Contest Problems and Preliminary Solutions

Problem 1: Find all strictly increasing sequences $1 = a_1 < a_2 < a_3 < \cdots$ of positive integers satisfying

$$3(a_1 + a_2 + \cdots + a_n) = a_{n+1} + a_{n+2} + \cdots + a_{2n}$$

for all positive integers n.

Solution: The strictly increasing sequence (a_n) with $a_n = 2n - 1$ for all $n \in \mathbb{Z}^+$ satisfies $a_1 = 1$ and solves the given equation, since $1 + 3 + \cdots + (2n-1) = n^2$ and $(2n+1) + (2n+3) + \cdots + (4n-1) = (2n)^2 - n^2 = 3n^2$ for all $n \in \mathbb{Z}^+$.

We claim that no other sequence is suitable. Let (b_n) be a sequence that meets all requirements of the problem.

Let $k \in \mathbb{Z}^+$. Note that the given equation for k and $k+1$ implies

$$3 \cdot \sum_{l=1}^{k} b_\ell = \sum_{l=k+1}^{2k} b\ell,$$
$$3 \cdot \sum_{l=1}^{k+1} b_\ell = \sum_{l=k+2}^{2k+2} b_\ell;$$

the difference of the two equations yields $3b_{k+1} = -b_{k+1} + b_{2k+1} + b_{2k+2}$. In other words, the equation

$$4b_{k+1} = b_{2k+1} + b_{2k+2} \tag{*}$$

holds for all $k \in \mathbb{Z}^+$.

Equation (*) implies that the numbers b_{2k+1} and b_{2k+2} have the same parity for every $k \in \mathbb{Z}^+$. Since (b_n) is strictly increasing, we can deduce that $b_{2k+2} \geq b_{2k+1} + 2$. Shifting indices we also obtain $4b_{k+2} = b_{2k+3} + b_{2k+4}$ from equation (*). Note that $b_{2k+3} \geq b_{2k+2} + 1 \geq b_{2k+1} + 3$. Similarly, since b_{2k+3} and b_{2k+4} must have the same parity, $b_{2k+4} \geq b_{2k+3} + 2 \geq b_{2k+2} + 3$, so that

$$\begin{aligned} 4b_{k+2} &= b_{2k+3} + b_{2k+4} \\ &\geq (b_{2k+1} + 3) + (b_{2k+2} + 3) \\ &= 4b_{k+1} + 6. \end{aligned}$$

We can conclude that

$$b_{k+2} \geq b_{k+1} + 2 \text{ for all } k \in \mathbb{Z}^+. \tag{**}$$

Now we are ready to show that $b_n = 2n - 1$ for all $n \in \mathbb{Z}^+$. More precisely, we use strong induction to show that $b_{2k-1} = 4k - 3$ and $b_{2k} = 4k - 1$ for all $k \in \mathbb{Z}^+$. The claim implies $b_n = 2n - 1$ for all $n \in \mathbb{Z}^+$.

For the start of the induction, note that we have $b_1 = 1$ by definition; the given condition for $n = 1$ implies $b_2 = 3b_1 = 3$. Hence, the equations $b_{2k-1} = 4k - 3$ and $b_{2k} = 4k - 1$ are true for $k = 1$.

For the induction step, let $k \geq 1$ and assume that $b_{2\ell-1} = 4\ell - 3$ and $b_{2\ell} = 4\ell - 1$ for all $l \in \{1, \ldots, k\}$. We want to show that $b_{2k+1} = 4k + 1$ and $b_{2k+2} = 4k + 3$.

Since $k+1 \leq 2k$ the induction hypothesis implies $b_{k+1} = 2k+1$. Equation (*) implies $b_{2k+1} + b_{2k+2} = 8k + 4$. By induction hypothesis $b_{2k} = 4k - 1$, so that by virtue of inequality (**) we have $b_{2k+1} \geq 4k + 1$ and $b_{2k+2} \geq 4k + 3$. Since the sum of the two function values is $8k + 4$, we must have $b_{2k+1} = 4k + 1$ and $b_{2k+2} = 4k + 3$.

Problem 2: Let $a_1, a_2, \ldots, a_{2023}$ be positive real numbers with

$$a_1 + a_2^2 + a_3^3 + \cdots + a_{2023}^{2023} = 2023.$$

Show that

$$a_1^{2023} + a_2^{2022} + \cdots + a_{2022}^2 + a_{2023} > 1 + \frac{1}{2023}.$$

Solution: Let us prove that conversely, the condition

$$a_1^{2023} + a_2^{2022} + \cdots + a_{2023} \le 1 + \frac{1}{2023}$$

implies that

$$S := a_1 + a_2^2 + \cdots + a_{2023}^{2023} < 2023.$$

This is trivial if all a_i are less than 1. So suppose that there is an i with $a_i \ge 1$, clearly it is unique and $a_i < 1 + \frac{1}{2023}$. Then we have

$$\begin{aligned} a_i^i &< \left(1 + \frac{1}{2023}\right)^{2023} = 1 + \sum_{k=1}^{2023} \frac{1}{k!} \cdot \frac{2023}{2023} \cdot \frac{2022}{2023} \cdots \cdot \frac{2023 - k + 1}{2023} \\ &< 1 + \sum_{k=1}^{2023} \frac{1}{k!} \le 1 + \sum_{k=0}^{2022} \frac{1}{2^k} < 3, \end{aligned}$$

$$\sum_{\substack{k=1,\\ k\neq i}}^{1011} a_k^k \le 1011 \quad \text{and} \quad \sum_{\substack{k=1012,\\ k\neq i}}^{2023} a_k^k \le \sum_{\substack{k=1012,\\ k\neq i}}^{2023} a_k^{2024-k} < \frac{1}{2023}.$$

Hence we have

$$S = a_i^i + \sum_{\substack{k=1,\\ k\neq i}}^{1011} a_k^k + \sum_{\substack{k=1012,\\ k\neq i}}^{2023} a_k^k < 3 + 1011 + \frac{1}{2023} < 2023.$$

Remark: While the estimates might seem crude, the resulting bound is not so far away from the truth: If we replace 2023 by n and the bound by $1 + c_n$, then our argument shows that $c_n \ge \frac{1}{n}$, at least for large n, while the optimal bound has $c_n \asymp \frac{\log n}{n}$ (as in fact a slightly more careful version of our argument immediately shows!).

Problem 3: Denote a set of equations in the real numbers with variables $x_1, x_2, x_3 \in \mathbb{R}$ *Flensburgian* if there exists an $i \in \{1, 2, 3\}$ such that every solution of the set of equations where all the variables are pairwise different, satisfies $x_i > x_j$ for all $j \neq i$.

Determine for which positive integers $n \geq 2$, the following set of two equations

$$a^n + b = a \text{ and } c^{n+1} + b^2 = ab$$

in the three real variables a, b, c is Flensburgian.

Solution: The set of equations given in the problem statement is Flensburgian precisely when n is even.

To see that it is not Flensburgian when $n \geq 3$ is odd, notice that if (a, b, c) satisfies the set of equations then so does $(-a, -b, -c)$. Hence, if there exists a single solution to the set of equation where all the variables are different then the set of equations cannot be Flensburgian. This is in fact the case, e.g., consider $(a, b, c) = \left(\frac{1}{2}, \frac{2^{n-1}-1}{2^n}, \left(\frac{2^{n-1}-1}{2^{2n}}\right)^{\frac{1}{n+1}}\right)$.

The rest of the solution is dedicated to prove that the set of equations is indeed Flensburgian when n is even.

The first equation yields $b = a - a^n \leq a$, since $a^n \geq 0$ when n is even. The inequality is strict whenever $a \neq 0$ and the case $a = 0$ implies $b = 0$, i.e. $a = b$, which we can disregard. Substituting the relation $b = a - a^n$ into the second equation yields

$$\begin{aligned} 0 &= c^{n+1} + (a - a^n)^2 - a(a - a^n) = c^{n+1} + a^{2n} - a^{n+1}, \text{ i.e.} \\ c^{n+1} &= a^{n+1} - a^{2n} < a^{n+1} \end{aligned}$$

since we can disregard $a = 0$ and $2n$ is even. Since $n+1$ is odd, the polynomial x^{n+1} is strictly increasing, implying that $c < a$. Hence, when n is even, all solutions of the set of equations where a, b, c are pairwise different satisfy $a > b$ and $a > c$.

Problem 4: Determine all functions $f\colon \mathbb{R} \to \mathbb{R}$ that satisfy

$$f(f(x)+y)+xf(y)=f(xy+y)+f(x)$$

for all real numbers x and y.

Solution: Let $P(x,y)$ denote the assertion of the given functional equation.

Claim 1: $f(0)=0$.

Proof. Note that $P(0,y)$ and $P(x,0)$ gives us the following:

$$\begin{aligned} f(y+f(0)) &= f(y)+f(0) \\ f(f(x))+xf(0) &= f(0)+f(x). \end{aligned}$$

Consider the first expression. Plugging $y=-f(0)$ in it yields

$$f(-f(0)+f(0))=f(-f(0))+f(0), \text{ i.e. } f(-f(0))=0.$$

If we denote $-f(0)=a$, then we have $f(a)=0$. Plugging $x=a$ in the second expression gives us:

$$f(f(a))+af(0)=f(0)+f(a), \text{ i.e. } af(0)=0.$$

This either means that $a=0$, i.e. $f(0)=0$ or $f(0)=0$. In both cases the claim is proved. □

Since $f(0)=0$, the expression $P(x,0)$ becomes

$$f(f(x))=f(x). \tag{*}$$

Claim 2: $f(1)=1$ or $f(x)=0$ for all real numbers x.

Proof. Consider $P(x,1)$:

$$f(f(x)+1)+xf(1)=f(x+1)+f(x).$$

Replacing x by $f(x)$ and using (*) leads to:

$$\begin{aligned} f(f(f(x))+1)+f(x)f(1) &= f(f(x)+1)+f(f(x)) \\ f(f(x)+1)+f(x)f(1) &= f(f(x)+1)+f(x) \\ f(x)f(1) &= f(x). \end{aligned}$$

Suppose that there does not exist such b that $f(b)\neq 0$, then $f(x)=0$ for all real numbers x. Otherwise $f(b)f(1)=f(b)$ implies $f(1)=1$ as desired. □

Claim 3: If $f(1) = 1$ and $f(a) = 0$, then $a = 0$.

Proof. Suppose $f(a) = 0$ for some real number a. Then $P(a, 1)$ gives us

$$\begin{aligned} f(f(a) + 1) + af(1) &= f(a + 1) + f(a) \\ f(1) + a &= f(a + 1) = a + 1. \end{aligned}$$

On the other hand $P(1, a)$ leads us to the following:

$$\begin{aligned} f(f(1) + a) + f(a) &= f(2a) + f(1) \\ f(a + 1) &= f(2a) + 1 \\ a + 1 &= f(2a) + 1 \\ f(2a) &= a. \end{aligned}$$

Taking f from both sides in the last relation and using (*) leads to:

$$0 = f(a) = f(f(2a)) = f(2a) = a.$$

This proves the claim. □

To finish the problem, consider $P(x, x - f(x))$:

$$xf(x - f(x)) = f((x - f(x)) \cdot (x + 1)).$$

Setting $x = -1$ gives us

$$-f(-1 - f(-1)) = f((-1 - f(-1)) \cdot 0) = f(0) = 0.$$

From Claim 3 for $f \not\equiv 0$ we obtain that $-1 - f(-1) = 0$ implies $f(-1) = -1$. Now looking at $P(-1, y)$ and replacing y by $y + 1$, we get that

$$f(y - 1) = f(y) - 1 \text{ implies } f(y + 1) = f(y) + 1.$$

On the other hand, $P(x, 1)$, the previous relation and (*) give us the following:

$$\begin{aligned} f(f(x) + 1) + x &= f(x + 1) + f(x) \\ f(f(x)) + 1 + x &= f(x) + 1 + f(x) \\ f(x) + x &= 2f(x) \\ f(x) &= x. \end{aligned}$$

Thus, the only possible functions that satisfy the given relation are $f(x) = x$ and $f(x) = 0$. It is easy to check that they indeed solve the functional equation.

Problem 5: Find the smallest positive real number α, such that

$$\frac{x+y}{2} \geq \alpha\sqrt{xy} + (1-\alpha)\sqrt{\frac{x^2+y^2}{2}}$$

for all positive real numbers x and y.

Solution: Let us prove that $\alpha = \frac{1}{2}$ works. Then the following inequality should hold for all positive real numbers x and y:

$$\begin{aligned}
&\frac{x+y}{2} \geq \frac{1}{2}\sqrt{xy} + \frac{1}{2}\sqrt{\frac{x^2+y^2}{2}} \\
\iff &(x+y)^2 \geq xy + \frac{x^2+y^2}{2} + 2\sqrt{xy \cdot \frac{x^2+y^2}{2}} \\
\iff &(x+y)^2 \geq 4\sqrt{xy \cdot \frac{x^2+y^2}{2}} \\
\iff &(x+y)^4 \geq 8xy(x^2+y^2) \\
\iff &(x-y)^4 \geq 0
\end{aligned}$$

which is true, so we showed that $\alpha = \frac{1}{2}$ actually works.

Now it remains to show that $\alpha \geq \frac{1}{2}$. Let's consider $x = 1+\varepsilon$ and $y = 1-\varepsilon$ where $\varepsilon < 1$. Then the inequality becomes

$$1 \geq \alpha\sqrt{1-\varepsilon^2} + (1-\alpha)\sqrt{1+\varepsilon^2}, \text{ i.e. } \alpha \geq \frac{\sqrt{1+\varepsilon^2}-1}{\sqrt{1+\varepsilon^2}-\sqrt{1-\varepsilon^2}}.$$

Notice that

$$\begin{aligned}
&\frac{\sqrt{1+\varepsilon^2}-1}{\sqrt{1+\varepsilon^2}-\sqrt{1-\varepsilon^2}} \\
&= \frac{(\sqrt{1+\varepsilon^2}-1)(\sqrt{1+\varepsilon^2}+1)(\sqrt{1+\varepsilon^2}+\sqrt{1-\varepsilon^2})}{(\sqrt{1+\varepsilon^2}-\sqrt{1-\varepsilon^2})(\sqrt{1+\varepsilon^2}+\sqrt{1-\varepsilon^2})(\sqrt{1+\varepsilon^2}+1)} \\
&= \frac{\varepsilon^2(\sqrt{1+\varepsilon^2}+\sqrt{1-\varepsilon^2})}{2\varepsilon^2(\sqrt{1+\varepsilon^2}+1)} = \frac{\sqrt{1+\varepsilon^2}+1-1+\sqrt{1-\varepsilon^2}}{2(\sqrt{1+\varepsilon^2}+1)} \\
&= \frac{1}{2} - \frac{1-\sqrt{1-\varepsilon^2}}{2(\sqrt{1+\varepsilon^2}+1)} = \frac{1}{2} - \frac{(1-\sqrt{1-\varepsilon^2})(1+\sqrt{1-\varepsilon^2})}{2(\sqrt{1+\varepsilon^2}+1)(1+\sqrt{1-\varepsilon^2})} \\
&= \frac{1}{2} - \frac{\varepsilon^2}{2(\sqrt{1+\varepsilon^2}+1)(1+\sqrt{1-\varepsilon^2})} > \frac{1}{2} - \frac{\varepsilon^2}{4\cdot(1+\sqrt{2})}.
\end{aligned}$$

As ε can be arbitrarily small this expression can get arbitrarily close to $\frac{1}{2}$. This means that $\alpha < \frac{1}{2}$ cannot hold, as desired.

2nd Solution: We substitute $p = xy$, $q = \frac{x^2+y^2}{2}$. Note that $(x+y)^2 = 2(p+q)$. Hence, the given inequality is equivalent to

$$\sqrt{\frac{p+q}{2}} \geq \alpha\sqrt{p} + (1-\alpha)\sqrt{q}. \tag{*}$$

By the inequality between arithmetic and geometric mean, we always have $q \geq p$. Conversely, given $q \geq p > 0$ we can always find $x, y > 0$ with $p = xy$, $q = \frac{x^2+y^2}{2}$, namely

$$x = \sqrt{q + \sqrt{q^2 - p^2}}, \quad y = \sqrt{q - \sqrt{q^2 - p^2}}.$$

Hence, α satisfies the condition if and only if (*) holds for all $q \geq p > 0$.

Now if $\alpha = \frac{1}{2}$ then (*) reads $\sqrt{\frac{p+q}{2}} \geq \frac{\sqrt{p}+\sqrt{q}}{2}$, which follows directly from the inequality between arithmetic and quadratic mean.

We now show that $\alpha < \frac{1}{2}$ does not work. We consider $p = 1$ and write

$$g(q) = \sqrt{\frac{1+q}{2}} - \alpha - (1-\alpha)\sqrt{q}$$

for $q \geq 1$. Note that $g(1) = 0$ and

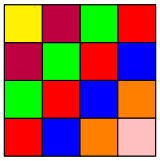
$$g'(q) = \frac{1}{2\sqrt{2(1+q)}} - \frac{1-\alpha}{2\sqrt{q}}.$$

Hence, $g'(1) = \frac{1}{4} - \frac{1-\alpha}{2} = \frac{2\alpha-1}{4}$. If $\alpha < \frac{1}{2}$ we thus have $g'(1) < 0$, which means that $g(q) < 0$ for q sufficiently close to 1. This shows that the inequality (*) is false for such a choice of q, which completes the proof.

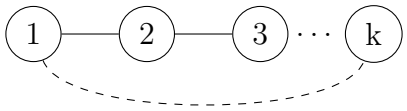
Problem 6: Let n be a positive integer. Each cell of an $n \times n$ table is coloured in one of k colours where every colour is used at least once. Two different colours A and B are said to touch each other, if there exists a cell coloured in A sharing a side with a cell coloured in B. The table is coloured in such a way that each colour touches at most 2 other colours. What is the maximal value of k in terms of n?

Solution: $k = 2n - 1$ when $n \neq 2$ and $k = 4$ when $n = 2$.

$k = 2n - 1$ is possible by colouring diagonally as shown in the figure below and when $n = 2$, $k = 4$ is possible by colouring each cell in a unique colour.



We consider the graph, where each node represents a colour and two nodes are linked, if the colours they represent touch. This graph is connected and since each colour touches at most 2 colours every node has at most degree 2. This means that the graph is either one long chain or one big cycle.



We now look at the case when n is odd. Consider the cell in the center of the table. From this cell we can get to any other cell by passing through at most $n - 1$ cells. Therefore from the node representing this cell, we can get to any node through at most $n - 1$ edges. But if the graph has $2n$ or more nodes, then for every node there is a node which is more than $n - 1$ edges away. So we must have $k \leq 2n - 1$ for all odd n.

When n is even we consider the 4 center cells. If they all have a different colour, then they form a 4-cycle in the graph, meaning the graph has only 4 nodes. If two of the center cells have the same colour, then from this colour you will be able to get to all other cells passing thorugh at most $n - 1$ cells. By same the arguments as in the odd case, we get $k \leq \max(2n - 1, 4)$ for even n.

So overall we have $k \leq 2n - 1$ for $n \neq 2$ and $k \leq 4$ for $n = 2$ as desired.

Problem 7: A robot moves in the plane in a straight line, but every one meter it turns 90° to the right or to the left. At some point it reaches its starting point without having visited any other point more than once, and stops immediately. What are the possible path lengths of the robot?

Solution: Let us define the coordinates system with unit length of one meter, point of origin in the starting point and vertical-horizontal axes. W.l.o.g. assume that the first move was east and the path had length of n. Then each odd move changed x coordinate of the robot by 1 and each even move changed y coordinate by 1.

At the end of the day both coordinates were equal to zero again, so there had to be even number of odd and even number of even moves. That implies that only n divisible by 4 can fulfill the conditions.

For $n = 4$ we have a square path. For $n = 8$ we had 4 changes of x coordinate and 4 changes of y, so the whole path was inside some 2×2 square. Unfortunately that's not possible without reaching some point twice.

Now, we will prove that all $n > 8$ divisible by 4 are good. For $n = 12$ there is a path in shape of "+" with first 4 moves like $(\rightarrow, \uparrow, \rightarrow, \uparrow)$. Now we can change the middle $(\uparrow, \rightarrow)$ sequence by $(\downarrow, \rightarrow, \uparrow, \rightarrow, \uparrow, \leftarrow)$. Thanks to this change the robot explored new territory south-east from the one before explored. We got +4 of length of the path. There we can do it again and again, reaching any length of $4k + 8$ for all $k \in \mathbb{Z}^+$.

Problem 8: In the city of Flensburg there is a single, infinitely long, street with houses numbered 2, 3, ... The police in Flensburg is trying to catch a thief who every night moves from the house where she is currently hiding to one of its neighbouring houses.

To taunt the local law enforcement the thief reveals every morning the highest prime divisor of the number of the house she has moved to.

Every Sunday afternoon the police searches a single house, and they catch the thief if they search the house she is currently occupying. Does the police have a strategy to catch the thief in finite time?

Solution: We will prove that the police is always able to catch the thief in finite time.

Let h_i denote the house the thief stays at the i-th night and p_i denote the greatest prime divisor of h_i.

The police knows that she stays at different neighbouring houses every night, so $h_{i+1} - h_i = 1$ for all non-negative integers i. Let us assume that the police is given the address of the thief's first two hiding spots, then we will prove by induction that the police can determine h_i precisely except being unable to distinguish between houses numbered 2 and 4.

Assume the police knows h_{i-2} and h_{i-1}, then they known that $h_i = h_{i-2}$ or $h_i = 2h_{i-1} - h_{i-2}$. In the first case they will receive $p_i = p_{i-2}$ and in the latter case they will receive p_i as the biggest prime divisor of $2h_{i-1} - h_{i-2}$. Assume that they are unable to distinguish between these two cases, i.e., that $p_i = p_{i-2}$, which implies

$$p_{i-2} \mid 2h_{i-1} - h_{i-2}, \text{ i.e. } p_{i-2} \mid 2h_{i-1}, \text{ i.e. } p_{i-2} \mid 2, \text{ i.e. } p_{i-2} = 2$$

since $h_{i-1} - h_{i-2} = 1$ implies $\gcd(h_{i-1}, h_{i-1}) = 1$. Moreover, since $p_i = p_{i-2} = 2$ are the biggest prime divisors of $h_i = 2h_{i-1} - h_{i-2}$ and h_{i-2} they must both be powers of 2. However, the only powers of two with a difference of exactly 2 are 2 and 4. Hence $\{h_{i-2}, 2h_{i-1} - h_{i-2}\} = \{2, 4\}$, i.e. $h_{i-1} = \frac{2+4}{2} = 3$.

Thus, either the police will with certainty be able to determine h_i or $h_{i-1} = 3$, in which case h_i may equal either 2 or 4. To complete the inductive step we observe that the police is always able to determine the parity of h_j, since it changes every day. Thus, in the future if the police knows that $h_j \in [2, 4]$, then they can either determine $h_j = 3$ or $h_j \in \{2, 4\}$. However, the only way for the thief to leave the interval $[2, 4]$ is to go to house number 5, in which case the police will be alerted by receiving $p_j = 5$, and they can again with certainty determine $h_j = 5$ and $h_{j-1} = 4$ preserving our inductive hypothesis.

To summarize, if the police knows both h_0 and h_1, then they can always determine h_i with certainty until $h_{i-1} = 3$. After this point they will with known the two last hiding places of the thief if she leaves the interval $[2, 4]$, restoring the inductive hypothesis, or otherwise, if she never leaves $[2, 4]$ be able to determine his position, up to confusion about 2 and 4 using the parity of the day.

Now, to catch the thief in finite time, they may methodically try to guess all viable pairs of (h_0, h_1), i.e $h_0, h_1 \in \mathbb{N}_{\geq 2}$ and $h_0 - h_1 = 1$, of which there are countably many.

For each viable starting position, let us consider either the immediate Sunday or the one after that, since each week has an odd amount of days, we are certain that exactly one of these days gives us that the thief is hiding in an odd house (given our assumption on his starting position). Thus, due to our inductive hypothesis, we can precisely determine where the thief will be, and search this house.

If the thief is hiding in that house, the police wins, and if not, they will with certainty know that their guess of starting positions was incorrect, and move onto the next guess. By the above argument, each guess of initial starting positions requires at most two weeks, meaning that the police will catch the thief in finite time.

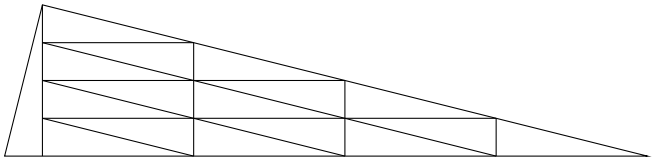
Remark: Note that if a week contained an even number of days then the police would not be able to guarantee that they would be able to catch the thief, if the thief moves between houses number 3 and $\{2, 4\}$.

Problem 9: Determine if there exists a triangle that can be cut into 101 congruent triangles.

Solution: Answer: Yes, there is.

Choose an arbitrary positive integer m and draw a height in the right triangle with ratio of legs $1 : m$. This height cuts the triangle in two similar triangles with similarity coefficient m. The largest of them can further be cut into m^2 smaller equal triangles by splitting all sides in m equal parts and connecting corresponding points with parallel lines. Thus a triangle can be split into $m^2 + 1$ equal triangles.

The figure shows this for $m = 4$, but in our problem we must take $m = 10$.



Problem 10: On a circle, $n \geq 3$ points are marked. Each marked point is coloured red, green or blue. In one step, one can erase two neighbouring marked points of different colours and mark a new point between the locations of the erased points with the third colour. In a final state, all marked points have the same colour which is called the colour of the final state. Find all n for which there exists an initial state of n marked points with one missing colour, from which one can reach a final state of any of the three colours by applying a suitable sequence of steps.

Solution: **Answer:** All even numbers n greater than 2.

We show first that required initial states are impossible for odd n. Note that if one colour is missing then the numbers of marked points of existing two colours have different parities, i.e., the difference of these numbers is odd. Each step keeps the parity of the difference of the numbers of marked points of these two colours unchanged. Hence in every intermediate state and also in the final state, one of these two colours is represented. Consequently, a final state of the third colour is impossible.

For every even number $n > 2$, an initial state with 2 consecutive points marked with one colour and $n-2$ points marked with another colour satisfies the conditions of the problem. Indeed, if $n > 4$ then with two symmetric steps, one can reach a similar state where the number of points marked with the more popular colour is 2 less. Hence it suffices to solve the case $n = 4$. In this case, making one step leads to a state with 3 marked points, all with different colours. In order to obtain a final state of any given colour, one can replace points of the other two colours with a new point of the given colour. This completes the solution.

2nd Solution:

Definition: Call a configuration *colourful*, if the final state may have any of the three colours.

The case of n being odd is excluded as in the first solution, so let $n > 2$ be even. To construct *colourful* configurations, we consider linear configurations, i.e. one where the points are placed on a line instead of a circle. There is only difference to the circular situaton: We may not choose the two end points for the replacement step. So it suffices to construct linear *colourful* configurations.

We start by providing explicit examples for $n = 4$ and $n = 6$ (with the bold letters being replaced):

$$\mathbf{RG}RG \to B\mathbf{RG} \to BB$$

$$R\mathbf{GR}G \to R\mathbf{BG} \to RR$$

$$R\mathbf{GR}G \to \mathbf{RB}G \to GG$$

$$\mathbf{RG}RRGR \to BRR\mathbf{GR} \to BR\mathbf{RB} \to B\mathbf{RG} \to BB$$

$$R\mathbf{GR}RGR \to RB\mathbf{RG}R \to \mathbf{RB}BR \to \mathbf{GB}R \to RR$$

$$R\mathbf{GR}RGR \to RB\mathbf{RG}R \to \mathbf{RB}BR \to G\mathbf{BR} \to GG.$$

Next observe that the concatenation of several linear *colourful* configurations is again *colourful*: Indeed, each part can be transformed into the desired colour independently. So the building blocks for $n = 4$ and $n = 6$ can produce *colourful* configurations of any even length.

Actually one can prove a lot more about *colourful* configurations:

Proposition: Denote the number of red resp. green resp. blue points in the initial state by R resp. G resp. B. A circular configuration is *colourful* if and only if

$$R \equiv G \equiv B \pmod 2$$

and it contains at least two colours.

Proof. We have already seen in the solution above that $R - G \bmod 2$, $G - B \bmod 2$ and $B - R \bmod 2$ are invariants. Moreover it is obvious that we need at least two colours to be able to do anything. So the conditions are necessary.

We prove that they are sufficient: For $n = 3$ the conditions require $R = G = B = 1$ and the configuration indeed *colourful*. We continue by induction for $n > 3$: As $n > 3$, there is at least one colour with more than one point, so assume wlog. $R > 1$. Having at least two colours, we can find a pair of two different colours, one of which is red. Assume w.l.o.g. that the other is green. As a first step replace these two points. The resulting configuration has $R - 1$ red, $G - 1$ green and $B + 1$ blue points, so it satisfies $R - 1 = G - 1 = B + 1 \bmod 2$. Moreover due to $R > 1$ is has at least one red and one blue point. So by induction the configuration is *colourful*, and hence so was our original state. □

This classification of *colourful* configuration, has some nice consequences:

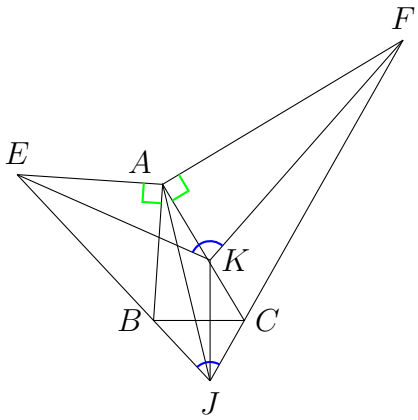
Proposition: If a circular configuration is *colourful*, then so is any permutation of its points.

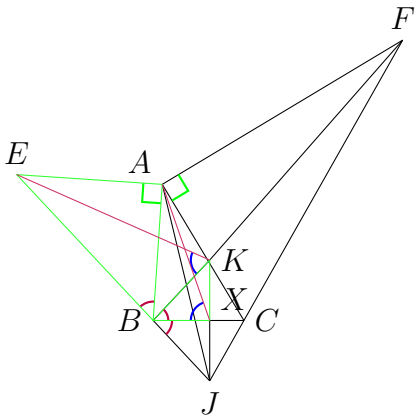
Proof. Immediate. □

Problem 11: Let ABC be a triangle and let J be the centre of the A-excircle. The reflection of J in BC is K. The points E and F are on BJ and CJ, respectively, such that $\angle EAB = \angle CAF = 90°$. Prove that $\angle FKE + \angle FJE = 180°$.

Remark: The A-excircle is the circle that touches the side BC and the extensions of AC and AB.

Solution:





Let JK intersect BC at X. We will prove a key claim:

Claim: BEK is similar to BAX.

Proof. Note that $\angle EAB = 90° = \angle KXB$. Also, since BJ bisects $\angle CBA$, we get $\angle ABE = \angle JBX = \angle XBK$. Hence $EBA \sim KBX$. From that, we see that the spiral similarity that sends the line segment EA to KX has centre B. So the spiral similarity that sends the line segment EK to AX has centre B. Thus $BEK \sim BAX$. □

In a similar manner, we get CFK is similar to CAX.

Now, using the similar triangles and the fact that K and J are symmetric in BC, we have

$$\begin{aligned}\angle FKE + \angle FJE &= \angle FKE + \angle BKC \\ &= 360° - \angle EKB - \angle CKF \\ &= 360° - \angle AXB - \angle CXA \\ &= 360° - 180° \\ &= 180°\end{aligned}$$

as desired. □

Problem 12: Let ABC be an acute triangle with $AB > AC$. The internal angle bisector of $\angle BAC$ intersects BC at D. Let O be the circumcentre of ABC. Let AO intersect the segment BC at E. Let J be the incentre of AED. Prove that if $\angle ADO = 45^\circ$ then $OJ = JD$.

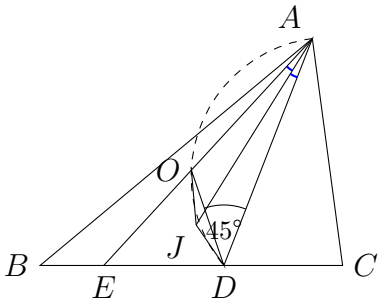
Solution: Let $\alpha = \angle BAC$, $\beta = \angle CBA$, $\gamma = \angle ACB$. We have

$$\begin{aligned}\angle DJA &= 90^\circ + \frac{1}{2}\angle DEA = 90^\circ + \frac{1}{2}(\angle EBA + \angle BAE)\\ &= 90^\circ + \frac{1}{2}(\beta + 90^\circ - \gamma) = 135^\circ + \frac{\beta}{2} - \frac{\gamma}{2}\end{aligned}$$

and

$$\begin{aligned}\angle DOA &= 180^\circ - \angle OAD - \angle ADO = 180^\circ - (\angle OAC - \angle DAC) - 45^\circ\\ &= 135^\circ - \left(90^\circ - \beta - \frac{\alpha}{2}\right) = 135^\circ - \left(\frac{1}{2}(\alpha + \beta + \gamma) - \beta - \frac{\alpha}{2}\right)\\ &= 135^\circ + \frac{\beta}{2} - \frac{\gamma}{2}.\end{aligned}$$

Therefore, $\angle DJA = \angle DOA$, hence quadrilateral $ADJO$ is cyclic. Since AJ is the bisector of $\angle OAD$, the arcs OJ and JD are equal. Hence $OJ = JD$.



Problem 13: Let ABC be an acute triangle with $AB < AC$ and incentre I. Let D be the projection of I onto BC. Let H be the orthocentre of ABC. Given $\angle IDH = \angle CBA - \angle ACB$, prove that $AH = 2 \cdot ID$.

Solution: Let H' be the reflection of H in BC. It is well-known (and easy to prove) that H' lies on the circumcircle of ABC. Let O be the circumcentre of ABC. We have

$$\begin{aligned}\angle OH'A = \angle HAO &= \angle BAC - \angle BAH - \angle OAC \\ &= \angle BAC - 2\,(90^\circ - \angle CBA) = \angle CBA - \angle ACB \\ &= \angle IDH = \angle H'HD = \angle DH'A,\end{aligned}$$

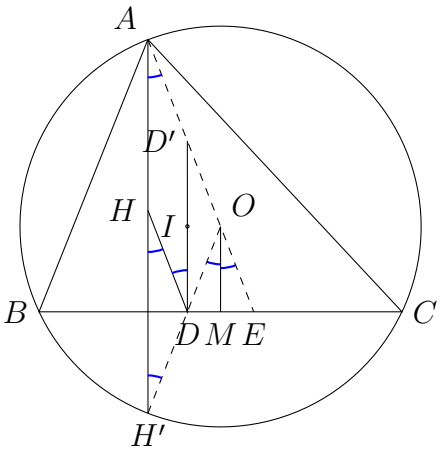
hence O, D, H' are collinear. Also note that $\angle HAO = \angle H'HD$ implies that $AO \parallel HD$.

Let M be the midpoint of BC. Let E be the reflection of D in M. We have

$$\angle MOE = \angle DOM = \angle OH'A = \angle HAO.$$

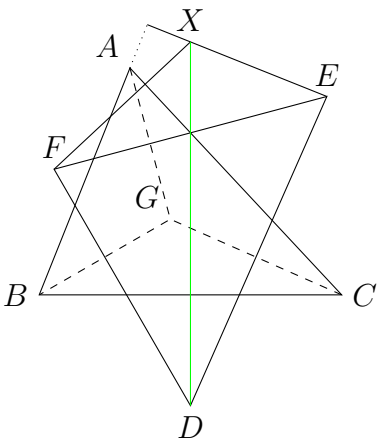
Since $OM \parallel AH$, the above equality gives that A, O, E are collinear.

Let D' be the reflection of D in I. It is well-known (and easy to prove) that D' lies on AE. Since $AH \parallel OM$ and $AD' \parallel HD$, quadrilateral $AHDD'$ is a parallelogram. Therefore $AH = DD' = 2 \cdot ID$.



Problem 14: Let ABC be a triangle with centroid G. Let D, E and F be the circumcentres of BCG, CAG and ABG, respectively. Let X be the intersection of the perpendiculars from E to AB and from F to AC. Prove that DX bisects the segment EF.

Solution:



In all three solutions we will prove that the D-median coincides with the perpendicular bisector of the segment BC. Thus the solutions con- sist of two parts, proving that X lies on the perpendicular bisector of BC and proving that the midpoint of EF lies on the perpendicular bisector of BC.

The two parts may be completed independently, and in the three solutions below we demonstrate different approaches to both parts, though one can create valid solutions combining either first part with either second part.

Let ω_B, ω_C denote the circumcircles of triangles ABG and ACG respectively, and the points Y and Z the second intersection of the line through B parallel to AC and ω_B and the second intersection of the line through C parallel to AB and ω_C.

The lines BY and CZ thus intersects at A', the reflection of A across the midpoint of BC, and in particular on the A-median. Using Power of a Point from A' with respect to the circles ω_B and ω_C we obtain $A'B \cdot A'Y = A'A \cdot A'G = A'C \cdot A'E$ implying from the converse of Power of a Point that the quadrilateral $YBCZ$ is cyclic. The perpendicular bisector of BY is orthogonal to $BY \parallel AC$ and passes through F and thus X as well. Similarly, the perpendicular bisector of CZ passes through Z. Hence X is the centre of circle $(YBCZ)$ and thus on the perpendicular bisector of the line BC.

Let M and N denote the midpoints of BC and EF, respectively. To prove that N lies on the perpendicular bisector of BC, let V and W denote the second intersections of ω_B and ω_C with the line BC, respectively.

From Power of a Point from M with respect to ω_B and ω_C we obtain $MV \cdot MB = MG \cdot MA = WM \cdot CM$, i.e. $MV = WM$, so M is the midpoint of the segment VW. Let E', N', F' denote the projections of E, N and F onto BC respectively. Since N is the midpoint of EF, N' will be the midpoint of $E'F'$.

Moreover, from the fact that E and F are the centres of ω_B and ω_C we get that E' and F' are the midpoints of BV and WC, and hence M is the midpoint $E'F'$ as well, implying $N' = M$ and that N is on the perpendicular bisector of BC.

2nd Solution: Let G' denote the reflection of G across the midpoint of BC. We begin by proving that triangles ABC and DFE are orthological, with orthology centres G' and X.

Observe that G' is on the A-median and thus $AG' \perp EF$. Furthermore, quadrilateral $BGCG'$ is a parellelogram and hence $BG' \parallel CG \perp DE$ and $CG' \parallel BG \perp DF$. Hence, G' is the first orthology centre of ABC and DFE.

Thus, by the property of orthologoical triangle, the second orthology centre must exists, which is defined as the common intersection of the normal from D to BC, E to AB and F to AC, i.e. the point X. Since D is on the perpendicular bisector of BC, by virtue of being the circumcentre of triangle BGC, and $XD \perp BC$ so must point X.

Moreover, let O denote the circumcentre of triangle ABC. Then $EO \perp AC \perp FX$ implies $EO \parallel FX$ and $FO \perp AB \perp EX$ implies $FO \parallel EX$, meaning that quadrilateral $FOEX$ is a parallelogram. Hence, the midpoint of EF lies on the line $\overline{XOD}$ i.e. the perpendicular bisector of segment BC.

3rd Solution: Let M be the midpoint of BC. Let N be the intersection of EF and DM. We claim that N is the midpoint of EF.

Namely, we have $DEN \sim CGM$ because corresponding pairs of sides are orthogonal. Similarly, $DFN \sim BGM$. Hence

$$\frac{EN}{ND} = \frac{GM}{MC} = \frac{GM}{MB} = \frac{FN}{ND},$$

proving that $EN = FN$, as desired.

Next, let X' resp. X'' denote the intersection of DN with the perpendicular from E to AB resp. the perpendicular from F to AC. Just as above we have $ENX' \sim AMB$ and $FNX'' \sim AMC$, thus

$$\frac{X'N}{NE} = \frac{BM}{MA} = \frac{CM}{MA} = \frac{X''N}{NF}.$$

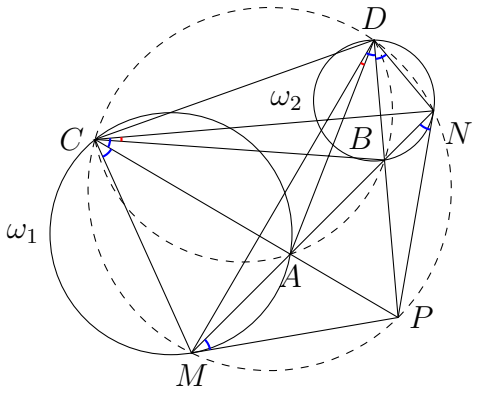
Since N is the midpoint of EF, we get $X'N = X''N$, hence $X' = X''$ for orientation reasons (note that by the above similarities, X' and X'' must lie on the same side of EF).

This shows that $X = X' = X''$ lies on DN.

Remark: That the medians of triangle DEF coincide with the perpendicular bisectors of triangle ABC implies that the centroid of DEF coincides with the circumcentre of ABC. It is possible to ask for this in the problem instead, but then the problem becomes significantly easier, only requiring the second part of the first solution.

Problem 15: Let ω_1 and ω_2 be circles with no common points, such that neither circle lies inside the other. Points M and N are chosen on the circles ω_1 and ω_2, respectively, such that the tangent to the circle ω_1 at M and the tangent to the circle ω_2 at N intersect at P and such that PMN is an isosceles triangle with $PM = PN$. The circles ω_1 and ω_2 meet the segment MN again at A and B, respectively. The line PA meets the circle ω_1 again at C and the line PB meets the circle ω_2 again at D. Prove that $\angle BCN = \angle ADM$.

Solution:



Since MPN is an isosceles triangle, we have $\angle PMA = \angle PMN = \angle MNP = \angle BNP$. By tangent and chord theorem, $\angle MCA = \angle PMA = \angle BNP = \angle BDN$.
Since $\angle MCP = \angle MNP$, the quadrilateral $CMPN$ is cyclic. Analogously, from $\angle PDN = \angle PMN$, we get that $NDMP$ is cyclic. Since C and D both lie on the circumcircle of NPM, points P, N, M, C and D are concyclic.
From inscribed angles subtending arcs with the same length, we get that $\angle MDP = \angle MCP = \angle MNP = \angle PDN = \angle PMN = \angle PCN$.

The power of P with respect to ω_1 gives us that $PM^2 = PA \cdot PC$. The power of P with respect to ω_2 gives us that $PN^2 = PB \cdot PD$. Since $PM = PN$, the powers of P with respect to ω_1 and ω_2 are equal (P lies on the radical axis). Hence, $PA \cdot PC = PB \cdot PD$, which implies that $ABDC$ is cyclic. From inscribed angles subtending the arc AB, we get that $\angle ACB = \angle ADB$.

Hence, $\angle BCN = \angle ACN - \angle ACB = \angle MDB - \angle ADB = \angle MDA$.

Remark: There are several other ways to show that $\angle MDP = \angle PCN$, for example by observing that CP bisects the angle $\angle MCN$ (since $MPNC$ is cyclic and MPN is isosceles) and similarly DP bisects $\angle MDN$.

Another option is to apply inversion around P with radius $PM = PN$, noting that it interchanges A and C (resp. B and D).

Problem 16: Prove that there exist nonconstant polynomials f and g with integer coefficients such that, for infinitely many primes p, there are no integers x and y with $p \mid f(x) - g(y)$.

Solution: We take $f(x) = (x^2+1)^2$ and $g(y) = -(y^2+1)^2$ and prove for all $p \equiv 3 \pmod 4$ that $f(x) \equiv g(y) \pmod p$ has no solution. Famously, there are infinitely many primes congruent to 3 modulo 4.

Recall the fact that if $p \equiv 3 \pmod 4$ then the only solution to $a^2 + b^2 \equiv 0 \pmod p$ is $a \equiv b \equiv 0 \pmod p$. Hence, for $f(x) \equiv g(y) \pmod p$ to hold, we need

$$(x^2+1)^2 + (y^2+1)^2 \equiv 0 \pmod p$$

and thus

$$x^2 + 1 \equiv y^2 + 1 \equiv 0 \pmod p,$$

which is impossible for $p \equiv 3 \pmod 4$.

Problem 17: Let $S(m)$ be the sum of the digits of the positive integer m. Find all pairs (a, b) of positive integers such that $S(a^{b+1}) = a^b$.

Solution: **Answer:** $(a, b) \in \{(1, b) \mid b \in \mathbb{Z}^+\} \cup \{(3, 2), (9, 1)\}$.

Let k denote the number of digits of a. Then $10^{k-1} \le a < 10^k$ and, therefore, $10^{(k-1)b} \le a^b$ and $a^{b+1} < 10^{k(b+1)}$. Of course, the digits are at most 9, so $S(a^{b+1}) \le 9 \cdot k(b+1)$. We get

$$10^{(k-1)b} \le a^b = S(a^{b+1}) \le 9 \cdot k(b+1), \text{ i.e. } 10^{(k-1)b} \le 9 \cdot k(b+1).$$

Let us consider the case where $k \ge 2$. Then $k \le 2(k-1)$ and note that $b+1 \le 2b$ as $b \ge 1$. Put $(k-1)b =: x$, then $k(b+1) \le 4(k-1)b = 4x$. So $10^x \le 36x$. It is obvious that the only solutions in nonnegative integers to this inequality are $x = 0$ and $x = 1$. Indeed, for $x \ge 2$, the left hand side grows faster. Therefore, either $k = 1$ or $k = 2$ and $b = 1$.

Now we have only two cases left.

Case 1: $b = 1$ and $k = 2$. We are left with the equation $S(a^2) = a$, for $10 \le a < 100$. Then $a^2 < 10^4$, so $a = S(a^2) \le 9 \cdot 4 = 36$.

Moreover, taking into account the fact that the sum of digits does not change the number modulo 9, $a^2 \equiv a \pmod 9$, i.e., $a(a-1) \equiv 0 \pmod 9$, therefore $a \equiv 0 \pmod 9$ or $a \equiv 1 \pmod 9$. So now we are left only with numbers $a \in \{10, 18, 19, 27, 28, 36\}$, which we can easily check by substitution and see that there are no solutions.

Case 2: $k = 1$. In the same way, looking modulo 9, we get that $a^{b+1} \equiv a^b \pmod 9$ implies $a^b(a-1) \equiv 0 \pmod 9$. Therefore either $a = 1$ or a is divisible by 3. $a = 1$ is an obvious solution with all $b \in \mathbb{Z}^+$.

Otherwise, $a \in \{3, 6, 9\}$. But then $a^{b+1} < 10^{b+1}$ and $S(a^{b+1}) \le 9(b+1)$. Therefore, $3^b \le a^b = S(a^{b+1}) \le 9(b+1)$. But from $3^b \le 9(b+1)$, we can conclude $b \le 3$. Indeed, for $b \ge 4$, the left hand side increases faster. So we are left with $a \in \{3, 6, 9\}$ and $b \le 3$. We check all these cases to determine that only $(a, b) = (3, 2)$ or $(a, b) = (9, 1)$ are solutions.

Problem 18: Let $p > 7$ be a prime number and let A be a subset of $\{0, 1, \ldots, p-1\}$ consisting of at least $\frac{p-1}{2}$ elements. Show that for each integer r, there exist (not necessarily distinct) numbers $a, b, c, d \in A$ such that

$$ab - cd \equiv r \pmod{p}.$$

Solution: Let P be the set of residues modulo p of possible products ab, for $a, b \in A$. Clearly, we have $|P| \geq \frac{p-1}{2}$, since we get $|A|$ different products by fixing an arbitrary $0 \neq a \in A$ and let run b through A. If $|P| \geq \frac{p+1}{2}$, then $|r + P| \geq \frac{p+1}{2}$ as well. Hence, $|P| + |r + P| \geq p + 1 > p$, so, by the Pigeonhole Principle, P and $r + P$ must have an element in common. In other words, there are p_1, p_2 with $p_1 \equiv r + p_2 \pmod{p}$ and hence $p_1 - p_2 \equiv r \pmod{p}$, which gives a solution of the desired shape from the definition of P. So the only remaining case is that of $|P| = |A| = \frac{p-1}{2}$.

Multiplying all elements of A with the same constant and reducing modulo p, if necessary, we may assume w.l.o.g. that $1 \in A$. Then $A \subseteq P$ and hence $A = P$. This means that the product of each two non-zero elements of A is an element of A as well. Furthermore, for a fixed $0 \neq a \in A$ the products ab all differ modulo p. (It follows, that for every $0 \neq a \in A$ there is an element $b \in A$ with $ab \equiv 1 \pmod{p}$. Hence, the non-zero elements of A form a group.) Thus, if we denote $A^\star := A \setminus \{0\}$, for a fixed non-zero $a \in A$ we have

$$\prod_{b \in A^\star} b \equiv \prod_{b \in A^\star} (ab) = a^{|A^\star|} \cdot \prod_{b \in A^\star} b \pmod{p}.$$

Hence $a^{|A^\star|} \equiv 1 \pmod{p}$.

If $0 \in A$ we have $|A^\star| = \frac{p-3}{2}$. So $a^{p-3} = a^{2|A^\star|} \equiv 1 \pmod{p}$. But from Fermat's little theorem we know $a^{p-1} \equiv 1 \pmod{p}$, hence $a^2 \equiv 1 \pmod{p}$ and $a \equiv \pm 1 \pmod{p}$. We get $\frac{p-3}{2} = |A^\star| \leq 2$. This is impossible for $p > 7$.

Consequently, $0 \notin A$ and we have $A^\star = A$.

We now use the well-known fact that for every prime p there exists a primitive root, that is an integer $0 < q < p$ where the residues modulo p of the powers q^1, q^2, $\ldots$, q^{p-1} are (in some order) $1, 2, \ldots, p-1$. That is, we can write every non-zero element $a \in A$ as q^i with some $1 \leq i \leq p-1$.

If A is not the set of quadratic residues modulo p, that is the set of residues of $q^{2\cdot 1}$, $q^{2\cdot 2}$, $\ldots$, $q^{2\cdot \frac{p-1}{2}}$, then it would contain two elements with consequtive exponents, say q^i and q^{i+1}. But then we have $q^{(i+1)-i} = q \in A$ and, therefore, all powers of q. This contradicts $|A| = \frac{p-1}{2} < p-1$. Hence A exactly the set of the quadratic residues modulo p.

Replacing r by $r+p$, if necessary, one may assume r to be odd. Then we can put $b := d := 1 \in A$, as well as

$$a \equiv \left(\frac{r+1}{2}\right)^2 \pmod{p} \quad \text{and} \quad c \equiv \left(\frac{r-1}{2}\right)^2 \pmod{p}.$$

Then $a, c \in A$ as well. This yields

$$ad - bc \equiv a - c \equiv \left(\frac{r+1}{2}\right)^2 - \left(\frac{r-1}{2}\right)^2 \equiv r \pmod{p},$$

as required.

Remark: This solution avoids using knowledge from basic group theory. But clearly, with this, it could be stated in a shorter way.

Probably the result is also very far from being sharp and the $\frac{p-1}{2}$ can be replaced by something even smaller. Determining the sharp bound (or even its order of magnitude) here is most likely a very difficult problem.

2nd Solution: Since the problem only considers residue classes modulo p we reduce every number modulo p, if necessary. That is instead of the set $\{0, 1, \ldots, p-1\}$ we are working with the group of residue classes modulo p, namely $\mathbb{Z}/p\mathbb{Z}$, so the sum, product, and difference of such two residue classes always is such a residue class as well.

Claim: Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$ a set with exactly $\frac{p-1}{2}$ elements. Then for every residue class $r \in \mathbb{Z}/p\mathbb{Z}$, with at most two exceptions, there exist $a, b \in A$ with $a - b = r$.

Proof. Let r such an integer with no solutions for $a - b = r$ and $a, b \in A$. Then $r \neq 0$. Let $I \subseteq \mathbb{Z}/p\mathbb{Z}$ be the set of all i with $ir \in A$. Since $r \neq 0$ we have $|I| = |A| = \frac{p-1}{2}$. If $i \in I$ we have $i + 1 \notin I$. Otherwise $r = (i+1)r - ir$ would be a difference of two elements of A. But $|\mathbb{Z}/p\mathbb{Z} \setminus I| = p - \frac{p-1}{2} = |I| + 1$. So there is exactly one $i_0 \in I$ with $i_0 + 1, i_0 + 2 \notin I$ and for all other $i_0 \neq i \in I$ we have $i + 1 \notin I$ and $i + 2 \in I$. That is $I = \{i_0, i_0 + 3, i_0 + 5, \ldots, i_0 + p - 2\}$ and all the residue classes $\pm 3r$, $\pm 5r$, $\ldots$, $\pm(p-2)r$ are expressible as the difference of two elements of A. But these are all, with exception of $\pm r$. □

Now let r be an arbitrary residue class in $\mathbb{Z}/p\mathbb{Z}$. If there is an $0 \neq a \in A$ such that $a^{-1}r$ can be expressed as $b - d$ with $b, d \in A$, we have $r = ab - ad$. But $|\{a^{-1}r \mid a \in A, a \neq 0\}| \geq |A| - 1 = \frac{p-3}{2}$ and from the claim we know that at least $p - 2$ residue classes are expressable as difference of two elements of A. So by the Pigeonhole Principle such a solution is guaranteed if $\frac{p-3}{2} + (p-2) > p$, namely for all p with $p > 7$.

Problem 19: Show that the sum of the digits of $2^{2^{2\cdot 2023}}$ is greater than 2023.

Solution: We will prove the more general statement that, for every positive integer n, the sum of decimal digits of $2^{2^{2n}}$ is greater than n.

Let $m = 2^{2n} = 4^n$, so that we need to consider the digits of 2^m. It will suffice to prove that at least n of these digits are different from 0, since the last digit is at least 2.

Let $0 = e_0 < e_1 < \cdots < e_k$ be the positions of non-zero digits, so that $2^m = \sum_{i=0}^{k} d_i \cdot 10^{e_i}$ with $1 \le d_i \le 9$. Considering this number modulo 10^{e_j}, for some $0 < j \le k$, the residue $\sum_{i=0}^{j-1} d_i \cdot 10^{e_i}$ is a multiple of 2^{e_j}, hence at least 2^{e_j}, but on the other hand it is bounded by $10^{e_{j-1}+1}$.

It follows that $2^{e_j} < 10^{e_{j-1}+1} < 16^{e_{j-1}+1}$, and hence $e_j < 4(e_{j-1}+1)$. With $e_0 = 4^0 - 1$ and $e_j \le 4(e_{j-1}+1) - 1$, it follows that $e_j \le 4^j - 1$, for all $0 \le j \le k$. In particular, $e_k \le 4^k - 1$ and hence

$$2^m = \sum_{i=0}^{k} d_i \cdot 10^{e_i} < 10^{4^k} < 16^{4^k} = 2^{4\cdot 4^k} = 2^{4^{k+1}},$$

which yields $4^n = m < 4^{k+1}$, i.e., $n - 1 < k$. In other words, 2^m has $k \ge n$ non-zero decimal digits, as claimed.

Problem 20: Let n be a positive integer. A *German set* in an $n \times n$ square grid is a set of n cells which contains exactly one cell in each row and column. Given a labelling of the cells with the integers from 1 to n^2 using each integer exactly once, we say that an integer is a *German product* if it is the product of the labels of the cells in a German set.

(a) Let $n = 8$. Determine whether there exists a labelling of an 8×8 grid such that the following condition is fulfilled: The difference of any two German products is always divisible by 65.

(b) Let $n = 10$. Determine whether there exists a labelling of a 10×10 grid such that the following condition is fulfilled: The difference of any two German products is always divisible by 101.

Solution:

(a) No, there is no such labelling.

On the contrary, we show that for every labelling there exist two German products whose difference is not divisible by 65. Suppose that an 8×8 square grid is labelled with the numbers 1, 2, ..., 64 such that no number is used twice.

We can construct a German product that is divisible by 13 by choosing a German set that includes the cell with the label 13 and seven others in different rows and columns, but otherwise arbitrarily.

We can construct a German product that is not divisible by 13 as follows. Notice that only four labels are divisible by 13, namely 13, 26, 39, and 52. These four labels are located in at most four rows; we denote the index set of these rows $R \subseteq [1, 8]$. Similarly, there are at least four columns that do not contain any of these four labels; we denote the index set of these columns $C \subseteq [1, 8]$. Since $R \leq C$ it is possible to choose cells of a German set from rows R using only columns from C. The remaining cells are chosen from the remaining rows accordingly to the definition, but otherwise arbitrarily. The resulting German product is not divisible by 13 since the German set avoids the cells whose labels are divisible by 13.

The difference of the two German products is not divisible by 13, since one German product is divisible by 13 whereas the other one is not. Hence the difference is not divisible by 65.

(b) Yes, there is such a labelling.

For $k \in [0, 99]$ we define $a_k = 2^k \pmod{101}$; in other words, a_k is the remainder of 2^k when divided by 101. Note that $a_k \neq 0$ since no power of 2 is divisible by 101. Hence $1 \leq a_k \leq 100$ for all $k \in [0, 99]$.

We label the cells of the square grid with the numbers a_k as follows:

a_0	a_1	a_2	$\cdots$	a_9
a_{10}	a_{11}	a_{12}	$\cdots$	a_{19}
a_{20}	a_{21}	a_{22}	$\cdots$	a_{29}
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_{90}	a_{91}	a_{92}	$\cdots$	a_{99}

More precisely, if we label the rows and columns of the chessboard by $\{0, 1, 2, \ldots, 9\}$, then the cell with coordinates (i, j) gets the label a_{10i+j}.

Note that $a_{10i+j} \equiv 2^{10i+j} \pmod{101}$ and that $2^{10i+j} = (2^{10})^i \cdot 2^j$. Hence for this labelling any rook product is congruent to

$$\left(2^{10}\right)^{0+1+2+\ldots+9} \cdot 2^{0+1+2+\ldots+9}$$

modulo 101. Hence the difference of any two German products is divisible by 101 for this labelling.

It remains to show that the a_k are pairwise different. (In more elaborate language, we would say that 2 is a primitive root modulo 101.) To do this, we denote by s the smallest positive integer such that $2^s \equiv 1 \pmod{101}$. Using long division, we may write $100 = qs + r$ with non-negative integers q and r such that $0 \leq r \leq s - 1$. By virtue of Fermat's little theorem we have

$$1 \equiv 2^{100} \equiv 2^{qs+r} \equiv (2^s)^q \cdot 2^r \equiv 1^q \cdot 2^r \equiv 2^r \pmod{101}.$$

Since $r < s$ and s is the smallest positive integer with $2^s \equiv 1 \pmod{101}$, we must have $r = 0$. In other words, 100 is divisible by s; in other words, s is a divisor of 100.

We claim that $s = 100$. If this was not the case, we would have $s|20$ or $s|50$, which implies that $2^{20} \equiv 1 \pmod{101}$ or $2^{50} \equiv 1 \pmod{101}$. However $2^{10} = 1024 \equiv 14 \pmod{101}$, so that $2^{20} \equiv 14^2 \equiv 196 \equiv -6 \not\equiv 1 \pmod{101}$ and $2^{50} \equiv (2^{20})^2 \cdot 2^{10} \equiv (-6)^2 \cdot 14 \equiv 504 \equiv -1 \not\equiv 1 \pmod{101}$.

Now assume that $k, \ell \in [0, 99]$ are positive integers with $k > \ell$ and $a_k = a_\ell$. Then we have $2^k \equiv 2^\ell \pmod{101}$ and $0 \equiv 2^k - 2^\ell \equiv 2^\ell \cdot (2^{k-\ell} - 1) \pmod{101}$. Since 2^ℓ and 101 are coprime, it follows that $2^{k-\ell} - 1 \equiv 0 \pmod{101}$ and $2^{k-\ell} \equiv 1 \pmod{101}$. This cannot be true, since $k - \ell \in [1, 99]$, but $s = 100$ is the smallest positive integer with $2^s \equiv 1 \pmod{101}$. Hence $a_k \neq a_\ell$.

We conclude that the numbers a_k with $k \in [0, 99]$ are a hundred pairwise different numbers from the set $[1, 100]$, hence they are a permutation of the set $[1, 100]$ as it was required.

2nd Solution:
Definition: Let p be a prime. Consider an $n \times n$ square grid of elements $a_{i,j} \in \mathbb{F}_p^*$ (for $i, j = 1, \ldots, n$), which are not necessarily distinct. We call it *rooky*, if all its German products are equal as elements in $\mathbb{F}_p^*$.

We will provide a classification of all *rooky* square grids. Of course, most of this is not necessary when writing down a solution to the given problem, but it may still be interesting...

Lemma: A square grid is *rooky* if and only if for all i, j, k, ℓ:

$$a_{i,j} \cdot a_{k,\ell} = a_{i,\ell} \cdot a_{k,j}. \quad (1)$$

Proof. If we swap the rows of two cells in a German set and keep their columns, it turns one valid German set into another. When comparing their German products, we can ignore all $n-2$ labels of cells that were not moved. The remaining values are $a_{i,j} \cdot a_{k,\ell}$ resp. $a_{i,\ell} \cdot a_{k,j}$ for certain i, j, k, ℓ. This gives equality (1) for *rooky* square grids.

Conversely assume that (1) holds. Then we have to compare two arbitrary German products. But they can transformed into each other by a sequence of several swaps of two cells. Due to (1) the German product does not change at any of these steps, so the rook products of the original configurations are the same as well. □

Lemma: A *rooky* square grid is uniquely determined by the elements of its first row and first column.

Proof. Indeed the previous lemma implies that

$$a_{i,j} \cdot a_{1,1} = a_{i,1} \cdot a_{1,j}$$

which determines $a_{i,j}$ uniquely because $a_{1,1}$ is a unit. □

One can actually prove directly that the square grid obtained that way is *rooky*, but it is simpler to continue directly to

Proposition: Let $\lambda_i \in \mathbb{F}_p^*$ $(i = 1, \ldots, n)$ and $\mu_j \in \mathbb{F}_p^*$ $(j = 1, \ldots, n)$ arbitrary elements. Then the square grid with

$$a_{i,j} = \lambda_i \cdot \mu_j$$

is *rooky*. Moreover any *rooky* square grid can be obtained this way.

Proof. The square grid with $a_{i,j} = \lambda_i \cdot \mu_j$ is *rooky*, because any German product has the value

$$\prod_i \lambda_i \cdot \prod_j \mu_j.$$

Let us prove the converse: By the previous lemma, it suffices to find λ_is and μ_js that recreate the values of the first row and column. For this simply set $\lambda_i = a_{i,1}$ and $\mu_j = \frac{a_{1,j}}{a_{1,1}}$. □

Proposition: For any prime $p > n^2$, there exists a *rooky* square grid with only distinct elements.

Proof. Choose any primitive root $\alpha \in \mathbb{F}_p^*$. Then set $\lambda_i = \alpha^{i-1}$, $\mu_j = \alpha^{n\cdot(j-1)}$ and $a_{i,j} = \lambda_i \cdot \mu_j = \alpha^{i-1+n\cdot(j-1)}$. This provides indeed a *rooky* square grid. The values in the square are α^0, α^1, …, α^{n^2-1}. As we have chosen a primitive root, these are all distinct. □

For $n = 10$, $p = 101$ and $\alpha = 2$, this reproduces exactly the construction given in the previous solution.