

Algebra

- A1** (IMO 1). Given any set $A = \{a_1, a_2, a_3, a_4\}$ of four distinct positive integers, we denote the sum $a_1 + a_2 + a_3 + a_4$ by s_A . Let n_A denote the number of pairs (i, j) with $1 \leq i < j \leq 4$ for which $a_i + a_j$ divides s_A . Find all sets A of four distinct positive integers which achieve the largest possible value of n_A .

Answer. All sets in the form $\{d, 5d, 7d, 11d\}$ and $\{d, 11d, 19d, 29d\}$ with $d \in \mathbb{N}$.

Solution. We first show that $n_A \leq 4$. Since the numbers are distinct, we can order them as $a_1 < a_2 < a_3 < a_4$ and we have $a_3 + a_4 < s_A = a_1 + a_2 + a_3 + a_4 < a_3 + a_4 + a_3 + a_4 = 2(a_3 + a_4)$ we have $a_3 + a_4 \nmid s_A$. Similarly $a_2 + a_4 < s_A = a_1 + a_2 + a_3 + a_4 < a_2 + a_2 + a_4 + a_4 = 2(a_2 + a_4)$ we also have $a_2 + a_4 \nmid s_A$. Therefore to achieve the maximum we need $n_A = 4$ (as we will show later that this is attainable), we need all $a_1 + a_2, a_1 + a_3, a_1 + a_4, a_2 + a_3$ to divide s_A . We can also see that this condition forces $a_1 + a_4$ and $a_2 + a_3$ to divide each other, and therefore these two sums must be equal, i.e. $a_1 + a_4 = a_2 + a_3 = s_A$.

Now there must exist integers k and ℓ such that $s_A = k(a_1 + a_2) = \ell(a_1 + a_3)$, so $a_1 + a_2 = \frac{1}{k}s_A$ and $a_1 + a_3 = \frac{1}{\ell}s_A$. Adding these up gives $\frac{s_A}{2} = a_2 + a_3 < 2a_1 + a_2 + a_3 = s_A(\frac{1}{k} + \frac{1}{\ell})$ and we have both $a_1 + a_2 < a_2 + a_3$ and $a_1 + a_2 < a_2 + a_3$, so $k, \ell > 2$. However $\frac{1}{k} + \frac{1}{\ell} > \frac{1}{2}$ we can easily see the the smaller of them, i.e. ℓ , must be equal to 3, and k must be equal to 4 or 5.

If $k = 4$ then we can solve $a_1, a_2, a_3, a_4 = (d, 5d, 7d, 11d)$ and if $k = 5$ we can solve $a_1, a_2, a_3, a_4 = (d, 11d, 19d, 29d)$. It's not hard to show that these answers work.

Remark 1: my solution in the real contest is way messier than this, where I wrote $a_4 = a_2 + a_3 - a_1$ and solve the other variables in terms of k and ℓ (though it worked in the end).

Remark 2: the relation $\frac{1}{k} + \frac{1}{\ell} > \frac{1}{2}$ also (kind of) resembles the reason why there are only 5 platonic solids.

- A2** Determine all sequences $(x_1, x_2, \dots, x_{2011})$ of positive integers, such that for every positive integer n there exists an integer a with

$$\sum_{j=1}^{2011} jx_j^n = a^{n+1} + 1$$

Answer. The only possible sequence is $x_1 = 1$ and $a = x_2 = \dots = x_{2011} = 2 + 3 + \dots + 2011$.

Solution. First, for each j we have $\sum_{j=1}^{2011} jx_j^n - 1 \geq jx_j^n$ since each term is positive.

Also using the notion of limits $\lim_{n \rightarrow \infty} (jx_j^n)^{\frac{1}{n+1}} = \lim_{n \rightarrow \infty} j^{\frac{1}{n+1}} x_j^{\frac{n}{n+1}} = j^0 x_j^1 = x_j$, so we can conclude that $a \geq x_j$ for n sufficiently large. In other words, for n sufficiently large we have $a \geq X = \max\{x_1, x_2, \dots, x_{2011}\}$. On the other hand we have $\sum_{j=1}^{2011} jx_j^n - 1 \leq X^n(1 + \dots + 2011) - 1 < CX^n$ where $C = 1 + \dots + 2011$. As usual $\lim_{n \rightarrow \infty} (CX^n)^{\frac{1}{n+1}} = C^{\frac{1}{n+1}} X^{\frac{n}{n+1}} = C^0 X^1 = X$ so we have $a \leq X$ too for n sufficiently large, too. Hence we have $a = X$ for all sufficiently large n .

Now we have $X^{n+1} = \sum_{j=1}^{2011} jx_j^n - 1$, and dividing each side by X^n we have $X = \sum_{j=1}^{2011} j \left(\frac{x_j}{X}\right)^n - \left(\frac{1}{X}\right)^n$ for all sufficiently large n . Since each $x_j \leq X$, $j \left(\frac{x_j}{X}\right)^n$ converges to j if $x_j = X$ and 0 if $x_j < X$ (when $n \rightarrow \infty$). Thus it's not hard to see that

$$X = \lim_{n \rightarrow \infty} \sum_{j=1}^{2011} j \left(\frac{x_j}{X}\right)^n - \left(\frac{1}{X}\right)^n = \sum_{1 \leq j \leq 2011, x_j = X} j$$

and therefore for n sufficiently large we have

$$\begin{aligned} \sum_{1 \leq j \leq 2011, x_j = X} j &= \sum_{j=1}^{2011} j \left(\frac{x_j}{X} \right)^n - \left(\frac{1}{X} \right)^n \\ &= \sum_{1 \leq j \leq 2011, x_j = X} j \left(\frac{x_j}{X} \right)^n + \sum_{1 \leq j \leq 2011, x_j < X} j \left(\frac{x_j}{X} \right)^n - \left(\frac{1}{X} \right)^n \\ &= \sum_{1 \leq j \leq 2011, x_j = X} j + \sum_{1 \leq j \leq 2011, x_j < X} j \left(\frac{x_j}{X} \right)^n - \left(\frac{1}{X} \right)^n \end{aligned}$$

which we can conclude that $\sum_{1 \leq j \leq 2011, x_j < X} j \left(\frac{x_j}{X} \right)^n - \left(\frac{1}{X} \right)^n = 0$ for all sufficiently large

n . Multiplying by X^n again we get $1 = \sum_{1 \leq j \leq 2011, x_j < X} j x_j^n$ for all sufficiently large n .

Thus the only j that can have $x_j < X$ is $j = 1$, in which $x_1 = 1$. The other j has $x_j = X = \sum_{1 \leq j \leq 2011, x_j = X} j = 2 + \dots + 2011$, as desired.

A3 Determine all pairs (f, g) of functions from the set of real numbers to itself that satisfy

$$g(f(x+y)) = f(x) + (2x+y)g(y) \quad (1)$$

for all real numbers x and y .

Answer. Either $f \equiv g \equiv 0$, or $f(x) = x^2 + C$ and $g(x) = x$ for some constant C . The first one gives both side $= 0$; the second one gives both sides $= 0 \cdot x^2 + C$.

Solution. We'll first show that g is linear. Fix constant c , and substitute $x+c$ into x and $-x$ into y into Eqn 1, we get

$$g(f(c)) = f(x+c) + (x+2c)g(-x) \quad (2)$$

and comparing $x-c$ and $y-c$ in place of x in 2 we get

$$f(x) - f(y) = (y+c)g(-(y-c)) - (x+c)g(-(x-c)) \quad (3)$$

which holds for all x, y , and c . Thus 3 tells us that, compared to $c=0$,

$$f(x) - f(y) = (y+c)g(-(y-c)) - (x+c)g(-(x-c)) = yg(-y) - xg(-x) \quad (4)$$

and similarly, consider substituting $x-c, y-c$ into 3 and $-c$ and 0 , respectively into c gives

$$f(x-c) - f(y-c) = (y-c)g(-(y-c)) - (x-c)g(-(x-c)) = (y-2c)g(-y) - (x-2c)g(-x) \quad (5)$$

Thus subtracting 4 by 5 (matching like terms) give

$$2cg(-(y-c)) - 2cg(-(x-c)) = 2cg(-y) - 2cg(-x) \quad (6)$$

i.e. for all $c \neq 0$, $g(-(y-c)) - g(-(x-c)) = g(-y) - g(-x)$, meaning that $(-x, g(-x)), (-y, g(-y))$ and $(-(x-c), g(-(x-c))), (-(y-c), g(-(y-c)))$ are two lines with the same slope. This would mean there exists m (the gradient), d_1, d_2 such that

$$g(-x) = -mx + d_1, g(-y) = -my + d_1, g(-(x-c)) = -m(x-c) + d_2, g(-(y-c)) = -m(y-c) + d_2$$

which, substituting into 4 gives

$$(y-x)d_1 = (y-x)d_2$$

so whenever $x \neq y$, we have $d_1 = d_2$. This means when $x \neq y, c \neq 0$ we have the four points

$$(-x, g(-x)), (-y, g(-y)) - (x - c, g(-(x - c))), (-(y - c), g(-(y - c)))$$

all lie on the same line. Thus fixing some x and y (say, 0 and 1) and consider all other $c \neq 0$ we have all $(x, g(x))$ on the same line, hence g linear.

Now we can write $g(x) = mx + c$, and substitute this into 1 once again. If $m = 1$ then considering $y = 0$ we have $f(x) + c = f(x) + 2xc$ for all x , so $c = 0$ (i.e. $g(x) = x$). Now putting $x = 0$ into 1 and $g(x) = x$ gives $f(y) = f(0) + y^2$, establishing $f(x) = x^2 + C$.

If $m \neq 1$, then with $y = 0$ into 1 we have $mf(x) + c = f(x) + 2xc$, and therefore $f(x) = \frac{(2x-1)c}{m-1}$. This implies

$$m \left(\frac{(2x + 2y - 1)c}{m - 1} \right) + c = \frac{(2x - 1)c}{m - 1} + (2x + y)(my + c)$$

The only combination that works for all x and y is $m = c = 0$.

- A5** Prove that for every positive integer n , the set $\{2, 3, 4, \dots, 3n + 1\}$ can be partitioned into n triples in such a way that the numbers from each triple are the lengths of the sides of some obtuse triangle.

Solution. The idea is to form the triples (a, b, c) such that, if $a < b < c$ then $c - b \in \Theta(a)$ as compared to other a (and when n grows big). We form the n triples in the following way: all the n smallest numbers $2, \dots, n + 1$ will be in different triples as the smallest element in the triple. For the remaining $2n$ numbers, we need the following: let k be the greatest number such that $2^0 + 2^1 + \dots + 2^k \leq n$, then $n = 2^0 + 2^1 + \dots + 2^k + \ell$ with $\ell < 2^{k+1}$. We now sort $2^0, \dots, 2^k, \ell$ in nondecreasing order a_1, a_2, \dots, a_{k+1} (ℓ could be 0 for degenerate case, and we shall omit it for time being). For each $i = 1, 2, \dots, n$, let j be the minimal index with $a_1 + a_2 + \dots + a_j \leq i$. We now name the i -th triple as follow: let $a_1 + \dots + a_{j-1} = p$, then the i -th triple is $(i + 1, n + 1 + 2p + (i - p), n + 1 + 2p + a_j + (i - p))$.

To show that this triple works, we first need to see that it's disjoint and all within the range $\{2, 3, \dots, 3n + 1\}$. Observe that the first element $i + 1$ corresponds to the i -th triple, so they are in the range $\{2, \dots, n + 1\}$. Then, the partition of a_1, a_2, \dots, a_{k+1} puts them into $k + 1$ different "buckets". In the explanation above, i is in the j -th bucket and the middle elements in this j -th bucket are in between $n + 1 + 2p + 1$ to $n + 1 + 2p + a_j$ (inclusive) and the largest elements in this bucket are in between $n + 1 + 2p + a_j + 1$ and $n + 1 + 2p + 2a_j$, so recall that $p = a_1 + \dots + a_{j-1}$ we infer that the numbers are all distinct from $n + 1 + 2(a_1 + \dots + a_{j-1}) + 1$ too $n + 1 + 2(a_1 + \dots + a_j)$. The largest possible number (considering all j 's) is then $n + 1 + 2(a_1 + \dots + a_{k+1}) = n + 1 + 2n = 3n + 1$, completing the claim.

We now show that the resulting triples are the side lengths of obtuse triangles. To this end, if $a < b < c$ are the elements of the triples then we need $c - b < a$ but then $(c - b)(c + b) = c^2 - b^2 > a^2$. Let's use the example from above, i.e. our description. In the triple $(i + 1, n + 1 + 2p + (i - p), n + 1 + 2p + a_j + (i - p))$ we have $a = i + 1$, $b = n + 1 + 2p + (i - p)$ and $c = n + 1 + 2p + a_j + (i - p)$. We have $c - b = a_j$. Recall also that, $a_1 + a_2 + \dots + a_{j-1} < i \leq a_1 + a_2 + \dots + a_j$. For $a_j > 1$, m is the biggest number such that $2^m < a_j$ then the numbers $1, 2, \dots, 2^m$ must all appear before a_j so $a_1 + \dots + a_{j-1} \geq 1 + \dots + 2^m = 2^{m+1} - 1$. By the maximality of m we also have $a_j \leq 2^{m+1}$, and since $i > a_1 + \dots + a_{j-1} \geq 2^{m+1} - 1$, $i \geq 2^{m+1}$ and so $a = i + 1 > 2^{m+1} \geq a_j = c - b$, so (a, b, c) is indeed side of a triangle.

To see from above that (a, b, c) is indeed obtuse, we have $c^2 - b^2 = (c - b)(c + b) = a_j(a_j + 2(n + 1 + 2p + (i - p)))$ and we need to show that this is strictly greater than

$a^2 = (i+1)^2$. We first notice that i is at most $a_1 + a_2 + \cdots + a_j$, therefore:

$$\begin{aligned} \frac{i+1}{a_j} &\leq \frac{a_1 + a_2 + \cdots + a_j + 1}{a_j} \\ &= \frac{a_1 + a_2 + \cdots + a_{j-1} + 1}{a_j} + 1 \end{aligned}$$

If a_j is not in the form 2^m then $a_j = 2^{j-2} + c$ with $a_\ell = 2^{\ell-1}$ for $\ell < j$ so $a_1 + a_2 + \cdots + a_{j-1} + 1 = 1 + 2 + \cdots + 2^{j-2} + 1 = 2^{j-1}$ so $\frac{a_1 + a_2 + \cdots + a_{j-1} + 1}{a_j} + 1 = \frac{2^{j-1}}{2^{j-2} + c} + 1 \leq 2 + 1 = 3$; otherwise $a_j = 2^m$ and $a_1 + \cdots + a_j \leq 1 + 2 + \cdots + 2^m = 2^{m+1} - 1$ so in this case we also have $\frac{a_1 + a_2 + \cdots + a_{j-1} + 1}{a_j} + 1 \leq 3$, too. This means, $i+1 \leq 3a_j$. Next, we investigate the number $a_j + 2(n+1+2p+(i-p)) = a_j + 2(n+1) + 4p + 2(i-p) \geq a_j + 2i + 4p + 2(i-p)$. We have $i-p \geq 1$ since $p = a_1 + \cdots + a_{j-1} < i$. Also, recall that $i+1 \leq a_1 + a_2 + \cdots + a_j + 1$ so $a_j + 4p = a_j + 4(a_1 + \cdots + a_{j-1}) \geq a_j + a_1 + \cdots + a_{j-1}$, with equality only if $a_1 + \cdots + a_{j-1} = p = 0$. This only happens when $i = 1$, in which case we have $(2, n+2, n+3)$ which is obtuse since $(n+3)^2 - (n+2)^2 = 2n+5 > 4$. For $i > 1$ we have $p \geq 1$ so $a_j + 4(a_1 + \cdots + a_{j-1}) \geq a_j + a_1 + \cdots + a_{j-1} + 3 > i+1$, so $a_j + 4p > i+1$ and $2(n+1) + 2(i-p) \geq 2i+2$, resulting in $a_j + 2(n+1+2p+(i-p)) > 3(i+1)$. Summarizing above, we have $c-b = a_j \geq \frac{i+1}{3} = \frac{a}{3}$ and $c+b > 3(i+1) = 3a$. Thus $c^2 - b^2 = (c-b)(c+b) > \frac{a}{3} \times 3a = a^2$, as desired.

- A6** (IMO 3) Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be a real-valued function defined on the set of real numbers that satisfies

$$f(x+y) \leq yf(x) + f(f(x))$$

for all real numbers x and y . Prove that $f(x) = 0$ for all $x \leq 0$.

Solution. As per the official solution, we need to first show that $f(x) \leq 0$ for all x . Let x_0 be a number such that $f(x_0) > 0$. Then $f(x_0 + y) \leq yf(x_0) + f(f(x_0))$. This means, for each threshold M , for all $y < \frac{M - f(f(x_0))}{f(x_0)}$ we have $f(x_0 + y) \leq yf(x_0) + f(f(x_0)) < M$. This means, for all sufficiently small x we have $f(x) < M$. Now, if $x + y = x_0$ then $yf(x) + f(f(x)) \geq f(x_0) > 0$. Choose x such that $y = x_0 - x > 0$ (i.e. $x < x_0$) and x small enough such that $f(x), f(f(x)) < 0$. (That is, if m_0 is such that $f(x) < 0$ for all $x < m_0$ and m_1 is such that $f(x) < m_0$ for all $x < m_1$ then we choose $x < \min\{m_0, m_1, x_0\}$ so $f(x) < 0$ and $f(f(x)) < 0$, too. Now, $y = x_0 - x > 0$, $f(x) < 0$ and $f(f(x)) < 0$ so $yf(x) + f(f(x)) < 0$ but then $f(x+y) = f(x_0) > 0$, contradiction.

Having established this, we need to show that 0 is a value of f . Suppose not, then $f(x) < 0$ for all x . We notice that $f(f(x)) < 0$ so $f(x+y) \leq yf(x) + f(f(x)) < yf(x)$. This means $f(x+y) < yf(x) < f(x)$ if $y \geq 1$, or equivalently $f(x-1) > f(x)$. Consider, for now, the number $f(-1)$. Then for all $x \leq -2$ we have $f(x) > f(-1)$. So by choosing $x < \min\{f(-1), -2\}$ we have $f(x) > f(-1) > x$, i.e. $f(x) > x$. Consider one such x_2 and by the lemma above, $f(x_2-1) > f(x_2) > x_2$. Plugging $y = 0$ gives $f(x_2-1) \leq f(f(x_2-1))$. But since $f(x_2-1) > x_2$, $f(f(x_2-1)) < f(x_2-1)$, which is a contradiction. Thus f cannot be all negative.

Now that $f(x_1) = 0$ for some x_1 , by plugging $y = 0$ we get $f(x_1) \leq f(f(x_1))$, i.e. $f(0) \geq 0$ so $f(0) = 0$ by the first lemma. Now for all $x > 0$ we have $0 = f(0) = f(x-x) \leq xf(-x) + f(f(x)) \leq xf(-x)$ since $f(f(x)) \leq 0$. Since x is positive, $f(-x)$ must be nonnegative. Since $f(-x)$ is also nonpositive, we have $f(-x) = 0$ for all $x > 0$, so $f(x) = 0$ for all $x < 0$.

- A7** Let a, b and c be positive real numbers satisfying $\min(a+b, b+c, c+a) > \sqrt{2}$ and $a^2 + b^2 + c^2 = 3$. Prove that

$$\frac{a}{(b+c-a)^2} + \frac{b}{(c+a-b)^2} + \frac{c}{(a+b-c)^2} \geq \frac{3}{(abc)^2}.$$

Solution. We first show that $a+b-c, b+c-a, c+a-b$ are all positive. Suppose otherwise, then if $c = \max\{a, b, c\}$ then $c \geq a+b$. Now that $a+b > \sqrt{2}$, and $a^2 + b^2 \geq \frac{(a+b)^2}{2} > 1$, so $a^2 + b^2 + c^2 > 1 + (a+b)^2 > 1 + 2 = 3$, contradicting that $a^2 + b^2 + c^2 = 3$. Hence these three quantities mentioned must all be positive.

Now we can write $a = x + y, b = x + z, c = y + z$ for some $x, y, z > 0$, i.e. a, b, c are sides of a triangle. This transforms the inequality into $\frac{x+y}{(2z)^2} + \frac{x+z}{(2y)^2} + \frac{y+z}{(2x)^2} \geq \frac{3}{(x+y)^2(x+z)^2(y+z)^2}$. We also have $(x+y)^2 + (y+z)^2 + (z+x)^2 = 3$ so $x^2 + y^2 + z^2 + xy + yz + zx = \frac{3}{2}$. Since it's not hard to show that $xy + yz + zx \leq x^2 + y^2 + z^2$ (i.e. $xy + yz + zx \leq 34$), we have

$$(x+y+z)^2 = x^2 + y^2 + z^2 + 2(xy + yz + zx) = \frac{3}{2} + xy + yz + zx \leq \frac{3}{2} + \frac{3}{4} = \frac{9}{4}$$

and consequently $x+y+z \leq \frac{3}{2}$. This means $\frac{x+y}{(2z)^2} + \frac{x+z}{(2y)^2} + \frac{y+z}{(2x)^2} \geq \frac{2}{3}(x+y+z)(\frac{x+y}{(2z)^2} + \frac{x+z}{(2y)^2} + \frac{y+z}{(2x)^2})$ and thus it suffices to show that this is \geq the right hand side. Multiplying RHS by $\frac{1}{27}((x+y)^2 + (y+z)^2 + (z+x)^2)^3$ to homogenize it, and cancelling the denominators, we have the following to prove:

$$\begin{aligned} 3(x+y+z)(x^2y^2(x+y) + y^2z^2(y+z) + z^2x^2(z+x))(x+y)^2(x+z)^2(y+z)^2 \\ \geq 2x^2y^2z^2((x+y)^2 + (y+z)^2 + (z+x)^2)^3 \end{aligned}$$

Denoting \sum by the symmetric sum, we have the left-hand-side as

$$\begin{aligned} 3 \sum x^8y^4z^0 + 6 \sum x^8y^3z^1 + 3 \sum x^8y^2z^2 + 12 \sum x^7y^5z^0 + 33 \sum x^7y^4z^1 + 39 \sum x^7y^3z^2 \\ + 9 \sum x^6y^6z^0 + 69 \sum x^6y^5z^1 + 102 \sum x^6y^4z^2 + 51 \sum x^6y^3z^3 + 69 \sum x^5y^5z^2 + 153 \sum x^5y^4z^3 \\ + 27 \sum x^4y^4z^4 \end{aligned}$$

and the right hand side as

$$\begin{aligned} 8 \sum x^8y^2z^2 + 48 \sum x^7y^3z^2 + 96 \sum x^6y^4z^2 + 72 \sum x^6y^3z^3 \\ + 56 \sum x^5y^5z^2 + 240 \sum x^5y^4z^3 + 56 \sum x^4y^4z^4 \end{aligned}$$

Muirhead now settles everything.

Combinatorics

- C1** (IMO 4) Let $n > 0$ be an integer. We are given a balance and n weights of weight $2^0, 2^1, \dots, 2^{n-1}$. We are to place each of the n weights on the balance, one after another, in such a way that the right pan is never heavier than the left pan. At each step we choose one of the weights that has not yet been placed on the balance, and place it on either the left pan or the right pan, until all of the weights have been placed. Determine the number of ways in which this can be done.

Answer. $1 \times 3 \times \dots \times (2n-1)$.

Solution. The key to the problem is to notice that if a_1, a_2, \dots, a_k are distinct nonnegative integers and $M = \max\{a_1, \dots, a_k\}$ then $2^M \leq 2^{a_1} + \dots + 2^{a_k} \leq 2^{M+1} - 1 < 2^{M+1}$. Therefore, a sequence is valid if and only if at each time, either the right pan is empty, or both pans are nonempty and the heaviest weight on the left pan is heavier than the heaviest weight on the right pan. We can also see that the pans can never be of the same weight for this reason, unless both pans are empty.

Having known these, we can use induction to show that if $f(n)$ is the number of ways when n is the number weights, then $f(1) = 1$ and $f(n) = (2n-1)f(n-1)$. Base case

$n = 1$ is simple: the only weight can only be added on the left. Now consider a sequence of n weights $n \geq 2$ and consider the lightest of the weights (i.e. 1). By removing this weight from the sequence, we see that both pans contain weights in the set $\{2^1, \dots, 2^{n-1}\}$, and moreover the pans have a weight difference of at least 2. Therefore, adding the weight 1 on either side will never change the validity of the pans (i.e. the left pan is heavier before the addition of 1 iff the left pan becomes heavier after that). We then infer that a valid sequence of n weights comes from the valid sequence of $n - 1$ weights, with 1 inserted. This 1 can be inserted anywhere in the sequence and on any pan, except that if it's the first to be placed it has to be on the left pan. This gives $2n - 1$ ways, making $f(n) = (2n - 1)f(n - 1)$.

It's also technically possible to induct on the heaviest weight, i.e. the one with weight 2^{n-1} . For each $1 \leq k \leq n$, suppose that this weight is the k -th weight to be placed onto the pans. We notice the following:

- This heaviest weight must be on the left.
- The $k - 1$ previous weights must follow the rule of "max of left $>$ max of right", so within the $k - 1$ weights themselves, there are $f(k - 1)$ ways to arrange them. Notice that we also have $\binom{n - 1}{k - 1}$ to choose those $k - 1$ weights from the $n - 1$ remaining weights.
- Finally, the $n - k$ subsequent weights can be placed arbitrarily. This gives $(n - k)!$ permutations of the $n - k$ weights, each with 2 possible choices, left or right.

Thus considering all these we have the summation $\sum_{k=1}^n f(k - 1) \binom{n - 1}{k - 1} (n - k)! 2^{n-k} = \sum_{k=1}^n f(k - 1) 2^{n-k} \frac{(n - 1)!}{(k - 1)!}$, with $f(0) = 1$ by convention (we used the fact that $\binom{n - 1}{k - 1} = \frac{(n - 1)!}{(k - 1)!(n - k)!}$). If we look at the term $f(k - 1) 2^{n-k} \frac{(n - 1)!}{(k - 1)!}$ more carefully, by the assumption $f(k - 1) = 1 \times 3 \times \dots \times (2k - 3)$ we have

$$\begin{aligned} f(k - 1) 2^{n-k} \frac{(n - 1)!}{(k - 1)!} &= 1 \times 3 \times \dots \times (2k - 3) 2^{n-k} k \times (k + 1) \times \dots \times (n - 1) \\ &= 1 \times 3 \times \dots \times (2k - 3) \times 2k \times (2k + 2) \times \dots \times (2n - 2) \end{aligned}$$

The final (and ultimate) computation requires us to do some telescoping sum. Fixing n , let $g(k) = 1 \times 3 \times \dots \times (2k - 3) \times 2k \times (2k + 2) \times \dots \times (2n - 2)$, then we show that $g(1) + \dots + g(k) = 1 \times 3 \times \dots \times (2k - 1) \times 2k \times (2k + 2) \times \dots \times (2n - 2)$. Again we can do induction on k : $g(1) = 2 \times \dots \times (2n - 2) = 1 \times 2 \times \dots \times (2n - 2)$ and

$$\begin{aligned} g(0) + \dots + g(k) + g(k + 1) &= 1 \times 3 \times \dots \times (2k - 1) \times 2k \times (2k + 2) \times \dots \times (2n - 2) \\ &\quad + 1 \times 3 \times \dots \times (2k - 1) \times (2k + 2) \times (2k + 2) \times \dots \times (2n - 2) \\ &= 1 \times 3 \times \dots \times (2k - 1) \times (2k + 1) \times (2k + 2) \times \dots \times (2n - 2) \end{aligned}$$

as desired. Thus letting $k = n$ we have $f(n) = g(1) + \dots + g(n) = 1 \times 3 \times \dots \times (2n - 1)$, as desired.

C2 Suppose that 1000 students are standing in a circle. Prove that there exists an integer k with $100 \leq k \leq 300$ such that in this circle there exists a contiguous group of $2k$ students, for which the first half contains the same number of girls as the second half.

Solution. Now consider the students as numbers x_1, \dots, x_{1000} , indices taken modulo 1000, with boys representing 0 and girls representing 1. We are to find an ℓ and k (with

k within the constraint) such that $\sum_{i=\ell}^{\ell+k-1} x_i = \sum_{i=\ell+k}^{\ell+2k-1} x_i$. Consider, now, the ℓ_0 such that $\sum_{i=\ell_0}^{\ell_0+100-1} x_i$ is the maximum, then $\sum_{i=\ell_0}^{\ell_0+100-1} x_i \geq \sum_{i=\ell_0+k}^{\ell_0+200-1} x_i$ and $\sum_{i=\ell_0-100}^{\ell_0-1} x_i \leq \sum_{i=\ell_0}^{\ell_0+100-1} x_i$.

We shall consider the count $c(\ell) = \sum_{i=\ell}^{\ell+100-1} x_i - \sum_{i=\ell+k}^{\ell+200-1} x_i$ as ℓ ranges from $\ell_0 - 100$ to ℓ .

Now, $c(\ell_0 - 100) \leq 0$ and $c(\ell_0 + 100) \geq 0$. If $c(\ell) = 0$ for some ℓ then we are done, so assume they are all nonzero between $\ell_0 - 100$ and ℓ_0 . The inequality also suggests that $c(\ell)$ changes sign somewhere.

Consider, now, an ℓ such that $c(\ell) < 0$ and $c(\ell+1) > 0$, which also means $c(\ell+1) - c(\ell) \geq 1 + 1 = 2$. We recognize that

$$\begin{aligned} c(\ell+1) - c(\ell) &= \left(\sum_{i=\ell+1}^{\ell+100} x_i - \sum_{i=\ell+k+1}^{\ell+200} x_i \right) - \left(\sum_{i=\ell}^{\ell+100-1} x_i - \sum_{i=\ell+k}^{\ell+200-1} x_i \right) \\ &= -x_\ell + 2x_{\ell+100} - x_{\ell+200} \\ &\leq -0 + 2(1) - (0) \\ &= 2 \end{aligned}$$

so all the inequalities above are inequality, and $x_\ell = x_{\ell+200} = 0$, $x_{\ell+100} = 1$. In addition,

$$\text{we have } \sum_{i=\ell+1}^{\ell+99} x_i = \sum_{i=\ell+101}^{\ell+199} x_i.$$

Let p be the maximal integer such that $x_{\ell+200} = \dots = x_{\ell+200+p-1} = 0$, and also $x_\ell =$

$$\begin{aligned} \dots = x_{\ell-p+1} = 0. \text{ By above, } p \geq 1. \text{ We now notice that, for } k = 100 + p, \sum_{i=\ell+100}^{\ell+200+p-1} x_i = \\ 1 + \sum_{i=\ell+101}^{\ell+199} x_i + \sum_{i=\ell+200}^{\ell+200+p-1} 0 = 1 + \sum_{i=\ell+101}^{\ell+199} x_i. \text{ Similarly, we have } \sum_{i=\ell-p}^{\ell+99} x_i = x_{\ell-p} + \sum_{i=\ell-p+1}^{\ell} 0 + \\ \sum_{i=\ell+1}^{\ell+99} x_i = x_{\ell-p} + \sum_{i=\ell+1}^{\ell+99} x_i. \text{ Assume that } p \leq 200. \text{ If } x_{\ell-p} = 1 \text{ then by } \sum_{i=\ell+1}^{\ell+99} x_i = \sum_{i=\ell+101}^{\ell+199} x_i \end{aligned}$$

then $x_{\ell-p} + \sum_{i=\ell+1}^{\ell+99} x_i = 1 + \sum_{i=\ell+101}^{\ell+199} x_i$ and we get a contagious pair of $100 + p$ students each

with same sum, solving the problem. Otherwise, $x_{\ell-p} = 0$. By considering $\sum_{i=\ell+101}^{\ell+200+p} x_i$ and

$\sum_{i=\ell-p+1}^{\ell+100} x_i$ we can either conclude that either these two are the contagious pair of $100 + p$ elements, or $x_{\ell+200+p} = 0$. Now if none of the $100 + p$ -pairs works, we have $x_{\ell-p} = x_{\ell+200+p} = 0$, which contradicts the maximality of p .

Now suppose that $p > 200$ instead, which means there are a consecutive row of 201 0's. Simply consider 200 of them, split them into contagious pairs of 100 0's each, and we are done.

C6 Let n be a positive integer, and let $W = \dots x_{-1}x_0x_1x_2\dots$ be an infinite periodic word, consisting of just letters a and/or b . Suppose that the minimal period N of W is greater than 2^n .

A finite nonempty word U is said to appear in W if there exist indices $k \leq \ell$ such that $U = x_kx_{k+1}\dots x_\ell$. A finite word U is called ubiquitous if the four words Ua , Ub , aU , and bU all appear in W . Prove that there are at least n ubiquitous finite nonempty words.

Solution. For each positive integer k we consider the words appearing in W of length k ; by the periodicity of W we also know that such set (of words of length k) is finite and won't exceed N . Of all such words, we also record the number of times each word appear as $x_\ell x_{\ell+1} \cdots x_{\ell+k-1}$ for $\ell = 0, 1, \dots, N-1$ (we only need to consider the first N words and the others are just periodically repeating) and record $M(k)$, the highest of those frequencies with respect to k . The key to this problem is to exploit the properties of $M(k)$:

- We first show that $M(N) = 1$. Otherwise, there's a word appearing at least two times. Now, let $x_k x_{k+1} \cdots x_{k+N-1} = x_\ell x_{\ell+1} \cdots x_{\ell+N-1}$ with $0 \leq k < \ell \leq N-1$. This means, $x_{k+i} = x_{\ell+i}$ for all $i = 0, 1, \dots, N-1$. But since W is periodic with period N , for each $i \in \mathbb{Z}$, choose $i' \equiv i \pmod{N}$ and $0 \leq i' < N$ and we have $x_{k+i} = x_{k+i'} = x_{\ell+i'} = x_{\ell+i}$, so W is also periodic with period $\ell - k$. But $0 < \ell - k < N$, contradicting the minimality of N . Therefore $M(N) = 1$.
- Next, we see how $M(k)$ compares to $M(k+1)$. We show that $M(k) \leq 2M(k+1)$. Indeed, if U is a word of length k with frequency $M(k)$, then one of Ua and Ub must have frequency at least $\frac{M(k)}{2}$, so $M(k+1) \geq \frac{M(k)}{2}$, as claimed.
- We should also see what happens if $M(k) > M(k+1)$ for some k , and we claim that the word U of length k and frequency $M(k)$ is ubiquitous. Now, the sum of frequencies of Ua and Ub is $M(k)$ and since $M(k+1) < M(k)$, both the frequencies are strictly less than $M(k)$. Hence both the frequencies must also be at least 1. Similarly, both the frequencies of aU and bU must also be at least 1, so U is ubiquitous. In essence this means if $M(k+1) < M(k)$ then there exists a word of length k that is ubiquitous.

In view of the last bullet point it suffices to show that there are at least n numbers k such that $M(k+1) < M(k)$. That is, the function $M(k)$ decreases at least k times. We first notice that $M(1) = \max\{\text{freq}(a), \text{freq}(b)\} \geq \frac{N}{2} > \frac{2^n}{2} = 2^{n-1}$, and $M(N) = 1$. Also, whenever M decreases, it never decreases more than half based on the second bullet point. It follows that it must decrease at least $\log_2(M(1)) > \log_2(2^{n-1}) = n-1$ times, i.e. decrease at least n times, which finishes the claim.

C7 On a square table of 2011 by 2011 cells we place a finite number of napkins that each cover a square of 52 by 52 cells. In each cell we write the number of napkins covering it, and we record the maximal number k of cells that all contain the same nonzero number. Considering all possible napkin configurations, what is the largest value of k ?

Answer. $2011^2 - 2 \times 17 \times 2011 + 38 \times 17^2 = 3986729$.

Solution. An example has been shown in the official solution, whereby a total of 39^2 napkins is used: label the napkins as (i, j) with $1 \leq i, j \leq 39$ (notice that $2011 = 38 \times 52 + 35$). If $i + j \leq 39$ then (i, j) covers row from $52(i-1) + 1$ to $52i$ and $52(j-1) + 1$ to $52j$, inclusive; if $i + j = 40$ (i, j) covers row from $52(i-1) + 1$ to $52i$ and $52(j-1) - 16$ to $52j - 17$, inclusive (except $(39, 1)$ which covers the bottom left corner, as in the next case); finally if $i + j \geq 41$ then (i, j) covers row from $52(i-1) - 16$ to $52i - 17$ and $52(j-1) - 16$ to $52j - 17$. This way, all squares have frequency 1 except the following cells: those in the form $52(i-1) + k, 52(39-i) + \ell$ and $52(i-1) + \ell, 52(39-i) + k$ for $1 \leq i \leq 39, 1 \leq k \leq 52$ (but $52(i-1) + k \leq 2011$) and $36 \leq k \leq 52$. The first case corresponds to 2011×17 of the cells; same goes to the second case. But then for the case $k \geq 36$ we double-counted so the number of cells not with frequency 1 is $2 \times 17 \times 2011 - 38 \times 17^2$.

To show that this is indeed an upper bound, for each row, now, we investigate those cells with frequency the same frequency $k > 0$. Also we classify the cells into four categories: for a cell (i, j) with remainder (i', j') when divided by 52 ($1 \leq i', j' \leq 52$) we have category 1: $1 \leq i', j' \leq 35$, category 2: $1 \leq i' \leq 35, 36 \leq j' \leq 52$, category 3: $36 \leq i' \leq 52, 1 \leq j' \leq 35$ and category 4: $36 \leq i', j' \leq 52$. Consider each row r with cells (r, j) ,

$1 \leq j \leq 2011$. We notice that for each $1 \leq j' \leq 52$, there are 38 cells congruent to j' mod 52 if $36 \leq j' \leq 52$ and 39 cells congruent to j' otherwise. We also notice that, consider each cell with coordinates modulo 52, for each $(i', j') \in \mathbb{Z}_{52}^2$, each napkin covers (i', j') exactly once. This means that if the number of napkins covering row r is strictly less than $39k$, then for each $1 \leq j' \leq 35$ there is at least one cell congruent to j' mod 52 that has frequency strictly less than k ; call those cells deficient. Analogously, if the number of napkins covering row r is strictly more than $38k$, then for each $36 \leq j' \leq 52$ there is at least one cell congruent to j' mod 52 that has frequency strictly more than k ; call those cells excessive. Since at least one of the scenarios above happen, we infer that for each row either there's at least 35 deficient cells or 17 excessive cells; moreover the 35 deficient cells are of category 1 if $1 \leq r' \pmod{52} \leq 35$ and category 3 otherwise; the 17 excessive cells are of category 2 if $1 \leq r' \pmod{52} \leq 35$ and category 4 otherwise. In a similar way, for each column c there's also either at least 35 deficient cells (category 1 or 2 depending on c), or at least 17 excessive cells (category 3 or 4 depending on c).

Now let d and e be rational numbers such that there are exactly $35d$ deficient type 1 cells and $17e$ excessive type 4 cells. Since there are 35×39 rows (and respectively columns) that are of remainder $1 \leq r \leq 35$, there must be at least $17(35 \times 39 - d)$ excessive type 2 cells (by considering the rows) and similarly $17(35 \times 39 - d)$ excessive type 3 cells. Likewise, since there are 17×38 rows (and respectively columns), there must be at least $\max\{35(17 \times 38 - e), 0\}$ deficient type 2 cells and similarly $\max\{35(17 \times 38 - e), 0\}$ deficient type 3 cells. The cells in the two scenarios are mutually disjoint: the deficient and excessive cells of same category can't overlap since we cannot have the frequency of some cell to be $> k$ and $< k$ simultaneously. The cells with frequency not k induced by d in category 1 is at least

$$\begin{aligned} 35d + 2 \times 17(35 \times 39 - d) &= 2 \times 17 \times 35 \times 39 + d \\ &\geq 2 \times 17 \times 35 \times 39 \end{aligned}$$

The cells with frequency not k induced by e in category 4 is lower-bounded by $17e + 2 \max\{35(17 \times 38 - e), 0\}$. When $e \leq 17 \times 38$ we have $17e + 2 \times 35 \times 17 \times 38 - 70e = 2 \times 35 \times 17 \times 38 - 53e \geq 2 \times 35 \times 17 \times 38 - 53(17 \times 38) = 17^2 \times 38$; when $e \geq 17 \times 38$ this count is simply $17(17 \times 38)$. Hence the lower bound here is 38×17^2 .

Summing up, a lower bound of the cells with frequency not k is $2 \times 17 \times 35 \times 39 + 38 \times 17^2 = 17(2 \times 35 \times 39 + 38 \times 17) = 17(2011 - 38 \times 17)$, as desired.

Geometry

G1 Let ABC be an acute triangle. Let ω be a circle whose centre L lies on the side BC . Suppose that ω is tangent to AB at B' and AC at C' . Suppose also that the circumcentre O of triangle ABC lies on the shorter arc $B'C'$ of ω . Prove that the circumcircle of ABC and ω meet at two points.

Solution. Let R be circumradius of ABC and r the radius of ω . It suffices to show that $R < 2r$. Henceforth we denote $\angle A = \angle BAC$.

Case 1. $\angle A < 60^\circ$. Denote h as the distance from O to BC , then

$$r = OL \geq h = R \cos \frac{\angle BOC}{2} = R \cos \angle BAC > \frac{R}{2}$$

Case 2. $\angle A \geq 60^\circ$. Here we make use of O on shorter arc $B'C'$, i.e. O lies inside the quadrilateral $AB'LC'$. Given also that the projection on O to AB and AC are the mid-points of AB and AC , respectively, we have $AB' \geq B'B$ and $AC' \geq C'C$. Consequently, we also have $AL \geq LB$ and $AL \geq LC$.

Let AL intersect the circumcircle again at M , then by power of point theorem we have $LM \leq BL$ and $LM \leq LC$. W.l.o.g. let $AB \leq AC$. Then $\frac{\angle A}{2} = \angle CBM \leq \angle BML$, so $ML \leq BM \cdot \frac{\sin \angle A/2}{\sin \angle A}$ and given $MB^2 = ML \cdot MA = ML \cdot (ML + LA)$,

$$LA = \frac{BM^2}{ML} - ML \geq BM \cdot \left(\frac{\sin \angle A}{\sin \angle A/2} - \frac{\sin \angle A/2}{\sin \angle A} \right)$$

Finally, we have $r = LB' = LC' = AL \sin \frac{A}{2}$ and $BM = 2R \sin \frac{\angle A}{2}$. This gives

$$r = AL \sin \frac{A}{2} \geq 2R \sin^2 \frac{A}{2} \cdot \left(\frac{\sin \angle A}{\sin \angle A/2} - \frac{\sin \angle A/2}{\sin \angle A} \right) = 2R \sin^2 \frac{A}{2} \cdot \left(\frac{\sin^2 \angle A - \sin^2 \angle A/2}{\sin \angle A/2 \sin \angle A} \right)$$

and using the identity $\sin^2 A - \sin^2 B = \sin(A - B) \sin(A + B)$ we get

$$\begin{aligned} 2R \sin^2 \frac{A}{2} \cdot \left(\frac{\sin^2 \angle A - \sin^2 \angle A/2}{\sin \angle A/2 \sin \angle A} \right) &= 2R \sin^2 \frac{A}{2} \cdot \left(\frac{\sin(A/2) \sin(3A/2)}{\sin \angle A/2 \sin \angle A} \right) \\ &= 2R \sin^2 \frac{\angle A}{2} \sin \frac{3\angle A}{2} \div \sin \angle A \end{aligned}$$

which, for $\angle A \geq 60^\circ$, has value $\frac{1}{\sqrt{3}}R > \frac{1}{2}R$.

G2 Let $A_1A_2A_3A_4$ be a non-cyclic quadrilateral. Let O_1 and r_1 be the circumcentre and the circumradius of the triangle $A_2A_3A_4$. Define O_2, O_3, O_4 and r_2, r_3, r_4 in a similar way. Prove that

$$\frac{1}{O_1A_1^2 - r_1^2} + \frac{1}{O_2A_2^2 - r_2^2} + \frac{1}{O_3A_3^2 - r_3^2} + \frac{1}{O_4A_4^2 - r_4^2} = 0.$$

Solution. Let diagonals A_1A_3 and A_2A_4 meet at point P . Notice that the quantity $O_iA_i - r_i^2$ is actually the power of point from A_i to the circumcircle of triangle not containing A_i . To meaningfully compute these power of points, we need to consider the “signed lengths” of PA_1, PA_2, PA_3, PA_4 : if for some angle, $\angle A_i > 180^\circ$ (i.e. nonconvex) then we let $PA_i < 0$.

Now consider PA_1 . We have $A_1A_3 = PA_1 + PA_3$, and if Y is the second intersection of the circle $A_2A_3A_4$ and A_1A_3 then power of point theorem (on point P) says $PA_2PA_4 = PA_3PY$. Consequently, the power of point of A_1 to this circle is $A_1A_3 \cdot (PA_1 - PY) = (PA_1 + PA_3) \cdot (PA_1 - \frac{PA_2PA_4}{PA_3}) = (PA_1 + PA_3) \left(\frac{PA_1PA_3 - PA_2PA_4}{PA_3} \right)$. This gives $\frac{1}{O_1A_1^2 - r_1^2} = \frac{PA_3}{(PA_1 + PA_3)(PA_1PA_3 - PA_2PA_4)}$. Similarly, $\frac{1}{O_2A_2^2 - r_2^2} = \frac{PA_4}{(PA_2 + PA_4)(PA_2PA_4 - PA_1PA_3)}$, $\frac{1}{O_3A_3^2 - r_3^2} = \frac{PA_1}{(PA_1 + PA_3)(PA_1PA_3 - PA_2PA_4)}$ and $\frac{1}{O_4A_4^2 - r_4^2} = \frac{PA_2}{(PA_2 + PA_4)(PA_2PA_4 - PA_1PA_3)}$. Thus the desired sum becomes

$$\begin{aligned} \sum_{i=1}^4 \frac{1}{O_iA_i^2 - r_i^2} &= \frac{PA_1 + PA_3}{(PA_1 + PA_3)(PA_1PA_3 - PA_2PA_4)} + \frac{PA_2 + PA_4}{(PA_2 + PA_4)(PA_2PA_4 - PA_1PA_3)} \\ &= \frac{1}{PA_1PA_3 - PA_2PA_4} + \frac{1}{PA_2PA_4 - PA_1PA_3} \\ &= \frac{1}{PA_1PA_3 - PA_2PA_4} - \frac{1}{PA_1PA_3 - PA_2PA_4} \\ &= 0 \end{aligned}$$

as desired.

G3 Let $ABCD$ be a convex quadrilateral whose sides AD and BC are not parallel. Suppose that the circles with diameters AB and CD meet at points E and F inside the quadrilateral. Let ω_E be the circle through the feet of the perpendiculars from E to the lines AB, BC and CD . Let ω_F be the circle through the feet of the perpendiculars from F to

Let $a = \angle MPR$ and $b = \angle MRP$, and d the diameter of circle P, Q, O_M, E . Then $MR = d \sin a$ and $PM = d \sin b$. We would also have $MO_E = d \sin |\frac{a-b}{2}|$ and $OE_P = OE_Q = d \sin \frac{a+b}{2}$. Therefore,

$$\begin{aligned} MO_E^2 - OE_P^2 &= d^2(\sin^2 |\frac{a-b}{2}| - \sin^2 \frac{a+b}{2}) = -4d^2 \sin \frac{a}{2} \sin \frac{b}{2} \cos \frac{a}{2} \cos \frac{b}{2} \\ &= -d^2 \sin a \sin b = -PM \cdot MR \end{aligned}$$

as desired.

Similarly, if the perpendicular from F to AB and CD are U and V respectively then the power of point from M to ω_F is $-MU \cdot MV$. Notice that both EP and FU are perpendicular to AB , hence parallel to each other. The 'midline' between the two line (that is, the line equidistant to the two aforementioned parallel lines) passes through the midpoint of EF (i.e. M), and with PU perpendicular to these parallel lines we have $MP = MU$ and similarly $MR = MV$. Therefore $MP \cdot MR = MU \cdot MV$, so M lies on the radical axis of ω_E and ω_F , as desired.

- G4** Let ABC be an acute triangle with circumcircle Ω . Let B_0 be the midpoint of AC and let C_0 be the midpoint of AB . Let D be the foot of the altitude from A and let G be the centroid of the triangle ABC . Let ω be a circle through B_0 and C_0 that is tangent to the circle Ω at a point $X \neq A$. Prove that the points D, G and X are collinear.

Solution. W.l.o.g. suppose that $AB < AC$. We first determine the ratio $\frac{BX}{XC}$. Observe, first, that $\frac{AB}{AC} = \frac{C_0X}{B_0X}$. Indeed: the circle tangency condition implies that $\angle BXC_0 = \angle CXB_0$, and

$$\frac{1}{2} = \frac{BC_0}{BA} = \frac{XC_0 \sin \angle BXC_0}{AX \sin \angle BXA} = \frac{XC_0 \sin \angle BXC_0}{AX \sin \angle BCA}$$

and similarly $\frac{1}{2} = \frac{XB_0 \sin \angle CXB_0}{AX \sin \angle CBA}$. Comparing the two ratio, we have $\frac{XC_0}{XB_0} = \frac{\sin \angle BCA}{\sin \angle ABC} = \frac{AB}{AC}$.

Next, Stewart's theorem says that $AC_0^2 + C_0B^2 + 2XC_0^2 = BX^2 + AX^2$, and similarly $AB_0^2 + B_0C^2 + 2XB_0^2 = CX^2 + AX^2$. Since $\frac{AC_0}{AB_0} = \frac{C_0B}{B_0C} = \frac{C_0X}{B_0X} = \frac{AB}{AC}$, we deduce that $\frac{BX^2 + AX^2}{CX^2 + AX^2} = \frac{AB^2}{AC^2} = \frac{BX^2 + AX^2 - 2BX \cdot AX \cdot \cos \angle BXA}{CX^2 + AX^2 - 2CX \cdot AX \cdot \cos \angle CXA}$. the latter by cosine rule. Doing cross multiplication on the fraction terms, we get

$$\frac{AB^2}{AC^2} = \frac{BX \cdot AX \cdot \cos \angle BXA}{CX \cdot AX \cdot \cos \angle CXA} = \frac{BX \cdot \cos \angle BCA}{CX \cdot \cos \angle CBA} \quad (7)$$

so it follows that $\frac{BX}{CX} = \frac{AB^2 \cdot \cos \angle CBA}{AC^2 \cos \angle BCA}$.

Now let A_0 be the midpoint of BC . We see that $A_0DC_0B_0$ is an isocles trapezoid. Consider the homothety centered at G with scale -2 (which brings B_0 to B , C_0 to C , and A_0 to A). Suppose that it brings D to T , then $ATCB$ is also an isocles trapezoid, so A, T, C, B, X are concyclic. In addition, we have

$$\frac{|\triangle TBX|}{|\triangle TCX|} = \frac{TB \cdot BX \cdot \sin \angle TBX}{TC \cdot CX \cdot \sin \angle TCX} = \frac{AC \cdot AB^2 \cdot \cos \angle CBA}{AB \cdot AC^2 \cdot \cos \angle BCA} = \frac{AB \cos \angle CBA}{AC \cos \angle BCA} \quad (8)$$

where we used $\angle TBX + \angle TCX = 180^\circ$ (and therefore the sine of the angles are equal). Meanwhile, $\frac{BD}{DC} = \frac{AB \sin \angle BAD}{AC \sin \angle CAD} = \frac{AB \cos \angle ABC}{AC \sin \angle ACB}$. Thus we have $\frac{|\triangle TBX|}{|\triangle TCX|} = \frac{BH}{HC}$, so TX passes through D . Since D, G, T are collinear (by the definition of homothety), X also lies on this line.

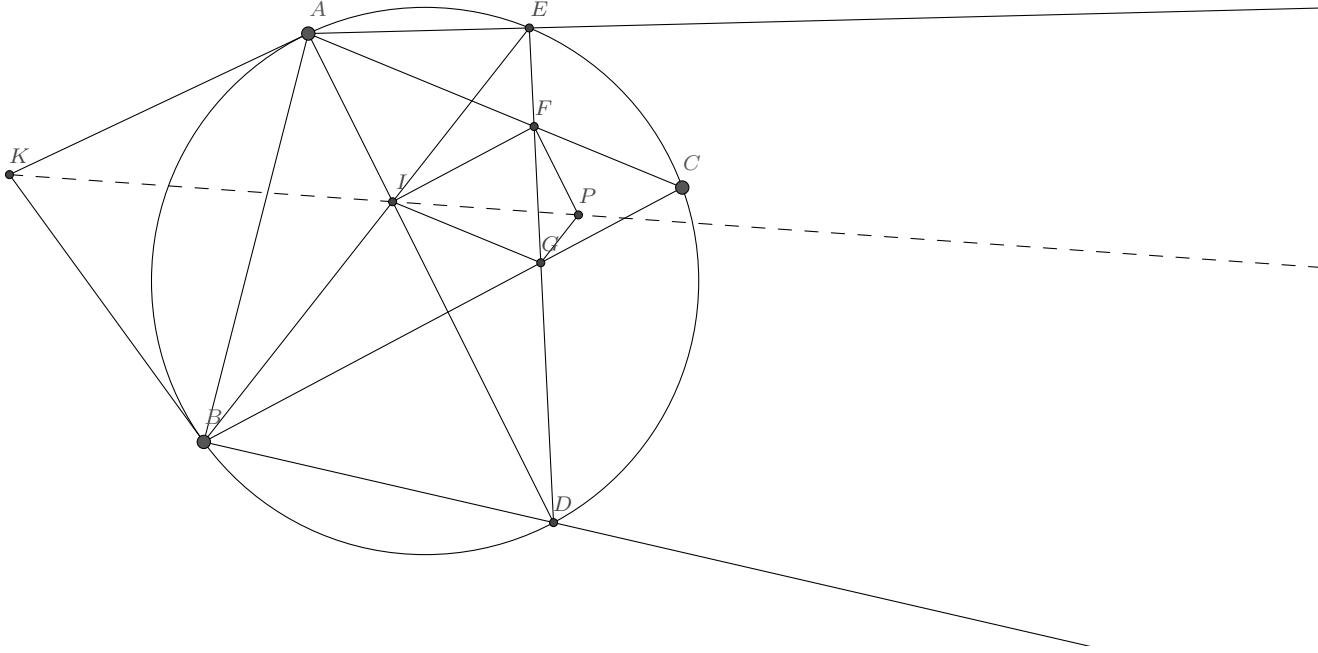
- G5** Let ABC be a triangle with incenter I and circumcircle ω . Let D and E be the second intersection points of ω with the lines AI and BI , respectively. The chord DE meets AC at a point F , and BC at a point G . Let P be the intersection point of the line through F parallel to AD and the line through G parallel to BE . Suppose that the tangents to ω

at A and at B meet at a point K . Prove that the three lines AE , BD , and KP are either parallel or concurrent.

Solution: We first establish this.

Lemma 1. K, I, P are collinear.

Proof. First notice that $\angle DEB = \angle DAB = \frac{\angle A}{2} = \angle CAD = \angle CED$ and similarly $\angle CDE = \frac{\angle B}{2} = \angle EDA$. Therefore $\triangle CED \cong \triangle IED$ and ED is the perpendicular bisector of segment CI . This entails that $CF = CG$ and $\angle CFG = \angle CGF = \angle IFG = \angle IGF = 90^\circ - \frac{\angle C}{2}$. Knowing that $FP \parallel AI$ and $GP \parallel BI$, we want to prove that $\angle FPI = \angle AIK$, or equivalently $\angle GPI = \angle BIK$. It suffices to prove that $\frac{\sin \angle FPI}{\sin \angle GPI} = \frac{\sin \angle AIK}{\sin \angle BIK}$.



Recall that $FP \parallel AI \Rightarrow \angle CFP = \angle CAI$, $GP \parallel BI \Rightarrow \angle CPG = \angle CBI$. Thus $CFIG$ is a rhombus and $FI = GI$. This gives

$$\frac{\sin \angle FPI}{\sin \angle GPI} = \frac{FI}{GI} \cdot \frac{\sin \angle PFI}{\sin \angle PGI} = \frac{\sin(\angle CFI - \angle CFP)}{\sin(\angle CGI - \angle CGP)} = \frac{\sin(180^\circ - \angle C - \frac{\angle A}{2})}{\sin(180^\circ - \angle C - \frac{\angle B}{2})} = \frac{\sin(\angle C + \frac{\angle A}{2})}{\sin(\angle C + \frac{\angle B}{2})}$$

Given also that $AK = BK$, we have

$$\frac{\sin \angle AIK}{\sin \angle BIK} = \frac{AK}{BK} \cdot \frac{\sin \angle IAK}{\sin \angle IBK} = \frac{\sin(\angle C + \frac{\angle A}{2})}{\sin(\angle C + \frac{\angle B}{2})} = \frac{\sin \angle FPI}{\sin \angle GPI},$$

as desired. \square

For convenience we assume that AE and BD are not parallel; the limit case (i.e. parallel) happens when $\angle C = 60^\circ$ and quadrilateral $AIBK$ is cyclic, which is left as an exercise (no trigo needed because angle chasing method becomes straightforward). Now let AE and BD intersect at Q . We need $\frac{\sin \angle AKQ}{\sin \angle BKQ} = \frac{\sin \angle AKI}{\sin \angle BKI}$, or $\frac{AQ}{BQ} \cdot \frac{\sin \angle QAK}{\sin \angle QBK} = \frac{AI}{BI} \cdot \frac{\sin \angle IAK}{\sin \angle IBK}$. Now $\frac{AQ}{BQ} = \frac{\sin \angle QBA}{\sin \angle QAB} = \frac{\sin \angle DBA}{\sin \angle EAB} = \frac{DA}{EB}$ and $\angle QAK = \angle EAK = 180^\circ - \angle EBA$ so $\sin \angle EAK = \sin \angle EBA$. Similarly $\sin \angle QBK = \sin \angle DAB$. Thus,

$$\frac{\sin \angle QAK}{\sin \angle QBK} = \frac{\sin \angle EBA}{\sin \angle DAB} = \frac{AI}{BI} = \frac{\sin \frac{\angle B}{2}}{\sin \frac{\angle A}{2}}$$

and $\frac{\sin \angle IAK}{\sin \angle IBK} = \frac{\sin \angle DAK}{\sin \angle EBK} = \frac{AD}{EB}$. Therefore $\frac{AQ}{BQ} \cdot \frac{\sin \angle QAK}{\sin \angle QBK} = \frac{\sin \frac{\angle B}{2}}{\sin \frac{\angle A}{2}} \cdot \frac{AD}{EB} = \frac{AI}{BI} \cdot \frac{\sin \angle IAK}{\sin \angle IBK}$. ■

- G6** Let ABC be a triangle with $AB = AC$ and let D be the midpoint of AC . The angle bisector of $\angle BAC$ intersects the circle through D, B and C at the point E inside the triangle ABC . The line BD intersects the circle through A, E and B in two points B and F . The lines AF and BE meet at a point I , and the lines CI and BD meet at a point K . Show that I is the incentre of triangle KAB .

Solution. To show that BI bisects $\angle ABK$ is the same as showing that BE bisects $\angle ABD$. If D' is the second intersection of AB and the circle $BEDC$ then D and D' are symmetric to each other in the line AE , hence $ED = ED'$ and so $\angle ABE = \angle D'BE = \angle EBD$, establishing the claim.

To finish the rest, we consider a third circle centered at D and passes through C and A . We claim that F is on this circle too by showing that $DA = DF$. Now by angle chasing we have $\angle ADB = 180^\circ - \angle BDC = 180^\circ - \angle BEC = \text{refl} \angle BEC - 180^\circ = 2\angle AEB - 180^\circ = 2\angle AFB - 180^\circ = 2(180^\circ - \angle AFD) - 180^\circ = 180^\circ - 2\angle AFD$ (the refl notation means reflex angle). Thus, $\angle ADB = 180^\circ - 2\angle AFD$ and we have $\angle AFD + \angle FAD = 2\angle AFD$, so $\angle AFD = \angle FAD$ so $DA = DF$, as claimed.

Now, we consider the three circles: $BEDC$, $AEFB$ and AFC , with the first two given in the problem and third defined on our own. The first two circles have BE as the radical axis, and the last two has AF as the radical axis. Hence, the intersection, I , is the radical center of the three circles. Since C is on both circles $BEDC$ and AFC , CI is the radical axis of these two circles. This means, if O is the center of the circle $BEDC$ then $DO \perp CI$. Since O is the center of BDC we have $\angle CDO + \angle DBC = 90^\circ$; since $DO \perp CI$ we have $\angle CDO + \angle DCI = 90^\circ$. Therefore $\angle DBC = \angle DCI = \angle DCK$, and equivalently, $\angle DKC = \angle DCB$. Knowing this, the last part is to observe the following:

$$\begin{aligned} \angle ABI + \angle FIK &= \frac{\angle ABF}{2} + (180^\circ - \angle IFK - \angle IKF) \\ &= \frac{\angle ABC - \angle DBC}{2} + (180^\circ - \angle AFD - \angle DKC) \\ &= \frac{\angle ABC - \angle DBC}{2} + (180^\circ - \frac{180^\circ - \angle ADF}{2} - \angle DCB) \\ &= \frac{\angle ABC - (180^\circ - \angle BDC - \angle DCB)}{2} + (180^\circ - \frac{\angle BDC}{2} - \angle DCB) \\ &= 90^\circ - \frac{\angle DCB}{2} + \frac{\angle ABC}{2} \\ &= 90^\circ \end{aligned}$$

which shows that the line KI passes through the circumcenter O' of the triangle AIB . Thus considering the circumcircle of triangle $AO'B$, we see that, if K' is the second intersection of the line KI with this circle (other than O') then I is the incentre of triangle $K'AB$, and therefore $\angle ABI = \angle IBK'$ but as shown before, $\angle ABI = \angle IBK$, so $\angle IBK = \angle IBK'$ and since both K and K' are on KI , we have $K = K'$, showing that I is indeed the incentre of KAB .

- G7** Let $ABCDEF$ be a convex hexagon all of whose sides are tangent to a circle ω with centre O . Suppose that the circumcircle of triangle ACE is concentric with ω . Let J be the foot of the perpendicular from B to CD . Suppose that the perpendicular from B to DF intersects the line EO at a point K . Let L be the foot of the perpendicular from K to DE . Prove that $DJ = DL$.

Solution. Let the circumradius of ACE to be R , and the radius of ω to be r . Then the distance of sides AB, BC, CD, DE, EF, FA to O is r and therefore we have $\cos \angle BAO = \cos \angle OAF = \cos \angle OEF = \cos \angle OED = \cos \angle DCO = \cos \angle OCB = \frac{r}{R}$, so $\angle BAO =$

$\angle OAF = \angle OEF = \angle OED = \angle DCO = \angle OCB$; denote this common angle as θ . We also have $BA = BC$, $DC = DE$, $FE = FA$: we have $OC = OA$ and $\angle OCB = \angle OCA$ so it's not hard to see that CBO and ABO must be congruent. The other equivalences can be established similarly. Having known these, consider DJ and DL in terms of signed lengths, and let CJ be positive iff J is on ray DC beyond C ; similarly let FL be positive iff L is on ray DF beyond F . Then we have $DJ = DC + CJ$ and $DL = DE + EL$, so it suffices to prove that $CJ = EL$. Moreover, in terms of unsigned length we have $|CJ| = |BC| \cdot |\cos BCJ|$ and we can infer that $CJ > 0$ iff $\cos BCJ > 0$ ($\cos BCD < 90^\circ$ means that J will be on the same side as D w.r.t. C so $CJ < 0$ in this case). Thus $CJ = BC \cdot \cos BCJ = -BC \cos BCD = -BC \cos 2\theta$. Also since $\theta < 90^\circ$, if K extends beyond OE then $\angle KEL = \angle OED = \theta$ and in this case $EL = EK \cos \theta > 0$, so $EL > 0$ iff K extends beyond OE , so we have to do our computation in that direction.

The immediate previous argument means that when considering the lengths DK and FK we have $\angle DEK = 180^\circ - \theta$ so

$$DK^2 = DE^2 + EK^2 - 2DE \cdot EK \cdot \cos(180^\circ - \theta) = DE^2 + EK^2 + 2DE \cdot EK \cdot \cos \theta$$

and

$$FK^2 = FE^2 + EK^2 + 2FE \cdot EK \cdot \cos \theta$$

We can then conclude that

$$DK^2 - FK^2 = DE^2 - FE^2 + 2EK \cos \theta (DE - FE)$$

The condition $BK \perp DF$ also implies $BD^2 - BF^2 = KD^2 - KF^2$ but according to cosine rule, we have

$$BD^2 = BC^2 + CD^2 - 2 \cdot BC \cdot CD \cdot \cos 2\theta \quad BF^2 = BA^2 + AF^2 - 2 \cdot BA \cdot AF \cdot \cos 2\theta$$

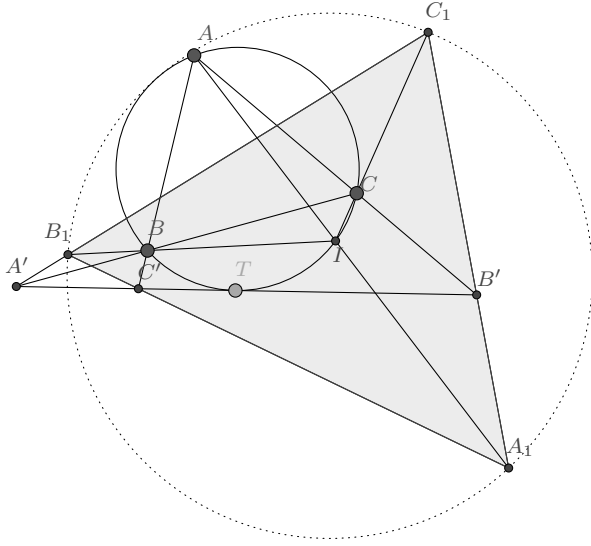
and bearing in mind that $BC = BA$, the difference in square becomes

$$BD^2 - BF^2 = CD^2 - AF^2 - 2 \cdot BC \cos 2\theta (CD - AF)$$

and coupling with the fact that $CD = DE$ and $AF = FE$, and that the two sum of squares are the same we have $DE^2 - FE^2 + 2EK \cos \theta (DE - FE) = CD^2 - AF^2 - 2 \cdot BC \cos 2\theta (CD - AF)$ so $EK \cos \theta (DE - FE) = -BC \cos 2\theta (DE - FE)$. We may assume that $CD \neq AF$, otherwise K won't be uniquely determined. This allows us to cancel $DE - FE$ from the equation and we have $EK \cos \theta = -BC \cos 2\theta$. Finally, recall that $CJ = -BC \cos 2\theta$ and $EL = EK \cos \theta$ so we in turn have $EL = EK \cos \theta = -BC \cos 2\theta = CJ$, as desired.

- G8** (IMO 6) Let ABC be an acute triangle with circumcircle Γ . Let ℓ be a tangent line to Γ , and let ℓ_a, ℓ_b and ℓ_c be the lines obtained by reflecting ℓ in the lines BC, CA and AB , respectively. Show that the circumcircle of the triangle determined by the lines ℓ_a, ℓ_b and ℓ_c is tangent to the circle Γ .

Solution. (cited directly from my notes for the IMO training camp).



Denote A_1, B_1, C_1 as $\ell_b \cap \ell_c, \ell_a \cap \ell_c, \ell_a \cap \ell_b$, respectively.

Lemma 2. AA_1, BB_1, CC_1 concur on Γ , and the common point I is the incenter of triangle $A_1B_1C_1$.

Proof. Now denote the intersection of BC, CA, AB with ℓ as A', B' and C' , respectively. let us consider triangle $B_1A'C'$. Since $A'B$ bisects $\angle B_1A'C'$ and $C'B$ bisects $\angle B_1C'A'$, we know that B is either the incenter or excenter of $B_1A'C'$ and it follows that B_1B bisects angle $A'B_1C'$, which then follows that BB_1 passes through the circumcentre of $BA'C'$. Using the notation of directed angles it follows that $\angle(BB_1, AB) = \angle(BB_1, BC') = 90^\circ - \angle(A'C', A'B) = 90^\circ - \angle(\ell, BC)$ and $\angle(BB_1, BC) = \angle(BB_1, BA') = 90^\circ - \angle(A'C', C'B) = 90^\circ - \angle(\ell, AB)$. In a similar way, $\angle(CC_1, AC) = 90^\circ - \angle(\ell, BC)$ and $\angle(CC_1, BC) = 90^\circ - \angle(\ell, AC)$. Now $\angle(BB_1, CC_1) = \angle(BB_1, BC) - \angle(CC_1, BC) = (90^\circ - \angle(\ell, AB)) - (90^\circ - \angle(\ell, AC)) = \angle(AB, AC)$, yielding that BB_1 and CC_1 indeed intersect on Γ . The concurrence of AA_1, BB_1 and CC_1 follows from the fact that they intersect at either the incenter or excenter of triangle $A_1B_1C_1$, hence we are done.

Now we need the fact that I is the incenter (not excentre opposite to any of the sides), given that ABC is an acute triangle. Now let's investigate the relationship between $\angle A, \angle B, \angle C$ (of $\triangle ABC$) and $\angle A_1, \angle B_1, \angle C_1$ (of $\triangle A_1B_1C_1$). Take B again. If $\angle A'BC' < 90^\circ$ then $\angle B = \angle A'BC'$, and it can be verified that B is now the excentre of $\triangle B_1A'C'$ and $\angle B_1A'C' = 180^\circ - 2\angle A'BC' = 180^\circ - 2\angle B$. On the other hand, if $\angle A'BC$ is obtuse then $\angle B = 180^\circ - \angle A'BC$ and B is the incenter of $\triangle B_1A'C'$ so $\angle B_1A'C' = 2\angle A'BC - 360^\circ = 2(180^\circ - \angle B) - 180^\circ = 180^\circ - 2\angle B$. So $\angle B_1$ is either $2\angle B$ or $180^\circ - 2\angle B$, depending whether BB_1 is the external or internal angle bisector of angle B_1 , respectively. Same goes for line angles A_1 and C_1 . If I is the excentre, then exactly two of the lines AA_1, BB_1, CC_1 are the external angle bisectors of the respective angles. So let say AA_1 and BB_1 are the external angle bisectors of angles A_1 and B_1 then angles A_1, B_1, C_1 are $2\angle A, 2\angle B$ and $180^\circ - 2\angle C$ respectively. As the three angles sum up to 180° and $\angle A + \angle B + \angle C = 180^\circ$, comparing the two equations yields $\angle C = 90^\circ$ (contradiction). \square

Now let's proceed to the solving of the main problem. Denote T as the tangent point of ℓ and Γ , and a, b, c as $\angle(TA, \ell), \angle(TB, \ell), \angle(TC, \ell)$. Speaking in modulo 180° , $\angle A$ is congruent to $b - c$, so $\sin \angle A = |\sin(b - c)|$. Similarly $\sin \angle B = |\sin(c - a)|$ and $\sin \angle C = |\sin(a - b)|$. (we can change the \pm sign to modulus, though). Let's now show the following:

Lemma 3. *In unsigned length, among the three quantities $A_1B_1 \cdot t(C_1)$, $C_1A_1 \cdot t(B_1)$, $B_1C_1 \cdot t(A_1)$, one of them is the sum of the other two, where $t(K)$ is the length of tangent from point K to Γ .*

Proof. Notice that it is the ratio $A_1B_1 \cdot t(C_1) : C_1A_1 \cdot t(B_1) : B_1C_1 \cdot t(A_1)$ that matters, so we can divide each of them by a constant whenever necessary. By power of point theorem we have

$$t(A_1) = \sqrt{A_1I \cdot A_1A}$$

Define r as the inradius of triangle $A_1B_1C_1$ and r_A the distance from A to lines A_1B' , A_1C' and $B'C'$ (or ℓ) (the distance to the three lines are the same because A is the incentre or excentre of $A_1B'C'$.) Now

$$A_1A = \frac{r_A}{\sin \angle A_1B'A} = \frac{r_A}{\sin(90^\circ - \angle A)} = \frac{r_A}{\cos \angle A}$$

as $\angle A_1 = 180^\circ - 2\angle A$. Similarly $\angle A_1I = \frac{r}{\cos \angle A}$ so $t(A_1) = \sqrt{A_1I \cdot A_1A} = \frac{\sqrt{r \cdot r_A}}{\cos \angle A}$. Now $B_1C_1 = D \sin \angle A_1 = D \sin \angle(180^\circ - 2\angle A) = D \sin 2\angle A$, where D is the diameter of circumcircle $A_1B_1C_1$ so $B_1C_1 \cdot t(A_1) = D \sin 2\angle A \cdot \frac{\sqrt{r \cdot r_A}}{\cos \angle A} = 2D \sin \angle A \cdot \sqrt{r \cdot r_A}$.

The original ratio now becomes $\sin \angle A \cdot \sqrt{r_A} : \sin \angle B \cdot \sqrt{r_B} : \sin \angle C \cdot \sqrt{r_C}$ by eliminating constants D and r . Now if d is the diameter of Γ then it is not hard to notice that $r_A = \text{distance from } A \text{ to } \ell = TA \sin \angle(TA, \ell) = (d \sin a) \cdot \sin a = d \sin^2 a$. Meanwhile $\sin \angle A = |\sin(b - c)|$. So our original ratio becomes $\sin a \cdot |\sin(b - c)| : \sin a \cdot |\sin(c - a)| : \sin c \cdot |\sin(a - b)|$. Nevertheless,

$$\sin a \cdot \sin(b - c) + \sin a \cdot \sin(c - a) + \sin c \cdot \sin(a - b) = 0$$

which means one of them is the sum of the other two when we package them into absolute number. \square

Finally, notice that A_1, B_1, C_1 must all lie outside Γ . W.l.o.g. let T be opposite A on Γ , then given that ABC is acute, OC' lies between ℓ and AB . It then follows that ℓ_C , the reflection of ℓ in AB , has no intersection with Γ (since ℓ is tangent to Γ). Similarly, ℓ_B has no intersection with Γ , hence the two reflections must lie entirely outside Γ , and therefore so are A_1, B_1, C_1 . Therefore, this and Lemma 2 means that the conclusion follows by applying Casey's theorem to degenerate circles A_1, B_1, C_1 and circle Γ .

Number Theory

N1 For any integer $d > 0$, let $f(d)$ be the smallest possible integer that has exactly d positive divisors (so for example we have $f(1) = 1, f(5) = 16$, and $f(6) = 12$). Prove that for every integer $k \geq 0$ the number $f(2^k)$ divides $f(2^{k+1})$.

Solution. Recall that each positive integer can be written as a nonnegative but finite length of product of primes, i.e. each $n \in \mathbb{N}$ can be written uniquely (up to reordering)

as $\prod_{i=1}^k p_i^{\alpha_i}$, and we also know that in this case the number of divisors of n is $\prod_{i=1}^k (\alpha_i + 1)$.

Thus, if n has 2^k positive divisors then each $\alpha_i + 1$ must be a power of 2.

In view of this, for each k , we can write $f(2^k)$ as $\prod_{i=1}^m p_i^{2^{d_i}-1}$ with $\sum_{i=1}^m d_i = k$. Now let

$f(2^{k+1}) = \prod_{i=1}^m q_i^{2^{e_i}-1}$ with $\sum_{i=1}^{\ell} e_i = k + 1$. By inserting "trivial factors" into each $f(2^k)$

and $f(2^{k+1})$ (i.e. multiply by $1 = p^0 = p^{2^0-1}$ for arbitrary p) we may assume that they have the following form: $f(2^k) = \prod_{i=1}^m p_i^{2^{d_i}-1}$ and $f(2^{k+1}) = \prod_{i=1}^m p_i^{2^{e_i}-1}$, with $\sum_{i=1}^m d_i = k$ and $\sum_{i=1}^m e_i = k+1$.

Since $\sum e_i > \sum d_i$, there exists an index j such that $e_j > d_j$. In particular, since $d_j \geq 0$, $e_j \geq 1$. Now let $d'_i = d_i$ if $i \neq j$, and $d'_j = d_j + 1$. Then $\sum_{i=1}^m d'_i = k+1$ and $\prod_{i=1}^m p_i^{2^{d'_i}-1} = p_j^{2^{d_j}} \prod_{i=1}^m p_i^{2^{d_i}-1} = p_j^{2^{d_j}} f(2^k)$ has 2^{k+1} positive divisors. By the definition of f we have $p_j^{2^{d_j}} f(2^k) \geq f(2^{k+1})$, i.e. $p_j^{2^{d_j}} \geq \frac{f(2^{k+1})}{f(2^k)}$. Similarly, define e'_i as $e'_i = e_i$ if $i \neq j$, and $e'_j = e_j - 1$. Then $\sum_{i=1}^m e'_i = k$ and $\prod_{i=1}^m p_i^{2^{e'_i}-1} = p_j^{2^{-e'_j}} \prod_{i=1}^m p_i^{2^{e_i}-1} = p_j^{2^{-e'_j}} f(2^{k+1})$ has 2^k positive divisors (recall that $e_j \geq 1$ so $e'_j \geq 0$). Again by the definition of f we have $p_j^{2^{-e'_j}} f(2^{k+1}) \geq f(2^k)$, or $\frac{f(2^{k+1})}{f(2^k)} \geq p_j^{2^{e'_j}}$. Combining these two inequalities we have $p_j^{2^{e'_j}} \leq \frac{f(2^{k+1})}{f(2^k)} \leq p_j^{2^{d_j}}$, so $e'_j \leq d_j$. However, we have $e_j > d_j$, so $e'_j = e_j - 1 \geq d_j$, and therefore $p_j^{2^{e'_j}} = p_j^{2^{d_j}}$. Thus all inequalities above become equality and thus $\frac{f(2^{k+1})}{f(2^k)} = p_j^{2^{d_j}}$, i.e. $f(2^k) \mid f(2^{k+1})$.

- N2** Consider a polynomial $P(x) = \prod_{j=1}^9 (x + d_j)$, where d_1, d_2, \dots, d_9 are nine distinct integers. Prove that there exists an integer N , such that for all integers $x \geq N$ the number $P(x)$ is divisible by a prime number greater than 20.

Solution. First, for each j , we consider the remainder of $\frac{P(x)}{x+d_j}$ when being divided by $x + d_j$. As each d_j is distinct, the remainder is nonzero. Since $\deg(x + d_j) = 1$, the remainder has degree 0, hence must in the form of c_j for some nonzero integer constant c_j (that is, $\frac{P(x)}{x+d_j} = Q_j(x)(x + d_j) + c_j$ for some polynomial $Q_j(x)$; such $Q_j(x)$ has integer coefficient since $x + d_j$ is monic). Now for each x_0 , the number $\frac{P(x_0)}{x_0+d_j}$ is divisible by $x_0 + d_j$ if and only if c_j is divisible by $x_0 + d_j$ (we have $Q_j(x_0)$ an integer). This is false for all $x_0 > |c_j| - d_j$, so in terms of integers we have $x_0 + d_j \nmid \frac{P(x_0)}{x_0+d_j}$ for x_0 sufficiently large. This also means that there exists a prime number $p(x_0, j)$ such that $v_{p(x_0, j)}(x_0 + d_j) > v_{p(x_0, j)}\left(\frac{P(x_0)}{x_0+d_j}\right) = \sum_{1 \leq i \leq 9, i \neq j} v_{p(x_0, j)}(x_0 + d_i)$ (here $v_p(q)$ is the highest exponent of the prime p dividing the number q). Since $v_p(q) \geq 0$ for all primes p and all integers q , we have $v_{p(x_0, j)}(x_0 + d_j) > v_{p(x_0, j)}(x_0 + d_i)$ for all $i \neq j$. Consider $N = \max\{|c_j| - d_j\} + 1$, then for all $x_0 \geq N$ and for each j there exists a prime $p(x_0, j)$ such that $v_{p(x_0, j)}(x_0 + d_j) > v_{p(x_0, j)}(x_0 + d_i)$ for all $i \neq j$. All such primes $p(x_0, j)$ must therefore be distinct (if $p(x_0, j) = p(x_0, i)$ for some $i \neq j$ then $v_{p(x_0, j)}(x_0 + d_j) > v_{p(x_0, j)}(x_0 + d_i)$ and $v_{p(x_0, j)}(x_0 + d_i) > v_{p(x_0, j)}(x_0 + d_j)$ hold simultaneously, which is absurd), and since $v_{p(x_0, j)}(x_0 + d_j) \geq 1$ for each j , $P(x_0)$ is divisible by $p(x_0, j)$ for each j . In particular, $P(x_0)$ has at least 9 distinct prime divisors, so one of them must be greater than 20 (since there are exactly 8 prime numbers less than 20).

- N3** Let $n \geq 1$ be an odd integer. Determine all functions f from the set of integers to itself, such that for all integers x and y the difference $f(x) - f(y)$ divides $x^n - y^n$.

Answer. $f(x) = \pm x^d + c$ for any d a positive divisor of n and c any constant. It's not hard to see that this works because $x^d - y^d \mid x^n - y^n$.

Solution. It now remains to see that these are all the functions that work. First,

notice that if f is a function satisfying the condition, and c is an arbitrary constant, then $g(x) := f(x) + c$ is also a working function. Hence we can assume that $f(0) = 0$.

Consider any prime p . We have $f(p) \mid p^n$ and $f(-p) \mid (-p)^n$. Thus each $f(p)$ and $f(-p)$ must be in the form $\pm p^d$ for some nonnegative integer $d \leq n$. Considering that there are only finitely many nonnegative integers $d \leq n$, and that there are infinitely many primes, there exists a d_0 such that, either $f(p) = p^{d_0}$ for infinitely many primes p , or $f(p) = -p^{d_0}$ for infinitely many primes p .

Let's assume the first case, and notice that for each nonzero integer y , we have $f(p) - f(y) \mid p^n - y^n$. Since there's infinitely many p with $f(p) = p^{d_0}$, we have $p^{d_0} - f(y) \mid p^n - y^n$ for infinitely many p . Consider the polynomial $q(x) = x^{d_0}$ we have $q(x) - f(y) \mid x^n - y^n$ for infinitely many x , too. If $r(x)$ is the remainder polynomial of $x^n - y^n$ when divided by $q(x) - f(y)$, then $q(x) - f(y) \mid r(x)$ for infinitely many positive integers x . But since $\deg(r) - \deg(q)$, $|r(x)| < |q(x) - f(y)|$ for all sufficiently large x , so we must have $r(x) = 0$ for infinitely many x (i.e. whenever $|r(x)| < |q(x) - f(y)|$ and $q(x) - f(y) \mid r(x)$). The only possibility is $r \equiv 0$, so $q(x) - f(y) \mid x^n - y^n$ as a polynomial. Consider any complex solution x_0 to the equation $x^{d_0} = f(y)$, then $x_0^{d_0} - f(y) = 0$ and therefore $x_0^n - y^n = 0$, too, by the divisibility of polynomial (so $x_0^n = y^n$). We now have the following observations:

- If $x^{d_0} = f(y)$ and ϵ is a root of unity of degree d_0 , then $(\epsilon x_0)^{d_0} = f(y)$ and therefore $(\epsilon x_0)^n = y^n$. Thus $x_0^n = \epsilon^n x_0^n$. Since $x_0 \neq 0$ as assumed (otherwise $f(y) = 0$ and by the injectivity of f we have $y = 0$), we have $\epsilon^n = 1$. Thus $\epsilon^{d_0} = 1 \rightarrow \epsilon^n = 1$ for all complex number ϵ , which happens only when $d_0 \mid n$.
- The above also implies that d_0 is odd, so the equation $x^{d_0} = f(y)$ actually has a unique real solution x_0 (recall that the mapping $x \rightarrow x^{d_0}$ for an odd d_0 is bijective if viewed from reals to reals). Consider one such x_0 and since $x_0^n = y^n$ too, we have $x_0 = y$ since n is also odd. Thus $f(y) = y^{d_0}$, as confirmed.

Thus we have shown that $f(x) = x^{d_0}$ for some $d_0 \mid n$ in the first case, i.e. infinitely many primes p satisfying $f(p) = p^{d_0}$. The second case is similar, and we get $f(x) = -x^{d_0}$ for some $d_0 \mid n$.

N4 For each positive integer k , let $t(k)$ be the largest odd divisor of k . Determine all positive integers a for which there exists a positive integer n , such that all the differences

$$t(n+a) - t(n); t(n+a+1) - t(n+1), \dots, t(n+2a-1) - t(n+a-1)$$

are divisible by 4.

Answer. $a = 1, 3, 5$. For each of those we can choose the pairs $(a, n) = (1, 1), (3, 1), (5, 4)$.

Solution. It now remains to show that these are all the possible a 's. If a is even, then among the numbers $n, n+1, \dots, n+a-1$, exactly one of them, say $ka + \frac{a}{2}$, must be congruent to $\frac{a}{2}$ modulo a . Now consider $t(ka + \frac{a}{2} + a) - t(ka + \frac{a}{2})$. Now $ka + \frac{a}{2} = \frac{a}{2}(1+2k)$ and $ka + \frac{a}{2} + a = \frac{a}{2}(3+2k)$ so $t(ka + \frac{a}{2} + a) = t(\frac{a}{2})(3+2k)$ and $t(ka + \frac{a}{2}) = t(\frac{a}{2})(1+2k)$ and therefore $t(ka + \frac{a}{2} + a) - t(ka + \frac{a}{2}) = 2t(\frac{a}{2})$ and since $t(\frac{a}{2})$ is odd, $4 \nmid 2t(\frac{a}{2})$. Hence a cannot be even.

Next, let $a \geq 7$ be odd. Now one of n and $n+a$ is odd, while the other is even. W.l.o.g. let n be odd, then $n, n+2, n+4, n+6$ are all odd, and therefore $t(n+k) = n+k$ for all $k = 0, 2, 4, 6$. Now $n+a, n+2+a, n+4+a, n+6+a$ are all even, and since $4 \mid t(n+a+k) - t(n+k) = t(n+a+k) - (n+k)$ for $k = 0, 2, 4, 6$. Since $n \equiv n+4$ and $n+2 \equiv n+6$ (mod 4), we have $t(n+a) \equiv t(n+a+4)$ (mod 4) and $t(n+a+2) \equiv t(n+a+6)$ (mod 4). If $n+a \equiv 2$ (mod 4) then so is $n+a+4$, and therefore $t(n+a+4) - t(n+a) = (\frac{n+a+4}{2}) - (\frac{n+a}{2}) = 2 \not\equiv 0$ (mod 4), contradiction. If $n+a \equiv 0$ (mod 4), then $n+a+2 \equiv n+a+6 \equiv 2$ (mod 4), so $t(n+a+6) - t(n+a+2) = \frac{n+a+6}{2} - \frac{n+a+2}{2} = 2 \not\equiv 0$ (mod 4), another contradiction. Therefore $a < 7$ is necessary.

N5 (IMO 5) Let f be a function from the set of integers to the set of positive integers. Suppose that, for any two integers m and n , the difference $f(m) - f(n)$ is divisible by $f(m - n)$. Prove that, for all integers m and n with $f(m) \leq f(n)$, the number $f(n)$ is divisible by $f(m)$.

Solution. We first notice that:

$$f(m - 0) \mid f(m) - f(0) \quad \rightarrow \quad f(0) \text{ is divisible by } f(m) \text{ for all integers } m \quad (9)$$

And also

$$f(-n) = f(0 - n) \mid f(0) - f(n) \quad \rightarrow \quad f(-n) \mid f(n) \quad (10)$$

the last one follows from $f(n) \mid f(0)$ for all integers n . By symmetry, $f(n) \mid f(-n)$ and since both are positive, we have $f(n) = f(-n)$ for all n .

Next, we'll show that $f(n) \mid f(kn)$ for all integers k, n . Notice that for all $k \geq 0$ we have

$$f((k + 1)n - kn) = f(n) \mid f((k + 1)n) - f(kn) \quad (11)$$

and by considering $k = 1$ as base case and perform induction from there, we have $f(n) \mid f(kn)$ for all $k \geq 1$. But since f is an even function with $f(n) = f(-n)$ for all n , we have $f(n) \mid f(kn)$ for all k .

Now consider m, n arbitrary, and let $\gcd(m, n) = d$. By Euclidean algorithm there exist integers a and b such that $am + bn = d$. We know by above, $f(d) \mid f(am)$ and $f(d) \mid f(bn)$. This gives us the following relation:

$$f(am) = f(d - bn) \mid f(d) - f(bn); \quad f(bn) = f(d - am) \mid f(d) - f(am)$$

W.L.O.G. let $f(bn) \leq f(am)$, then since $f(d)$ and $f(am)$ are both positive, we have $|f(d) - f(am)| < \max\{f(d), f(am)\} \leq f(bn)$ (we have $f(d) \mid f(bn)$ so $f(d) \leq f(bn)$, too. This means that the only possibility is $f(d) - f(am) = 0$, so $f(d) = f(am)$. But then $f(d) \mid f(m) \mid f(am) = f(d)$ so we also have $f(d) = f(m)$. Finally, $f(m) = f(d) \mid f(n)$ since $d \mid n$, completing the problem solution.

N6 Let $P(x)$ and $Q(x)$ be two polynomials with integer coefficients, such that no nonconstant polynomial with rational coefficients divides both $P(x)$ and $Q(x)$. Suppose that for every positive integer n the integers $P(n)$ and $Q(n)$ are positive, and $2^{Q(n)} - 1$ divides $3^{P(n)} - 1$. Prove that $Q(x)$ is a constant polynomial.

Solution. Suppose that Q is nonconstant. We first show that there exist infinitely many primes p such that there exists x (that depends on x) where p divides $P(x)$ and $Q(x)$ simultaneously. For each number q with $\gcd(q, 3) = 1$, denote $g(q) = \text{ord}_q(3)$, i.e. the smallest $n > 0$ such that $q \mid 3^n - 1$. A quick check yields that $Q(x)$ even implies that $3 \mid 2^{Q(x)} - 1$ but $3 \nmid 3^{P(x)} - 1$. Thus Q can only take odd values.

By Schur's theorem, there are infinitely many odd primes p that divides one of $\{Q(1), Q(2), \dots\}$ (since Q is nonconstant). Among those primes, consider those such that $2^p > 3^{P(1)}$ (which there are also infinitely many of these since $3^{P(1)}$ is bounded), which then follows that $2^p - 1 \nmid 3^{P(1)} - 1$ and therefore $g(2^p - 1) \nmid P(1)$. For each such prime p , let n_p be such that $p \mid Q(n_p)$. Using the fact that $x - y \mid Q(x) - Q(y)$ for each pairs x, y , we have $p \mid Q(n_p + kp)$ for each integer $k \geq 0$. Since $2^p - 1 \mid 2^{p^q} - 1$ for all nonnegative integers q , we have $2^p - 1 \mid 2^{Q(n_p + kp)} - 1 \mid 3^{P(n_p + kp)} - 1$, which also means $g(2^p - 1) \mid P(n_p + kp)$ for all integers $k \geq 0$. Suppose that $p \nmid g(2^p - 1)$, i.e. $\gcd(p, g(2^p - 1)) = 1$. Then $\{n_p + kp \pmod{g(2^p - 1)} : k \geq 0\}$ is complete residue mod $g(2^p - 1)$. Using $x - y \mid P(x) - P(y)$, we have $g(2^p - 1) \mid P(x)$ for all $x \geq 1$. This contradicts $g(2^p - 1) \nmid P(1)$. It then follows that $p \mid g(2^p - 1) \mid P(n_p)$, and so p divides $P(n_p)$ and $Q(n_p)$ simultaneously.

We now consider the following sequence following iteration Bezout's theorem: set $P_0 = P, Q_0 = Q$, and subsequently, $P_{n+1} = Q_n, Q_{n+1}$ is the remainder of P_n when divided by Q_n

(i.e. there exists a polynomial A_n such that $P_n = Q_{n+1} + Q_n A$, and $\deg(Q_{n+1}) < \deg Q_n$; such A_n must have rational coefficients). This process persists until one of the terms hit constant or 0. Since P and Q has no nonconstant polynomial divisors (with rational coefficients), this also applies to each pair (P_i, Q_i) . It follows that there exists an n such that $Q_n \equiv d$ for some nonzero constant d . Since all the terms A_n involved are of rational coefficients, it follows that d is also rational. This means that there exist A, B of rational coefficients such that $AP + BQ = d_0 \neq 0$ for some rational constant d_0 . Multiplying by some suitable nonzero integer, we may assume that A, B are of integer coefficient, and that d_0 is an integer. This means that for each x , $\gcd(A(x), B(x)) \mid d_0$. This contradicts the claim that there are infinitely many primes p such that for some n_p , p divides $P(n_p), Q(n_p)$ simultaneously.

N7 Let p be an odd prime number. For every integer a , define the number $S_a = \sum_{j=1}^{p-1} \frac{a^j}{j}$. Let $m, n \in \mathbb{Z}$, such that

$$S_3 + S_4 - 3S_2 = \frac{m}{n}$$

Prove that p divides m .

Solution. We denote the following:

$$O_a = \sum_{1 \leq j \leq p-1, j \text{ odd}} \frac{a^j}{j} \quad E_a = \sum_{1 \leq j \leq p-1, j \text{ even}} \frac{a^j}{j} \quad (12)$$

Observe that $S_a = O_a + E_a$ for all integers a . In addition, we will consider the modulo of a rational number mod p so long as the denominator is not divisible by p , via multiplicative inverse. Thus from now on, all the equivalences are in modulo p .

We first consider the following:

Lemma 4. $S_{a+1} \equiv E_a - O_a$

Proof. Expanding S_{a+1} gives us the following:

$$\begin{aligned} S_{a+1} &= \sum_{j=1}^{p-1} \frac{1}{j} \sum_{\ell=0}^j \binom{j}{\ell} a^\ell \\ &= \sum_{\ell=0}^{p-1} a^\ell \sum_{j=\max(1, \ell)}^{p-1} \frac{1}{j} \binom{j}{\ell} \\ &= \sum_{\ell=1}^{p-1} \frac{a^0}{\ell} + \sum_{\ell=1}^{p-1} a^\ell \sum_{j=\ell}^{p-1} \frac{1}{j} \binom{j}{\ell} \\ &= S_1 + \sum_{\ell=1}^{p-1} a^\ell \sum_{j=\ell}^{p-1} \frac{(j-1)!}{\ell!(j-\ell)!} \\ &= S_1 + \sum_{\ell=1}^{p-1} \frac{a^\ell}{\ell} \sum_{j=\ell}^{p-1} \binom{j-1}{\ell-1} \end{aligned} \quad (13)$$

To proceed, notice the following:

$$S_1 = \sum_{j=1}^{p-1} \frac{1}{j} = \sum_{j=1}^{(p-1)/2} \frac{1}{j} + \frac{1}{p-j} = \sum_{j=1}^{(p-1)/2} \frac{p}{j(p-j)} \equiv 0 \quad (14)$$

and also by telescoping sum, we have

$$\sum_{j=\ell}^{p-1} \binom{j-1}{\ell-1} = \sum_{j=\ell}^{p-1} \binom{j}{\ell} - \binom{j-1}{\ell} = \binom{p-1}{\ell} - \binom{\ell-1}{\ell} = \binom{p-1}{\ell} \quad (15)$$

Finally, we also have $\binom{p-1}{\ell} = \frac{(p-1)\cdots(p-\ell)}{\ell!} \equiv \frac{(-1)\cdots(-\ell)}{\ell!} = (-1)^\ell$, therefore

$$S_{a+1} = S_1 + \sum_{\ell=1}^{p-1} \frac{a^\ell}{\ell} \sum_{j=\ell}^{p-1} \binom{j-1}{\ell-1} \equiv 0 + \sum_{\ell=1}^{p-1} \frac{a^\ell}{\ell} (-1)^\ell = E_a - O_a \quad (16)$$

□

Now we have the next one:

Lemma 5. $S_{a^2} \equiv 2E_a + 2aO_a$

Proof. Again we have the following expansion:

$$S_{a^2} = \sum_{j=1}^{p-1} \frac{a^{2j}}{j} = \sum_{j=1}^{(p-1)/2} \left(\frac{a^{2j}}{j} + \frac{a^{2j+(p-1)}}{(p-1)/2+j} \right) \equiv \sum_{j=1}^{(p-1)/2} a^{2j} \left(\frac{1}{j} + \frac{1}{-\frac{1}{2}+j} \right) \quad (17)$$

which can then be decomposed into the following:

$$\sum_{j=1}^{(p-1)/2} \frac{a^{2j}}{j} = 2 \sum_{j=1}^{(p-1)/2} \frac{a^{2j}}{2j} = 2E_a \quad (18)$$

and also

$$\sum_{j=1}^{(p-1)/2} \frac{a^{2j}}{-\frac{1}{2}+j} \equiv \sum_{j=1}^{(p-1)/2} \frac{2a^{2j}}{2j-1} = 2a \sum_{j=1}^{(p-1)/2} \frac{a^{2j-1}}{2j-1} = 2aO_a \quad (19)$$

□

Therefore considering $a = 2$ we have

$$S_3 + S_4 - 3S_2 \equiv (E_2 - O_2) + (2E_2 + 2 \cdot 2 \cdot O_2) - 3(E_2 + O_2) = 0 \quad (20)$$

as desired.

N8 Let $k \in \mathbb{Z}^+$ and set $n = 2^k + 1$. Prove that n is a prime number if and only if the following holds: there is a permutation a_1, \dots, a_{n-1} of the numbers $1, 2, \dots, n-1$ and a sequence of integers g_1, \dots, g_{n-1} , such that n divides $g_i^{a_i} - a_{i+1}$ for every $i \in \{1, 2, \dots, n-1\}$, where we set $a_n = a_1$.

Solution. We note that n is odd. Let's first show that if such sequence exists, then n must be prime. Suppose n is composite, then there are two cases:

- There's a odd prime number p with $p^2 \mid n$. If $a_{\ell+1} = p$ and $a_{m+1} = 2p$, which means $g_\ell^{a_\ell}$ and $g_m^{a_m}$ must both be divisible by p but not p^2 . This implies $p \mid g_\ell, g_m$ and $a_\ell = a_m = 1$, which is impossible.
- n is squarefree with at least two distinct prime divisors. We see that among $1, \dots, n-1$, $\frac{n-1}{2}$ are even. Also, if a_i is even, then a_{i+1} must be a quadratic residue mod n . Now, for each prime p , the number of quadratic residues modulo p is $\frac{p+1}{2}$. This means that if p_1, \dots, p_k are prime divisors of n then the number of quadratic residue (excluding 0) is

$$\left(n \cdot \prod \frac{p_i+1}{2p_i} \right) - 1$$

where the -1 is considering that we need to subtract 0 off. This means $\left(n \cdot \prod \frac{p_i+1}{2p_i} \right) \geq \frac{n-1}{2}$, or $\prod \frac{p_i+1}{2p_i} > \frac{1}{2}$. On the other hand, for each prime p_i , $\frac{p_i+1}{2} = \frac{1}{2} + \frac{1}{2p_i} \leq \frac{1}{2} + \frac{1}{6} = \frac{2}{3}$ so with $k \geq 2$, we have $\prod \frac{p_i+1}{2p_i} \leq \left(\frac{2}{3}\right)^2 = \frac{4}{9} < \frac{1}{2}$.

It now remains to provide a construction when such n is prime. Observe that k must be a power of 2; if $k = ab$ for some odd $a > 1$ then $2^b + 1 \mid 2^{ab} + 1$ (thus not prime). We write $k = 2^m$ for some $m \geq 0$. In fact, we may settle the case where $k = 1$ immediately by just letting $a_1 = g_1 = 1, a_2 = g_2 = 1$, so $k \geq 2$ and so $m \geq 1$. This would also mean that $n \equiv 2 \pmod{3}$.

Consider, now, a bipartite graph with $(1, 1), \dots, (1, n-1)$ appearing on one side, and $(2, 1), \dots, (2, n-1)$ appearing on the other side. Denote $\nu_2(x)$ as the highest power of 2 dividing x , and consider any primitive root g of n . Then $g^1, \dots, g^{n-2}, g^{n-1} = 1$ are all distinct mod n , so in our graph we can have edges $(1, a)$ and $(2, g^b)$ for all pairs (a, b) satisfying $\nu_2(a) = \nu_2(b)$. Note that a perfect matching exists: just take $(1, a), (2, g^a)$.

Now we consider a directed graph (V, E) where $V = \{1, \dots, n-1\}$, and $E = \{a \rightarrow b\}$ is determined by the perfect matching. Observe that each node has an indegree and outdegree of 1 each, so the resulting graph is a set of disjoint cycles (including possible self-loop). We now consider the following claim:

Lemma 6. *By modifying the graph such that a new edge $a \rightarrow b$ can only be added if there is an edge between $(1, a), (2, b)$ (but there is no rule of edge deletion), we can produce (V, E) with a single cycle that traverses all vertices (Hamiltonian).*

Proof. Consider, now, any two cycles C_1 and C_2 . We claim that if $a \in C_1$ and $b \in C_2$ such that $\nu_2(a) = \nu_2(b)$, then it is possible to merge C_1 and C_2 into one. Indeed, let C_1 be $a_1 \rightarrow \dots \rightarrow a_u \rightarrow a_1$ and $b_1 \rightarrow \dots \rightarrow b_v \rightarrow b_1$, with $\nu_2(a_1) = \nu_2(b_1)$. Then by our construction, $a_2 = g^{c_2}$ and $b_2 = g^{d_2}$ for some c_2, d_2 such that $\nu_2(a_1) = \nu_2(b_1) = \nu_2(c_2) = \nu_2(d_2)$. We can therefore take the cycle $a_1 \rightarrow b_2 \rightarrow \dots \rightarrow b_v \rightarrow b_1 \rightarrow a_2 \dots \rightarrow a_u \rightarrow a_1$, justifying such a merge (in other words we delete $a_1 \rightarrow a_2, b_1 \rightarrow b_2$ and replace by $a_1 \rightarrow b_2, b_1 \rightarrow a_2$ to maintain the structure of disjoint cycles).

Now suppose after several such merging steps we can no longer proceed. In particular, all odd numbers are in the same cycle, say C_1 . It then follows that all the quadratic nonresidues are also in C_1 . We now show that C_1 contains all $1, \dots, n-1$.

We have shown the case $n = 3$ above. For $n = 5$, using $g = 3$ (i.e. $g, g^2, g^3, g^4 = 3, 4, 2, 1$) we have the cycle $1 \rightarrow 3 \rightarrow 2 \rightarrow 4 \rightarrow 1$, hence we may assume $n \geq 17$. Since $n \equiv 2 \pmod{3}$ and $n \equiv 1 \pmod{4}$, we use the famous property of Legendre's symbol $(\frac{3}{n})(\frac{n}{3}) = (-1)^{\frac{(3-1)(n-1)}{2}} = 1$, and with $(\frac{n}{3}) = -1, (\frac{3}{n}) = -1$. In other words, $\frac{3}{n}$ is not a quadratic residue. On the other hand, since $2^k \equiv -1$ (i.e. $2^{2k} \equiv 1$) and $2k < 2^k$ for $k \geq 4$, 2 is a quadratic residue of n . This means that $3 \cdot 2^\ell$ is a quadratic nonresidue for $\ell = 0, \dots, k-2$, which means for each $\ell = 0, \dots, 2^\ell$, C_1 contains at least a member in the form $\nu_2(\cdot) = \ell$. Since we can no longer merge two different cycles, all numbers with $\nu_2(\cdot) \leq k-2$ must be in this cycle C_1 .

Finally, the only numbers not in the form $\nu_2(\cdot) \leq k-2$ are 2^{k-1} and 2^k . But in our matching, the only outdegree from 2^k is to 1, and the only outdegree from 2^{k-1} is to $-1 = 2^k$. Thus both numbers are in C_1 (since 1 is in this cycle), completing the proof. \square

Now we can finish the solution. In our single cycle above, we get $a_1 \rightarrow \dots \rightarrow a_{n-1} \rightarrow a_1$. By the method we construct our edges, $a_i \rightarrow a_{i+1}$ implies that if $a_{i+1} = g^{b_{i+1}}$ then $\nu_2(a_i) = \nu_2(b_{i+1})$. It then follows that a suitable g_i can be found such that $g_i^{a_i} = a_{i+1}$ given that a_{i+1} is the $2^{\nu_2(a_i)}$ -th power residue of n and $\gcd(n-1, a_i) = 2^{\nu_2(a_i)}$.