

Problem 1. The sides of an acute-angled triangle are pairwise different, its orthocentre is M , the centre of its inscribed circle is K , and the centre of its circumscribed circle is O . Prove that if a circle passes through the points K , O , M and a vertex of the triangle, then it also passes through another vertex.

Solution 1. The points K , O , M lie in the interior of the triangle. If the vertices are denoted by A , B , C and the corresponding angles by α , β , γ , then $\angle BAM = 90^\circ - \beta = \angle CAO$. The second equality is true because in the isosceles triangle AOC , $\angle AOC = 2\beta$, since the angle at the centre is twice the angle at the circumference. The line AK bisects the angle BAC , so the rays AM and AO lie symmetrically on either side of the ray AK . The three rays do not coincide (or else the triangle would be isosceles). Thus the line segments KM and KO subtend equal angles at the vertex A , and the line AK separates the points M and O . It is clear that this statement remains valid if we replace A with any other vertex of the triangle.

Assume now that the points A , M , K , O are concyclic. Being so, the converse of the theorem about angles at the circumference implies that the line segments KM and KO are equal. As we have seen, they subtend equal angles at the vertices of the triangle. Let us examine, therefore, the locus of the points P where the two edges subtend equal angles.

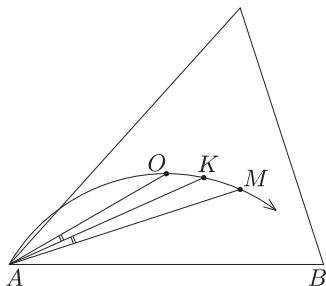


Figure 1

If that angle is φ for a given P , then P lies on one of the two arcs where the segment KM subtends an angle φ , and also on one of the two arcs where the segment KO subtends an angle φ . Let these arcs be i and j , respectively. We will call the arc i an inward arc if the arc lies on the same side of the line KM as the point O , and an outward arc if they lie on the opposite side. There will be no ambiguity, since the points K , O , M cannot be collinear. This terminology can be extended to the arc j as well, if we interchange the roles of points O and M .

If both i and j are outward arcs, their intersection (if any) lies on the perpendicular bisector f of the line segment MO , since the two arcs are congruent due to $KM = KO$. The same holds if both arcs are inward ones. The only exception is the case when the two arcs have at least two further common points in addition to their common endpoint K . This happens if and only if the two arcs are incident to the same circle, that is the circle through the points K , O , M .

Is it possible that we have one outward arc (say, the arc i) and one inward arc? In that case, the two arcs intersect each other if and only if φ is smaller than the angle KMO . Then j intersects the extension of the ray OM beyond M . At that point KM and KO subtend equal angles, so that point must be the intersection of the two arcs. Such a point, however, cannot be a vertex of the triangle ABC , since a circle through that vertex and K would not separate the points M and O .

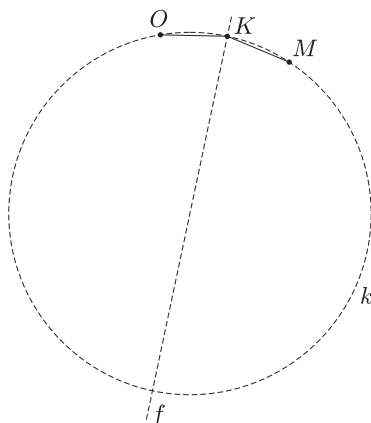


Figure 2

We can conclude that each vertex of the triangle lies either on the line f or on the circle k . Since the point K lies on f , at most one of the vertices may lie on f , and thus at least two of them must lie on the circle k . The claim is hence proved.

Solution 2 (based on the solution by *Rácz, Béla András*). Let A, B, C denote the vertices of the triangle, and assume that the points A, M, K, O are on a circle k . Note that this circle is unique since the four points are all different. According to the previous solution, $KM = KO$, that is, K lies on the perpendicular bisector f of the line segment MO . Note that the points B, O and M cannot be collinear, or else AB and BC would be equal.

Consider the intersection L of the angle bisector e of the angle MBO with the circle ℓ circumscribed about the triangle MBO . The converse of the theorem about the angles subtended at the circumference of a circle implies $ML = LO$, that is, the point L lies on f , too. As shown in the first part of the previous proof, the point K also lies on the lines e and f . Therefore, if the lines e and f do not coincide, then $K = L$, that is, the points B, O, K, M all lie on the circle ℓ . Since the points K, O, M are different, k and ℓ must be identical, and thus k passes through the vertex B as well.

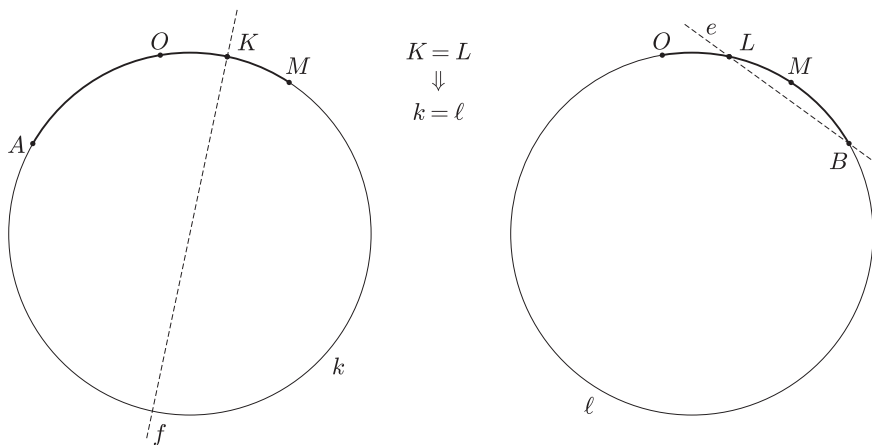


Figure 3

If the lines e and f coincide, then f passes through the vertex B , that is, $BM = BO = R$, where R is the radius of the circumcircle of the triangle ABC . If M_C is the perpendicular projection of M on the side AB , then

$$BM_C = BC \cos \beta = 2R \sin \alpha \cos \beta,$$

that is,

$$BM = \frac{BM_C}{\sin \alpha} = 2R \cos \beta.$$

Thus $\cos \beta = \frac{1}{2}$, $\beta = 60^\circ$. A simple calculation yields that the edge AC subtends a 120° angle at each of the points M, K and O . Since the points M, K, O lie on the same side of the line AC , it is the points A, M, K, O, C that lie on one circle this time, and that circle must be identical to k .

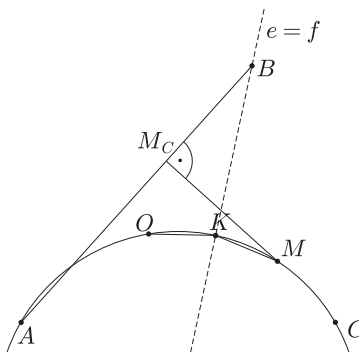


Figure 4

Solution 3 (based on the solution by *Harangi, Viktor*). As seen above, the points K, O, M are different, $KM = KO$ and the line OM does not pass through any vertex of the triangle. Assume that the line OM separates the vertex A from the other two. Then the perpendicular bisector f of the line segment OM (which passes through the point K) must intersect the side BC , otherwise one of the points M and O (say, M) would lie closer to each of the points B and C than the other one. Since K lies on both the bisector of the angle MBO and that of the angle MCO , and an angle bisector divides the opposite side in the ratio of the adjacent sides, it follows that both of the lines BK and CK would intersect the line segment OM closer to its endpoint M , and thus K would also lie closer to M than O . That is contradiction.

Thus one of the vertices B and C lies on the same side of the line f as the point M , and the other one lies on the same side as O . Without loss of generality, we may assume that $BM \leq BO$ and $CM \geq CO$, where at least one of these relations is a strict inequality. Therefore the line BK intersects the line segment MO closer to M , and the line CK intersects it closer to O . (One, but not both of the intersections may coincide with the midpoint of the edge MO). Consequently, the line OM separates the point K from the vertices B and C . We can establish, therefore, that both vertices B and C lie between the arms of the angle MKO .

Reflect now the point C in the line f to get the point C' . Since $\angle KC'O = \angle KCM = \angle KCO$, and C and C' are on the same side of the line KO , the points K, C, C', O are clearly concyclic, and for symmetry reasons their circle also passes through the point M . Thus C lies on the circumscribed circle of the triangle KOM . For the same reason, vertex B is also incident to this circle but vertex A is not, since the line MO does not separate the points A and K . That completes the proof.

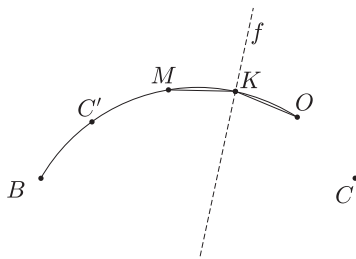


Figure 5

Remarks. Is it a necessary condition that the sides of the triangle are pairwise different? If the triangle is isosceles, then the points K, O, M are collinear. A circle can pass through all these points only if two of them coincide, that is, if the triangle is equilateral. Thus it would have been enough to require that the triangle is a non-equilateral acute-angled triangle.

If the triangle is not acute-angled, it cannot be equilateral either, and such a restriction is not needed. If the triangle is right-angled, the point M coincides with a vertex. Thus if a circle passes through the points K, O, M , then it necessarily passes through a vertex of the triangle. However, it can pass through another vertex only if the third angle is 60° . (Why?) The statement is hence not true for right triangles. And what about an obtuse triangle? In that case the solution is more complicated, but the claim still holds.

Exercises

1) The orthocentre of an obtuse-angled triangle is M , the centre of its inscribed circle is K , and the centre of its circumscribed circle is O . Prove that if a circle passes through the points K, O, M and a vertex of the triangle, then it also passes through another vertex.

2) If a triangle is not right-angled, then there exists a circle passing through the points K, O, M and a vertex if and only if one angle of the triangle is 60° .

Problem 2. Consider the sequence of the Fibonacci numbers defined by the recursion

$$f_1 = f_2 = 1, \quad f_n = f_{n-1} + f_{n-2} \quad (n \geq 3).$$

Assume that the fraction $\frac{a}{b}$, where a and b are positive integers, is smaller than one of the fractions $\frac{f_n}{f_{n-1}}$ and $\frac{f_{n+1}}{f_n}$ but is greater than the other. Show that $b \geq f_{n+1}$.

Solution 1 (based on the solutions by *Kocsis, Albert Tihamér* and *Zsbán, Ambrus*). The proof is by induction on n . Let us check the claim first for $n = 2$ and 3 . For $n = 2$, the condition is $1 < \frac{a}{b} < 2$, and hence $b \geq 2 = f_3$. For $n = 3$, $\frac{3}{2} < \frac{a}{b} < 2$ implies $b \geq 3 = f_4$. Assume now that $m \geq 3$ and the statement is already proved for $2 \leq n \leq m$.

Let $n = m + 1$, and assume that $\frac{f_n}{f_{n-1}} < \frac{f_{n+1}}{f_n}$, and the positive integers a and b satisfy

$$\frac{f_{m+1}}{f_m} = \frac{f_n}{f_{n-1}} < \frac{a}{b} < \frac{f_{n+1}}{f_n} = \frac{f_{m+2}}{f_{m+1}}.$$

Reducing the terms in the inequality by 1, we get

$$\frac{f_{m-1}}{f_m} = \frac{f_{m+1} - f_m}{f_m} < \frac{a - b}{b} < \frac{f_{m+2} - f_{m+1}}{f_{m+1}} = \frac{f_m}{f_{m+1}}.$$

Since there are positive numbers at both ends (and thus in the middle as well), the inequality is reversed when switching to the reciprocals:

$$\frac{f_m}{f_{m-1}} > \frac{b}{a - b} > \frac{f_{m+1}}{f_m}.$$

It follows from the assumption that $a - b \geq f_{m+1}$. If the terms are reduced by 1 once more and the reciprocals are taken, the inequality

$$\frac{f_{m-1}}{f_{m-2}} < \frac{a-b}{2b-a} < \frac{f_m}{f_{m-1}}$$

is obtained, and then it follows from the assumption that $2b - a \geq f_m$.

Adding the two results yields

$$b = (2b - a) + (a - b) \geq f_m + f_{m+1} = f_{m+2} = f_{n+1},$$

thus the statement is true for $n = m + 1$.

The same reasoning applies when

$$\frac{f_{m+1}}{f_m} = \frac{f_n}{f_{n-1}} > \frac{a}{b} > \frac{f_{n+1}}{f_n} = \frac{f_{m+2}}{f_{m+1}},$$

only one should interchange the roles of the relations „<” and „>”.

Solution 2 (based on the solution by *Egri, Attila*). Let us assume that

$$\frac{f_n}{f_{n-1}} < \frac{a}{b} < \frac{f_{n+1}}{f_n}.$$

Multiplying through the inequality by the positive quantity $bf_{n-1}f_n$ we get

$$bf_n^2 < af_{n-1}f_n < bf_{n-1}f_{n+1}.$$

The difference between the first two numbers is $f_n \cdot (af_{n-1} - bf_n)$, a positive integer divisible by f_n , whose value is therefore at least f_n . For similar reasons, the difference $f_{n-1} \cdot (bf_{n+1} - af_n)$ between the last two numbers is at least f_{n-1} . Therefore the difference between the first and last numbers is:

$$b(f_{n-1}f_{n+1} - f_n^2) \geq f_n + f_{n-1} = f_{n+1}.$$

Hence it is enough to prove that $k_n = f_{n-1}f_{n+1} - f_n^2 = 1$.

If $n = 2$ then $k_n = 1$, and if $n = 3$ then $k_n = -1$. If we go on checking the values of k_n , we find alternating values of $+1$ and -1 , that is, $k_n = (-1)^n$. This is true for $n = 2$, and if it holds for some integer $n \geq 2$, then it follows that

$$\begin{aligned} k_{n+1} &= f_n f_{n+2} - f_{n+1}^2 = f_n(f_n + f_{n+1}) - f_{n+1}^2 \\ &= f_n^2 - f_{n+1}(f_{n+1} - f_n) = f_n^2 - f_{n+1}f_{n-1} = -k_n = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Since in our case b and f_{n+1} are both positive, k_n must also be positive and thus its value is 1, as we set out to prove. A similar argument works if

$$\frac{f_n}{f_{n-1}} > \frac{a}{b} > \frac{f_{n+1}}{f_n}.$$

Remark. This argument also yields the general statement that if a, b, x, y, z, v are positive integers, $yz - xv = 1$ and $\frac{x}{y} < \frac{a}{b} < \frac{z}{v}$, then $b \geq y + v$.

Solution 3. Assume for simplicity that n is even. According to the relation $f_{n-1}f_{n+1} - f_n^2 = (-1)^n$ used in the previous solution, the inequality

$$\frac{f_n}{f_{n-1}} < \frac{a}{b} < \frac{f_{n+1}}{f_n}$$

holds in this form. The difference

$$\frac{a}{b} - \frac{f_n}{f_{n-1}} = \frac{af_{n-1} - bf_n}{bf_{n-1}}$$

is positive, so being an integer, the numerator is at least 1. Therefore,

$$\frac{1}{bf_{n-1}} \leq \frac{a}{b} - \frac{f_n}{f_{n-1}} < \frac{f_{n+1}}{f_n} - \frac{f_n}{f_{n-1}} = \frac{1}{f_{n-1}f_n},$$

and hence $bf_{n-1} > f_{n-1}f_n$, that is, $b > f_n$.

Consider the fraction $\frac{f_{n+2}}{f_{n+1}}$ which is smaller than $\frac{f_{n+1}}{f_n}$. If

$$\frac{f_{n+2}}{f_{n+1}} < \frac{a}{b} < \frac{f_{n+1}}{f_n},$$

then a reasoning similar to the one above yields

$$\frac{1}{bf_n} \leq \frac{f_{n+1}}{f_n} - \frac{a}{b} < \frac{f_{n+1}}{f_n} - \frac{f_{n+2}}{f_{n+1}} = \frac{1}{f_{n+1}f_n},$$

and therefore $b > f_{n+1}$.

If $\frac{a}{b} = \frac{f_{n+2}}{f_{n+1}}$, then $b \geq f_{n+1}$ for f_{n+2} and f_{n+1} are relatively prime. This is shown as follows: if a positive integer d divides both f_{n+2} and f_{n+1} , then it also divides their difference $f_n = f_{n+2} - f_{n+1}$, and so on, d divides all the numbers $f_{n-1}, f_{n-2}, \dots, f_1$. Since $f_1 = 1$, d must be 1.

There remains the case

$$\frac{f_n}{f_{n-1}} < \frac{a}{b} < \frac{f_{n+2}}{f_{n+1}}.$$

Consider the difference $\ell_n = f_{n+2}f_{n-1} - f_n f_{n+1}$. By induction we get $\ell_n = (-1)^n$, and therefore

$$\frac{1}{bf_{n-1}} \leq \frac{a}{b} - \frac{f_n}{f_{n-1}} < \frac{f_{n+2}}{f_{n+1}} - \frac{f_n}{f_{n-1}} = \frac{1}{f_{n+1}f_{n-1}},$$

and again we can conclude that $b > f_{n+1}$.

A similar argument yields the claim if n is odd.

Several papers used the theory of the Farey sequence. Here is an example.

Solution 4. (based on the solution by *Pallos, Péter*). Starting from the sequence $\mathcal{F}_1 = \left(\frac{0}{1}, \frac{1}{1}\right)$, proceed using the following recurrence. Having defined the sequence \mathcal{F}_n , insert the fraction $\frac{a+c}{b+d}$ between any two consecutive terms $\frac{a}{b}$ and $\frac{c}{d}$ of \mathcal{F}_n . If the sequence \mathcal{F}_n is strictly increasing, then so is the next sequence \mathcal{F}_{n+1} . The solution is based on the following two theorems: 1. *Each fraction appears in the sequence \mathcal{F}_n in lowest terms.* 2) *Every rational number between 0 and 1 belongs to some sequence \mathcal{F}_n .*

Note that $\frac{f_{n-1}}{f_n}$ and $\frac{f_n}{f_{n+1}}$ are consecutive terms of the sequence \mathcal{F}_n . This is the case if $n = 2$, and if $\frac{f_{n-1}}{f_n}$ and $\frac{f_n}{f_{n+1}}$ are consecutive terms of \mathcal{F}_n for an integer $n \geq 2$, then the fraction inserted between them in the next sequence \mathcal{F}_{n+1} is equal to

$$\frac{f_{n-1} + f_n}{f_n + f_{n+1}} = \frac{f_{n+1}}{f_{n+2}},$$

therefore the statement is also true for $n + 1$.

Since f_n is strictly increasing, the fraction $\frac{a}{b}$ is greater than 1. According to the above properties, the fraction $\frac{b}{a}$ thus occurs in some sequence \mathcal{F}_m , reduced to lowest terms in a form $\frac{b'}{a'}$. Since $\frac{b'}{a'}$ is greater than one of the fractions $\frac{f_{n-1}}{f_n}$ and $\frac{f_n}{f_{n+1}}$ and smaller than the other one, clearly $m > n$. The construction of the sequences \mathcal{F}_m implies that the numerator of every fraction inserted between $\frac{f_{n-1}}{f_n}$ and $\frac{f_n}{f_{n+1}}$ is at least $f_{n-1} + f_n$, and hence

$$b \geq b' \geq f_{n-1} + f_n = f_{n+1}.$$

The proof is hence complete.

Remark. In this solution, a sledgehammer was used to crack a nut, since the proofs of the stated properties of Farey sequences are actually based on considerations contained in the previous solutions.

Problem 3. *Prove that the set of edges formed by the sides and diagonals of a convex 3^n -gon can be partitioned into sets of three edges, such that the edges in each triple form a triangle.*

Solution 1 (based on the solution by *Csikvári, Péter*). Let us assign to the vertices of the polygon the numbers $0, 1, 2, \dots, 3^n - 1$, written in base-3 notation. Each number consists of n digits at most. If the number of digits is less than n , then adding leading zeros we have a sequence of n digits of 0, 1 or 2. In other words, we assign to the vertices of the polygon those sequences of length n whose terms are either 0, 1, or 2.

Consider the triangles satisfying the following condition: Whichever position is chosen from the first to the n -th, the three numbers assigned to the vertices of the triangle either have the same digit at the given position, or all three of them have different digits at that position. It is clear that for any pair of vertices of the polygon there is exactly one additional vertex available such that the three of them satisfy the above condition. Thus every single side and

diagonal of our polygon is the side of exactly one such triangle, and hence the sets of three edges forming the sides of such triangles will have the required property.

Solution 2. The proof is by induction on n . The claim is obvious if $n = 1$. Assume that the statement is already proved for some positive integer n and consider a convex 3^{n+1} -gon whose vertices are A_i, B_i, C_i where $1 \leq i \leq 3^n$. By the induction hypothesis the edges connecting the vertices A_i can be divided into triplets as required. The same is true for the edges connecting the vertices B_i and for those connecting the vertices C_i .

The rest of the edges can be grouped as follows: The edges A_iB_j, B_jC_k and C_kA_i are put together whenever $i + j + k$ is divisible by 3^n . It is clear that three such edges form a triangle. On the other hand, if any two of the numbers i, j, k are fixed, the divisibility condition uniquely determines the third one, and hence every edge occurs in exactly one triplet. The statement is hence true for $n + 1$, and the induction step is complete.

Solution 3 (based on the solution by *Steller, Gábor*). As in the previous solutions, the task is to find triangles such that their vertices are vertices of the original polygon, and each given edge is a side of one and only one triangle. In other words, any pair of triangles have at most one vertex in common. We also use mathematical induction to prove that this can be done. Assume that we have found suitable triangles $P_iP_jP_k$ for a polygon $P_1P_2 \dots P_{3^n}$. It follows from the conditions that the number of triangles is one third of the total number of edges, that is,

$$\frac{1}{3} \binom{3^n}{2} = \frac{3^{n-1}(3^n - 1)}{2}.$$

Let A_i, B_i, C_i ($1 \leq i \leq 3^n$) denote the vertices of a convex 3^{n+1} -gon. Consider the triangles $A_iB_iC_i$ where $1 \leq i \leq 3^n$, and call them triangles of the first kind. Consider now each triangle $P_iP_jP_k$ of the above partition, and construct the triangles $A_iA_jA_k, B_iB_jB_k, C_iC_jC_k$ (second kind) and the triangles $A_iB_jC_k, A_iC_jB_k, B_iA_jC_k, B_iC_jA_k, C_iA_jB_k, C_iB_jA_k$ (third kind). One gets

$$9 \cdot \frac{3^{n-1}(3^n - 1)}{2} + 3^n = \frac{3^n(3^{n+1} - 3)}{2} + 3^n = \frac{3^n(3^{n+1} - 1)}{2}$$

triangles altogether, which is equal to the number of triangles needed for a suitable partition. Therefore, it is enough to show that any pair of triangles listed above have at most one vertex in common.

It is clear that triangles of the first kind have no vertex in common at all, and they cannot have more than one common vertex with any triangle of the second kind either. Two triangles of the second kind either have no common vertex, or by the induction hypothesis they have at most one such vertex. Triangles of the third kind may have at most one vertex in common with triangles of the other two kinds. Finally, two triangles of the third kind may have at most one common vertex. This follows from the induction hypothesis, since if, say, $A_iB_jC_k$ and $A_iB_jC_{k'}$ are both triangles of the third kind, then the partition of the original 3^n -gon must have contained both the triangles $P_iP_jP_k$ and $P_iP_jP_{k'}$. That can only happen if $k = k'$.

Solution 4 (based on the solution by *Harangi, Viktor*). We can assume without the loss of generality that the polygon is regular. This opens the way for a geometric argument. The solution is once again by induction on n . For $n = 1$, the statement is trivial. Assume that the problem is already solved for some $n \geq 1$, and consider a regular 3^{n+1} -gon P . Label the vertices with the three letters A, B, C , going around the polygon in some direction. Vertex A is always followed by B , then C and then A again. The vertices labelled identically form three 3^n -gons, and the edges of each can be partitioned as required. There remains to take care of the edges connecting differently labelled vertices.

Consider the symmetry axis t of the polygon through a vertex marked A . Since P has an odd number of vertices, this axis does not contain any other vertex. The image after a reflection of a vertex marked A about the axis t is another vertex marked A , that of a reflection of a vertex marked B is a vertex marked C , and that of a reflection of a vertex marked C is a vertex marked B . Similarly, if the axis is through a vertex marked B or C , it is the vertices marked B and C , respectively, that map onto vertices of the same kind.

We proceed now as follows: the edges of a triangle of type ABC are grouped together if and only if the triangle is symmetrical about the axis of the polygon passing through the vertex A . We show that every edge of type AB, BC or CA of the polygon P is used exactly once, which means that the induction works.

An edge of type AB belongs exactly to one such triangle, the one whose third vertex is obtained by reflecting B about the axis through A . The image will be a vertex of type C as said above. By symmetry, each edge of type AC belongs to exactly one triangle as well. Finally, consider an edge of type BC . Its perpendicular bisector is a symmetry axis of P , so it passes through a particular vertex of P , which must be a vertex of type A for the reasons mentioned above. That vertex, and only that may be the third vertex of the required triangle.

Finally, let us examine the solution that reveals the genuine geometrical (or algebraic, if you like) background of the problem. The required partition can be accomplished in terms of the lines of the n -dimensional affine space over the three-element field. The argument below will hopefully reveal the point of the story.

Solution 5 (based on the solution by *Rácz, Béla András*). Let p be an arbitrary prime number. We are going to prove the following general theorem: The edges of a complete graph on p^n vertices can be partitioned into sets forming the edges of a complete graph on p points each. For $p = 3$, this is simply the original problem. See on the front page.

Consider the sequences $\mathbf{a} = (a_1, a_2, \dots, a_n)$ where, for every i , a_i is a non-negative integer less than p . The number of such sequences is clearly p^n . They represent the points of the n -dimensional affine space over the p -element field, which we will identify with the vertices of the given complete graph. We may also think of them as vectors, similar to the way the position vectors are identified with their endpoints in 3-dimensional Euclidean space. The sum of two points \mathbf{a} and \mathbf{v} is defined as

$$\mathbf{a} + \mathbf{v} = (a_1 + v_1, a_2 + v_2, \dots, a_n + v_n),$$

where the sums $a_i + v_i$ are meant modulo p . We can also say that the point \mathbf{a} is shifted by the vector \mathbf{v} . The difference between two points can be defined in a similar way, and $\mathbf{a} + (\mathbf{b} - \mathbf{a}) = \mathbf{b}$ will be true. α times a point (or vector) \mathbf{v} is defined as the point (or vector)

$$\alpha \mathbf{v} = (\alpha v_1, \alpha v_2, \dots, \alpha v_n),$$

where $\alpha \in \{0, 1, \dots, p-1\}$ and αv_i is also considered modulo p . If the integers α and β are congruent modulo p , $\alpha \mathbf{v}$ and $\beta \mathbf{v}$ define the same point.

How can we define a line through two different points \mathbf{a} and \mathbf{b} ? Let us add the multiples of the vector $\mathbf{v} = \mathbf{b} - \mathbf{a}$ to the point \mathbf{a} , as we would do in the Euclidean case. It is easy to show that any such line consists of p distinct points. On one hand, there may be at most p points on the line since it is enough to add the vector \mathbf{v} to the point \mathbf{a} $0, 1, \dots, p-1$ times. On the other hand, if $\mathbf{a} + j\mathbf{v} = \mathbf{a} + k\mathbf{v}$ for two different numbers $j, k \in \{0, 1, \dots, p-1\}$ then $jv_i = kv_i$ modulo p for each coordinate v_i of \mathbf{v} . Thus $(k-j)v_i$ is divisible by p , which can only happen if every v_i is zero. That contradicts \mathbf{a} and \mathbf{b} being different points.

Any pair of distinct points determine a line passing through exactly p points. The crucial observation is that any pair of different lines have at most one point in common, or in other words, any pair of points belong to exactly one line. Hence the statement follows: the complete graphs on p points to be found correspond to the different lines.

Exercises

- 1) Prove that the roles of \mathbf{a} and \mathbf{b} can be interchanged in the definition of the line through \mathbf{a} and \mathbf{b} .
- 2) Prove that if $\mathbf{c} = \mathbf{a} + \alpha(\mathbf{b} - \mathbf{a})$ and $\mathbf{d} = \mathbf{a} + \beta(\mathbf{b} - \mathbf{a})$ are two different points of the line through the points \mathbf{a} and \mathbf{b} , then \mathbf{a} and \mathbf{b} lie on the line determined by \mathbf{c} and \mathbf{d} . How does this imply the „crucial” observation mentioned in the solution?
- 3) How can we define two lines to be parallel?
- 4) How can planes be defined? How many points will a plane have? What would the set of common points of two planes look like?
- 5) What problems would we face if, formulating the statement of the above general theorem with a composite number m in the place of the prime p , we tried to apply the same ideas to obtain a proof?