the end creates a nice permutation of $\{1, 2, \dots, n\}$.

If $a_n = 1$ then $(a_1-1, a_2-1, \dots, a_{n-1}-1)$ is a permutation of $\{1, 2, \dots, n-1\}$. It is also nice because the number

$$2\big((a_1-1) + \cdots + (a_k-1)\big) = 2(a_1 + \cdots + a_k) - 2k$$

is divisible by k, for any $k \le n - 1$. And again, any one of the F_{n-1} nice permutations $(b_1, b_2, \dots, b_{n-1})$ of $\{1, 2, \dots, n-1\}$ gives rise to a nice permutation of $\{1, 2, \dots, n\}$ whose last term is 1, namely $(b_1+1, b_2+1, \dots, b_{n-1}+1, 1)$.

The bijective correspondences established in both cases show that there are F_{n-1} nice permutations of $\{1, 2, \dots, n\}$ with the last term 1 and also F_{n-1} nice permutations of $\{1, 2, \dots, n\}$ with the last term n. Hence follows the recurrence $F_n = 2F_{n-1}$. With the base value $F_3 = 6$ this gives the outcome formula $F_n = 3 \cdot 2^{n-2}$ for $n \ge 3$.

C3. In the coordinate plane consider the set S of all points with integer coordinates. For a positive integer k, two distinct points $A, B \in S$ will be called *k-friends* if there is a point $C \in S$ such that the area of the triangle ABC is equal to k. A set $T \subset S$ will be called a *k-clique* if every two points in T are k-friends. Find the least positive integer k for which there exists a k-clique with more than 200 elements.

Solution. To begin, let us describe those points $B \in S$ which are k-friends of the point $(0,0)$. By definition, $B = (u,v)$ satisfies this condition if and only if there is a point $C = (x,y) \in S$ such that $\frac{1}{2}|uy - vx| = k$. (This is a well-known formula expressing the area of triangle ABC when A is the origin.)

To say that there exist integers x, y for which $|uy - vx| = 2k$, is equivalent to saying that the greatest common divisor of u and v is also a divisor of $2k$. Summing up, a point $B = (u,v) \in S$ is a k-friend of $(0,0)$ if and only if $\gcd(u,v)$ divides $2k$.

Translation by a vector with integer coordinates does not affect k-friendship; if two points are k-friends, so are their translates. It follows that two points $A, B \in S$, $A = (s,t)$, $B = (u,v)$, are k-friends if and only if the point $(u-s, v-t)$ is a k-friend of $(0,0)$; i.e., if $\gcd(u-s, v-t) | 2k$.

Let n be a positive integer which does not divide $2k$. We claim that a k-clique cannot have more than n^2 elements.

Indeed, all points $(x,y) \in S$ can be divided into n^2 classes determined by the remainders that x and y leave in division by n. If a set T has more than n^2 elements, some two points $A, B \in T$, $A = (s,t)$, $B = (u,v)$, necessarily fall into the same class. This means that $n | u - s$ and $n | v - t$. Hence $n | d$ where $d = \gcd(u-s, v-t)$. And since n does not divide $2k$, also d does not divide $2k$. Thus A and B are not k-friends and the set T is not a k-clique.

Now let $M(k)$ be the *least* positive integer which does not divide $2k$. Write $M(k) = m$ for the moment and consider the set T of all points (x,y) with $0 \le x, y < m$. There are m^2 of them. If $A = (s,t)$, $B = (u,v)$ are two distinct points in T then both differences $|u-s|$, $|v-t|$ are integers less than m and at least one of them is positive. By the definition of m, every positive integer less than m divides $2k$. Therefore $u - s$ (if nonzero) divides $2k$, and the same is true of $v - t$. So $2k$ is divisible by $\gcd(u-s, v-t)$, meaning that A, B are k-friends. Thus T is a k-clique.

It follows that the maximum size of a k-clique is $M(k)^2$, with $M(k)$ defined as above. We are looking for the minimum k such that $M(k)^2 > 200$.

By the definition of $M(k)$, $2k$ is divisible by the numbers $1, 2, \ldots, M(k)-1$, but not by $M(k)$ itself. If $M(k)^2 > 200$ then $M(k) \ge 15$. Trying to hit $M(k) = 15$ we get a contradiction immediately ($2k$ would have to be divisible by 3 and 5, but not by 15).

So let us try $M(k) = 16$. Then $2k$ is divisible by the numbers $1, 2, \ldots, 15$, hence also by their least common multiple L, but not by 16. And since L is not a multiple of 16, we infer that $k = L/2$ is the least k with $M(k) = 16$.

Finally, observe that if $M(k) \ge 17$ then $2k$ must be divisible by the least common multiple of $1, 2, \ldots, 16$, which is equal to $2L$. Then $2k \ge 2L$, yielding $k > L/2$.

In conclusion, the least k with the required property is equal to $L/2 = 180180$.

C4. Let n and k be fixed positive integers of the same parity, $k \geq n$. We are given $2n$ lamps numbered 1 through $2n$; each of them can be *on* or *off*. At the beginning all lamps are *off*. We consider sequences of k steps. At each step one of the lamps is switched (from *off* to *on* or from *on* to *off*).

Let N be the number of k-step sequences ending in the state: lamps $1, \ldots, n$ *on*, lamps $n+1, \ldots, 2n$ *off*.

Let M be the number of k-step sequences leading to the same state and not touching lamps $n+1, \ldots, 2n$ at all.

Find the ratio N/M.

Solution. A sequence of k switches ending in the state as described in the problem statement (lamps $1, \ldots, n$ *on*, lamps $n+1, \ldots, 2n$ *off*) will be called an *admissible process*. If, moreover, the process does not touch the lamps $n+1, \ldots, 2n$, it will be called *restricted*. So there are N admissible processes, among which M are restricted.

In every admissible process, restricted or not, each one of the lamps $1, \ldots, n$ goes from *off* to *on*, so it is switched an odd number of times; and each one of the lamps $n+1, \ldots, 2n$ goes from *off* to *off*, so it is switched an even number of times.

Notice that $M > 0$; i.e., restricted admissible processes do exist (it suffices to switch each one of the lamps $1, \ldots, n$ just once and then choose one of them and switch it $k - n$ times, which by hypothesis is an even number).

Consider any restricted admissible process $\mathbf{p}$. Take any lamp ℓ, $1 \leq \ell \leq n$, and suppose that it was switched k_ℓ times. As noticed, k_ℓ must be odd. Select arbitrarily an even number of these k_ℓ switches and replace each of them by the switch of lamp $n+\ell$. This can be done in $2^{k_\ell - 1}$ ways (because a k_ℓ-element set has $2^{k_\ell - 1}$ subsets of even cardinality). Notice that $k_1 + \cdots + k_n = k$.

These actions are independent, in the sense that the action involving lamp ℓ does not affect the action involving any other lamp. So there are $2^{k_1 - 1} \cdot 2^{k_2 - 1} \cdots 2^{k_n - 1} = 2^{k-n}$ ways of combining these actions. In any of these combinations, each one of the lamps $n+1, \ldots, 2n$ gets switched an even number of times and each one of the lamps $1, \ldots, n$ remains switched an odd number of times, so the final state is the same as that resulting from the original process $\mathbf{p}$.

This shows that every restricted admissible process $\mathbf{p}$ can be modified in 2^{k-n} ways, giving rise to 2^{k-n} distinct admissible processes (with all lamps allowed).

Now we show that every admissible process $\mathbf{q}$ can be achieved in that way. Indeed, it is enough to replace every switch of a lamp with a label $\ell > n$ that occurs in $\mathbf{q}$ by the switch of the corresponding lamp $\ell - n$; in the resulting process $\mathbf{p}$ the lamps $n+1, \ldots, 2n$ are not involved.

Switches of each lamp with a label $\ell > n$ had occurred in $\mathbf{q}$ an even number of times. So the performed replacements have affected each lamp with a label $\ell \leq n$ also an even number of times; hence in the overall effect the final state of each lamp has remained the same. This means that the resulting process $\mathbf{p}$ is admissible—and clearly restricted, as the lamps $n+1, \ldots, 2n$ are not involved in it any more.

If we now take process $\mathbf{p}$ and reverse all these replacements, then we obtain process $\mathbf{q}$. These reversed replacements are nothing else than the modifications described in the foregoing paragraphs.

Thus there is a one–to–(2^{k-n}) correspondence between the M restricted admissible processes and the total of N admissible processes. Therefore $N/M = 2^{k-n}$.

C5. Let $S = \{x_1, x_2, \ldots, x_{k+\ell}\}$ be a $(k+\ell)$-element set of real numbers contained in the interval $[0,1]$; k and ℓ are positive integers. A k-element subset $A \subset S$ is called *nice* if

$$\left| \frac{1}{k} \sum_{x_i \in A} x_i - \frac{1}{\ell} \sum_{x_j \in S \setminus A} x_j \right| \le \frac{k+\ell}{2k\ell}.$$

Prove that the number of nice subsets is at least $\dfrac{2}{k+\ell}\dbinom{k+\ell}{k}$.

Solution. For a k-element subset $A \subset S$, let $f(A) = \dfrac{1}{k} \displaystyle\sum_{x_i \in A} x_i - \dfrac{1}{\ell} \sum_{x_j \in S \setminus A} x_j$. Denote $\dfrac{k+\ell}{2k\ell} = d$. By definition a subset A is nice if $|f(A)| \le d$.

To each permutation $(y_1, y_2, \ldots, y_{k+\ell})$ of the set $S = \{x_1, x_2, \ldots, x_{k+\ell}\}$ we assign $k+\ell$ subsets of S with k elements each, namely $A_i = \{y_i, y_{i+1}, \ldots, y_{i+k-1}\}$, $i = 1, 2, \ldots, k+\ell$. Indices are taken modulo $k+\ell$ here and henceforth. In other words, if $y_1, y_2, \ldots, y_{k+\ell}$ are arranged around a circle in this order, the sets in question are all possible blocks of k consecutive elements.

Claim. At least two nice sets are assigned to every permutation of S.

Proof. Adjacent sets A_i and A_{i+1} differ only by the elements y_i and y_{i+k}, $i = 1, \ldots, k+\ell$. By the definition of f, and because $y_i, y_{i+k} \in [0,1]$,

$$|f(A_{i+1}) - f(A_i)| = \left| \left(\frac{1}{k} + \frac{1}{\ell} \right) (y_{i+k} - y_i) \right| \le \frac{1}{k} + \frac{1}{\ell} = 2d.$$

Each element $y_i \in S$ belongs to exactly k of the sets $A_1, \ldots, A_{k+\ell}$. Hence in k of the expressions $f(A_1), \ldots, f(A_{k+\ell})$ the coefficient of y_i is $1/k$; in the remaining ℓ expressions, its coefficient is $-1/\ell$. So the contribution of y_i to the sum of all $f(A_i)$ equals $k \cdot 1/k - \ell \cdot 1/\ell = 0$. Since this holds for all i, it follows that $f(A_1) + \cdots + f(A_{k+\ell}) = 0$.

If $f(A_p) = \min f(A_i)$, $f(A_q) = \max f(A_i)$, we obtain in particular $f(A_p) \le 0$, $f(A_q) \ge 0$. Let $p < q$ (the case $p > q$ is analogous; and the claim is true for $p = q$ as $f(A_i) = 0$ for all i).

We are ready to prove that at least two of the sets $A_1, \ldots, A_{k+\ell}$ are nice. The interval $[-d, d]$ has length $2d$, and we saw that adjacent numbers in the circular arrangement $f(A_1), \ldots, f(A_{k+\ell})$ differ by at most $2d$. Suppose that $f(A_p) < -d$ and $f(A_q) > d$. Then one of the numbers $f(A_{p+1}), \ldots, f(A_{q-1})$ lies in $[-d, d]$, and also one of the numbers $f(A_{q+1}), \ldots, f(A_{p-1})$ lies there. Consequently, one of the sets $A_{p+1}, \ldots, A_{q-1}$ is nice, as well as one of the sets $A_{q+1}, \ldots, A_{p-1}$. If $-d \le f(A_p)$ and $f(A_q) \le d$ then A_p and A_q are nice.

Let now $f(A_p) < -d$ and $f(A_q) \le d$. Then $f(A_p) + f(A_q) < 0$, and since $\sum f(A_i) = 0$, there is an $r \ne q$ such that $f(A_r) > 0$. We have $0 < f(A_r) \le f(A_q) \le d$, so the sets $f(A_r)$ and $f(A_q)$ are nice. The only case remaining, $-d \le f(A_p)$ and $d < f(A_q)$, is analogous.

Apply the claim to each of the $(k+\ell)!$ permutations of $S = \{x_1, x_2, \ldots, x_{k+\ell}\}$. This gives at least $2(k+\ell)!$ nice sets, counted with repetitions: each nice set is counted as many times as there are permutations to which it is assigned.

On the other hand, each k-element set $A \subset S$ is assigned to exactly $(k+\ell)\, k!\, \ell!$ permutations. Indeed, such a permutation $(y_1, y_2, \ldots, y_{k+\ell})$ is determined by three independent choices: an index $i \in \{1, 2, \ldots, k+\ell\}$ such that $A = \{y_i, y_{i+1}, \ldots, y_{i+k-1}\}$, a permutation $(y_i, y_{i+1}, \ldots, y_{i+k-1})$ of the set A, and a permutation $(y_{i+k}, y_{i+k+1}, \ldots, y_{i-1})$ of the set $S \setminus A$.

In summary, there are at least $\dfrac{2(k+\ell)!}{(k+\ell)\, k!\, \ell!} = \dfrac{2}{k+\ell}\dbinom{k+\ell}{k}$ nice sets.

C6. For $n \geq 2$, let $S_1, S_2, \ldots, S_{2^n}$ be 2^n subsets of $A = \{1, 2, 3, \ldots, 2^{n+1}\}$ that satisfy the following property: There do not exist indices a and b with $a < b$ and elements $x, y, z \in A$ with $x < y < z$ such that $y, z \in S_a$ and $x, z \in S_b$. Prove that at least one of the sets $S_1, S_2, \ldots, S_{2^n}$ contains no more than $4n$ elements.

Solution 1. We prove that there exists a set S_a with at most $3n + 1$ elements.

Given a $k \in \{1, \ldots, n\}$, we say that an element $z \in A$ is *k-good* to a set S_a if $z \in S_a$ and S_a contains two other elements x and y with $x < y < z$ such that $z - y < 2^k$ and $z - x \geq 2^k$. Also, $z \in A$ will be called *good* to S_a if z is k-good to S_a for some $k = 1, \ldots, n$.

We claim that each $z \in A$ can be k-good to at most one set S_a. Indeed, suppose on the contrary that z is k-good simultaneously to S_a and S_b, with $a < b$. Then there exist $y_a \in S_a$, $y_a < z$, and $x_b \in S_b$, $x_b < z$, such that $z - y_a < 2^k$ and $z - x_b \geq 2^k$. On the other hand, since $z \in S_a \cap S_b$, by the condition of the problem there is no element of S_a strictly between x_b and z. Hence $y_a \leq x_b$, implying $z - y_a \geq z - x_b$. However this contradicts $z - y_a < 2^k$ and $z - x_b \geq 2^k$. The claim follows.

As a consequence, a fixed $z \in A$ can be good to at most n of the given sets (no more than one of them for each $k = 1, \ldots, n$).

Furthermore, let $u_1 < u_2 < \cdots < u_m < \cdots < u_p$ be all elements of a fixed set S_a that are not good to S_a. We prove that $u_m - u_1 > 2(u_{m-1} - u_1)$ for all $m \geq 3$.

Indeed, assume that $u_m - u_1 \leq 2(u_{m-1} - u_1)$ holds for some $m \geq 3$. This inequality can be written as $2(u_m - u_{m-1}) \leq u_m - u_1$. Take the unique k such that $2^k \leq u_m - u_1 < 2^{k+1}$. Then $2(u_m - u_{m-1}) \leq u_m - u_1 < 2^{k+1}$ yields $u_m - u_{m-1} < 2^k$. However the elements $z = u_m$, $x = u_1$, $y = u_{m-1}$ of S_a then satisfy $z - y < 2^k$ and $z - x \geq 2^k$, so that $z = u_m$ is k-good to S_a.

Thus each term of the sequence $u_2 - u_1, u_3 - u_1, \ldots, u_p - u_1$ is more than twice the previous one. Hence $u_p - u_1 > 2^{p-1}(u_2 - u_1) \geq 2^{p-1}$. But $u_p \in \{1, 2, 3, \ldots, 2^{n+1}\}$, so that $u_p \leq 2^{n+1}$. This yields $p - 1 \leq n$, i. e. $p \leq n + 1$.

In other words, each set S_a contains at most $n + 1$ elements that are not good to it.

To summarize the conclusions, mark with red all elements in the sets S_a that are good to the respective set, and with blue the ones that are not good. Then the total number of red elements, counting multiplicities, is at most $n \cdot 2^{n+1}$ (each $z \in A$ can be marked red in at most n sets). The total number of blue elements is at most $(n + 1)2^n$ (each set S_a contains at most $n + 1$ blue elements). Therefore the sum of cardinalities of $S_1, S_2, \ldots, S_{2^n}$ does not exceed $(3n + 1)2^n$. By averaging, the smallest set has at most $3n + 1$ elements.

Solution 2. We show that one of the sets S_a has at most $2n + 1$ elements. In the sequel $|\cdot|$ denotes the cardinality of a (finite) set.

Claim. For $n \geq 2$, suppose that k subsets $S_1, \ldots, S_k$ of $\{1, 2, \ldots, 2^n\}$ (not necessarily different) satisfy the condition of the problem. Then

$$\sum_{i=1}^{k} (|S_i| - n) \leq (2n - 1)2^{n-2}.$$

Proof. Observe that if the sets S_i $(1 \leq i \leq k)$ satisfy the condition then so do their arbitrary subsets T_i $(1 \leq i \leq k)$. The condition also holds for the sets $t + S_i = \{t + x \mid x \in S_i\}$ where t is arbitrary.

Note also that a set may occur more than once among $S_1, \ldots, S_k$ only if its cardinality is less than 3, in which case its contribution to the sum $\sum_{i=1}^{k}(|S_i| - n)$ is nonpositive (as $n \geq 2$).

The proof is by induction on n. In the base case $n = 2$ we have subsets S_i of $\{1, 2, 3, 4\}$. Only the ones of cardinality 3 and 4 need to be considered by the remark above; each one of them occurs at most once among $S_1, \dots, S_k$. If $S_i = \{1,2,3,4\}$ for some i then no S_j is a 3-element subset in view of the condition, hence $\sum_{i=1}^{k}(|S_i| - 2) \le 2$. By the condition again, it is impossible that $S_i = \{1,3,4\}$ and $S_j = \{2,3,4\}$ for some i, j. So if $|S_i| \le 3$ for all i then at most 3 summands $|S_i| - 2$ are positive, corresponding to 3-element subsets. This implies $\sum_{i=1}^{k}(|S_i| - 2) \le 3$, therefore the conclusion is true for $n = 2$.

Suppose that the claim holds for some $n \ge 2$, and let the sets $S_1, \dots, S_k \subseteq \{1, 2, \dots, 2^{n+1}\}$ satisfy the given property. Denote $U_i = S_i \cap \{1, 2, \dots, 2^n\}$, $V_i = S_i \cap \{2^n + 1, \dots, 2^{n+1}\}$. Let

$$I = \{i \mid 1 \le i \le k,\ |U_i| \ne 0\}, \qquad J = \{1, \dots, k\} \setminus I.$$

The sets S_j with $j \in J$ are all contained in $\{2^n + 1, \dots, 2^{n+1}\}$, so the induction hypothesis applies to their translates $-2^n + S_j$ which have the same cardinalities. Consequently, this gives $\sum_{j\in J}(|S_j| - n) \le (2n-1)2^{n-2}$, so that

$$\sum_{j\in J}(|S_j| - (n+1)) \le \sum_{j\in J}(|S_j| - n) \le (2n-1)2^{n-2}. \tag{1}$$

For $i \in I$, denote by v_i the least element of V_i. Observe that if V_a and V_b intersect, with $a < b$, $a, b \in I$, then v_a is their unique common element. Indeed, let $z \in V_a \cap V_b \subseteq S_a \cap S_b$ and let m be the least element of S_b. Since $b \in I$, we have $m \le 2^n$. By the condition, there is no element of S_a strictly between $m \le 2^n$ and $z > 2^n$, which implies $z = v_a$.

It follows that if the element v_i is removed from each V_i, a family of pairwise disjoint sets $W_i = V_i \setminus \{v_i\}$ is obtained, $i \in I$ (we assume $W_i = \emptyset$ if $V_i = \emptyset$). As $W_i \subseteq \{2^n + 1, \dots, 2^{n+1}\}$ for all i, we infer that $\sum_{i\in I}|W_i| \le 2^n$. Therefore $\sum_{i\in I}(|V_i| - 1) \le \sum_{i\in I}|W_i| \le 2^n$.

On the other hand, the induction hypothesis applies directly to the sets U_i, $i \in I$, so that $\sum_{i\in \mathcal{I}}(|U_i| - n) \le (2n-1)2^{n-2}$. In summary,

$$\sum_{i\in I}(|S_i| - (n+1)) = \sum_{i\in I}(|U_i| - n) + \sum_{i\in I}(|V_i| - 1) \le (2n-1)2^{n-2} + 2^n. \tag{2}$$

The estimates (1) and (2) are sufficient to complete the inductive step:

$$\begin{aligned}\sum_{i=1}^{k}(|S_i| - (n+1)) &= \sum_{i\in I}(|S_i| - (n+1)) + \sum_{j\in J}(|S_j| - (n+1)) \\ &\le (2n-1)2^{n-2} + 2^n + (2n-1)2^{n-2} = (2n+1)2^{n-1}.\end{aligned}$$

Returning to the problem, consider $k = 2^n$ subsets $S_1, S_2, \dots, S_{2^n}$ of $\{1, 2, 3, \dots, 2^{n+1}\}$. If they satisfy the given condition, the claim implies $\sum_{i=1}^{2^n}(|S_i| - (n+1)) \le (2n+1)2^{n-1}$. By averaging again, we see that the smallest set has at most $2n + 1$ elements.

Comment. It can happen that each set S_i has cardinality at least $n + 1$. Here is an example by the proposer.

For $i = 1, \dots, 2^n$, let $S_i = \{i + 2^k \mid 0 \le k \le n\}$. Then $|S_i| = n + 1$ for all i. Suppose that there exist $a < b$ and $x < y < z$ such that $y, z \in S_a$ and $x, z \in S_b$. Hence $z = a + 2^k = b + 2^l$ for some $k > l$. Since $y \in S_a$ and $y < z$, we have $y \le a + 2^{k-1}$. So the element $x \in S_b$ satisfies

$$x < y \le a + 2^{k-1} = z - 2^{k-1} \le z - 2^l = b.$$

However the least element of S_b is $b + 1$, a contradiction.

Geometry

G1. In an acute-angled triangle ABC, point H is the orthocentre and A_0, B_0, C_0 are the midpoints of the sides BC, CA, AB, respectively. Consider three circles passing through H: ω_a around A_0, ω_b around B_0 and ω_c around C_0. The circle ω_a intersects the line BC at A_1 and A_2; ω_b intersects CA at B_1 and B_2; ω_c intersects AB at C_1 and C_2. Show that the points A_1, A_2, B_1, B_2, C_1, C_2 lie on a circle.

Solution 1. The perpendicular bisectors of the segments A_1A_2, B_1B_2, C_1C_2 are also the perpendicular bisectors of BC, CA, AB. So they meet at O, the circumcentre of ABC. Thus O is the only point that can possibly be the centre of the desired circle.

From the right triangle OA_0A_1 we get

$$OA_1^2 = OA_0^2 + A_0A_1^2 = OA_0^2 + A_0H^2. \tag{1}$$

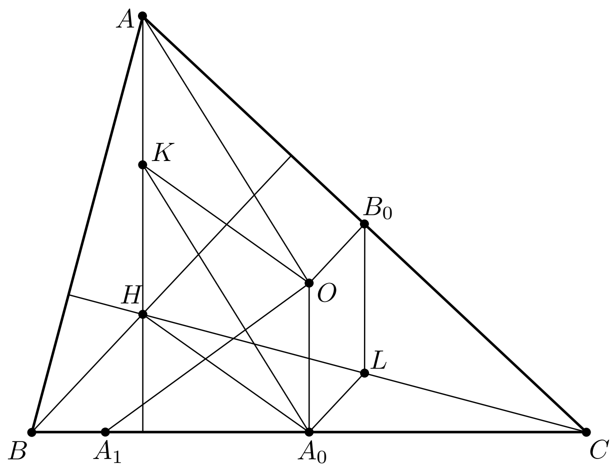
Let K be the midpoint of AH and let L be the midpoint of CH. Since A_0 and B_0 are the midpoints of BC and CA, we see that $A_0L \| BH$ and $B_0L \| AH$. Thus the segments A_0L and B_0L are perpendicular to AC and BC, hence parallel to OB_0 and OA_0, respectively. Consequently OA_0LB_0 is a parallelogram, so that OA_0 and B_0L are equal and parallel. Also, the midline B_0L of triangle AHC is equal and parallel to AK and KH.

It follows that AKA_0O and HA_0OK are parallelograms. The first one gives $A_0K = OA = R$, where R is the circumradius of ABC. From the second one we obtain

$$2(OA_0^2 + A_0H^2) = OH^2 + A_0K^2 = OH^2 + R^2. \tag{2}$$

(In a parallelogram, the sum of squares of the diagonals equals the sum of squares of the sides).

From (1) and (2) we get $OA_1^2 = (OH^2 + R^2)/2$. By symmetry, the same holds for the distances OA_2, OB_1, OB_2, OC_1 and OC_2. Thus A_1, A_2, B_1, B_2, C_1, C_2 all lie on a circle with centre at O and radius $(OH^2 + R^2)/2$.

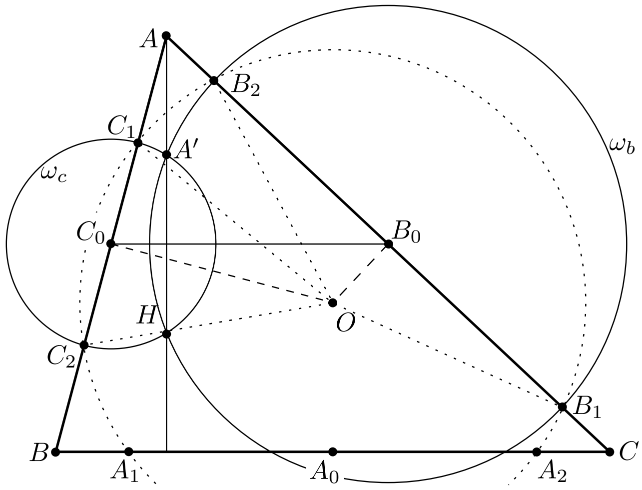


Solution 2. We are going to show again that the circumcentre O is equidistant from the six points in question.

Let A' be the second intersection point of ω_b and ω_c. The line B_0C_0, which is the line of centers of circles ω_b and ω_c, is a midline in triangle ABC, parallel to BC and perpendicular to the altitude AH. The points A' and H are symmetric with respect to the line of centers. Therefore A' lies on the line AH.

From the two circles ω_b and ω_c we obtain $AC_1 \cdot AC_2 = AA' \cdot AH = AB_1 \cdot AB_2$. So the quadrilateral $B_1B_2C_1C_2$ is cyclic. The perpendicular bisectors of the sides B_1B_2 and C_1C_2 meet at O. Hence O is the circumcentre of $B_1B_2C_1C_2$ and so $OB_1 = OB_2 = OC_1 = OC_2$.

Analogous arguments yield $OA_1 = OA_2 = OB_1 = OB_2$ and $OA_1 = OA_2 = OC_1 = OC_2$. Thus A_1, A_2, B_1, B_2, C_1, C_2 lie on a circle centred at O.



Comment. The problem can be solved without much difficulty in many ways by calculation, using trigonometry, coordinate geometry or complex numbers. As an example we present a short proof using vectors.

Solution 3. Let again O and R be the circumcentre and circumradius. Consider the vectors

$$\overrightarrow{OA} = \mathbf{a}, \quad \overrightarrow{OB} = \mathbf{b}, \quad \overrightarrow{OC} = \mathbf{c}, \quad \text{where} \quad \mathbf{a}^2 = \mathbf{b}^2 = \mathbf{c}^2 = R^2.$$

It is well known that $\overrightarrow{OH} = \mathbf{a} + \mathbf{b} + \mathbf{c}$. Accordingly,

$$\overrightarrow{A_0H} = \overrightarrow{OH} - \overrightarrow{OA_0} = (\mathbf{a} + \mathbf{b} + \mathbf{c}) - \frac{\mathbf{b} + \mathbf{c}}{2} = \frac{2\mathbf{a} + \mathbf{b} + \mathbf{c}}{2},$$

and

$$OA_1^2 = OA_0^2 + A_0A_1^2 = OA_0^2 + A_0H^2 = \left(\frac{\mathbf{b} + \mathbf{c}}{2}\right)^2 + \left(\frac{2\mathbf{a} + \mathbf{b} + \mathbf{c}}{2}\right)^2$$

$$= \frac{1}{4}(\mathbf{b}^2 + 2\mathbf{bc} + \mathbf{c}^2) + \frac{1}{4}(4\mathbf{a}^2 + 4\mathbf{ab} + 4\mathbf{ac} + \mathbf{b}^2 + 2\mathbf{bc} + \mathbf{c}^2) = 2R^2 + (\mathbf{ab} + \mathbf{ac} + \mathbf{bc});$$

here $\mathbf{ab}$, $\mathbf{bc}$, etc. denote dot products of vectors. We get the same for the distances OA_2, OB_1, OB_2, OC_1 and OC_2.

G2. Given trapezoid $ABCD$ with parallel sides AB and CD, assume that there exist points E on line BC outside segment BC, and F inside segment AD, such that $\angle DAE = \angle CBF$. Denote by I the point of intersection of CD and EF, and by J the point of intersection of AB and EF. Let K be the midpoint of segment EF; assume it does not lie on line AB.

Prove that I belongs to the circumcircle of ABK if and only if K belongs to the circumcircle of CDJ.

Solution. Assume that the disposition of points is as in the diagram.

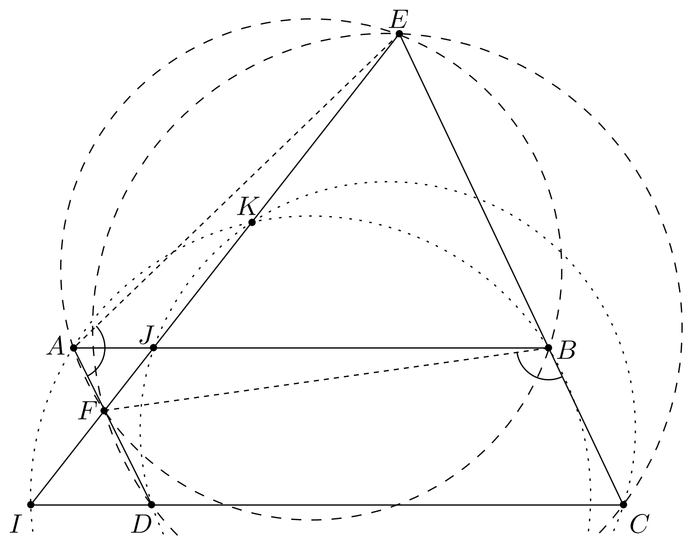
Since $\angle EBF = 180° - \angle CBF = 180° - \angle EAF$ by hypothesis, the quadrilateral $AEBF$ is cyclic. Hence $AJ \cdot JB = FJ \cdot JE$. In view of this equality, I belongs to the circumcircle of ABK if and only if $IJ \cdot JK = FJ \cdot JE$. Expressing $IJ = IF + FJ$, $JE = FE - FJ$, and $JK = \frac{1}{2}FE - FJ$, we find that I belongs to the circumcircle of ABK if and only if

$$FJ = \frac{IF \cdot FE}{2IF + FE}.$$

Since $AEBF$ is cyclic and AB, CD are parallel, $\angle FEC = \angle FAB = 180° - \angle CDF$. Then $CDFE$ is also cyclic, yielding $ID \cdot IC = IF \cdot IE$. It follows that K belongs to the circumcircle of CDJ if and only if $IJ \cdot IK = IF \cdot IE$. Expressing $IJ = IF + FJ$, $IK = IF + \frac{1}{2}FE$, and $IE = IF + FE$, we find that K is on the circumcircle of CDJ if and only if

$$FJ = \frac{IF \cdot FE}{2IF + FE}.$$

The conclusion follows.



Comment. While the figure shows B inside segment CE, it is possible that C is inside segment BE. Consequently, I would be inside segment EF and J outside segment EF. The position of point K on line EF with respect to points I, J may also vary.

Some case may require that an angle φ be replaced by $180° - \varphi$, and in computing distances, a sum may need to become a difference. All these cases can be covered by the proposed solution if it is clearly stated that *signed* distances and angles are used.

G3. Let $ABCD$ be a convex quadrilateral and let P and Q be points in $ABCD$ such that $PQDA$ and $QPBC$ are cyclic quadrilaterals. Suppose that there exists a point E on the line segment PQ such that $\angle PAE = \angle QDE$ and $\angle PBE = \angle QCE$. Show that the quadrilateral $ABCD$ is cyclic.

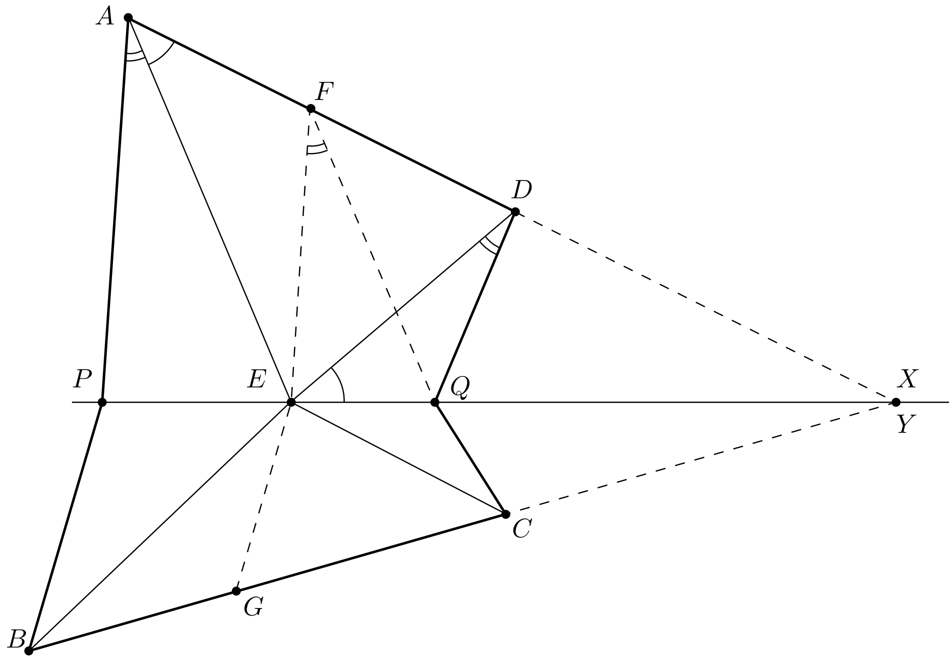
Solution 1. Let F be the point on the line AD such that $EF \| PA$. By hypothesis, the quadrilateral $PQDA$ is cyclic. So if F lies between A and D then $\angle EFD = \angle PAD = 180° - \angle EQD$; the points F and Q are on distinct sides of the line DE and we infer that $EFDQ$ is a cyclic quadrilateral. And if D lies between A and F then a similar argument shows that $\angle EFD = \angle EQD$; but now the points F and Q lie on the same side of DE, so that $EDFQ$ is a cyclic quadrilateral.

In either case we obtain the equality $\angle EFQ = \angle EDQ = \angle PAE$ which implies that $FQ \| AE$. So the triangles EFQ and PAE are either homothetic or parallel-congruent. More specifically, triangle EFQ is the image of PAE under the mapping f which carries the points P, E respectively to E, Q and is either a homothety or translation by a vector. Note that f is uniquely determined by these conditions and the position of the points P, E, Q alone.

Let now G be the point on the line BC such that $EG \| PB$. The same reasoning as above applies to points B, C in place of A, D, implying that the triangle EGQ is the image of PBE under the same mapping f. So f sends the four points A, P, B, E respectively to F, E, G, Q.

If $PE \neq QE$, so that f is a homothety with a centre X, then the lines AF, PE, BG—i.e. the lines AD, PQ, BC—are concurrent at X. And since $PQDA$ and $QPBC$ are cyclic quadrilaterals, the equalities $XA \cdot XD = XP \cdot XQ = XB \cdot XC$ hold, showing that the quadrilateral $ABCD$ is cyclic.

Finally, if $PE = QE$, so that f is a translation, then $AD \| PQ \| BC$. Thus $PQDA$ and $QPBC$ are isosceles trapezoids. Then also $ABCD$ is an isosceles trapezoid, hence a cyclic quadrilateral.



Solution 2. Here is another way to reach the conclusion that the lines AD, BC and PQ are either concurrent or parallel. From the cyclic quadrilateral $PQDA$ we get

$$\angle PAD = 180° - \angle PQD = \angle QDE + \angle QED = \angle PAE + \angle QED.$$

Hence $\angle QED = \angle PAD - \angle PAE = \angle EAD$. This in view of the tangent-chord theorem means that the circumcircle of triangle EAD is tangent to the line PQ at E. Analogously, the circumcircle of triangle EBC is tangent to PQ at E.

Suppose that the line AD intersects PQ at X. Since XE is tangent to the circle (EAD), $XE^2 = XA \cdot XD$. Also, $XA \cdot XD = XP \cdot XQ$ because P, Q, D, A lie on a circle. Therefore $XE^2 = XP \cdot XQ$.

It is not hard to see that this equation determines the position of the point X on the line PQ uniquely. Thus, if BC also cuts PQ, say at Y, then the analogous equation for Y yields $X = Y$, meaning that the three lines indeed concur. In this case, as well as in the case where $AD \| PQ \| BC$, the concluding argument is the same as in the first solution.

It remains to eliminate the possibility that e.g. AD meets PQ at X while $BC \| PQ$. Indeed, $QPBC$ would then be an isosceles trapezoid and the angle equality $\angle PBE = \angle QCE$ would force that E is the midpoint of PQ. So the length of XE, which is the geometric mean of the lengths of XP and XQ, should also be their arithmetic mean—impossible, as $XP \neq XQ$. The proof is now complete.

Comment. After reaching the conclusion that the circles (EDA) and (EBC) are tangent to PQ one may continue as follows. Denote the circles $(PQDA)$, (EDA), (EBC), $(QPBC)$ by ω_1, ω_2, ω_3, ω_4 respectively. Let ℓ_{ij} be the radical axis of the pair (ω_i, ω_j) for $i < j$. As is well-known, the lines ℓ_{12}, ℓ_{13}, ℓ_{23} concur, possibly at infinity (let this be the meaning of the word *concur* in this comment). So do the lines ℓ_{12}, ℓ_{14}, ℓ_{24}. Note however that ℓ_{23} and ℓ_{14} both coincide with the line PQ. Hence the pair ℓ_{12}, PQ is in both triples; thus the four lines ℓ_{12}, ℓ_{13}, ℓ_{24} and PQ are concurrent.

Similarly, ℓ_{13}, ℓ_{14}, ℓ_{34} concur, ℓ_{23}, ℓ_{24}, ℓ_{34} concur, and since $\ell_{14} = \ell_{23} = PQ$, the four lines ℓ_{13}, ℓ_{24}, ℓ_{34} and PQ are concurrent. The lines ℓ_{13} and ℓ_{24} are present in both quadruples, therefore all the lines ℓ_{ij} are concurrent. Hence the result.

G4. In an acute triangle ABC segments BE and CF are altitudes. Two circles passing through the points A and F are tangent to the line BC at the points P and Q so that B lies between C and Q. Prove that the lines PE and QF intersect on the circumcircle of triangle AEF.

Solution 1. To approach the desired result we need some information about the slopes of the lines PE and QF; this information is provided by formulas (1) and (2) which we derive below.

The tangents BP and BQ to the two circles passing through A and F are equal, as $BP^2 = BA \cdot BF = BQ^2$. Consider the altitude AD of triangle ABC and its orthocentre H. From the cyclic quadrilaterals $CDFA$ and $CDHE$ we get $BA \cdot BF = BC \cdot BD = BE \cdot BH$. Thus $BP^2 = BE \cdot BH$, or $BP/BH = BE/BP$, implying that the triangles BPH and BEP are similar. Hence

$$\angle BPE = \angle BHP. \tag{1}$$

The point P lies between D and C; this follows from the equality $BP^2 = BC \cdot BD$. In view of this equality, and because $BP = BQ$,

$$DP \cdot DQ = (BP - BD) \cdot (BP + BD) = BP^2 - BD^2 = BD \cdot (BC - BD) = BD \cdot DC.$$

Also $AD \cdot DH = BD \cdot DC$, as is seen from the similar triangles BDH and ADC. Combining these equalities we obtain $AD \cdot DH = DP \cdot DQ$. Therefore $DH/DP = DQ/DA$, showing that the triangles HDP and QDA are similar. Hence $\angle HPD = \angle QAD$, which can be rewritten as $\angle BPH = \angle BAD + \angle BAQ$. And since BQ is tangent to the circumcircle of triangle FAQ,

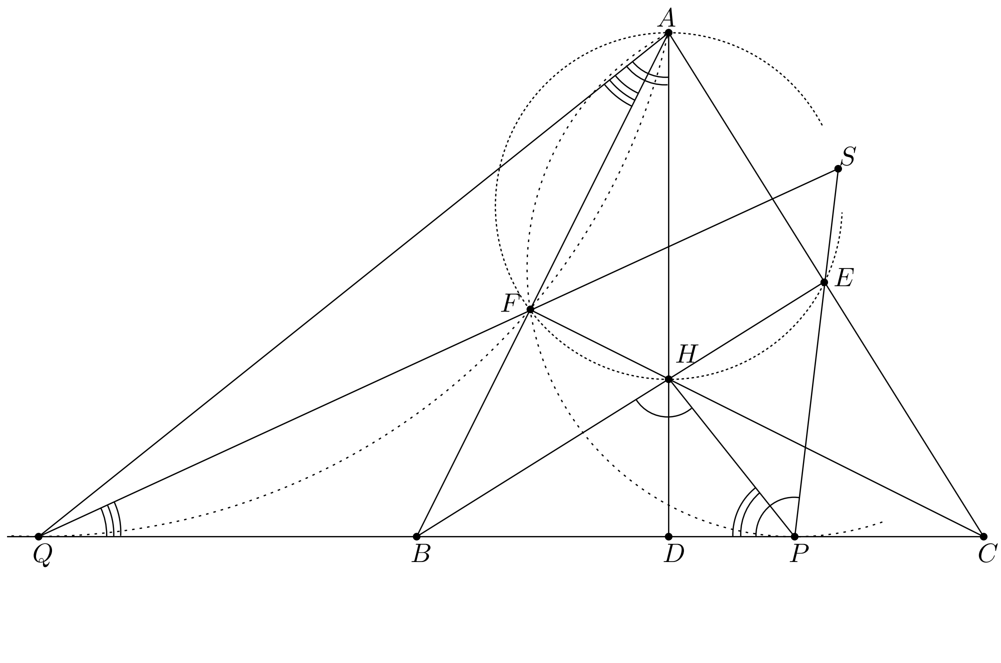
$$\angle BQF = \angle BAQ = \angle BPH - \angle BAD. \tag{2}$$

From (1) and (2) we deduce

$$\begin{aligned}\angle BPE + \angle BQF &= (\angle BHP + \angle BPH) - \angle BAD = (180^\circ - \angle PBH) - \angle BAD \\ &= (90^\circ + \angle BCA) - (90^\circ - \angle ABC) = \angle BCA + \angle ABC = 180^\circ - \angle CAB.\end{aligned}$$

Thus $\angle BPE + \angle BQF < 180^\circ$, which means that the rays PE and QF meet. Let S be the point of intersection. Then $\angle PSQ = 180^\circ - (\angle BPE + \angle BQF) = \angle CAB = \angle EAF$.

If S lies between P and E then $\angle PSQ = 180^\circ - \angle ESF$; and if E lies between P and S then $\angle PSQ = \angle ESF$. In either case the equality $\angle PSQ = \angle EAF$ which we have obtained means that S lies on the circumcircle of triangle AEF.



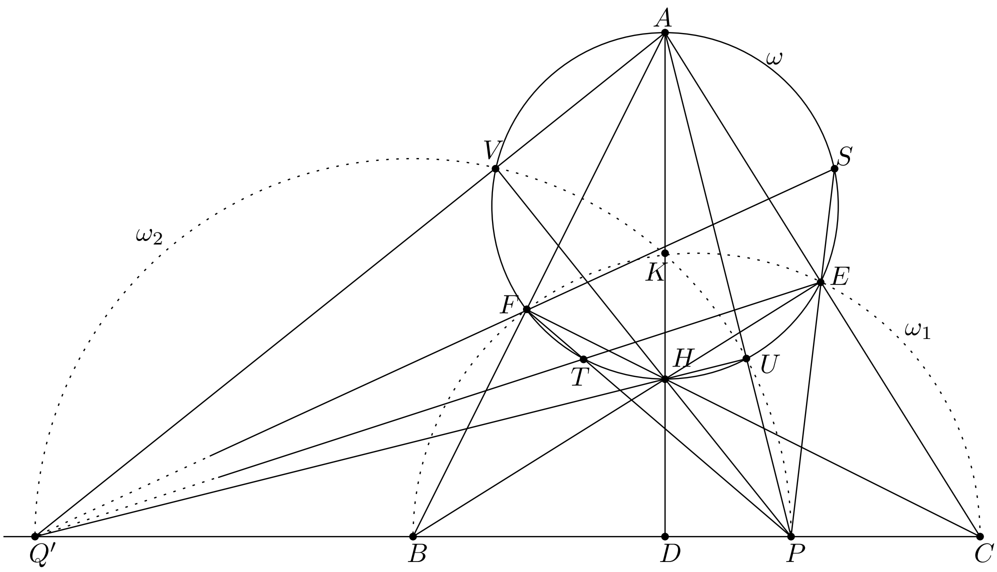
Solution 2. Let H be the orthocentre of triangle ABC and let ω be the circle with diameter AH, passing through E and F. Introduce the points of intersection of ω with the following lines emanating from P: $PA \cap \omega = \{A, U\}$, $PH \cap \omega = \{H, V\}$, $PE \cap \omega = \{E, S\}$. The altitudes of triangle AHP are contained in the lines AV, HU, BC, meeting at its orthocentre Q'.

By Pascal's theorem applied to the (tied) hexagon $AESFHV$, the points $AE \cap FH = C$, $ES \cap HV = P$ and $SF \cap VA$ are collinear, so FS passes through Q'.

Denote by ω_1 and ω_2 the circles with diameters BC and PQ', respectively. Let D be the foot of the altitude from A in triangle ABC. Suppose that AD meets the circles ω_1 and ω_2 at the respective points K and L.

Since H is the orthocentre of ABC, the triangles BDH and ADC are similar, and so $DA \cdot DH = DB \cdot DC = DK^2$; the last equality holds because BKC is a right triangle. Since H is the orthocentre also in triangle $AQ'P$, we analogously have $DL^2 = DA \cdot DH$. Therefore $DK = DL$ and $K = L$.

Also, $BD \cdot BC = BA \cdot BF$, from the similar triangles ABD, CBF. In the right triangle BKC we have $BK^2 = BD \cdot BC$. Hence, and because $BA \cdot BF = BP^2 = BQ^2$ (by the definition of P and Q in the problem statement), we obtain $BK = BP = BQ$. It follows that B is the centre of ω_2 and hence $Q' = Q$. So the lines PE and QF meet at the point S lying on the circumcircle of triangle AEF.



Comment 1. If T is the point defined by $PF \cap \omega = \{F, T\}$, Pascal's theorem for the hexagon $AFTEHV$ will analogously lead to the conclusion that the line ET goes through Q'. In other words, the lines PF and QE also concur on ω.

Comment 2. As is known from algebraic geometry, the points of the circle ω form a commutative groups with the operation defined as follows. Choose any point $0 \in \omega$ (to be the neutral element of the group) and a line ℓ exterior to the circle. For $X, Y \in \omega$, draw the line from the point $XY \cap \ell$ through 0 to its second intersection with ω and define this point to be $X + Y$.

In our solution we have chosen H to be the neutral element in this group and line BC to be ℓ. The fact that the lines AV, HU, ET, FS are concurrent can be deduced from the identities $A + A = 0$, $F = E + A$, $V = U + A = S + E = T + F$.

Comment 3. The problem was submitted in the following equivalent formulation:

Let BE and CF be altitudes of an acute triangle ABC. We choose P on the side BC and Q on the extension of CB beyond B such that $BQ^2 = BP^2 = BF \cdot AB$. If QF and PE intersect at S, prove that $ESAF$ is cyclic.

G5. Let k and n be integers with $0 \le k \le n-2$. Consider a set L of n lines in the plane such that no two of them are parallel and no three have a common point. Denote by I the set of intersection points of lines in L. Let O be a point in the plane not lying on any line of L.

A point $X \in I$ is colored red if the open line segment OX intersects at most k lines in L. Prove that I contains at least $\frac{1}{2}(k+1)(k+2)$ red points.

Solution. There are at least $\frac{1}{2}(k+1)(k+2)$ points in the intersection set I in view of the condition $n \ge k+2$.

For each point $P \in I$, define its *order* as the number of lines that intersect the open line segment OP. By definition, P is red if its order is at most k. Note that there is always at least one point $X \in I$ of order 0. Indeed, the lines in L divide the plane into regions, bounded or not, and O belongs to one of them. Clearly any corner of this region is a point of I with order 0.

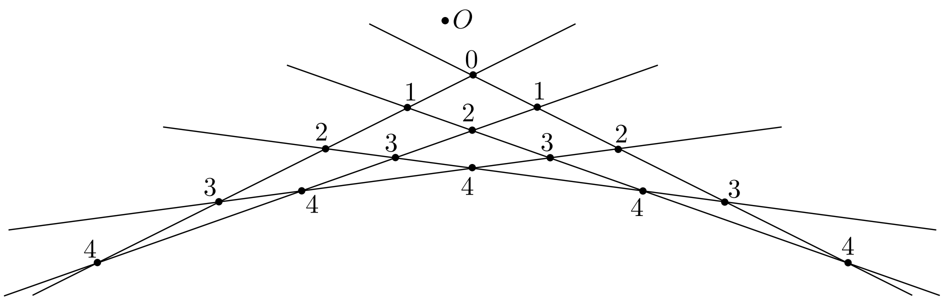
Claim. Suppose that two points $P, Q \in I$ lie on the same line of L, and no other line of L intersects the open line segment PQ. Then the orders of P and Q differ by at most 1.

Proof. Let P and Q have orders p and q, respectively, with $p \ge q$. Consider triangle OPQ. Now p equals the number of lines in L that intersect the interior of side OP. None of these lines intersects the interior of side PQ, and at most one can pass through Q. All remaining lines must intersect the interior of side OQ, implying that $q \ge p-1$. The conclusion follows.

We prove the main result by induction on k. The base $k=0$ is clear since there is a point of order 0 which is red. Assuming the statement true for $k-1$, we pass on to the inductive step. Select a point $P \in I$ of order 0, and consider one of the lines $\ell \in L$ that pass through P. There are $n-1$ intersection points on ℓ, one of which is P. Out of the remaining $n-2$ points, the k closest to P have orders not exceeding k by the Claim. It follows that there are at least $k+1$ red points on ℓ.

Let us now consider the situation with ℓ removed (together with all intersection points it contains). By hypothesis of induction, there are at least $\frac{1}{2}k(k+1)$ points of order not exceeding $k-1$ in the resulting configuration. Restoring ℓ back produces at most one new intersection point on each line segment joining any of these points to O, so their order is at most k in the original configuration. The total number of points with order not exceeding k is therefore at least $(k+1) + \frac{1}{2}k(k+1) = \frac{1}{2}(k+1)(k+2)$. This completes the proof.

Comment. The steps of the proof can be performed in reverse order to obtain a configuration of n lines such that equality holds simultaneously for all $0 \le k \le n-2$. Such a set of lines is illustrated in the Figure.



G6. There is given a convex quadrilateral $ABCD$. Prove that there exists a point P inside the quadrilateral such that

$$\angle PAB + \angle PDC = \angle PBC + \angle PAD = \angle PCD + \angle PBA = \angle PDA + \angle PCB = 90^\circ \qquad (1)$$

if and only if the diagonals AC and BD are perpendicular.

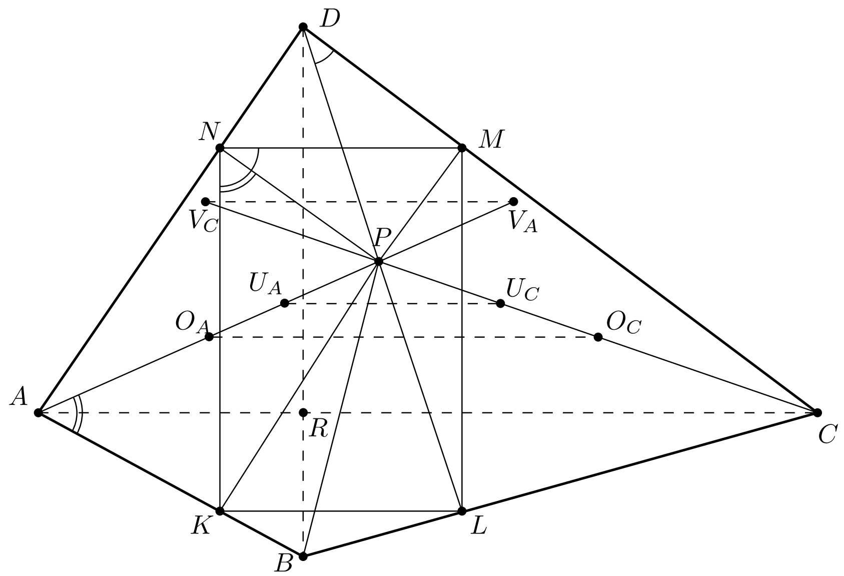
Solution 1. For a point P in $ABCD$ which satisfies (1), let K, L, M, N be the feet of perpendiculars from P to lines AB, BC, CD, DA, respectively. Note that K, L, M, N are interior to the sides as all angles in (1) are acute. The cyclic quadrilaterals $AKPN$ and $DNPM$ give

$$\angle PAB + \angle PDC = \angle PNK + \angle PNM = \angle KNM.$$

Analogously, $\angle PBC + \angle PAD = \angle LKN$ and $\angle PCD + \angle PBA = \angle MLK$. Hence the equalities (1) imply $\angle KNM = \angle LKN = \angle MLK = 90^\circ$, so that $KLMN$ is a rectangle. The converse also holds true, provided that K, L, M, N are interior to sides AB, BC, CD, DA.

(i) Suppose that there exists a point P in $ABCD$ such that $KLMN$ is a rectangle. We show that AC and BD are parallel to the respective sides of $KLMN$.

Let O_A and O_C be the circumcentres of the cyclic quadrilaterals $AKPN$ and $CMPL$. Line O_AO_C is the common perpendicular bisector of LM and KN, therefore O_AO_C is parallel to KL and MN. On the other hand, O_AO_C is the midline in the triangle ACP that is parallel to AC. Therefore the diagonal AC is parallel to the sides KL and MN of the rectangle. Likewise, BD is parallel to KN and LM. Hence AC and BD are perpendicular.



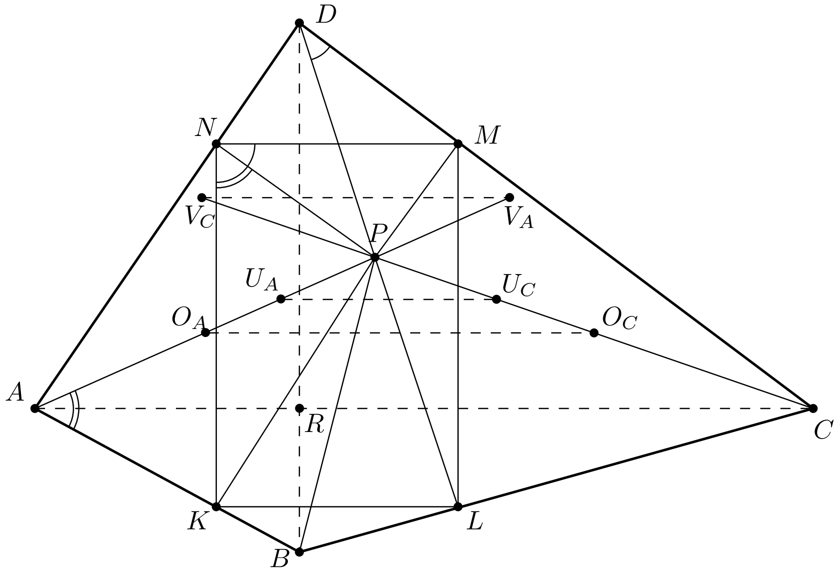
(ii) Suppose that AC and BD are perpendicular and meet at R. If $ABCD$ is a rhombus, P can be chosen to be its centre. So assume that $ABCD$ is not a rhombus, and let $BR < DR$ without loss of generality.

Denote by U_A and U_C the circumcentres of the triangles ABD and CDB, respectively. Let AV_A and CV_C be the diameters through A and C of the two circumcircles. Since AR is an altitude in triangle ADB, lines AC and AV_A are isogonal conjugates, i. e. $\angle DAV_A = \angle BAC$. Now $BR < DR$ implies that ray AU_A lies in $\angle DAC$. Similarly, ray CU_C lies in $\angle DCA$. Both diameters AV_A and CV_C intersect BD as the angles at B and D of both triangles are acute. Also U_AU_C is parallel to AC as it is the perpendicular bisector of BD. Hence V_AV_C is parallel to AC, too. We infer that AV_A and CV_C intersect at a point P inside triangle ACD, hence inside $ABCD$.

Construct points K, L, M, N, O_A and O_C in the same way as in the introduction. It follows from the previous paragraph that K, L, M, N are interior to the respective sides. Now O_AO_C is a midline in triangle ACP again. Therefore lines AC, O_AO_C and U_AU_C are parallel.

The cyclic quadrilateral $AKPN$ yields $\angle NKP = \angle NAP$. Since $\angle NAP = \angle DAU_A = \angle BAC$, as specified above, we obtain $\angle NKP = \angle BAC$. Because PK is perpendicular to AB, it follows that NK is perpendicular to AC, hence parallel to BD. Likewise, LM is parallel to BD.

Consider the two homotheties with centres A and C which transform triangles ABD and CDB into triangles AKN and CML, respectively. The images of points U_A and U_C are O_A and O_C, respectively. Since U_AU_C and O_AO_C are parallel to AC, the two ratios of homothety are the same, equal to $\lambda = AN/AD = AK/AB = AO_A/AU_A = CO_C/CU_C = CM/CD = CL/CB$. It is now straightforward that $DN/DA = DM/DC = BK/BA = BL/BC = 1-\lambda$. Hence KL and MN are parallel to AC, implying that $KLMN$ is a rectangle and completing the proof.



Solution 2. For a point P distinct from A, B, C, D, let circles (APD) and (BPC) intersect again at Q ($Q = P$ if the circles are tangent). Next, let circles (AQB) and (CQD) intersect again at R. We show that if P lies in $ABCD$ and satisfies (1) then AC and BD intersect at R and are perpendicular; the converse is also true. It is convenient to use directed angles. Let $\measuredangle(UV, XY)$ denote the angle of counterclockwise rotation that makes line UV parallel to line XY. Recall that four noncollinear points U, V, X, Y are concyclic if and only if $\measuredangle(UX, VX) = \measuredangle(UY, VY)$.

The definitions of points P, Q and R imply

$$\begin{aligned}
\measuredangle(AR, BR) &= \measuredangle(AQ, BQ) = \measuredangle(AQ, PQ) + \measuredangle(PQ, BQ) = \measuredangle(AD, PD) + \measuredangle(PC, BC), \\
\measuredangle(CR, DR) &= \measuredangle(CQ, DQ) = \measuredangle(CQ, PQ) + \measuredangle(PQ, DQ) = \measuredangle(CB, PB) + \measuredangle(PA, DA), \\
\measuredangle(BR, CR) &= \measuredangle(BR, RQ) + \measuredangle(RQ, CR) = \measuredangle(BA, AQ) + \measuredangle(DQ, CD) \\
&= \measuredangle(BA, AP) + \measuredangle(AP, AQ) + \measuredangle(DQ, DP) + \measuredangle(DP, CD) \\
&= \measuredangle(BA, AP) + \measuredangle(DP, CD).
\end{aligned}$$

Observe that the whole construction is reversible. One may start with point R, define Q as the second intersection of circles (ARB) and (CRD), and then define P as the second intersection of circles (AQD) and (BQC). The equalities above will still hold true.

Assume in addition that P is interior to $ABCD$. Then

$$\measuredangle(AD, PD) = \angle PDA,\ \measuredangle(PC, BC) = \angle PCB,\ \measuredangle(CB, PB) = \angle PBC,\ \measuredangle(PA, DA) = \angle PAD,$$
$$\measuredangle(BA, AP) = \angle PAB,\ \measuredangle(DP, CD) = \angle PDC.$$

(i) Suppose that P lies in $ABCD$ and satisfies (1). Then $\measuredangle(AR, BR) = \angle PDA + \angle PCB = 90°$ and similarly $\measuredangle(BR, CR) = \measuredangle(CR, DR) = 90°$. It follows that R is the common point of lines AC and BD, and that these lines are perpendicular.
(ii) Suppose that AC and BD are perpendicular and intersect at R. We show that the point P defined by the reverse construction (starting with R and ending with P) lies in $ABCD$. This is enough to finish the solution, because then the angle equalities above will imply (1).

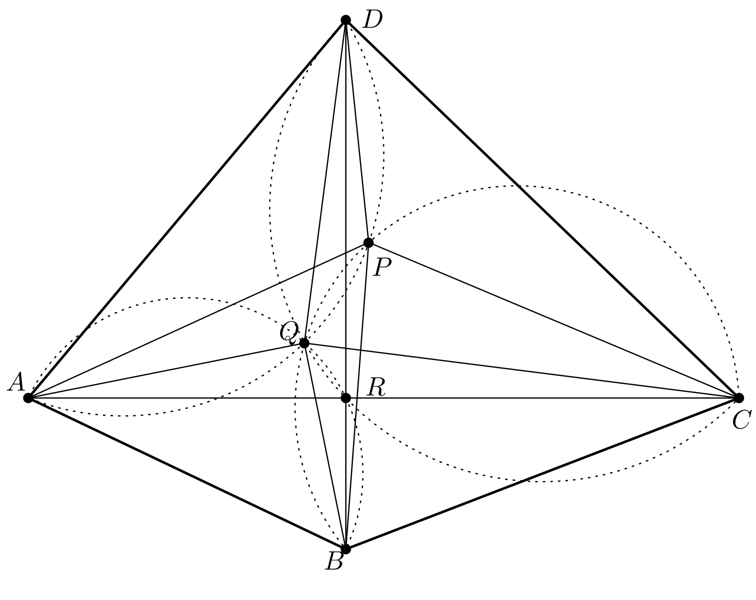
One can assume that Q, the second common point of circles (ABR) and (CDR), lies in $\angle ARD$. Then in fact Q lies in triangle ADR as angles AQR and DQR are obtuse. Hence $\angle AQD$ is obtuse, too, so that B and C are outside circle (ADQ) ($\angle ABD$ and $\angle ACD$ are acute).

Now $\angle CAB + \angle CDB = \angle BQR + \angle CQR = \angle CQB$ implies $\angle CAB < \angle CQB$ and $\angle CDB < \angle CQB$. Hence A and D are outside circle (BCQ). In conclusion, the second common point P of circles (ADQ) and (BCQ) lies on their arcs ADQ and BCQ.

We can assume that P lies in $\angle CQD$. Since

$$\angle QPC + \angle QPD = (180° - \angle QBC) + (180° - \angle QAD) =$$
$$= 360° - (\angle RBC + \angle QBR) - (\angle RAD - \angle QAR) = 360° - \angle RBC - \angle RAD > 180°,$$

point P lies in triangle CDQ, and hence in $ABCD$. The proof is complete.



G7. Let $ABCD$ be a convex quadrilateral with $AB \neq BC$. Denote by ω_1 and ω_2 the incircles of triangles ABC and ADC. Suppose that there exists a circle ω inscribed in angle ABC, tangent to the extensions of line segments AD and CD. Prove that the common external tangents of ω_1 and ω_2 intersect on ω.

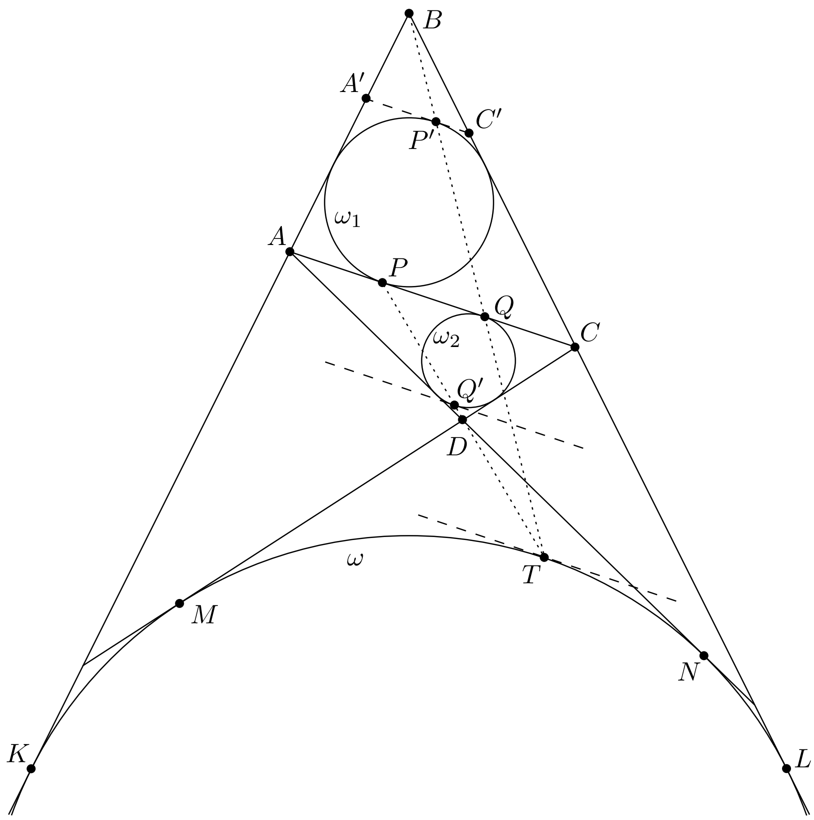
Solution. The proof below is based on two known facts.

Lemma 1. Given a convex quadrilateral $ABCD$, suppose that there exists a circle which is inscribed in angle ABC and tangent to the extensions of line segments AD and CD. Then $AB + AD = CB + CD$.

Proof. The circle in question is tangent to each of the lines AB, BC, CD, DA, and the respective points of tangency K, L, M, N are located as with circle ω in the figure. Then

$$AB + AD = (BK - AK) + (AN - DN), \quad CB + CD = (BL - CL) + (CM - DM).$$

Also $BK = BL$, $DN = DM$, $AK = AN$, $CL = CM$ by equalities of tangents. It follows that $AB + AD = CB + CD$.



For brevity, in the sequel we write "excircle AC" for the excircle of a triangle with side AC which is tangent to line segment AC and the extensions of the other two sides.

Lemma 2. The incircle of triangle ABC is tangent to its side AC at P. Let PP' be the diameter of the incircle through P, and let line BP' intersect AC at Q. Then Q is the point of tangency of side AC and excircle AC.

Proof. Let the tangent at P' to the incircle ω_1 meet BA and BC at A' and C'. Now ω_1 is the excircle $A'C'$ of triangle $A'BC'$, and it touches side $A'C'$ at P'. Since $A'C' \parallel AC$, the homothety with centre B and ratio BQ/BP' takes ω_1 to the excircle AC of triangle ABC. Because this homothety takes P' to Q, the lemma follows.

Recall also that if the incircle of a triangle touches its side AC at P, then the tangency point Q of the same side and excircle AC is the unique point on line segment AC such that $AP = CQ$.

We pass on to the main proof. Let ω_1 and ω_2 touch AC at P and Q, respectively; then $AP = (AC + AB - BC)/2$, $CQ = (CA + CD - AD)/2$. Since $AB - BC = CD - AD$ by Lemma 1, we obtain $AP = CQ$. It follows that in triangle ABC side AC and excircle AC are tangent at Q. Likewise, in triangle ADC side AC and excircle AC are tangent at P. Note that $P \neq Q$ as $AB \neq BC$.

Let PP' and QQ' be the diameters perpendicular to AC of ω_1 and ω_2, respectively. Then Lemma 2 shows that points B, P' and Q are collinear, and so are points D, Q' and P.

Consider the diameter of ω perpendicular to AC and denote by T its endpoint that is closer to AC. The homothety with centre B and ratio BT/BP' takes ω_1 to ω. Hence B, P' and T are collinear. Similarly, D, Q' and T are collinear since the homothety with centre D and ratio $-DT/DQ'$ takes ω_2 to ω.

We infer that points T, P' and Q are collinear, as well as T, Q' and P. Since $PP' \parallel QQ'$, line segments PP' and QQ' are then homothetic with centre T. The same holds true for circles ω_1 and ω_2 because they have PP' and QQ' as diameters. Moreover, it is immediate that T lies on the same side of line PP' as Q and Q', hence the ratio of homothety is positive. In particular ω_1 and ω_2 are not congruent.

In summary, T is the centre of a homothety with positive ratio that takes circle ω_1 to circle ω_2. This completes the solution, since the only point with the mentioned property is the intersection of the the common external tangents of ω_1 and ω_2.

Number Theory

N1. Let n be a positive integer and let p be a prime number. Prove that if a, b, c are integers (not necessarily positive) satisfying the equations

$$a^n + pb = b^n + pc = c^n + pa,$$

then $a = b = c$.

Solution 1. If two of a, b, c are equal, it is immediate that all the three are equal. So we may assume that $a \neq b \neq c \neq a$. Subtracting the equations we get $a^n - b^n = -p(b-c)$ and two cyclic copies of this equation, which upon multiplication yield

$$\frac{a^n - b^n}{a-b} \cdot \frac{b^n - c^n}{b-c} \cdot \frac{c^n - a^n}{c-a} = -p^3. \qquad (1)$$

If n is odd then the differences $a^n - b^n$ and $a - b$ have the same sign and the product on the left is positive, while $-p^3$ is negative. So n must be even.

Let d be the greatest common divisor of the three differences $a-b$, $b-c$, $c-a$, so that $a - b = du$, $b - c = dv$, $c - a = dw$; $\gcd(u, v, w) = 1$, $u + v + w = 0$.

From $a^n - b^n = -p(b-c)$ we see that $(a-b)|p(b-c)$, i.e., $u|pv$; and cyclically $v|pw$, $w|pu$. As $\gcd(u, v, w) = 1$ and $u + v + w = 0$, at most one of u, v, w can be divisible by p. Supposing that the prime p does not divide any one of them, we get $u|v$, $v|w$, $w|u$, whence $|u| = |v| = |w| = 1$; but this quarrels with $u + v + w = 0$.

Thus p must divide exactly one of these numbers. Let e.g. $p|u$ and write $u = pu_1$. Now we obtain, similarly as before, $u_1|v$, $v|w$, $w|u_1$ so that $|u_1| = |v| = |w| = 1$. The equation $pu_1 + v + w = 0$ forces that the prime p must be even; i.e. $p = 2$. Hence $v + w = -2u_1 = \pm 2$, implying $v = w\ (= \pm 1)$ and $u = -2v$. Consequently $a - b = -2(b - c)$.

Knowing that n is even, say $n = 2k$, we rewrite the equation $a^n - b^n = -p(b-c)$ with $p = 2$ in the form

$$(a^k + b^k)(a^k - b^k) = -2(b - c) = a - b.$$

The second factor on the left is divisible by $a - b$, so the first factor $(a^k + b^k)$ must be ± 1. Then exactly one of a and b must be odd; yet $a - b = -2(b - c)$ is even. Contradiction ends the proof.

Solution 2. The beginning is as in the first solution. Assuming that a, b, c are not all equal, hence are all distinct, we derive equation (1) with the conclusion that n is even. Write $n = 2k$.

Suppose that p is odd. Then the integer

$$\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2}b + \cdots + b^{n-1},$$

which is a factor in (1), must be odd as well. This sum of $n = 2k$ summands is odd only if a and b have different parities. The same conclusion holding for b, c and for c, a, we get that a, b, c, a alternate in their parities, which is clearly impossible.

Thus $p = 2$. The original system shows that a, b, c must be of the same parity. So we may divide (1) by p^3, i.e. 2^3, to obtain the following product of six integer factors:

$$\frac{a^k + b^k}{2} \cdot \frac{a^k - b^k}{a - b} \cdot \frac{b^k + c^k}{2} \cdot \frac{b^k - c^k}{b - c} \cdot \frac{c^k + a^k}{2} \cdot \frac{c^k - a^k}{c - a} = -1. \tag{2}$$

Each one of the factors must be equal to ± 1. In particular, $a^k + b^k = \pm 2$. If k is even, this becomes $a^k + b^k = 2$ and yields $|a| = |b| = 1$, whence $a^k - b^k = 0$, contradicting (2).

Let now k be odd. Then the sum $a^k + b^k$, with value ± 2, has $a + b$ as a factor. Since a and b are of the same parity, this means that $a + b = \pm 2$; and cyclically, $b + c = \pm 2$, $c + a = \pm 2$. In some two of these equations the signs must coincide, hence some two of a, b, c are equal. This is the desired contradiction.

Comment. Having arrived at the equation (1) one is tempted to write down all possible decompositions of $-p^3$ (cube of a prime) into a product of three integers. This leads to cumbersome examination of many cases, some of which are unpleasant to handle. One may do that just for $p = 2$, having earlier in some way eliminated odd primes from consideration.

However, the second solution shows that the condition of p being a prime is far too strong. What is actually being used in that solution, is that p is either a positive odd integer or $p = 2$.

N2. Let $a_1, a_2, \ldots, a_n$ be distinct positive integers, $n \geq 3$. Prove that there exist distinct indices i and j such that $a_i + a_j$ does not divide any of the numbers $3a_1, 3a_2, \ldots, 3a_n$.

Solution. Without loss of generality, let $0 < a_1 < a_2 < \cdots < a_n$. One can also assume that $a_1, a_2, \ldots, a_n$ are coprime. Otherwise division by their greatest common divisor reduces the question to the new sequence whose terms are coprime integers.

Suppose that the claim is false. Then for each $i < n$ there exists a j such that $a_n + a_i$ divides $3a_j$. If $a_n + a_i$ is not divisible by 3 then $a_n + a_i$ divides a_j which is impossible as $0 < a_j \leq a_n < a_n + a_i$. Thus $a_n + a_i$ is a multiple of 3 for $i = 1, \ldots, n-1$, so that $a_1, a_2, \ldots, a_{n-1}$ are all congruent (to $-a_n$) modulo 3.

Now a_n is not divisible by 3 or else so would be all remaining a_i's, meaning that $a_1, a_2, \ldots, a_n$ are not coprime. Hence $a_n \equiv r \pmod 3$ where $r \in \{1, 2\}$, and $a_i \equiv 3 - r \pmod 3$ for all $i = 1, \ldots, n-1$.

Consider a sum $a_{n-1} + a_i$ where $1 \leq i \leq n-2$. There is at least one such sum as $n \geq 3$. Let j be an index such that $a_{n-1} + a_i$ divides $3a_j$. Observe that $a_{n-1} + a_i$ is not divisible by 3 since $a_{n-1} + a_i \equiv 2a_i \not\equiv 0 \pmod 3$. It follows that $a_{n-1} + a_i$ divides a_j, in particular $a_{n-1} + a_i \leq a_j$. Hence $a_{n-1} < a_j \leq a_n$, implying $j = n$. So a_n is divisible by all sums $a_{n-1} + a_i$, $1 \leq i \leq n-2$. In particular $a_{n-1} + a_i \leq a_n$ for $i = 1, \ldots, n-2$.

Let j be such that $a_n + a_{n-1}$ divides $3a_j$. If $j \leq n-2$ then $a_n + a_{n-1} \leq 3a_j < a_j + 2a_{n-1}$. This yields $a_n < a_{n-1} + a_j$; however $a_{n-1} + a_j \leq a_n$ for $j \leq n-2$. Therefore $j = n-1$ or $j = n$.

For $j = n-1$ we obtain $3a_{n-1} = k(a_n + a_{n-1})$ with k an integer, and it is straightforward that $k = 1$ ($k \leq 0$ and $k \geq 3$ contradict $0 < a_{n-1} < a_n$; $k = 2$ leads to $a_{n-1} = 2a_n > a_{n-1}$). Thus $3a_{n-1} = a_n + a_{n-1}$, i. e. $a_n = 2a_{n-1}$.

Similarly, if $j = n$ then $3a_n = k(a_n + a_{n-1})$ for some integer k, and only $k = 2$ is possible. Hence $a_n = 2a_{n-1}$ holds true in both cases remaining, $j = n-1$ and $j = n$.

Now $a_n = 2a_{n-1}$ implies that the sum $a_{n-1} + a_1$ is strictly between $a_n/2$ and a_n. But a_{n-1} and a_1 are distinct as $n \geq 3$, so it follows from the above that $a_{n-1} + a_1$ divides a_n. This provides the desired contradiction.

N3. Let $a_0, a_1, a_2, \ldots$ be a sequence of positive integers such that the greatest common divisor of any two consecutive terms is greater than the preceding term; in symbols, $\gcd(a_i, a_{i+1}) > a_{i-1}$. Prove that $a_n \geq 2^n$ for all $n \geq 0$.

Solution. Since $a_i \geq \gcd(a_i, a_{i+1}) > a_{i-1}$, the sequence is strictly increasing. In particular $a_0 \geq 1$, $a_1 \geq 2$. For each $i \geq 1$ we also have $a_{i+1} - a_i \geq \gcd(a_i, a_{i+1}) > a_{i-1}$, and consequently $a_{i+1} \geq a_i + a_{i-1} + 1$. Hence $a_2 \geq 4$ and $a_3 \geq 7$. The equality $a_3 = 7$ would force equalities in the previous estimates, leading to $\gcd(a_2, a_3) = \gcd(4, 7) > a_1 = 2$, which is false. Thus $a_3 \geq 8$; the result is valid for $n = 0, 1, 2, 3$. These are the base cases for a proof by induction.

Take an $n \geq 3$ and assume that $a_i \geq 2^i$ for $i = 0, 1, \ldots, n$. We must show that $a_{n+1} \geq 2^{n+1}$. Let $\gcd(a_n, a_{n+1}) = d$. We know that $d > a_{n-1}$. The induction claim is reached immediately in the following cases:

$$\begin{array}{lll} \text{if } a_{n+1} \geq 4d & \text{then} & a_{n+1} > 4a_{n-1} \geq 4 \cdot 2^{n-1} = 2^{n+1}\,; \\ \text{if } a_n \geq 3d & \text{then} & a_{n+1} \geq a_n + d \geq 4d > 4a_{n-1} \geq 4 \cdot 2^{n-1} = 2^{n+1}\,; \\ \text{if } a_n = d & \text{then} & a_{n+1} \geq a_n + d = 2a_n \geq 2 \cdot 2^n = 2^{n+1}. \end{array}$$

The only remaining possibility is that $a_n = 2d$ and $a_{n+1} = 3d$, which we assume for the sequel. So $a_{n+1} = \frac{3}{2}a_n$.

Let now $\gcd(a_{n-1}, a_n) = d'$; then $d' > a_{n-2}$. Write $a_n = md'$ (m an integer). Keeping in mind that $d' \leq a_{n-1} < d$ and $a_n = 2d$, we get that $m \geq 3$. Also $a_{n-1} < d = \frac{1}{2}md'$, $a_{n+1} = \frac{3}{2}md'$. Again we single out the cases which imply the induction claim immediately:

$$\begin{array}{lll} \text{if } m \geq 6 & \text{then} & a_{n+1} = \frac{3}{2}md' \geq 9d' > 9a_{n-2} \geq 9 \cdot 2^{n-2} > 2^{n+1}\,; \\ \text{if } 3 \leq m \leq 4 & \text{then} & a_{n-1} < \frac{1}{2} \cdot 4d', \text{ and hence } a_{n-1} = d', \\ & & \qquad a_{n+1} = \frac{3}{2}ma_{n-1} \geq \frac{3}{2} \cdot 3a_{n-1} \geq \frac{9}{2} \cdot 2^{n-1} > 2^{n+1}. \end{array}$$

So we are left with the case $m = 5$, which means that $a_n = 5d'$, $a_{n+1} = \frac{15}{2}d'$, $a_{n-1} < d = \frac{5}{2}d'$. The last relation implies that a_{n-1} is either d' or $2d'$. Anyway, $a_{n-1} | 2d'$.

The same pattern repeats once more. We denote $\gcd(a_{n-2}, a_{n-1}) = d''$; then $d'' > a_{n-3}$. Because d'' is a divisor of a_{n-1}, hence also of $2d'$, we may write $2d' = m'd''$ (m' an integer). Since $d'' \leq a_{n-2} < d'$, we get $m' \geq 3$. Also, $a_{n-2} < d' = \frac{1}{2}m'd''$, $a_{n+1} = \frac{15}{2}d' = \frac{15}{4}m'd''$. As before, we consider the cases:

$$\begin{array}{lll} \text{if } m' \geq 5 & \text{then} & a_{n+1} = \frac{15}{4}m'd'' \geq \frac{75}{4}d'' > \frac{75}{4}a_{n-3} \geq \frac{75}{4} \cdot 2^{n-3} > 2^{n+1}\,; \\ \text{if } 3 \leq m' \leq 4 & \text{then} & a_{n-2} < \frac{1}{2} \cdot 4d'', \text{ and hence } a_{n-2} = d'', \\ & & \qquad a_{n+1} = \frac{15}{4}m'a_{n-2} \geq \frac{15}{4} \cdot 3a_{n-2} \geq \frac{45}{4} \cdot 2^{n-2} > 2^{n+1}. \end{array}$$

Both of them have produced the induction claim. But now there are no cases left. Induction is complete; the inequality $a_n \geq 2^n$ holds for all n.

N4. Let n be a positive integer. Show that the numbers

$$\binom{2^n-1}{0},\quad \binom{2^n-1}{1},\quad \binom{2^n-1}{2},\quad \ldots,\quad \binom{2^n-1}{2^{n-1}-1}$$

are congruent modulo 2^n to $1, 3, 5, \ldots, 2^n-1$ in some order.

Solution 1. It is well-known that all these numbers are odd. So the assertion that their remainders (mod 2^n) make up a permutation of $\{1, 3, \ldots, 2^n-1\}$ is equivalent just to saying that these remainders are all distinct. We begin by showing that

$$\binom{2^n-1}{2k} + \binom{2^n-1}{2k+1} \equiv 0 \pmod{2^n} \quad \text{and} \quad \binom{2^n-1}{2k} \equiv (-1)^k \binom{2^{n-1}-1}{k} \pmod{2^n}. \tag{1}$$

The first relation is immediate, as the sum on the left is equal to $\binom{2^n}{2k+1} = \frac{2^n}{2k+1}\binom{2^n-1}{2k}$, hence is divisible by 2^n. The second relation:

$$\binom{2^n-1}{2k} = \prod_{j=1}^{2k} \frac{2^n-j}{j} = \prod_{i=1}^{k} \frac{2^n-(2i-1)}{2i-1} \cdot \prod_{i=1}^{k} \frac{2^{n-1}-i}{i} \equiv (-1)^k \binom{2^{n-1}-1}{k} \pmod{2^n}.$$

This prepares ground for a proof of the required result by induction on n. The base case $n=1$ is obvious. Assume the assertion is true for $n-1$ and pass to n, denoting $a_k = \binom{2^{n-1}-1}{k}$, $b_m = \binom{2^n-1}{m}$. The induction hypothesis is that all the numbers a_k $(0 \le k < 2^{n-2})$ are distinct (mod 2^{n-1}); the claim is that all the numbers b_m $(0 \le m < 2^{n-1})$ are distinct (mod 2^n).

The congruence relations (1) are restated as

$$b_{2k} \equiv (-1)^k a_k \equiv -b_{2k+1} \pmod{2^n}. \tag{2}$$

Shifting the exponent in the first relation of (1) from n to $n-1$ we also have the congruence $a_{2i+1} \equiv -a_{2i} \pmod{2^{n-1}}$. We hence conclude:

If, for some $j, k < 2^{n-2}$, $a_k \equiv -a_j \pmod{2^{n-1}}$, *then* $\{j,k\} = \{2i, 2i+1\}$ *for some* i. (3)

This is so because in the sequence $(a_k\colon k < 2^{n-2})$ each term a_j is complemented to 0 (mod 2^{n-1}) by only one other term a_k, according to the induction hypothesis.

From (2) we see that $b_{4i} \equiv a_{2i}$ and $b_{4i+3} \equiv a_{2i+1} \pmod{2^n}$. Let

$$M = \{m\colon 0 \le m < 2^{n-1},\ m \equiv 0 \text{ or } 3 \pmod 4\}, \quad L = \{l\colon 0 \le l < 2^{n-1},\ l \equiv 1 \text{ or } 2 \pmod 4\}.$$

The last two congruences take on the unified form

$$b_m \equiv a_{\lfloor m/2 \rfloor} \pmod{2^n} \quad \text{for all} \quad m \in M. \tag{4}$$

Thus all the numbers b_m for $m \in M$ are distinct (mod 2^n) because so are the numbers a_k (they are distinct (mod 2^{n-1}), hence also (mod 2^n)).

Every $l \in L$ is paired with a unique $m \in M$ into a pair of the form $\{2k, 2k+1\}$. So (2) implies that also all the b_l for $l \in L$ are distinct (mod 2^n). It remains to eliminate the possibility that $b_m \equiv b_l \pmod{2^n}$ for some $m \in M$, $l \in L$.

Suppose that such a situation occurs. Let $m' \in M$ be such that $\{m', l\}$ is a pair of the form $\{2k, 2k+1\}$, so that (see (2)) $b_{m'} \equiv -b_l \pmod{2^n}$. Hence $b_{m'} \equiv -b_m \pmod{2^n}$. Since both m' and m are in M, we have by (4) $b_{m'} \equiv a_j$, $b_m \equiv a_k \pmod{2^n}$ for $j = \lfloor m'/2 \rfloor$, $k = \lfloor m/2 \rfloor$.

Then $a_j \equiv -a_k \pmod{2^n}$. Thus, according to (3), $j = 2i$, $k = 2i+1$ for some i (or vice versa). The equality $a_{2i+1} \equiv -a_{2i} \pmod{2^n}$ now means that $\binom{2^{n-1}-1}{2i} + \binom{2^{n-1}-1}{2i+1} \equiv 0 \pmod{2^n}$. However, the sum on the left is equal to $\binom{2^{n-1}}{2i+1}$. A number of this form cannot be divisible by 2^n. This is a contradiction which concludes the induction step and proves the result.

Solution 2. We again proceed by induction, writing for brevity $N = 2^{n-1}$ and keeping notation $a_k = \binom{N-1}{k}$, $b_m = \binom{2N-1}{m}$. Assume that the result holds for the sequence $(a_0, a_1, a_2, \ldots, a_{N/2-1})$. In view of the symmetry $a_{N-1-k} = a_k$ this sequence is a permutation of $(a_0, a_2, a_4, \ldots, a_{N-2})$. So the induction hypothesis says that this latter sequence, taken (mod N), is a permutation of $(1, 3, 5, \ldots, N-1)$. Similarly, the induction claim is that $(b_0, b_2, b_4, \ldots, b_{2N-2})$, taken (mod $2N$), is a permutation of $(1, 3, 5, \ldots, 2N-1)$.

In place of the congruence relations (2) we now use the following ones,

$$b_{4i} \equiv a_{2i} \pmod{N} \qquad \text{and} \qquad b_{4i+2} \equiv b_{4i} + N \pmod{2N}. \tag{5}$$

Given this, the conclusion is immediate: the first formula of (5) together with the induction hypothesis tells us that $(b_0, b_4, b_8, \ldots, b_{2N-4})$ (mod N) is a permutation of $(1, 3, 5, \ldots, N-1)$. Then the second formula of (5) shows that $(b_2, b_6, b_{10}, \ldots, b_{2N-2})$ (mod N) is exactly the same permutation; moreover, this formula distinguishes (mod $2N$) each b_{4i} from b_{4i+2}.

Consequently, these two sequences combined represent (mod $2N$) a permutation of the sequence $(1, 3, 5, \ldots, N-1,\ N+1, N+3, N+5, \ldots, N+N-1)$, and this is precisely the induction claim.

Now we prove formulas (5); we begin with the second one. Since $b_{m+1} = b_m \cdot \frac{2N-m-1}{m+1}$,

$$b_{4i+2} = b_{4i} \cdot \frac{2N-4i-1}{4i+1} \cdot \frac{2N-4i-2}{4i+2} = b_{4i} \cdot \frac{2N-4i-1}{4i+1} \cdot \frac{N-2i-1}{2i+1}.$$

The desired congruence $b_{4i+2} \equiv b_{4i} + N$ may be multiplied by the odd number $(4i+1)(2i+1)$, giving rise to a chain of successively equivalent congruences:

$$\begin{aligned}
b_{4i}(2N-4i-1)(N-2i-1) &\equiv (b_{4i}+N)(4i+1)(2i+1) && \pmod{2N},\\
b_{4i}(2i+1-N) &\equiv (b_{4i}+N)(2i+1) && \pmod{2N},\\
(b_{4i}+2i+1)N &\equiv 0 && \pmod{2N};
\end{aligned}$$

and the last one is satisfied, as b_{4i} is odd. This settles the second relation in (5).

The first one is proved by induction on i. It holds for $i = 0$. Assume $b_{4i} \equiv a_{2i}$ (mod $2N$) and consider $i+1$:

$$b_{4i+4} = b_{4i+2} \cdot \frac{2N-4i-3}{4i+3} \cdot \frac{2N-4i-4}{4i+4}; \qquad a_{2i+2} = a_{2i} \cdot \frac{N-2i-1}{2i+1} \cdot \frac{N-2i-2}{2i+2}.$$

Both expressions have the fraction $\frac{N-2i-2}{2i+2}$ as the last factor. Since $2i+2 < N = 2^{n-1}$, this fraction reduces to ℓ/m with ℓ and m odd. In showing that $b_{4i+4} \equiv a_{2i+2}$ (mod $2N$), we may ignore this common factor ℓ/m. Clearing other odd denominators reduces the claim to

$$b_{4i+2}(2N-4i-3)(2i+1) \equiv a_{2i}(N-2i-1)(4i+3) \pmod{2N}.$$

By the inductive assumption (saying that $b_{4i} \equiv a_{2i}$ (mod $2N$)) and by the second relation of (5), this is equivalent to

$$(b_{4i}+N)(2i+1) \equiv b_{4i}(2i+1-N) \pmod{2N},$$

a congruence which we have already met in the preceding proof a few lines above. This completes induction (on i) and the proof of (5), hence also the whole solution.

Comment. One can avoid the words *congruent modulo* in the problem statement by rephrasing the assertion into: *Show that these numbers leave distinct remainders in division by 2^n.*

N5. For every $n \in \mathbb{N}$ let $d(n)$ denote the number of (positive) divisors of n. Find all functions $f\colon \mathbb{N} \to \mathbb{N}$ with the following properties:

(i) $d(f(x)) = x$ for all $x \in \mathbb{N}$;

(ii) $f(xy)$ divides $(x-1)y^{xy-1}f(x)$ for all $x, y \in \mathbb{N}$.

Solution. There is a unique solution: the function $f\colon \mathbb{N} \to \mathbb{N}$ defined by $f(1) = 1$ and

$$f(n) = p_1^{p_1^{a_1}-1} p_2^{p_2^{a_2}-1} \cdots p_k^{p_k^{a_k}-1} \text{ where } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ is the prime factorization of } n > 1. \quad (1)$$

Direct verification shows that this function meets the requirements.

Conversely, let $f\colon \mathbb{N} \to \mathbb{N}$ satisfy (i) and (ii). Applying (i) for $x = 1$ gives $d(f(1)) = 1$, so $f(1) = 1$. In the sequel we prove that (1) holds for all $n > 1$. Notice that $f(m) = f(n)$ implies $m = n$ in view of (i). The formula $d\left(p_1^{b_1} \cdots p_k^{b_k}\right) = (b_1 + 1) \cdots (b_k + 1)$ will be used throughout.

Let p be a prime. Since $d(f(p)) = p$, the formula just mentioned yields $f(p) = q^{p-1}$ for some prime q; in particular $f(2) = q^{2-1} = q$ is a prime. We prove that $f(p) = p^{p-1}$ for all primes p.

Suppose that p is odd and $f(p) = q^{p-1}$ for a prime q. Applying (ii) first with $x = 2$, $y = p$ and then with $x = p$, $y = 2$ shows that $f(2p)$ divides both $(2-1)p^{2p-1}f(2) = p^{2p-1}f(2)$ and $(p-1)2^{2p-1}f(p) = (p-1)2^{2p-1}q^{p-1}$. If $q \neq p$ then the odd prime p does not divide $(p-1)2^{2p-1}q^{p-1}$, hence the greatest common divisor of $p^{2p-1}f(2)$ and $(p-1)2^{2p-1}q^{p-1}$ is a divisor of $f(2)$. Thus $f(2p)$ divides $f(2)$ which is a prime. As $f(2p) > 1$, we obtain $f(2p) = f(2)$ which is impossible. So $q = p$, i. e. $f(p) = p^{p-1}$.

For $p = 2$ the same argument with $x = 2$, $y = 3$ and $x = 3$, $y = 2$ shows that $f(6)$ divides both $3^5 f(2)$ and $2^6 f(3) = 2^6 3^2$. If the prime $f(2)$ is odd then $f(6)$ divides $3^2 = 9$, so $f(6) \in \{1, 3, 9\}$. However then $6 = d(f(6)) \in \{d(1), d(3), d(9)\} = \{1, 2, 3\}$ which is false. In conclusion $f(2) = 2$.

Next, for each $n > 1$ the prime divisors of $f(n)$ are among the ones of n. Indeed, let p be the least prime divisor of n. Apply (ii) with $x = p$ and $y = n/p$ to obtain that $f(n)$ divides $(p-1)y^{n-1}f(p) = (p-1)y^{n-1}p^{p-1}$. Write $f(n) = \ell P$ where ℓ is coprime to n and P is a product of primes dividing n. Since ℓ divides $(p-1)y^{n-1}p^{p-1}$ and is coprime to $y^{n-1}p^{p-1}$, it divides $p-1$; hence $d(\ell) \le \ell < p$. But (i) gives $n = d(f(n)) = d(\ell P)$, and $d(\ell P) = d(\ell)d(P)$ as ℓ and P are coprime. Therefore $d(\ell)$ is a divisor of n less than p, meaning that $\ell = 1$ and proving the claim.

Now (1) is immediate for prime powers. If p is a prime and $a \ge 1$, by the above the only prime factor of $f(p^a)$ is p (a prime factor does exist as $f(p^a) > 1$). So $f(p^a) = p^b$ for some $b \ge 1$, and (i) yields $p^a = d(f(p^a)) = d\left(p^b\right) = b + 1$. Hence $f(p^a) = p^{p^a - 1}$, as needed.

Let us finally show that (1) is true for a general $n > 1$ with prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. We saw that the prime factorization of $f(n)$ has the form $f(n) = p_1^{b_1} \cdots p_k^{b_k}$. For $i = 1, \ldots, k$, set $x = p_i^{a_i}$ and $y = n/x$ in (ii) to infer that $f(n)$ divides $\left(p_i^{a_i} - 1\right) y^{n-1} f\left(p_i^{a_i}\right)$. Hence $p_i^{b_i}$ divides $\left(p_i^{a_i} - 1\right) y^{n-1} f\left(p_i^{a_i}\right)$, and because $p_i^{b_i}$ is coprime to $\left(p_i^{a_i} - 1\right) y^{n-1}$, it follows that $p_i^{b_i}$ divides $f\left(p_i^{a_i}\right) = p_i^{p_i^{a_i}-1}$. So $b_i \le p_i^{a_i} - 1$ for all $i = 1, \ldots, k$. Combined with (i), these conclusions imply

$$p_1^{a_1} \cdots p_k^{a_k} = n = d(f(n)) = d\left(p_1^{b_1} \cdots p_k^{b_k}\right) = (b_1 + 1) \cdots (b_k + 1) \le p_1^{a_1} \cdots p_k^{a_k}.$$

Hence all inequalities $b_i \le p_i^{a_i} - 1$ must be equalities, $i = 1, \ldots, k$, implying that (1) holds true. The proof is complete.

N6. Prove that there exist infinitely many positive integers n such that n^2+1 has a prime divisor greater than $2n+\sqrt{2n}$.

Solution. Let $p \equiv 1 \pmod 8$ be a prime. The congruence $x^2 \equiv -1 \pmod p$ has two solutions in $[1, p-1]$ whose sum is p. If n is the smaller one of them then p divides n^2+1 and $n \le (p-1)/2$. We show that $p > 2n+\sqrt{10n}$.

Let $n = (p-1)/2 - \ell$ where $\ell \ge 0$. Then $n^2 \equiv -1 \pmod p$ gives

$$\left(\frac{p-1}{2}-\ell\right)^2 \equiv -1 \pmod p \qquad \text{or} \qquad (2\ell+1)^2+4 \equiv 0 \pmod p.$$

Thus $(2\ell+1)^2+4 = rp$ for some $r \ge 0$. As $(2\ell+1)^2 \equiv 1 \equiv p \pmod 8$, we have $r \equiv 5 \pmod 8$, so that $r \ge 5$. Hence $(2\ell+1)^2+4 \ge 5p$, implying $\ell \ge \left(\sqrt{5p-4}-1\right)/2$. Set $\sqrt{5p-4} = u$ for clarity; then $\ell \ge (u-1)/2$. Therefore

$$n = \frac{p-1}{2} - \ell \le \frac{1}{2}\left(p-u\right).$$

Combined with $p = (u^2+4)/5$, this leads to $u^2 - 5u - 10n + 4 \ge 0$. Solving this quadratic inequality with respect to $u \ge 0$ gives $u \ge \left(5+\sqrt{40n+9}\right)/2$. So the estimate $n \le \left(p-u\right)/2$ leads to

$$p \ge 2n + u \ge 2n + \frac{1}{2}\left(5+\sqrt{40n+9}\right) > 2n+\sqrt{10n}.$$

Since there are infinitely many primes of the form $8k+1$, it follows easily that there are also infinitely many n with the stated property.

Comment. By considering the prime factorization of the product $\prod_{n=1}^{N}(n^2+1)$, it can be obtained that its greatest prime divisor is at least $cN\log N$. This could improve the statement as $p > n\log n$.

However, the proof applies some advanced information about the distribution of the primes of the form $4k+1$, which is inappropriate for high schools contests.