International Mathematical Camp

Maths Beyond Limits

Camp Brochure
(electronic edition)

Milówka 2018
Text preparation and drafting: Anna Łeń, Paweł Piwek, Szymon Zwara

Problems, solutions: Grzegorz Dłużewski, Jan Fornal, Mateusz Kobak, Tomasz Przybyłowski

Handouts: Łukasz Bożyk, Tomasz Cieśla, Gábor Damásdi, Andrzej Grzesik, Jan Kociniak, Mark Krusemeyer, Anna Łeń, Alina Yan

Typesetting (with \TeX/\LaTeX): Łukasz Bożyk

Cover project: Łukasz Bożyk, Bartłomiej Żak

ISBN: 978-83-901470-2-4
Copyright © by Polish Children’s Fund
Warsaw 2019

Free electronic edition, available online at mathsbeyonlimits.eu
Version E-2 (March 30, 2019).

Maths Beyond Limits
e-mail: mathsbeoyunlimits@gmail.com
www: mathsbeoyunlimits.eu
Facebook fanpage: facebook.com/mathsbeyondlimits

Polish Children’s Fund
ul. Pasteura 7, 02-093 Warsaw
tel. (+48 22) 848 24 68
e-mail: fundusz@fundusz.org
www: fundusz.org

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.
About the camp

Maths Beyond Limits is a Europe-wide camp for high school students interested in maths. MBL 2018 was the third edition of this initiative and was held from 9th to 21st September 2018 in Milówka, Poland. 60 students from Belgium, Belarus, Czech Republic, Denmark, Estonia, Hungary, Norway, Poland, Romania, Slovakia, Sweden and Ukraine (who filled in the Applicant Questionnaire and solved problems from the Qualifying Quiz), along with 16 tutors (from the aforementioned countries as well as from the UK and the US) and 6 organisers, took part in it.

The aim of the project is to create space for development of young maths enthusiasts through working on interesting and demanding mathematical subjects. It is designed to encourage participants to share their knowledge and passion with others as well as to enhance cooperation and integration of European mathematical societies. Moreover, our goal is to awaken youth’s curiosity and to help them make important habits of creative thinking, self-development, ambition and ability to cooperate.

MBL 2018 was a 12-day-long programme, filled with numerous events. Every regular day there were three 80-minute-long blocks of Mathematical Classes. They were devoted to some of the most beautiful concepts in mathematics from outside the high school’s curriculum. During every block there were 3 lecture sessions to choose from, each concerning different mathematical field, which contributed to the diversity of academic experience participants had on the camp. Classes were followed by an hour-long TAU, which stands for Time Academic Unscheduled that was designated for the students to work on the problems independently or with the help of tutors. It was also a great opportunity to clarify any points of the classes that were found hard or insufficiently explained. The last regular mathematical events were Camper Talks, i.e. a 30-minute-long presentations given by some participants on topics connected to mathematics they were interested in. Their main goal was to give participants the opportunity to practice important skills of clear presentation of mathematical topics in English while inspiring others with their passions. Students had prepared them beforehand and consulted them with staff members during the camp.

Maths was not the only thing the camp was about, therefore the hard work was followed by Evening Activities. They were fun, challenging, educational or thought-provoking. Most of them were run by the participants, while other by the staff. Lastly, there was also time for Sports in the beautiful scenes of Beskidy mountains. Activities included running and workouts as well as playing volleyball, football and frisbee.

At MBL we do not let anyone get bored, therefore also quite a few special events were organised. We went for a Hike in Beskid mountains and solved a bunch of puzzles during the Puzzle Hunt, as well as had fun playing guitars and singing by the Campfire. Participants also got a chance to talk about careers, universities and olympiads with tutors and organisers during the Questions Evening Café. Moreover, they were able to improve their problem solving skills thanks to Relays (team competition similar to Náboj) and Mathematical Matches. There were 3 divisions of Mathematical Matches differing in difficulty, each of them was a team contest where teams got problem sets in the evening and presented their solutions by the board the next day. All these little things contributed to making MBL 2018 such a great, inspiring and unforgettable camp.
People of the camp

The following is the list of all people that took part in MBL 2018.

**Participants**

- Andreas Alberg
- Mykhailo Bondarenko
- Jagoda Bracha
- Katarzyna Cuper
- Jadwiga Czyżewska
- Jakub Dobrowolski
- Witold Drzewakowski
- Hugo Eberhard
- Fredrik Ekholm
- Paweł Gadziński
- Mikołaj Grzebieluch
- Ágoston Győrffy
- Stanisław Hauke
- András Imolay
- Justyna Jaworska
- Łukasz Kamiński
- Anna Kerekes
- Wojciech Kolesiński
- Antoni Koszowski
- Adam Křivka
- Marta Kuczma
- Richard Luhtaru
- Miroslav Macko
- Simon Martin
- Mateusz Masłowski
- Dávid Matolcsi
- Magdaléna Mšinová
- Karina Nechiporuk
- Aliaksandra Novik
- Jakub Parada
- Gábor Pituk
- Arkadiusz Pospieszny
- Małgorzata Róg
- Szymon Rusiecki
- Ádám Schweitzer
- Paulina Skalik
- Jakub Skrajny
- Tomasz Ślusarczyk
- Dávid Szabó
- Kristóf Szabó
- Jakub Szulc
- Michał Szwej
- Ádám Tiszay
- Nguyen Tran Bach
- Mariusz Trela
- Hendrik Vija
- Alex Villaro y Krüger
- Carl Westerlund
- Fedir Yudin
- Alicja Ziarko
- Vladyslav Zveryk
- Piotr Zygmunt

**Semitutors**

- Marcin Augustynowicz
- Denis Chirita
- Aleksandra Kowalska
- Natalia Kucharczuk
- Bartłomiej Lewandowski
- George Adrian Picu
- Kacper Walentynowicz
- Jakub Wornbard

**Tutors**

- Piotr Ambroszczyk
- Łukasz Bożyk
- Tomasz Cieśla
- Robert Crumplin
- Gábor Damásdi
- Anna Doležalová
- Andrzej Grzesik
- Jan Kociński
- Mark Krusemeyer
- Michał Pilipczuk
- Paweł Poczobut
- Marian Poljak
- Maria Ulan
- Kada Williams
- Alina Yan
- Bartłomiej Żak
ORGANISERS

• Grzegorz Dłużewski
• Anna Łeń
• Marta Mościcka
• Paweł Piwek
• Tomasz Przybyłowski
• Szymon Zwara

OTHERS

• Mikołaj Opatowski
  Camera operator & film editor
• Michał Wiraszka
  Photographer

EVENTS OF THE CAMP

MATHEMAMITICAL CLASSES

• Algebraic Geometry, Mathematical Physics and Robotics [Maria Ulan]
• Automata and Language Theory [Marta Mościcka]
• Banach-Tarski Paradox [Jan Kociniak]
• Central Limit Theorem [Marian Polyak]
• Circles of Various People [Piotr Ambroszczyk & Natalia Kucharczuk]
• Compact Topologies [Robert Crumplin]
• Crash Course on Abstract Algebra [Paweł Poczobut]
• Cycles in Permutations [Łukasz Bożyk]
• Desargues Involution Theorem [Denis Chirita]
• Elementary Topology [Gábor Damásdi]
• Galois Theory [Paweł Poczobut]
• Game Theory [Aleksandra Kowalska & Kacper Walentynowicz]
• Graph Embeddings, Well-quasi-orderings, and Structural Graph Theory [Michał Pilipczuk]
• Infinitive Set Theory [Robert Crumplin]
• Introduction to Category Theory [Anna Doleżalová]
• Introduction to Combinatorial Designs [Anna Łeń & Łukasz Bożyk]
• Introduction to Graph Limits [Andrzej Grzesik]
• Introduction to Graphs and Graph Coloring [Gábor Damásdi]
• Lattices in Number Theory [Alina Yan]
• Linear Algebra with Applications to Combinatorics [Jakub Wornbard & Bartłomiej Lewandowski & Marcin Augustynowicz]
• Random Walks [Bartłomiej Żak]
• The A-Humpty Point of a triangle and Radius 0 Circles [George Picu]
• The Zoo of Olympiad Problems [Kada Williams]
• Transfinite Induction [Tomasz Cieśla]
Evening Activities

- 1 Out of MBL [Kacper Walentynowicz]
- Astronomical Observations [Wojciech Kolesiński]
- Bridge [Marta Kuczma & Jakub Wornbard]
- A Brief Introduction to Tea [Alicja Ziarko]
- A Short Lesson of Icelandic [Justyna Jaworska]
- Debate Tournament [Denis Chirita]
- Introduction to Mathematical Linguistics [Michał Szwej]
- Karate [Adam Křivka]
- Make a Postcard! [Paweł Piwek]
- MathemaTINA making [Anna Łeń & Paweł Piwek]
- Nordic folk/metal [Jakub Wornbard]
- Origami [Magdaléna Mišinová & Mikołaj Grzebieluch]
- Photo Hunt [Denis Chirita & Richard Luhtaru]
- Polish Song! [Jagoda Bracha]
- PowerPoint Karaoke
- Rock’n’Roll [Bartłomiej Lewandowski]
- Run Without Fatigue [Katarzyna Cuper]
- Singing Workshops [Hendrik Vija]
- Survival [Katarzyna Cuper]
- Tango Session [Ádám Tiszay]
- Team Trivia [Jakub Dobrowolski, Anna Łeń, Simon Martin & Michał Szwej]
- Theatre Workshops [Jadwiga Czyżewska]
- Xiangqi [Tomasz Ślusarczyk]

Special Events

- Ice-breaking Game
- Puzzle Hunt
- Questions Evening Cafe
- Relays
- Mathematical Match
- Hike
Camper Talks

- Basel Problem [Tomasz Ślusarczyk]
- Bashing Inequalities with Muirhead and co. [Ágoston Győrffy]
- Bertrand’s Postulate [Witold Drzewakowski]
- Carnot’s Theorem and Japanese Theorem [Justyna Jaworska]
- Expansions of Numbers [Gábor Pituk]
- Fibonacci Word and Fractal [Simon Martin]
- Frobenius Coin Problem [Łukasz Kamiński]
- Introduction to Data Science [Ádám Tiszay]
- Intuitive Topology [Alex Villaro Y Krüger]
- Miquel Point [Anna Kerekesz]
- Nash Equilibrium [Paulina Skalik]
- Rotations [Katarzyna Cuper]
- Fuhrmann Circl [Michał Szwej]
- The Law of Quadratic Reciprocity [Jakub Dobrowolski]
Testimonials

• **Andreas Alberg** (participant): Maths Beyond Limits is not only a possibility to be introduced to a variety of different mathematical topics by skilled lecturers, do math continuously for twelve whole days and improve your skill in olympic math. This is also an opportunity to meet interesting people from all over Europe, share experiences, play games, compete and make long-lasting friendships. In addition, MBL help you with choosing university and afterwards the application. Thank you for twelve wonderful days!

• **Jagoda Bracha** (participant): On MBL I didn’t have any time to do nothing. I’d like to be in a few places in each moment. There were great mathematical classes, variety of non-mathematical activities (where else would I experience for example survival lesson, rock and roll lesson and introduction to Icelandic language in one place?) and a lot of friendly, open-minded people. MBL is also about the atmosphere of equality, friendliness and freedom — no one shouts that you should go to sleep at 10 or not eat on the class.

• **Witold Drzewakowski** (participant): Friendly atmosphere, interesting conversations, inspiration, frequent frisbee/football, great lectures, random activities — this is MBL for me.

• **Hugo Eberhard** (participant): MBL gave me the opportunity to learn new things about mathematics, and has left me with motivation and inspiration to learn more. But it wasn’t only about mathematics, it was also about making new friends. The friendly, open-minded and welcoming atmosphere at the camp made it easy to talk to new people and made me feel welcome. It was a great experience and I would definitely recommend it!

• **Anna Kerekes** (participant): I’ve been to many different maths camps over the years, but the mathematical program was the best here.

• **Marta Kuczma** (participant): MBL was the best camp I’ve ever attended! The camp combines having fun, doing sports and learning maths on a very high academic level. Not only have I extended my understanding of the mathematical world, but I’ve also met wonderful people from all around the world and I hope to stay in touch with them forever. I cannot imagine any other place to meet so many passionate young people, this is what makes MBL’s atmosphere so special.

• **Simon Martin** (participant): MBL 2018 was 12 days of Maths, 12 days of new experiences and 12 days of fun. I appreciated every moment of it. It allowed me to discover challenging new Maths subject and learn a lot about them. It allowed me to improve in English, to meet a lot of new interesting people and to try activities that I would never have done otherwise (eg: Theater, Bridge, etc.).

• **Mateusz Masłowski** (participant): For me MBL was the greatest opportunity to rethink studies. After it I’m sure that I want to become a part of international society because I would love to be surrounded by different mindsets, cultures and the most intelligent people in Europe. I liked talking with people from Ukraine, Scandinavia or Romania more than with my natives because their ideas, future plans and daily basis were completely different than mine.
• **Hendrik Vija (participant):** This camp opened my eyes in so many ways: First, I understood why people are so sad after large international events, I really felt the same after MBL. Second, I realised that mathematicians are the best people to spend time with, everyone is a little quirky and different and we don’t have to hide it, it only makes things more enjoyable. Third, it taught me to take most of the time I have, since after the first days, I realised that I cherish every moment of the camp and that I want to spend it having fun, getting to know people and learning about maths, different cultures and so much more, even if doing it all means losing some sleep.

• **Vladyslav Zveryk (participant):** MBL is a well-organised camp with exciting events, high-level mathematical lectures and incredible atmosphere. People here are always ready to talk with each other, and I had a great chance to make friends from different countries, to share thoughts, and to discover a lot of interesting things while communicating with everyone here. There were a lot of really smart people whose achievements and passion encouraged me to work more and more in learning maths and striving for my goals.

• **Jakub Wornbard (semitutor):** The camp was a great opportunity to extend my knowledge, meet interesting people and enjoy myself by participating in a number of well-organized activities. I would recommend it to anyone passionate about mathematics.

• **Robert Crumplin (tutor):** It was fantastic to return as a tutor again this year. I got to meet new faces as well as those great friends I made last year and share our thoughts on interesting topics, especially on set theory and topology from my classes. It is inspiring to meet sure able and driven people who share their cultures as well as their common ground love for mathematics. An activity I particularly enjoyed was the hike as its a great time to have long conversations and reflect on the maths from the previous few days. I will certainly be returning in future!

• **Marian Poljak (tutor):** Maths, sports, music, new ideas, inspirational people and tons of fun. That’s what Maths Beyond Limits is.

• **Alina Yan (tutor):** It was great to meet so many people passionate about maths — people, who gave me a new inspiration about it. And it was pleasing to see such thorough organisation.

• **Bartłomiej Żak (tutor):** What do mathematicians do? They attend lectures, solve problems and talk to each other about them. They attend to competitions. They involve proving theorems, sometimes computing the answer, sometimes teaching others and sometimes running. But wait, there is more! They also play Frisbee of football, they run and dance. Some of they even perform a ultra workout in their time. They hike, play cards, sing or sometimes even wrestle.

Don’t believe it? See for yourself!
Sponsors and project partners

Running MBL would not be possible without the help of numerous people involved in organising, fundraising and working at the camp itself. All the tutors were volunteers who contributed their free time to prepare classes and come to the camp. MBL was free of charge to all the participants thanks to generous sponsors and wonderful project partners, which we had great pleasure of cooperating with.

**Sponsors and project partners**

Polish Children’s Fund’s mission is to support exceptionally gifted children and teenagers from all of Poland in order to enable them to fully develop their talents and scientific as well as artistic passions. The innovative, original aid programme conducted by the Fund for the last 33 years aims to support young people who cannot find opportunities to fully develop their potential in their local environment (both home and school).

**Trojsten** is a civic association that organizes mathematics, physics and informatics events in Slovakia for elementary and secondary school students. It organises KMS (Correspondent Mathematical Seminar), well-established international mathematical competition Náboj in Slovakia, the International Programming Competition ICPS and co-organises the International Mathematical Seminar iKS.

**The Joy of Thinking Foundation** supports gifted Hungarian students in fully developing their talents, reaching their goals in life, and becoming useful members of society. It attains this goals via furthering students’ abilities in math camps, math circles, one-to-one sessions and small group activities. Among the biggest initiatives of the Foundation are: the weekend math camps and Math is Fun! Camps (abbreviated MaMuT in Hungarian).

**Faculty of Mathematics and Physics of Charles University** offers maths and computer science programmes open to international students. It also organises manifold conferences, summer schools, camps and competitions for Czech youth such as: an international mathematical competition Náboj, physics competitions FYKOS and Fyzikláni and Czech Linguistics Olympiad.
Main Sponsors

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe. Grant support is given to original projects namely in the areas of culture, science and research, youth exchanges, cross-border cooperation and tourism promotion, as well as in other priority areas defined in calls for proposals published on the fund’s website.

Akademeia High School is a new international, academically-selective school in Warsaw, offering A-levels and GCSEs. The school focuses on developing both students’ academic abilities and their artistic, athletic and leadership potential. The majority of their students are preparing to study at Oxbridge, Russell group, and Ivy League universities as well as acclaimed architecture, art and music schools. The school offers a substantial scholarship program with about 20% of students being scholars.

ADAMED SmartUP is a scientific and educational programme that aims to give you a chance to discover the fascinating world of both the physical and natural sciences. On their website you can draw inspiration from the best Polish and foreign lecturers. You will get advice on where to study in Poland and abroad and find out what a scientific career looks like. You can enroll to an exceptional science camp and compete for a scientific scholarship.

With offices in New York, London, Hong Kong, and Amsterdam, Jane Street is a trading firm that operates around the clock and around the globe, trading a wide range of financial products. They are a global liquidity provider and market maker, trading mostly products that are listed on exchanges. They offers internships (as a trader, developer, business developer or researcher) for all university students from freshmen to post-doctoral scholars.
Selected Handouts
We define a **density** of a graph $H$ in a graph $G$ as the probability that randomly chosen subset of $|H|$ vertices of $G$ induces a graph isomorphic to $H$, i.e.,

$$d(H,G) = \frac{\text{number of induced copies of } H \text{ in } G}{\binom{|G|}{|H|}}.$$ 

1. Find $d(\mathcal{I}, \Box), d(\Delta, \Box), d(\mathcal{L}, \Box)$ and $d(\Lambda, K_{n,n})$.

We say that a sequence of graphs $(G_n)_{n \in \mathbb{N}}$ of growing orders is **convergent** if for every graph $H$ the sequence of densities $d(H,G_n)$ is convergent.

2. Decide which of the following graph sequences $(G_n)_{n \in \mathbb{N}}$ are convergent:

   a) $G_n = K_{n,3n}$;
   
   b) $G_n$ is any graph on $n$ vertices of maximum degree 10;
   
   c) $G_n$ is the graph on $n$ vertices containing a clique on $p$ vertices and the remaining vertices are isolated, where $p$ is the smallest prime divisor of $n$.

A **graphon** is a symmetric measurable function $W : [0,1]^2 \to [0,1]$, where symmetric means that $W(x,y) = W(y,x)$ for all $x,y \in [0,1]$.

We define the **density** of a graph $H$ in a graphon $W$ to be the probability that the random graph obtained by sampling $|H|$ points $x_1, \ldots, x_{|H|}$ in $[0,1]$ and joining the $i$-th vertex and the $j$-th vertex of the graph by an edge with probability $W(x_i,x_j)$, is isomorphic to $H$, i.e.,

$$d(H,W) = \frac{|H|!}{|\text{Aut}(H)|} \int_{[0,1]^{\times |H|}} \prod_{v_i,v_j \in E(H)} W(x_i,x_j) \prod_{v_i,v_j \notin E(H)} (1-W(x_i,x_j)) \, dx_1 \cdots x_{|H|},$$

where $V(H) = \{v_1, \ldots, v_{|H|}\}$ and $\text{Aut}(H)$ is the automorphism group of $H$.

We say that a graphon $W$ is the **limit** of a convergent sequence $(G_n)_{n \in \mathbb{N}}$ of graphs if

$$d(H,W) = \lim_{n \to \infty} d(H,G_n)$$

for every graph $H$.

For every convergent sequence of graphs there exists a graphon, which is the limit of this sequence. The limit is unique up to measure preserving transformations. Every graphon is the limit of a convergent sequence of graphs.

3. What sequences of graphs can converge to the following graphons? (value 0 is white, value 1 is black, the origin is in the top left corner)
4. To what graphons are converging the sequences from the previous problem on convergent sequences?

5. Consider a real number $p \in [0,1]$ and a graphon $W$ such that $W(x,y) = p$ if $x,y \in [1-2^{-n+1},1-2^{-n}]$ for some $n \in \mathbb{N}$, and $W(x,y) = 0$ otherwise. For any $k \in \mathbb{N}$ determine the density of $K_k$ in $W$.

6. Express $d(\overset{\circ}{\bullet}, W')$ in terms of $d(\overset{\circ}{\bullet}, W)$, $d(\bullet, W)$, $d(\Lambda, W)$ and $d(\Delta, W)$, where $W'$ is the depicted graphon containing two equal-sized parts, one with the graphon $W$ and one with the complete graphon.

For shortening, from now on, we identify a graph $H$ with the density of $H$ in any graphon.

For example, Mantel’s theorem saying that any triangle-free graph on $n$ vertices has at most $\frac{n^2}{4}$ edges, for graphons can be stated as $\Delta = 0 \Rightarrow I \leq \frac{1}{2}$.

One can calculate the density of a graph $H$ not only by choosing $|H|$ random vertices, but also by choosing $k \geq |H|$ random vertices and then looking at the density of $H$ in the chosen graph on $k$ vertices. Thus we can write

\[ H = \sum_{G: |G| = k} d(H,G) \cdot G. \]  

7. Express $\Lambda$ using densities of graphs on 4 vertices.

We define multiplication of graphs as

\[ H_1 \cdot H_2 = \sum_{H: |H| = |H_1| + |H_2|} P(H_1,H_2;H) \cdot H, \]

where $P(H_1,H_2;H)$ is the probability that two random disjoint subsets of $|H_1|$ and $|H_2|$ vertices of $H$ induce graphs $H_1$ and $H_2$.

Linearly extending such defined multiplication to sums of graphs and identifying all equalities of the form (1), we obtain an algebra called flag algebra.

8. Calculate $\overset{\circ}{\Lambda}$, $\overset{\circ}{\bullet} \cdot \overset{\circ}{\bullet}$ and $\Delta \cdot \overset{\circ}{\bullet}$.

Everything can be defined in the same way for rooted graphs, i.e., graphs with fixed vertices (called roots, on pictures denoted by unfilled circles). For example $d(\overset{\circ}{\bullet}, G)$ is the degree of the fixed vertex devided by $|G| - 1$.

9. Calculate $d(\overset{\circ}{\bullet}, G)$.

10. Express $\nabla$ using densities of graphs on 4 vertices with one vertex fixed.

11. Calculate $\overset{\circ}{\nabla}$, $\nabla \cdot \overset{\circ}{\bullet}$ and $\nabla \cdot \overset{\circ}{\bullet}$.

For a rooted graph $G$ we define an averaging operator $[G]$ as $[G] = q(G) \cdot F$, where $F$ is the unrooted graph obtained from $G$ by removing all the roots (keeping them as unrooted vertices) and $q(G)$ is the probability that a random choice of roots on $F$ will create $G$.

12. Calculate $[\overset{\circ}{\bullet}]$, $[\nabla]$ and $[\nabla \nabla]$. 

□□□□
13. Using the inequality \( [(I-\varepsilon)^2] \geq 0 \) prove that \( \Delta + \varepsilon \geq 1/4 \).

14. Prove Mantel’s theorem for limits, i.e., if \( \Delta = 0 \) then \( I \leq 1/2 \).

15. By considering the sequence of blow-ups of a hypothetical counterexample, prove Mantel’s theorem stating that each \( n \)-vertex triangle-free graph has at most \( n^2/4 \) edges.

16. Consider a convergent sequence of graphs, where vertices of each \( n \)-vertex graph are of degree \( n/3 \) or \( 2n/3 \). Prove that in the limit \( \varepsilon + \Delta = 1/3 \).

For every rooted graphs \( G \) and \( H \) the following Cauchy-Schwarz inequality holds

\[ [G^2][H^2] \geq [GH]^2. \]

17. Using the inequality \( [I^2] \geq [I]^2 \) prove Goodman’s bound, i.e., \( \Delta \geq I(2I-1) \).

18. Inspect the proof of Mantel’s theorem and deduce the structure of the extremal graphs, i.e., graphs with \( \Delta = 0 \) and \( I = 1/2 \).

19. Inspect the proof of Goodman’s bound and deduce the structure of the extremal graphs, i.e., graphs with \( \Delta = I(2I-1) \).

20. Prove the inequality \( \Delta \leq 3\varepsilon + 3/8 \) and argue that any extremal graph satisfies \( I = 1/4 \) for almost all possible placements of the root.

21. Prove that for every integer \( k \geq 3 \) it holds \( K_k \geq ((k-1)I-(k-2))K_{k-1} \), and deduce Turán’s theorem stating that the density of edges in every \( K_k \)-free graph is at most \( \frac{k-2}{k-1} \). Find the structure of the extremal graphs.
Problems

1. There is a hunter and a squirrel standing on opposite sides of a tree. They circle around the tree once such that they remain on opposite sides of the tree during the movement. Is it true that the hunter goes around the squirrel?

2. Given a closed curve on the plane that partitions the plane into regions. Prove that the regions can be colored with two colors such that no two neighbours have the same color.

3. You have a picture with a string connected to two of its corners and you have two nails in a wall. Can you hang the picture on the wall, such that after removing any one of the nails the picture falls down?

4. a) There is an island containing four towns — the blue tribe live in two of the towns and the green tribe live in the other two. The people from the green towns are enemies of the people from the blue towns, so they decide to build a wall to separate green towns from blue towns. The tribes want to stick together, so the wall must not separate one green town from another, or one blue town from another. The wall must be continuous, it must not intersect itself, it must not split, it must not pass through a town, and each end of the wall must be at the coast. Let us call such a wall a dividing wall. Prove that it is always possible to build a dividing wall.

b) Is it true that we can connect the two blue towns and the two green towns with a road such that the two roads never intersect?

5. Can we find some kind of dividing wall on a torus?

6. Is it always possible to find a dividing wall if there are more green and blue towns?

7. This time you have $n$ nails in the wall and a list of subsets of the nails. Can you hang the picture on the wall, such that after removing any one of the given subsets the picture falls down?

8. What is the fundamental group of the torus?
Abstraction

Let $I$ denote the $[0,1]$ interval. A path on the plane is a continuous function $I \rightarrow \mathbb{R}^2$. Paths are usually denoted by greek letters, such as $\alpha, \beta, \gamma$. Note that a path is allowed to be self intersecting. Let $\alpha$ be a path. $\alpha(0)$ is the start point of the path and $\alpha(1)$ is the end point. This also gives direction to the path. If $\alpha(0) = \alpha(1)$, in other words the path ends in its starting position, then the path is called a loop.

Let $\alpha$ and $\beta$ be two paths that start and end at the same points. We say $\alpha$ and $\beta$ are homotopic if one can be moved into the other in a continuous manner, while fixing the endpoints. If $\alpha$ and $\beta$ are homotopic we use the following notation: $\alpha \sim \beta$.

Abstractly this can be stated like this: $\alpha$ and $\beta$ are homotopic if there exists a collection of paths, denoted by $\gamma_t$ for $t \in [0,1]$ such that they satisfy the following conditions: $\gamma_0 = \alpha$ and $\gamma_1 = \beta$ and $\gamma_t$ is a path from $\alpha(0)$ to $\alpha(1)$ for all $t \in [0,1]$ and $\gamma_t$ depends on $t$ continuously.

Operations on paths

The concatenation of a path $\alpha$ from $P$ to $Q$ with a path $\beta$ from $Q$ to $R$ leads to a path $\gamma = \alpha \ast \beta$ from $P$ to $R$. Formally let $\gamma(t) = \alpha(2t)$ for $t \leq 0.5$ and $\gamma(t) = \beta(2t - 1)$ for $t \geq 0.5$.

And the inverse of $\alpha$ is just $\alpha^{-1}$ from $Q$ to $P$, travelling backwards:

Let $P$ be a fixed point and let $\alpha$ be a path that starts at $P$. Let $1$ denote the constants path $1(t) = P$. With these definitions we have $\alpha \ast \alpha^{-1} \sim 1$. Let $\alpha, \beta$ and $\gamma$ be loops that start and end at $P$. Then $\alpha \ast (\beta \ast \gamma) \sim (\alpha \ast \beta) \ast \gamma$.

Let $X$ be a topological space. For example $X$ could be $\mathbb{R}^2$ or $\mathbb{R}^2 \setminus \{q\}$ or a torus, etc. Let $P$ be a fixed point of $X$. Then $\Pi_1(X;P)$ is the set of all loops in $X$ starting at $P$, where homotopic loops are identified. $\Pi_1(X;P)$ is the fundamental group of $X$. (In the cases that we investigate $\Pi_1(X;P)$ doesn’t depend on $P$, but generally it does.)

Further reading

- About the picture hanging puzzle: arxiv.org/pdf/1203.3602.pdf
- The article that gave me the idea for this course: www.mathematik.hu-berlin.de/~ploog/topology_in_school.pdf
- A very good introduction to winding numbers: plus.maths.org/content/list-by-author/Ian%20Short
- More on the fundamental group: en.wikipedia.org/wiki/Fundamental_group
We take two intersecting lines in the plane and two distances. Consider the family of lines that are parallel to the first line and at a distance an integral multiple of the first distance and then the same for the second line and the second distance. All these lines altogether are a **parallelogram lattice**.

Parallelograms made by two pairs of neighbouring lines from each family we will call **base parallelograms**.

The points of intersection are called **lattice points**, and all these points together form a **point lattice**.

It is pretty obvious that the parallelogram lattice uniquely determines the point lattice. However, the converse is not true.

Let us put the origin in a lattice point, and let vectors \( \vec{p} \) and \( \vec{q} \) be sides of one of the base parallelograms which contain the origin as a vertex. Now every lattice point can be described by a vector \( \vec{r} = u \cdot \vec{p} + v \cdot \vec{q} \), \( u,v \in \mathbb{Z} \), moreover, in the unique way. Also for Cartesian coordinates, provided that the vectors have the following coordinates \( \vec{r}(k,l) \), \( \vec{p}(m,n) \) and \( \vec{q}(x,y) \) we have \( x = uk + vm \), \( y = ul + vn \). For us this means that the solutions of such equations can be considered as a lattice.

**Properties**

1. If we translate a lattice so that one lattice point is moved onto another, then the entire lattice is moved onto itself.

   *Corollary:* If three points of a parallelogram are lattice points, the 4th point is also a lattice point.

   We will need to prove that some figures (actually, the bounded) can have only finitely many lattice points inside them. For this let us first prove the following property.

2. There is a positive number such that the distance between (distinct) lattice points is never smaller than this number.

   *Problem.* Which regular polygons can occur as lattice polygons? (Answer: Only triangles, squares and hexagons)

   *Hint:* Use the corollary from property 1 (about the forth point of a parallelogram being a lattice point).

**Lattice line** — a line which contains at least two lattice points.

It contains infinitely many points, all of them are equally spaced. Draw all lines parallel to it through every lattice point. All of them will be lattice lines too. And when we look at the family of all such lines, they are equally spaced.

We want to know when a parallelogram generates a given point lattice. Obviously, such a parallelogram must have lattice points as its vertices and cannot contain points neither on its boundary nor in the interior (we will call such parallelograms **empty**). Turns out that for any empty parallelogram its lattice coincides with the given point lattice.

**Theorem.** If a straight line is not parallel to a lattice line, then on each side of the line there are lattice points arbitrarily close to the line.
Problem. Prove Kronecker's theorem using the above theorem: \( \forall (a,b) \subset [0,1] \exists k \in \mathbb{Z}: \{ k\alpha \} \in (a,b) \).

Solution. Let us consider Cartesian coordinates and the lines \( y = ax - a, \ y = ax - b \). They are not parallel to lattice lines because all lattice lines have the rational slope, so there is a point \((x_0, y_0)\) between them: \( ax_0 - a > y_0 > ax_0 - b \Rightarrow a < ax_0 - y_0 < b \).

**Minkowski’s theorem.** In a parallelogram lattice in which base parallelograms have area \( d \), every convex, centrally symmetric region of area greater than \( d \), centered at a lattice point, contains a lattice point in its interior in addition to its center.

We do need all of these assumptions. You can come up with the examples which show that you cannot just give up: a) area of \( 4d \) b) convexity c) central symmetry (even having the origin as the center of gravity).

**Note:** The theorem also works for higher dimensions.

Do we actually need the parallelogram lattice? It depends only on the point lattice if there is a point inside a given figure. It seems that so does \( d \). Indeed, if we had empty parallelograms \( P_1 \) and \( P_2 \) with different areas \( d_1 < d_2 \), then parallelogram, made of four \( P_2 \) parallelograms with a common vertex (the origin), would have area \( 4d_2 > 4d_1 \) but no points in its interior except the origin. We get a contradiction with the theorem for the lattice with base parallelogram \( P_1 \). Therefore, all empty parallelograms in a point lattice have the same area.

**Diophantine approximations.** We want to approximate \( \alpha \in \mathbb{R} \setminus \mathbb{Q} \) with a fraction \( \frac{u}{v} \). It is obvious that we can find infinitely many pairs \((u,v)\) such that \( |\alpha - \frac{u}{v}| < \frac{1}{q} \). We want to find some better estimates \( |\alpha - \frac{u}{v}| < \phi(v) \), where \( \phi(v) \) is of the form \( \frac{1}{\sqrt{v^2}} \).

Try to prove these problems using the Minkowski’s theorem with the following extension: if a figure is closed and its area is exactly \( 4d \), then there is a lattice point in its interior or perimeter.

**Problem 1.** \( \forall \alpha \in \mathbb{R}, \ \forall q \in \mathbb{N} \ \exists u,v \in \mathbb{Z}: 1 \leq v \leq q, \ |v\alpha - u| \leq \frac{1}{q} \).

**Hint:** Consider a lattice which consists of all the points \((x,y)\) for which \( x = v\alpha - u, \ y = u \).

**Problem 2.** \( \forall \alpha \in \mathbb{R} \ \exists u,v \in \mathbb{Z} |\alpha - \frac{u}{v}| < \frac{1}{2v^2} \).

**Hint:** Consider the same lattice as in the previous problem and a rhombus \( c|x| + \frac{1}{c}|y| \leq \sqrt{2d} \).

**Problem 3.** There are infinitely many such pairs from **Problem 2**.

**Problem.** We would like to approximate the real numbers \( \alpha \) and \( \beta \) by two fractions with the same denominator, \( \frac{u}{w} \) and \( \frac{v}{w} \). What estimation can you find for the sum of the squares of the differences between the real numbers and their approximations if it must be true that \( 0 < w \leq q \) for a given positive number \( q \)?

**Hint.** Consider a lattice made of points \((w\alpha - u, w\beta - v, w)\) in the 3-dimensional space. The figure you need to consider is a cylinder of radius \( 2r \) and height \( q \).

**Theorem.** A positive integer \( n \) is expressible as a sum of 2 squares if and only if in the prime factorization of \( n \), every prime of the form \( 4k + 3 \) occurs an even number of times.

**Theorem.** An odd prime number \( p \) can be represented as a sum of two squares \( \iff \ p = 4k + 1 \).

**Proof.** For primes \( p \) of the form \( 4k + 1 \) there exist an integer \( a \) for which \( a^2 + 1 \) is divisible by \( p \). For such an \( a \), consider the lattice generated by vectors \((p,0)\) and \((a,1)\), as in the picture. The area of the base parallelogram \( d = p \).
This lattice can also be described as the points with coordinates \( x = pu + av, y = v \), where \( u \) and \( v \) are integers. For every lattice point the sum of the squares of coordinates is divisible by \( p \), since \( x^2 + y^2 = p(au^2 + 2auv) + (a^2 + 1)v^2 \), which is divisible by \( p \) by the choice of \( a \).

Applying Minkowski’s theorem to a circle of radius \( \sqrt{\frac{4p}{\pi}} \), we get that there exists a lattice point other than the origin whose coordinates satisfy \( x^2 + y^2 \leq \frac{4p}{\pi} \leq 2p \). But the sum \( x^2 + y^2 \) also is positive and divisible by \( p \). This is possible only if \( x^2 + y^2 = p \).

**Problem** (Lagrange’s four-square theorem). Prove that for every \( n \in \mathbb{N} \) there exist integers \( x, y, z, t \) such that \( n = x^2 + y^2 + z^2 + t^2 \). Volume of a 4-dimensional ball is \( \pi^2 R^4 \). 

**Hints.** At first prove it only for primes (and then show then the product of two numbers, both of which can be represented as the sum of four squares, can be represented as the sum of four squares itself). You will also need integer numbers \( r \) and \( s \) for which \( r^2 + s^2 + 1 \) is divisible by a given prime \( p \).
**Definition (balanced incomplete block design).** Let $V$ be a $v$-element set, $2 \leq k < v$, $\lambda \geq 1$. Family $\mathcal{D} \subseteq \mathcal{P}_k(V)$ of $k$-element subsets of $V$ is called a $(v,k,\lambda)$-design iff
\[ \forall A \in \mathcal{P}_2(V) \ | \{B \in \mathcal{D} : A \subseteq B\}| = \lambda, \]
i.e. every pair of elements of $V$ is a subset of precisely $\lambda$ sets from $\mathcal{D}$. Elements of $\mathcal{D}$ are called blocks.

**Problem 1.** Prove that the following descriptions yield combinatorial designs and in each case determine the parameters $(v,k,\lambda)$.

(a) $V = \mathbb{Z}_2^4 \setminus \{0\}$, $\mathcal{D} = \{\{x,y,z\} : x,y,z \in V, x+y+z = 0\}$.

(b) $n \geq 2$, $V = \mathbb{Z}_3^n$, $\mathcal{D} = \{\{x,y,z\} : x,y,z \in V, x+y+z = 0\}$.

(c) $V$ — edges of $K_5$, $\mathcal{D}$ — triples of edges forming paths (without repeated vertices).

(d) $V$ — edges of $K_5$, $\mathcal{D}$ — quadruples of edges of one of three forms: having a common vertex, forming a triangle and vertex-disjoint edge, or forming a cycle.

(e) $V$ — edges of $K_6$, $\mathcal{D} = \{B_e : e \in V\}$, $B_e$ — the edges having exactly one common vertex with $e$.

(f) $V$ — edges of $K_6$, $\mathcal{D}$ — triples of edges forming triangles or matchings (i.e. being mutually vertex-disjoint).

(g) $V$ — vertices of a four-dimensional hypercube, $\mathcal{D} = \{B_w : w \in V\}$, $B_w$ — vertices neither adjacent, nor opposite to $w$.

(h) $V = \mathbb{Z}_{16}$ arranged in a $4 \times 4$ array as shown in the picture, $\mathcal{D} = \{B_i\}_{i=0}^{15}$, where $B_i$ are the elements different from $i$, which share with $i$ either a row, or a column.

(i) $V$ — vertices of a toroidal graph in the picture, $\mathcal{D} = \{B_w : w \in V\}$, $B_w$ — vertices adjacent to $w$. 

\[ \begin{array}{cccc}
0 & 1 & 2 & 3 \\
4 & 5 & 6 & 7 \\
8 & 9 & 10 & 11 \\
12 & 13 & 14 & 15 \\
\end{array} \]
**Theorem (necessary conditions for parameters).** If $\mathcal{D}$ is a $(v,k,\lambda)$-design over $V$ and $|\mathcal{D}| = b$, then every element of $V$ belongs to $r$ blocks, where

$$\lambda(v-1) = r(k-1) \quad \text{and} \quad bk = vr.$$  

**Problem 2.** Let $|V| = v$ and $\mathcal{D} = \mathcal{P}_k(V)$, where $2 \leq k < v$. Prove that $\mathcal{D}$ is a $(v,k,\lambda)$-design and find the parameter $\lambda$. Do there exist other $(v,2,1)$-designs than $\mathcal{P}_2(V)$ for some $V$?

**Problem 3.** For $k \geq 2$ let $\lambda^*(k)$ be the least $\lambda$ such that the necessary conditions of existence of a $(v,k,\lambda)$-design are fulfilled for every $v > k$. Prove that

$$\lambda^*(k) = \begin{cases} \frac{1}{2}k(k-1) & \text{for } 2 \mid k; \\ k(k-1) & \text{for } 2 \nmid k. \end{cases}$$

**Problem 4.** Prove that (a) $(6,3,1)$-design; (b) $(19,4,1)$-design doesn’t exist.

**Problem 5.** Prove that the Fano plane cannot be embedded in the Euclidean plane, i.e. it cannot be drawn in such a way that all its lines are straight lines.

**Problem 6.** Consider the Set deck.

(a) To how many sets does one particular card belong?

(b) How many sets are there?

(c) How many sets of four different types are there (i.e. such that the cards have exactly $i$ common attributes for $i = 0, 1, 2, 3$)?

(d) During the game of Set 26 sets were taken and three cards remained on the table. Prove that they form a set.

(e) Two players use the Set deck in the following game. They take turns selecting one card from the deck and placing it on a table. The player whose move results in appearance of a set on the table loses. Who’s got the winning strategy?

(f) For as small $n \leq 81$ as you can, prove the following statement: Among any $n$ Set cards there are always three cards forming a set.

(g) Find an example of 9 red cards such that there is no set among them.

(h) Find an example of 20 cards such that there is no set among them.
**Problem 7.** Consider the Dobble incomplete (i.e. 55-card) deck.

(a) What is the common symbol of the two missing cards?

(b) What exactly are the two missing cards?

**Problem 8.** Let $V_n$ be the set of vertices of a regular $n$-gon ($n \geq 3$). Define

$$\mathcal{D}_{n,k} = \{ S \in \mathcal{P}_k(V_n) : S \text{ has an axe of symmetry} \}.$$ 

Take (a) $k = 3$; (b) $k = 4$. Find all $n$ with the property that $\mathcal{D}_{n,k}$ is a $(n,k,\lambda)$-design for some $\lambda$ and determine this parameter (as a function of $n$).

**Definition (Latin square).** An $n \times n$ array $L$ such that in every cell exactly one element of an $n$-element set $S$ is written is called a latin square over $S$ iff every element of $S$ appears exactly once in every row and every column of $L$. The element in $i$-th row and $j$-th column is denoted by $L(i,j)$.

**Problem 9.** Let $L$ be a latin square over set $S = \{1,2,3,4,5,6\}$. For $V = S^2$ and $(i,j) \in V$ define

$$B_{(i,j)} = \{(\ell,m) \in V \setminus \{(i,j)\} : \ell = i \text{ or } m = j \text{ or } L(\ell,m) = L(i,j)\}.$$ 

Prove that $\mathcal{D} = \{B_{(i,j)} : (i,j) \in V\}$ is a $(36,15,6)$-design.

**Problem 10.** Prove that for every $(v,k,1)$-design $\mathcal{D}$ holds $|\mathcal{D}| \geq v$.

**Definition (Isomorphism of designs).** We will say that designs $\mathcal{D}_1$, $\mathcal{D}_2$ over sets $V_1$, $V_2$, respectively, are isomorphic iff there exists a bijection $\phi : V_1 \rightarrow V_2$ such that

$$B \in \mathcal{D}_1 \iff \phi(B) := \{\phi(a) : a \in B\} \in \mathcal{D}_2.$$ 

This basically means that one can label elements of $V_2$ with elements of $V_1$ in such a way that the block structure is preserved.

**Problem 11.** Prove that there exists a unique (up to isomorphism)

(a) $(7,3,1)$-design,  (b) $(9,3,1)$-design,  (c) $(6,3,2)$-design,

(d) $(13,4,1)$-design,  (e) $(11,5,2)$-design,  (f) $(7,3,2)$-design.

**Problem 12.** Are any two designs described in **Problem 1.** isomorphic?

**Definition (Strongly regular graph).** A graph (simple, undirected) is called $(v,k,\lambda,\mu)$-strongly regular iff it has $v$ vertices, each of degree $k$, every two connected vertices have exactly $\lambda$ common neighbours and every two vertices which are not connected have exactly $\mu$ common neighbours.

**Problem 13.** Given is $(v,k,1)$-design $\mathcal{D}$. Consider a graph whose vertices are blocks of $\mathcal{D}$ and the edge $\{B,B'\}$ exists iff $B \cap B' = \emptyset$. Prove that this graph is $(v',k',\lambda,\mu)$-strongly regular and determine its parameters.
**Problem 14.**

(a) Prove that if a \((v, k, \lambda, \lambda)\)-strongly regular graph exists, then a \((v, k, \lambda)\)-design exists.

(b) Suppose there exists a \((2k^2 - k, k, 1)\)-design. Prove that there exists a \((4k^2 - 1, 2k^2, k^2)\)-design.

**Definition (Complementary design).** If \(D\) is a \((v, k, \lambda)\)-design, then

\[
\overline{D} := \{V \setminus B : B \in D\}
\]

is called the *complementary design* of \(D\).

**Problem 15.** Prove that \(\overline{D}\) is in fact a \((v, v - k, \overline{\lambda})\)-design and determine its parameter \(\overline{\lambda}\).

**Problem 16.** Is any of the designs described in Problem 1. isomorphic to the complementary design of another one?

**Definition \((t\text{-design})\).** Let \(V\) be a \(v\)-element set, \(t \leq k < v\), \(\lambda_t \geq 1\). Family \(D \subseteq \mathcal{P}_k(V)\) of \(k\)-element subsets of \(V\) is called a \(t\)-(\(v, k, \lambda_t\))-design, iff

\[
\forall A \in \mathcal{P}_t(V) \mid \{B \in D : A \subseteq B\} = \lambda_t,
\]

i.e. for every \(t\)-element subset of \(V\) there are exactly \(\lambda_t\) blocks containing it. In particular, 2-design is simply a design.

**Problem 17.** Prove that if \(t \leq k < v\), then there exists a \(t\)-(\(v, k, \lambda_t\))-design with \(\lambda_t = (v-t)_{k-t}\).

**Problem 18.** Is any design described in Problem 1. a 3-design?

**Problem 19.** Consider the set \(V\) of edges of \(K_7\) and family \(D\) of 5-element subsets of \(V\) consisting of: stars (5-tuples of edges having a common vertex), pentagons (cycles), sets of the form ‘\(\triangle = \)’ (triangle and two vertex-disjoint edges). Prove that \(D\) is a 3-(21, 5, 3)-design.

**Problem 20.**

(a) Prove that if \(D\) is a \(t\)-(\(v, k, \lambda_t\))-design, then it is also a \(s\)-(\(v, k, \lambda_s\))-design for every \(s \leq t\).

(b) From part (a) follows that to every \(t\)-(\(v, k, \lambda\))-design can be assigned a vector \((\lambda_i)_{i=0}^t\) such that \(\lambda_i\) is the number of blocks containing \(i\) fixed elements of \(V\). In particular \(\lambda_0 = b, \lambda_1 = r\). Prove that the complementary design \(\overline{D}\) is a \(t\)-(\(v, v - k, \overline{\lambda_t}\))-design with

\[
\overline{\lambda_t} = \sum_{i=0}^t (-1)^i \binom{t}{i} \lambda_i.
\]

□□□■ 25 ■□□■
PROBLEM 21. Prove that if a 3-(v, 6, 3)-design exists, then \( v \equiv 2 \pmod{20} \) or \( v \equiv 6 \pmod{20} \).

PROBLEM 22. Prove that if \( t-(v,k,1) \)-design exists, then \( v \geq (t+1)(k-t+1) \).

PROBLEM 23. Prove that for every \( n \geq 3 \) there exists a 3-(\( 2^n \), 4, 1)-design.

DEFINITION (DERIVED DESIGN). For fixed \( I \subseteq V \), \( |I| < t \) and \( \mathcal{D} \) — a \( t-(v,k,\lambda_t) \)-design, family
\[
\mathcal{D}_I := \{B \setminus I : I \subseteq B \in \mathcal{D}\}
\]
is called a **derived design** of \( \mathcal{D} \) with respect to \( I \).

PROBLEM 24. Prove that if \( |I| = i \), then \( \mathcal{D}_I \) is a \( (t-i)-(v-i,k-i,\lambda_i) \)-design.

PROBLEM 25. Let \( i + j \leq t \), \( I,J \in \mathcal{P}(V) \), \( I \cap J = \emptyset \), \( |I| = i \), \( |J| = j \) and \( \mathcal{D} \) be a \( t-(v,k,\lambda) \)-design over \( V \). Determine \( |\{B \in \mathcal{D} : I \subseteq B \subseteq V \setminus J\}| \).

PROBLEM 26. Let \( n \geq 2 \) be 1 or 3 modulo 6. Consider sets \( A \) — vertices of a regular \( 2n \)-gon, \( B \) — vertices and the center of a regular \( (2n-1) \)-gon, and families
\[
A = \{S \in \mathcal{P}_4(A) : S \text{ has an axe of symmetry}\}, \quad B = \{S \in \mathcal{P}_4(B) : S \text{ has an axe of symmetry}\}.
\]

(a) Prove that \( A \) and \( B \) are 3-(\( 2n,4,3 \))-designs.

(b) Are these designs isomorphic?

(c) Let \( a \in A \), \( b,c \in B \), where \( b \) is a vertex and \( c \) is the center of the \( (2n-1) \)-gon. Are any two of derived designs \( \mathcal{A}_{\{a\}}, \mathcal{B}_{\{b\}}, \mathcal{B}_{\{c\}} \) isomorphic?

DEFINITION (STEINER TRIPLE SYSTEM). Any \((v,3,1)\)-design \( \mathcal{D} \) is called a **Steiner triple system** and denoted \( \mathcal{D} =: \text{STS}_v \). We also consider a trivial design \( \text{STS}_3 \) (with one block and \( v = k \)).

PROBLEM 27. Prove that if \( \text{STS}_v \) exists, then \( v \equiv 1 \pmod{6} \) or \( v \equiv 3 \pmod{6} \).

THEOREM (KIRKMAN). If \( v \equiv 1 \pmod{6} \) or \( v \equiv 3 \pmod{6} \), then \( \text{STS}_v \) exists.

PROBLEM 28. Given \( \text{STS}_x \) and \( \text{STS}_y \), construct \( \text{STS}_{xy} \).

PROBLEM 29.

(a) Given \( \text{STS}_x \), construct \( \text{STS}_{2x+1} \).

(b) Provide a construction allowing to obtain \( \text{STS}_{15} \) defined in PROBLEM 1. (a) from the Fano plane.
**Problem 30.** Let $V$ be a set of perfect matchings in $K_6$ and $D$ — family of such triples of perfect matchings, which edgewise xor is isomorphic to $K_4 \oplus K_2$ or $K_{3,3}$. Prove that $D$ is isomorphic to STS$_{15}$ from Problem 1. (f).

Does there exist an isomorphism which comes down to selecting one of three edges in each matching?

**Theorem (Fisher’s inequality).** If there exists a $(v, k, \lambda)$-design, then $b \geq v$.

**Problem 31.** Prove that every two different blocks of a $(\frac{1}{2}k(k+1), k, 2)$-design have either exactly one, or exactly two common elements.

**Definition (symmetric design).** A design is called symmetric (square) iff $b = v$ or equivalently $k = r$. Number $n := k - \lambda > 0$ is called the order of the design. A symmetric design with $n = 1$ (i.e. $k = v - 1$ and $D = \mathcal{P}_{v-1}(V)$) is called trivial.

**Theorem (dual designs).** If $D$ is a symmetric $(v, k, \lambda)$-design over $V$, then

$$D^* := \{\{B \in D: a \in B\}: a \in V\}$$

is a symmetric $(v, k, \lambda)$-design over $D$.

**Problem 32.** Let $D$ be a $(v, k, \lambda)$-design and $B \in D$. Prove that

$$|\{B' \in D: B \cap B' \neq \emptyset, B \neq B'\}| \geq \frac{k(r-1)^2}{(k-1)(\lambda-1)+r-1}$$

and determine, when does the equality hold above.

**Problem 33.** Prove that if $D$ is a nontrivial symmetric $(v, k, \lambda)$-design, then its complement $\overline{D}$ is a $(v, v-k, v-2k+\lambda)$-design of the same order.

**Theorem (inequalities with $v$ and $n$ in symmetric designs).** If there exists a nontrivial symmetric $(v, k, \lambda)$-design of order $n$, then

$$4n - 1 \leq v \leq n^2 + n + 1.$$
**Definition (finite projective plane).** If \( n > 1 \), then \( (n^2 + n + 1, n + 1, 1) \)-design is called a finite projective plane of order \( n \). Blocks of this design are usually called lines and its elements — points.

**Definition (Hadamard design).** If \( n \geq 1 \), then \( (4n - 1, 2n - 1, n - 1) \)-design is called a Hadamard design of order \( n \).

**Theorem (extreme cases of symmetric designs).** If \( \mathcal{D} \) is a nontrivial symmetric \((v, k, \lambda)\)-design of order \( n \) and

(a) \( v = n^2 + n + 1 \), then either \( \mathcal{D} \), or \( \overline{\mathcal{D}} \) is a finite projective plane;

(b) \( v = 4n - 1 \), then either \( \mathcal{D} \), or \( \overline{\mathcal{D}} \) is a Hadamard design.

**Problem 34.** Prove that any symmetric design with \( \lambda = 1 \) is a projective plane.

**Problem 35.**

(a) Set \( M \) consists of \( m \) points of finite projective plane of order \( n \), no three of which are collinear. Prove that \( m \leq n + 2 \) for \( 2 \mid n \) and \( m \leq n + 1 \) for \( 2 \not\mid n \).

(b) Suppose that \( m = n + 1 \) and \( 2 \mid n \). Prove that all lines intersecting \( M \) in exactly one point have a common point.

**Problem 36.** The points of finite projective plane \( \mathcal{D} \) over \( V \) are coloured with four colours in such a way that every colour is used at least once. Prove that there exist a quadruple \( \{x, y, z, t\} \subseteq V \) of points in four different colours and \( B \in \mathcal{D} \) such that \( \{x, y, z\} \subseteq B \), \( t \notin B \).

**Definition (resolvable design).** Design \( \mathcal{D} \) over \( V \) is called resolvable, if all of its blocks can be grouped into families \( R_j = \{B_{j_i}\}_{i \in I} \subseteq \mathcal{D} \) of mutually disjoint blocks such that for every \( j \)

\[
\bigcup_{i \in I} B_{j_i} = V.
\]

Each such family is called a parallelity class.

**Problem 37.** Prove that if a \((v, k, 1)\)-design is resolvable, then \( b \geq v + r - 1 \).

**Problem 38.** Prove that a resolvable \((v, 2, 1)\)-design exists iff \( v \) is even and \( v \geq 4 \).

**Problem 39.** Prove that the design from Problem 1. (a) is resolvable.
Problem 40.

(a) Prove that every \((n^2,n,1)\)-design is resolvable.

(b) Prove that a \((n^2,n,1)\)-design exists iff a projective plane of order \(n\) exists.

Problem 41. Prove that if \(p\) is prime, then a \((p^2,p,1)\)-design exists.

Problem 42. Construct a Hadamard design of order 9.

Problem 43. Prove that if \(D\) is a Hadamard design of order \(n\) over \(V\), then
\[
\mathcal{E} = \{V \setminus B : B \in D\} \cup \{B \cup \{\infty\} : B \in D\}
\]
is a 3-(4n,2n,n−1)-design over \(V \cup \{\infty\}\).

Problem 44. Prove that every resolvable \((2k,k,\lambda)\)-design is a 3-(2k,k,\lambda_3)-design and determine its parameter \(\lambda_3\).

Problem 45. Let \(D\) be a 3-(v,k,\lambda_3)-design with the property that \(D\{p\}\) for some \(p \in V\) is a symmetric design. Prove that \(v = 2k\) or \((\lambda_3 + 1)(\lambda_3 + 2) \in \{k,k/2\}\).

The rest of the handout is for those familiar with the basics of linear algebra.

**Definition (Incidence Matrix).** Given a design \(D\) a binary matrix \(A \in \mathcal{M}^{b \times v}(\mathbb{R})\) such that
\[
a_{ij} = \begin{cases} 
1 & \text{the } j\text{-th element belongs to the } i\text{-th block} \\
0 & \text{otherwise}
\end{cases}
\]
is called an incidence matrix of \(D\).

Problem 47. Let \(I = \text{id}_{v \times v}, J = [1]_{v \times v}\) and \(A\) — incidence matrix of a \((v,k,\lambda)\)-design. Prove that \(A^T A = (r-\lambda)I + \lambda J\).


Problem 49. Restate dual designs theorem using the notion of incidence matrices, and prove it using methods of linear algebra.

**Definition (Hadamard Matrix).** Matrix \(H \in \mathcal{M}^{n \times n}(\mathbb{R})\) is called a Hadamard matrix of order \(n\), iff \(|h_{ij}| = 1\) and the columns of \(H\) are mutually orthogonal.

Problem 50.

(a) Prove that if \(H\) is a Hadamard matrix of order \(n\) and \(n > 2\), then \(4 \mid n\).

(b) Prove that a Hadamard matrix of order \(4m\) exists iff a Hadamard design of order \(m\) exists.
Cubic Curves and Intersections

Mark Krusemeyer

1. For an algebraic curve \( f(x,y) = 0 \) of degree \( d \) (that is, the polynomial \( f(x,y) \) has degree \( d \)), how many coefficients are there?

(For example, for \( d = 2 \) we have a conic section

\[
c_1 x^2 + c_2 xy + c_3 y^2 + c_4 x + c_5 y + c_6 = 0
\]

and there are six coefficients \( c_1, c_2, \ldots, c_6 \).)

Algebraic definition of the projective plane

Points: Lines through the origin in 3-space.

The line through \((0,0,0)\) and \((X,Y,Z)\) is \([X,Y,Z]\), so \([\lambda X, \lambda Y, \lambda Z] = [X,Y,Z] \) for \( \lambda \neq 0 \).

If \( Z = 0 \) is the line at infinity (usual choice), then points with \( Z \neq 0 \): \([X,Y,Z] = [X/Z, Y/Z, 1] = (x,y) \) \((x = X/Z, y = Y/Z)\) correspond to points “at finite distance” (in the ordinary plane).

Equation of a curve \((d = \text{degree of } f)\):

\[
f(x,y) = 0 \rightarrow f(X/Z, Y/Z) = 0 \rightarrow Z^d f(X/Z, Y/Z) = 0
\]

homogeneous polynomial \( F(X,Y,Z) \)

Example (from class):

\[
y - x^3 = 0 \rightarrow Y Z^2 - X^3 = 0
\]

“homogeneous equation” for the curve.

2. Consider a circle \((x-a)^2 + (y-b)^2 = r^2\).

a) Find the homogeneous equation for the circle.

b) Show that, unsurprisingly, there are no real points at infinity (with \( Z = 0 \)).

c) Find the complex points at infinity. How many are there? Note that they are the same for every circle; they are called the circular points in the complex projective plane.

d) Suppose you have two concentric circles. Bézout’s Theorem suggests that they should intersect in four points. However, they don’t intersect anywhere at finite distance (why?). So what’s going on?

3. (Make friends with one cubic curve.)

Sketch the curve \( xy^2 + x^2y - xy - 1 = 0 \).

(If necessary, see hint below).

\( \text{Hint: Solve for } y \text{ in terms of } x, \text{ and look at what happens when } x \rightarrow \pm \infty \) and when \( x \rightarrow 0 \). You could, of course, also use technology; that could show you very quickly what the curve looks like, but not why.)
4. (Exploring intersections.) For each of the following pairs of curves,

i) state how many intersection points Bézout’s theorem tells you they should have;

ii) find their actual points of intersection that have real coordinates;

iii) if there is a discrepancy between your answers from parts i) and ii), account for it as best you can. (You may not be able to give complete proofs; in general, defining and computing multiplicities of intersections is hard.)

a) \( xy = 4, \ x^2 + y^2 = 17 \) (that is, \( xy - 4 = 0, \ x^2 + y^2 - 17 = 0 \))

b) \( xy = 4, \ x^2 + y^2 = 8 \)

c) \( x = y^2, \ y = x^2 \)

d) \( y = x^2, \ y = 2 - x^2 \)

e) \( y = x^2, \ y = x^2 + 1 \)

f) \( y = x^2, \ y = x^3 \)

5. (Only recommended if you’re very comfortable with partial derivatives and the multivariable chain rule; otherwise, ignore this problem.)

Show that at a point along the curve \( f(x,y) = 0 \) so that \( y \) is a function of \( x \) near that point, the curve can have a point of inflection (where \( \frac{d^2y}{dx^2} \) changes sign) only if

\[
\frac{\partial^2 f}{\partial x^2} \left( \frac{\partial f}{\partial y} \right)^2 - \frac{\partial^2 f}{\partial y \partial x} \cdot \frac{\partial f}{\partial x} \cdot \frac{\partial f}{\partial y} - \frac{\partial^2 f}{\partial x \partial y} \cdot \frac{\partial f}{\partial y} \cdot \frac{\partial f}{\partial x} + \left( \frac{\partial f}{\partial x} \right)^2 \frac{\partial^2 f}{\partial y^2} = 0.
\]

For the following problems, feel free to use

- Bézout’s theorem (the “weak” version should be enough)

- A fact from linear algebra: Any homogeneous system of \( m \) linear equations in \( n \) unknowns for which \( m < n \) has infinitely many solutions. (“Homogeneous” means the system has the form

\[
\begin{align*}
\alpha_{11}x_1 + \cdots + \alpha_{1n}x_n &= 0 \\
&\vdots \\
\alpha_{m1}x_1 + \cdots + \alpha_{mn}x_n &= 0,
\end{align*}
\]

with zeros on the right-hand side.)

6.

a) Show that through any five distinct points \( P_1, P_2, \ldots, P_5 \) in the plane, there is some conic section. (See hint below if you’re stuck.)
b) Show that the conic section from part a) is unique unless (at least) four of the five points lie on the same line. What happens in that special case? (See hint below.)

Hint: Consider linear equations that you can get from the points, and don’t scale them. Use Bézout’s theorem.

7. Show that an irreducible algebraic curve of degree 4 can have at most 3 singular points. (See hint below.)

Hint: Suppose there were 4 singular points, and somehow use problem 6.

8. Find, with proof, the maximum possible number of singular points on an irreducible algebraic curve of degree $d$. (From class and from problem 7, we know the answer is 0 for $d \leq 2$, 1 for $d = 3$, 3 for $d = 4$.)

9.

a) Show that for a cubic curve $C$ with a singular point $P$, every line through $P$ meets (intersects) $C$ in at most one other point (besides $P$).

b) Now let $C$ be the curve $y^2 = x^3$ and $P$ be the singular point (cusp) at the origin. Let $t$ be a parameter, and consider the line through $P$ with slope $\frac{1}{t}$. Where (besides the origin) does this line meet the curve $C$? What happens if $t = 0$?

c) Still for the curve $y^2 = x^3$, let $Q_1$, $Q_2$ be the points associated with the parameter values $t_1$, $t_2$ (as in part b)), with $t_1 \neq t_2$, and let $\ell$ be the line through $Q_1$ and $Q_2$. By Bézout’s Theorem, $\ell$ should intersect $C$ in a third point, $Q_3$. Find the parameter value $t_3$ that corresponds to the point $Q_3$. (Your answer will be a function of $t_1$ and $t_2$. See hint below.)

d) Show that the set of all nonsingular points on the curve $y^2 = x^3$ is a group under “addition” $\oplus$, where the operation is defined as follows: Given two points $Q_1$, $Q_2$, with $Q_1 \neq Q_2$ for now, connect them by a straight line, and (as in part c)) find the third point of intersection of that line with the curve. Then reflect that third point $Q_3$ across the $x$-axis to get the “sum” $Q_1 \oplus Q_2$ of the points $Q_1$, $Q_2$. (If you’ve never seen groups, don’t worry about this problem — or ask somebody.) What is the identity element of this group? What is the “additive inverse” $-Q$ of a point $Q$? And how should you “add” a point to itself, that is, how do you find $Q \oplus Q$?

Hint: Expect a slightly messy calculation, but Vieta’s formulas can help.

10. Recall the Cayley-Bacharach theorem: If two cubic curves $C_1$, $C_2$ meet in (exactly) nine distinct points $P_1, \ldots, P_9$, and if a third cubic curve $C$ goes through eight of these points, then $C$ also goes through the ninth point. Use this theorem to prove Pascal’s hexagon theorem: If $A_1$, $A_2$, $A_3$, $B_1$, $B_2$, $B_3$ are distinct points on a (nondegenerate = irreducible) conic section, and if $P$, $Q$, $R$ are the intersection points of $A_1B_2$, $A_2B_1$; $A_1B_3$, $A_3B_1$; $A_2B_3$, $A_3B_2$ respectively, then $P$, $Q$, $R$ are collinear.
Well orders

**Definition 1.** Let $X$ be a set or a class. We say that a relation $\prec$ on $X$ is a **well-order** if it satisfies the following conditions:

1. If $x \prec y$ and $y \prec z$ then $x \prec z$.
2. For every $x, y$ exactly one of the following is true: $x \prec y$, $y \prec x$, $x = y$.
3. Every non-empty $S \subseteq X$ has the least element.

**Exercise.** Prove that (3) is equivalent to the following condition:

There do not exist $x_0, x_1, x_2, x_3, \ldots \in X$ with $x_{n+1} \prec x_n$ for every integer $n$. In other words, there are no infinite decreasing sequences.

**Example.** The following relations are well-orders:

- The empty relation on the empty set.
- Any linear order on any finite set.
- The relation $<$ on $\mathbb{N}$.
- The relation $<$ on $\{\frac{n}{n+1} : n \in \mathbb{N}\} \cup \{1\}$.
- The relation $<$ on $\{m + \frac{n}{n+1} : m, n \in \mathbb{N}\}$.

**Nonexample.** The following relations are not well-orders:

- The relation $<$ on $\mathbb{Z}$.
- The relation $<$ on the interval $[0, 1]$.
- The relation $>$ on $\mathbb{N}$

Ordinal numbers

**Definition 2.** We say that a set $\alpha$ is an **ordinal number** (or simply: **ordinal**) if the following conditions hold:

1. If $\beta \in \alpha$ then $\beta \subset \alpha$.
2. The relation of membership (that is: $\in$) is a well-order on $\alpha$. 
The class of all ordinal numbers is denoted by \( \text{Ord} \). (Some authors use other notations such as ON or On.)

**Fact 3.** The following statements are true:

1. There exist ordinal numbers (e.g. \( \emptyset \) is an ordinal).
2. If \( \alpha \in \text{Ord} \) then \( \alpha \cup \{\alpha\} \in \text{Ord} \).
3. If \( \alpha \in \text{Ord} \) then \( \alpha \notin \alpha \).
4. If \( \alpha, \beta \in \text{Ord} \) then exactly one of the following is true: \( \alpha = \beta \), \( \alpha \in \beta \), \( \beta \in \alpha \).
5. The relation \( \in \) is a well order on \( \text{Ord} \). If \( \alpha, \beta \in \text{Ord} \) and \( \alpha \in \beta \) then we write \( \alpha < \beta \).
6. If \( \alpha \in \text{Ord} \) then \( \alpha = \{ \beta \in \text{Ord} : \beta < \alpha \} \)

We identify the ordinal number \( \emptyset \) with the integer number 0.

If \( \alpha \in \text{Ord} \) then the ordinal \( \alpha \cup \{\alpha\} \) is called a *successor* of \( \alpha \) and is denoted by \( \alpha + 1 \). A (non-zero) ordinal which is not a successor is called a *limit* ordinal.

So, with the identification \( \emptyset \equiv 0 \) we have:

\[
\begin{align*}
\{\emptyset\} &= \{0\} = 0 + 1 \overset{\text{def}}{=} 1 \\
\{\emptyset, \{\emptyset\}\} &= \{0, 1\} = 1 + 1 \overset{\text{def}}{=} 2 \\
\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} &= \{0, 1, 2\} = 2 + 1 \overset{\text{def}}{=} 3 \\
\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}\} &= \{0, 1, 2, 3\} = 3 + 1 \overset{\text{def}}{=} 4
\end{align*}
\]

and so on.

The smallest infinite ordinal is denoted by \( \omega \) and is equal to \( \{0, 1, 2, 3, \ldots\} \). Thus one can think of \( \omega \) as the set of all natural numbers.

The smallest uncountable ordinal is denoted by \( \omega_1 \).

**Transfinite induction**

**Theorem 4** (Transfinite induction theorem). Let \( \alpha \) be an ordinal. Let \( P(\xi) \) be some statement depending on an ordinal \( \xi \). If for every \( \beta \leq \alpha \) the following implication holds:

\[
(\forall \gamma < \beta \ P(\gamma)) \implies P(\beta)
\]

then the statement \( P(\alpha) \) is true.

This is a generalization of the mathematical induction known from school. To see it, one has to take \( \alpha = \omega \).
**Definition 5.** Let $\alpha \in \text{Ord}$. A transfinite sequence of length $\alpha$ is any collection $(x_\beta)_{\beta<\alpha}$ of some objects indexed by the ordinals smaller than $\alpha$.

This generalizes the notion of a sequence known from school. If $\alpha$ is equal to some integer $n$, we get a definition of an $n$-element sequence. Taking $\alpha = \omega$, we get an ordinary infinite sequence.

Let us formulate the next theorem in an informal way.

**Theorem 6** (Transfinite recursion theorem). One can define transfinite sequences recursively.

The meaning of this is the following. Suppose we want to construct a transfinite sequence $(x_\beta)_{\beta<\alpha}$. For every $\beta < \alpha$ we can define $x_\beta$ provided that we already defined $x_\gamma$ for every $\gamma < \beta$. Transfinite recursion theorem says that this procedure yields a valid definition of a transfinite sequence $(x_\beta)_{\beta<\alpha}$.

---

**Cardinal numbers**

**Fact 7.** If $\prec$ is a well-order on a set $X$ then there exists an ordinal $\alpha$ such that $\prec$ is isomorphic to the well-order $<$ on $\alpha = \{\beta : \beta < \alpha\}$. We say that $\alpha$ is the order type of $\prec$.

**Theorem 8** (Zermelo). Every set can be well-ordered.

We denote by $|X|$ the smallest ordinal number $\alpha$ such that there is a bijection $f : X \to \alpha$. $|X|$ is called the cardinality of $X$. We refer to cardinalities as cardinal numbers. Also note that for every ordinal $\beta < |X|$ one has $|\beta| < |X|$.

**Corollary 9.** For every set $X$ there is a well order on $X$ of order type $|X|$. Thus, $X$ can be written in the form

$$X = \{x_\alpha : \alpha < |X|\}.$$ 

The class of cardinal numbers is denoted by $\text{Card}$. It turns out that the class of infinite cardinal numbers can be well-ordered: there is an order-preserving bijection

$$\text{Ord} \ni \alpha \mapsto \aleph_\alpha \in \text{Card} \setminus \{0, 1, 2, \ldots\}.$$

Thus $\aleph_0$ is the cardinality of any infinite countable set. The smallest uncountable cardinal is $\aleph_1$.

**Fact 10.** Let $X$ and $Y$ be non-empty sets. Then the following conditions are equivalent:

- There exists an injection $f : X \to Y$
- There exists a surjection $g : Y \to X$

**Theorem 11** (Cantor-Bernstein-Schröder). If $|X| \leq |Y|$ and $|Y| \leq |X|$ then $|X| = |Y|$.

We define addition, multiplication and exponentation of cardinal numbers as follows:

$$|X| + |Y| = |(X \times \{0\}) \cup (Y \times \{1\})|,$$

$$|X| \cdot |Y| = |X \times Y|,$$

$$|X|^{|Y|} = |X^Y|.$$ 

Here, $X^Y$ denotes the set of all functions from $Y$ to $X$. 

---

□□■□ 35 □□■□
Question. Why didn’t we simply define $|X| + |Y| = |X \cup Y|$?

Theorem 12 (Hessenberg). If $\kappa$ is an infinite cardinal then $\kappa \cdot \kappa = \kappa$.

Corollary 13. If $\kappa, \lambda$ are infinite cardinals then $\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$.

Theorem 14 (Cantor). One has $\kappa < 2^\kappa$ for every cardinal $\kappa$.

We denote $\mathfrak{c} = 2^{\aleph_0}$.

Problems

Problem 1. Prove that there exists a set $A \subset \mathbb{R}^2$ such that for every line $\ell \subset \mathbb{R}^2$ we have $|A \cap \ell| = 2$.

Problem 2. Prove that there exists a decomposition of $\mathbb{R}^3$ into disjoint unit circles.

Problem 3. Prove that every function $f: \mathbb{R} \to \mathbb{R}$ is the sum of two injective functions.

Problem 4. Prove that there exists a function $f: \mathbb{R} \to \mathbb{R}$ such that the image of every interval $(a, b) \subset \mathbb{R}$ is $\mathbb{R}$.

Problem 5. Let $\mathcal{F}$ be a family of subsets of $\mathbb{R}$ such that $|\mathcal{F}| = \mathfrak{c}$ and $|F| = \mathfrak{c}$ for every $F \in \mathcal{F}$. Prove that there exists a family $\mathcal{G} = \{G_F : F \in \mathcal{F}\}$ such that the following conditions hold:

1. For every $F \in \mathcal{F}$ the set $G_F$ is a subset of $F$.
2. For every $F \in \mathcal{F}$ we have $|G_F| = \mathfrak{c}$.
3. For every $F \in \mathcal{F}$ we have $|F \setminus G_F| = \mathfrak{c}$.
4. The sets $G_F$ are pairwise disjoint.

Problem 6. Prove that there exists a set $A \subset \mathbb{R}$ such that every $x \in \mathbb{R}$ has unique representation $x = a + b$ with $a < b$ and $a, b \in A$.

Problem 7. Prove that there exists a set $B \subset \mathbb{R}$ such that for every uncountable closed set $A \subset \mathbb{R}$ the sets $A \setminus B$, $B \cap A$ are non-empty.

Problem 8. Prove that there exists a set $A \subset \mathbb{R}^2$ with the following property: for every positive real number $x$ there exists a unique segment $PQ$ of length $x$ whose endpoints $P$ and $Q$ lie in $A$.

Problem 9. Suppose that every line $\ell \subset \mathbb{R}^2$ is labelled with some cardinal number $\kappa_\ell$ with $2 \leq \kappa_\ell \leq \mathfrak{c}$. Prove that there exists a set $A$ such that for every line $\ell$ we have $|A \cap \ell| = \kappa_\ell$.

Problem 10. Prove that there exists a transfinite sequence $(A_\alpha)_{\alpha < \omega_1}$ of subsets of $\mathbb{N}$ such that for every $\alpha < \beta < \omega_1$ the set $A_\alpha \setminus A_\beta$ is infinite and the set $A_\beta \setminus A_\alpha$ is finite.
Introduction to Graphs and Graph Coloring
Gábor Damásdi

All graphs are simple in these problems. (No parallel edges or loops.)

Introductory problems

1. Solve the following sodoku.

2. Given $n$ lines in the plane, such that no three of them are concurrent. We want to color the intersections such that if two intersections are neighbours along a line, then they have different colors. Show that such coloring always exists using three colors.

3. The owner of a hotel receives the bookings for the year in a big table. Every row of the table belongs to a guest and contains which days are booked by the guest. One booking is always a continuous set of days. The owner would like to use as few rooms as possible during the year. Gave a simple algorithm to calculate how many rooms are needed.

4. Suppose you have an art gallery containing priceless paintings and sculptures. You would like it to be supervised by security guards, and you want to employ enough of them so that at any one time the guards can between them oversee the whole gallery. How many guards will you need? Suppose the gallery is a simple polygon on $n$ vertices. Show that $\left\lfloor \frac{n}{3} \right\rfloor$ guard is always sufficient.

5. Suppose you are a teacher and you are creating some tests for your students. You know that if two students are friends they will try to cheat during the exam, so you need to give them different tests. What is the minimal number of tests you need to prepare if these are the friendships in your class: $(A,D), (A,E), (A,I), (B,C), (B,E), (B,G), (C,D), (C,F), (D,J), (E,H), (F,I), (F,H), (G,I), (G,J), (H,J)$.

Coloring problems

1. Finish the coloring of the following graph.

2. Prove that $\chi(K_n) = n$. Show that $\chi(C_k)$ is 2 if $k$ is even and it is 3 otherwise.
3. Let $G = (V, E)$ be a simple connected graph where every degree is at most $k$. Prove that $G$ is $k+1$-colorable. Prove that deleting a vertex of $G$ makes it $k$ colorable.

4. What are the chromatic numbers of the following graphs?

5. Calculate the chromatic number of the following graphs.

(a) The vertices of the graph is the numbers 1,2,...,100. We connect $i$ and $j$ if one divides the other.

(b) The vertices of the graph is the numbers 1,2,...,100. We connect $i$ and $j$ if they are relative primes.

6. Consider the infinite graph $G$ defined as follows. The vertex set is $\mathbb{R}^2$. Two points in $\mathbb{R}^2$ are adjacent if their Euclidean distance is 1. Show that $4 \leq \chi(G) \leq 7$.

7. The vertices of the $(n,k)$-Kneser graph are the $k$-element subsets of $\{1,2,\ldots,n\}$. Two subset is connected by and edge if they are disjoint. Prove that the chromatic number of the $(n,k)$-Kneser graph is at most $n-2k+2$.

8. Consider a set $S$ of great circles on a sphere with no three circles meeting at a point. The arrangement graph of $S$ has a vertex for each intersection point, and an edge for each arc directly connecting two intersection points. Prove an upper bound on the chromatic number of this graph, as small as you can.

9. Let $G$ is a triangulated polygon if it is obtained by taking a polygon in the plane and adding inner diagonals until every region becomes a triangle. Show that if $G$ is a triangulated polygon then $\chi(G) \leq 3$. 
10. (Brooks) Let $G$ be a connected graph, then $\chi(G) \leq \Delta(G)$, unless $G$ is a complete graph or an odd cycle.

**Properties of coloring**

1. Prove that a graph is bipartite if and only if it does not contain an odd cycle.

2. Show that every graph $G$ has a vertex ordering with respect to which the greedy coloring uses $\chi(G)$ colors.

3. Show a graph with chromatic number $\infty$ that has finite degrees.

4. Show that $\chi(G)\chi(\overline{G}) \geq n$

5. Show that $\chi(G) + \chi(\overline{G}) \leq n + 1$

6. Prove that $\chi(G) \geq w(G)$ and $\chi(G) \geq \frac{|V|}{\alpha(G)}$

7. Let $G$ be a graph. Is it true that there is a proper coloring of $G$ such that one of the color classes contains exactly $\alpha(G)$ points?

8. Show that $\chi(G \times H) \leq \min(\chi(G), \chi(H))$

9. Show that $\chi(G \Box H) = \max(\chi(G), \chi(H))$

10. Show that interval graphs are prefect. Show that chordal graphs are perfect.

11. Let $G$ be a graph where every two odd cycles have at least a vertex in common. Prove that $\chi(G) \leq 5$. 

□□■□  39  □■■■
Coloring maps, the four color theorem

1. How many colors are needed for the following map?

2. Prove that the edges and vertices of a polyhedron form a planar graph.

3. In any graph, the sum of the degrees of the vertices is equal to twice the number of edges.

4. In any planar graph, the sum of the degrees of the faces is equal to twice the number of edges.

5. In any connected planar graph with $V$ vertices, $E$ edges, and $F$ faces we have $V - E + F = 2$.

6. Let $G$ be a connected planar graph with $V \geq 3$. Then $E \leq 3(V - 2)$.

7. Let $G$ be a connected planar graph. Then $G$ has at least one vertex of degree 5 or less.

8. Let $G = (V, E)$ be a planar graph. Prove that $G$ is 6 colorable.

9. Let $G = (V, E)$ be a planar graph. Prove that $G$ is 5 colorable.

Contact: gabor.damasdi@gmail.com
1 Introduction, basic probability

As you can see, these handouts are "course-styled" and they contain only the theory being taught, to help you catch up with the lecture. The space to have it all clearly explained, proved, or demonstrated with problems will be at the lecture. The definitions may look scary, however, we will not spend a lot of time with them. Our goal is to understand and demonstrate the Central Limit Theorem, one of the greatest practical achievements of mathematics in general.

**Definition 1.1** (Probability space). Consider nonempty set $\Omega$ and some subset of $2^\Omega$ $\mathcal{F}$ (more precisely, a $\sigma$-algebra on $\Omega$). Let $P: \mathcal{F} \to [0,1]$ be mappings such that

1. $P(\Omega) = 1$
2. For any pairwise disjoint $A_1, A_2, \ldots \in \mathcal{F}$ it holds

\[ P\left( \bigcup_{i=1}^{\infty} A_i \right) = \sum_{i=1}^{\infty} P(A_i). \]

Then $P$ is called *probability measure* on $\mathcal{F}$. The triple $(\Omega, \mathcal{F}, P)$ is called *probability space*.

This definition is rather cryptic, but it is not that far from our intuitive actual understanding of probability.

**Definition 1.2** (Example - discrete probability space). Let $\Omega$ be nonempty finite or countable set. Let $\mathcal{F} = 2^\Omega$ and consider for each $\omega \in \Omega$ value $p_\omega$ such that

\[ \forall \omega \ p_\omega \geq 0, \text{ and } \sum_{\omega \in \Omega} p_\omega = 1. \]

Define

\[ P(A) = \sum_{\omega \in A} p_\omega \text{ for any } A \in \mathcal{F}. \]

Then $(\Omega, \mathcal{F}, P)$ is *discrete probability space*.

**Theorem 1.1** (Intuitive probability space properties). Let $(\Omega, \mathcal{F}, P)$ be a probability space. Then

1. $P(\emptyset) = 0$.
2. For any $A \in \mathcal{F}$ it holds $P(\Omega \setminus A) = 1 - P(A)$.
3. For any $A, B \in \mathcal{F}$ it holds $A \subset B \Rightarrow P(A) \leq P(B)$ and $P(B \setminus A) = P(B) - P(A)$.

**Definition 1.3** (Conditional probability). Consider $(\Omega, \mathcal{F}, P)$. Let $B \in \mathcal{F}$ be random event such that $P(B) > 0$. Then

\[ P(A|B) = \frac{P(A \cap B)}{P(B)} \]

is called *conditional probability of $A$ given $B$*. 

□□■□ 41  ■□□■
**Definition 1.4** (Independence). Random events $A, B$ are *independent* if $P(A \cap B) = P(A)P(B)$.

**Theorem 1.2** (Gradual conditioning). Let $E_1, E_2, \ldots, E_n$ be random events such that $P(E_1 \cap \cdots \cap E_{n-1}) > 0$. Then

$$P(E_1 \cap E_2 \cap \cdots \cap E_n) = P(E_n|E_1 \cap \cdots \cap E_{n-1})P(E_{n-1}|E_1 \cap \cdots \cap E_{n-2}) \cdots P(E_2|E_1)P(E_1).$$

**Theorem 1.3** (Inclusion and exclusion). Let $A_1, A_2, \ldots, A_n$ be random events. Then

$$P\left(\bigcap_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} P(A_i) - \sum_{1 \leq i < j \leq n} P(A_i \cap A_j) + \sum_{1 \leq i < j < k \leq n} P(A_i \cap A_j \cap A_k) - \cdots + (-1)^{n-1}P\left(\bigcap_{i=1}^{n} A_i\right).$$

**Theorem 1.4** (Total probability). Let $A_1, A_2, \ldots$ be disjoint decomposition of $\Omega$. Then for any random event $B$

$$P(B) = \sum_{i} P(B|A_i)P(A_i).$$

**Theorem 1.5** (Bonferroni inequality). Let $A_1, A_2, \ldots, A_n$ be random events. Prove that

$$P\left(\bigcap_{i=1}^{n} A_i\right) \geq 1 - \sum_{i=1}^{n} (1 - P(A_i)).$$

2 Random variables and well-known distributions

A random variable is a variable whose possible values are outcomes of a random phenomenon. Concerning the definition, it’s basically "anything we can think of", as long as it is built on top of a probability space.

**Definition 2.1** (Random variable). Let $(\Omega, \mathcal{F}, P)$ be a probability space. Function $X : \Omega \to \mathbb{R}$ is called *random variable* if $\{\omega \in \Omega ; X(\omega) \leq a\} \in \mathcal{F}$ for all $a \in \mathbb{R}$.

**Definition 2.2** (Distribution of r.v.). Probability measure $P_X$ defined on $\mathbb{R}$ by

$$P_X((-\infty, a]) = P(\{\omega ; X(\omega) \leq a\})$$

is called *distribution of random variable* $X$.

**Definition 2.3** (Distribution function and density). Let $P_X$ be a distribution of discrete random variable $X$. Function

$$F_X(x) = P_X((-\infty, x]) = P[X \leq x]$$

is called *distribution function* of r.v. $X$. Function

$$f_X(x) = P_X(\{x\}) = P[X = x]$$

is called *density with respect to the arithmetic measure of discrete r.v. $X$*.

**Example 1.** Consider fair six-sided dice. Throw the dice two times independently. Then we may choose the probability space as $\Omega = \{(i, j); i = 1, \ldots, 6, j = 1, \ldots, 6\}$, $\mathcal{F} = 2^\Omega$ and $P(i, j) = 1/36$ for all $(i, j) \in \Omega$. Random variable $X(i, j) = i + j$ describes the sum of the two results. The distribution $P_X$ of $X$ is a probability measure on set $\{2, 3, \ldots, 12\}$.
Both distribution function and density uniquely determine the distribution of a random variable.

**Bernoulli (alternative) distribution** Let \( p \in (0,1) \). Distribution given by

\[
p_0 = 1 - p, \quad p_1 = p
\]

is called alternative, or Bernoulli distribution. Corresponding random variable is two-valued. \( X = 1 \) denotes success and \( X = 0 \) denotes failure in the experiment. Such experiment (with success or failure outcome with success probability \( p \)) is called Bernoulli trial.

**Binomial distribution** Let \( n > 0, \ n \in \mathbb{N}, \) and \( p \in (0,1) \). Distribution on the set \( \{0,1,\ldots,n\} \) given by

\[
p_i = \binom{n}{i} p^i (1-p)^{n-i}
\]

is called binomial with parameters \( n \) and \( p \). Binomial distribution is the distribution of number of successes in \( n \) independent Bernoulli trials.

**Geometric distribution** Let \( p \in (0,1) \). Distribution on the set \( \{0,1,\ldots\} \) given by

\[
p_i = p (1-p)^i
\]

is called geometric distribution with parameter \( p \). Geometric distribution is the distribution of number of failures preceding the first success in a series of independent Bernoulli trials.

**Uniform distribution** Let \(-\infty < a < b < \infty \). Random variable \( X \) has uniform distribution on the interval \((a,b)\) if the density \( f_X \) is constant on \((a,b)\) and zero elsewhere.

\[
f_X(x) = \begin{cases} 
\frac{1}{b-a} & \text{for } x \in (a,b), \\
0 & \text{elsewhere}. 
\end{cases}
\]

**Exponential distribution** Let \( \mu > 0 \). Random variable \( X \) has exponential distribution with parameter \( EX = \mu \) if it has density

\[
f_X(x) = \begin{cases} 
\frac{1}{\mu} \exp\left(-\frac{x}{\mu}\right) & \text{for } x > 0, \\
0 & \text{elsewhere}.
\end{cases}
\]

**Definition 2.4** (Mean value of random variable (general)). Let \( X \) be random variable defined on probability space \((\Omega,\mathcal{F},P)\). The mean value (or expected value) of \( X \) is defined as

\[
EX = \int_{\Omega} X(\omega) P(\omega)
\]

if the integral on the right hand side exists.

**Theorem 2.1** (Jensen’s inequality). Let \( X \) be a random variable and \( f \) be a convex function. If both \( EX \) and \( Ef(X) \) exist then

\[
f(\mathbb{E}X) \leq \mathbb{E}f(X)
\]
3 Estimates

Behold the most important distribution in statistics. The reason is that it connects mathematics with nature.

**Normal (Gaussian) distribution** Let $\mu \in \mathbb{R}$, and $\sigma^2 > 0$. Random variable $X$ has normal distribution (also called Gaussian distribution) if its density has form

$$f_X(x) = \frac{1}{\left(2\pi \sigma^2\right)^{1/2}} \exp\left(-\frac{(x - \mu)^2}{2\sigma^2}\right), \quad x \in \mathbb{R}.$$ 

For $X$ it holds $EX = \mu$ and $\text{var} \ X = \sigma^2$.

**Definition 3.1** ((Random) sample). A sequence $X_1, X_2, \ldots, X_n$ of independent and identically distributed (iid) random variables is called a sample of size $n$ (from distribution $P_X$).

**Definition 3.2** (Sample moments). Let $X_1, \ldots, X_n$ be a random sample. Then

1. $\overline{X}_n = \frac{1}{n} \sum_{i=1}^{n} X_i$ is called sample mean.
2. $S_n^2 = \frac{1}{n-1} \sum_{i=1}^{n} (X_i - \overline{X}_n)^2$ is called sample variance.
3. $\hat{F}_n(x) = \frac{1}{n} \sum_{i=1}^{n} \chi(X_i \leq x)$, where $\chi(\cdot)$ is the indicator function, is called empirical distribution function.

**Theorem 3.1** (Weak Law of large numbers). Let $X_1, X_2, \ldots$ be independent and identically distributed random variables with finite mean $EX_1 = \mu$ and finite variance $\text{var}X_1 = \sigma^2$. Then

$$P\left(\left|\frac{1}{n} \sum_{i=1}^{n} X_i - \mu\right| > \epsilon\right) \to 0 \quad \text{as} \quad n \to \infty,$$

**Theorem 3.2** (Consistency of empirical d.f.). Let $X_1, X_2, \ldots$ be independent and identically distributed random variables with c.d.f. $F_X$. Then for any $x$

$$P\left(\left|\hat{F}_n(x) - F_X(x)\right| > \epsilon\right) \to 0 \quad \text{as} \quad n \to \infty.$$

**Theorem 3.3** (Central limit theorem). Let $X_1, X_2, \ldots$ be independent and identically distributed random variables with finite mean $EX_1 = \mu$ and finite positive variance $0 < \text{var}X_1 = \sigma^2$. Then

$$P\left(\sqrt{n} \frac{\overline{X}_n - \mu}{\sigma} \leq x\right) \to \Phi(x),$$

where $\Phi(\cdot)$ is the distribution function of standard normal distribution (with zero mean and unit variance). Equivalently we write

$$\sqrt{n} \frac{\overline{X}_n - \mu}{\sigma} \overset{d}{\to} N(0,1),$$

or

$$\frac{\sum_{i=1}^{n} X_i - n\mu}{\sqrt{n}\sigma^2} \overset{d}{\to} N(0,1),$$

or

$$\sqrt{n} \left(\overline{X}_n - \mu\right) \overset{d}{\to} N(0,\sigma^2).$$

The text is an excerpt from NMAI059-EN Probability and Statistics, a course text for MFF UK students by doc. RNDr. Daniel Hlubinka, Ph.D. Many thanks for the help he provided!
Permutation of an \( n \)-element set (for short: \( n \)-permutation) is any assignment of exactly one element of this set to every its element.

Permutation can be also considered as an ordering of the set, i.e. an assignment to its elements the numbers of positions from the set \( \{1,2,\ldots,n\} \). This is the set \( n \)-permutations are often considered over (and will be henceforth unless stated otherwise); another convenient way is to take \( \{0,1,\ldots,n-1\} \).

Matrix notation of a permutation \( \sigma \) of the set \( \{1,2,\ldots,n\} \) is an arrangement of the form
\[
\begin{pmatrix}
1 & 2 & 3 & \ldots & i & \ldots & n \\
\sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(i) & \ldots & \sigma(n)
\end{pmatrix},
\]
where \( \sigma(i) \) is the element assigned by \( \sigma \) to \( i \). This permutation can be shortly and uniquely encoded with the bottom row of the matrix above, i.e. an \( n \)-term sequence in which every number from 1 to \( n \) appears exactly once.

For example, 9-permutation \((1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9)\), which (as a function) maps 1 to 4, 2 to 2, 3 to 1, etc. can be shortly encoded as 421378695. If the mapping is denoted by an arrow, we can write
\[
1 \mapsto 4 \mapsto 3 \mapsto 1, \quad 2 \mapsto 2, \quad 5 \mapsto 7 \mapsto 6 \mapsto 8 \mapsto 9 \mapsto 5,
\]
which gives motivation to look at \( n \)-permutations in a different way.

A cycle of permutation \( \sigma \) containing element \( i \) is a maximal sequence of mutually different terms
\[(i, \sigma(i), \sigma(\sigma(i)), \sigma(\sigma(\sigma(i))), \ldots)\]
and any of its cycle shifts. In the example above there are three cycles: \((1,4,3)\), \((2)\) and \((5,7,6,8,9)\), where \( k \)-element cycles can be written in \( k \) ways, e.g. \((1,4,3) = (4,3,1) = (3,1,4)\).

A one-element cycle is called a fixed point of a permutation.

Cycle notation of a permutation \( \sigma \) shows decomposition of \( \sigma \) into disjoint cycles (possibly omitting fixed points), where every cycle starts with its least element and the cycles are sorted increasingly with respect to their least elements. For instance \((1,4,3)(2)(5,7,6,8,9)\) or \((1\ 4\ 3)(5\ 7\ 6\ 8\ 9)\) is a cycle notation of the permutation given in the example.

The permutations treated as compositions of cycles can be interpreted as ways for \( n \) people to sit around some tables, where two such arrangements are considered equivalent iff everyone has the same right neighbour in both of them. Each table corresponds to a cycle and right neighbour of person \( i \) is just \( \sigma(i) \).

\[
1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9
\]

1 \( \mapsto \) 4 \( \mapsto \) 3 \( \mapsto \) 1, 2 \( \mapsto \) 2, 5 \( \mapsto \) 7 \( \mapsto \) 6 \( \mapsto \) 8 \( \mapsto \) 9 \( \mapsto \) 5
The number of $n$-permutations is equal to $n!:=1\cdot 2\cdot 3\cdots n$ (\textit{n factorial}). Indeed, every permutation is uniquely determined by a series of choices for consecutive $\sigma(i)$. Value $\sigma(1)$ can be chosen in exactly $n$ ways, $\sigma(2)$ — in $n-1$ (from the numbers different from $\sigma(1)$), $\sigma(3)$ — in $n-2$ ways etc., finally there are two choices for $\sigma(n-1)$ and only one choice for $\sigma(n)$ (the one unused number). We also put $0! = 1$.

The method of choosing a permutation described above is connected with the matrix notation — we basically choose the bottom row. There is also a method concerning cycle notation; we will present it via sittings around tables. Suppose that people numbered from 1 to $n$ are subsequently choosing a place to sit. The person $i$ can either open a new table (constructing a new cycle), or put their chair directly to the right of one of already sitting $i-1$ people (prolonging one of the existing cycles); there are $i$ choices altogether. Thus the total number of possible sittings equals $n!$ (as different sets of choices yield different sittings).

The permutation described in the example could have therefore be chosen in the following manner: person 1 opened the first cycle (there was no choice for them), person 2 also chose a new table, person 3 sat to the right of 1, person 4 — to the right of 1 (taking place between 3 and 1), person 5 opened third cycle, and 6, 7, 8, 9 had their chairs put to the right of 5, 5, 6, 8, respectively.

**Exercise 1.** Give the matrix and the cycle notation for the permutation illustrated below.

Who did person 7 choose to sit to the right of (if the cycle scheme of permutation choice is considered)?

**Exercise 2.** (a) Consider the set $\{0,1,\ldots,9\}$ and a mapping $\sigma$, which assigns to $d$ the last digit of the number $7d$. Check that $\sigma$ is a permutation and find its cycle decomposition.

(b) Consider the set of residues modulo 9 and functions $f$, $g$, $h$ defined on it in the following way:

\[ x \mapsto 2x + 1 \mod 9, \quad x \mapsto 3x + 1 \mod 9, \quad x \mapsto 4x + 1 \mod 9. \]

Determine, which functions are permutations of the given set and find their cycle decompositions.

(c) For which pairs of integers $a$, $b$ is $f(x) = ax + b \mod m$ a permutation of the set of residues modulo $m$?

**2. Random permutations**

The methods of choosing a permutation described before can be easily modified to obtain methods of selecting them at random, i.e. in such a way that each possible choice of a $n$-permutation is equally probable (so the probability equals $\frac{1}{n!}$).

In the case of matrix notation we start with drawing $\sigma(1)$ (each possible value with chance $\frac{1}{n}$), then we draw $\sigma(2)$ from among the remaining numbers (chance $\frac{1}{n-1}$ for each of them), etc. Each $n$-permutation has then a chance of being chosen equal to $\frac{1}{n} \cdot \frac{1}{n-1} \cdots \frac{1}{2} \cdot 1 = \frac{1}{n!}$.
We similarly modify the scheme with tables: \(i\)-th person (or generally \(i\)-th element) with equal probability \(\frac{1}{i}\) chooses one of \(i\) options: either takes a seat right to one of already sitting \(i-1\) people (joins an existing cycle), or sits by an empty table (opens a new cycle). Every arrangement (so every permutation) has probability of obtaining: \(1 \cdot \frac{1}{2} \cdot \ldots \cdot \frac{1}{n-1} \cdot \frac{1}{n} = \frac{1}{n!}\).

Answers in the problems below do not need to be formalized with use of probabilistic tools; they can base upon intuition. A bit more precise combinatorial arguments will appear later.

2.1. (a) What is the probability that element 1 is a fixed point of a random \(n\)-permutation?
(b) What is the average number of fixed points in an \(n\)-permutation?

2.2. (a) What is the probability that elements 1 and 2 are in the same cycle of a random \(n\)-permutation?
(b) What is the probability that elements \(i\) and \(j\) \((1 \leq i < j \leq n)\) are in the same cycle of a random \(n\)-permutation?

2.3. (a) What is the probability that a random \(n\)-permutation contains exactly one cycle?
(b) How many \(n\)-permutations are composed of exactly one cycle?
(c) Let \(1 \leq k \leq n\). What is the probability that every cycle of a random \(n\)-permutation contains an element not greater than \(k\)?

2.4. What is the average number of cycles in an \(n\)-permutation?

3. Stirling numbers of the first kind

Definition. Number of \(n\)-permutations decomposing into exactly \(k\) cycles is called a Stirling number of the first kind and denoted \([n \, k]\).

Moreover we put \([n \, 0] = 0\) for \(n \geq 1\) and \([0 \, 0] = 1\).

Exercise 3. Calculate (directly from the definition): \([3 \, 1]\), \([4 \, 3]\), \([4 \, 2]\), \([7 \, 4]\).

3.1. Prove that:

(a) \([n \, 1] = (n-1)!\),
(b) \([n \, n-1] = \binom{n}{2}\),
(c) \(\sum_{k=0}^{n} [n \, k] = n!\).

3.2. Find a formula for \([n \, n-2]\) in a form of a polynomial of variable \(n\).

3.3. Prove that for every \(1 \leq k \leq n\) holds

\([n+1 \, k] = n [n \, k] + [n \, k-1]\).
The last recurrence relation combined with boundary conditions \([0]_0 = 1, [n]_0 = 0\) for \(n \geq 1\) and \([n]_k = 0\) for \(k > n\), allows for a systematic calculation of \([n]_k\) for consecutive \(n\) (resulting in so called Stirling triangle).

<table>
<thead>
<tr>
<th>(n)</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>24</td>
<td>50</td>
<td>35</td>
<td>10</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>120</td>
<td>274</td>
<td>225</td>
<td>85</td>
<td>15</td>
<td>1</td>
</tr>
</tbody>
</table>

**Exercise 4.** Write down the next row, i.e. find \([7]_k\) for \(0 \leq k \leq 7\).

**3.4.** Prove that for \(n \geq 2\):
\[
\sum_{k=1}^{n} (-1)^k \left[\begin{array}{c}n \\ k\end{array}\right] = 0.
\]

**3.5.** Prove that:

(a) \(\sum_{k=0}^{n} \binom{n}{k} \left[\begin{array}{c}n-k \\ a\end{array}\right] \left[\begin{array}{c}n-k \\ b\end{array}\right] = \left[\begin{array}{c}n \\ a+b\end{array}\right] \left(\begin{array}{c}a+b \\ a\end{array}\right)\),

(b) \(\sum_{k=0}^{m} \binom{n+k}{k} \left[\begin{array}{c}n+k \\ k\end{array}\right] = \left[\begin{array}{c}n+m+1 \\ m\end{array}\right]\),

(c) \(\sum_{k=m}^{n} \left[\begin{array}{c}k \\ m\end{array}\right] \frac{n!}{k!} = \left[\begin{array}{c}n+1 \\ m+1\end{array}\right]\).

**3.6.** Prove that for every \(n \geq 1\) and \(x \in \mathbb{R}\) holds
\[
\prod_{k=1}^{n} (x+k-1) = \sum_{k=1}^{n} \left[\begin{array}{c}n \\ k\end{array}\right] x^k.
\]

Algebraic interpretation of the symbol \([n]_k\) from the previous exercise allows to find alternative solutions to many other problems.

**Exercise 5.** Solve as many problems from this script as possible using the identity from the previous problem, choosing adequate value for \(x\).

**Definition.** The sum \(H_n := \sum_{k=1}^{n} \frac{1}{k}\) is called \(n\)-th harmonic number.
3.7. (a) Fix a cycle of length $k$. To how many different $n$-permutations does it belong?
(b) How many different cycles of length $k$ and elements from the set $\{1,2,\ldots,n\}$ are there?
(c) What is the total number of cycles in all $n$-permutations?
(d) Prove that $n$-permutation has $H_n$ cycles on average.

3.8. Prove that $\left\lfloor \frac{n+1}{2} \right\rfloor = n!H_n$.

4. The Transition Lemma

Sometimes instead of the classical cycle notation another is worth considering: such that the least elements of the cycles (each positioned at the beginning) appear in a decreasing order (and we do not omit fixed points). For instance, 9-permutation $(1\ 4\ 3)(5\ 7\ 6\ 8\ 9)$ is encoded as $(5\ 7\ 6\ 8\ 9)(2)(1\ 4\ 3)$.

The key feature of the notation described above is that we can omit the brackets and it remains unique. The structure of cycle decomposition can be then encoded with use of ‘ordinary’ ordering of elements. Existence of this particular bijection is called the transition lemma.

Exercise 6. (a) Which 9-permutation would be encoded as 974658213?
(b) Prove the described property, i.e. that after omitting the brackets they can be uniquely added (allowing for reconstruction of the initial permutation).

4.1. Prove directly (not having used previous problems) that $\sum_{k=1}^{n} k \left[ \frac{n}{k} \right] = \left[ \frac{n+1}{2} \right]$.

4.2. Prove that:

$$\sum_{k=m}^{n} \left[ \frac{n}{k} \right] \left( \frac{k}{m+1} \right) = \left[ \frac{n+1}{m+1} \right], \quad \text{(b) } \sum_{k=0}^{n} \left[ \frac{n}{k} \right] 2^k = (n+1)!.$$ 

4.3. (a) In how many $n$-permutations does element 1 belong to a cycle of length $k$?
(b) Prove that the average sum of squares of lengths of cycles of a random $n$-permutation is equal to $\frac{1}{2}n(n+1)$.

4.4. Let $1 \leq k \leq n$. What is the probability that all elements not greater than $k$ of a random $n$-permutation belong: (a) to the same cycle; (b) to $k$ different cycles?

Lockbox riddle. There are $n$ locked boxes and $n$ keys, each matching a different lock. The keys are put in the boxes randomly (exactly one key in each box). We can force opening of exactly $k$ boxes (e.g. by cutting the locks), where $0 \leq k \leq n$. Then we might get access to some keys allowing for opening other locked boxes, keys from which would allow to open yet other ones etc.

4.5. What is the probability that (after cutting $k$ locks) we will succeed to open all the boxes?
Plane riddle. In a plane there are \( n \) seats (\( n \geq 2 \)), each on a ticket of exactly one passenger. The first \( n-1 \) passengers enter the plane and take their seats at random (independently on a seat number on their tickets). When the last passenger enters the board: if his seat is free he takes it, otherwise he asks the passenger sitting on the taken seat to switch place to the one they have on their ticket. Then the other passenger stands up, goes to their seat and the procedure is repeated (he sits if his seat is free and asks for switching seats otherwise). This goes on until someone sits on the empty place.

4.6. (a) What is the probability that the passenger who was first to enter the plane would have to switch seats?
(b) What is the average (expected) number of passengers who would have to switch seats?

5. Structure of cycle decomposition

5.1. (a) Let \( \frac{1}{2} n < k \leq n \). How many \( n \)-permutations contain a cycle of length \( k \)?
(b) Let \( \frac{n}{m+1} < k \leq \frac{n}{m} \), where \( 1 \leq m \leq n \). In how many \( n \)-permutations is the longest cycle of length \( k \)?

Prisoners riddle. Head officer of a prison offered the following deal to 100 prisoners (numbered from 1 to 100). In his office he had put a collection of 100 boxes (numbered from 1 to 100) in which he had located numbers of prisoners (each in exactly one box) at random. The prisoners enter the office one after another and everyone is allowed to open and look into exactly 50 boxes (of their own choice and in whatever order they want); then the boxes are locked again. If every prisoner succeed to find their number, all of them can go free, otherwise (if at least one of them does not find their number) — they remain imprisoned forever. Before the first prisoner enters the office they have time to discuss the strategy, but then they lose any possibility of communication with each other.

For instance if they agree to choose boxes randomly, then one particular prisoner will succeed with chance \( \frac{1}{2} \), so all of them will be set free with probability \( \frac{1}{2^{100}} \approx 8 \cdot 10^{-31} \ldots \)

5.2. Provide a strategy giving the prisoners over 30\% chance to be set free.

5.3. (a) Suppose that the head officer did not put the numbers at random but he deduced the prisoners’ strategy and located the numbers dastardly. How does it affect the chances of the prisoners?
(b) Suppose now that the head officer is gracious and allowed the first prisoner not only to see the contents of all boxes, but also to swap the numbers in two of them (of his choice). How does it affect the chances of the prisoners?

5.4. Let \( (m_k)_{k=1}^{n} \) be nonnegative integers such that \( \sum_{k=1}^{n} km_k = n \). Prove that the number of \( n \)-permutations which have exactly \( m_k \) cycles of length \( k \) equals

\[
 n! \prod_{k=1}^{n} \frac{1}{k^{m_k} m_k!}. 
\]
5.5. Let $p$ be a prime number.
(a) Prove that if $2 \leq k \leq p-1$, then $\left[ \frac{p}{k} \right]$ is divisible by $p$.
(b) Prove that $(p-1)!+1$ is divisible by $p$.
(c) Prove that if $p>3$, then $\left[ \frac{p}{2} \right]$ is divisible by $p^2$.
(d) Deduce the following theorems from previous parts:

**WILSON’S THEOREM.** An integer $n \geq 2$ is prime iff $n \mid (n-1)!+1$.

**WOLSTENHOLME’S THEOREM.** If $p>3$ is prime, then the numerator of the fraction $H_{p-1}$ (written in the reduced form) is divisible by $p^2$.

5.6. Prove that $\binom{n}{k} = \frac{n!}{k!} \sum_{\sum_{i=1}^{k} r_i = n} \prod_{i=1}^{k} \frac{1}{r_i}$, where $r_i \geq 1$.

5.7. (a) How many $(2m)$-permutations have all the cycles of even length?
(b) Let $n = km$. Prove that the number of $n$-permutations having only cycles of length divisible by $k$ is equal to
\[
\frac{n!}{k^mm!} \prod_{i=1}^{m-1} (ki+1).
\]

6. DERANGEMENTS AND FIXED POINTS

**DEFINITION.** An $n$-permutation with no fixed points is called an $n$-derangement. Denote the number of $n$-derangements by $D_n$; also put $D_0 = 1$.

**EXERCISE 7.** Calculate (directly from the definition) $D_k$ for $k=1,2,3,4,5$.

6.1. Prove that $\sum_{k=0}^{n} \binom{n}{k} D_{n-k} = \sum_{k=0}^{n} k \binom{n}{k} D_{n-k}$.

6.2. Prove that if $n \geq 2$, then $D_n = (n-1)(D_{n-1} + D_{n-2})$.

6.3. Prove that:
(a) $D_n = n! \cdot \sum_{k=0}^{n} \frac{(-1)^k}{k!}$,  
(b) $D_n = nD_{n-1} + (-1)^n$.

The power series representation of the exponential function, i.e. the fact that for every real $x$
\[
e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!},
\]
where $e \approx 2.71828$ is the base of natural logarithm, allows to deduce from the first part of the previous problem that $D_n \approx n!/e$.  

□□■■  51  □□■■
6.4. There are \( n \) people at a party, each having a hat. When leaving, every person took a random hat. What is the probability that at least one person took their own hat? How can this probability be approximated for large \( n \)?

6.5. How many \( n \)-permutations do not contain any cycle of length \( k \)? Argue that for large \( n \) this number is approximately equal to \( e^{-1/k} \).

6.6. Prove that the number of \( n \)-derangements decomposing into exactly \( k \) cycles is equal to

\[
\sum_{i=0}^{k} \binom{n}{i} \frac{n-i}{k-i} (-1)^i.
\]

7. **One combinatorial identity**

7.1. Prove that

\[
\sum_{k=1}^{n} \binom{n}{k} 2^{n-k} = (2n-1)!!.
\]

7.2. Consider the following experiment. Choose an \( n \)-permutation at random and paint each of its cycles red or blue (independently for each cycle the chances for both colours are \( \frac{1}{2} \)).

(a) What is the probability that exactly \( k \) elements will be painted red?

(b) Prove that

\[
\sum_{k=0}^{n} \binom{2k}{k} \binom{2n-2k}{n-k} = 4^n.
\]

**Bibliography**

- Martin Aigner
  *A Course in Enumeration*

- Arthur T. Benjamin, Jennifer Quinn
  *Proofs That Really Count*
  (2003) pp. 91–107

- Miklós Bóna
  *A Walk Through Combinatorics*

- Miklós Bóna
  *Combinatorics of Permutations*

- Miklós Bóna
  *Introduction to Enumerative Combinatorics*

- Richard P. Stanley
  *Bijective Proof Problems*
  (2009) pp. 10–18

- Richard P. Stanley
  *Enumerative Combinatorics Vol. 1*
  (2011) pp. 29–37
1 Probability

1.1 "School" standard probabilistic models and definitions

**Definition 1.** A standard probabilistic model is defined by $\Omega$. The $\Omega$ is a set of all possible events (we call them elementary). We express each non-elementary event as a set of some elementary events. Probability of event $A$ is denoted by $P(A)$ and defined as

$$P(A) = \frac{|A|}{|\Omega|}$$

Example: If our random experiment is a K6 dice-roll, then:

- $\Omega = \{1,2,3,4,5,6\}$ (set of all possible outcomes)
- Exemplary event $B$ defined as rolling number divisible by 3, is a set $\{3,6\}$ and its probability is $P(B) = \frac{2}{6} = \frac{1}{3}$.

**Remark.** This definition is appropriate only when dealing with finite $\Omega$.

1.2 More general probabilistic models and definitions

**Definition 2.** A probabilistic model is given by a triplet $\Omega, F, P$, where $\Omega$ is set of all possible events, $P$ is probability function and $F$ are all sets upon which $P$ is defined. $P$ needs to have several properties, for instance it cannot be negative, $P(\Omega) = 1$ and probability of sum of disjoint events is a sum of probabilities of those events.

**Remark.** It is possible and common, that not all subsets of $\Omega$ can have probability defined. Thus explicitly defining $F$ is required.

In this lecture we will use a specific probabilistic model: model of a random walk, defined by a coin toss.

Lets assume that sides of a coin are $\{-1,1\}$ (we will also call them tails/heads) and probability of getting 1 is equal to $p$. Then this model can be roughly specified this way:

- Each infinite sequence is a elementary event.
- Simplest sets for which we can define probability will be all sets that have value 1 (or $-1$) at some selected index $i$ and their probability is $p$ (or $1-p$ respectively).
- Finite intersections of sets mentioned above (we can call this intersections "cylinders") also have probability defined (we will show how in a second).
\[ F \text{ will be defined as an extension of a set of cylinders by using operations of compliment, countable union and countable sum. We will assume that this is a reasonable mathematical object. How does } P \text{ get defined upon a new sets? For set } A, \text{ probability of it's compliment is a } 1 - P(A). \text{ For sequence of sets } A_1, A_2, A_3, ..., \text{ we know what is the probability of their finite union and their finite sum (I leave this without proof). Sequence of probabilities of finite union is a descending sequence then we'll define probability of infinite union as the limit of this sequence (it is monotonous, so the limit exists). We define the probability of countable sum in analogous way.}

**Definition 3.** A model of random walk is given by a triplet \( \Omega, F, P \), where \( \Omega = \{-1, 1\}^{\mathbb{Z}^+} \), \( P \) is a Borel measure defined on a sigma field generated by cylinders. Cylinder can be specified by two sequences of \( h_1, h_2, ..., t_1, t_2, \ldots, h_i \neq t_j; \) for each sequences there exists a set of all events that had 1 on positions \( h_i \) and -1 on positions \( t_i \). It's probability is \( p^n (1-p)^m \).

**Remark.** In this model all elementary events have probability 0. This does not mean that they can't happen.

Intuition "\( P(A) = 0 \) means the event can't happen" is correct in finite models but it fails us when it comes to general probability models. More appropriate is to think about probability in terms of "repetitions": When we repeat a experiment, probability of a event can be understood as a ratio of number of recurrences of the event and experiment repetitions. Probability equal to 0 means simply that event will not reoccur often enough to be significant.

At the same time when discussing events we say something that has probability 0 is irrelevant.

**Remark.** Probability "adds up" for countable sums of disjoint events, but doesn't need to for sums sets of events that are larger than \( |\mathbb{Z}_+| \).

While not giving proof that there is more that one infinity, we see that there is infinite number of elementary events of probability 0, that add up to a set that has probability 1.

At the same time countable sum of sets that have probability 0, still has probability 0. This prompt us to belief, that there are more of those elementary events than natural numbers (they are uncountable).

**Definition 4.** We call events "independent" if knowing that one of them happened does not influence probability of second happening.

Simple example from standard probabilistic models would be this:

Let's roll a 6-sided dice. Let event \( A \) be rolling number that is even, and event \( B \) rolling a number divisible by 3. We see that \( P(B) = \frac{1}{3} \) since out of 6 outcomes two (3,6) are divisible by 3. If we assume that \( A \) happened, then we know that dice rolled one of three outcomes 2, 4, 6, each with the same probability. So, if \( A \) happened, probability that \( B \) happened is still \( \frac{1}{3} \).

In our case we will talk about random walks and it is important that those are given by a series of coin tosses that are independent from each other.

**Remark.** If \( A \) is independent of \( B \), then \( P(A \cap B) = P(A) \cdot P(B) \)

**Remark.** If \( A \) is independent of \( B \), then \( B \) is independent of \( A \).

**Definition 5** (Almost precise). A random variable is a function \( \Omega \rightarrow \mathbb{R} \) such that for any interval \([a, b]\), set \( f^{-1}([a, b]) \in F \).
This condition means that for random variable \( X \), the "value \( X \text{ is } \in [a,b] \)" is a valid event, which means that it exists in \( F \) and we can measure it’s probability.

**Remark.** If \( A \) is an event, then simplest random variable is denoted by \( 1_A \). This variable is equal to 1 if \( A \) and 0 otherwise.

Exemplary random variable could represent a winnings from a lottery:

If there is a lottery in which you pick 4 numbers, machine takes random 4 and gives you rewards proportional to the numbers of "guessed correctly", then we could construct a variable to represent our winnings. For fixed selected by us combination of numbers, we can define events \( A_n \) meaning we predicted \( n \) numbers correctly. Let’s say for hitting 2 numbers we get 100 dollars, for 3 prize is 10.000 dollars and for all 4 prize is 1.000.000 dollars. Then our random variable is:

\[
X = 1_{A_0} \cdot 0 + 1_{A_1} \cdot 0 + 1_{A_2} \cdot 100 + 1_{A_3} \cdot 10.000 + 1_{A_4} \cdot 1.000.000
\]

Probability that random variable \( X \) is equal to \( k \) is denoted by \( P(X = k) \).

**Definition of expected value** is introduced in section "Symmetric random walks".

**Definition of variance** is introduced in section "Weak law of large numbers".

# Random walks

We’ll consider random walks described in previous chapter.

## 2.1 Asymmetric random walks

**Lemma 1.** Probability of event that we obtain heads only is 0.

While we already stated that elementary events have probability 0, we will prove this fact as a exercise.

**Proof.** Event that in infinite sequence of coin-tosses we obtain only heads is a countable intersection of events \( A_i \), where \( A_i \) means that in first \( i \) tosses we obtained heads. \( P(A_i) = p^i \). Probability of our event is a limit of \( p^i \) when \( i \) tends to \( \infty \) which is 0. \( \square \)

**Lemma 2.** Probability of event that we obtain only sequence of heads and tails such that for selected \( n \) and for any \( k \), for some \( i \) from the set \( \{kn+1, kn+2, \ldots, kn+n\} \) in \( i \)-th coin-toss we got heads is 0. By completion this means a probability that for selected \( n \) there exists \( k \) such that for all indices from \( \{kn+1, kn+2, \ldots, kn+n\} \) we obtain tails is 1.

**Proof.** Let’s divide sequence of heads and tails into disjoint groups of \( n \) elements. Lets denote 1 if in one group there are only tails, and \( -1 \) if there is at least one head. Then we obtain sequence of \( -1 \) and \( 1 \) probability of getting 1 is \((1-p)^n\). By previous lemma probability of getting sequence of just -1’s is 0. This proves this lemma. \( \square \)
At this point we only talked about coin-tosses. Now let’s start to speak about true random walks.

Lemma 3. For random walk defined by a coin tosses $X_1, X_2, X_3, \ldots$ probability of event that for selected $n$ and for all $K$, $|\sum_{i=1}^{K} X_i| \leq n$ is 0. This property means that any random walk exits any symmetric interval with probability 1.

Using previous lemmas, the proof is simple.

**Proof.** If there is a sequence of values $-1, 1$, then if any sum of $k$ first elements is smaller with regards to absolute value than $n+1$ then it means that any $2n+2$ consecutive elements can have all the same sign. So our random walk that never exits interval $[-n, n]$ is a sequence that doesn’t have $2n+2$ consecutive ones. This due to previous lemmas this obviously gives us random walk that happens with probability 0.

If random walk exits through one of edges of the intervals, then we can ask ourselves question, which one.

Lemma 4. If probability of obtaining 1 is $p$, then probability of reaching edge $n$ before $-n$ is equal to $\frac{p^n}{p^n + (1-p)^n}$.

While this fact isn’t obvious on the first glance, it can be proved by the symmetry.

**Proof.** Let $L_m, R_m$ be the events meaning that a random walk exited through the left or right edge of the interval respectively before $m$ steps. We know that $P(L_m \cup R_m) = P(L_m) + P(R_m)$ since this events are disjoint, and $\lim_{m \to \infty} P(L_m + R_m) = 1$. At the same time, for any trajectory the random walk can have before hitting $n$ there exists exactly mirrored trajectory. First trajectory has $n$ more 1’s than -1’s, second exactly the same, while having exactly the same steps. This means that ration of probabilities of taking those trajectories is $\left(\frac{p}{1-p}\right)^n$. If we sum by all of those finite number of finite trajectories we obtain that $\frac{P(L_m)}{P(R_m)} = \left(\frac{p}{1-p}\right)^n$. If we take $L = \bigcup L_m; R = \bigcup R_m$ and we know that $L_m, R_m$ are a ascending sums of sets, $P(L) = \lim_{m \to \infty} (P(L_m)), P(R) = \lim_{m \to \infty} (P(R_m))$ we obtain that $P(L) + P(R) = 1$ and the ratio is preserved. This gives us that $P(R) = \frac{p^n}{p^n + (1-p)^n}$.

Since our random walk is independent of it’s position and time, then probability of reaching 2 before $-2$ staring from 0 at time 0 is absolutely the same as probability of reaching 5 before 1 starting from 3 at time 11. This "time independence" and "position independence" will be crucial later on.

Now we are going to investigate what is the probability for our random walk to enter zero. Let’s assume $p > \frac{1}{2}$.

Lemma 5. If $X_1 = 1$, then there is a non-zero probability that $\forall n \sum_{k=1}^{n} X_k \neq 0$.

**Proof.** Let $Y_1$ be a event, that a random walk that is at point 1 reaches 2 before it reaches 0. We can apply previous lemma, since it holds even after moving random walk by 1. $P(Y_1) = \frac{p}{p + (1-p)}$.

Let $Y_2$ be a event, that a random walk, starting at point 1 reaches 2 before 0 and then it reaches 4 before 0. We can apply previous lemma again. $P(Y_2) = P(Y_1) \cdot \frac{p^2}{p^2 + (1-p)^2}$.
We can define \( Y_{n+1} \) by induction. Assuming some event happened form \( Y_n \) and we are in \( 2^n - 1 \), we can either go to \( 2^{n+1} \) or \( 0 \). \( P(Y_{n+1}) = P(Y_n) \frac{P_{2^n} - 1}{(1-p)^{2^n}} \). Then entering \( 1 \), and never returning to \( 0 \) is an event that can be expressed as \( \bigcap Y_n \). Probability of such event can be expressed as a limit \( \lim_{n \to \infty} \prod_{k=0}^{n} p^{2^k} + (1-p)^{2^k} \)

\[
> \prod_{k=0}^{n} \left( 1 - \frac{1}{p^{2^k} + (1-p)^{2^k}} \right) = \prod_{k=0}^{n} \left( 1 - \frac{1}{p^{2^k} + (1-p)^{2^k}} \right) = \prod_{k=0}^{n} \left( 1 - \frac{1}{(p^{-1})^{2^k} + 1} \right)
\]

We know that since \( p > \frac{1}{2} \), series \( \frac{1-p}{p} < 1 \), so series \( \left( \frac{1-p}{p} \right)^k \) converges so product above has positive limit. So probability that starting from \( 1 \) random walk never reaches \( 0 \) is non-zero.

When it comes to the other side, the situation is different.

**Lemma 6.** If \( X_1 = -1 \), then probability that \( \forall n \sum_{k=1}^{n} X_k \neq 0 \) is 0.

**Proof.** Here reasoning is much simpler: for each interval \([-n,n]\) probability of leaving it through the left side is not larger than \( \frac{1}{2} \). Let \( Z_1 \) be an event such that a random walk reaches \(-2\) before it reaches \( 0 \). This probability is not larger than \( \frac{1}{2} \). Let \( Z_2 \) be an event such that a random walk reaches \(-2\) and then \(-4\) before \( 0 \). Probability of this is not larger than \( \frac{1}{2} \). If we define \( Z_k \) by induction. \( P(Z_k) \leq \frac{1}{2^k} \). This means that \( P(\bigcap Z_k) \) is 0. At the same time for each interval \([-2^k,0]\) probability of staying in this interval is 0.

Summing up, for a asymmetric random walk, when leaving \( 0 \) by going to \(-1\), probability is 1 that we return to \( 0 \). When leaving \( 0 \) by going to \( 1 \) probability is non-zero that we will never return to \( 0 \). This means that each time we are at \( 0 \), there is a non-zero probability, that this is our last time being at \( 0 \). Due to time independence we obtain the following result.

**Remark.** Asymmetric random walk enters \( 0 \) finite number of times.

### 2.2 Symmetric random walks

Picking up where we left of from previous chapter let’s assume the random walk is symmetric so \( p = \frac{1}{2} \). Using proof from previous chapter (all we used in it is that probability of leaving through one side of the interval is not greater than \( \frac{1}{2} \)) we see that property given by lemma [6] is retained but it applies both for \( X_1 = 1 \) and \( X_1 = -1 \), meaning that when random walk leaves point \( 0 \), it returns to it with probability 1. Since random walk is time independent, each time we enter \( 0 \), we return to it with probability 1. Such property is called "recurrence".

**Remark.** Symmetric 1-dimensional random walk enters \( 0 \) infinite number of times.
Proof is a standard exercise.

Proof. Let $A_n$ be all random walks that enter 0 at least $n$ times. $\forall n P(A_n) = 1$. So $P(\bigcap A_n) = \lim_{n \to \infty} P(A_n) = 1$. \qed

Now we'll switch from talking about events and probability to random variables and expected value.

**Definition 6** (Narrow definition). Expected value of a random variable $X$ with countable set of nonnegative values named $v_i$ is equal to:

$$E_X = \sum_{k=1}^{n} v_i \cdot P(X = v_i)$$

where $n$ is either a natural number or $+\infty$, depending on the size of set of values. Expected value in this setting is either a real number or a $+\infty$.

Finite examples are simple, for instance for variable $K_6$ denoting number of "points" obtained on a dice roll has a expected value equal to $E K_6 = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \frac{1}{6} \cdot 3 + \frac{1}{6} \cdot 4 + \frac{1}{6} \cdot 5 + \frac{1}{6} \cdot 6 = \frac{7}{2}$.

A infinite example that is in tune with the rest of this chapter is following: denote $H$, number of consequent coin tosses required to obtain heads. This variable can be described by formula $\forall x \not\in \mathbb{Z}^+ P(H = x) = 0; \forall n \in \mathbb{Z}^+ P(H = n) = \frac{1}{2^n}$. It has a countable set of values ($\mathbb{Z}^+$) and it’s expected value is given by a series $\sum_{k=1}^{\infty} \frac{1}{2^n} \cdot n = 2$.

Since such expected value of positive random variables is "nothing more than a series" it behaves normally when multiplied or added: $E X \cdot n = E n X$, $E (X + Y) = E X + E Y$. Also simple inequalities apply, if for all elementary events $\omega$, $X(\omega) \leq Y(\omega)$ then $E X \leq E Y$.

**Remark.** Some intuition, how to understand expected value is "value we get on average". This intuition however does not explain what does it mean that variable has infinite expected value.

Let’s get back to our symmetric random walks. We know that each time we leave the point 0, we will return to it at some point. And as it appears the expected value of time needed to return to the 0 is infinite.

**Lemma 7.** Let $T$ be a variable denoting time required for a random walk to return to a point 0 for the first time. $T$ is finite with probability 1, but $E T$ is infinite.

Proof. Lets return to construction before. Given a random walk that at moment 1 is at point 1, it can leave interval $[0, 2]$ through any of his edges, each with the same probability $\frac{1}{2}$. Random walk that reaches point 2 will at some point exit interval $[0, 4]$ through one of his edges each with probability $\frac{1}{2}$. If we continue we can construct a countable number of sets $A_n; n \in \mathbb{Z} \cup \{0\}$ such that $A_n$ is probability that a random walk will reach $2^n$ point before returning to 0 and then it will return to 0 before reaching $2^{n+1}$. $\forall n \in \mathbb{Z} \cup \{0\} P(A_n) = \frac{1}{2^{n+1}}$.

Now we know that if a random walk is in $A_n$ then it means it reached $2^n$ and then 0 in that order. That means that the time of returning to 0 is at least equal to $2^{n+1}$. This means that our
variable can be bounded from below by:

\[ H_b = \sum_{n=0}^{\infty} 1_{A_n} 2^{n+1} \]

At the same time it is easy to compute the \( \mathbb{E}H_b \):

\[
\mathbb{E}H_b = \sum_{n=0}^{\infty} P(A_n) \cdot 2^{n+1} = \sum_{n=0}^{\infty} \frac{1}{2^n + 1} \cdot 2^{n+1} = \sum_{n=0}^{\infty} 1 = \infty
\]

This means that the expected value of time needed to return to 0 is \( \infty \)  

So how to understand the expected value? As we will show in chapter about weak law of large numbers it generally means what will be average of the variable if we obtain multiple values of it. Infinite expected value means simply that for each natural \( N \) when obtaining such average the more variables we take, the greater the probability we exceeded \( N \).

Now let’s talk about multidimensional random walks. We will investigate random walks such that are superpositions of simple 1-dimensional random walk. 2-dimensional random walk will be defined as \( X = (X_1, X_2) \) where \( X_1 \) and \( X_2 \) independent random walks, 3 and more dimensional walks are defined analogously. This brings up the question of recurrence again. We see that now, for a random walk \( X \) to return to point 0 multiple random walks need to "synchronize". So is multidimensional random walk recurrent?

First let’s prove a simple recurrence criterion:

**Lemma 8.** Random walk is recurrent if and only if expected number of returns to point 0 is infinite.

**Proof.** If random walk enters 0 infinite number of times with probability 1, then obviously it’s expected value is infinite. So let’s assume random walk is non-recurrent. This implies, there is a probability \( p > 0 \) that random walk does not return to 0. Then probability that our random walk will return to 0 exactly \( n \) times is equal to \( (1-p)^n p \). With probability 1 it returns finite number of times. So last thing left is to calculate the expected value, but we know that sum of series \( n(1-p)^n p \) is finite, which concludes our lemma.

Now we’ll prove the critical lemma:

**Lemma 9.** 1,2-dimensional random walks are recurrent, 3-and-above dimensional random walks are not.

**Proof.** For convenience we will try to check if expected number of returns to 0 is finite or not. We will use following trick: the number of returns to the 0 will be \( N \) and \( A_{2n} \) will be event of returning to the 0 in exactly \( 2n \) steps (it is impossible to do in odd number of steps). Then:

\[
N = \sum_{k=1}^{\infty} 1_{A_{2n}}
\]
The reasoning is simple for a elementary event that returns to 0 in 2,10,32 steps only $N = 3$, $1_A = 1$, $A_{10} = 1$, and all other $1_A_{32}$ are 0. So we can take expected value:

$$\mathbb{E}N = \sum_{k=1}^{\infty} \mathbb{E}1_{A_{2k}}.$$ 

The $\mathbb{E}1_{A_{2n}}$ expression is just $P(A_{2n})$. This is a probability a random walk enters 0 in exactly $2n$ steps. For 1-dimensional random walks it is equal to $f_n = \frac{\binom{2n}{n}}{2^{2n}}$. For $k$-dimensional it is $f_n^k$. So the question comes down to: for what $k$ the series $\sum_{n=1}^{\infty} f_n^k$ converges.

Expression for $f_n$ is still unpleasant so we will use something simpler. First:

$$\frac{f_{n+1}}{f_n} = \frac{(2n+2)!n!n!}{4 \cdot 2n!(n+1)!(n+1)!} = \frac{(2n+2)(2n+1)}{4(n+1)(n+1)} = \frac{2n+1}{2n+2}$$

This gives us nice recurrent expression.

Now we can prove by induction that: $\frac{1}{\sqrt{n+1}} \geq f_n \geq \frac{1}{2\sqrt{n}}$.

For $n = 1$ $f_n = \frac{1}{2}$ so: $\frac{1}{\sqrt{2}} > \frac{1}{2} \geq \frac{1}{2}$. So this holds. Now:

$$\frac{1}{\sqrt{n+1}} \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{n+2}} \iff \left(1 - \frac{1}{2n+2}\right) < \sqrt{\frac{n+1}{n+2}}$$

$$\iff \left(1 - \frac{1}{2n+2}\right)^2 < \frac{n+1}{n+2} \iff 1 - \frac{1}{n+1} + \frac{1}{(2n+2)^2} < 1 - \frac{1}{n+2}$$

$$\iff \frac{1}{(2n+2)^2} < \frac{1}{n+1} - \frac{1}{n+2} \iff \frac{1}{(2n+2)^2} < \frac{1}{(n+1)(n+2)}$$

Last expression holds so first does as well. This implies that for any $n$, $\frac{1}{\sqrt{n+2}} \geq \frac{1}{\sqrt{n+1}} \cdot \frac{2n+1}{2n+2} \geq f_n \cdot \frac{f_{n+1}}{f_n} = f_{n+1}$. This proves that right hand side inequality holds for all $n$.

Now:

$$\frac{1}{\sqrt{n}} \cdot \frac{2n+1}{2n+2} > \frac{1}{\sqrt{n+1}} \iff \frac{2n+1}{2n+2} \geq \sqrt{\frac{n}{n+1}} \iff \left(1 - \frac{1}{2n+2}\right)^2 > 1 - \frac{1}{n+1}$$

$$\iff 1 - \frac{1}{n+1} + \frac{1}{(2n+2)^2} > 1 - \frac{1}{n+1} \iff \frac{1}{(2n+2)^2} > 0$$

This is true and similarly we can obtain that $f_n \cdot \frac{f_{n+1}}{f_n} \geq \frac{2}{\sqrt{n}} \cdot \frac{2n+1}{2n+2} > \frac{2}{\sqrt{n+1}}$.

Now we know that $f_n$ can be bounded by a series $\frac{1}{\sqrt{n}}$. Since that:

$$\sum_{n=2}^{\infty} \left(\frac{1}{\sqrt{n}}\right)^k \geq \sum_{n=1}^{\infty} f_n^k \geq \frac{1}{2^k} \sum_{n=1}^{\infty} \left(\frac{1}{\sqrt{n}}\right)^k$$

So it is enough to check if such series converges $\sum_{n=1}^{\infty} \left(\frac{1}{\sqrt{n}}\right)^k = \sum_{n=1}^{\infty} \frac{1}{n^{1.5}}$ (in mathematical jargon we proved that series $f_n$ is asymptotically the same as $\frac{1}{\sqrt{n}}$). But this converges only for $\frac{k}{2} \leq 1$.

So it converges for 1,2 and for higher integers it doesn’t.

$\square$
As a final note it is worth mentioning that there may be many different definitions of recurrence. And it is because it is equivalent for a random walk to:

(a) return to point $0$ with probability $1$.

(b) return to point $0$ infinitely many times with probability $1$.

(c) reach any point with probability $1$.

(d) reach any point and return to it infinitely many times with probability $1$.

Proof. We already said why first and second conditions are equivalent.

Third condition implies second, if we reach any point with probability $1$, this implies we reach $0$ after we leave it.

Second conditions implies third. Reasoning is the following: for each point $P$ there is a sequence of moves we can take to get from $0$ to $P$ directly. Even though probability of it happening may be minuscule, we enter $0$ infinitely many times and each time we have a chance to perform this sequence. This means it will happen, so at least once we will enter $P$.

Second and third implies fourth: if we are in point $P$, then (as if we were in $0$) we will return to $P$ infinitely many times.

Fourth implies all of the above.

This implies that all this conditions are equivalent.

Third property is some formulation of mathematical phenomenon called "Gamblers Ruin". One of the descriptions is following: assume gambler plays a fair game with a bank, that results from one player taking $1$ one chip from another. Gambler can get bankrupt if he looses his $k$ chips, bank cannot get bankrupt. Then with probability $1$ the gambler gets bankrupt, since $1$-dimensional random walk moves will at some point appear in point $-k$.

2.3 Markov chain random walks

In this subject we will focus on expected values of reaching some one point from another in the Markov chain. Our model will have $n$ states in which random walk can currently be and a list of transitions specific for each state. In each state we can transition to some different state with probability dependent on our current state, but independent from time.

Simple example would be the following: imagine you simulate experiment in which you toss a symmetric coin until you get three heads in a row. At each point in time relevant to the experiment is only how much tails in "one streak" we have now. Then:

- Having 0-head streak we can remain in it with probability $\frac{1}{2}$ and with the same probability we can get a head and be in a 1-head streak.

- Having 1-head streak we can either obtain tails with probability $\frac{1}{2}$ thus moving to 0-head streak or get head and move to 2-head streak.
Similarly for 2-head streak we can move either to 0-head streak or 3-head streak, both moves happen with $\frac{1}{2}$ probability.

- Being in 3-head streak we remain in it since the experiment ends.

In this example we see 4 states with up to two transitions for each state. Of course examples can be numerous. For instance if we take 40 fields of the monopoly board, then from each field we can have 11 transitions, each defined by a probability of obtaining a number from 2 to 12 by rolling 2 dice.

General Markov chains are to broad to prove interesting properties, one needs to assume something for them for further work. We will assume the following: in every of our Markov chain there will be a state called final, such that it can be achieved by finite number of steps (there is a non-zero probability that starting from any state we end up in final step in at most $k$ steps, where $k$ is finite). We see that two presented Markov chains have that property, with a limitation that in the first one, the final state needs to be a "3-head streak" state.

We’re going to investigate those Markov chains, looking at the expected value of time required for them to reach the final state. First remark is the following:

**Lemma 10.** For finite Markov chain with "final state", for each of the other states expected time of reaching the final state is finite.

**Proof.** We see that for any starting state we can reach final state in at most $n$ steps with some positive probability. For each state $S_i$ there exists such probability $p_i$. Let’s take $p = \min_i(p_i)$. For each random walk we have at least $p$ chance that after $n$ moves we will reach final state. So each $n$ steps our probability of not reaching final state yet is decreasing by $(1-p)$. So expected time required for us to reach final state is less than $\sum_{k=1}^{\infty} nk(1-p)^{k-1}p$ which as we know is finite.

When we know that this expected value is finite we can calculate it directly. Let’s take the example with tossing a coin until we obtain 3 tails in the row. Lets name $T_0$, $T_1$ and $T_2$ the variables representing time required to reach state 3-heads in a row starting from state with 0, 1 or 2 respectively.

Let’s take a trajectory that starts in state 0. This trajectory can remain in 0 or move to 1. If it remains in 0, then the expected time of reaching state 3 is $1 + \mathbb{E}T_0$. If it moves to 1, then expected time of reaching 3 is $1 + \mathbb{E}T_1$. Each of this events happens with probability $\frac{1}{2}$. This gives us equation: $\mathbb{E}T_0 = \frac{1}{2} (1 + \mathbb{E}T_0) + \frac{1}{2} (1 + \mathbb{E}T_1)$.

This is a reasoning that allows us to believe that such equation holds, but is imprecise. True proof uses conditional expectation value which is a extremely powerful tool, way to hard to introduce in such lecture. So let’s just assume following holds.

If it does then we can repeat similar reasoning for all of the three non-trivial states and we obtain following equations:

- $\mathbb{E}T_0 = \frac{1}{2} (1 + \mathbb{E}T_0) + \frac{1}{2} (1 + \mathbb{E}T_1)$
- $\mathbb{E}T_1 = \frac{1}{2} (1 + \mathbb{E}T_0) + \frac{1}{2} (1 + \mathbb{E}T_2)$
\[ ET_2 = \frac{1}{2} (1 + ET_0) + \frac{1}{2} \cdot 1 \]

Since we know all of those expected values are finite, we can calculate them and obtain \( ET_0 = 14; ET_1 = 12; ET_2 = 8 \).

Can we do it every time? Probabilities we picked were arbitrary and constants were as well (one can think of them as a cost of performing a specific move). What happens when we take arbitrary probabilities and costs? Then using our previous method for a Markov chain that has \( n \) not final states and \( n+1 \)-th state is final we would obtain a following system of equations:

\[
\begin{align*}
ET_1 &= p_{1:1}(w_{1:1} + ET_1) + p_{1:2}(w_{1:2} + ET_2) \cdots p_{1:n}(w_{1:n} + ET_n) + p_{1:n+1}w_{1:n+1} \\
ET_2 &= p_{2:1}(w_{2:1} + ET_1) + p_{2:2}(w_{2:2} + ET_2) \cdots p_{2:n}(w_{2:n} + ET_n) + p_{2:n+1}w_{2:n+1} \\
& \vdots \\
ET_n &= p_{n:1}(w_{n:1} + ET_1) + p_{n:2}(w_{1:2} + ET_2) \cdots p_{n:n}(w_{n:n} + ET_n) + p_{n:n+1}w_{n:n+1}
\end{align*}
\]

Where \( p_{i,j}, w_{i,j} \) are probability and cost of transition from \( i \)-th state to \( j \)-th. Also following conditions need to be satisfied:

\[
\forall q,r \, w_{q;r} \geq 0, p_{q;r} \geq 0; \forall k \sum_{i=1}^{n+1} p_{k;i} \leq 1; \exists k p_{k;n+1} > 0
\]

This means exactly that weights are positive, probabilities of transition from a state cannot exceed 1 and there is a state in which we can "move to a final state" and stop the walk. As it appear this set of equations has a interesting for us solution:

**Lemma 11.** Following set of equations has a solution for each variable that is positive.

**Proof.** We will show that regardless of what \( ET_i \) we’re going to solve for, we will obtain the unique positive solution. Proof follows simply from induction. Lets assume with have set of 1 equation that has properties as defined. Then it is of the form:

\[
ET_1 = p_{1:1}(w_{1:1} + ET_1) + p_{1:2}w_{1:2}
\]

Then:

\[
ET_1 = \frac{p_{1:1}w_{1:1} + p_{1:2}w_{1:2}}{1 - p_{1:1}}
\]

Due to our conditions we know that \( p_{1:2} \) must be positive so \( p_{1:1} < 1 \) so this solution is positive.

Now let’s assume that set of \( n \) equations has positive solutions for each variable. Take set \( n+1 \) equations. Take it’s any equation (in each equation needs to have at \( p_{i;i} < 1 \) we will prove it later) on the right hand side. Lets assume by symmetry it’s the first equation:

\[
ET_1 = p_{1:1}(w_{1:1} + ET_1) + p_{1:2}(w_{1:2} + ET_2) \cdots p_{1:n}(w_{1:n} + ET_n) + p_{1:n+1}w_{1:n+1}
\]

Let’s transform this equation and normalize it:

\[
ET_1 = + \frac{p_{1:2}}{1 - p_{1:1}} (w_{1:2} + ET_2) + \cdots + \frac{p_{1:n}}{1 - p_{1:1}} (w_{1:n} + ET_n) + \frac{p_{1:n+1}}{1 - p_{1:1}} w_{1:n+1}
\]

Now we can substitute the \( ET_1 \) in all other equations. This means that we change system of \( n+1 \) equations into system of \( n \) equations. In new equations sums of \( p_{i,j} \) coefficients is retained, so it’s 1, and coefficients \( p_{:,n+1} \) do not decrease. So this is a system that also has following properties.
Final question is how do we know that for all $i$ it holds that $p_{i;i} < 1$? Let's take graph defined by this Markov Chain and see what happens when we "remove" one equation/state. As it appears we change one random walk into another such that moves as if the "removed" state exists but it doesn’t stop in it. Each state leading to state that is being removed gets connected with all of his neighbors. This means that at any phase of this process we can reach final state from any other state, so there is no state that has one edge that directs just to itself.

Summing up, taking any random walk on finite Markov chain with final state has a finite expected time of reaching final state. This solves simple mathematical problems and allows us to create models that have some predictive power. Finally we can programmatically compute the solution, since solving linear equation is a standard computing problem.

3 Weak law of large numbers

After understanding notion of probability and expected value, it is important to understand the notion of variance. There are two alternative definitions of variance:

$$\text{VAR}(X) = E\left( (X - E(X))^2 \right) = E(X^2) - (E(X))^2$$

Variance is a notion that "describes randomness". As definition suggests the more values can deviate from expected value the greater the variance. Some distributions that are parametrized by two variables often have a variable that stands for it.

Variance has following properties:

**Lemma 12.** $\text{VAR}(nX) = n^2 \text{VAR}(X)$

The proof is straightforward and I’ll omit it.

**Remark.** As first definition indicates variance is nonnegative. Applying this knowledge to the second equation we obtain that $E(X^2) \geq (E(X))^2$. This is some form of the Cauchy-Schwartz inequality.

To get a better feel of variance we’ll compute it for the variable $X$ such that $P(X = 1) = p; P(X = 0) = 1-p$.

$$E(X) = p \cdot 1 + (1-p) \cdot 0 = p$$

$$\text{VAR}(X) = E(X^2) - (E(X))^2 = E(X) - (E(X))^2 = p - p^2.$$ 

Now let’s assume that we have variable $Y$ with finite expected value for which $P(|Y - EY| > k) > q$.

What does that say about variance?

$$\text{VAR}(Y) = E\left( (Y - EY)^2 \right) \geq E\left( (Y - EY)^2 1_{|Y - EY| > k} \right) > E\left( k^2 \cdot 1_{|Y - EY| > k} \right) > k^2 \cdot q.$$ This means that for given $k, q$ we know that variance is sufficiently large. This also means that given variance and $k$, we know that $q$ must be sufficiently small: $q < \frac{\text{VAR}(Y)}{k^2}$. This gives us important (Chebyshev) inequality:

\[\square\]
Now let’s prove following remark:

**Remark.** Variance of a sum of independent random variables is a sum of variances.

**Proof.** For all variables $X$ and $Y$ with finite variance:

$$\text{VAR}(X + Y) = \mathbb{E}(X + Y)^2 - (\mathbb{E}(X + Y))^2 =$$

$$= \mathbb{E}X^2 + 2\mathbb{E}XY + \mathbb{E}Y^2 - (\mathbb{E}X)^2 - 2\mathbb{E}X\mathbb{E}Y - (\mathbb{E}Y)^2 =$$

$$= \text{VAR}(X) + \text{VAR}(Y) + 2\mathbb{E}XY - 2\mathbb{E}X\mathbb{E}Y$$

If we know that $X$ and $Y$ are independent, then $\mathbb{E}XY = \mathbb{E}X \cdot \mathbb{E}Y$. This proves following remarks.$\square$

This property allows us to deal with the following problem.

**Lemma 13** (Weak law of large numbers). Let $X_1, X_2, X_3, \ldots$ be a independent random variables with the same distribution and finite expected value and variance. Let $S_n = \frac{\sum_{k=1}^{n} X_k}{n}$. Let $\delta, \epsilon > 0$. Then for sufficiently large $n$: $P(|S_n - \mathbb{E}X_1| > \delta) < \epsilon$.

**Proof.** To be exact we will prove that for fixed $\delta$ this probability converges to 0, but since we don’t need to know what is a limit of non-monotonous series we will call it differently. Nevertheless technique will be the same: we will bound sequence of probabilities by some decreasing sequence that will have it’s limit in 0. The tools are already here. Using remark $n-1$ times we obtain that $\text{VAR}(\sum_{k=1}^{n} X_k) = n \text{VAR}(X_1)$. So:

$$\text{VAR}(S_n) = \text{VAR}\left(\frac{\sum_{k=1}^{n} X_k}{n}\right) = \frac{\text{VAR}(\sum_{k=1}^{n} X_k)}{n^2} = \frac{1}{n} \text{VAR}(X_1)$$

This means that variance is steadily decreasing. This leads us to final inequality.

$$P(|S_n - \mathbb{E}X_1| > \delta) < \frac{\text{VAR}(S_n)}{\delta^2} = \frac{\text{VAR}(X_1)}{n\delta^2}$$

So

$$\forall n \quad n > \frac{\text{VAR}(X_1)}{\epsilon \delta^2}; \quad P(|S_n - \mathbb{E}X_1| > \delta) < \epsilon$$

$\square$

Explaining this in terms of the original problem if we have variable $X$ that can have values 0 and 1, then we know it’s variance is less then one (see calculations above). If we want to know $\mathbb{E}X$ then with 0.01 precision with 99% confidence, then we need to take $n > \frac{1}{100} \left(\frac{1}{0.01}\right)^2 = 10^6$ values and take their average.
Conditional sampling is a solution for a problem that can be expressed like this: given random variables from distribution $A$, how can we simulate random variable from distribution $B$? Simplest example of such problem is: how to simulate 5-sided dice, given one 6-sided dice? Answer using conditional sampling would be *roll the dice as long as you obtain something other than 6*.

Solution for real problems are algorithms that should be easy to implement and should not suffer from floating point errors (imprecision due rounding errors), plus it should use most lightweight arithmetic operations. Thus this algorithm should involve many additions, deletions, multiplications of integers, dividing by 2, rounding, some divisions, not use much special functions like exponents, trigonometric functions and avoid harder computation.

Such optimizations can be done in various ways. For instance, let’s say you want to get a random point from a unit disc, given a generator of random variables $I$ from interval $[0,1]$. Trivial algorithm to do it would be: get values of $I_1, I_2$, multiply by $2\pi$ and compute $I_2 \cos(2\pi I_1), I_2 \sin(2\pi I_1)$. This approach is based on a disk parametrization by distance from $(0,0)$ ($I_2$) and angle($2\pi I_1$).

Other approach is to get values is to take $2I_1-1, 2I_2-1$, check if those values lie in unit circle by taking checking if $(2I_1-1)^2 + (2I_2-1)^2 < 1$. It its false, then repeat. Second algorithm involves multiplying by a real number and re-rolling random variables that is still relatively lightweight.

More adequate examples of conditional sampling can be found when simulating random variables with hard do cumulative distribution functions. Understanding of cumulative distribution functions in our case can be like this:

If $f: \mathbb{R} \to [0,1]$ is a cumulative distribution, then to obtain a random variable from this distribution perform following "algorithm":

(a) Draw plot of a function $f$.

(b) Obtain a value of $I$ from uniform distribution on $[0,1]$.

(c) Draw a horizontal line on the height given by value of $I$.

(d) Denote the point $(x,y)$ where this line intersects with plot.

(e) $x$ is a sample of this distribution.

From mathematical standpoint this algorithm is easy, obtain a value of $I$, apply inverse of $f$ and "you’re done". But it is not easy task in terms of elementary computation. Take normal distribution for example with mean 0 and variance 1. It’s CDF is equal to:

$$f(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$$

This integral is already something that computer cannot compute precisely and taking such inverse is hard. At the same time generating normal random variable up to some precision can be done for example by $\sum_{i=1}^{12} I_i - 6$.

This is obviously a approximation but there is also a algorithm that is better, named Box-Müller algorithm. It goes like this:
(a) Let $\phi = 2\pi I_1$

(b) Let $R = \sqrt{-2\ln(I_2)}$

(c) Let $N_1 = R\cos\phi; N_2 = \sin\phi$

Resulting $N_1, N_2$ are normal independent random variable.

As a final note it needs to be said that in case of simple problems algorithms should perform rather lightweight operations, but when problems get harder even using "heavier operations" like trigonometric functions is reasonable and gives us benefit over solving the problem "directly".
1 Tucker circles

**Definition 1.** Let \( P \) and \( Q \) be the points lying on the distinct sides of the given triangle. The side of the triangle is corresponding to the line \( PQ \) if contains neither \( P \) nor \( Q \).

**Theorem 1.** Given \( \triangle ABC \). Let \( P_1 \) be an arbitrary point on the line \( AB \). Now let \( P_2 \in AC \) be the point s.t. \( P_1 P_2 \parallel BC \). Then for \( i \in \{3,4,5,6,7\} \) if line \( P_{i-2}P_{i-1} \) is parallel to its corresponding side of the \( \triangle ABC \), choose \( P_i \) on this side s.t. \( P_i P_{i-1} \) is antiparallel to its corresponding side. Analogously, if the line was antiparallel we construct parallel one. Then \( P_7 = P_1 \) and the obtained hexagon is inscribed in a circle with center lying on the Brocard line \(^1\) of \( \triangle ABC \).

In the following problems we will be using \( \triangle ABC \) and hexagon \( P_1P_2P_3P_4P_5P_6 \) from **theorem 1**. Moreover, assume that hexagon \( P_1P_2P_3P_4P_5P_6 \) has circumcircle \( \omega \).

**Exercise 1.** Let \( \triangle XYZ \) be triangle formed by lines parallel to the sides of \( \triangle ABC \) – \( P_1P_2 \), \( P_3P_4 \) and \( P_5P_6 \). Prove that the center of \( \omega \) is the midpoint of the segment connecting the circumcenters of \( \triangle ABC \) and \( \triangle XYZ \).

**Exercise 2.** Let \( M, N \) and \( P \) be midpoints of the antiparallel sides of \( P_1P_2P_3P_4P_5P_6 \) – \( P_4P_5 \), \( P_6P_1 \) and \( P_2P_3 \) respectively. Then circumcircle of \( \triangle MNP \) is tangent to segment \( P_4P_5 \).

2 Special cases of Tucker circles

2.1 Taylor circle

**Theorem 2.** Let \( D, E \) and \( F \) be the feet of altitudes from vertices \( A, B \) and \( C \) in \( \triangle ABC \) respectively. Let \( D_B \) and \( D_C \) be the projections of \( D \) onto \( AC \) and \( AB \) respectively. Similarly define points \( E_A, E_C, F_A \) and \( F_B \). Then hexagon \( F_AE_AD_BF_BE_CD_C \) is inscribed in a circle with center being the radical center of the circles with centers in \( A, B \) and \( C \) and radii \( AD, BE \) and \( CF \) respectively.

**Exercise 3.** The antiparallel sides of the above hexagon form a triangle with vertices at midpoints of the sides of \( \triangle DEF \).

2.2 Lemoine Circles

**Theorem 3.** (First) Let \( K \) and \( O \) be the Lemoine point and the circumcenter of \( \triangle ABC \) respectively. Then lines through \( K \) and parallel to the sides of the \( \triangle ABC \) intersect these sides at 6 points lying on a one circle with center at the midpoint of \( OK \).

\(^1\)Brocard line is line going through the circumcenter and the Lemoine point of a given triangle.
Theorem 4. (Second aka Cosine Circle) Let \( K \) and \( O \) be the Lemoine point and the circumcenter of \( \triangle ABC \) respectively. Then lines through \( K \) and antiparallel to the sides of the \( \triangle ABC \) intersect these sides in 6 points lying on a one circle.

Theorem 5. (Third) Let \( K \) be the Lemoine point of \( \triangle ABC \). Then circumcircles of \( \triangle BKC \), \( \triangle AKC \) and \( \triangle AKB \) intersect lines \( BC \), \( AB \) and \( AC \) at 6 points, different from vertices of \( \triangle ABC \), lying on a one circle.

2.3 Bu(r)i’s Circle

Theorem 6. Let \( \omega_a \) be the circle tangent to circumcircle of \( \triangle ABC \) at \( A \) and going through its Lemoine point \( K \). Let \( \omega_a \) intersect \( AB \) and \( AC \) at \( C_a \) and \( B_a \) respectively. Similarly define \( A_b, C_b, A_c \) and \( B_c \). Then points \( A_b, A_c, B_a, B_c, C_a \) and \( C_b \) lie on a one circle.

2.4 Adams’ Circle

Theorem 7. Let \( G \) and \( I \) be the Gergonne point and the center of the circle inscribed in \( \triangle ABC \) respectively. Incircle of \( \triangle ABC \) touches sides \( BC \), \( CA \) and \( AB \) at the points \( D \), \( E \) and \( F \) respectively. Then lines through \( G \) and parallel to the sides of the \( \triangle DEF \) intersect sides of \( \triangle ABC \) at 6 points lying on a one circle with center at \( I \).

3 Brocard Circle

Theorem 8. Let \( K \) and \( O \) be the Lemoine point and the circumcenter of the \( \triangle ABC \) respectively. Then two Brocard points\(^2\) and vertices of the first Brocard triangle\(^3\) lie on the circle with diameter \( OK \).

Definition 2. Let \( A' \) be an intersection of the line tangent to circumcircle of \( \triangle ABC \) at \( A \) and line \( BC \). Similarly define \( B' \) and \( C' \). Then points \( A', B' \) and \( C' \) lie on one line called Lemoine axis.

Exercise 4. The Lemoine axis is a radical axis of the Brocard circle and the circumcircle of the \( \triangle ABC \).

Exercise 5. The radical axis of any two distinct Tucker circles is parallel to the Lemoine axis.

4 Droz-Farny Circles

Theorem 9. (First) Given \( \triangle ABC \). Let \( M_a, M_b \) and \( M_c \) be midpoints of the sides \( BC \), \( CA \) and \( AB \) respectively. Let \( R > 0 \) be a real number. Circle centered at \( A \) with radius \( R \) intersects line

\[ <BAP_1 = <CBP_1 = <ACP_1 \text{ and } <CAP_2 = <ABP_2 = <BCP_2. \]

\[ \triangle ABC \text{ is a triangle with vertices at: } AP_1 \cap BP_2, \quad BP_1 \cap CP_2 \text{ and } CP_1 \cap AP_2. \]
\section{Problems!}

\textbf{Exercise 6.} (1st stage of Polish Mathematical Olympiad) Triangle $A_1A_2A_3$ is given. Assuming $A_4=A_1$ and $A_5=A_2$, we define points $X_t$ and $Y_t$ for $t=1$, 2, 3 respectively. Let $\Gamma_t$ with center at $I_t$ be an excircle of triangle $A_1A_2A_3$ tangent to the side $A_{t+1}A_{t+2}$. Let $\Gamma_t$ be tangent to $A_tA_{t+1}$ and $A_tA_{t+2}$ at $P_t$ and $Q_t$ respectively. Line $P_tQ_t$ intersects lines $I_tA_{t+1}$ and $I_tA_{t+2}$ at $X_t$ and $Y_t$ respectively. Prove that points $X_1$, $Y_1$, $X_2$, $Y_2$, $X_3$ and $Y_3$ lie on one circle.

\textbf{Exercise 7.} Given is $\triangle ABC$ and its orthocenter $H$. Let $M$, $N$ and $P$ be midpoints of the sides $BC$, $CA$ and $AB$ respectively. Line perpendicular to $MH$ at the point $H$ intersects $BC$ at $A'$. Similarly define points $B'$ and $C'$. Prove that the points $A'$, $B'$ and $C'$ lie on one line perpendicular to the Euler line of $\triangle ABC$.

\textbf{Exercise 8.} Let incircle of $\triangle ABC$ touch sides $BC$, $CA$ and $AB$ at the points $D$, $E$ and $F$ respectively. Circle $\omega_d$ goes through points $E$, $F$ and intersects lines $BE$, $CF$ at the points $X$, $Y$ respectively. Let $\omega_a$ be circumcircle of $\triangle XED$ and let $\omega_f$ be circumcircle of $\triangle YFD$. Let $\omega_d$ intersects lines $DE$ and $DF$ at the points $D_1$ and $D_2$. Analogously define points $E_1$, $E_2$, $F_1$ and $F_2$. Prove that points $D_1$, $D_2$, $E_1$, $E_2$, $F_1$ and $F_2$ lie on one circle.

\textbf{Exercise 9.} Given $\triangle ABC$. Let $M$, $N$ and $P$ be the midpoints of the major arcs $\overline{BAC}$, $\overline{CBA}$ and $\overline{ACB}$ respectively. Prove that the Simson lines of the points:

- $M$, $N$ and $P$ with respect to $\triangle ABC$
- $A$, $B$ and $C$ with respect to $\triangle MNP$

are concurrent at the center of the Taylor circle of the excentral triangle\footnote{Excental triangle is triangle formed by the centers of excircles of the given triangle.} of $\triangle ABC$.

\textbf{Problem \ref{problem1}}. Given $\triangle ABC$ with orthocenter $H$. Let $H_a$, $H_b$, and $H_c$ be the midpoints of the segments $HA$, $HB$ and $HC$ respectively. Prove that the Simson lines of the points $H_a$, $H_b$ and $H_c$ with respect to the orthic triangle\footnote{Orthic triangle is triangle formed by feet of the altitudes of the given triangle.} of $\triangle ABC$ form a triangle having as orthocenter the center of the Taylor circle of the $\triangle ABC$. 
1 First steps

1.1 Essentials

Theorem 1.1. (Axiom of choice) For any collection $X$ of nonempty sets, there exists a set which contains exactly one element from each set of $X$.

Definition 1.1. Given a set $A$ we say that nonempty subsets $A_1, A_2, \ldots, A_n \subseteq A$ are the partition of $A$ if $A_1 \cup A_2 \cup \cdots \cup A_n = A$ and $A_1, A_2, \ldots, A_n$ are pairwise disjoint.

Definition 1.2. Let $A, B \subseteq \mathbb{R}^3$. $A$ is said to be piecewise congruent to $B$ if $A$ and $B$ can be partitioned into $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_n$ and $A_i$ can be translated and rotated to be $B_i$ for $1 \leq i \leq n$. We denote it by $A \approx B$.

Definition 1.3. Given a set $P \subseteq \mathbb{R}^3$, we call it paradoxical if there exist two disjoint subsets $A, B \subseteq P$ such that $A \approx P \approx B$.

Theorem 1.2. (Banach-Tarski theorem) The ball of any radius in $\mathbb{R}^3$ is paradoxical.

Definition 1.4. We denote the group of isometries of $\mathbb{R}^3$ preserving orientation (rotations and translations) by $O_3$.

1.2 Basic facts about groups

Definition 1.5. The group $(G, \cdot)$ is a set $G$ with a binary operation $\cdot$ which satisfies the following conditions:

- If $a, b \in G$, then $a \cdot b \in G$. We say that the set $G$ is closed under the operation of $\cdot$. We usually skip the dot and write $ab$.

- For any $a, b, c \in G$, then $(ab)c = a(bc)$. We say that the operation $\cdot$ is associative.

- There exists an element $e \in G$ such that for every $a \in G$ the equation $ea = a = ae$ holds. One can prove that such element is unique. We call it the identity element.

- For any $a \in G$ there exists an element $b \in G$ such that $ab = e$. We say that $b$ is an inverse of $a$. One can prove that such element is unique. We denote an inverse of $a$ by $a^{-1}$.

We usually abbreviate $(G, \cdot)$ to $G$. Additionally, if for every $a, b \in G$ the equation $ab = ba$ holds, then we say that $G$ is abelian or commutative.
**Definition 1.6.** We say that a group $G$ acts on a set $S$ if we have a function $\varphi : G \times S \to S : (g, x) \mapsto \varphi(g, x)$ which satisfies following conditions (where we denote $\varphi(g, x)$ as $g(x)$):

- $e(x) = x$ for all $x \in S$, where $e$ is the identity element of $G$.
- $(gh)(x) = g(h(x))$ for all $x \in S$ and $g, h \in G$.

We say that for fixed $x \in S$ the set $\{g(x) : g \in G\}$ is the orbit of $x$.

At first glance the definition of a group acting on a set may be a little abstract and disorienting, but we just want to formalize the situation when we have a set of actions which we can compose and apply to the elements of some other set. The basic example is the group of rotations of the equilateral triangle which acts on the set of its vertices.

### 1.3 G-equidecomposition

**Definition 1.7.** Suppose a group $G$ acts on a set $X$. Let $A, B \subseteq X$. Then $A$ and $B$ are $G$-equidecomposable if $A$ and $B$ can be partitioned into $A_1, A_2, \ldots, A_n$ and $B_1, B_2, \ldots, B_m$ such that for $1 \leq i \leq n$ exists $g_i \in G$ such that $g_i(A_i) = B_i$. We denote it by $A \approx_G B$.

**Proposition 1.1.** $\approx_G$ is an equivalence relation on the elements of $P(X)$.

**Corollary 1.1.** If $A, B \subseteq \mathbb{R}^3$ and $G$ is a subgroup of $O_3$ then $A \approx_G B$ implies $A \approx B$.

## 2 More about groups

### 2.1 Free groups

**Definition 2.1.** The free group $F_s$ with free generating set $S$ is the set of all reduced words (finite sequences of elements) created of elements of $S$ and their inverses with the operation of concatenation (followed by reduction if necessary). The identity element is the empty word $e$. By ‘reduced’ we mean that in these words there is no element next to its inverse.

For example the word $ab^{-1}cc^{-1}bd$ is reduced this way: $ab^{-1}cc^{-1}bd \to ab^{-1}bd \to ad$. When we concatenate two words the outcome must be reduced too, so if we concatenate $abc$ and $c^{-1}b^{-1}a^{-1}$ then we get the empty word.

**Definition 2.2.** Let $G$ be a group acting on a set $X$. Suppose there exist a set $E \subseteq X$, mutually disjoint subsets $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_m \subseteq E$ and $g_1, g_2, \ldots, g_n, h_1, h_2, \ldots, h_m \in G$ such that

$$\bigcup_{i=1}^{n} g_i A_i = E = \bigcup_{i=1}^{m} h_i B_i.$$  

We say that $E$ is $G$-paradoxical.

**Corollary 2.1.** Let $G$ be a subgroup of $O_3$ acting on a set $X$. If $E \subseteq X$ is $G$-paradoxical, then $E$ is paradoxical.
Proposition 2.1. Suppose $G$ is a group acting on a set $X$ and that $E$ and $E'$ are $G$-equidecomposable subsets of $X$. If $E$ is $G$-paradoxical, so is $E'$.

2.2 The $F_2$ free group

Now we’ll focus on one special kind of free groups — the $F_2$ free group. It’s a free group with free generating set consisting only of two elements $a, b$.

Proposition 2.2. The free group $F_2$ is paradoxical.

Lemma 2.1. Given a group $G$ and a set $X$, if $G$ is paradoxical and acts on $X$ with no non-trivial fixed points then $X$ is $G$-paradoxical.

Corollary 2.2. If $F_2$ acts on a set $X$ with no non-trivial fixed points then $X$ is $F_2$-paradoxical.

Now we are ready to find some connection of $F_2$ and $\mathbb{R}^3$ which will help us in proving the Banach-Tarski theorem.

Lemma 2.2. Let $\rho$ and $\sigma$ be counterclockwise rotations about $x$-axis and $z$-axis, respectively, each by an angle of $\arccos(1/3)$. Then $\rho$ and $\sigma$ generate a subgroup of $SO(3)$ (the group of all rotations about the origin in $\mathbb{R}^3$) isomorphic to $F_2$.

3 Construction of the paradox

In the final chapter, we’ll construct the paradox. Firstly we’ll consider only the surface $S^2$ of the ball. Let $F$ be the group constructed in Lemma 2.2.

Lemma 3.1. (Hausdorff’s paradox) There exists a countable subset $D$ of $S^2$ such that $S^2 \setminus D$ is $F$-paradoxical.

Lemma 3.2. If $D$ is a countable subset of $S^2$ then $S^2 \approx_{SO(3)} S^2 \setminus D$.

Corollary 3.1. $S^2$ is $SO(3)$-paradoxical.

After proving that the sphere is paradoxical, we can proceed to the last part of the proof.

Lemma 3.3. Let $B$ be the closed ball in $\mathbb{R}^3$. Let $P$ be the center of $B$. Then $B \setminus \{P\}$ is paradoxical.

Lemma 3.4. Let $S^1$ be the circle on the plane. Let $P$ be a point on $S^1$. Then $S^1 \approx S^1 \setminus \{P\}$.

Combining Lemma 3.3 and Lemma 3.4 we prove that the closed ball in $\mathbb{R}^3$ is paradoxical. □
Mathematical Matches
**Younger Match — Problems**

1. Given are real numbers $a_1, a_2, a_3, \ldots, a_n$ $(n \geq 4)$ satisfying inequalities
   
   \[ a_1 + a_2 + \ldots + a_n \geq n \quad \text{and} \quad a_1^2 + a_2^2 + \ldots + a_n^2 \geq n^2. \]

   Prove that at least one of the numbers $a_1, a_2, \ldots, a_n$ is not less than 2.

2. Given are real numbers $a, b, c \geq 1$. Prove that
   
   \[ \frac{1}{\sqrt[3]{b+c+1}} + \frac{1}{\sqrt[3]{c+a+1}} + \frac{1}{\sqrt[3]{a+b+1}} \geq 1. \]

3. Let $a_1, a_2, \ldots, a_n$ be positive integers such that $\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n} = 1$. Prove that $a_1 \leq n^{2^n}$.

4. Two distinct positive integers $a, b$ are written on the board. The smaller of them is replaced with the number $\frac{ab}{a-b}$. This process is repeated as long as the two numbers are not equal. Prove that eventually the two numbers on the board will be equal.

5. An $n \times n$ matrix with integer entries has the following property: any two adjacent (vertical or horizontal) entries have the difference not greater than 1. Prove that there exists an integer that appears at least $n$ times in the matrix.

6. Prove that for any $n$ and $m > 1$ the set $\{1, 2, 3, \ldots, 2m\}$ can be split into $m$ pairs of numbers, so that no matter how we choose a representative from each of these pairs, the sum of the representatives isn’t equal to $n$.

7. Let $I$ be the incenter of a triangle $ABC$, $M$ — the midpoint of the side $AB$ and $W$ — the midpoint of the arc $BC$ of the circumcircle of $ABC$ not containing $A$. It is known that $\angle BIM = 90^\circ$. Find ratio $AI/IW$.

8. Let $ABC$ be an acute triangle with orthocenter $H$ and circumcenter $O$. Let $K$ be the midpoint of the segment $AH$. The line perpendicular to $BK$ passing through $K$ intersects the line $AC$ at $P$. Prove that $OP \parallel BC$.

9. Let $M$ be the midpoint of the hypotenuse $BC$ of a right triangle $ABC$. Let $\omega_1$ be the circle passing through $B, M$ and touching $AC$ at $X$. Similarly, let $\omega_2$ be the circle passing through $C, M$ and touching $AB$ at $Y$, where $X$ and $Y$ lie on the same side of the line $BC$. Prove that the line $XY$ passes through the midpoint of arc $BC$ of the circumcircle of $ABC$.

10. Let $a$ and $b$ be natural numbers such that $\frac{a+1}{b} + \frac{b+1}{a}$ is an integer. Show that the greatest common divisor of $a$ and $b$ is not greater than $\sqrt{a+b}$.

11. Find all polynomials $f$ with integer coefficients such that for every prime $p$ and every natural numbers $u$ and $v$ satisfying the condition $p\mid uv - 1$ it holds that $p \mid f(u)f(v) - 1$. 

\[ \Box \square \quad 76 \quad \square \Box \]
1. Let \( a_1, a_2, \ldots, a_n \) be real numbers. Prove that
\[
\prod_{i=1}^{n} (a_i^2 + n - 1) \geq n^{n-2} \left( \sum_{i=1}^{n} a_i \right)^2.
\]

2. Prove that every polynomial with real coefficients can be written as a sum of 2019 polynomials being 2019-th powers of polynomials with real coefficients.

3. Let \( p, q, n \) be positive integers with \( p+q < n \). Let \((x_0, x_1, \ldots, x_n)\) be an \((n+1)\)-tuple of integers satisfying the following conditions
   a) \( x_0 = x_n = 0 \);  b) for each \( i \) with \( 1 \leq i \leq n \), either \( x_i - x_{i-1} = p \), or \( x_i - x_{i-1} = -q \).
   Show that there exists a pair \((i, j)\) of distinct indices with \((i, j) \neq (0, n)\) such that \( x_i = x_j \).

4. An Aztec diamond of rank \( n \) is a figure consisting of those squares of a gridded coordinate plane lying entirely inside the diamond \( \{(x, y) : |x| + |y| \leq n+1\} \). For any covering of an Aztec diamond by dominoes \((1 \times 2 \text{ rectangles})\), we may rotate by 90° any 2 \times 2 \text{ square covered by exactly two dominoes. Prove that at most} \( \frac{1}{2} n (n+1)(2n+1) \text{ rotations are needed to transform an arbitrary covering into the covering consisting only of horizontal dominoes.} \)

5. We have the following system of boxes: in the bottom one there are 2 smaller boxes, in each of those boxes there are 2 smaller boxes and so on. In the \( n \)-th layer there are \( 2^n \) boxes each with a coin, which is either heads or tails. In each move we can choose any of those boxes and flip all the coins that are in it. Prove that regardless of the initial heads-tails layout of coins, we can perform at most \( n \) moves so that there will be the same number of heads and tails.

6. Let \( X \) be a point inside a triangle \( ABC \) such that \( XA \cdot BC = XB \cdot AC = XC \cdot AB \). Let \( I_1, I_2, I_3 \) be the incenters of the triangles \( XBC, XCA, XAB \), respectively. Prove that the lines \( AI_1, BI_2 \) and \( CI_3 \) are concurrent.

7. Let \( ABC \) be a triangle with \( AB = AC \). Let \( P, Q \) be points inside the triangle such that \( \angle BAP + \angle CAQ = \frac{1}{2} \angle BAC \). Moreover, it is known that \( BP = PQ = CQ \). Let \( AP \) intersect \( BQ \) at \( X \) and \( AQ \) intersect \( CP \) at \( Y \). Prove that the quadrilateral \( PQXY \) is cyclic.

8. Let the incircle of a triangle \( ABC \) with \( AB < AC \) be tangent to the sides \( BC, CA, AB \) at points \( D, E, F \), respectively. Let \( A \) and \( T \) be the intersection points of the circumcircles of triangles \( AEF \) and \( ABC \). The line perpendicular to the line \( EF \) passing through \( D \) meets side \( AB \) at \( X \). Prove that \( TX \perp TF \).

9. Let \( p \) be a prime and \( k \) be a positive integer. Set \( S \) consists of all positive integers \( a \) less than \( p \) such that there exists a natural number \( x \) such that \( x^k \equiv a \pmod{p} \). Suppose that \( 3 \leq |S| \leq p - 2 \). Prove that the elements of \( S \), when arranged in increasing order, do not form an arithmetic progression.

10. For every positive integer \( m \) denote by \( d(m) \) the number of positive divisors of a positive integer \( m \) and by \( \omega(m) \) the number of distinct prime divisors of \( m \). Let \( k \) be a positive integer. Prove that there exist infinitely many positive integers \( n \) such that \( \omega(n) = k \) and \( d(n) \) does not divide \( d(a^2 + b^2) \) for any positive integers \( a, b \) satisfying \( a + b = n \).
11. For each positive integer $n$ define $L(n)$ to be the number of integers $1 \leq a \leq n$ such that $n \mid a^n - 1$. Also, if $p_1, p_2, \ldots, p_k$ are all prime divisors of $n$, let $T(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$. Prove that

(a) $\varphi(n) \mid L(n)T(n)$ holds for each $n \in \mathbb{N}$;

(b) if $\gcd(n, T(n)) = 1$, then $\varphi(n) = L(n)T(n)$. 

□■□□
Older Match — Problems

1. Does there exist a sequence \( (a_n)_{n=1}^\infty \) of nonnegative real numbers such that \( \sum_{n=1}^\infty a_n < \infty \) and for each prime number \( p \) holds \( \sum_{k=1}^\infty a_{kp} = \frac{1}{p} \)?

2. Prove that for any integers \( n, p, 0 < n \leq p \), all the roots of polynomial \( P_{n,p} \) are real, where

\[
P_{n,p}(x) = \sum_{j=0}^n \binom{p}{j} \left( \frac{p}{n-j} \right) x^j.
\]

3. Call a nonempty set \( S \) of complex roots of 1 mango when the sum of all its elements is equal to 0. A mango set is minimal if its each nonempty subset is not mango. Prove that there are only finitely many minimal mango sets \( S \) for which \( 1 \in S \) and \( |S| = 2018 \).

4. On a school ball danced \( 2n \) girls and \( 2n \) boys. It is known that for any pair of girls the number of boys who danced with only one of them equals \( n \). Prove that for any pair of boys the number of girls who danced with only one of them equals \( n \).

5. In a chess tournament \( 2n+3 \) players take part. Every two play exactly once. The schedule is such that no two matches are played at the same time, and each player after taking part in a match is free in at least \( n \) next (consecutive) matches. Prove that one of the players who play in the opening match will also play in the closing match.

6. During the Night Criminal Game at MBL, suddenly all the lights went off, leaving the startled campers with \( k \) torches, each illuminating a sector of \( \frac{360}{k} \) degrees. Prove that they can rotate the torches (without moving them) in a way that the whole plane will be lit up.

7. Let \( M \) be the midpoint of the side \( BC \) of a triangle \( ABC \). Points \( E, F \) lie on the sides \( AB, AC \), respectively, in such a way that \( ME = MF \). Let the circumcircles of the triangles \( ABC \) and \( AEF \) intersect at \( A \) and \( P \). The tangents at \( E, F \) to the circumcircle of \( AEF \) intersect each other at \( K \). Prove that \( \angle KPA = 90^\circ \).

8. Let \( ABC \) be a triangle and \( A', B', C' \) be the midpoints of the sides \( BC, CA, AB \), respectively. Let \( P \) and \( P' \) be points such that \( PA = P'A' \), \( PB = P'B' \), \( PC = P'C' \). Prove that all lines \( PP' \) pass through a fixed point.

9. Rectangles \( ABA_1B_2, BCB_1C_2 \) and \( CAC_1A_2 \) lie outside triangle \( ABC \). Let \( C' \) be a point such that \( C'A_1 \perp A_1C_2 \) and \( C'B_2 \perp B_2C_1 \). Points \( A' \) and \( B' \) are defined analogously. Prove that the lines \( AA', BB' \) and \( CC' \) concur.

10. A cubic polynomial with integer coefficients has 3 pairwise distinct real roots \( u, v, w \not\in \mathbb{Q} \). Moreover, it is known that there exist integers \( a, b, c \) satisfying equality \( av^2 + bv + c = u \). Prove that the number \( b^2 - 2b - 4ac - 7 \) is a perfect square.

11. Let \( p \) be a prime, \( M = \{0, 1, \ldots, p-1\} \) and let \( a_i \in M \) for \( i = 1, \ldots, k \), where \( k < p \). Prove that there exist pairwise distinct elements \( x_1, x_2, \ldots, x_k \) of the set \( M \) such that the numbers \( a_1 + x_1, a_2 + x_2, \ldots, a_k + x_k \) are pairwise distinct modulo \( p \).
1. Suppose that \( a_i < 2 \) for all \( i \in \{1, 2, \ldots, n\} \). Assume that \( a_i > 2 - n \) for all \( i \in \{1, 2, \ldots, n\} \). Then

\[
0 > \sum_{i=1}^{n} (a_i - 2)(a_i + n - 2) = \sum_{i=1}^{n} (a_i^2 + (n-4)a_i - 2n + 4) = \\
= \sum_{i=1}^{n} a_i^2 + (n-4) \sum_{i=1}^{n} a_i - 2n(n-2) \geq n^2 + (n-4)n - 2n(n-2) = 0,
\]

which is a contradiction with problem’s conditions.

Therefore, there exists some \( i \in \{1, 2, \ldots, n\} \) for which \( a_i \leq 2 - n \). As a consequence

\[
a_1 + a_2 + \ldots + a_{i-1} + a_{i+1} + \ldots + a_n \geq 2(n-1).
\]

In other words, the arithmetic mean of numbers \( a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \) is not less than 2, which implies that one of these numbers is not less than 2.

2. From Bernoulli’s inequality we obtain

\[
(b+c+1)^2 \leq 1 + \frac{b+c}{a} = \frac{a+b+c}{a} \quad \Rightarrow \quad \frac{1}{\sqrt{b+c+1}} \geq \frac{a}{a+b+c}.
\]

Similarly, \( \frac{1}{\sqrt{c+a+1}} \geq \frac{b}{a+b+c} \) and \( \frac{1}{\sqrt{a+b+1}} \geq \frac{c}{a+b+c} \). Summing up these three inequalities proves the problem’s statement.

3. We prove that for each \( i \in \{1, 2, \ldots, n\} \) holds \( a_i \leq n^{2^n} \). Without loss of generality assume that \( a_1 \leq a_2 \leq \ldots \leq a_n \). It yields \( a_1 \leq n \). Note that the number

\[
a_1 a_2 \cdots a_i \cdot \left( \frac{1}{a_{i+1}} + \frac{1}{a_{i+2}} + \ldots + \frac{1}{a_n} \right)
\]

is a positive integer. Therefore, it’s greater than or equal to 1. It follows that

\[
a_1 a_2 \cdots a_i \cdot \frac{n-i}{a_{i+1}} \geq a_1 a_2 \cdots a_i \cdot \left( \frac{1}{a_{i+1}} + \frac{1}{a_{i+2}} + \ldots + \frac{1}{a_n} \right) \geq 1,
\]

so \( (n-i) \cdot a_1 a_2 \cdots a_i \geq a_{i+1} \) for each \( i \in \{1, 2, \ldots, n-1\} \).

Now, by induction we prove that for each \( i \in \{1, 2, \ldots, n\} \) holds \( a_i \leq n^{2^n-1} \). For \( i=1 \) the statement is clear, since \( a_1 \leq n \). Assume that the statement is true for all \( i \leq k < n \). Then

\[
a_{k+1} \leq (n-k) \cdot a_1 a_2 \cdots a_k \leq (n-k) \cdot n \cdot n^{2^1} \cdots n^{2^{k-1}} \leq n^{2^k},
\]

which finishes the proof.

4. Instead of keeping track of numbers \( x \) and \( y \) on the board that arise in the given procedure, let’s focus on \( x' := \frac{ab}{x} \) and \( y' := \frac{ab}{y} \). Note that if \( x < y \), then \((x, y)\) will be substituted with
Therefore, this process induces the Euclidean Algorithm on the second sequence of numbers (that is, if we have on the board \( x_1, x_2, \ldots \), then \( y_1, y_2, \ldots \) satisfying \( x_k y_k = ab \) follows the Euclidean Algorithm). This process starts from \( \frac{ab}{a} = b \) and \( \frac{ab}{b} = a \), i.e. from two integers, so it leads to a situation where two consecutive elements of the sequence are equal. This implies that the corresponding numbers on the board are equal, as required.

5. Let’s first note that the difference in values between two adjacent tiles is at most 1. It means that in every column each integer between the minimal and maximal entry of this column will be attained at least once.

Set \( a_k \) and \( b_k \) to be the minimum and maximum of the values written in the \( k \)-th column, respectively. Due to the remark above, we see that if \( \max_k a_k \leq \min_k b_k \), then \( m = \max_k a_k \) appears at least once in each column and as a result appears at least \( n \) times in the matrix. If \( \max_k a_k > \min_k b_k \), then there exist \( i, j \) such that \( b_i < a_j \). Again using the fact that the difference of numbers in adjacent cells is at most 1, we get that number \( b_i \) appears in each row at least once. Hence in each row the values in the \( i \)-th column and in the \( j \)-th column are not greater and greater than \( b_i \), respectively. Thus also in this case we obtain that \( b_i \) appears at least \( n \) times in the matrix, as desired.

6. Consider three splits:

\[
(1, m+1), \ (2, m+2), \ \ldots , \ (m−1, 2m−1), \ (m, 2m);
\]
\[
(1, m), \ (2, m+1), \ \ldots , \ (m−2, 2m−3), \ (m−1, 2m−2), \ (2m−1, 2m);
\]
\[
(1, m+2), \ (2, m+3), \ \ldots , \ (m−2, 2m−1), \ (m−1, 2m), \ (m, m+1).
\]

In the first split each possible sum is of the form \( \frac{m(m+1)}{2} + am \), where \( 0 \leq a \leq m \) is the number of chosen numbers greater than \( m \).

In the second split each possible sum is of one the forms

\[
\frac{m(m+1)}{2} + (b+1)(m−1) \quad \text{or} \quad \frac{m(m+1)}{2} + (b+1)(m−1)+1,
\]

where \( b \in \{0, \ldots, m−1\} \).

Finally in the third split all possible sums have one of the forms

\[
\frac{m(m+1)}{2} + c(m+1) \quad \text{or} \quad \frac{m(m+1)}{2} + c(m+1)+1,
\]

where \( c \in \{0, \ldots, m−1\} \).

Now we will prove that there is no triple \( a, b, c \) for which respective sums are equal. This would mean that for each \( n \) one of the splits above will have the desired property.
If such a triple existed, then \( m \) would divide \((b+1)(m-1)\) or \((b+1)(m-1)+1\). The first case leads to \( b = m - 1 \), and the second to \( b = 0 \). If \( b = m - 1 \), then \( c(m+1) = m(m-1) \) or \( c(m+1)+1 = m(m-1) \). None of these cases is possible, as \( m + 1 \) divides neither \( m(m-1) \) nor \( m(m-1)-1 \) for \( m > 1 \).

7. Firstly, we prove the following

**Four-leaf Clover Lemma.** Let \( I \), \( J \) be the centers of the incircle and the \( A \)-excircle of triangle \( ABC \), respectively. Let \( W \) be the midpoint of the arc \( BC \) of the circumcircle of triangle \( ABC \) not containing point \( A \). Then \( W \) is the circumcircle of \( BJCI \).

For the proof note that \( \angle JBI = \angle ICJ = 90^\circ \), so quadrilateral \( BJCI \) is inscribed. Denote by \( W' \) its center. Then, as \( J \) lies on the bisector of \( BAC \), we get that \( W' \) belongs to \( AI \). Moreover,

\[
\angle IW'B = 2 \cdot \angle ICB = \angle ACB = \angle IW'B,
\]

where the first equality follows from \( W' \) being the center of the circumcircle of \( BJCI \), whereas the last one — from cyclicity of \( ABWC \). Thus \( W = W' \).

Going back to the problem, we see that \( MI \) is parallel to \( BJ \), so as \( M \) is the midpoint of \( AB \) we deduce that \( MI \) is the midline of the triangle \( ABJ \). Consequently, \( I \) is the midpoint of the segment \( AJ \), so by the lemma \( \frac{AI}{IW} = \frac{2 \cdot AI}{IJ} = 2 \).

8. Denote by \( P' \) point on the side \( CA \) such that \( P'O \parallel BC \). We will prove \( BK \perp KP' \), which is equivalent to the statement.

Let \( R \) be point on \( BC \) such that \( P'R \perp BC \) and \( M \) be the midpoint of \( BC \). By definition of \( P' \) we obtain that quadrilateral \( OMRP' \) is a rectangle. It is a known fact that \( 2 \cdot OM = AH \). Hence, \( AK = KH = OM = P'R \), so quadrilaterals \( AKRP' \) and \( KHRP' \) are parallelograms.
Consequently, $KR \parallel AC$ and we obtain $BH \perp KR$. Thus, point $H$, as an intersection of two altitudes of triangle $BKR$, is its orthocenter. Therefore $RH \perp BK$, but as $RH \parallel KP'$ we get $BK \perp KP'$.

9. Let $S$ be the midpoint of arc $BC$ of the circumcircle of $ABC$ not containing $A$. Observe that

$$CX^2 = \text{Pow}_{\omega_1}(C) = CM \cdot CB = \frac{1}{2}BC^2,$$

so $CX = CS$. Similarly, we obtain $BX = BS$.

Therefore

$$\angle CSX + \angle YSB = \frac{180^\circ - \angle ACS}{2} + \frac{180^\circ - \angle SBA}{2} = 180^\circ - 90^\circ = \angle CSB,$$

where at the second equality we made use of the fact that $ABCS$ is an inscribed quadrilateral. Above equality implies the statement.

10. Let $a = dk$ and $b = dl$ where $d$ is the greatest common divisor of $a$ and $b$. Rewriting the statement in this terms, we need to prove that $d \leq k + l$. Since $\frac{a+1}{b} + \frac{b+1}{a}$ is an integer,

$$d^2kl \mid a^2 + b^2 + a + b \quad \Rightarrow \quad d^2kl \mid d^2k^2 + d^2l^2 + dk + dl \quad \Rightarrow \quad dkl \mid dk^2 + dl^2 + k + l.$$

This means that $d$ divides $k + l$ which in turn yields $d \leq k + l$.

11. Observe that $f$ cannot be the zero polynomial. Let $g(x) = x^n \cdot f\left(\frac{1}{x}\right)$, where $n$ is the degree of $f$. Note that $g$ is a polynomial with integer coefficients.

Fix a nonzero $u$ and consider any prime $p$ not dividing $u$. Denote by $v$ the reciprocal of $u$ modulo $p$. By problem’s conditions we get $p \mid f(u)f(v) - 1$ and therefore $p \mid f(u) \cdot u^n f(v) - u^n$, which yields $p \mid f(u)g(u) - u^n$. Each prime not dividing $u$ divides $f(u)g(u) - u^n$, so $f(u)g(u) = u^n$ for each $u \neq 0$. Since $f$ is a polynomial of degree $n$, and both $f$ and $g$ have integer coefficients, it follows that $f = x^n$ or $f = -x^n$.

Directly checking obtained solutions we conclude that all polynomials satisfying problem’s conditions have form $\pm x^n$ for $n \geq 0$. 
1. We are going to use the following fact, which can be easily proved by induction: if numbers \( x_1, x_2, \ldots, x_k \) are all of the same sign, then

\[
\prod_{i=1}^{n} (1 + x_i) \geq 1 + \sum_{i=1}^{n} x_i.
\]

Note that the given inequality can be rewritten as

\[
\prod_{i=1}^{n} \left( 1 + \frac{a_i^2 - 1}{n} \right) \geq \left( \frac{1}{n} \sum_{i=1}^{n} a_i \right)^2.
\]

Without loss of generality (possibly changing the numeration of the given numbers) assume that \( a_1, \ldots, a_k \geq 1 \) and \( a_{k+1}, \ldots, a_n \leq 1 \) and all \( a_i \) are nonnegative. From the invoked fact we then get

\[
\prod_{i=1}^{k} \left( 1 + \frac{a_i^2 - 1}{n} \right) \geq \frac{a_1^2 + \ldots + a_k^2 + n - k}{n} \quad \text{and} \quad \prod_{i=k+1}^{n} \left( 1 + \frac{a_i^2 - 1}{n} \right) \geq \frac{k + a_{k+1}^2 + \ldots + a_n^2}{n}.
\]

To end the solution it suffices to prove that

\[
(a_1^2 + \ldots + a_k^2 + n - k)(k + a_{k+1}^2 + \ldots + a_n^2) \geq \left( \sum_{i=1}^{n} a_i \right)^2,
\]

which is a direct application of Cauchy-Schwarz inequality to \( n \)-term sequences \((a_1, \ldots, a_k, 1, \ldots, 1)\) and \((1, \ldots, 1, a_{k+1}, \ldots, a_n)\).

2. Let \( \Delta(P(x)) = P(x+1) - P(x) \) and note that for every polynomial \( P \) with real coefficients and \( \deg P(x) > 0 \) we have \( \deg \Delta(P(x)) = \deg P(x) - 1 \). So there exist numbers \( b \neq 0 \) and \( c \), such that \( bx + c = \Delta^{2018}(x^{2019}) \) for every \( x \in \mathbb{R} \). Plugging \( x = \frac{P(t) - c}{b} \) yields

\[
P(t) = \Delta^{2018} \left( \left( \frac{P(t) - c}{b} \right)^{2019} \right)
\]

and the expression on the right-hand side is a sum of 2019 polynomials, each of them being a 2019-th power of other polynomial.

3. Note that w.l.o.g., we can assume that \( p \) and \( q \) are coprime. Indeed, otherwise it suffices to consider the problem in which all \( x_i \)'s and \( p, q \) are divided by \( \gcd(p, q) \).

Let \( k, l \) be the numbers of indices \( i \) with \( x_{i+1} - x_i = p \) and the number of those \( i \) with \( x_{i+1} - x_i = -q \) (where \( 0 \leq i < n \)). From \( x_0 = x_n = 0 \) we get \( kp = lq \), so for some integer \( t > 1 \), \( k = qt \), \( l = pt \), and \( n = (p+q)t \).

Consider the sequence \( y_i = x_{i+p+q} - x_i \), \( i = 0, \ldots, n-p-q \). We claim that at least one of \( y_i \)'s equals zero. We begin by noting that each \( y_i \) is of the form \( up - vq \), where \( u+v = p+q \); therefore

\[
y_i = (u+v)p - v(p+q) = (p-v)(p+q)
\]
is always divisible by \( p+q \). Moreover,

\[
y_{i+1} - y_i = (x_{i+p+q+1} - x_{i+p+q}) - (x_{i+1} - x_i)
\]
is 0 or \( \pm(p+q) \). We conclude that if no \( y_i \) is 0 then all \( y_i \)'s are of the same sign. But this is in contradiction with the relation \( y_0 + y_{p+q} + \ldots + y_{n-p-q} = x_n - x_0 = 0 \). Consequently some \( y_i \) is zero, as claimed.

4. Let's first note that regardless of the current layout of dominoes in the Aztec diamond we can perform a sequence of moves that reduces the number of vertical dominoes by 2 (provided it is not equal to 0).

Let's consider the highest row in which there are vertical tiles. Since each row has an even number of squares, it follows that there must be an even number of vertical tiles intersecting it. Let's choose some two of them so that all the tiles between them (in the given row, not necessarily in the one below) are horizontal. Looking at the row below between those tiles, we again see that the number of vertical tiles there must be even (but can be 0).

Therefore again we obtain two vertical tiles with only horizontal tiles in the top row between them but closer to each other. Proceeding this way, we finally we get two vertical tiles with only horizontal tiles between them in both rows. Call such a pair a sandwich.

Suppose now that there are \( 2k \) horizontal tiles between the tiles forming a sandwich. Using \( k \) operations we can turn all the horizontal tiles between them into vertical ones and then pairing the vertical tiles so that the sandwich tiles are included, we can make \( k+1 \) operations to make all these tiles horizontal, thus reducing the number of vertical tiles in the Aztec Diamond by 2.

Using this strategy, all the vertical tiles will be paired into sandwiches and eventually got horizontal. The only thing it suffices to show is that the number of moves using this strategy is at most \( \frac{1}{6}n(n+1)(2n+1) \).

We have already seen that the number of moves required (using our strategy) to make a sandwich with \( 2k \) tiles in-between horizontal is \( 2k+1 \). Therefore, the number of operations required to make all the tiles horizontal is bounded above by the half of the sum of the distances between the centers of the cells of sandwich tiles in each row.

**Lemma.** The sum of the distances between the cells of sandwich tiles in a single row of length \( 2k \) is bounded above by \( k^2 \).

**Proof.** We get that this sum equals

\[
(b_1 - a_1) + (b_2 - a_2) + \ldots + (b_l - a_l) = (b_1 + b_2 + \ldots + b_l) - (a_1 + a_2 + \ldots + a_l),
\]

where \( a_i, b_i \in \{1, 2, \ldots, 2k\} \) are positions of tiles of the \( i \)-th sandwich. We see that this is maximized when \( \{b_1, b_2, \ldots, b_n\} = \{k+1, k+2, \ldots, 2k\} \) and \( \{a_1, a_2, \ldots, a_n\} = \{1, 2, \ldots, k\} \) and then this sum equals

\[
(k+1-k) + (k+2-(k-1)) + \ldots + (2k-1) = 1 + 3 + 5 + \ldots + (2k-1) = k^2.
\]

Hence indeed the sum of the distances is bounded above by \( k^2 \). \( \square \)

We see that our algorithm will terminate in at most \( 1^2 + 2^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1) \) moves as required.
5. Let’s define the *deficit* of the layout of coins to be the difference of the number of heads and tails. Since the number of all coins in the bottom box is even, then at each time deficit is an even number. We will prove that in each move we can make an operation that divides the absolute value of current deficit $|d|$ by at least 2, which would imply the desired result.

Without loss of generality we may assume that $d > 0$, which implies $d \geq 2$. Suppose by a contradiction that there exists a layout of coins such that no operation would divide the deficit $d$ by 2. Let’s note that if $d'$ is a deficit of some box, then after switching all the coins in it, the deficit becomes $d - 2d'$. Since $|d - 2d'| > \frac{d}{2}$, we obtain that $d' < \frac{d}{4}$ or $d' > \frac{3d}{4}$.

Observe that in all boxes with just one coin deficit is equal 1 or $-1$, so for them holds $d' < \frac{d}{4}$. However, let’s note that if we have a box such that both boxes inside it satisfy $d' < \frac{d}{4}$, then its deficit is smaller than $\frac{d}{2}$ and as an effect we get that it also has to satisfy $d' < \frac{d}{4}$.

Therefore, we obtain that all the boxes except for the biggest one must satisfy $d' < \frac{d}{4}$ and hence the biggest box has the deficit satisfying $d < \frac{d}{4}$, which is impossible. Hence indeed it follows that we can make even number of heads and tails in just $n$ operations.

6. By Desergues’s theorem, to prove that $AI_1, BI_2, CI_3$ concur it is enough to show that intersections of pairs of lines $I_2I_3$ with $BC$, $I_3I_1$ with $CA$ and $I_1I_2$ with $AB$ are collinear.

Denote by $P$ the intersection point of the bisector of angle $XBA$ with line $AX$. By the angle bisector theorem we get

$$\frac{AP}{PX} = \frac{AB}{BX} = \frac{AC}{CX},$$

so $P$ also lies on the bisector of angle $ACX$. Let $K$ be the intersection point of $I_2I_3$ with $BC$. By Menelaus theorem for $BPC$:

$$\frac{BK}{KC} = \frac{BI_3}{I_3P} \cdot \frac{PI_2}{I_2C} = (*) .$$

Since $I_3$ lies on the bisector of angle $BAX$ and $I_2$ lies on the bisector of angle $XAC$, we get

$$(*) = \frac{BA}{AP} \cdot \frac{PA}{AC} = -\frac{BA}{AC} \implies \frac{BK}{KC} = -\frac{BA}{AC} .$$

Points $L$ and $M$ can be defined in a similar manner to get $\frac{CL}{LA} = -\frac{CB}{BA}$ and $\frac{AM}{MB} = -\frac{AC}{CB}$. Finally, by acquired equalities the collinearity of $K$, $L$, $M$ follows from Menelaus theorem.
7. Denote by $D$ the reflection of $B$ in line $AP$. By the conditions of the problem we see that $\angle DAQ = \angle CAQ$ and $AD = AB = AC$, so $D$ is also the reflection of $C$ in line $AQ$. Moreover, $\angle PDX = \angle XBP = \angle PQX$, where the first equality is a conclusion from the symmetry, whereas the second one follows from $BP = PQ$. Thus point $X$ belongs to the circumcircle of triangle $PDQ$. Similarly, $Y$ also lies on this circumcircle, which finishes the proof.

8. We will make use of the following

Lemma. Denote by $M$ the midpoint of the arc $BC$ of the circumcircle of $ABC$ not containing $A$. Then points $T$, $D$, $M$ are collinear.

Proof. Consider an inversion at $M$ with radius $MB = MI = MC$, where $I$ is the center of the incircle of triangle $ABC$. Under this transformation, the image of the circumcircle of $ABC$ is line $BC$, so the image of $T$ belongs to $BC$. Moreover, the image $A'$ of $A$ also lies on $BC$, and $I$ maps to $I$. As $AI$ is the diameter of the circumcircle of $AEFT$, $D'I$ is the diameter of the image of the circumcircle of $AEFT$. Therefore $D$ belongs to the image of this circle. Consequently, the image of $T$ is $D$, so $T$, $D$ and $M$ are collinear.

Now, let $Y$, $G$ be intersection points of line $DX$ with lines $AC$, $EF$, respectively. Note that $\angle BTD = \angle BTM = \angle BAM = \angle BXD$, so points $B$, $D$, $G$, $T$ are concyclic. Thus, since $T$ lies on the circumcircle of triangle $ABC$, it is Miquel point for lines $CY$, $YX$, $XB$ and $BC$. Therefore, $T$ lies also on the circumcircle of triangle $AXY$. Consequently, since it belongs to the circumcircle of triangle $AEF$, it is also

□■□■ 87 □■■■
Miquel point for lines $EY$, $YX$, $XF$ and $FE$. Then $T$ belongs to the circumcircle of triangle $XGF$. But as $\angle XGF = 90^\circ$ it implies $\angle XTF = 90^\circ$, which completes the solution.

9. We proceed by contradiction. For $p = 2, 3$ the inequality in the statement cannot hold, so assume $p > 3$. Note that $S$ is a subgroup of a cyclic group $\mathbb{Z}_p^\times$, which implies that $S$ is also cyclic. Therefore we can write $S = \{g^0, \ldots, g^{d-1}\}$ modulo $p$ for $g \in \{2, 3, \ldots, p-2\}$, where $d$ properly divides $p-1$. Then, as $g \not\equiv \pm 1$, we get

$$\sum_{s \in S} s \equiv g^0 + \ldots + g^{d-1} = \frac{g^d - 1}{g - 1} \equiv 0 \mod p,$$

$$\sum_{s \in S} s^2 \equiv g^0 + \ldots + g^{2(d-1)} = \frac{g^{2d} - 1}{g^2 - 1} \equiv 0 \mod p.$$ 

Since elements of $S$ form in some arrangement an arithmetic sequence, hence we may assume $S = \{1, 1+k, \ldots, 1+(d-1)k\}$ mod $p$ for some positive $k < p-1$. Observe that

$$\sum_{s \in S} s = \sum_{i=0}^{d-1} (1+ik) = d + \frac{d(d-1)}{2} k,$$

$$\sum_{s \in S} s^2 = \sum_{i=0}^{d-1} (1+ik)^2 = d + d(d-1)k + \frac{d(d-1)(2d-1)}{6} k^2.$$ 

Both of above sums are 0 mod $p$, which implies

$$1 + \frac{d-1}{2} k \equiv 1 + (d-1)k + \frac{(d-1)(2d-1)}{6} k^2 \equiv 0 \mod p.$$ 

Then $1 \equiv -\frac{d-1}{2} k$, which inserted to the second equality yields

$$k^2 \left( \frac{(d-1)^2}{4} - \frac{(d-1)^2}{2} + \frac{(d-1)(2d-1)}{6} \right) \equiv 0 \mod p.$$ 

This means

$$\frac{d-1}{4} - \frac{d-1}{2} + \frac{2d-1}{6} \equiv 0 \mod p \quad \Rightarrow \quad d \equiv p-1 \mod p,$$

which is a contradiction with the initial assumption.

10. Take $n = 2^{p-1} \cdot 3^1 \cdot 5^1 \cdots q_k$, where $q_k$ is the $k$-th prime number and $p$ is a sufficiently large prime. Then $\omega(n) = k$ and $d(n) = 2^{k-1}p$.

Now

$$d(n) \mid d\left(a^2 + b^2\right) \Rightarrow d\left(a^2 + b^2\right) \Rightarrow Q^{p-1} \mid a^2 + b^2$$

for some prime number $Q$. Thus

$$Q^{p-1} \leq a^2 + b^2 \leq (a+b)^2 = n^2 = 4^{p-1} \cdot 3^2 \cdot 5^2 \cdots q_k^2.$$ 

Now if $Q > 4$, then by taking sufficiently large $p$ we get a contradiction. Thus $Q = 2$ or $Q = 3$.

If $Q = 3$, then

$$3^{p-1} \mid a^2 + b^2 \quad \Rightarrow \quad 3^{p-1} \mid a^2, b^2$$
as $-1$ is not a quadratic residue modulo $3$. But then

$$3^{\frac{n-1}{2}} \mid a,b \implies 3^{\frac{n-1}{2}} \mid a+b = n$$

which is a contradiction if $p$ is sufficiently large.

Thus $Q = 2$ so

$$2^{p-1} \mid a^2 + b^2 \implies 2^{p-1} \mid a^2, b^2$$

as $-1$ is not a quadratic residue modulo $4$ (and $p$ is sufficiently large). Thus $2^{\frac{p-1}{2}} \mid a, b$. Hence we can write $a = 2^{\frac{p-1}{2}} \alpha$, $b = 2^{\frac{p-1}{2}} \beta$, where $\alpha + \beta = 2^{\frac{p-1}{2}} \cdot 3 \cdot 5 \cdots q_k$ — note that $\alpha + \beta$ is even. Then $a^2 + b^2 = 2^{p-1} (\alpha^2 + \beta^2)$.

Now as $\alpha + \beta$ is even, so is $\alpha^2 + \beta^2$, and furthermore the largest power of $2$ that can possibly divide $\alpha^2 + \beta^2$ is $2^p-1$. Thus $a^2 + b^2 = 2^{p+x} \cdot s$ where $s$ is odd and $0 \leq x \leq p-2$. Therefore we get $d (a^2 + b^2) = (p+x+1) d (s)$. So

$$d(n) | d (a^2 + b^2) \implies 2^{k-1} p | (p+x+1) d (s).$$

But as $0 \leq x \leq p-2$, we have that numbers $p$ and $p+x+1$ are coprime. Thus $p | d (s)$ so exists some odd prime $R$ such that $R^{p-1} \mid s$.

But

$$s = \frac{a^2 + b^2}{2^p + x} \leq \frac{a^2 + b^2}{2^p} \leq \frac{n^2}{2^p} = 2p-2 \cdot 3^2 \cdot 5^2 \cdots q_k^2.$$

By making $p$ sufficiently large we get a contradiction with the existence of $R$, which finishes the proof.

11. (a) In general, in a finite abelian group, if $t \mid |G|$, then the number of elements $x$ such that $x^t = 1$ is a multiple of $t$. We apply this to the group $G = (\mathbb{Z}/n\mathbb{Z})^\times$ of invertible residues modulo $n$ with $t = (n, \varphi (n))$.

If $n = p_1^{a_1} \cdots p_k^{a_k}$, then by the above, $p_1^{a_1-1} \cdots p_k^{a_k-1} \mid (n, \varphi (n)) = L(n)$ (*) After multiplying the leftmost and the rightmost terms in (*) by $T(n)$ we get $\varphi(n) | L(n) T(n)$.

(b) In this case, $a^n = 1$ (in the group $G$) iff $a^{\varphi(n) / T(n)} = 1$ (#). $G$ is the direct product of a group of order $\varphi(n) / T(n)$ and one of order $T(n)$, and these orders are coprime. This means that the solutions to (#) are precisely the elements of the former group, so there are $\varphi(n) / T(n)$ of them. The desired result follows.
1. Yes, there exists such a sequence. Define for $i \geq 1$

\[ a_i = \begin{cases} 
\frac{1}{p_n} - \frac{1}{p_{n+1}}, & \text{for } i = p_1p_2 \ldots p_n, \\
0, & \text{in the other case},
\end{cases} \]

where $p_n$ is the $n$-th prime number. We see that $\sum_{n=1}^{\infty} a_n = \frac{1}{2} < \infty$ and for each prime $p_m$ holds

\[ \sum_{k=1}^{\infty} a_{kp_m} = \left( \frac{1}{p_m} - \frac{1}{p_{m+1}} \right) + \left( \frac{1}{p_{m+1}} - \frac{1}{p_{m+2}} \right) + \ldots = \frac{1}{p_m}. \]

2. We start with the following

Lemma 1. Let $c$ be a real number and $f$ be a polynomial with real coefficients having only real roots. Then polynomial $f' - cf$ has also only real roots.

Proof. Consider $g(x) = e^{-cx}f(x)$ and let $\deg f = n$. Note that $g$ has $n$ real roots (counting multiplicities). Then

\[ g'(x) = e^{-cx}f'(x) - ce^{-cx}f(x) = e^{-cx}(f'(x) - cf(x)). \]

Let $x_1 < x_2 < \ldots < x_k$ be different roots of $g$. Note that if $x_i$ is a root of $g$ with multiplicity $m_i$, then $x_i$ is a root of $g'$ with multiplicity $m_i - 1$. Moreover, by Rolle’s theorem, in each interval $(x_i, x_{i+1})$ for $i = 1, 2, \ldots, k - 1$ lies some root of $g'$. Therefore $g'$ has at least $n - 1$ real roots (counting multiplicities), thus polynomial $f' - cf$ has at least $n - 1$ real roots as well. Its degree is at most $n$, so all its roots are real, as desired.

Lemma 2. Let $f = a_nx^n + \ldots + a_0$ and $g$ be polynomials with real coefficients such that all their roots are real. Then all roots of polynomial

\[ h(x) = a_ng^{(n)} + a_{n-1}g^{(n-1)} + \ldots + a_1g' + a_0g \]

are real.

Proof. Let $x_1, x_2, \ldots, x_n$ be all roots of $f$. Applying lemma 1. for $g$ and $c = x_1$, we get that all roots of polynomial $h_1 = g' - x_1g$ are real. Applying lemma 1. for $h_1$ and $c = x_2$ we get that all roots of polynomial $h_2 = g'' - (x_1 + x_2)g' + x_1x_2g$ are real. Repeating this process $n - 2$ times more we obtain that all roots of polynomial

\[ h_n = g^{(n)} - \left( \sum_{1 \leq i \leq n} x_i \right) g^{(n-1)} + \left( \sum_{1 \leq i < j \leq n} x_ix_j \right) g^{(n-2)} + \ldots + (-1)^nx_1 \ldots x_ng \]

are real. But by Vieta’s formulas $h = a_nh_n$, which means that all roots of $h$ are real.

Applying lemma 2. for polynomials $(1+x)^p$ and $x^n$ we get that all roots of polynomial

\[ h(x) = \sum_{j=0}^{p} \binom{p}{j} \cdot (x^n)^{(j)} = \sum_{j=0}^{p} \binom{p}{j} \frac{n!}{(n-j)!}x^{n-j} \]

□■□■ □□□□
are real. Therefore, applying lemma 2. for polynomials \( h \) and \( x^p \) we obtain that all roots of polynomial
\[
\sum_{j=0}^{n} \binom{p}{j} \frac{n!}{(n-j)!} \cdot (x^p)^{(n-j)} = n! \sum_{j=0}^{n} \binom{p}{j} \binom{p}{n-j} x^{p-n+j}
\]
are real, which yields the statement.

3. Let \( S \) be a minimal mango set satisfying problem’s condition and set \( n \) to be the least number such that each element of \( S \) raised to the \( n \)-th power is equal to 1.

Firstly, we will prove that \( n \) is squarefree. Suppose that \( n = kp \), where \( p \mid k \) and \( p \) is a prime. For each \( t \), let \( \omega_t := e^{2\pi i/t} \). Note that \( S \subset \mathbb{Q}[\omega_n] \). Since cyclotomic polynomials are irreducible over \( \mathbb{Q} \), we get \([\mathbb{Q}[\omega_t] : \mathbb{Q}] = \phi(t)\). By Tower Law we obtain
\[
[\mathbb{Q}[\omega_n] : \mathbb{Q}[\omega_t]] = \frac{[\mathbb{Q}[\omega_n] : \mathbb{Q}]}{[\mathbb{Q}[\omega_t] : \mathbb{Q}]} = \frac{\phi(n)}{\phi(t)} = p.
\]

Let \( B = \{1, \omega_n, \omega_n^2, \ldots, \omega_n^{p-1}\} \). Note that \( 1, \omega_n, \omega_n^2, \ldots, \omega_n^{n-1} \) span \( \mathbb{Q}[\omega_n] \) as a \( \mathbb{Q} \)-vector space. Since for any \( l \) we can write \( \omega_n^l = \omega_n^{pi + j} = (\omega_n^p)^i \omega_n^j = \omega_n^i \omega_n^j \), so \( B \) spans \( \mathbb{Q}[\omega_n] \) as a \( \mathbb{Q}[\omega_k] \)-vector space and each \( n \)-th root of unity is a one-element linear combination of elements from \( B \).

Set \( B \) has \( p \) elements, so as \( [\mathbb{Q}[\omega_n] : \mathbb{Q}[\omega_t]] = p \), we get that \( B \) is a basis of \( \mathbb{Q}[\omega_n] \) over \( \mathbb{Q}[\omega_k] \).

Writing each element of \( S \) as one-element linear combination of elements from \( B \) with coefficients from \( \mathbb{Q}[\omega_k] \), we get that
\[
0 = \sum_{s \in S} s = a_0 + a_1 \omega_n + a_2 \omega_n^2 + \ldots + a_p \omega_n^{p-1}, \quad \text{with } a_i \in \mathbb{Q}[\omega_k].
\]

Since \( B \) is a basis we conclude \( a_0 = a_1 = \ldots = a_{p-1} = 0 \), so in particular \( a_0 = 0 \). Therefore the subset \( S' \) of \( S \) consisting only of elements in \( \mathbb{Q}[\omega_k] \) forms a mango set (it is nonempty as \( 1 \in S \)). Since \( S \) is minimal we conclude \( S' = S \). It means that each element of \( S \) is \( k \)-th root of unity, which is a contradiction with the assumption about minimality of \( n \). Therefore \( n \) is square-free.

Now we will prove that \( n \) can’t have large prime divisors. Suppose that \( n = pm \), where \( p > 2018 \) is a prime. Then as \( n \) is square-free we get
\[
[\mathbb{Q}[\omega_n] : \mathbb{Q}[\omega_m]] = \frac{[\mathbb{Q}[\omega_n] : \mathbb{Q}]}{[\mathbb{Q}[\omega_m] : \mathbb{Q}]} = \frac{\phi(n)}{\phi(m)} = p - 1.
\]

In the same manner as before, we have
\[
0 = \sum_{s \in S} s = a_0 + a_1 \omega_n + a_2 \omega_n^2 + \ldots + a_{p-1} \omega_n^{p-1}, \quad \text{with } a_0, a_1, \ldots, a_{p-1} \in \mathbb{Q}[\omega_m].
\]

If \( a_i = 0 \) for some \( i \), then
\[
a_0 + a_1 \omega_n + a_2 \omega_n^2 + \ldots + a_{i-1} \omega_n^{i-1} + a_{i+1} \omega_n^{i+1} + \ldots + a_{p-1} \omega_n^{p-1} = 0.
\]

As set \( 1, \omega_n^1, \ldots, \omega_n^{i-1}, \omega_n^{i+1}, \ldots, \omega_n^{p-1} \) forms a basis for vector space \( \mathbb{Q}[\omega_n] \) over \( \mathbb{Q}[\omega_m] \), we obtain that \( a_0 = \ldots = a_{p-1} = 0 \), so subset \( S' \) of \( S \) consisting of elements from \( \mathbb{Q}[\omega_m] \) is mango set. Since \( S \)
is minimal, then $S' = S$. Consequently, each element of $S$ is $m$-th root of unity, which contradicts minimality of $n$.

Thus $a_i 
eq 0$ for all $0 \leq i < p$. This means that for each $i$ there is at least one element of $S$ contributing to $a_i$. This yields that $S$ has at least $p > 2018$ elements, which is impossible.

Therefore, we obtain that if $S$ is minimal mango set and $n$ is minimal number such that $S \subseteq \mathbb{Q}[\omega_n]$, then $n$ divides the product of all prime numbers less than 2018. However, there are only finitely many roots of unity in $\mathbb{Q}[\omega_{2018}]$, so as well finitely many subsets of them. This concludes the proof.

4. Let’s consider $2n \times 2n$ matrix $A = (a_{ij})$, where $a_{ij} = 1$ if girl $i$ danced with boy $j$ and $a_{ij} = -1$ in the other case. In this setup the problem’s conditions yield that for any $k, l$ there are exactly $n$ $j$’s such that $a_{kj}a_{lj} = 1$ and $n$ other $j$’s such that $a_{kj}a_{lj} = -1$. This means that rows of $A$ are mutually orthogonal, so $AA^T = 2nI$. Then $A^T A = 2nI$, which considered in the same manner as above is the problem’s statement.

5. Let’s note that in any $n+3$ consecutive matches exactly 3 players played twice. Indeed, due to the condition that everyone needs to rest for at least $n$ matches and no pair of people played with each other twice, we obtain that $2n+2$ different players played in any $n+1$ consecutive days. Since the match in $(n+2)$-nd day couldn’t be the same as the first one, then the $(2n+5)$-th player played in it and exactly one player from the first match played in $(n+2)$-nd day and one in $(n+3)$-rd day.

We will prove that there is a player that always rested $n+1$ days. This would imply that the difference between his last and first game is $(2n+1)(n+2) = 2n^2 + 5n + 2 = \left(\frac{2n+3}{2}\right)^2 - 1$ which would in turn imply that he has played in the first and the last match. Suppose contrary. Let $X$ be the player that was the last person to have a break of exactly $n$ consecutive matches. Let $Y$ be the player that he encountered during his match after first break of $n$ matches.

Note that $Y$ must have had only breaks of length $n+1$ matches before this match. Indeed, if he had break of $n$ matches and then $k$ breaks of $n+1$ matches, then $X$ and $Y$ must have met $n+1+k(n+2)$ before the match we’ve already considered. However, this means that $Y$ had his break of $n$ consecutive matches later than $X$, contradicting the assumption about him. This proves that indeed there is a player that played in the first and the last match of the tournament.

6. We start with the following

Lemma. Let $A$, $O$, $B$ be points such that $\angle AOB = k\alpha$, where $\alpha = \frac{2\pi}{n}$. Denote by $A'$, $B'$ points symmetric to $A$, $B$ in $O$, respectively. Call $X$ the sector bounded by angle $AOB$ and $Y$ the sector symmetric to $X$ in $O$. Suppose there are $k$ campers in the sector $X$ with torches illuminating sector of angle $\alpha$. Then we can arrange campers’ torches in order to illuminate sector $Y$.

Proof. We will proceed by induction on $k$. The case of $k = 1$ is clear. Let $M$ be the camper that is the closest to the ray $OB$ (and among such the one furthest from $O$). Rotate the torch of $M$ in such a way that one side of its light is parallel to $OB$ and it illuminates at least some part of $Y$. Due to the definition of $M$ we can apply the inductive hypothesis for $k-1$ points in the sector bounded by lines $OA$ and $m$, where $m$ is the side of $M$’s light not parallel to $OB$. Hence the result follows.
If $k$ is even, then there is a line that splits the campers into two equinumerous parts (if some campers stay on the line, then we can choose arbitrarily to which part we want assign each of them). Applying the lemma with sector of angle $\pi$, we get that we can adjust the lights of the campers in such a way that each of the halves of the plane illuminates the other half, thus illuminating the whole plane.

Assume $k$ is odd. Consider the convex hull of campers and let $A$ be some vertex of it (which is simultaneously a camper). Let $m$ be line passing through $A$, which splits other campers into two equinumerous groups. Let $m'$ be the ray of $m$ rooted at $A$ intersecting the convex hull of campers and $m''$ — the ray of $m$ rooted at $A$ not intersecting the convex hull. Rotate torch at $A$ in such a way that $m'$ is a bisector of sector illuminated by $A$. Denote by $n$, $l$ the sides of this sector. Note that the lemma yields that one group of campers can illuminate sector bounded by $m''$ and $n$, and the other group — sector bounded by $m''$ and $l$. Therefore campers can illuminate the whole plane, as desired.

7. Lemma. Let $H$ be the orthocenter of a triangle $ABC$. Denote by $M$ the midpoint of $BC$ and let the circle of diameter $AH$ intersect the circumcircle of $ABC$ for the second time at $P$. Then $\angle MPA = 90^\circ$.

Proof. Let $H'$ be the reflection of $H$ in $M$. Then $AH'$ is a diameter of the circumcircle of $ABC$, so $\angle H'PA = 90^\circ = \angle HPA$. Thus $P$ lies on the line $HH'$. As $M$ is the middle of $HH'$, then $M$, $H$, $P$ are collinear and consequently $\angle MPA = \angle HPA = 90^\circ$.

Denote by $N$ the midpoint of $EF$. Let $X$ and $Y$ be points on $AB$, $AC$, respectively, such that $XF \perp AC$ and $YE \perp AB$. Observe that a quadrilateral $XYFE$ is inscribed with a diameter $XY$. As $\angle XEK = \angle AFE = \angle YXE$, then $EK$ intersects $XY$ at the midpoint. Similarly, $FK$ intersects $XY$ at the midpoint, thus $K$ is the midpoint of $XY$. Note that $N$, $K$, $M$ are collinear.

As $P$ is the intersection of circumcircles of $AEF$ and $ABC$, then $P$ is the center of spiral similarity $\phi$, such that $\phi(BE) = CF$. Let $X' = \phi(X)$. Let $K'$ be the midpoint of $XX'$. By properties of spiral similarity, we know that points $N$, $M$, $K'$ are collinear. We claim $X'=Y$. If not, then $K' \neq K$ and therefore $KK' \parallel XY$, so $NM \parallel FC$ and hence $BE \parallel CF$, which is impossible. Consequently, $\phi(X) = Y$.

Thus, circumcircle of $AXY$ passes through $P$ and by the lemma we conclude $\angle KPA = 90^\circ$. 

\[\square\]
8. Denote by $\omega$ the circumcircle of triangle $ABC$. Consider a homothety transforming $A'B'C'$ to $ABC$ and denote by $Q$ the image of $P'$. Then

$$QA = 2PA, \quad QB = 2PB \quad \text{and} \quad QC = 2PC,$$

so $\omega$ is the Appolonian circle for points $Q$, $P$ with ratio 2. Therefore $PQ$ passes through the circumcenter $O$ of $ABC$. Let denote by $X$ and $Y$ intersections of $PQ$ with $\omega$, where $X$ lies between $P$, $Q$ and let $PX = 1$. Then $XQ = 2$ and $PY = 3$ as $\omega$ is the Appolonian circle of $Q$ and $P$ with ratio 2. Since $O$ is the midpoint of $XY$, then $PO = 1$ and $PQ = 3$.

Let $M$ be the centroid of $ABC$ and $S$ be the intersection of $PP'$ and $MO$. By Menelaos theorem for triangle $QMO$ and line $PP'$ we get

$$-1 = \frac{MP'}{PP'} \cdot \frac{QP}{PO} \cdot \frac{OS}{SM} = -\frac{1}{3} \cdot 3 \cdot \frac{OS}{SM} \quad \Rightarrow \quad \frac{OS}{SM} = 1.$$

Therefore each line $PP'$ passes through the midpoint of $OM$, which is a fixed point.

9. Firstly, we will prove that $B'C' \parallel C_1B_2$. Denote by $k$, $l$ lines $B_2C'$, $C_1B'$ and by $b$, $c$ lines $BC_2$, $CB_1$, respectively. Let $\phi$ be a projective transformation of line $k$ to $l$, which is a composition of the following projective transformations:

(a) a projection of range $b$ onto pencil $A_1$,
(b) a rotation of pencil $A_1$ about $90^\circ$,
(c) a projection of pencil $A_1$ onto range $b$,
(d) a projection of range $b$ onto range $c$ through the direction of $BC$, (so just translation of vector $BC$),
(e) a projection of range $c$ onto pencil $A_2$,
(f) a rotation of pencil $A_2$ about $90^\circ$,
(g) a projection of pencil $A_2$ onto range $l$.

By definition $\phi(C') = B'$, so if we proved that $\phi$ is just a translation of vector $B_2C_1'$ (so in terms of projective transformations — a projection of range $k$ onto range $l$ through the direction of $B_2C_1$), then we would be done. But each projective transformation of 2-dimensional object is determined by giving values on 3 arguments, so to prove that $\phi$ is a translation it’s enough to prove that it’s a translation for 3 arguments (i.e. points). Let’s do so.

By definition of $\phi$ we get $\phi(B_2) = C_1$, so clearly $C_1$ is a translation of $B_2$ of a vector $B_1C_2$.

Now, let $X$ be a point on $k$ such that $XA_1 \parallel BC$ and let $Y = \phi(X)$. Hence, by definition of $\phi$, $YA_2 \parallel BC$. Let $Z$ be a point $BC$ such that $AZ \parallel B_2X \parallel C_1Y$. Observe that triangles $ABZ$ and $B_2A_1X$ are congruent as they have parallel sides and $AB = B_2A_1$, which implies $B_2X = AZ$. Similarly, triangles $ACZ$ and $C_1A_2Y$ are congruent and thus $AZ = C_1Y$. Therefore $B_2X = C_1Y$ and so we see that $XY = B_2C_1$.

Let $P$ be the direction of $B_2C'$. Denote by $K$ a point on $b$ such that $KA_1 \perp B_2C'$ and let $L$ be a point on $c$ such that $CL = BK$. If we proved that $A_2L \perp C_1Y$ then we would obtain $\phi(P) = P$ and
hence $P$ would be the third needed point. Let $S$ be point on $B_2C_1$ such that $AS \parallel B_2C'$. Then triangles $A_1KB$ and $B_2SA$ are congruent as they have parallel sides and $A_1B = B_2A$. Hence $BK = AS$. Thus triangles $C_1SA$ and $A_2LC$ are also congruent since they $AS = CL$, $AC_1 = CA_2$ and $C_1A \parallel A_2C$ and $AS \parallel CL$. It yields $A_2L \parallel C_1S$, which implies $A_2L \perp C_1Y$. 

To sum up, $\phi$ is a translation on points $B_2$, $X$ and $P$, so in general $\phi$ is a translation.

Analogously, we obtain that $C'A'C_2A_1$ and $A'B'A_2B_1$ are rectangles. Let $T$ be a point such that $TA' = BC_2$, $TB' = CA_2$ and $TC' = AB_2$ (such point exists as triangles $AC_1B_2$, $BA_1C_2$ and $CB_1A_2$ glue up to triangle $A'B'C'$). Then $TA \parallel B_2C_1$, so $TA \perp B'A'C'$. Similarly, $TB \perp C'A'$ and $TC\perp A'B'$. In other words, triangle $ABC$ is orthological to triangle $A'B'C'$ with the center of orthology $T$.

Note that as $TB \parallel A'C_2$ and $TC \parallel A'B_1$ and $BC = C_2B_1$, then triangles $TBC$ and $A'C_2B_1$ are congruent and therefore $TBC$ is a translated triangle $A'C_2B_1$ along the vector $C_2B$. Hence $A'Z \perp BC$. Similarly, $TB' \perp CA$ and $TC' \perp AB$. Hence $T$ is also a center of orthology of triangle $A'B'C'$ to $ABC$. Thus, by converse of Sondat’s theorem, since centers of orthology of $ABC$ and $A'B'C'$ conincide, then $AA'$, $BB'$ and $CC'$ concur.
10. Denote the cubic polynomial by \( \varphi \). Observe that \( \varphi \) is irreducible over \( \mathbb{Q} \) — otherwise it would have in its factorization a linear factor with rational coefficients and thus a rational root, which is a contradiction. Therefore \( \varphi \) is a minimal polynomial for \( u, v, w \).

Hence polynomial \( \varphi(ax^2 + bx + c) \) has \( v \) as its root, so \( u \) and \( w \) are its roots as well. This means that \( aw^2 + bw + c \in \{u, v, w\} \). If \( aw^2 + bw + c = w \), then minimal polynomial for \( w \) would have degree at most 2, which is impossible. Moreover, if \( aw^2 + bw + c = u = av^2 + bv + c \), then \( (v - w)(a(v + w) + b) = 0 \), which means that \( v + w \) is rational. So by Vieta’s formulas for \( \varphi \) we get that \( w \) is rational, which is again a contradiction. Therefore \( aw^2 + bw + c = v \) and similarly \( au^2 + bu + c = w \). Finally, observe that \( a \) and \( b \) are nonzero.

Let \( k = a(u - s) \), \( l = a(v - s) \) and \( m = a(w - s) \), where \( s = \frac{u + v + w}{3} \). Then \( k + l + m = 0 \) and

\[
\frac{k}{a} + s = a \left( \frac{l}{a} + s \right)^2 + b \left( \frac{l}{a} + s \right) + c \quad \implies \quad k = l^2 + (2as + b)l + a(as^2 + bs + c - s).
\]

Let \( a' = 1 \), \( b' = 2as + b \) and \( c' = a(as^2 + bs + c - s) \). Note that \( b' \) and \( c' \) are rational as \( s \) is rational by Vieta’s formulas. In this notation we obtain

\[
\begin{align*}
k &= l^2 + b'l + c' \\
l &= m^2 + b'm + c' \\
m &= k^2 + b'k + c'.
\end{align*}
\]

Moreover,

\[
b'^2 - 2b' - 4a'c' - 7 = (2as + b)^2 - 2(2as + b) - 4a(as^2 + bs + c - s) - 7 = b^2 - 4b - 4ac - 7.
\]

Summing up acquired equations yields \( k^2 + l^2 + m^2 = -3c' \), so as \( k + l + m = 0 \), then

\[
kl + lm + mk = \frac{3c'}{2}.
\]

Expressing \( k, l, m \) in terms of RHS in (*) , we obtain

\[
kl + lm + mk = \sum_{\text{sym}} k^2l^2 + b' \sum_{\text{sym}} k^2l + 2c' \sum_{\text{sym}} k^2 + b'^2 \sum_{\text{sym}} kl + 2b'c' \sum_{\text{sym}} k + 3c'^2.
\]

Note that

\[
\sum_{\text{sym}} k^2l^2 = (kl + lm + mk)^2 - 2klm(k + l + m) \quad \text{and} \quad \sum_{\text{sym}} k^2l = (k + l + m)(kl + lm + mk) - 3klm,
\]

which with previous equality leads to

\[
klm = \frac{2b'^2c' - c'^2 - 2c'}{4b'}.
\]

Taking differences of equalities from (*) gives \( k - l = (l - m)(l + m + b') = (l - m)(b' - k) \). Multiplying such relations yields

\[
(b' - k)(b' - l)(b' - m) = 1.
\]
Plugging derived expressions for $kl + lm + ml$ and $klm$ in above equation gives
\[ c'^2 + 2(2b'^2 + 1)c' + 4(b'^4 - b') = 0 \implies (c' + 2b'^2 - 2b')(c' + 2b'^2 + 2b' - 2) = 0. \]

If $c' = -2(b'^2 - b')$, then $kl + lm + mk = -3(b'^2 - b')$ and $klm = -2b'^3 + 3b'^2 - 1$, so $k$, $l$, $m$ are irrational roots of polynomial $x^3 - 3(b'^2 - b')x + (2b'^3 - 3b'^2 + 1)$, which admits a rational root $b' - 1$ — contradiction. Therefore $c' = -2(b'^2 + b' + 1)$ and finally number
\[ b'^2 - 2b - 4ac - 7 = b'^2 - 2b' - 4a'c' - 7 = (3b' + 1)^2 \]
is a square of rational, so as integer is a perfect square.

11. Consider the following polynomial
\[ P(t_1, t_2, \ldots, t_k) = \prod_{1 \leq i < j \leq k} (t_j + a_j - t_i - a_i) \prod_{1 \leq i < j \leq k} (t_j - t_i). \]

Note that if we assign to each $t_i$ one of the values from $M$ in such a way that polynomial $P$ does not vanish, then such $t_i$ will satisfy the statement.

Degree of polynomial $P$ is at most $k(k-1)$, so if we proved that in $P$ the coefficient for $\prod_{1 \leq i \leq k} t_i^{k-1}$ does not vanish, then by Combinatorial Nullstellensatz the polynomial $P$ does not vanish for some $t_1, t_2, \ldots, t_k \in M$.

Observe that the coefficient that we are interested in is equal to the coefficient by the same monomial in
\[ Q(t_1, \ldots, t_k) = \prod_{1 \leq i < j \leq k} (t_j - t_i)^2 = \det \begin{pmatrix} 1 & t_1 & t_1^2 & \cdots & t_1^{k-1} \\ 1 & t_2 & t_2^2 & \cdots & t_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & t_k & t_k^2 & \cdots & t_k^{k-1} \end{pmatrix}^2, \]

where last equality is a consequence of the Vandermonde determinant. This determinant is a sum of expressions $\text{sgn}(\sigma) \cdot t_1^{\sigma(1)-1} t_2^{\sigma(2)-1} \cdots t_k^{\sigma(k)-1}$, where $\sigma$ is some permutation. For each $\sigma \in S_k$ there is exactly one $\pi \in S_k$ such that for all $i$ we have $\sigma(i) + \pi(i) = k + 1$. To get expression $\prod_{1 \leq i \leq k} t_i^{k-1}$ in $Q$, we have to multiply each $\text{sgn}(\sigma) \cdot t_1^{\sigma(1)-1} t_2^{\sigma(2)-1} \cdots t_k^{\sigma(k)-1}$ in one determinant by $\text{sgn}(\pi) \cdot t_1^{\pi(1)-1} t_2^{\pi(2)-1} \cdots t_k^{\pi(k)-1}$ in the second determinant. So the coefficient we are looking for is a sum of $\text{sgn}(\sigma) \cdot \text{sgn}(\pi)$ for $\sigma \in S_k$. Sign of each permutation $\sigma \circ \pi$ is equal to $(-1)^{k(k-1)/2}$, as $\sigma \circ \pi^{-1} = (1 k)(2 (k-1)) \ldots$. Therefore, the desired coefficient is equal to $(-1)^{k(k-1)/2} k!$. It does not vanish as we work in $\mathbb{Z}_p$, which completes the solution.
QUALIFYING QUIZ


**Problems**

**Problem 1.** Prove that for every natural number $n > 1$ there exist $n$ consecutive natural numbers such that their product is divisible by all primes less than $2n+2$, but it is not divisible by any other prime.

**Problem 2.** There are 130212 distinct points (no three points collinear), every two of which are connected by a line segment. Marta and Ania take turns erasing line segments, so that Marta is allowed to erase only one line segment per turn, and Ania is allowed to erase two or three line segments per turn. The person after whose move there is a point connected to no other points loses. Marta makes the first move. Who has the winning strategy?

**Problem 3.** Let $H_A, H_B, H_C$ be feet of altitudes from vertices $A$, $B$, $C$ of triangle $ABC$, respectively. Line parallel to $CA$ passing through $B$ intersects line $H_BH_C$ at point $X$. Point $M$ is the middle of segment $AB$. Show that

\[
\angle ACM = \angle XHA B.
\]

**Problem 4.** Let $a, b, c$ be positive real numbers such that $a+b+c=3$. Prove that

\[
(a^2-ab+b^2)(b^2-bc+c^2)(c^2-ca+a^2) \leq 12.
\]

**Problem 5.** Show that for each prime $p \geq 7$ there exists a positive integer $n$ and integers $x_i, y_i$ ($i=1, \ldots, n$) such that $x_i$, $y_i$ are not divisible by $p$ for each $i=1, \ldots, n$ and

\[
\begin{align*}
x_1^2 + y_1^2 &\equiv x_2^2 \pmod{p} \\
x_2^2 + y_2^2 &\equiv x_3^2 \pmod{p} \\
&\vdots \\
x_n^2 + y_n^2 &\equiv x_1^2 \pmod{p}.
\end{align*}
\]

**Problem 6.** An invisible rabbit Szymon is moving along a straight line on the Euclidean plane by making identical jumps every minute. Paweł — the hunter — sets his Trap every hour as he wishes to catch Szymon. The Trap catches rabbit when hunter puts it precisely at the moment when rabbit lands on the place of the Trap.

a) Assume Paweł’s Trap is a unit square that can be put on the plane only in such a way its vertices are lattice points (i.e. they have integer coordinates). Moreover, he knows that Szymon starts at the origin (but of course neither direction nor length of Szymon’s jump is known to the hunter). Can Paweł catch Szymon in finite time?

b) Now, Paweł’s Trap is just a point, but it can be put at any place. He doesn’t know where Szymon starts, but he knows that at each minute Szymon jumps from a lattice point to lattice point. Can Paweł catch Szymon in finite time?

**Problem 7.** Let $P$ be a point in the plane of triangle $ABC$ such that

\[
\frac{AP}{BC} = \frac{BP}{CA} = \frac{CP}{AB}.
\]

Prove that $P$ lies on the Euler line of triangle $ABC$. 

□■□□ 100 □■□□
CONTENTS

ABOUT THE CAMP

About the camp ......................................................... 3
People of the camp ................................................... 4
Events of the camp ..................................................... 5
Testimonials ............................................................... 8
Sponsors and project partners ....................................... 10

SELECTED HANDOUTS

Introduction to Graph Limits — Andrzej Grzesik .................. 14
Elementary Topology — Gábor Damásdi ............................ 17
Lattices in Number Theory — Alina Yan ............................ 19
Introduction to Combinatorial Designs — Łukasz Bożyk & Anna Łeń 22
Cubic Curves and Intersections — Mark Krusemeyer .............. 30
Transfinite Induction — Tomasz Cieśla ............................ 33
Introduction to Graphs and Graph Coloring — Gábor Damásdi .... 37
Central Limit Theorem — Marian Poljak .......................... 41
Cycles in Permutations — Łukasz Bożyk .......................... 45
Random Walks — Bartłomiej Żak ................................ 53
Tucker Circles — Piotr Ambroszczyk & Natalia Kucharczuk .... 68
Banach-Tarski Paradox — Jan Kociniak ........................... 71

MATHEMATICAL MATCHES

Younger Match — Problems ........................................ 76
Middle Match — Problems ......................................... 77
Older Match — Problems ........................................... 79
Younger Match — Solutions ....................................... 80
Middle Match — Solutions ......................................... 84
Older Match — Solutions ........................................... 90

QUALIFYING QUIZ

Problems ................................................................. 100