

T. Golenishcheva-Kutuzova, A. Kazantsev,  
Yu. Kudryashov, A. Kustarev,  
G. Merzon, I. Yashchenko

# Basics of Mathematics in Problems

with solutions  
and comments

PART 1

MCCME  
2018

Copyright © 2018 MCCME.

All rights reserved. No part of the material protected by this copyright notice may be reproduced in any form, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without written permission from the copyright owner.

Tatiana Golenishcheva-Kutuzova  
Alexander Kazantsev  
Yury Kudryashov  
Andrei Kustarev  
Grigory Merzon  
Ivan Yashchenko

Basics of Mathematics in Problems (with solutions and comments)  
Part I  
ISBN 978-5-4439-2842-5

Translated into English by  
Stepan Kazanin, Fiodor Kogan, Pavel Kovalev, and Alexey Sossinsky.

Russian original edition published as “Elementy Matematiki v Zadachakh. Part I”,  
MCCME, Moscow, 2010

The book contains a part of the one-year course of mathematics taught via problems and used for several years in School #57 of Moscow. As presented here, the course was given to the ‘B’ graduating class of 2008. This volume (Part I) consists of the topics studied in the 8th form.  
The problems are supplied with solutions and commentaries. Many topics (‘problem leaflets’) can be studied independently of the others.  
The book is intended for the reader interested in teaching mathematics to high school students beyond ordinary syllabus.

## Contents

Introduction . . . . .	5
About our aims . . . . .	6
About the leaflet system . . . . .	7
About the contents of the leaflets . . . . .	10
On cooperation and coercion . . . . .	13
The instructors . . . . .	16
Acknowledgements . . . . .	18
<i>Leaflet 1. Set Theory 1 . . . . .</i>	<i>21 / 71</i>
<i>Leaflet 2. Set Theory 2. Mappings of Sets . . . . .</i>	<i>24 / 81</i>
<i>Leaflet 3. Combinatorics 1 . . . . .</i>	<i>27 / 89</i>
<i>Leaflet 1a. Permutations 1. Walking around Cycles . . . . .</i>	<i>29 / 99</i>
<i>Leaflet 4. Mathematical Induction . . . . .</i>	<i>31 / 106</i>
<i>Leaflet 5. Combinatorics 2. The Binomial Theorem . . . . .</i>	<i>34 / 117</i>
<i>Leaflet 6. Graph Theory 1 . . . . .</i>	<i>36 / 128</i>
<i>Leaflet 2a. Permutations 2 . . . . .</i>	<i>39 / 141</i>
<i>Leaflet 7. Integers 1. Divisibility of Integers . . . . .</i>	<i>41 / 148</i>
<i>Leaflet 8. Integers 2. The Euclidean Algorithm . . . . .</i>	<i>43 / 157</i>
<i>Leaflet 9. Equivalence Relations . . . . .</i>	<i>46 / 168</i>
<i>Leaflet 10. Integers 3. Modular Arithmetic . . . . .</i>	<i>48 / 180</i>
<i>Leaflet 11. Integers 4. Practical Problems . . . . .</i>	<i>50 / 190</i>
<i>Leaflet 12. Group Theory . . . . .</i>	<i>52 / 194</i>
<i>Leaflet 3a. Graph Theory 2 . . . . .</i>	<i>55 / 206</i>
<i>Leaflet 13. Graphical representation of functions . . . . .</i>	<i>60 / 218</i>
<i>Leaflet 4a. Group Theory 2. Homomorphisms . . . . .</i>	<i>63 / 226</i>

Problems / Solutions



## Introduction

In the mathematical classes of School #57, the well-known Moscow secondary school specializing in mathematics, besides lessons in algebra and geometry, there is another subject, traditionally called ‘mathematical analysis’. Unlike the lessons in other subjects, the lessons in that subject involve practically no explanations at the blackboard. Instead, the pupils are regularly given problem sheets, called *leaflets* (*listochki* in Russian<sup>1</sup>), which contain several problems, stated together with the necessary definitions.

The pupils solve and write down the solutions of the problems, each pupil at his/her own pace; there are no formal homework assignments, the pupil’s work is not marked (although twice a year an examination with marks is conducted); in class, each pupil individually discusses the solutions with one of the instructors – there is a team of 4-6 instructors at each lesson. It is those instructors who prepare the leaflets.

The present book contains all the leaflets given out to the ‘B’ class of Moscow School #57 that graduated in 2008, together with solutions and commentaries. This volume is Part I of the book. It includes the leaflets given out to the class when it was in the 8th form (out of 11). Additional problems are marked by a star (\*), additional leaflets, by the letter ‘a’ added to the leaflet’s number.

### About this introduction.

Please, she asked, don’t finish telling the story. First let’s recall some details.

Grigoriy Oster, *A Fairy Tale with Details*

Nobody ever reads long introductions. So we have decided to limit ourselves to a brief description of the teaching process in our class and a varied collection of details, in which the reader will perhaps find answers to possible questions.

**On different approaches.** We immediately warn the reader that different teams of instructors working with leaflets teach in different ways. So it makes little sense to speak of the ‘general approach to teaching math classes in teams’, and what follows is a description of how our own particular team worked and how we understand the teaching process.

---

<sup>1</sup>The English word ‘leaflet’ has a somewhat negative connotation, as in the expressions ‘political leaflets’, ‘advertising leaflets’, but the Russian word ‘listok’ does not bring to mind any negative associations.

What is more, it so happened that our team itself consisted of people of dissimilar temperaments, varying biases, different world outlook, diverse views on the teaching of mathematics<sup>2</sup>.

During the teaching process, we often disagreed with each other and would spend a lot of time in heated discussions after classes. And, although most of the time none of us would change his/her position, the arguments of our colleagues often made us look at things from a different angle.

### About our aims

I candidly admit that in my long life I have never told my pupils anything about the ‘meaning’ of music; if there is such a thing, it has no need of me. Conversely, I always paid a great deal of attention to teaching my pupils to correctly count off eighths and sixteenths. Whether you are a teacher, a scientist, or a musician – revere ‘meaning’, but don’t imagine that it can be taught.

Herman Hesse, *The Glass Bead Game*

Let us say at once that our unique (or even our main) aim is not to bring up future professional mathematicians (although we try to give those pupils who aspire to become research mathematicians a chance to do that, provided they have the potential for it).

The things that we intend to teach the pupils can be divided into two groups. First of all – no matter how pretentious this may sound – we teach the pupils to think, to independently obtain new results, to experience mathematical discovery. If a pupil graduating from one of our math classes will never do any mathematics again, this experience will eventually help in one way or another.

On the other hand, since thinking and making mathematical discoveries is a complicated and creative activity, it is not clear how one should go about teaching such things. Therefore, during lessons, we are formally occupied with the second type of (much more modest) activity. We can say that we teach how to do four things: read, write, speak, and listen (the pupil *reads* the definitions and problems in the problem sheet, *writes* the solutions, *tells* them to the instructor, and *listens* to the instructor’s comments – this is what we try to teach; but solving problems is something the pupils learn to do themselves).

We hope that such an approach to studying mathematics helps develop at least three skills, which are useful outside the class as well: ‘the first is

---

<sup>2</sup>And this, in a sense, is not a bad thing – for instance, it gives the pupils the possibility to choose a preferred instructor to work with. Evidence of this diversity can probably be noticed in this book.

the ability to distinguish between truth and lies (lies understood in the mathematical sense, i.e., without intent to deceive); the second, to distinguish the meaningful from the meaningless; the third, to distinguish the comprehensible from the incomprehensible' (Vladimir Uspensky).

Besides all this, we would like our alumni to have some understanding of what mathematics is and how one works with it. This is useful not only to those who will be doing mathematics after leaving school, but also to those who will do no more mathematics – if only to make the latter group understand what it is, and abandon mathematics at the right time.

Finally, it just so happens that the classroom turns out to be the meeting place of youngsters who want to study mathematics and instructors who know and love the subject, and strive to share their knowledge. Perhaps it is the resulting communication which is the main goal of the process – just as it is in a musical society or a macramé club.

### About the leaflet system

**Leaflets.** Mathematics is a creative activity; but there is no efficient *technology* for acquiring new mathematical knowledge. Now the only way to learn to swim is to try to swim in one way or another; looking at how others do it does not suffice. Similarly, the only way to learn how to make mathematical discoveries is practice: solving problems that provide the pupils with *new knowledge*.

Of course, this knowledge, its underlying facts have been known to humanity for a long time, but this isn't of much help to the pupils (only psychologically – in order to do something, it is useful to know that it can be done).

Incidentally, the last statement may be a bit misleading. The actual sequence of problems in each topic proposed to the pupils allows the pupils to move upwards, like up the steps of a staircase. To this end, the steps should be made high enough for the process to be interesting, but low enough so that each step is accessible to each pupil<sup>3</sup>. And such a step-by-step construction of each leaflet is based on the fact that the instructors know the solutions to the problems quite well.

At the same time, we include some difficult problems in the leaflets, sometimes even unsolved ones. The pupils will see that outwardly these

---

<sup>3</sup>Here we cannot avoid mentioning that the independent search for and choice of problems is an important part of a mathematician's work and it is *not* taught to the pupils in the framework of the leaflet system. Even the necessity of such an activity is hidden from the pupils working within that system – and this can give a distorted picture of how a research mathematician works.

problems appear to be of the same kind as the others, and try to solve them. It is pleasant to note that some pupils working within our system have obtained results worthy of publication in scientific journals<sup>4</sup>.

Besides, each leaflet is an outline of sorts for a mathematical paper of the definition-theorem-proof kind, in which the pupil is asked to fill in the missing proofs. Thus each leaflet conveys an accepted method of structuring mathematical knowledge<sup>5</sup>.

**About the individual approach.** We think that the idea of teaching a whole class according to the same program is counterproductive.

For that reason, besides the main program for all, there are additional leaflets about diverse topics (often diverging noticeably from the basic course); the pupils choose these additional leaflets according to their own taste. These leaflets (together with the additional problems in the required leaflets) compensate the difference in the pace of work of different pupils.

Besides different expectations and requirements imposed on the pupils, they are given different hints and tips, or, to the contrary, additional simplifying questions. These questions, together with the instructor's comments, fill in the gaps between the problems and the definitions in the leaflets, thereby creating (at least ideally) an individual course for each pupil.

Each instructor can only work in this way with small number of pupils whom he/she knows well enough. For this reason, the class needs several instructors, each one working with 3-5 fixed pupils. During the lesson, the instructors move around the classroom and periodically sit down next to one of 'their' pupils to discuss the problems. Usually twice a year a redistribution of pupils among the instructors occurs. Also, the pupils must pass a graded oral examination, which they never take with their own instructor.

**About traditional methods.** The main feature that distinguishes our approach from traditional lessons in school and the lecture-exercise class system at university is that we try to teach our pupils to discover something for themselves instead of following a given routine or using ideas explained by the teacher. It is precisely for this reason that we do not force the pupils to learn facts and prepared schemes by heart, and push them to invent new (for them!) methods of solution.

---

<sup>4</sup>E.g., Yu. Makarychev. A short proof of Kuratowski's graph planarity criterion // *J. of Graph Theory*, 1997, Vol. 25, 129–131; A. Kustarev, Boundedness of finite vector sums and a proof of the Levi–Steinitz theorem // *Mathematical Enlightenment*, Ser. 3, no. 7 [in Russian].

<sup>5</sup>The fact that this method is not the only one possible can easily be seen by comparing articles on the same subject in mathematics and physics.



Let us immediately point out that, at later stages, prepared expositions (books, lectures) are not only useful, but necessary. First of all, the study of any topic by solving problems requires a lot of time. Secondly, even if we assume that any topic can be expounded by means of a series of problems (which is not obvious), for most topics this has not been done (if only because this requires serious work by someone who has mastered the topic). Thus the idea that a sufficient (say, for doing serious mathematics) amount of knowledge can be obtained via the system of leaflets is not very realistic. Therefore, beginning with the 10th form, we give the pupils books to read and discuss, and organize lectures for them on certain topics.

But, at least at the beginning, the pupils must acquire a firm foundation of problems and theorems that they truly understand because they have discovered the proofs by themselves.

It should also be kept in mind that besides the analysis (calculus) course, School #57 always has courses in algebra and geometry<sup>6</sup> taught in a more traditional way.

**About explanations at the blackboard.** In forms 8–9, we gave explanations at the board only in two cases.

First, just before handing out a new leaflet, we sometimes explain the main ideas and motivations in an informal way, without stating rigorous theorems or going into the technical details of definitions; such explanations occur when there is no previous knowledge in the given topic.

Second, during the consultations that take place before each of the examinations, we present problem solutions, including the technical details. By that time the pupils have been working on the given topic for long enough and so can recognize problems that they may have spent a good deal of time thinking about.

**About the examinations.**

- ...And was there a hole for the math examinations?
- Sure, said Serpens as his eyes sparkled, ten elbows deep.
- Just as for us! They put us in the hole, gave us problems, and those who couldn't solve them were never lifted out. I can tell you that the sight of the whitening bones of your predecessors really assists the mental process.

Anna Korosteleva, *The Carmarthern School*

The examinations have several purposes.

---

<sup>6</sup>In particular, we recommend the brilliant geometry course of Rafail Gordin (who not only taught the traditional math courses in our class (8th 'B', but was also the class supervisor).

On one hand, they give the pupils the opportunity to understand what it is that they really know, and what they don't know, and this happens not only during the exam, but also in the preparation for it.

Generally speaking, preparation for the examination may be more useful than the exam itself. The approaching examination motivates (and that is another reason that we conduct it). During ordinary periods, the pupils have lots of other things to do – from strolling in the park to doing homework assignments in other subjects. While before the math exam, pupils concentrate on mathematics: preparation for the exam is a good occasion to recall what one has learned, to systematize that knowledge and to finally check out the fine points and problems from old leaflets that had not been solved.

To work all the time in such a regime is impossible – and that's why we conduct exams only twice a year – but doing it from time to time is very beneficial (it is impossible to walk slowly up an ice covered ridge, but one can make it to the top by running; in the same way, intense studies can yield a qualitative breakthrough only if they are interspersed with ordinary measured ones).

On the other hand, it is also interesting for us to find out what we have actually taught our pupils. Here the important thing is not how well they have 'mastered the material', and not even how well they have learned to solve problems (that is usually clear from everyday work in the classroom), but especially to find lacunas in the most unexpected places. Rather, what we are really interested in is their aptitude for mathematical communication (the instructor, working with the same pupil for a long period of time, can no longer objectively assess how well the pupil expresses his/her thoughts).

Finally, in forms 10-11 we invite to the examinations professional mathematicians, personal contacts with whom are interesting and beneficial to the pupils.

### About the contents of the leaflets

**On the choice of topics.** The transmission of a maximal amount of knowledge is not one of our main goals; the concrete material that we choose is only a means, a convenient setting for the communication between pupils and instructors during the lessons. Hence the actual choice of topics is mainly motivated by the mathematical tastes of our team: it is always important to teach only the things that you like yourself.

In that context, we try to use topics that do not require too much preliminary knowledge; here we have in mind not only formally used defini-

tions and theorems, but also facts needed to motivate the questions under study; insufficiently motivated and excessively abstract topics are badly assimilated by pupils in the 8th and 9th forms.

At the same time, a chosen topic must be sufficiently significant to ensure that its study will not reduce to a formal game with definitions. Otherwise, a situation arises in which an alumnus of a mathematics class knows a lot of fancy words, but is unable to prove or even to understand the proof of a nontrivial theorem.

Besides, we try to choose the topics so that the course will not be an incoherent collection of disconnected themes but will – at least to some extent – give an impression of *ascent*<sup>7</sup>. In our course for the 8th and 9th forms, the guideline is the construction of the real numbers: starting from basic set theory via the integers, rational numbers, ordered fields and on to calculus.

Finally, although the volume of acquired knowledge is secondary (as compared to acquiring skills in mathematical investigation), we try to include into the program a certain minimum without which the study of mathematics is impossible. For this reason, we sometimes hand out leaflets aiming at filling up lacunas in the pupil's knowledge. This is especially important at the beginning, when the pupils come to us with a completely different background of knowledge.

**Writing the leaflets.** It would seem that nothing is simpler: just take any sufficiently closed mathematical text (an article or chapter from a book) and copy from it the definitions, and state the lemmas and theorems in the form of problems (and possibly include a few additional intermediate lemmas). But it is clear that in this case all the comments that are formally not necessary for the proofs of the main results will be irredeemably lost. Thus, at a minimum, one must add (in the form of problems, possibly very easy ones, which simply fix certain assertions) examples and counterexamples demonstrating the necessity of assumptions in the theorems, as well as consequences of theorems showing their significance, and so on. As to the things that could not be set forth in this way – for instance, informal ideas and analogies – the instructor must keep them in mind in the discussion of the problems with the pupils; of course, this imposes definite requirements concerning the instructor's qualifications.

Let us say a few words about the composition of the leaflet. As the physicist Richard Feynman wrote, 'to understand means to get used to

---

<sup>7</sup>The majority of the leaflets combine into a more or less linear route, while the additional leaflets provide bifurcations in quite different directions.

and learn how to use.’ And so each leaflet begins with sufficiently simple problems which allow the pupil to grasp the meaning of the basic concepts<sup>8</sup>. But of course one cannot learn mathematics by only solving simple problems, and so near the end of the leaflet the difficulty level of the problems increases, and in the longer leaflets two such difficulty peaks occur, one in the middle and the other at the end.

This composition, resembling an ascending staircase, allows the pupil to ‘independently’ obtain the proofs of significant theorems. Correspondingly (unlike the situation in the solution of technical exercises), the pupil can see the convincing result of his work, say that ‘I have proved the fundamental theorem of arithmetic’. Here (in contrast with most olympiad problems), the obtained result is not only interesting *per se*, but is useful for what follows.

Of course, this type of outline of the leaflets imposes certain restrictions on the choice of material: since the size of the leaflet is limited<sup>9</sup>, and each subsequent leaflet begins with easy problems, the effect of ‘catching one’s second breath’ arises: such an ascending staircase never reaches the really difficult things, no matter how many leaflets are covered. This difficulty can be overcome (by the stronger pupils) thanks to the additional problems and extra leaflets (numbered 1, 2, ... with letter ‘a’ for additional), the latter being longer and more difficult than the required leaflets, and, for all the pupils, by discussions with the instructor.

In conclusion of our discussion on the compilation of leaflets, we would like to warn against copying the leaflets from our course literally: on the one hand, they were written for a concrete group of pupils, and on the other hand, they reflect the mathematical tastes of concrete instructors. Nevertheless, we hope that this book will be useful for selecting the material to study in a math class.

**On the axiomatic method and set theory.** The road going up a mountain range is not direct and steep, it slowly winds along the slope of the mountain. The same is true in mathematics: beginning our course, we must first forget all the mathematics that was taught previously (our calculus course is formally self-contained: there are no references in the leaflets to any previous school material, and facts known from it cannot be used

---

<sup>8</sup>It sometimes happens that highly qualified instructors (especially when working with strong pupils) try to rapidly skim through problems that seem too simple and insufficiently meaningful; as a rule, this does not lead to good results.

<sup>9</sup>A ten page long mathematical paper is regarded as short, but a four page leaflet is so long that not every pupil will reach its end, and some of our colleagues believe that each leaflet must fit on one page – else it can no longer be called a ‘leaflet’.

without proof) and we start from scratch, but at a different level<sup>10</sup>. In particular, on a different level of rigor: the course is based on the (informal) axiomatic method. The foundation on which the course is built consists of the undefined concepts of set and whole number. Our ‘mathematical analysis’ (calculus) course begins with an introduction to (naive) set theory.

To some extent this is a tribute to tradition, but it has its own reasons: this topic is usually new for our pupils, and this allows us to draw a clear line from the outset (which is very appropriate when the aims, the form, and the contents are completely changed); on new, easy to understand material it is simpler to specify the requirements concerning the rigor<sup>11</sup> of solutions and their written form. The choice of the axiomatic method as the foundation of our course was not the only possible one and, for us, it did not seem obvious. We do not advise following us in that choice before carefully assessing the *pros* and *cons*. And if one does begin the course in this way, it should be done accurately, taking into account the difference of level of the pupils: some have studied the subject in math circles and are ready for a higher degree of formalism, while others, if subjected to overly formal requirements, will lose all interest whatsoever in doing mathematics.

### On cooperation and coercion

**About mathematical discussions.** From the very first lesson (and often before, in math circles), we try to show the pupils that we relate to them as colleagues, and so attempt to create an atmosphere of joint scientific work. This work usually consists in pupil and instructor jointly trying to assess the pupil’s solution of a problem.

For such a relationship to be fruitful, we try to teach, from the very beginning, the *skills of mathematical dialogue* (which are valuable in themselves): to understand what is given, what must be proved, and what can be used in the process; to distinguish what has been proved from what hasn’t; to coherently present one’s thoughts, orally and in written form;

---

<sup>10</sup>And the amplitude increases as compared with the previous school course: we move down deeper, all the way to set theory, then wind up slowly (going through the integers and real numbers again) and end up at a much higher level.

<sup>11</sup>There is an opposite opinion about this, according to which, first of all, the solution of a problem (in this case, the axiomatic method as the solution to the problem of the foundations of mathematics) cannot be adequately understood unless the contents the problem (mathematics) are familiar, and, second, any method should be studied on significant examples, not on the simplest ones.

to state the negation of an assertion; to correct errors and fill up gaps in arguments. During the first lessons, most of the time is taken up by such apparently simple, but actually fundamental, things.

**About writing down solutions.** We work with pupils who usually think quite rapidly. This is wonderful and interesting, but the pupils usually think faster than they talk, and much faster than they write. And a lot of effort (and authority) is spent not only teaching them how to express thoughts on paper, but in actually convincing them that this is really necessary.

The main reason for insisting on this is that only when one begins to write out a solution does the structure of the argument become clear, and only then does one understand what is being said. A typical situation at the beginning of our studies is this: an 8th form student explains something and does not agree to write it down, saying that anyway it is *obvious*. The instructor then writes out what the pupil explained; the pupil sees that what is written is exactly what he/she said, but reading the text, exclaims: 'It seems I gave a correct solution, but what's written here is some kind of nonsense with lots of mistakes, it's basically incorrect'. To explain to him/her that there is an error in her oral argument is much harder, in particular because in response to the indication of an error the pupil can 'change the testimony' (and quite sincerely – in the process of a long conversation, it is difficult to remember what was said at the beginning), claiming that he/she didn't say that; besides, orally it is easier (consciously or not) to hide defects in the argument by means of rhetoric.

A solution written down on paper helps the pupil to structure his/her thoughts, to better grasp the logic of the argument (invented by the pupil), to follow through the whole chain of assertions. In particular, it is not unusual for students to find an error in their arguments.

**About checking the solutions.** Here it is important not to overdo the formal requirements of rigor to the detriment of substance. In practice, the verification of solutions always involves a competitive element: the pupil tries to convince the instructor that his/her argument is correct, while the instructor tries to find an error in it; if the instructor 'wins', then the pupil returns to the problem and tries to find an acceptable solution again. But we must not forget that the main goal of the instructor is not to find as many formal inaccuracies as possible, but to find out, together with the pupil, the gist of the matter. We would like each lesson to be a collaboration, not a competition.

In the converse case, – even leaving aside the psychological aspects of the situation, where at each lesson the pupil must compete with a person who is older and knows the subject matter much better – by the end of such studies, the pupil will reach the conclusion that mathematics reduces to formal manipulations with symbols according to fixed rules; for us, who definitely disagree with that viewpoint, this is something we would not like to happen.

**About coercion.** In our opinion, no teaching is possible without a certain amount of coercion. Those who believe that mathematics (as well as many other things) can be easily taught to a child in an atmosphere of happiness and love, are completely mistaken. But it is impossible to do creative work under the fear of punishment, so we must delicately use various means of compulsion, minimizing the more negative aspects.

The most important is to create an atmosphere in which it is *accepted* that studying and solving problems is a prestigious activity. Besides, we must create an atmosphere in which a pupil who has come to a lesson without any solved problems should feel uneasy meeting an instructor, as when meeting a colleague with whom you intended to work and discuss something, but came in vain, simply wasting other people's time.

In this context, we try to minimize the role of school marks, making the pupils understand that they are not working for formal grades (in the 8th form, many pupils, including some of the best ones, still believe that), but are working to solve problems, to appreciate the beauty of mathematics, and the highest prize is the pleasure of finding a solution, the esteem of colleagues (instructors and classmates) for the solution. Here the most important is the personal pleasure of finding a solution.

Clearly, teaching according to this approach is not efficient (or simply impossible) if the child doesn't like mathematics and doesn't want to study it. Incidentally, for this reason it is easy for us to screen our class from potential pupils whose parents, often friends of the instructors or of members of the school administration, pressure us to accept their siblings: we simply honestly explain that, as friends, the best we can do for the child is to protect him/her from life in such a penitentiary as our mathematics class.

**About copying.** The unpleasant situation when pupils copy solutions from classmates is basically eliminated if the instructors have enough patience and pedagogical skill to free the pupil from the psychological anxiety of getting a failing mark: we must work things out so that the pupils do not tend to laziness, but without punishing them for not submit-

ting solutions, without visibly counting the number of solved problems. Otherwise, at that age it is very difficult not to succumb to the temptation of copying (and no development of creativity can then occur). We try to explain to the pupils (and to their parents) that the assessment of the results is not carried out by the formal count of the number of solved problems and that a successfully copied problem does not help the pupil to achieve the goals of our studies.

**About the tempo.** Due to the different initial levels of mathematical preparedness and different styles of thinking, our pupils solve problems at different speed, and we try to avoid any competition based on the formal number of solved problems. We immediately explain that we judge (both formally and informally) the individual work of each pupil, the intensity of his/her assiduity, on the basis of the pupil's possibilities at the given moment, and not in comparison to some fixed mean level.

Under this approach, the final marks given to the pupils are largely based on the subjective assessment of the instructor and makes no claim to objectivity. But in our practice, it usually turns out that the pupil's mark is a surprise to no one, and the pupils usually agree with the instructor's assessment.

As we mentioned before, there are no formal homework assignments, but the instructor indicates to the pupil (explicitly or implicitly) when it is time to finish working on the given leaflet (i.e., submit all the required problems in it). We try to work things out so that unfinished required leaflets do not accumulate, so we give out new leaflets only when the majority of pupils have worked out the old ones, and help out the lagging pupils.

## The instructors

**Students.** The instructor in a math class does not necessarily have to be a mathematician, but it is important for that person to be interested in mathematics and know the subject. Actually, it turns out that the best instructors in a math class are undergraduate and graduate students in mathematics, who have recently graduated from a math class.

Such instructors feel closer to the pupils, there are no psychological barriers between them and their pupils (and so it is not surprising that the communication between them is not limited to lessons – there are short camping trips, campfire songs with a guitar, discussions about books and movies, and often this continues after graduation). These instructors



have an overwhelming desire to share the knowledge recently acquired in school and at university. Finally, they still remember attitude from their own experience as school pupils *how* they were taught; and not only what worked, but what didn't. For this reason, they don't need any special pedagogical education, and so are ready to teach according to the given approach, provided that they are appropriately guided.

Such instructors usually constitute the majority of the team (it is for this reason that the specialized math school system is so stable<sup>12</sup>). This was so in our case.

**The head of the team.** When the atmosphere in the class is very informal, it is more difficult to maintain a reasonable level of discipline. The distinction between a creative atmosphere and total chaos is a very fine one. And when a critical mass of pupils who won't do any work is formed, the class falls apart: either the pupils openly stop doing anything, or an imitation of activity sets in (fortunately, this never happened in our classes).

The role of the leader (besides taking part in checking the solutions of problems) is, first of all, to have a correct feeling of what is going on in the class in general, and for each pupil in particular, and to accurately regulate the situation: praise one, reprimand another (without losing psychological contact), in some cases even change one of the instructors. Also, the head of the team must assess the level of the material, and choose the topics of study.

Of course, this choice is made collectively (not necessarily as the result of a discussion – on some topics the opinion of the team is unanimous), and in most cases the leader's opinion coincides with that of the rest of the team. In general, when things go well, the head of the team without being noticed works like the other instructors (it may even seem that no team leader is needed), but as soon as problems arise – he is the one who must make the appropriate decisions.

In conclusion – and this is most important, the team leader is the one who charges the pupils as well as his team with positive energy. And coming to each lesson, the leader must leave all his affairs and problems outside the classroom.

---

<sup>12</sup>That is what usually happens in efficiently working systems – their stability is due, to a great extent, to inertia: the students coming to teach in math schools believe that the way they were taught there is the most natural and correct one (modulo some small details), and don't bother to think about the reasons for deciding on the chosen approach, nor do they look for alternatives. Probably, we also are not entirely free of this point of view.

## Acknowledgements

The course acquired its present form (and this book was written) thanks to the help of many wonderful people:

- Nikolai Konstantinov, who first applied the ‘leaflet method’ in mathematical classes, and Boris Davidovich, the teacher of one of us, whose course strongly influenced us;

- our friends and colleagues who worked with one of us in the math classes in 1996 and 2002 at School #57 and helped create the previous versions of the course: Dima Botin, Sergey Dorichenko, Victor Kryukov, Sergey Markelov, Vladimir Piterbarg, Arkadiy Skopenkov, Roman Fedorov, Stanislav Shalunov, and others.

- all those who conducted classes in ‘analysis’ in the 8th form ‘B’ of the class of 2008 and discussed the contents of the leaflets with us: Elena Koritskaya, Petr Mitrichev, and Vladimir Rychev.

- the pupils of the 8th form ‘B’ of the class of 2008 who – amazingly! – were able to learn all this while enjoying mathematics with us, inspiring us to create the course and write this book.

The number of errors in the text was considerably decreased thanks to the attentive reading of Alex Bokhenek, Serge Lvovsky, Alexey Kapliev, Andrey Semyonov, and Victor Shuvalov. We are grateful to Alexey Sossinsky who supervised translation of this book into English and we also want to thank Keith Conrad for his help with translation. Special thanks go to Vadim Radionov, who not only typeset the book, but corrected a number of errors and made several valuable suggestions. Finally, we are grateful to the late Vitaly Arnold for valuable remarks about writing this introduction.

We shall be grateful to the readers for pointing out mistakes and misprints (email: merzon@mccme.ru, Grigory Merzon).

# Leaflets



# Set Theory 1

Leaflet 1 / September 2004

The notion of set is one of the primitive notions in mathematics. To specify a set is to say what elements it contains. One of the ways of specifying a set is listing its elements in curly braces.

One writes ' $x \in M$ ' for 'an element  $x$  lies in  $M$ ' and ' $x \notin M$ ' for 'an element  $x$  does not lie in  $M$ '.

**Problem 1.** How many elements does each of the following sets contain?

- a)  $\{1\}$ ,  $\{1, 2, 3\}$ ,  $\{\text{Vasya}\}$ ; b)  $\{\{1\}\}$ ; c)  $\{1, \{2, 3\}\}$ ;
- d) the set of letters in the word 'crocodile'; e)  $\{\{1\}, 1\}$ ;
- f) the set of names of students in your class.

**Definition 1.** Two sets  $A$  and  $B$  are *equal*, written  $A = B$ , if every element of  $A$  lies in  $B$  and every element of  $B$  lies in  $A$ .

**Definition 2.** A set  $A$  is said to be a *subset* of a set  $B$ , written  $A \subset B$ , provided every element of  $A$  lies in  $B$ . One of the ways of specifying a subset is to impose a property that all of its elements must possess:

$$\{x \in A \mid x \text{ has the property } \dots\}.$$

**Problem 2.** a) Let  $A$  be the set of one-digit natural numbers. Write the subset  $\{2, 4, 6, 8\}$  of  $A$  using the method in Definition 2.

b) Let  $A$  be the set of cities in your country. List the elements of the following subset of  $A$ :  $\{x \in A \mid \text{the population of city } x \text{ is greater than } 1\,000\,000 \text{ people}\}$ .

**Problem 3.** For each pair of sets below, determine whether one of them is a subset of the other:  $\{1\}$ ,  $\{1, 2\}$ ,  $\{1, 2, 3\}$ ,  $\{\{1\}, 2, 3\}$ ,  $\{\{1, 2\}, 3\}$ ,  $\{3, 2, 1\}$ ,  $\{\{2, 1\}\}$ .

**Problem 4.** Prove that a set  $A$  is a subset of a set  $B$  if and only if every element that does not lie in  $B$  is also not an element of  $A$ .

**Problem 5.** Prove that for any sets  $A$ ,  $B$ , and  $C$ , the following holds:

- a)  $A \subset A$ ; b)  $A \subset B$  and  $B \subset C \Rightarrow A \subset C$ ; c)  $A = B \Leftrightarrow A \subset B$  and  $B \subset A$ .

**Definition 3.** A set is said to be *empty*, written  $\emptyset$ , if it contains no elements.

The second part of the next exercise shows that it makes sense to refer to  $\emptyset$  as *the* empty set.

**Problem 6.** a) Prove that the empty set is a subset of every set.

- b) Prove that the empty set is unique.

**Problem 7.** Determine how many elements there are in each of the sets below:

$$\emptyset, \{1\}, \{1, 2\}, \{1, 2, 3\}, \{\{1\}, 2, 3\}, \{\{1, 2\}, 3\}, \{\emptyset\}, \{\{2, 1\}\}.$$

**Problem 8.** a) List all subsets of each of the sets in the previous problem.

b) For  $i = 1, 2, 3$ , determine how many subsets there are in a set  $S$  if  $S$  has  $i$  elements.

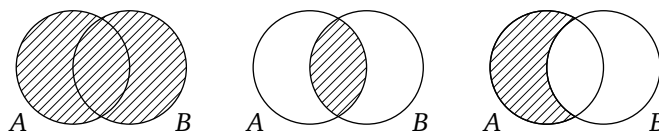
**Problem 9.** Is it true that the set of flying crocodiles is a subset of the set of students in your class? Is it true that the set of students in your class is a subset of the set of all forms of the school?

**Problem 10.** Can a set contain precisely a) 0; b) 7; c) 16 subsets?

**Definition 4.** The *union* of two sets  $A$  and  $B$ , written  $A \cup B$ , is the set of elements  $x$  such that  $x \in A$  or  $x \in B$ .

The *intersection* of two sets  $A$  and  $B$ , written  $A \cap B$ , is the set of elements  $x$  such that  $x \in A$  and  $x \in B$ .

The *difference* of two sets  $A$  and  $B$ , written  $A \setminus B$ , is the set of elements  $x$  such that  $x \in A$  and  $x \notin B$ .



**Problem 11.** Consider the sets  $A = \{1, 3, 7, 137\}$ ,  $B = \{3, 7, 23\}$ ,  $C = \{0, 1, 3, 23\}$ , and  $D = \{0, 7, 23, 2004\}$ . Identify the following sets:

- a)  $A \cup B$ ; b)  $A \cap B$ ; c)  $(A \cap B) \cup D$ ; d)  $C \cap (D \cap B)$ ;
- e)  $(A \cup B) \cap (C \cup D)$ ; f)  $(A \cup (B \cap C)) \cap D$ ;
- g)  $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$ ; h)  $(A \cup B) \setminus (C \cap D)$ ;
- i)  $A \setminus (B \setminus (C \setminus D))$ ; j)  $((A \setminus (B \cup D)) \setminus C) \cup B$ .

**Problem 12.** Let  $A$  be the set of even numbers and  $B$  be the set of numbers divisible by three. Identify  $A \cap B$ .

**Problem 13.** Prove that for all sets  $A$ ,  $B$ , and  $C$ , one has the following:

- a)  $A \cup B = B \cup A$ ;  $A \cap B = B \cap A$ ;
- b)  $A \cup (B \cap C) = (A \cup B) \cap C$ ;  $A \cap (B \cap C) = (A \cap B) \cap C$ ;
- c)  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ ;
- d)  $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ ;  $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ .

**Problem 14.** Is it true that for all sets  $A$ ,  $B$ , and  $C$ , the following equalities hold?

- a)  $A \cap \emptyset = \emptyset$ ;  $A \cup \emptyset = A$ ; b)  $A \cup A = A$ ;  $A \cap A = A$ ;  
 c)  $A \cap B = A \iff A \subset B$ ; d)  $(A \setminus B) \cup B = A$ ; e)  $A \setminus (A \setminus B) = A \cap B$ ;  
 f)  $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$ ; g)  $(A \setminus B) \cup (B \setminus A) = A \cup B$ ?

**Problem 15.** a) Three polygons, each having an area of at least 3 units, are placed inside a geometric shape of area 6 units. Show that there exist two polygons whose intersection has an area of at least 1 unit.

b\*) Seven polygons, each having an area of at least 1 unit, are placed inside a geometric shape of area 4 units. Show that there exist two polygons whose intersection has an area of at least  $1/7$  units.

**Problem 16\*.** a) Is it possible to write the intersection of two sets using the operations of difference and union exclusively?

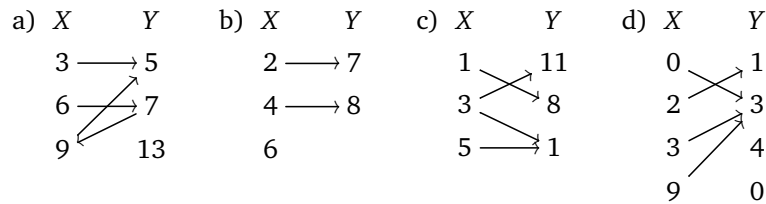
b) Is it possible to write the difference of two sets using the operations of union and intersection exclusively?

## Set Theory 2. Mappings of Sets

Leaflet 2 / September 2004

**Definition 1.** If to every element  $x$  in a set  $X$  there corresponds one and only one element  $f(x)$  of a set  $Y$ , then we say that  $f$  is a *map* from the set  $X$  to the set  $Y$  and write  $f: X \rightarrow Y$ . If  $f(x) = y$ , then the element  $y$  is called the *image* of the element  $x$  under the map  $f$ , and the element  $x$  is called a *preimage* of the element  $y$  under the map  $f$ .

**Problem 1.** Which of the following pictures define maps?



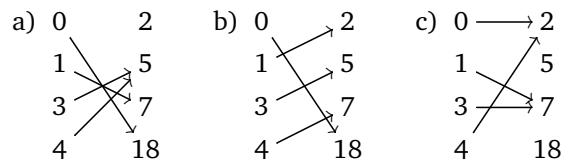
**Problem 2.** Draw all possible maps from the set  $\{7, 8, 9\}$  to the set  $\{0, 1\}$ .

**Definition 2.** Let  $f: X \rightarrow Y$ ,  $y \in Y$ ,  $A \subset X$ ,  $B \subset Y$ . The (complete) *preimage* of an element  $y$  under the map  $f$ , written  $f^{-1}(y)$ , is the set

$$\{x \in X \mid f(x) = y\}.$$

The *image* of the set  $A \subset X$  under the map  $f$ , written  $f[A]$ , is the set  $\{f(x) \mid x \in A\}$ . The *preimage* of the set  $B \subset Y$ , written  $f^{-1}[B]$ , is the set  $\{x \in X \mid f(x) \in B\}$ .

**Problem 3.** For a map  $f: \{0, 1, 3, 4\} \rightarrow \{2, 5, 7, 18\}$  defined by one of the figures below, determine  $f[\{0, 3\}]$ ,  $f[\{1, 3, 4\}]$ ,  $f^{-1}(2)$ ,  $f^{-1}[\{2, 5\}]$ , and  $f^{-1}[\{5, 18\}]$ .



**Problem 4.** Let  $f: X \rightarrow Y$ ,  $A_1, A_2 \subset X$ , and  $B_1, B_2 \subset Y$ . Are the following always true?

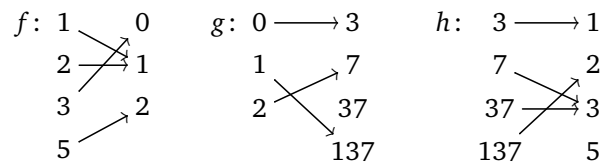
- a)  $f[X] = Y$ ; b)  $f^{-1}[Y] = X$ ; c)  $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$ ;
- d)  $f[A_1 \cap A_2] = f[A_1] \cap f[A_2]$ ; e)  $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$ ;
- f)  $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$ ; g)  $f[A_1] \subset f[A_2] \Rightarrow A_1 \subset A_2$ ;
- h)  $f^{-1}[B_1] \subset f^{-1}[B_2] \Rightarrow B_1 \subset B_2$ ?



**Definition 3.** The *composition of maps*  $f: X \rightarrow Y$  and  $g: Y \rightarrow Z$ , written  $g \circ f$ , is the map that assigns to an element  $x$  in  $X$  the element  $g(f(x))$  in  $Z$ . (In other words, the composition  $g \circ f$  is the successive application of the maps  $f$  and  $g$ .)

**Problem 5.** Prove that for any maps  $f: X \rightarrow Y$ ,  $g: Y \rightarrow Z$ , and  $h: Z \rightarrow W$ , the following holds:  $h \circ (g \circ f) = (h \circ g) \circ f$  (i.e., one can omit parentheses in the expression  $h \circ g \circ f$ ).

**Problem 6.** Let  $f: \{1, 2, 3, 5\} \rightarrow \{0, 1, 2\}$ ,  $g: \{0, 1, 2\} \rightarrow \{3, 7, 37, 137\}$ , and  $h: \{3, 7, 37, 137\} \rightarrow \{1, 2, 3, 5\}$  be the maps defined by the figures below.

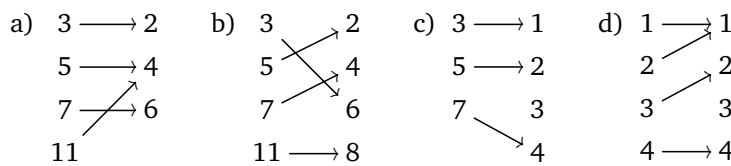


Draw (i.e., represent pictorially) the following maps:

a)  $g \circ f$ ; b)  $h \circ g$ ; c)  $f \circ h \circ g$ ; d)  $g \circ h \circ f$ .

**Definition 4.** A map  $f: X \rightarrow Y$  is said to be *bijective* if for every  $y \in Y$ , there is one and only one  $x \in X$  such that  $f(x) = y$ .

**Problem 7.** For each of the maps defined pictorially below, determine whether it is bijective or not:



**Problem 8.** Draw all bijective maps a) from  $\{1, 2\}$  to  $\{3, 4, 5, 6\}$ ; b) from  $\{1, 2, 3\}$  to  $\{4, 5, 6\}$ .

**Problem 9.** Let  $f: X \rightarrow Y$  and  $g: Y \rightarrow Z$ . Is it true that if  $f$  and  $g$  are bijective, then so is  $g \circ f$ ?

**Definition 5.** A map  $f$  is said to be *injective* provided it maps distinct elements to distinct elements, i.e., if  $f(x) = f(x')$  implies  $x = x'$ .

A map  $f: X \rightarrow Y$  is said to be *surjective* if every element  $y \in Y$  has at least one preimage, i.e.,  $f^{-1}(y) \neq \emptyset$  for every  $y \in Y$ .

**Problem 10.** Show that the following properties of a map  $f: X \rightarrow Y$  are equivalent:

- 1)  $f$  is bijective;
- 2)  $f$  is both injective and surjective;
- 3)  $f$  is *invertible*, i.e., there is a map<sup>13</sup>  $g: Y \rightarrow X$  such that  $g \circ f = \text{Id}_X$ ,  $f \circ g = \text{Id}_Y$ , where  $\text{Id}_M: M \rightarrow M$ ,  $m \mapsto m$  is the identity map.

**Problem 11.** For each pair of the sets below, determine whether there is a bijection from one set to the other.

- a) the set of natural numbers;
- b) the set of even natural numbers;
- c) the set of natural numbers without the number 3;
- d) the set of integers.

---

<sup>13</sup>One then says that  $g$  is the *inverse* of  $f$  and writes  $g = f^{-1}$ .

## Combinatorics 1

Leaflet 3 / September 2004

**Problem 1.** Determine the number of ‘words’<sup>14</sup> consisting of a) two; b) three letters of the alphabet.

**Problem 2.** Determine the number of necklaces consisting of a) three beads of different colors; b) two red and two blue beads; c) three red and two blue beads.

**Problem 3.** How many ways are there to choose two hall monitors together with one senior hall monitor out of 10 people?

**Problem 4.** How many ways are there to choose three hall monitors out of a) five; b) seven; c) ten people?

**Problem 5.** How many ways are there to seat five people in a bus if the bus has a) 4; b) 5; c) 6; d) 7 vacant seats?

**Problem 6.** Seven students of your class decided to ride in the following amusement rides together:

- a) a ride called ‘train’ consisting of seven one-seater rail cars;
- b) a carousel with seven seats;
- c) a ‘train’ with ten one-seater rail cars;
- d) a carousel with ten seats.

In how many ways can they do that?

**Problem 7.** Consider grids of the following sizes: a)  $2 \times 2$ ; b)  $3 \times 3$ ; c\*)  $5 \times 5$ . Suppose that starting at the lower left corner, one can go one step up or one step to the right at each move, until the upper right corner is reached. How many such paths exist?

**Problem 8.** In how many ways can one express the numbers 5, 10, and 20 as a sum of a) two; b) three natural numbers?

**Problem 9.** How many different expressions can one obtain by inserting parentheses into the expression  $a + b - c \cdot d$ ?

**Problem 10.** a) Show that the number of subsets in the set  $\{a, b, c, d, e\}$  equals the number of maps from this set to the set  $\{0, 1\}$ . b) Further, show that this number is also equal to the number of sequences of length five consisting only of zeros and ones.

---

<sup>14</sup>Here, this term means not only words that one can find in a dictionary, but all words that can be obtained by combining letters of the alphabet.

**Problem 11\*.** What is the number of distinct collections of beads from which one can make precisely two distinct necklaces?

**Problem 12\*.** In city  $N$ , bus tickets have four-digit numbers. It is believed in the city that the tickets whose numbers have the property that the sum of the first two digits equals the sum of the last two bring luck. How many tickets in city  $N$  bring luck?

**Problem 13\*.** How many ways are there to paint a ferris wheel a) having 7 carriages, with 3 colors; b) having 10 carriages, with 2 colors? When painting, it is not necessary to use all the colors available.

**Problem 14.** Consider the following polygons: a) hexagon; b\*) heptagon; c\*) octagon. One cuts the above shapes into triangles along nonintersecting diagonals. How many distinct collections of triangles can one obtain?

**Problem 15.** How many distinct dice (i.e., cubes with each of their six faces showing a different number of dots from 1 to 6) exist?

## Permutations 1. Walking around Cycles

Leaflet 1A / October 2004

**Definition 1.** A *permutation on  $n$  elements* is a bijective map from the set  $\{1, 2, \dots, n\}$  to itself. The notation

$$\begin{pmatrix} i_1 i_2 \dots i_n \\ j_1 j_2 \dots j_n \end{pmatrix},$$

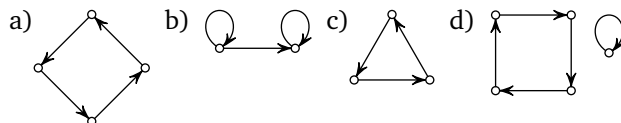
where each of the two collections  $i_1, i_2, \dots, i_n$  and  $j_1, j_2, \dots, j_n$  consists of distinct elements of the set  $\{1, 2, \dots, n\}$ , is used to denote the permutation  $a$  given by  $a(i_k) = j_k$  for all  $k \in \{1, 2, \dots, n\}$ . The set of all permutations of  $n$  elements is denoted by  $S_n$ . A permutation can be also represented pictorially as follows. One places the elements of the set  $\{1, 2, \dots, n\}$  on the plane and, for each  $i$ , one connects the element  $i$  to the element  $a(i)$  by an arrow. The resulting picture is called a *permutation graph*.

**Problem 1.** Which of the following tables define permutations?

- a)  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ; b)  $\begin{pmatrix} 123 \\ 123 \end{pmatrix}$ ; c)  $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ ; d)  $\begin{pmatrix} 123 \\ 234 \end{pmatrix}$ ; e)  $\begin{pmatrix} 123 \\ 333 \end{pmatrix}$ ; f)  $\begin{pmatrix} 514632 \\ 164253 \end{pmatrix}$ ;  
g)  $\begin{pmatrix} 4321 \\ 1234 \end{pmatrix}$ ; h)  $\begin{pmatrix} 5321 \\ 5321 \end{pmatrix}$ ; i)  $\begin{pmatrix} 1327 \\ 7231 \end{pmatrix}$ ; j)  $\begin{pmatrix} 123 \\ 112 \end{pmatrix}$ .

**Problem 2.** Write out and represent pictorially all the elements in the sets  $S_1$ ,  $S_2$ , and  $S_3$ .

**Problem 3.** Which of the following pictures are permutation graphs?



**Problem 4.** a) What is the number of elements in the set  $S_n$ ?

b) How many ways are there to write a permutation of  $n$  elements?

**Definition 2.** The *product* of two permutations  $a, b \in S_n$ , written  $ab$ , is the composition of the corresponding maps:  $ab = a \circ b$ .

**Problem 5.** Compute the following products:

- a)  $\begin{pmatrix} 123 \\ 312 \end{pmatrix} \begin{pmatrix} 312 \\ 123 \end{pmatrix}$ ; b)  $\begin{pmatrix} 1234 \\ 4321 \end{pmatrix} \begin{pmatrix} 1234 \\ 2143 \end{pmatrix}$ ; c)  $\begin{pmatrix} 124536 \\ 123456 \end{pmatrix} \begin{pmatrix} 642351 \\ 123456 \end{pmatrix}$ ;  
d)  $\begin{pmatrix} 12345 \\ 24531 \end{pmatrix} \begin{pmatrix} 12345 \\ 35124 \end{pmatrix}$ ; e)  $\begin{pmatrix} 123456 \\ 561423 \end{pmatrix} \begin{pmatrix} 123456 \\ 345261 \end{pmatrix}$ .

**Problem 6.** Is it true that for all permutations  $a, b \in S_n$ , one has the equality  $ab = ba$ ?

**Definition 3.** The permutation  $e = \begin{pmatrix} 12 \dots n \\ 12 \dots n \end{pmatrix}$  is called the *identity permutation*.

**Problem 7.** Prove the following assertions:

- a) for every permutation  $a \in S_n$ , one has  $ae = ea = a$ ;
- b) for all permutations  $a, b, c \in S_n$ , one has  $(ab)c = a(bc)$ ;
- c) for every permutation  $a \in S_n$ , there is one and only one permutation  $b \in S_n$  such that  $ab = ba = e$ .

**Definition 4.** Let  $1 \leq i, j \leq n$ ,  $i \neq j$ . Any permutation  $a$  such that  $a(i) = j$ ,  $a(j) = i$ , and  $a(k) = k$  for  $k \neq i, j$  is called a *transposition*. We shall use the symbol  $(i\ j)$  to denote such a transposition.

**Definition 5.** Let  $i_1, i_2, \dots, i_k$  be distinct elements of the set  $\{1, 2, \dots, n\}$ . Any permutation  $a$  that moves the elements  $i_1, i_2, \dots, i_k$  in a cyclic fashion, i.e., a permutation  $a$  such that  $a(i_j) = i_{j+1}$  for  $j \in \{1, 2, \dots, k-1\}$ ,  $a(i_k) = i_1$ , and  $a(s) = s$  for  $s \notin \{i_1, i_2, \dots, i_k\}$ , is said to be a *k-cycle*. We write  $(i_1\ i_2 \dots i_k)$  for such a cycle and call  $k$  the *length* of the cycle.

**Problem 8.** a) Which of the permutations in Problems 1 and 2 are cycles? Which of them are transpositions?

- b) How many cycles of length 57 does the set  $S_{57}$  contain?
- c) Determine the number of cycles and transpositions in  $S_5$ .
- d) When is the product of two transpositions a cycle?
- e\*) When is the product of two cycles a cycle?

**Definition 6.** Cycles made up of disjoint sets of indices are said to be *independent* or *disjoint*.

**Problem 9\*.** a) Show that every permutation can be written as a product of disjoint cycles.

- b) Show that every permutation can be written as a product of transpositions.
- c) Show that every permutation in  $S_n$  can be written as a product of at most  $n - 1$  transpositions.
- d) Is it true that any permutation in  $S_n$  can be written as a product of disjoint transpositions?

## Mathematical Induction

Leaflet 4 / October 2004

**Convention.** In this leaflet, the letters  $m$ ,  $n$  and  $k$  denote positive integers.

**Well-ordering principle.** Every nonempty subset of the set of natural numbers has a least element, meaning an element that is smaller than every other element in the subset.

**Problem 1.** a) Will the previous statement remain true if 'the set of natural numbers' is replaced by 'the set of integers'?

b) Will the previous statement remain true if 'least element' is replaced by 'greatest element'?

**Problem 2.** On an island all countries are shaped like a triangle. If two countries share an edge they are called neighbors. Prove that the countries can be colored using 3 colors so that every two neighbor countries will be of different colors.

**Principle of mathematical induction.** Let  $A_1, A_2, \dots, A_k, \dots$  be a sequence of statements such that:

1) Base of induction: The first statement is true.

2) Inductive step: For all  $n \geq 1$ , if  $A_n$  is true, then so is  $A_{n+1}$ .

Then all the statements are true.

(This principle may be used without proving it. Sometimes it is assumed as an axiom.)

**Problem 3\*.** Prove the principle of mathematical induction using the well ordering principle.

**Problem 4.** On an island any two cities are directly connected either by a highway or a railroad. Prove that either you can travel between any two cities by car or you can travel between any two cities by train.

**Problem 5.** The plane is divided into several regions by  $n$  lines. Prove that these regions can be colored using 2 colors so that any two regions sharing a common segment or ray will be of different colors.

**Problem 6.** Prove by induction that:

a)  $1 + \dots + n = \frac{n(n+1)}{2}$ ; b)  $1^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ ;

c)  $1^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$ .

**Problem 7.** Find a mistake in the following proofs.

a) Let us prove that  $n > n + 1$ .

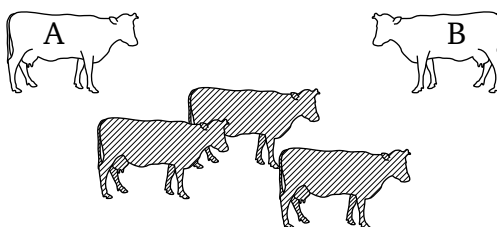
Suppose this statement is true for some  $n$ , meaning that  $n > n + 1$ . Adding one to both sides of the inequality we obtain  $n + 1 > n + 1 + 1$ , so the statement is also true for  $n + 1$ .

b) Let us prove that in any herd of  $N$  cows, all cows are of the same color.

Base of induction: in any herd of one cow, all cows are of the same color.

Inductive step. Suppose that in any herd of  $N$  cows, all cows are of the same color. Let us prove that in any herd of  $N + 1$  cows, all cows are of the same color.

Consider a herd of  $N + 1$  cows. Choose some cow A. The remaining  $N$  cows are all of the same color. Choose a different cow B. The remaining  $N$  cows are also all of the same color. In particular A is of the same color as all the cows, except maybe B, and B is of the same colors as all the cows, except maybe A (see figure). It follows that A, B and all the other cows are of the same color.



c) There are several cities in a country. Some of them are connected by roads, and every city is connected to at least one other city. Let us prove that we can travel from any city to any other city using the roads. The base of induction (when there is only one city) is obvious. Let us prove the inductive step. Take a country with  $n$  cities and add a new city. We can travel from any old city to any other old city, so it remains to show that we can travel from the new city to every old city. The new city must be connected to at least one other city. It follows that we can travel to at least one old city from the new one, and from then on we can travel to any old city. We have shown that in this new country we can travel from any city to any other city, so the induction step is complete.

**Problem 8.** Into how many regions do  $n$  lines in general position divide the plane? (We say that  $n$  lines are in general position if no two lines are parallel and no three intersect at a single point.)



**Problem 9.** Prove for all  $n \geq 1$  that:

- a)  $2^{5n+3} + 5^n \cdot 3^{n+2}$  is divisible by 17;
- b)  $n^{2m-1} + 1$  is divisible by  $n + 1$ ;
- c\*)  $2^{3^n} + 1$  is divisible by  $3^{n+1}$ .

**Problem 10 (Bernoulli's inequality).** Prove that if  $a > -1$ , then for all  $n \geq 1$

$$(1 + a)^n \geq 1 + na.$$

**Problem 11.** Prove that:

- a)  $2^n > n$  for  $n \geq 1$ ; b)  $2^n > n^2$  for  $n > 4$ ; c)  $n! > 2^n$  for  $n > 3$ ;
- d\*) there exists a  $k$  such that  $2^n > n^{2004}$  for all  $n > k$ .

**Problem 12.** The vertices of a convex polygon are colored using exactly 3 colors so that any two adjacent vertices are of different colors. Prove that the polygon can be divided into triangles, using its diagonals, so that each triangle has vertices of all 3 colors.

**Generalized principle of mathematical induction.** Let  $A_1, A_2, \dots, A_k, \dots$  be a sequence of statements such that:

- 1) Base of induction: The first statement is true,
  - 2) Inductive step: If  $A_1, A_2, \dots, A_n$  are true, then so is  $A_{n+1}$ .
- Then all the statements are true.

**Problem 13\*.** Prove the generalized principle of mathematical induction.

**Problem 14.** Prove that if  $a + 1/a$  is an integer, then  $a^k + 1/a^k$  is also an integer for any  $k$ .

**Problem 15\*.** In a class every noisy student is friends with at least one quiet student. A noisy student is silent if he/she has an odd number of his/her quiet friends in the classroom. Prove that the teacher can kick out of the classroom no more than half the students, so that all the noisy students will be silent.

**Problem 16\* (Sylvester's problem).** Given at least 3 points in the plane such that any line passing through two of them contains at least one more given point, prove that all the points are on one line.

**Problem 17\*.** Prove that  $n^{n+1} > (n+1)^n$  for  $n \geq 3$ .

## Combinatorics 2. The Binomial Theorem

Leaflet 5 / October 2004

**Definition 1.** Pascal's triangle is a triangular array constructed using the following rule: in the  $n$ -th row there are  $n$  numbers, the first and last number of every row is 1, and every other number is equal to the sum of the two closest numbers in the row above. The number in the  $(k + 1)$ -st column and  $(n + 1)$ -st row is denoted by  $\binom{n}{k}$ .

$$\begin{array}{cccccccc}
 & & & & 1 & & & \\
 & & & 1 & & 1 & & \\
 & & 1 & & 2 & & 1 & \\
 & 1 & & 3 & & 3 & & 1 \\
 1 & & 4 & & 6 & & 4 & & 1 \\
 \dots\dots\dots & & & & & & & & 
 \end{array}$$

**Problem 1.** Write out the two numbers in the  $n$ -th row closest to the number  $\binom{n}{m}$  in the form  $\binom{a}{b}$ .

**Problem 2.** Write out the first 11 rows of the Pascal's triangle.

**Problem 3.** Prove that  $\binom{n}{k} = \binom{n}{n-k}$  for  $n \geq 0$  and  $0 \leq k \leq n$ .

**Problem 4.** Prove that the number of paths from the bottom left corner to the upper right corner in an  $m \times n$  rectangle, moving only up and to the right along the cells, is equal to  $\binom{n+m}{m}$ .

**Problem 5.** Which rows of Pascal's triangle contain only odd numbers?

**Definition 2.** The number of subsets of size  $m$  in a set with  $n$  elements is denoted by  $C_n^m$ .

**Problem 6.** Find: a)  $C_{100}^1$ , b)  $C_4^2$ , c)  $C_5^2$ , d)  $C_6^4$ .

**Problem 7.** Prove that: a)  $C_n^k = C_n^{n-k}$ ; b)  $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$ .

**Problem 8.** Prove that  $\binom{n}{k} = C_n^k$  for all  $n \geq 0$  and  $0 \leq k \leq n$ .

**Problem 9.** Expand the expressions: a)  $(a+b)^3$ ; b)  $(a+b)^4$ ; c)  $(2a+3b)^4$ .

**Problem 10 (The Binomial Theorem).** a) Expand the expressions  $(a+b)$ ,  $(a+b)^2$ ,  $(a+b)^3$ ,  $(a+b)^4$  and write the results one under the other. Observe that the coefficients form Pascal's triangle.

b) Prove that

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{n}b^n.$$

**Problem 11.** Prove that:

- a)  $\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n$  for all  $n \geq 0$ ;  
 b)  $\binom{n}{0} - \binom{n}{1} + \dots + (-1)^n \binom{n}{n} = 0$  for all  $n \geq 1$ .

**Problem 12.** Prove that  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$  for all  $n \geq 0$  and  $0 \leq k \leq n$ .

**Problem 13.** Prove that:

- a)  $\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2 = \binom{2n}{n}$ ;  
 b)  $\binom{n}{0} + \binom{n+1}{1} + \dots + \binom{n+k-1}{k-1} + \binom{n+k}{k} = \binom{n+k+1}{k}$ ;  
 c)  $\binom{n}{1} + 2\binom{n}{2} + \dots + n\binom{n}{n} = n \cdot 2^{n-1}$ ;  
 d)  $\binom{n}{k} \cdot \binom{n-k}{m-k} = \binom{m}{k} \cdot \binom{n}{m}$ .

**Problem 14.** In a 16-element set, are there more subsets that contain less than 8 elements, more than 8 elements, or exactly 8 elements?

**Problem 15.** Find the number of 0-1 sequences of length 16 that contain at least three ones.

**Problem 16.** Solve the problems selected by the teacher from the leaflet 'Combinatorics 1' for arbitrary  $n$  and  $k$ .

**Problem 17\*.** How many ways are there to choose nonnegative integers  $x_1, x_2, \dots, x_m$  so that  $x_1 + x_2 + \dots + x_m = n$ ?

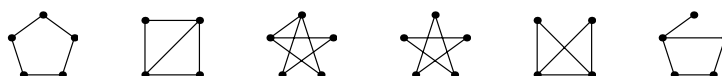
# Graph Theory 1

Leaflet 6 / November 2004

**Definition 1.** A graph<sup>15</sup> is a pair  $\Gamma = (V, E)$  consisting of a finite set of vertices  $V$  and set of edges  $E$ , whose elements are (unordered) pairs of vertices. A graph can be thought of as a set of points, some of which are connected by segments ('edges').

**Definition 2.** Two graphs  $\Gamma_1$  and  $\Gamma_2$  are called *isomorphic*, if there exist a bijection  $f: V(\Gamma_1) \rightarrow V(\Gamma_2)$  such that two vertices  $A$  and  $B$  in the graph  $\Gamma_1$  are connected by an edge if and only if the vertices  $f(A)$  and  $f(B)$  are connected by an edge in the graph  $\Gamma_2$ .

**Problem 1.** Which of the following graphs are isomorphic to each other?



**Problem 2.** Draw all possible graphs, no two being isomorphic, with at most 4 vertices.

**Problem 3.** Draw a graph whose vertices are the natural numbers 2 through 15, so that there is an edge connecting every two numbers such that one is divisible by the other.

**Problem 4.** a) Construct a graph with 5 vertices such that no three of its vertices are either all pairwise connected or all pairwise disconnected.

b) Prove that for any six people either there are three people who all know each other, or three people who do not know each other.

**Problem 5.** Suppose that in a company of people among any three at least two are friends. Is it always possible to divide the set into two groups of people such that everybody in each group are friends?

**Problem 6.** Find the greatest number of edges in a graph with  $n$  vertices, assuming that among any three of its vertices, there are at least two not connected by an edge.

**Definition 3.** The *degree* (or *valency*) of a vertex  $A$  is the number of edges connected to it. It is denoted by  $\deg A$ .

**Problem 7.** Compute the valencies of all the vertices in the graphs from Problems 1, 2 and 3.

**Problem 8.** Prove that in any graph with at least two vertices there must be two vertices of the same valency.

<sup>15</sup>more precisely, an *unoriented graphs with no loops or multiple edges*.

**Problem 9.** Prove that the sum of valencies of all the vertices in a graph is equal to twice the number of edges.

**Definition 4.** A *path* in a graph is a finite sequence of vertices and edges connecting them, i.e., a sequence of the form  $v_0e_1v_1e_2v_2\dots e_nv_n$ , where  $v_i$  is a vertex of the graph, and  $e_i$  is the edge connecting  $v_{i-1}$  and  $v_i$ . The number  $n$  is called the *length of the path*. A *cycle* is a path such that the first and the last vertex coincide.

In graphs with no multiple edges, each path is uniquely determined by the sequence of its vertices, so usually this sequence is the one written out. For technical reasons, it is convenient to include the edges in the definition.

**Definition 5.** A graph  $\Gamma$  is *Hamiltonian* if there exists a path that contains each vertex exactly once.

**Problem 10.** Prove that the vertices and edges of the dodecahedron and the icosahedron, viewed as graphs, are Hamiltonian.

**Definition 6.** A graph is *connected* if for any two vertices there is a path starting at one of them and ending at the other.

**Problem 11.** Which of the graphs from Problems 1, 2, and 3 are connected?

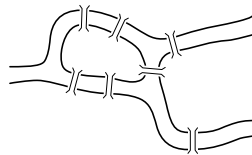
**Problem 12.** Prove that if a graph with more than one vertex is connected, then the valency of every vertex is nonzero. Is the converse true?

**Definition 7.** A *tree* is a connected graph that contains no cycles (i.e., no paths in which the first and last vertex coincide) all of whose edges are different.

**Problem 13.** Prove that in any tree there is: a) at least one vertex of valency 1; b) at least 2 vertices of valency 1.

**Problem 14.** Prove that a tree with  $n$  vertices has  $n - 1$  edges.

**Problem 15.** The figure below depicts the bridges of Königsberg in the 18th century. Is it possible to devise a walk that crosses each bridge exactly once?



**Definition 8.** A graph is *Eulerian* if there exists a cycle that visits each edge exactly once.

**Problem 16.** Which of the following graphs are Eulerian?



**Problem 17.** Prove that a graph is Eulerian if and only if it is connected and the valency of every vertex is even.

**Problem 18\*.**  $N$  teams participated in a tournament with no draws. Each team played every other team exactly once. Prove that the teams can be numbered so that for each  $i = 1, \dots, n-1$  the  $(i+1)$ -st team beat the  $i$ -th team.

**Problem 19\* (Ramsey's theorem).** a) Prove that for any two natural numbers  $m$  and  $n$  there exists a positive integer  $k$  such that in any graph with  $k$  vertices there are either  $m$  pairwise adjacent vertices or  $n$  pairwise nonadjacent ones. The smallest such number is denoted by  $R(m, n)$ .

b) Find  $R(3, 4)$ .

**Definition 9.** Define the *distance* between two vertices in a graph as the length of the shortest path between them (the length of every edge is assumed to be 1). The *diameter* of a graph is the greatest distance between two of its edges.

**Definition 10.** A graph is *k-regular* if the valency of each of its vertices is equal to  $k$ .

**Definition 11.** A *Moore graph* is a  $k$ -regular graph of diameter 2 and  $k^2 + 1$  vertices.

**Problem 20\*.** a) Prove that a  $k$ -regular graph of diameter 2 cannot have more than  $k^2 + 1$  vertices.

b) Give an example of a Moore graph for  $k = 1, 2, 3$ .

c) Does there exist a Moore graph for  $k = 7$ ?

d\*\*) Does there exist a Moore graph for  $k = 57$ ?

e) Prove that for other values of  $k$  no Moore graphs exist.

**Problem 21\*.** Doctor Faust is standing on a vertex of a regular 50-gon. He can do one of three things 1) move to the opposite vertex for free 2) pay Mephistopheles 1 dollar and 5 cents to move to the adjacent vertex in the counterclockwise direction 3) take 1 dollar and 5 cents from Mephistopheles and move to the adjacent vertex in the clockwise direction. Suppose Doctor Faust visits every vertex at least once. Prove that at some point one of them paid the other at least 25 dollars.

## Permutations 2

Leaflet 2A / December 2004

**Definition 1.** In a permutation  $\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ , a pair  $(k, l)$ ,  $1 \leq k < l \leq n$ , such that  $j_k > j_l$  is called an *inversion*. A permutation is *even* if it has an even number of inversions, and *odd* otherwise.

**Problem 0.** Define the *parity* of a permutation written in two-line form as the parity of the sum of the number of inversions in the top and bottom line. Prove that this definition is equivalent to the one above (i.e., all permutations that are even (odd) by Definition 1, are also even (odd) by this new definition, and vice versa).

**Problem 1.** Determine the parity of the permutations in Problems 1, 2 from the leaflet 'Permutations 1'.

**Problem 2.** Let  $a$  and  $b$  be permutations of a set of four elements:  $a = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}$  and  $b = \begin{pmatrix} 1234 \\ 4213 \end{pmatrix}$ . Determine the parities of the following permutations:

a)  $e$ ; b)  $a$ ; c)  $b$ ; d)  $b^2 = b \cdot b$ ; e)  $b^3 = b \cdot b \cdot b$ ; f)  $ab$ ; g)  $ba$ .

**Problem 3.** Prove that a) multiplying by a transposition (on either side) changes parity; b) the parity of the product of  $k$  transpositions is equal to the parity of  $k$ .

**Problem 4.** a) Express the parity of  $ab$  using the parity of  $a$  and the parity of  $b$ .

b) Express the parity of  $a^n$  using  $n$  and the parity of the permutation  $a$ .

**Problem 5.** Are there more odd or even permutations in  $S_n$ ?

**Problem 6\*.** Prove that if you swap the tiles '15' and '14' in the '15-puzzle', then while playing the game, it is impossible to get back to the initial arrangement shown below.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

**Problem 7\*.** Prove that from any starting arrangement of the tiles, you can either produce the initial arrangement or the arrangement described in the previous problem.

**Definition 2.** A permutation *inverse* to the permutation  $a$  is a permutation  $b$  such that  $ab = ba = e$ . It is denoted by  $a^{-1}$ .

**Problem 8.** Prove that  $(ab)^{-1} = b^{-1}a^{-1}$  for all permutations  $a$  and  $b$ .

**Problem 9.** Find all  $a \in S_n$  such that for every  $b \in S_n$  we have: a)  $ba = b$ ; b)  $ba = ab$ ; c\*)  $ba = ab^{-1}$ .

**Problem 10\* (change of labels).** Let  $a, c \in S_n$ , and  $b = cac^{-1}$ .

a) Prove that if the permutation  $a$  is given by the table  $a = \begin{pmatrix} i_1 \dots i_n \\ j_1 \dots j_n \end{pmatrix}$ , then  $b = \begin{pmatrix} c(i_1) \dots c(i_n) \\ c(j_1) \dots c(j_n) \end{pmatrix}$ .

b) Prove that if the permutation  $a$  is presented as a product of independent cycles  $a = (i_1 \dots i_k) \cdot (j_1 \dots j_l) \cdot \dots$ , then

$$b = (c(i_1) \dots c(i_k)) \cdot (c(j_1) \dots c(j_l)) \cdot \dots$$

**Problem 11.** Give a definition of the *power* of a permutation  $a^k$  for any integer  $k$  positive, negative or zero.

**Problem 12.** Prove that for all  $a, b \in S_n$  and all integers  $k$  and  $l$ , we have: a)  $a^0 = e$ ;  $a^1 = a$ ;  $a^{k+l} = a^k a^l$ ;  $a^{kl} = (a^k)^l$ ; b) if  $ab = ba$ , then  $(ab)^k = a^k b^k$ .

**Problem 13.** a) Prove that for any  $a, b \in S_n$ , there exist unique  $x, y \in S_n$ , such that  $ax = b$  and  $ya = b$ . Is  $x$  necessarily equal to  $y$ ?

b) Prove that for any  $a, b, c \in S_n$

$$(a = b) \Leftrightarrow (ac = bc) \Leftrightarrow (ca = cb).$$

**Problem 14.** Prove that for any  $a \in S_n$  there exists a natural number  $k$  such that  $a^k = e$ .

**Definition 3.** The *order* of a permutation  $a$  is the smallest natural number  $k$  such that  $a^k = e$ .

**Problem 15.** Let  $\sigma$  be equal to the product of disjoint cycles  $c_1, \dots, c_n$ . Prove that the order of the permutation  $\sigma$  is equal to  $\text{lcm}(|c_1|, \dots, |c_n|)$ , the least common multiple of  $|c_1|, \dots, |c_n|$  (here  $|c_i|$  denotes the length of the cycle  $c_i$ ).

**Problem 16.** Prove that if  $k$  is the order of a permutation  $a$ , then  $a^n = e$  if and only if  $n$  is divisible by  $k$ .

**Problem 17.** Compute: a)  $\begin{pmatrix} 123 \\ 321 \end{pmatrix}^{100}$ ; b)  $\begin{pmatrix} 1234 \\ 2341 \end{pmatrix}^{1000}$ ; c)  $\begin{pmatrix} 12345 \\ 35214 \end{pmatrix}^{-2007}$ ;  
d)  $\begin{pmatrix} 12345 \\ 45213 \end{pmatrix}^{500}$ ; e)  $\begin{pmatrix} 123456 \\ 452631 \end{pmatrix}^{-127}$ ; f)  $\begin{pmatrix} 1234567 \\ 7651234 \end{pmatrix}^{1001}$ .



## Integers 1. Divisibility of Integers

Leaflet 7 / December 2004

**Convention.** All numbers in this leaflet are assumed to be integers.

**Definition 1.** An integer  $a$  is *divisible* by a nonzero number  $b$ , written  $a : b$ , if there is an integer  $k$  such that  $a = kb$ . One also expresses this by saying that  $b$  *divides*  $a$  and writes  $b \mid a$ . The number  $b$  above is called a *divisor* of  $a$ .

**Problem 1.** Show that for each integer  $a$ , the following holds:

a) if  $a \neq 0$ , then  $a \mid a$ ; b)  $1 \mid a$ ; c) if  $a \neq 0$ , then  $a \mid 0$ .

**Problem 2.** Show that for all  $a, b, c, x$ , and  $y$ , the following holds:

- a) if  $b \mid a$  and  $c \mid b$ , then  $c \mid a$ ;
- b) if  $b \mid a$  and  $a \neq 0$ , then  $|a| \geq |b|$ ;
- c) if  $c \neq 0$ , then  $b \mid a \Leftrightarrow bc \mid ac$ ;
- d) if  $b \mid a$  and  $b \mid c$ , then  $b \mid (a \pm c)$ ;
- e) if  $b \mid a$  and  $b \mid c$ , then  $b \mid (ax + cy)$ ;
- f) if  $b \mid a$  and  $a \mid b$ , then  $a = b$  or  $a = -b$ ;
- g) if  $b \mid a$ , then  $b \mid ac$ ;
- h) if  $b \mid a$  and  $b \nmid c$ , then  $b \nmid (a + c)$ ;
- i) if  $ab = cd$  and  $c \mid a$  ( $c \neq 0$ ), then  $b \mid d$ .

**Problem 3.** Is it true that for all  $a, b, c$ , and  $d$ , the following holds?

- a) if  $b \mid a$  and  $c \nmid b$ , then  $c \nmid a$ ;
- b) if  $b \mid a$  and  $c \mid a$ , then  $bc \mid a$ ;
- c) if  $c \mid ab$ , then  $c \mid a$  or  $c \mid b$ .

**Problem 4.** State divisibility conditions by the following numbers: a) 2; b) 3; c) 4; d) 5; e) 9; f) 11.

**Problem 5.** Is it possible for a number whose digits add up to 2004 to be a perfect square?

**Problem 6\*.** A number  $a$  equals three times the sum of its digits. Prove that  $a$  is divisible by 27.

**Problem 7.** Prove the following: a) if  $(a + b) \mid a^2$ , then  $(a + b) \mid b^2$ ; b\*) if  $x + y + z \neq 0$ , then  $(x + y + z) \mid (x^3 + y^3 + z^3 - 3xyz)$ .

**Problem 8.** Which positive integers have an odd number of positive divisors?

**Definition 2.** A number  $p > 1$  is said to be *prime* if its only divisors are 1,  $-1$ ,  $p$ , and  $-p$ . The other natural numbers, 1 being excluded, are said to be *composite*.

**Problem 9.** Prove that there are infinitely many prime numbers.

**Problem 10.** Prove that for each  $n \geq 1$ , there exist  $n$  consecutive composite numbers.

**Problem 11\*.** Write  $n?$  for the product of all primes less than  $n$ . Show that  $n? > n$  provided  $n > 3$ .

**Problem 12.** a) Find all primes  $p$  such that both  $p + 2$  and  $p + 4$  are prime.

b\*\*) Show that there are infinitely many *twin primes*, i.e., primes  $p$  such that  $p + 2$  is prime.

**Problem 13 (The Sieve of Eratosthenes).** The integers from 2 through 1000 are listed on a board. Eratosthenes circles the number 2 and erases all multiples of 2 except 2 itself. He then proceeds similarly by circling the least number that is not circled and erases all multiples of that number, leaving the last circled number unerased. When no number on the board remains uncircled, the process terminates. What are the numbers left on the board? (You do not need to list them.)

**Problem 14.** List all primes less than 100.

**Problem 15.** Prove that  $a$ ,  $a > 1$ , is composite if and only if  $a$  is divisible by a prime no greater than  $\sqrt{a}$ .

**Problem 16.** Prove the following:

- a) Every integer greater than 1 can be written as a product of primes;
- b) Every integer  $x$  greater than 1 can be written as

$$x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

where  $p_1 < p_2 < \cdots < p_n$  are primes and  $a_1, a_2, \dots, a_n$  are positive integers;

c\*) (*Fundamental Theorem of Arithmetic*) If an integer  $x$  is written in the above form in two ways, i.e.,

$$x = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m},$$

then these factorizations coincide, i.e.,  $m = n$  and for all  $1 \leq i \leq n$ , one has  $p_i = q_i$  and  $a_i = b_i$ ;

d) If all  $a_i$  in the above decomposition are even, then  $x$  is a perfect square, i.e., there is an integer  $y$  such that  $x = y^2$ .

**Problem 17.** Factor the following into primes: 1024, 57, 84, 91, 391, 101, 1000, 1001, 1543.

## Integers 2. The Euclidean Algorithm

Leaflet 8 / December 2004

**Convention.** All numbers in this leaflet are assumed to be integers.

**Problem 1.** Show that for every  $a$  and every  $b \neq 0$ , there exist unique  $q$  and  $r$  such that 1)  $a = bq + r$ ; 2)  $0 \leq r < |b|$ .

**Definition 1.** Such  $q$  and  $r$  as above are called, respectively, the *quotient* and the *remainder* in the division of  $a$  by  $b$ .

**Problem 2.** Determine the quotient and the remainder in the division of  
a)  $-17$  by  $4$ ; b)  $23$  by  $-7$ ; c)  $-1$  by  $-5$ .

**Problem 3.** What are the possible quotients in division of the number  $59$ ?

**Problem 4.** Determine the quotient and the remainder in the division of  
a)  $n^2$  by  $n + 1$ ; b)  $n^2 + n + 2$  by  $n - 1$ , where  $n > 5$ ; c)  $2^{100} - 1$  by  $2^7 - 1$ ;  
d\*)  $2^m - 1$  by  $2^n - 1$ .

**Problem 5\*.** a) Show that  $a^{2k+1} + 1$  is always evenly divisible (i.e., divisible without remainder) by  $a + 1$ .

b) Find the remainder in the division of  $a^{2k} + 1$  by  $a + 1$ .

**Definition 2.** The *greatest common divisor* of two integers  $a$  and  $b$ , written  $\gcd(a, b)$ , is the largest integer  $d$  such that  $d \mid a$  and  $d \mid b$ .

**Problem 6.** Show that for all  $a$  and  $b$ , not both zero,  $\gcd(a, b)$  exists and is unique.

**Problem 7.** Show that for all  $a$  and  $b$ , where not both of  $a$  and  $b$  are zero, one has the following:

a)  $\gcd(a, b) \geq 1$ ; b)  $\gcd(a, b) = |a| \Leftrightarrow a \mid b$ ;

c)  $\gcd(a, ca + b) = \gcd(a, b)$ .

**Problem 8 (Euclidean Algorithm).** Consider the following procedure. Let  $(a, b)$  be a pair of positive integers such that  $a \geq b$ . Replace that pair by  $(b, r)$ ,  $r$  being the remainder in the division of  $a$  by  $b$ . Then replace the pair  $(b, r)$  following the same rule, and so on. The process stops once a pair of the form  $(d, 0)$  is obtained. Prove the following:

a) the above process always terminates;

b)  $d = \gcd(a, b)$ .

**Problem 9.** Using the Euclidean algorithm, compute the following:

a)  $\gcd(91, 147)$ ; b)  $\gcd(-144, -233)$ .

**Problem 10.** Let  $0 < a < 1000$ ,  $0 < b < 1000$ . Is it true that the Euclidean algorithm applied to  $(a, b)$  terminates after no more than a) 14; b) 13 steps?

**Problem 11.** Let  $a$  and  $b$  be integers. Demonstrate how, with the aid of the Euclidean algorithm, one can find integers  $k$  and  $l$  which satisfy the equation  $ak + bl = \gcd(a, b)$ .

**Problem 12.** Show that the equation  $ax + by = d$  has an integer solution if and only if  $\gcd(a, b) \mid d$ . In particular,  $\gcd(a, b)$  is the least possible natural number expressible in the form  $ax + by$ .

**Problem 13.** Given two angles of  $32^\circ$  and  $25^\circ$ , construct an angle of  $1^\circ$ .

**Problem 14.** Let  $p$  be a prime. Show that either  $a$  is divisible by  $p$ , or else there are  $x$  and  $y$  such that  $ax + py = 1$ .

**Problem 15.** Let  $p$  be a prime. Show that if  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

**Problem 16.** Prove the fundamental theorem of arithmetic (Problem 16c in the leaflet 'Integers 1').

**Definition 3.** The *least common multiple* of two numbers  $a$  and  $b$ , written  $\text{lcm}(a, b)$ , is the smallest positive integer  $d$  such that  $a \mid d$  and  $b \mid d$ .

**Problem 17.** Show that for any  $a$  and  $b$ , not both zero, the following holds:

- a)  $\text{lcm}(a, b)$  exists and is unique;
- b)  $\text{lcm}(a, b) \cdot \gcd(a, b) = ab$ .

**Problem 18.** Find  $\text{lcm}(12, 15)$  and  $\text{lcm}(120, 45)$ .

**Problem 19.** Let  $(x_0, y_0)$  be a solution of the equation  $ax + by = d$ . Write  $a_0$  and  $b_0$  for the numbers such that  $\gcd(a, b)a_0 = a$  and  $\gcd(a, b)b_0 = b$ . Show that every solution of the equation  $ax + by = d$  is of the form

$$x = x_0 + b_0 t, \quad y = y_0 - a_0 t,$$

where  $t \in \mathbb{Z}$ .

**Problem 20.** Solve the following equations in integers:

- a)  $121x + 91y = 1$ ; b)  $-343x + 119y = 42$ ; c)  $111x - 740y = 11$ .

**Problem 21\*.** Consider a chocolate bar having the form of an equilateral triangle whose side length is  $n$ . Suppose the bar is subdivided by furrows into equilateral triangles of side length 1. Two people play the following game. At each move, a player breaks off a chunk of chocolate in the shape

of a triangle bounded by the furrows, eats it, and gives the leftover to the second player. The one who obtains the last piece, a triangle of side length 1, wins. If a player cannot move, this player loses the game prematurely. Who wins, assuming that the game does not end prematurely?

## Equivalence Relations

Leaflet 9 / January 2005

**Definition 1.** Let  $M$  be a set. A (binary) relation on  $M$  is a collection of ordered pairs of elements of  $M$ , i.e., a subset  $R$  of the set  $\{(a, b) \mid a, b \in M\}$ . If  $(a, b) \in R$ , then one writes  $a \sim_R b$  or merely  $a \sim b$  for short.

**Problem 0.** Write the table and draw the graph  $(M, R)$  for each of the following relations:

- a)  $a \sim_R b$  if  $a \equiv b \pmod{2}$  on  $X = \{0, \dots, 9\}$ .
- b)  $a \sim_R b$  if  $b \mid a$  on  $X = \{2, \dots, 15\}$  (do not draw the relation graph for this relation).
- c)  $A \sim_R B$  if  $A \subset B$  on the set of all subsets of  $\{0, 1, 2\}$ .
- d)  $a \sim_R b$  if  $a = b$  on  $X = \{0, \dots, 5\}$ .
- e)  $a \sim_R b$  if  $a \geq b$  on  $X = \{0, \dots, 5\}$ .

**Definition 2.** A relation  $\sim$  on  $M$  is said to be

- 1) *reflexive* if for all  $a \in M$ , one has  $a \sim a$ ;
- 2) *symmetric* if for all  $a, b \in M$ ,  $a \sim b$  implies  $b \sim a$ ;
- 3) *transitive* if for all  $a, b, c \in M$ ,  $a \sim b$  and  $b \sim c$  implies  $a \sim c$ .

**Problem 1.** How many relations are there on an  $n$ -element set? How many of them are symmetric?

**Problem 2.** Give examples of relations satisfying exactly one and two conditions of Definition 2.

**Definition 3.** A relation  $\sim$  on  $M$  is called an *equivalence relation* if it is reflexive, symmetric, and transitive.

**Problem 3.** Which of the following relations are reflexive, symmetric, or transitive? Which of them are equivalence relations? (The conditions in quotes are those under which  $a \sim b$ .)

- a)  $a \sim b$  for all  $a, b \in M$  on a set  $M$ ;
- b)  $\emptyset$  on a set  $M$ ;
- c) ' $a \mid b$ ' on the set of natural numbers;
- d) ' $a$  and  $b$  can be joined by a path' on the set of vertices of a graph;
- e) ' $A \subset B$ ' on the set of subsets of a given set;
- f) ' $a$  and  $b$  have the same remainder when divided by 2' on the set of natural numbers;
- g) ' $a$  and  $b$  have the same last digit' on the set of natural numbers;
- h) ' $a$  and  $b$  study in the same form' on the set of students of your school;
- i) ' $a$  and  $b$  were born in the same month' on the set of students of your class.

- j) 'there is a bijection between  $a$  and  $b$ ' on the set of subsets of natural numbers;
- k) ' $a > b$ ' on the set of natural numbers;
- l) for a fixed subset  $X \subset M$ , the following relation on  $M$ : ' $a \sim a$ , and if  $a \neq b$ , then  $a \sim b$  if and only if  $a, b \in X$ ';
- m) for a fixed function  $f: X \rightarrow Y$ , the following relation on  $X$ : ' $a \sim b$  if and only if  $f(a) = f(b)$ ';
- n) ' $a$  and  $b$  are citizens of the same state' on the set of all people on Earth;
- o) 'triangle  $T_1$  has all three side lengths equal to those of triangle  $T_2$ ' on the set of all triangles in the plane;
- p) a relation of your choice on the set of natural numbers;
- q) a relation of your choice on the set of students of your school.

**Problem 4.** Prove that an equivalence relation on a set defines an equivalence relation on every subset of the set.

**Definition 4.** Let  $\sim$  be an equivalence relation on a nonempty set  $M$ , and  $a \in M$ . The set  $N_a = \{x \in M \mid a \sim x\}$  is called the *equivalence class* of the element  $a$ .

**Problem 5.** Given an equivalence relation on a set  $M$ , show that two subsets of  $M$  that are equivalence classes are either disjoint or coincide. Show that an equivalence relation on  $M$  determines a partition of  $M$  into equivalence classes, i.e.,  $M$  is subdivided into nonintersecting nonempty subsets, which are equivalence classes.

**Definition 5.** Let  $\sim$  be an equivalence relation on  $M$ . The set of equivalence classes under this relation is called the *quotient set* of  $M$  by  $\sim$  and is written as  $M/\sim$ .

**Problem 6.** For each equivalence relation defined in Problem 3, describe its equivalence classes and quotient sets.

**Problem 7.** Consider the following equivalence relation on the set  $S_n$ :  $a \sim b$  if there is a permutation  $c$  such that  $b = cac^{-1}$ .

a) Show that this relation is indeed an equivalence relation. (We note in passing that permutations like  $a$  and  $b$  above are said to be *conjugate* and the corresponding operation is sometimes called *conjugation* of  $a$  by  $c$ .)

b\*) Find a simple method to determine whether two permutations are equivalent and check which of the permutations your teacher gave to you are equivalent.

### Integers 3. Modular Arithmetic

Leaflet 10 / February 2005

**Definition 1.** Two numbers  $a$  and  $b$  are *congruent modulo  $m$* , which is written  $a \equiv b \pmod{m}$ , if  $m \mid (a - b)$ .

**Problem 1.** Show that  $a$  is congruent to  $b$  modulo  $m$  if and only if the remainders of the division of  $a$  and  $b$  by  $m$  are the same.

**Problem 2.** Show that congruence modulo  $m$  is an equivalence relation.

**Problem 3.** Show that for all  $a_1, a_2, b_1, b_2, c, m$ , the following holds:

- a)  $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ ;
- b)  $a_1 \equiv b_1 \pmod{m} \Rightarrow ca_1 \equiv cb_1 \pmod{m}$ ;
- c)  $a_1 \equiv b_1 \pmod{m}, a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}$ .

**Problem 4.** Let  $a \equiv b \pmod{m}$ . Show that

- a)  $a^n \equiv b^n \pmod{m}$  for every nonnegative  $n$ ;
- b\*) for every polynomial  $f(x)$  with integer coefficients,

$$f(a) \equiv f(b) \pmod{m}.$$

**Problem 5.** Is it true that  $2^a \equiv 2^b \pmod{m}$  whenever  $a \equiv b \pmod{m}$  and  $a, b \geq 0$ ?

**Problem 6.** Let  $\overline{a_n a_{n-1} \dots a_1 a_0}$  be the decimal representation of a number  $x$ . Show that

- a)  $x \equiv a_0 + \dots + a_n \pmod{3}, x \equiv a_0 + \dots + a_n \pmod{9}$ ;
- b)  $x \equiv a_0 \pmod{2}, x \equiv a_0 \pmod{5}$ ;
- c)  $x \equiv a_0 - a_1 + \dots + (-1)^n a_n \pmod{11}$ .

**Problem 7.** Prove that if  $x$  is odd, then  $x^2 \equiv 1 \pmod{8}$ .

**Problem 8\*.** Show that the following equations have no nonzero integer solutions: a)  $x^2 + y^2 = 3z^2$ ; b)  $x^2 + y^2 + z^2 = 4t^2$ .

**Problem 9\*.** Show that there are infinitely many natural numbers not expressible as the sum of three perfect a) squares; b) cubes.

**Problem 10.** Solve the following congruences:

- a)  $3x \equiv 1 \pmod{7}$ ; b)  $6x \equiv 5 \pmod{9}$ ; c)  $4x \equiv 2 \pmod{10}$ .

**Problem 11.** Prove that the congruence  $ax \equiv b \pmod{m}$  has a solution if and only if  $\gcd(a, m) \mid b$ .

**Problem 12.** Let  $p$  be a prime, and  $a \not\equiv 0 \pmod{p}$ . Prove that the congruence  $ax \equiv b \pmod{p}$  has a solution for each  $b$ . Moreover, show that any two such solutions are congruent modulo  $p$ .



**Problem 13\* (Chinese Remainder Theorem).** Assume that the numbers  $a_1, a_2, \dots, a_n$  are pairwise coprime, i.e., every pair of them have no common divisors. Prove that for all  $b_1, b_2, \dots, b_n$  there is an  $x$  such that

$$x \equiv b_i \pmod{a_i}, \quad i = 1, \dots, n.$$

Moreover, prove that any two numbers  $x$  satisfying the above are congruent modulo the product  $a_1 \dots a_n$ .

**Problem 14\*.** Find all solutions to the following system of congruences:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 4 \pmod{9}. \end{cases}$$

**Problem 15.** Let  $p$  be a prime. Prove the following:

- a)  $p \mid \binom{p}{k}$  for  $0 < k < p$ ;
- b)  $(a+b)^p \equiv a^p + b^p \pmod{p}$ ;
- c) (Fermat's Little Theorem)  $p \mid (a^p - a)$ .

**Problem 16\* (Wilson's Theorem).** Let  $p$  be a prime. Show that

$$(p-1)! \equiv -1 \pmod{p}.$$

**Problem 17.** What are the regular polygons that can be used to tile a plane?

**Problem 18.** Show that there are infinitely many primes of the following forms: a)  $4n+3$ ; b\*)  $4n+1$ ; c\*\*)  $an+b$ , where  $\gcd(a, b) = 1$ .

**Problem 19\*.** Determine the number of solutions to the congruence  $x^2 \equiv 1 \pmod{n}$  a) for  $n$  prime; b) for an arbitrary  $n$ .

## Integers 4. Practical Problems

Leaflet 11 / March 2005

**Problem 1.** Is it true that for all  $n > 1$ ,

- a)  $6 \mid (n^3 + 5n)$ ; b)  $6 \mid (2n^3 + 3n^2 + 7n)$ ; c)  $30 \mid (n^5 - n)$ ; d)  $6 \mid (2^{2n} - 1)$ ;  
e)  $148 \mid (11^{6n+3} + 1)$ ?

**Problem 2.** Give the definition of

- a) the gcd (greatest common divisor) of  $n$  integers  $a_1, a_2, \dots, a_n$ ;  
b) the lcm (least common multiple) of  $a_1, a_2, \dots, a_n$  ( $n > 2$ ).

**Problem 3.** Show that for all nonzero  $a, b$ , and  $c$ , we have

a)  $\gcd(a, b, c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$ ;

b)  $\text{lcm}(a, b, c) = \frac{|abc| \cdot \gcd(a, b, c)}{\gcd(a, b) \cdot \gcd(b, c) \cdot \gcd(a, c)}$ .

**Problem 4.** Does there exist a number that, when divided by 2, 3, 4, 5, and 6, gives the following remainders, respectively?

- a) 1, 2, 3, 4, 5; b) 0, 1, 2, 3, 4; c) 0, 1, 2, 3, 2.

**Problem 5.** Compute the gcd of the following numbers:

- a) 923 and 1207; b) 279 and  $-589$ ; c)  $-693$  and 2475;  
d)  $-697$  and  $-1377$ ; e) 1517 and 1591; f) 1134, 2268, and 1575.

**Problem 6.** Compute the lcm of the following numbers:

- a) 16 and 84; b) 819 and 504; c) 30, 56 and 72;  
d) 340, 990 and 46; e) 41, 85 and 36; f) 2, 5, 7, 9 and 11.

**Problem 7.** For  $n > 0$ , simplify the expressions below.

- a)  $1 \cdot 2 + 2 \cdot 3 + \dots + (n-1) \cdot n$ ;  
b)  $\frac{1}{4 \cdot 5} + \frac{1}{5 \cdot 6} + \dots + \frac{1}{(n+3)(n+4)}$ ;  
c\*)  $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \dots + n \cdot (n+1) \cdot (n+2)$ .

**Problem 8.** Prove the following identities:

- a)  $(n+1) \cdot (n+2) \cdot \dots \cdot (n+n) = 2^n \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1)$ ;  
b)  $1 - \frac{1}{2} + \frac{1}{3} - \dots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \dots + \frac{1}{2n}$ ;  
c)  $\left(1 - \frac{1}{4}\right) \cdot \left(1 - \frac{1}{9}\right) \cdot \dots \cdot \left(1 - \frac{1}{(n+1)^2}\right) = \frac{n+2}{2n+2}$ .

**Problem 9.** Solve the following equations in integers:

- a)  $7x + 5y = 1$ ; b)  $27x - 24y = 1$ ; c)  $12x - 33y = 9$ ;  
d)  $-56x + 91y = 21$ ; e)  $344x - 215y = 86$ ; f)  $3x + 5y + 7z = 1$ .

**Problem 10.** Is it true that for every natural  $n$ , the numbers  $10n + 7$  and  $10n + 5$  are relatively prime?

**Problem 11.** In each of the cases below, find numbers  $a$  and  $b$  such that  $ax + by = 1$ .

- a)  $x = 7, y = 9$ ; b)  $x = 17, y = 19$ ; c)  $x = 27, y = 29$ ;  
d)  $x = 37, y = 39$ ; e)  $x = 47, y = 49$ .

**Problem 12.** Define the sequence  $u(n)$  by the following rule:  $u(0) = 0$ ,  $u(1) = 1$ ,  $u(n) = u(n-1) + u(n-2)$  (the *Fibonacci numbers*).

- a) Show that  $u(1) + \dots + u(n) = u(n+2) - 1$ .  
b) Show that  $(u(1))^2 + \dots + (u(n))^2 = u(n) \cdot u(n+1)$ .  
c) (*Binet's Formula*) What is the relationship between  $u(n)$  and

$$\delta(n) = \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n ?$$

# Group Theory

Leaflet 12 / March 2005

**Convention.** All numbers in this leaflet are assumed to be integers;  $p$  is assumed to be a prime number.

**Definition 1.** A *binary operation*  $\cdot$  on a set  $M$  is a map from the set of all ordered pairs  $M^2 = \{(a, b) \mid a \in M, b \in M\}$  to  $M$ , i.e., an assignment of a unique element in  $M$  to each pair of elements in  $M$ . The image of a pair  $(a, b)$  is written as  $a \cdot b$ .

**Definition 2.** A pair  $(G, \cdot)$  consisting of a set  $G$  and a binary operation  $\cdot$  on  $G$  is a *group* (under  $\cdot$ ) provided the following conditions hold:

- 1)  $\forall a, b, c \in G: a \cdot (b \cdot c) = (a \cdot b) \cdot c$  (associativity);
- 2)  $\exists e \in G \forall a \in G: e \cdot a = a \cdot e = a$  (the existence of an identity);
- 3)  $\forall a \in G \exists a^{-1} \in G: a^{-1} \cdot a = a \cdot a^{-1} = e$  (the existence of inverses).

If  $G$  contains a finite number of elements, then  $G$  is said to be a *finite group*. The number of elements in a finite group  $G$ , written  $|G|$ , is called the *order* of  $G$ .

**Convention.** The condition that a binary operation be associative amounts to saying that the order in which the operation is applied to multiple terms is immaterial. This makes it legitimate to omit the parentheses in expressions containing more than two terms, which we shall do in the future.

**Problem 1.** Are the following pairs groups?

- a)  $(\mathbb{Z}, +)$ ; b)  $(\mathbb{Z}, -)$ ; c)  $(\mathbb{N}, \cdot)$ ; d)  $(S_n, \cdot)$ ;
- e) the set of even integers under addition;
- f) the set of odd integers under addition;
- g) the set of maps  $f: X \rightarrow X$  under composition;
- h) the set  $P(A)$  of subsets of a set  $A$  under the operation  $\cup$ ;
- i)  $(P(A), \cap)$ ; j)  $(P(A), \setminus)$ ;
- k)  $(P(A), \triangle)$ , where  $A \triangle B = (A \cup B) \setminus (A \cap B)$ ;
- l)  $(\mathbb{Z}/n\mathbb{Z}, +_n)$ , where  $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n-1\}$  and  $a +_n b$  is the remainder in the division of  $a + b$  by  $n$ ;
- m)  $(\mathbb{Z}/n\mathbb{Z}, \cdot_n)$ , where  $a \cdot_n b$  is the remainder in the division of  $ab$  by  $n$ ;
- n)  $(\mathbb{N}, \cdot)$ , where  $a \cdot b = a^b$ ;
- o)  $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \cdot_n)$ ;
- p)  $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot_n)$ , where  $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$ .

**Definition 3.** A group  $G$  is said to be *commutative* (or *Abelian*) provided for every  $a, b \in G$ , one has  $ab = ba$ .

**Problem 2.** Which of the groups from Problem 1 are commutative?

**Problem 3.** Prove the following:

- a) the identity in any group is unique;
- b) the inverse of every element in a group is unique;
- c)  $ba = e \Rightarrow b = a^{-1}$ ; d)  $ba = a \Rightarrow b = e$ ; e)  $(a^{-1})^{-1} = a$ .

**Problem 4\*.** Prove that if one replaces conditions 2 and 3 in Definition 2 by the following conditions:

- 2°)  $\exists e \in G \forall a \in G: ea = a$  (left identity);
- 3°)  $\forall a \exists a^{-1}: a^{-1}a = e$  (left inverse),

then this new definition is equivalent to Definition 2.

**Definition 4.** A map  $f: G \rightarrow H$  from a group  $G$  to a group  $H$  is said to be an *isomorphism* provided it is bijective and preserves the group operation, i.e.,  $\forall x, y \in G f(x * y) = f(x) * f(y)$ . If such a map exists, then the groups  $G$  and  $H$  are said to be *isomorphic*.

**Problem 5.** List all pairwise nonisomorphic groups of the following orders: a) 1, 2, 3; b) 4; c\*) 13.

**Definition 5.** A nonempty subset  $H$  of a group  $G$  closed under the two operations of  $\cdot$  and of taking inverses is called a *subgroup*.

**Problem 6.** Is it true that

- a) if  $H$  is a subgroup of  $G$ , then  $e \in H$ ;
- b) if  $H$  is a subgroup of  $G$ , then  $H$  is a group;
- c) if  $K$  is a subgroup of  $H$  and  $H$  is a subgroup of  $G$ , then  $K$  is a subgroup of  $G$ ;
- d) the union of two subgroups is a subgroup;
- e) the intersection of two subgroups is a subgroup?

**Problem 7.** Is it true that

- a)  $\mathbb{N}$  is a subgroup of  $\mathbb{Z}$ ;
- b)  $A_n$  is a subgroup of  $S_n$ , where  $A_n$  is the set of all even permutations of an  $n$ -element set;
- c)  $S_n \setminus A_n$  is a subgroup of  $S_n$ ?

**Problem 8.** List all subgroups of a)  $S_3$ ; b)  $\mathbb{Z}$ .

**Definition 6.** If  $a \in G$ , then the smallest positive integer  $k$  such that  $a^k = e$  is said to be the *order* of  $a$ , written  $\text{ord } a$ . If no such integer exists, then one says that  $\text{ord } a = \infty$ .

**Problem 9.** Prove that in a finite group,  $\text{ord } a < \infty$  for all  $a$ .

**Problem 10.** Prove that  $a^n = e$  if and only if  $\text{ord } a \mid n$ .

**Definition 7.** Let  $H$  be a subgroup of a group  $G$ . A *left* (respectively *right*) *coset* of  $H$  in  $G$  with respect to  $a \in G$  is the set  $aH = \{ax \mid x \in H\}$  (respectively  $Ha = \{xa \mid x \in H\}$ ).

**Problem 11.** Prove that two left cosets are either disjoint or coincide. Repeat this for right cosets.

**Problem 12.** For each group  $G$  and its subgroup  $H$  below, find the left and right  $H$ -coset decomposition of  $G$ .

a)  $G = \mathbb{Z}$ ,  $H = 2\mathbb{Z}$ ; b)  $G = S_4$ ,  $H = A_4$ ; c)  $H = S_3$ ,  $H = \langle (12) \rangle$ .

**Problem 13 (Lagrange's Theorem).** Prove that if  $G$  is a finite group, then the order of any subgroup of  $G$  divides the order of  $G$  (i.e.,  $|G|$  is divisible by  $|H|$ ).

**Problem 14.** Prove that the order of any element in a finite group  $G$  divides the order of  $G$  (i.e.,  $|G|$  is divisible by  $\text{ord } a$ ).

**Definition 8.** Write  $\varphi(n)$  for the number of positive integers up to the integer  $n$  that are relatively prime to  $n$ . The function  $\varphi(n)$  is called *Euler's  $\varphi$ -function*.

**Problem 15.** Calculate the following:

a)  $\varphi(2)$ ,  $\varphi(6)$ ,  $\varphi(30)$ ; b)  $\varphi(p)$ ; c)  $\varphi(p^n)$ .

**Problem 16.** Show that for all relatively prime integers  $m$  and  $n$ , one has  $\varphi(mn) = \varphi(m)\varphi(n)$ .

**Problem 17.** Calculate  $\varphi(p_1^{k_1} \cdots p_n^{k_n})$ .

**Problem 18 (Euler's theorem).** Prove that for any number  $a$  relatively prime to  $n$ , one has  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**Problem 19\*.** Describe the symmetry group of: a) the regular triangle; b) the square; c) the regular  $n$ -gon (the *dihedral group*  $D_n$ ).

## Graph Theory 2

Leaflet 3A / March 2005

**Problem 1.** There were  $n$  teams in a single elimination tournament. Find the number of matches they played.

**Problem 2.** Prove that a graph on  $n$  vertices, each of which is of valency at least  $(n-1)/2$ , is connected.

**Problem 3.** In a connected graph, all vertices have valency 100. Show that removing any vertex results in a connected graph.

**Problem 4.** Prove that every connected graph has a subgraph which is a tree that contains all the vertices of the given graph (a *spanning tree*).

**Problem 5.** Prove that given a connected graph, one can remove some vertex and all edges meeting it so that the resulting graph remains connected.

**Problem 6\*.** There were  $n^3$  unit cubes in a cube-shaped box of size  $n \times n \times n$ . The box was emptied; the cubes were drilled diagonally, strung together, and tied in a ring. For what values of  $n$  does the resulting 'necklace' fit into the original box?

**Problem 7\*.** Petya's 28 classmates all have a different number of friends in Petya's class. How many of them are Petya's friends? What if 28 is replaced by  $n$ ?

**Problem 8\* (Cayley's Formula).** In a graph on  $n$  vertices, every pair of distinct vertices is connected by (a unique) edge (such a graph is said to be *complete*). Show that there are precisely  $n^{n-2}$  ways to remove several edges in such a way that the resulting graph is a tree.

**Definition 1.** A *directed* (or *oriented*) *graph* is a graph whose edges have a direction associated with them. Its edges are called *arrows* (or *directed edges*, or *directed arcs*, or *directed lines*). More formally, a directed graph is a pair  $\Gamma = (V, E)$  consisting of a finite set of vertices  $V$  and a set of arrows  $E$ , the elements of the latter being ordered pairs of vertices of  $\Gamma$ .

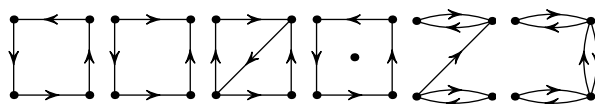
Note that directed graphs can admit *loops* (arrows that connect vertices to themselves), *multiple arrows* (several arrows from one vertex to another), and 'opposite' arrows (arrows from  $A$  to  $B$  and from  $B$  to  $A$ ).

From now on, we shall refer to what was called a graph above as a *nonoriented graph*.

**Problem 9.** Give (formal!) definitions of a *path* and a *cycle* in an oriented graph.

**Definition 2.** An oriented graph is said to be *strongly connected* provided it contains a directed path from  $u$  to  $v$  and one from  $v$  to  $u$  for all pairs of vertices  $u, v$ .

**Problem 10.** Which of the graphs below are strongly connected?



**Definition 3.** A directed graph is said to be *connected* if on removing the directions from its (directed) edges, it becomes a connected nonoriented graph.

**Problem 11.** a) Give an example of a connected oriented graph which is not strongly connected.

b) Give an example of a connected oriented graph having two vertices  $A$  and  $B$  with the property that there is no path from  $A$  (or  $B$ ) to  $B$  (resp. to  $A$ ).

**Problem 12.** Prove that one can assign directions to the edges of a connected nonoriented graph in such a way that one of its vertices has paths to the others.

**Problem 13.** Is there a way to assign directions to the edges of a complete nonoriented graph so that the resulting oriented graph has no cycles?

**Problem 14.** Suppose that the edges of a complete nonoriented graph have been assigned directions. Prove that there are paths from some vertex to all the others.

**Problem 15\* (Problem 18\* from the leaflet 'Graph Theory 1').**

Suppose that the edges of a complete nonoriented graph have been assigned arrows. Prove that the resulting oriented graph has a *Hamiltonian path* (i.e., a path that visits each vertex exactly once).

**Problem 16\*.** Suppose that the edges of a complete nonoriented graph with at least three vertices have been assigned arrows. Prove that one can replace no more than one arrow by the opposite one in such a way that the new graph is strongly connected.

**Definition 4.** The number of arrows entering (resp. leaving from) a vertex of an oriented graph is called the *input semi-degree* (resp. *output semi-degree*) of that vertex.



**Problem 17.** For each of the graphs from Problem 10, determine their input and output semi-degrees.

**Problem 18.** What can be said about the sum of all input semi-degrees and the sum of all output semi-degrees of a graph?

**Problem 19.** State and prove a criterion for an oriented graph to be Eulerian.

**Problem 20 (de Bruijn Cycle).** In order to unlock a combination lock (with buttons 0 through 9), one must enter a 4-digit code; the digits entered before the correct code are immaterial. What is the minimum number of times one must press the button to unlock it for sure?

**Problem 21.** Twenty students were solving 20 problems. Each one solved precisely two problems, and each problem was solved precisely by two students. Prove that one can arrange a problem solving session in such a way that each student presents the solution of one of the problems that this he/she has solved.

**Definition 5.** A graph is said to be *bipartite* provided its vertices can be divided into two disjoint nonempty sets (called *parts*)  $U$  and  $V$  such that every edge connects a vertex in  $U$  to one in  $V$ .

A *matching* is a set of edges of a graph such that each vertex in the graph is the tail (i.e., endpoint) of at most one edge from the set. A matching is *perfect* if each vertex is the tail of precisely one edge in the matching.

A coloring of the vertices of a graph is *proper* if no two vertices of the same color are connected by an edge. A graph is said to be *k-partite* if it can be properly colored in  $k$  colors and cannot be properly colored in  $l$  colors, where  $l < k$ .

**Problem 22.** Which of the graphs from Problems 1, 2, and 3 in the leaflet 'Graph Theory 1' are bipartite? For each of the remaining graphs, find  $k$  such that they are  $k$ -partite.

**Problem 23.** Is it true that a nonoriented graph is bipartite if and only if it has no cycles of odd length?

**Problem 24.** Is every tree a bipartite graph?

**Problem 25\* (Hall's Marriage Theorem).** Suppose there is a group of  $n$  young men. Fix  $k \in \{1, 2, \dots, n\}$ . Assume further that for any  $k$  of them, there exist at least  $k$  young women who know at least one of the  $k$  men under consideration. Is it possible to pair up (in marriage) the men and women so that each man knows the woman who is to become his wife? Is this condition necessary?

In other words, is it true that in a bipartite nonoriented graph with  $n$  vertices in its first part, there is a matching of size  $n$  if and only if at least  $k$  vertices from its second part are connected with those in every set of  $k$  vertices from the first part?

**Problem 26\* (A Generalization of Problem 21).** Prove that every regular bipartite nonoriented graph has a perfect matching.

**Problem 27\*.** Is it true that for every proper coloring of a  $k$ -partite non-oriented graph with  $k$  colors, there is a path consisting of  $k$  vertices of different colors?

**Definition 6.** A graph is said to be *planar* if it can be drawn in the plane in such a way that its vertices are points and its edges (or arrows) are nonintersecting curves. Such a drawing is referred to as a *plane graph*. The parts into which a plane graph divides the plane (the external part included) are called its *faces*.

**Problem 28.** Which of the graphs from Problems 1, 2, and 3 from the leaflet 'Graph Theory 1' are planar?

**Problem 29 (Euler's Formula).** Suppose a nonoriented plane connected graph contains  $V$  vertices,  $E$  edges, and  $F$  faces. Then  $V + E - F = 2$ .

**Problem 30.** Compute  $V + F - E$  for a disconnected nonoriented plane graph.

**Problem 31.** Let  $V$ ,  $E$ , and  $F$  be the number of vertices, edges, and faces of a polyhedron, respectively. Compute  $V + F - E$ .

**Problem 32.** a) Prove that for a plane nonoriented graph,  $2E \geq 3F$ .

b) Prove that for a plane bipartite nonoriented graph,  $E \geq 2F$ .

**Problem 33\*.** Prove that the following graphs are not planar:

a) the complete nonoriented graph on 5 vertices. This graph is denoted by  $K_5$ ;

b) the bipartite nonoriented graph with 3 vertices in its first part and 3 vertices in its second part, where every vertex of the first set is connected to every vertex of the second set (such a graph is called a *complete bipartite graph*). This graph is denoted by  $K_{3,3}$ ;

c) An arbitrary nonoriented graph, each vertex of which has degree at least 6.

**Definition 7.** A *subgraph* of a graph is a graph obtained from the initial one by removing some vertices and edges (or arrows).

Two nonoriented graphs are said to be *homeomorphic* if one of them can be obtained from the other via the following operations: 1) inserting

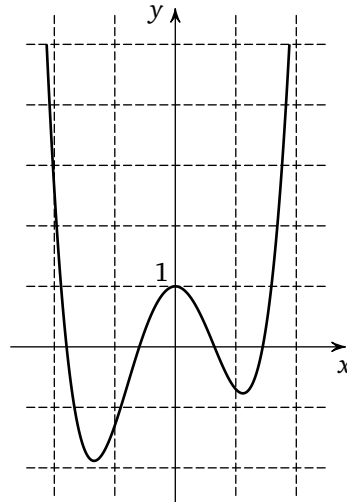
a vertex in the middle of an edge; 2) replacing a vertex of valency 2 and both edges issuing from it by a single edge (note that the two operations are mutually inverse).

**Problem 34\* (Kuratowski's Theorem).** Prove that a nonoriented graph is planar if and only if it has no subgraph homeomorphic to either  $K_5$  or  $K_{3,3}$ .

## Graphical representation of functions

Leaflet 13 / april 2005

**Problem 1.** Given the graphical representation of the function  $f$ , find  $f(0)$  and  $f(1)$ , solve the equations  $f(x) = 0$ ,  $f(x) = 1$  and  $f(x) = x$  graphically; find all  $c$  for which the equation  $f(x) = c$  has one, two, or three solutions.



**Definition 1.** The *integer part* of a number  $x$  is the greatest integer less than or equal to  $x$ . It is denoted by  $[x]$ .

**Definition 2.** The *fractional part* of a number  $x$  is the number  $\{x\}$  given by  $\{x\} = x - [x]$ .

**Definition 3.**  $\text{sign } x = \begin{cases} 1, & \text{if } x > 0; \\ 0, & \text{if } x = 0; \\ -1, & \text{if } x < 0. \end{cases}$

**Problem 2.** a) Find  $[3.5]$ ,  $[-2.2]$ ,  $\{1.1\}$ ,  $\{-2.7\}$ ,  $[0]$ ,  $\{0\}$ ,  $[5]$ ,  $\{5\}$ ,  $\text{sign}(5.6)$ ,  $\text{sign}(-2.4)$ ,  $\text{sign}(0)$ .

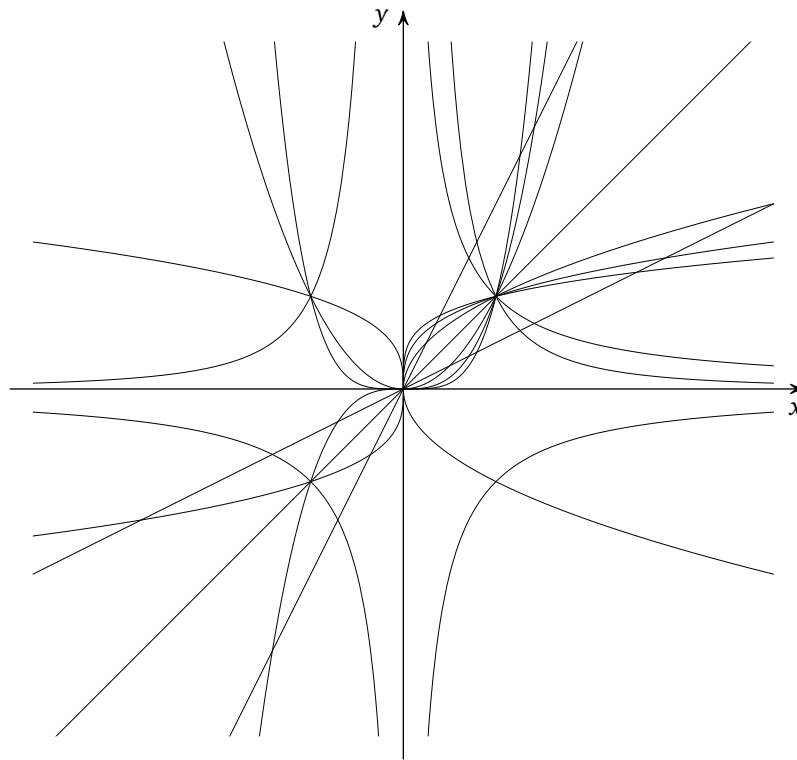
b) Is it true that  $\text{sign } xy = \text{sign } x \cdot \text{sign } y$ ,  $[xy] = [x][y]$ ,  $\{xy\} = \{x\}\{y\}$ ?

c) Is it true that  $\text{sign}(x + y) = \text{sign } x + \text{sign } y$ ,  $[x + y] = [x] + [y]$ ,  $\{x + y\} = \{x\} + \{y\}$ ?

d) Prove that  $x = |x| \cdot \text{sign } x$ ,  $x = [x] + \{x\}$ .

**Problem 3.** Plot the functions  $2x + 3$ ,  $x^2$ ,  $1/x$ ,  $[x]$ ,  $\{x\}$ ,  $\text{sign } x$ ,  $|x|/x$ ,  $|x|$ .

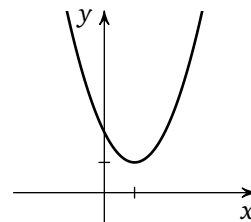
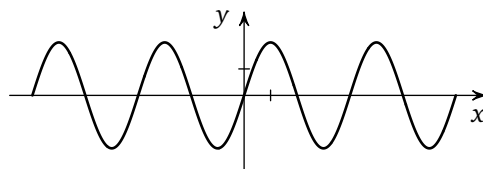
**Problem 4.** Plot the functions  $x/2$ ,  $x$ ,  $2x$ ,  $x^2$ ,  $x^3$ ,  $x^4$ ,  $x^6$ ,  $\sqrt{x}$ ,  $\sqrt[3]{x}$ ,  $\sqrt[4]{x}$ ,  $1/x$ ,  $1/x^2$  on the same figure using different colors.



**Problem 5.** For the functions  $f$  and  $g$ , proposed by your teacher, plot  $f(x) + g(x)$ ,  $f(x) \cdot g(x)$ ,  $f(x) - g(x)$ ,  $\sqrt{f(x)}$ ,  $1/f(x)$ .

**Problem 6.** Plot the functions

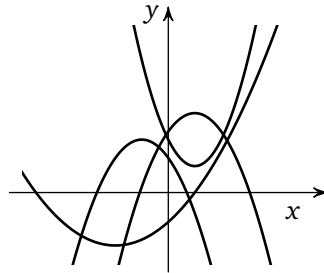
$f(|x|)$ ,  $|f(x)|$ ,  $f(x+1)$ ,  $f(x-1)$ ,  $f(x)+1$ ,  $f(x)-1$ ,  $f(2x)$ ,  
 $3f(x)$ ,  $f(x/3)$ ,  $-f(x)$ ,  $f(-x)$ ,  $f([x])$ ,  $f(\{x\})$ ,  $[f(x)]$ ,  
 if the graph of  $f$  is as shown below.



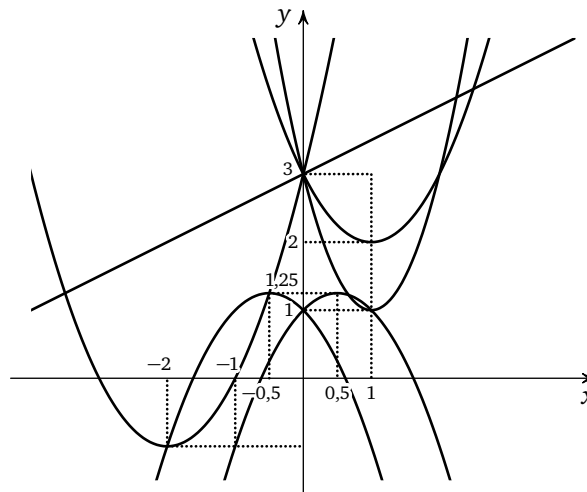
**Problem 7.** Represent the following functions:

a)  $x^2 + 2x + 3$ ; b)  $-2x^2 + 3x - 1$ ; c)  $x^2 - 2|x| + 1$ .

**Problem 8.** For the graphs of the functions of the form  $y = ax^2 + bx + c$  shown below, find sign  $a$ , sign  $b$ , and sign  $c$  for each of them.



**Problem 9.** The figure below shows the graphs of the functions  $x^2 - 2x + 3$ ,  $2x^2 - 4x + 3$ ,  $x^2 + 4x + 3$ ,  $-x^2 + x + 1$ ,  $x/2 + 3$ . Identify which graph corresponds to which function.



**Problem 10.** Draw the set of all points  $(p, q)$  for which the equation  $x^2 + px + q = 0$ : a) does not have any roots; b) has a unique root; c) has two roots.

**Problem 11\*.** Given the graph of the motion of a bus proposed by your teacher, plot its velocity.

## Group Theory 2. Homomorphisms

Leaflet 4A / may 2005

### I. HOMOMORPHISMS

**Definition 1.** A mapping  $f: G \rightarrow H$  from a group  $(G, *)$  to a group  $(H, \circ)$  is called a *homomorphism*, if for all  $a, b \in G$  we have  $f(a * b) = f(a) \circ f(b)$ . The set of all homomorphisms from  $G$  to  $H$  is denoted by  $\text{Hom}(G, H)$ .

A bijective homomorphism is called an *isomorphism*. An isomorphism of a group onto itself is called an *automorphism*. The set of all automorphisms of a group  $G$  is denoted by  $\text{Aut}(G)$ .

Groups  $G$  and  $H$  are called *isomorphic*, if there is an isomorphism between them; we write  $G \cong H$ . Informally, groups are isomorphic if one is obtained from another by ‘renaming elements’.

**Problem 1.** Prove that the relation ‘ $G \cong H$ ’ is an equivalence relation (strictly speaking, this holds for any set of groups, because the ‘set of all groups’ does not exist).

**Problem 2.** Which of the following maps are homomorphisms? Which of them are isomorphisms?

- a) The identity mapping  $g \mapsto g$  of any group;
- b) A constant mapping from a group onto the trivial group;
- c)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(n) = 2n$ ; d)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(n) = n + 1$ ;
- e)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ,  $f(n) = n^2$ ; f)  $f: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ ,  $f(n) = -n$ ;
- g)  $f: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ ,  $f(n) = n^{-1}$ ;
- h)  $f: (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ ,  $f(n) = n^{10}$ ;
- i)  $f: S_n \rightarrow S_n$ ,  $f(x) = ax$ ; j)  $f: S_n \rightarrow S_n$ ,  $f(x) = x^{-1}$ ;
- k)  $f: S_n \rightarrow S_n$ ,  $f(x) = axa^{-1}$ ; l)  $\text{sign}: S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ .

**Problem 3.** Prove that for every homomorphism  $f: G \rightarrow H$ , we have

- a)  $f(e_G) = e_H$ ; b)  $f(x^{-1}) = f(x)^{-1}$ ; c)  $f(x^n) = f(x)^n$ .

**Problem 4.** Let  $G$  be any group, and  $H$  be an Abelian group. Define a group structure: a) on  $\text{Hom}(G, H)$ , b) on  $\text{Aut}(G)$ .

**Problem 5.** Find all homomorphisms:

- a)  $f: \mathbb{Z} \rightarrow \mathbb{Z}$ ; b)  $f: \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$ ; c)  $f: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ .

**Problem 6.** a) Find all subgroups of  $\mathbb{Z}/4\mathbb{Z}$  and  $\mathbb{Z}/7\mathbb{Z}$ .

b) Prove that every subgroup of  $\mathbb{Z}/n\mathbb{Z}$  is isomorphic to a group of the form  $\mathbb{Z}/m\mathbb{Z}$ .

**Problem 7\*.** How many homomorphisms from a)  $\mathbb{Z}$ ; b)  $\mathbb{Z}/p\mathbb{Z}$  to  $G$  are there?

**Problem 8.** Which of the following groups are isomorphic to each other:  $\mathbb{Z}/2\mathbb{Z}$ ,  $(\mathbb{Z}/3\mathbb{Z})^\times$ ,  $S_2$ ,  $\mathbb{Z}/6\mathbb{Z}$ ,  $S_3$ ,  $(\mathbb{Z}/7\mathbb{Z})^\times$ ? (For the definition of  $(\mathbb{Z}/2\mathbb{Z})^\times$ , see Problem 1p in Leaflet 12.)

**Definition 2.** The set  $f(G)$  is called the *image* of the given homomorphism  $f: G \rightarrow H$ . It is denoted by  $\text{Im } f$ .

The set  $f^{-1}(e_H)$  is called the *kernel* of a homomorphism  $f: G \rightarrow H$ . It is denoted by  $\text{Ker } f$ .

**Problem 9.** Find the kernels and the images of the homomorphisms from Problem 2.

**Problem 10.** Let  $f: G \rightarrow H$  be a homomorphism. Prove that  $\text{Im } f$  and  $\text{Ker } f$  are subgroups of  $H$  and  $G$ , respectively.

**Problem 11.** Prove that a homomorphism  $f: G \rightarrow H$  is an isomorphism if and only if  $\text{Im } f = H$  and  $\text{Ker } f = \{e_G\}$ .

**Problem 12.** Find a homomorphism from the group  $\mathbb{Z}$  whose kernel is the subgroup of even integers.

## 2. COSETS

**Problem 13.** Does there exist a homomorphism from  $S_3$  with kernel  $\{e, (12)\}$ ?

**Problem 14.** Prove that for every  $a \in G$  and every homomorphism  $f: G \rightarrow H$  the equality  $a(\text{Ker } f) = (\text{Ker } f)a$  holds.

**Problem 15.** a) Prove that the well-known rule

$$\begin{aligned}\text{even} + \text{even} &= \text{odd} + \text{odd} = \text{even}, \\ \text{even} + \text{odd} &= \text{odd} + \text{even} = \text{odd}\end{aligned}$$

defines a group structure on the set  $\{\{2n \mid n \in \mathbb{Z}\}, \{2n+1 \mid n \in \mathbb{Z}\}\}$ .

b) Prove that a similar rule defines a group structure on the set  $\{A_n, S_n \setminus A_n\}$ .

**Definition 3.** Recall that the *left coset* of an element  $g$  of a group  $G$  modulo subgroup  $H$  is the set of the form  $gH = \{gh \mid h \in H\}$ . The set of all left cosets is denoted by  $G/H$ .

The set of all right cosets of  $G$  modulo  $H$  (sets of the form  $Hg$ ) is denoted by  $H \backslash G$ . (The quotient should not be confused with the difference of sets.)

**Definition 4.** A subgroup  $H$  of a group  $G$  is called *normal* if for every element  $a \in G$  one has  $aH = Ha$  (or, equivalently,  $aHa^{-1} = H$ ). We then write  $H \triangleleft G$ .



**Problem 16.** Prove that all subgroups of a commutative group are normal.

**Problem 17.** Which of the subgroups from Problem 12 in the leaflet ‘Group theory’ are normal?

**Problem 18.** Prove that a subgroup  $H$  of a group  $G$  is normal if and only if the partition of  $G$  into left cosets modulo  $H$  coincides with the partition into right cosets.

**Problem 19.** List all normal subgroups of  $S_3$ .

**Problem 20.** Prove that every subgroup  $H$  of a finite group  $G$  with  $2|H| = |G|$  is normal.

**Problem 21.** We define the product of the cosets  $aH$  and  $bH$  to be the coset  $(ab)H$ .

a) Prove that the product of cosets is well defined if and only if  $H$  is a normal subgroup.

b) Prove that in this case the set of all cosets of  $H$  in  $G$  form a group.

**Definition 5.** Let  $H$  be a normal subgroup of  $G$ . The group constructed in the previous problem is called the *quotient group* ( $G$  modulo  $H$ ). It is denoted by  $G/H$ .

**Problem 22.** Prove that for every homomorphism  $f: G \rightarrow H$ , we have  $\text{Im } f \cong G / \text{Ker } f$  (in particular,  $\text{Ker } f$  is a normal subgroup of  $G$ ).

### 3. ACTIONS

**Definition 6.** A homomorphism  $f$  from a group  $G$  to the transformation group of a set  $A$  (i.e., bijections of  $A$  onto itself) is called an *action* of  $G$  on this set. (So  $f$  assigns to each element  $g$  of  $G$  some bijection of  $A$  onto itself.) If the action is clear from the context, we write  $ga$  instead of  $f(g)(a)$ .

**Problem 23.** Which of the following maps are actions of a group on itself?

- a)  $f(g)(x) = gx$  (left translation);
- b)  $f(g)(x) = g^{-1}x$ ;
- c)  $f(g)(x) = xg$  (right translation);
- d)  $f(g)(x) = xg^{-1}$ ;
- e)  $f(g)(x) = gxg^{-1}$  (action by conjugation).

**Problem 24 (Cayley’s theorem).** Prove that every finite group is isomorphic to a subgroup of  $S_n$  for some  $n$ .

**Problem 25.** List all actions:

- a) of the group  $\mathbb{Z}$  on a two-element set (one-element set);
- b) of the group  $\mathbb{Z}/n\mathbb{Z}$  on a two-element set (one-element set);
- c) of the group  $\mathbb{Z}/n\mathbb{Z}$  on a three-element set;
- d) of the group  $\mathbb{Z}/2\mathbb{Z}$  on  $\mathbb{Z}$  (on the group  $\mathbb{Z}/4\mathbb{Z}$ ) such that any transformation  $f(g)$  is an isomorphism;
- e) of the group  $\mathbb{Z}/n\mathbb{Z}$  on the set of vertices of a square such that any transformation  $f(g)$  is a rotation.

**Definition 7.** The set  $Ga = \{ga \mid g \in G\}$  is called the *orbit* of the point  $a \in A$ .

**Definition 8.** The orbits of action of  $G$  on itself by conjugation are called *conjugacy classes*.

**Problem 26.** Prove that the relation ‘the point  $a$  lies in the orbit of  $b$ ’ is an equivalence relation.

**Problem 27.** a) Describe the orbits of actions from Problem 25.

- b) Describe the orbits of the action by left translation.
- c) Find all conjugacy classes in  $S_3$  and  $A_3$ .
- d) Find all conjugacy classes in  $S_n$ .
- e\*) Find all conjugacy classes in  $A_n$ .

**Definition 9.** The set  $\text{Stab } a = \{g \in G \mid ga = a\}$  (also denoted  $G_a$ ) is called the *stabilizer* of the point  $a \in A$ .

**Problem 28.** Find the stabilizers of actions from the previous problems.

**Problem 29.** Prove that  $|G_x| \cdot |Gx| = |G|$  when  $G$  is finite.

**Problem 30.** Prove that any group of  $p^2$  elements ( $p$  being prime) has at least two one-element conjugacy classes.

**Definition 10.** The set  $\text{Fix } g = \{a \in A \mid ga = a\}$  (also denoted by  $A^g$ ) is called the *fixed point set* of the element  $g$ . (In general, it depends on the action, but we do not specify the action, if it is clear from the context.)

**Problem 31.** Find fixed point sets for the action of the group  $\mathbb{Z}/4\mathbb{Z}$ : a) by left translation; b) by conjugation.

**Problem 32.** Find fixed point sets of all elements under the action of the group  $S_3$ : a) by left translation; b) by conjugation.

**Problem 33 (Burnside lemma).** A group  $G$  acts on a set  $X$ . Prove that the number of orbits of the action is given by

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix } g|.$$

**Problem 34.** a) Find the number of ways one can color an  $n$ -person merry-go-round in red and blue.

b) Find the number of ways one can color an  $n$ -bead necklace in red and blue.