7th International Tournament of Young Mathematicians

QUIZ

1.5 hours

- Each team (high school students only) is gathered in a separate room and works together. Written materials, electronics, literature or other sources are forbidden during the quiz, as well as any external help. Only brochures of the ITYM and paper language dictionaries are allowed.
- A solution for each of the 10 problems should be written **separately**.
- Indicate the **problem number** and page numbers on every solution.
- Please **don't** mention your country, team or other names anywhere.

Problem 1. A Laser Machine

1. Given a set of points in the real plane, when is it *convex*? **(1 point)**

2. In the case where P is a circle containing the center of the disk, σ is the diameter of P and w is negligible, find the minimal number of beams needed to determine σ with an error $\varepsilon \leq \frac{1}{2}$. **(4 points)**

3. Let P be a circle not necessarily containing the center of the disk. Suppose that the machine is broken and can only emit beams parallel to the x-axis with a non-negligible w. The engineer would like to determine the diameter of P with only two shots. What is the smallest possible ε he can guarantee regardless of the position of P? **(5 points)**

Solution

1. A *convex set* is a region such that with every two points it also contains the segment joining them.

2. *Answer:* 2

First, let us prove that it's impossible with only one beam. The orientation of the beam doesn't matter as we may use the symmetry of the figure. So let's suppose the beam is parallel to the x axis. For example $x = \alpha > 0$. Then there are two cases:

- The beams hits P. It means the minimal possible diameter for P is α and the maximal one is 2. So the difference is $2 - \alpha$.
- The beams doesn't hit P. The minimal possible diameter for P is 0 and the maximal one is $1 + \alpha$. The difference is $1 + \alpha$.

So the optimal choice of α to maximize the information is $\alpha = 1/2$. Then the difference is $3/2$ which means that $\varepsilon = 3/4$ at most.

Now let us study the following configuration: we have to parallel beams at $x = -1/2$ and $x = 1/2$. There are three possible cases (up to a symmetry):

- None of the beams hits P. It means the minimal possible diameter for P is 0 and the maximal one is 1. So the difference is 1.

- Only one of the beams hits P. It means the minimal possible diameter for P is $1/2$ and the maximal one is $3/2$. So the difference is 1.
- Both beams hit P. It means the minimal possible diameter for P is 1 and the maximal one is 2. So the difference is 1.

So anyway the interval in which the diameter can be has length 1 and by announcing the mean value the error ε is at most $1/2$.

3. Answer: $\varepsilon = 2/3$ for $w \le 4/3$, and $\varepsilon = w/2$ for $w > 4/3$

We can assume that that the shots one and two are performed with the distances a and b on the opposite sides from the center of the disk. Let us compute the minimal and maximal possible diameter of P depending on the results of these two shots:

Shot 1	Shot 2	min	max
no	no	0	$\max(1-a-\frac{w}{2}, 1-b-\frac{w}{2}, a+b-w)$
no	yes	0	$a+1-\frac{w}{2}$
yes	no	0	$b+1-\frac{w}{2}$
yes	yes	$a+b-w$	2

Here we always assume that $0 \le a, b \le 1$ (as we can perform shots only from the boundary of the disk) and $a+b \ge w$. Indeed, if $a+b < w$, then the two beams overlap. And in the case of "yes-yes" result we do not have any information on the possible diameter of P, which can be any number from 0 to 2.

The precision ε for estimating the diameter of P is exactly the half of the length of the $[\min, \max]$ interval:

Shot 1	Shot 2	$\max - \min$
no	no	$\max(1-a-\frac{w}{2}, 1-b-\frac{w}{2}, a+b-w)$
no	yes	$a+1-\frac{w}{2}$
yes	no	$b+1-\frac{w}{2}$
yes	yes	$2-a-b-w$

It is easy to see that the length of the $[\min, \max]$ interval for "no-no" result is always less or equal than this length in the case of either "yes-no" or "no-yes" result. So, we need to find a, b minimising the value of

$$2\varepsilon = \max(a+1-\frac{w}{2}, b+1-\frac{w}{2}, 2-a-b+w)$$

subject to the following restrictions: $0 \le a, b \le 1$, $w \le a+b$.

If $w \le 4/3$, then it is easy to see that the precision ε is minimal, when $a+1-\frac{w}{2} = b+1-\frac{w}{2} = 2-a-b+w$, and thus $a = b = 1/3 + \frac{w}{2}$. We have $\varepsilon = 2/3$, which does not depend on w in this case.

If however $w > 4/3$, then the minimum of ε is achieved when $a = b = 1$ and is equal to $\frac{w}{2}$.

The reader can check that the final result does not change, even if the position of the second shot is chosen depending on the result of the first shot.

Problem 2. Maximal Minimal Triangles

1. What is an *affine transformation* of the plane? How does it change area of plane regions? **(2 points)**

2. What is the maximal area of a triangle inscribed into an ellipse of area 1? **(3 points)**

3. A triangle is inscribed into a parabola. The upper side of the triangle together with the corresponding part of the parabola (see Figure 1) bound a region of area 1.

a) What is the maximal possible area of the triangle? **(4 points)**
b) For which triangles the maximal area is achieved? **(1 point)**

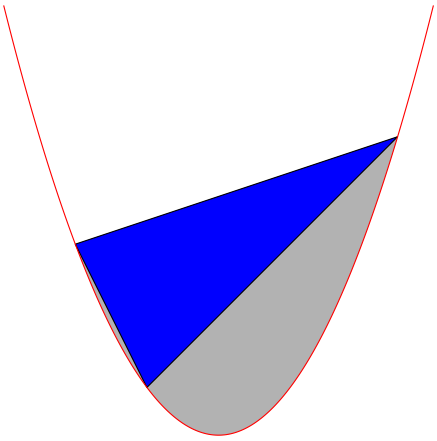

FIGURE 1. The area of the region bounded by the upper side of the triangle and the lower part of the parabola is 1.

Solution

1. An affine transformation of the plane is a bijective map that sends lines to lines. This automatically implies that this map:

- maps parallel lines to parallel lines;
- preserves the ratio of parallel line segments;
- is continuous (differentiable).

Any affine transformation can be written in coordinates as:

$$(x, y) \mapsto (ax + by + e, cx + dy + f), \quad \text{where } ad - bc \neq 0.$$

This can also be considered as an alternative definition of an affine map.

Affine maps do not in general preserve area of figures, but they scale it by the same non-zero factor, which is equal to $(ad - bc)$ in the above formula. In particular, the ratio of areas of two plane figures is preserved by affine transformations.

2. *Answer:* $\dfrac{3\sqrt{3}}{4\pi}$

We can reformulate the question by asking for the maximal possible ratio of an area of a triangle and an area of the ellipse it is inscribed to. This formulation is invariant under affine transformations. By means of such transformations we can always map an ellipse to a unit circle.

It is well-known that among all triangles inscribed into a unit circle the largest area is achieved by the equilateral one.[1] This area is equal to

$$\frac{3}{2} \cdot \sin(2\pi/3) = \frac{3\sqrt{3}}{4}.$$

So, the maximal ratio of the triangle area and the ellipse area is given as a ratio of the area of this equilateral triangle and the area of the unit circle.

3. *Answer:* 3/4

The maximum is achieved for the triangles satisfying the following property:

(PP): the tangent line to the parabola at the middle triangle vertex (the one which lies between the two others on the parabola) is parallel to the opposite side of the triangle.

[1] See a variety of proofs at: http://math.stackexchange.com/questions/1298379/finding-the-largest-triangle-inscribed-in-the-unit-circle.

Again, up to affine transformations, we can assume that the parabola is given by the equation $y = x^2$. The following affine transformations preserve this parabola:

$$(x, y) \mapsto (x + e, y + 2ex + e^2), \quad e \in \mathbb{R}.$$

Therefore, we can assume that the middle triangle vertex is exactly $(0, 0)$. Suppose other two have coordinates $(-a, a^2)$ and (b, b^2), $a, b > 0$. Then it is easy to compute that the area of the triangle is equal to

$$S = \tfrac{1}{2}(a^2 + b^2)(a + b) - \tfrac{1}{2}a^3 - \tfrac{1}{2}b^3 = \tfrac{1}{2}ab(a + b),$$

while the area of the parabola segment cut by the top triangle side is equal to:

$$S_p = \tfrac{1}{2}(a^2 + b^2)(a + b) - \tfrac{1}{3}a^3 - \tfrac{1}{3}b^3 = \tfrac{1}{6}(a^3 + b^3 + 3a^2b + 3ab^2) = \tfrac{1}{6}(a + b)^3.$$

So, we get:

$$\frac{S}{S_p} = \frac{3ab}{(a + b)^2} = \frac{3}{\frac{a}{b} + 2 + \frac{b}{a}}.$$

This expression achieves the maximum if and only if $a = b$, and the maximal ratio equals $3/4$.

The triangles maximizing the ratio S/S_p have the upper side parallel to the Ox axes and clearly satisfy property (PP). It is easy to see that this property is preserved by affine transformations. Conversely, any triangle satisfying this property can be transformed by affine transformations to the triangle with vertices $(-a, a^2)$, $(0, 0)$, (a, a^2) on the parabola $y = x^2$.

Problem 3. Coloured Circles

1. Give a definition of a closed *d-dimensional ball* of radius 1. **(1 point)**

2. Consider the game on the real line with all segments having length 1.

a) Show that $C_1(n, k) \leq 2k - 1$ for any natural n and k. **(2 points)**

b) Suppose that k is even and $n \geq 2k$. Prove that $C_1(n, k) \geq \frac{3}{2}k$. **(3 points)**

3. Suppose now that Carl is greedy and he applies a new colour only when he has to (if Clara puts a segment and Carl can colour it with one of the colours he has used previously, then he will certainly do it). Denote by $GC_1(n, k)$ the minimum number of colours that Carl would need to successfully colour n segments put by Clara on a line, provided that no point is covered by more than k segments. Show that $GC_1(n, k) = 2k - 1$. **(4 points)**

Solution

1. A closed *d-dimensional ball* of radius 1 centred at a point $c \in \mathbb{R}^d$ is the set of all points in $\mathbb{R}^d$ which are at distance at most 1 from c.

2. a) We will prove the inequality by induction on n. For $n = 1$ it is obviously true. Suppose that $C_1(n, k) \leq 2k - 1$, that is Carl managed to use at most $2k - 1$ colours for n segments put by Clara with the condition that no $k + 1$ segments have a common point. Let S be an $(n + 1)$-th segment put by Clara such that the condition is preserved. Then at most $k - 1$ segments contain the left endpoint of S and at most $k - 1$ segments contain the right endpoint of S. Since all segments are of the same length, each segment intersecting S contains its left and/or right endpoint. Thus, for the segment S, Carl can use at least $(2k - 1) - 2(k - 1) = 1$ colours, so that all $n + 1$ segments have at most $2k - 1$ different colours and no two intersecting segments have the same colour.

b) Let $k = 2m$ with $m \in \mathbb{N}$. We are going to show how Clara can force Carl to use at least $3m$ colours by putting $4m$ segments in a specific way. First, she puts a pile of m segments, one on top of another. Let R be their right endpoint. Carl needs to use m different colours (denote

this set of colours by σ). After that Clara puts $2m$ segments $S_1, \ldots, S_{2m}$ consecutively by the following algorithm (see Figure 2):

– put S_1 so that its left endpoint L_1 is $\frac{1}{2}$ to the right of R;
– if Carl uses a colour form σ, then the left endpoint L_2 of S_2 is $\frac{1}{4}$ to the left of L_1;
– if Carl uses a new colour, then the left endpoint L_2 of S_2 is $\frac{1}{4}$ to the right of L_1;
– ...
– if Carl uses a colour form σ, then the left endpoint L_{2m} of S_{2m} is $\frac{1}{2^{2m}}$ to the left of L_{2m-1};
– if Carl uses a new colour, then the left endpoint L_{2m} of S_2 is $\frac{1}{2^{2m}}$ to the right of L_{2m-1}.

Since all these segments intersect, Carl will need to use at least m new colours. According to the algorithm, all the segments among $S_1, \ldots, S_{2m}$ whose colours are new will be strictly to the left from those whose colours are from σ.

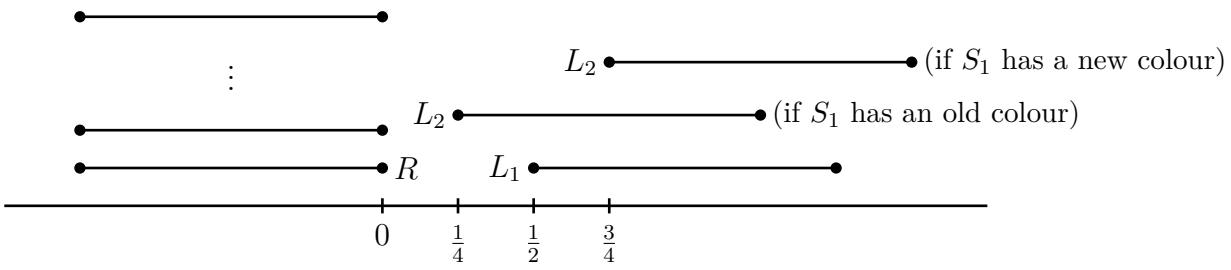

FIGURE 2. Clara puts $2m$ segments $S_1, \ldots, S_{2m}$.

Finally, Carla puts a pile of m segments intersecting the first pile of m segments and exactly m leftmost segments among $S_1, \ldots, S_{2m}$. Carl then will need to use m new colours – all together at least $3m$ colours.

See also the following paper: B. Bosek, S. Felsner, K. Kloch, T. Krawczyk, G. Matecki and P. Micek, On-line chain partitions of orders: a survey.

3. Analogically to 2a) we have $GC_1(n,k) \leq 2k-1$. Let us show that Clara can force Carl to use at least $2k-1$ colours. For that purpose, Clara first puts $2k$ segments $A_1 = [a_1^L, a_1^R]$, $B_1 = [b_1^L, b_1^R]$, ..., $A_k = [a_k^L, a_k^R]$, $B_k = [b_k^L, b_k^R]$ in this order, so that

- $a_i^R = a_i^L + 1$ and $b_i^R = b_i^L + 1$ for all $1 \leq i \leq k$;
- $b_i^L = a_i^R + 1 + \varepsilon$ for all $1 \leq i \leq k$, where ε is a positive real number strictly less than $\frac{1}{k}$;
- $a_{i+1}^L = a_i^L + \frac{1}{k}$ and $b_{i+1}^L = b_i^L + \frac{1}{k}$ for all $1 \leq i \leq k-1$.

Since Carl is greedy, he will use the same colour for each pair of intervals (A_i, B_i) – in total k colours (denote the set of these colours by σ).

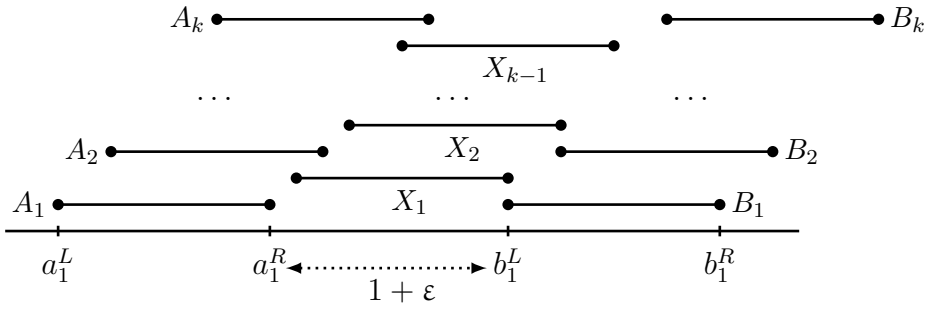

FIGURE 3. Clara puts $3k$ segments $A_1, B_1, \ldots, A_k, B_k$ and $X_1, \ldots, X_k$.

Now, Clara puts k new intervals $X_i = [x_i^L, x_i^R]$, where $i = 1, 2, \ldots, k-1$, such that

$$x_i^L = a_i^R + \varepsilon \quad \text{and} \quad x_i^R = b_i^L .$$

The intervals X_i intersects the intervals $B_1, \ldots, B_i, A_{i+1}, \ldots, A_k$ as shown in Figure 3. Moreover, the intervals X_i have a point in common. Thus Carl has to use $k-1$ new colours, and so $GC_1(n,k) \geq 2k-1$ which completes the proof.

Problem 4. Simple Paths in Grids

1. a) Give definitions of a *connected* graph and a *complete* graph. **(1 point)**

b) Show that a graph with n vertices and n edges must have a cycle. **(1 point)**

c) A graph is called *bipartite* if the set of its vertices can be divided into two disjoint subsets U and V such that every edge connects a vertex in U to one in V. Show that any $n \times n$ grid is a bipartite graph. **(1 point)**

2. Find and prove a formula for $D_n(2)$. **(3 points)**

3. Let $G = (V, E)$ be a graph. A *perfect matching* of G is a subset of its edges $P \subseteq E$ such that every vertex of G is an endpoint of **exactly** one edge in P.

Find the number $\rho(G)$ of perfect matchings of G in the following cases:

a) G is a complete graph on $2n$ vertices. **(2 points)**

b) $G = (U, V, E)$ is a *complete* bipartite graph on m and n vertices. In other words, the set of vertices of G consists of two disjoint sets U and V of size m and n, respectively, and E is the set of edges connecting every vertex in U with all vertices in V. **(2 points)**

Solution

1. a) A graph is *connected* if, for every two vertices of the graph, there is a path joining them. A graph is *complete* if any two vertices are connected by an edge.

b) Suppose that a graph G with n vertices and n edges doesn't have a cycle. Consider the connected components of G. Each component is a connected graph with no cycle, that is a *tree*. Since a tree on k vertices has exactly $k-1$ edges, we obtain that G has less than n edges. Contradiction.

c) It is easily verified by colouring the vertices of an $n \times n$ grid in a checkerboard fashion.

2. Denote by $C_n(2)$ the maximal number of edges in a subgraph H of the $n \times n$ grid, which doesn't have a simple path of length 2. Then $D_n(2) = 2n(n+1) - C_n(2)$. In the subgraph H, each vertex is an endpoint of at most 1 edge. Therefore, $C_n(2) \leq \lfloor \frac{(n+1)^2}{2} \rfloor$ where $\lfloor x \rfloor$ stands for the largest integer not exceeding x. On the other hand, it is easy to construct examples showing that $C_n(2) \geq \lfloor \frac{(n+1)^2}{2} \rfloor$. Hence, $D_n(2) = 2n(n+1) - \lfloor \frac{(n+1)^2}{2} \rfloor$.

3. a) *Answer:* $\rho(G) = \frac{(2n)!}{2^n n!}$

By definition of a perfect matching and a complete graph, $\rho(G)$ is number of ways to divide the set of $2n$ vertices into disjoint pairs. There are $\binom{k}{2} = \frac{k(k-1)}{2}$ ways to choose two vertices among k vertices, and so there are

$$\binom{2n}{2}\binom{2n-2}{2}\cdots\binom{2}{2} = \frac{(2n)!}{2^n}$$

sequences of n disjoint pairs of vertices. Since $n!$ distinct sequences correspond to the same set of n pairs, we obtain $\rho(G) = \frac{(2n)!}{2^n n!}$.

b) *Answer:* $\rho(G) = n!$

If $m \neq n$ then evidently $\rho(G) = 0$, since every edge connects a vertex from U to a vertex from V. If now $m = n$, then finding a perfect matching corresponds to assigning to each vertex from U a "match" in V so that distinct vertices have distinct matches. Therefore, $\rho(G)$ equals the number of permutations on n vertices, that is $\rho(G) = n!$.

Remark. Let H be a maximal subgraph of the $n \times n$ grid, which doesn't have a simple path of length 2. Then, for odd n, the set of edges of H is a perfect matching for the grid. As shown in 1c), an $n \times n$ grid is also a bipartite graph (but not complete when $n > 2$).

Problem 5. A Recursive Sequence

1. Give a definition that a real sequence (x_n) *converges* to a point $r \in \mathbb{R}$. **(1 point)**

2. Consider two sets $A \subset A' \subset [0,1]$. Let (u_n) and (u'_n) be recursive sequences for A and A', respectively, such that $u_0 = u'_0$. Prove that $u_n \leq u'_n$ for all $n \in \mathbb{N}$. **(3 points)**

3. Take $A = \left\{ \frac{k}{2^m} \mid k, m \in \mathbb{N} \cup \{0\} \text{ and } k \leq 2^m \right\}$.

a) Find $\mathscr{L}_0(A)$. **(2 points)**

b) Find $\mathscr{L}_\infty(A)$. **(4 points)**

Solution

1. A real sequence (x_n) *converges* to a point $r \in \mathbb{R}$ if, for any $\varepsilon > 0$, there exists $N = N(\varepsilon)$ such that

$$|x_n - r| < \varepsilon$$

for all natural $n > N$.

2. Let us show that the inequality $u_n \leq u'_n$ is true for all $n \in \mathbb{N} \cup \{0\}$ by induction. It is true for $n = 0$ and $n = 1$. Suppose that $n \geq 1$ and $u_n \leq u'_n$. Let us show that also $u_{n+1} \leq u'_{n+1}$. Consider the following sequences, where $k \in \mathbb{N} \cup \{0\}$:

$$\begin{aligned} c_0 = u_0 \quad &\text{and} \quad c'_0 = u'_0\,, \\ c_{k+1} = (k+1)u_{k+1} &= \{i \mid 0 \leq i \leq k \text{ and } u_i \in A\}\,, \\ c'_{k+1} = (k+1)u'_{k+1} &= \{i \mid 0 \leq i \leq k \text{ and } u'_i \in A'\}\,. \end{aligned}$$

These are non-decreasing sequences, such that $c_{k+1} \leq c_k + 1$ and $c'_{k+1} \leq c'_k + 1$. By inductive assumption, we have $c_n \leq c'_n$. If now $c_{n+1} > c'_{n+1}$ then necessarily $c_n = c'_n$ and $c_{n+1} = c_n + 1$ but $c'_{n+1} = c'_n$. So $u_n = u'_n$ and $u_n \in A$ but $u'_n \notin A'$. Contradiction to the fact that $A \subset A'$. Therefore, $c_{n+1} \leq c'_{n+1}$ or equivalently $u_{n+1} \leq u'_{n+1}$.

3. a) *Answer:* $\mathscr{L}_0(A) = \{\frac{1}{2}, 1\}$.

If $u_0 \notin A$ then we have $u_1 = 0 \in A$, $u_2 = \frac{1}{2} \in A$ and $u_3 = \frac{2}{3}$, and for all $n > 0$, u_n is neither 0 nor 1. We now prove by induction on k that, for all $k \geq 1$,

$$u_{2k} = \frac{1}{2} \quad \text{and} \quad u_{2k+1} = \frac{k+1}{2k+1}$$

It is true for $k = 1$. If it holds for some k, then exactly $k+1$ of the terms $u_0, u_1, \ldots, u_{2k}$ are in A and $u_{2k+1} \notin A$, since $0 < u_{2k+1} < 1\}$ and its denominator is odd. Hence, $u_{2k+2} = \frac{k+1}{2k+2} = \frac{1}{2} \in A$ and the same argument proves that $u_{2k+3} = \frac{k+2}{2k+3}$. We then have $u_n \to \frac{1}{2}$.

If $u_0 \in A$, then $u_1 = 1$ and since $1 \in A$ it is obvious by induction that $u_n = 1$ for all $n \geq 1$. We then have $u_n \to 1$.

b) *Answer:* $\mathscr{L}_\infty(A) = \left\{ \frac{1}{2^m} \mid m \in \mathbb{N} \cup \{0\} \right\}$.

First, the question 3a) shows that $1 \in \mathscr{L}_\infty(A)$. Now let $m > 0$. Choose $u_0 \in A$ and $u_1, \ldots, u_{2^m-1} \notin A$. Then $u_{2^m} = \frac{1}{2^m}$ and one can prove by induction that if $n = q \cdot 2^m + r$ with $q \geq 1$ and $1 \leq r \leq 2^m$, then $u_n = \frac{q+1}{q \cdot 2^m + r}$. Indeed, if $r \neq 2^m$ then $(q+1) \cdot 2^{m-1} < q \cdot 2^m + r < (q+1) \cdot 2^m$ and so $u_n \notin A$. Hence, $u_n \to \frac{1}{2^m}$ and $\frac{1}{2^m} \in \mathscr{L}_\infty(A)$.

Let (u_n) be a sequence verifying the recurrence relation for all $n \geq N$. If $u_0, \ldots, u_N \notin A$ then $u_{N+1} = 0 \in A$ and $u_{N+2} > 0$. If $u_i \in A$ for some $0 \leq i \leq N$, then we also have $u_{N+2} > 0$. When

$u_{N+2} = 1$, the sequence (u_n) obviously converges to 1. Assume that $0 < u_{N+2} < 1$, and let $m > 0$ be such that $\frac{1}{2^m} \leq u_{N+2} < \frac{1}{2^{m-1}}$. We will first prove that $(u_n)_{n \geq N+2}$ stays in $[\frac{1}{2^m}, \frac{1}{2^{m-1}}[$, then that it takes the value $\frac{1}{2^m}$ at least once and, finally, that it converges to $\frac{1}{2^m}$.

Suppose that there is an $n \geq N+2$ such that $u_n \geq \frac{1}{2^{m-1}}$ and take the minimal n with such a property. From $u_{n-1} < \frac{1}{2^{m-1}} \leq u_n$ follows that u_{n-1} must be in A. Write $u_{n-1} = \frac{c}{n-1} = \frac{p}{2^q}$ with p odd. Since $u_{n-1} = \frac{p}{2^q} < \frac{1}{2^{m-1}}$, we have $q > m-1$ and $p \leq 2^{q-m+1} - 1$ so that

$$u_n = \frac{c+1}{n} < \frac{c+1}{n-1} = u_{n-1} + \frac{1}{n-1} \leq u_{n-1} + \frac{1}{2^q} \leq \frac{2^{q-m+1}-1}{2^q} + \frac{1}{2^q} = \frac{1}{2^{m-1}}$$

which is a contradiction. Hence, for all $n \geq N$ we have $u_n < \frac{1}{2^{m-1}}$.

Now suppose that there is an $n \geq N+2$ such that $u_n < \frac{1}{2^m}$ and take the minimal n with such a property. Denote $c_n = n \cdot u_n$. Since $u_n < u_{n-1}$, we have $c_n = c_{n-1}$. The inequalities $u_n < \frac{1}{2^m} \leq u_{n-1}$ can be rewritten as $n-1 \leq 2^m c_n < n$. Thus $2^m c_n = n-1$ and $u_{n-1} = \frac{1}{2^m} \in A$, implying that $c_n = c_{n-1} + 1$. Contradiction. So $u_n \in [\frac{1}{2^m}, \frac{1}{2^{m-1}}[$ for $n \geq N+2$.

Now assume there is no $n \geq N+2$ for which $u_n = \frac{1}{2^m}$. Take an $n \geq N+2$ such that $u_n \in A$. Then $u_n = \frac{k}{2^a} = \frac{c_n}{n}$ and $\frac{1}{2^m} < u_n < \frac{1}{2^{m-1}}$, and so necessarily $a \geq m+1$ and 2^{m+1} divides n. Therefore, at most one out of 2^{m+1} consecutive terms of the sequence $(u_n)_{n \geq N+2}$ can be in the set A, that is $c_k \leq \frac{k}{2^{m+1}} + C$ for some constant C. Then

$$u_k = \frac{c_k}{k} \leq \frac{1}{2^{m+1}} + \frac{C}{k} \to \frac{1}{2^{m+1}} \quad \text{as} \quad k \to \infty\,,$$

and in particular $u_k < \frac{1}{2^m}$ for sufficiently large k, which we have already proved impossible.

Hence, there is an $n_0 \geq N+2$ such that $u_{n_0} = \frac{1}{2^m}$, that is $c_{n_0} = b$ and $n_0 = 2^m b$ for some $b \in \mathbb{N}$. And one shows by induction that

$$u_{2^m q + r} = \frac{q+1}{2^m q + r}\,,$$

for $q \geq b$ and $1 \leq r \leq 2^m$. So (u_n) converges to $\frac{1}{2^m}$.

Problem 6. Critical Points

1. Consider a function $f :]a, b[\to \mathbb{R}$ defined on an open interval $]a, b[$.

a) Give a definition of the derivative of f at a point $x_0 \in]a, b[$. Is it true that if f is differentiable at x_0 then it must be continuous at x_0? **(1 point)**

b) Give a geometric interpretation of the derivative. **(1 point)**

2. a) Show that the function $F(x) = \sum_{k=1}^{2016} \frac{1}{x-k}$ doesn't have critical points. **(1 point)**

b) Show that the following function

$$H(x) = \frac{1}{x-1} - \frac{1}{x-2} + \frac{1}{x-3}$$

has at most 4 critical points in its domain $\mathbb{R} \setminus \{1, 2, 3\}$. **(1 point)**

c) Prove that H has at least 2 critical points. **(3 points)**

3. Consider the function $F(x) = \sum_{k=1}^{2016} \frac{1}{x-k}$ as a ratio

$$F(x) = \frac{P(x)}{Q(x)}$$

of two polynomials $P(x)$ and $Q(x)$ of degrees 2015 and 2016 respectively. Prove that the polynomial $P(x)$ has 2015 distinct real roots. **(3 points)**

Solution

1. a) The *derivative* of f at a point $x_0 \in (a, b)$ is the following limit, if it exists and is finite,

$$f'(x_0) = \lim_{\varepsilon \to 0} \frac{f(x_0 + \varepsilon) - f(x_0)}{\varepsilon}\,.$$

Yes, a function must be continuous in the domain where it is differentiable.

b) It follows from the definition of the derivative that $f'(x_0) = \tan \alpha$, where α is the angle between the x-axis and the tangent line to the graph of f at the point $(x_0, f(x_0))$. This angle belongs to the interval $[0, \pi[$ and is calculated in the counter-clockwise direction starting from the x-axis.

Note in particular that x_0 is a critical point for f if and only if the tangent line at $(x_0, f(x_0))$ is parallel to the x-axis.

2. a) We see that the derivative $F(x) = -\sum\limits_{k=1}^{2016} \frac{1}{(x-k)^2}$ is always negative. Therefore, F doesn't have critical points.

b) The derivative of the function H is

$$H'(x) = -\frac{1}{(x-1)^2} + \frac{1}{(x-2)^2} - \frac{1}{(x-3)^2} \tag{1}$$

The numerator of the derivative H' is a polynomial of degree 4, namely $x^4 - 8x^3 + 28x^2 - 48x + 31$. It has at most 4 roots, and so H has at most 4 critical points.

c) For a function f and $a \in R$, denote by $f(a+)$ and $f(a-)$ the following limits

$$\lim_{x \to a,\, x > a} f(x), \quad \lim_{x \to a,\, x < a} f(x)$$

respectively, if they exist ($+\infty$ and $-\infty$ are also accepted).

According to the equation (1) we have

$$H'(1+) = -\infty, \quad H'(2-) = +\infty, \quad H'(2+) = +\infty, \quad H'(3-) = -\infty.$$

Since the derivative H' is continuous on the interval $]1, 2[$ and $H'(1+) = -\infty, H'(2-) = +\infty$, we conclude that the graph of H' must intersect the x-axis. In other words, there is $x_0 \in]1, 2[$ such that $H'(x_0) = 0$. The same is true for the interval $]2, 3[$. Therefore, H has at least two critical points.

3. *First method.* We have

$$Q(x) = \prod_{k=1}^{2016} (x - k) \quad \text{and} \quad P(x) = \sum_{k=1}^{2016} \frac{Q(x)}{(x-k)}\,.$$

Note that for every $m = 1, \ldots, 2016$, one has

$$\begin{aligned} P(m) &= (m-1) \cdots (m - (m-1)) \cdot (m - (m+1)) \cdots (m - 2016) \\ &= m! \cdot (-1)^{2016-m} (2016 - m)! = (-1)^m m! (2016 - m)! \end{aligned}$$

which is negative when m is odd and positive otherwise. Thus $P(1) < 0$, $P(2) > 0$, $P(3) < 0$, …, $P(2015) < 0$, $P(2016) > 0$. Since $P(x)$ is a continuous function, its graph must intersect the x-axis in each of the intervals $]1, 2[$, $]2, 3[$, …, $]2015, 2016[$. Therefore, $P(x)$ has 2015 distinct real roots.

Second method. One can note that $P(x) = Q'(x)$ and use the well-known theorem:

Theorem (Rolle)**.** *Let f be a real-valued function continuous a closed interval $[a, b]$ and differentiable on the open interval $]a, b[$. If $f(a) = f(b)$ then f has a critical point in $]a, b[$.*

Since $Q(1) = Q(2) = \ldots = Q(2016) = 0$, it follows from Rolle's theorem that $P(x)$ has a real root in each of the intervals $]k, k+1[$ for $k = 1, \ldots, 2015$.

Problem 7. Chain Stores

1. Let f be a piecewise continuous function on the interval $[0,1]$. Give a geometric interpretation of the integral $\int\limits_0^1 f(x)dx$. **(1 point)**

2. Let $n > 2$ be a natural number. Compare the following integrals:

$$I_1 = \int\limits_0^1 dist(x, S_1)dx \quad \text{and} \quad I_2 = \int\limits_0^1 dist(x, S_2)dx\,,$$

where $S_1 = \left\{\frac{k}{n}\right\}_{k=1}^{n-1}$ and $S_2 = \left\{\frac{k}{n} + \frac{1}{n^2}\right\}_{k=1}^{n-1}$ are sets of $n-1$ points in $[0,1]$. **(3 points)**

3. Take $f(x) = -2\,|2x-1| + 2$ and $n = 2$. Let S_{opt} be an optimal configuration of shops when the merchant builds the shops all at once, and let $\tilde{S}_{opt}$ be that when the merchant builds the shops one after another.

a) Find S_{opt} and $\tilde{S}_{opt}$. **(4 points)**

b) Find the ratio between $\int\limits_0^1 dist(x, S_{opt})f(x)\,dx$ and $\int\limits_0^1 dist(x, \tilde{S}_{opt})f(x)\,dx$. **(2 points)**

Solution

1. Consider the graph of the function f on $[0,1]$. Denote by D the domain in $\mathbb{R}^2$ bounded by the graph, the x-axis, the vertical lines $x = 0$ and $x = 1$ and the segments joining the points of the graph, where it is discontinuous. Then the integral $\int\limits_0^1 f(x)dx$ is the area of the part of D which is above the x-axis minus the area of that which is below the x-axis.

2. We will use the geometric interpretation of an integral. Both integrals are sums of areas of n distinct triangles: $n-2$ of these triangles are equal for I_1 and I_2 but the respective leftmost and rightmost triangles are distinct. Thus taking in the account the areas of the leftmost and the rightmost triangles, we get

$$I_1 - I_2 = \left(\frac{1}{2n^2} + \frac{1}{2n^2}\right) - \frac{1}{2}\left(\left(\frac{1}{n} + \frac{1}{n^2}\right)^2 + \left(\frac{1}{n} - \frac{1}{n^2}\right)^2\right) = -\frac{1}{n^4} < 0.$$

Hence, $I_1 < I_2$.

3. *Answer:* $S_{opt} = \left\{\frac{\sqrt{2}}{4}, 1 - \frac{\sqrt{2}}{4}\right\}$ and $\tilde{S}_{opt} = \left\{\frac{1+2\sqrt{2}}{14}, \frac{1}{2}\right\}$ or $\left\{\frac{1}{2}, \frac{13-2\sqrt{2}}{14}\right\}$

a) One can show that a configuration for two shops being built simultaneously should be symmetric. Thus we have to minimise the following integral, where y is the coordinate of the leftmost shop:

$$\int\limits_0^{\frac{1}{2}} |y - x|4x\,dx = \frac{4}{3}y^3 - \frac{1}{2}y + \frac{1}{6}$$

(we used the fact that $-2\,|2x-1| + 2 = 4x$ for $x < \frac{1}{2}$). The minimum is achieved for $y = \frac{\sqrt{2}}{4}$ and so $S_{opt} = \left\{\frac{\sqrt{2}}{4}, 1 - \frac{\sqrt{2}}{4}\right\}$.

When the merchant builds the shops one after another, his first shop should be in the centre. To calculate the coordinate of the second shop (suppose it is $< \frac{1}{2}$), we have to minimise the

following integral over $y \in [0, \frac{1}{2}]$:

$$\begin{aligned} g(y) &:= \int_0^1 dist(x, \{y, 1/2\}) f(x) dx \\ &= \int_0^{\frac{1}{2}y+\frac{1}{4}} |y-x| 4x\, dx + \int_{\frac{1}{2}y+\frac{1}{4}}^{\frac{1}{2}} \left(\frac{1}{2} - x\right) 4x\, dx + \int_{\frac{1}{2}}^1 \left(x - \frac{1}{2}\right)(4-4x)\, dx \\ &= \left(y^3 - \frac{1}{4}y^2 + \frac{1}{48}\right) + \left(\frac{1}{6}y^3 - \frac{1}{8}y + \frac{1}{24}\right) + \frac{1}{12} \\ &= \frac{7}{6}y^3 - \frac{1}{4}y^2 - \frac{1}{8}y + \frac{7}{48}\,. \end{aligned}$$

The derivative of this function is $g'(y) = \frac{1}{8}(28y^2 - 4y - 1) > 0$. The minimum of g on the interval $[0, \frac{1}{2}]$ is achieved for $y = \frac{1+2\sqrt{2}}{14}$. We obtain $\tilde{S}_{opt} = \left\{\frac{1+2\sqrt{2}}{14}, \frac{1}{2}\right\}$ or $\left\{\frac{1}{2}, \frac{13-2\sqrt{2}}{14}\right\}$.

b) *Answer:* $\frac{7^2}{6^2+4^2\sqrt{2}}$

We have

$$\int_0^1 dist(x, S_{opt}) f(x) dx = \frac{8}{3}\left(\frac{\sqrt{2}}{4}\right)^3 - \frac{\sqrt{2}}{4} + \frac{1}{3} = \frac{2-\sqrt{2}}{6}\,,$$

$$\int_0^1 dist(x, \tilde{S}_{opt}) f(x)\, dx = g\left(\frac{1+2\sqrt{2}}{14}\right) = \frac{20-2\sqrt{2}}{147}$$

The ratio is then

$$\frac{\int_0^1 dist(x, S_{opt}) f(x) dx}{\int_0^1 dist(x, \tilde{S}_{opt}) f(x) dx} = \frac{49}{2} \cdot \frac{2-\sqrt{2}}{20-2\sqrt{2}} = 49 \cdot \frac{1}{(20-2\sqrt{2})(2+\sqrt{2})} = \frac{49}{36+16\sqrt{2}} < 1\,.$$

Problem 8. A Diophantine Equation

1. a) Give a definition of a *multiplicative* function (in number theory). **(1 point)**

b) Let n be a natural number and denote by $\tau(n)$ the number of its natural divisors, including 1 and n. Give a formula for $\tau(n)$. **(1 point)**

2. Denote by $g(n)$ the number of solutions of the equation

$$xyz = n$$

in positive integers x, y, z. Prove that $g(n) < n^{\frac{1}{2015}}$ for sufficiently large n. **(3 points)**

3. A *Carmichael number* is a **composite** number n such that

$$n \text{ divides } x^{n-1} - 1$$

for all integers $1 < x < n$ which are relatively prime to n.

a) Prove that all Carmichael numbers are odd. **(2 points)**

b) A natural n is called *square-free* if it is not divisible by any square k^2, where $k > 1$ is an integer. Prove that a Carmichael number must be square-free. **(3 points)**

Solution

1. a) An arithmetic function f is *multiplicative* if $f(1) = 1$ and the equality

$$f(mn) = f(m)f(n)$$

holds for every coprime $m, n \in \mathbb{N}$.

b) The function $\tau(n)$ is multiplicative and $\tau(p^\alpha) = \alpha + 1$ for any prime p. Therefore, if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is a factorisation of n then $\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$.

2. We will need the following lemma:

Lemma. *For any positive real number $\varepsilon > 0$, one has $\tau(n) \ll n^\varepsilon$.*

Proof. For $n = p^\alpha$ with p prime, we have $\tau(p^\alpha) = \alpha + 1 = \log_p(n) + 1$ and

$$\frac{\tau(n)}{n^\varepsilon} \to 0 \text{ as } n = p^\alpha \to \infty.$$

Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ be a factorisation of n with $p_1 < \dots < p_k$. Then

$$\frac{\tau(n)}{n^\varepsilon} = \frac{\tau(p^{\alpha_1})}{p^{\alpha_1 \cdot \varepsilon}} \cdots \frac{\tau(p^{\alpha_k})}{p^{\alpha_k \cdot \varepsilon}}. \tag{2}$$

When n tends to ∞ we have one of the two following situations: either k stays bounded and some $p_i^{\alpha_i} \to \infty$, or k grows to ∞. In the first situation, some of the factors $\frac{\tau(p^{\alpha_i})}{p^{\alpha_i \cdot \varepsilon}}$ in the equation (2) tend to 0 and the others are bounded, so $\frac{\tau(n)}{n^\varepsilon} \to 0$. In the second situation, $p_k \to \infty$ as $k \to \infty$, and so the last factor $\frac{\tau(p^{\alpha_k})}{p^{\alpha_k \cdot \varepsilon}}$ tends to 0 (in particular it is less than 1 for sufficiently large k). Therefore, $\frac{\tau(n)}{n^\varepsilon} \to 0$ as $k \to \infty$. □

The number of possible pairs (x, y) such that $xyz = n$, for some $z \in \mathbb{N}$, doesn't exceed $(\tau(n))^2$, since x and y are divisors of n. Given x and y, one finds $z = n/(xy)$. Therefore, the number of solutions (x, y, z) of the equation is bounded: $g(n) \leq (\tau(n))^2$. By the lemma for any $\varepsilon > 0$, we have $g(n) \ll n^{2\varepsilon}$. In particular, for $\varepsilon = \frac{1}{4032}$ we get $g(n) \ll n^{\frac{1}{2016}} < n^{\frac{1}{2015}}$.

3. a) Suppose that a Carmichael number n is even, $n = 2k$. We have

$$(n-1)^{n-1} = (2k-1)^{2k-1} \equiv (-1)^{2k-1} = -1 \pmod{n}.$$

However, $n - 1$ is relatively prime to n and so $(n-1)^{n-1} \equiv 1 \pmod{n}$. Contradiction.

b) Suppose that there is a Carmichael number $n = p^k m$ with p prime, $k > 1$ and $p \nmid m$. Take $a = p^{k-1}m + 1$, it is relatively prime to n and so $a^{n-1} \equiv 1 \pmod{n}$. On the other hand,

$$a^{n-1} = (p^{k-1}m + 1)^{n-1} \equiv (n-1)p^{k-1}m + 1 \equiv -p^{k-1}m + 1 \not\equiv 1 \pmod{n}.$$

Contradiction.

Remark. Suppose that the number $f(a, b)$ of natural solutions (x, y, z) of the equation

$$xyz + a(x + y) = b$$

satisfies $f(a, b) \ll |ab|^\varepsilon$ for any $\varepsilon > 0$. Denote by $C_3(n)$ the number of Carmichael numbers not greater than n and having exactly three prime factors. Then one can show that $C_3(n) \ll n^{\frac{1}{3}+\varepsilon}$.

Problem 9. Framing Matrices

1. a) Give a definition of a *vector space* over a field K. **(1 point)**

b) When does a system of vectors is *linearly independent* over K? **(1 point)**

2. Find the number of framing pairs (A, B) such that:

- A is a diagonal 2×2 matrix of order 6 and
- $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. **(4 points)**

3. Three vectors $v_1, v_2, v_3 \in \mathbb{R}^3$ are randomly chosen with the condition that every coordinate of each vector is a real number from the interval $[0, 1]$. What is the probability that these three vectors are linearly independent over $\mathbb{R}$? **(4 points)**

Solution

1. a) A *vector space* over K is an additive group V together with a rule of multiplication $\lambda \cdot v$ of elements $v \in V$ by scalars $\lambda \in K$. Moreover, the following axioms must be satisfied for any $u, v \in V$ and $\lambda, \mu \in K$:

(1) $1 \cdot v = v$,
(2) $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$,
(3) $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$,
(4) $(\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v)$.

b) A system of vectors $v_1, \ldots, v_m$ is *linearly independent* over K if from an equality

$$\lambda_1 v_1 + \ldots + \lambda_m v_m = 0, \qquad \text{for some } \lambda_i \in K,$$

necessarily follows that $\lambda_1 = \ldots = \lambda_m = 0$

2. *Answer:* 12

Let us solve this problem is case A is a diagonal matrix of order n. Put $\lambda = \exp(2\pi i/n)$. Then any diagonal 2×2 matrix A of order n should be of the form $A = \begin{pmatrix} \lambda^r & 0 \\ 0 & \lambda^s \end{pmatrix}$, where r, s are elements of $\mathbb{Z}_n$. Additionally, they should generate $\mathbb{Z}_n$ additively. Otherwise A has order smaller than n.

If the pair (A, B) is framing then, in particular, the vectors $(A^x \cdot v)$, $(A^y \cdot v)$ are linearly independent for all $x \neq y \in \mathbb{Z}_n$. This means that

$$\det \begin{pmatrix} \lambda^{rx} & \lambda^{ry} \\ \lambda^{sx} & \lambda^{sy} \end{pmatrix} = \lambda^{rx+sy} - \lambda^{ry+sx} \neq 0.$$

This implies that $(r - s)x \neq (r - s)y \mod n$ for any $x \neq y \in \mathbb{Z}_n$. This is the case if and only if $r - s$ is an invertible element in $\mathbb{Z}_n$. There are exactly $n\phi(n)$ such pairs. Clearly, each such pair generates $\mathbb{Z}_n$.

It is easy to check that the pairs of vectors $(A^x \cdot v)$, $(A^y B \cdot v)$, $x, y \in \mathbb{Z}_n$, and $(A^x B \cdot v)$, $(A^y B \cdot v)$, $x \neq y \in \mathbb{Z}_n$ are linearly independent for generic v. Thus, there are exactly $n\phi(n)$ matrices A with the required properties.

For $n = 6$ we have $n\phi(n) = 6 \cdot 2 = 12$.

3. *Answer:* 1

We relabel the vectors u, v and w for clarity.

The probability that the three vectors are linearly *dependent* is the sum of the three following (and disjoint) cases:

- u is the null vector;
- v is a multiple of u, which is not the zero vector;
- w is a combination of u and v, which are linearly independent.

The first case has zero probability, because it only happens if all entries in $u = (u_1, u_2, u_3)$ are zero, and each of these events has zero probability.

Let's analyse the second case. Take a non-zero entry of u, without loss of generality let it be the first one. So once the first entry of v is chosen (say it is $v_1 \in [0, 1]$), then all other entries of v are determined by the ratio v_1/u_1. But the probability that any particular value in $[0, 1]$ is taken is zero, so the probability of the second case is zero.

Finally, we study the third case. Now, let E be the space spanned by u and v, and take a vector N normal to E; it has some non-zero coordinate. Without loss of generality, this is the third coordinate. In this case, once we are given the two first coordinates of w, there is only one

possibility for the third coordinate that makes w a vector perpendicular to N: this amounts to solving $w_3N_3 = -(w_1N_1 + w_2N_2)$. But a vector belongs to the plane spanned by u and v if and only if it is perpendicular to N. Again, the probability of having the third coordinate of w_3 a fixed number in $[0, 1]$ is zero, so again the third case has probability zero.

Therefore, the probability that the vectors are linearly dependent is zero. By taking the complementary event, we see that the probability that the three vectors u, v and w are linearly independent is 1.

Problem 10. Polynomial Groups

1. Give definitions of a *group* and an *abelian group*. **(1 point)**

2. Let $p \geq 2$ be a prime number.

a) Prove that any group G of order p^2 is abelian. The *order* of a group is the number of its elements. **(3 points)**

Indication. Consider the action of the group G on its elements by conjugation (for any $h \in G$ one has a map $f_h : G \to G$, $g \mapsto hgh^{-1}$). Present G as a disjoint union of orbits $G(g) = \{hgh^{-1} \mid h \in G\}$. Investigate how many elements there are in the center of the group G, namely in the subgroup $Z = \{g \in G \mid hgh^{-1} = g \text{ for all } h \in G\}$.

b) Show that the polynomial group $G_3(p)$ is abelian. **(1 point)**

3. Let $p \geq 3$ be an odd prime number. Consider the following set of upper-triangular matrices over the field $\mathbb{F}_p$:

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}.$$

a) Prove that H_p is a group. It is called the *Heisenberg group* over $\mathbb{F}_p$. **(2 points)**

b) Show that the group H_p is two-generator. **(3 points)**

Solution

1. A *group* is a set G together with an operation " $*$ " on G which satisfies three axioms:

a) The operation is *associative*: $(x * y) * z = x * (y * z)$ for any three elements of G.

b) There is an element e in G, called the *identity element*, such that $x * e = e * x = x$ for every x in G.

c) Each element x of G has a (so-called) *inverse* x^{-1} which belongs to the set G and satisfies $x^{-1} * x = x * x^{-1} = e$.

A group G is *abelian* if $x * y = y * x$ for every two elements x and y of G.

2. a) Indeed, let G be a group of order p^2. Denote by Z its center, that is the elements of G which commute with all elements of G,

$$Z = \left\{ g \in G \;\middle|\; hgh^{-1} = g \text{ for all } h \in G \right\}.$$

One can check that Z is a *subgroup* of G. In particular, the order of Z divides that of G and thus equals 1, p or p^2. By definition, the group G is abelian if and if $|Z| = p^2$.

The group G acts on its elements by conjugation. Then G is a disjoint union of orbits $G(g_1), \ldots, G(g_k)$. The length of each orbit divides the order of the group G (a known fact that can be easily proved). Moreover $|G(g_i)| = 1$ if and only if $hg_ih^{-1} = 1$ for all $h \in G$, that is $g_i \in Z$. Otherwise, $|G(g_i)|$ is equal to p or p^2. Therefore, we obtain that

$$p^2 = |G| = \sum_{i=1}^{k} |G(g_i)| = \sum_{g_i \in Z} 1 + \sum_{g_i \notin Z} |G(g_i)| = |Z| + \sum_{g_i \notin Z} |G(g_i)|.$$

Since the sum $\sum_{g_i \notin Z} |G(g_i)|$ is a multiple of p, the order of the center Z is a multiple of p as well. If $|Z| = p^2$ then the group $G = Z$ is abelian. Else $|Z| = p$, implying that both the subgroup Z and the quotient group G/Z are cyclic groups of order p (any group of order p is cyclic). Suppose that Z is generated by u and G/Z by vZ where $u, v \in G$. Then the group G is generated by u and v which commute because $u \in Z$. This means that G is abelian.

b) *First method.* The group $G_3(p)$ is of order p^2, and thus is abelian due to 2a).

Second method. One can directly check that the pair of elements $(x + x^2, x + x^3)$ generates $G_3(p)$ and these elements commute. Thus, the group is abelian.

3. a) Indeed, the product of two matrices from H_p

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & s & t \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+s & t+au+b \\ 0 & 1 & u+c \\ 0 & 0 & 1 \end{pmatrix}$$

is also in H_p. The identity element of H_p is the identity matrix (with 1's on the diagonal and 0's everywhere else). Since the determinant of any matrix from H_p is 1, it is invertible and the inverse

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & -b+ac \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \tag{3}$$

is also an element of H_p. The associativity of the product is straightforward.

b) Consider the following matrices

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

For any integers k, ℓ, m, one has modulo p

$$A^k = \begin{pmatrix} 1 & k & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad B^\ell = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \ell \\ 0 & 0 & 1 \end{pmatrix}, \quad C^m = \begin{pmatrix} 1 & 0 & m \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and so

$$A^k B^\ell C^m = \begin{pmatrix} 1 & k & m+k\ell \\ 0 & 1 & \ell \\ 0 & 0 & 1 \end{pmatrix} \mod p,$$

that is any matrix from H_p can be presented as a product $A^k B^\ell C^m$. Since $C = ABA^{-1}B^{-1}$, we conclude that the group H_p is generated by the pair (A, B).

Remark. It is possible to show that the polynomial group $G_4(p)$ and the Heisenberg group H_p are isomorphic. A proof uses the fact that for $p \geq 3$, up to isomorphism, there are 5 types of groups of order p^3, namely three abelian groups, a group of 2×2 matrices and the Heisenberg group. One checks that the polynomial group $G_4(p)$ isn't isomorphic to the four other groups.