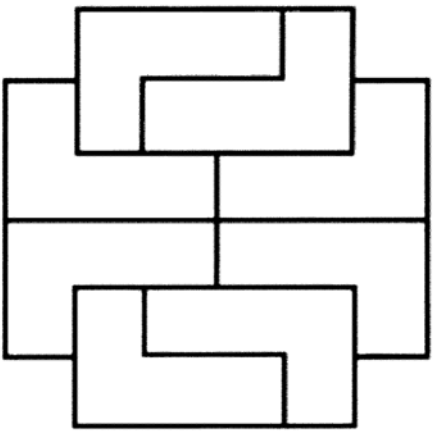
PROBLEM BOOKS IN MATHEMATICS

Arthur Engel

Problem-Solving Strategies



Springer

Problem Books in Mathematics

Edited by K. Bencsáth
P.R. Halmos

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Problem Books in Mathematics

Series Editors: K. Bencsáth and P.R. Halmos

Polynomials
by *Edward J. Barbeau*

Problems in Geometry
by *Marcel Berger, Pierre Pansu, Jean-Pic Berry, and Xavier Saint-Raymond*

Problem Book for First Year Calculus
by *George W. Bluman*

Exercises in Probability
by *T. Cacoullos*

An Introduction to Hilbert Space and Quantum Logic
by *David W. Cohen*

Unsolved Problems in Geometry
by *Hallard T. Croft, Kenneth J. Falconer, and Richard K. Guy*

Problem-Solving Strategies
by *Arthur Engel*

Problems in Analysis
by *Bernard R. Gelbaum*

Problems in Real and Complex Analysis
by *Bernard R. Gelbaum*

Theorems and Counterexamples in Mathematics
by *Bernard R. Gelbaum and John M.H. Olmsted*

Exercises in Integration
by *Claude George*

Algebraic Logic
by *S.G. Gindikin*

Unsolved Problems in Number Theory (2nd ed.)
by *Richard K. Guy*

(continued after index)

Arthur Engel

Problem-Solving Strategies

With 223 Figures

Springer

Angel Engel
Institut für Didaktik der Mathematik
Johann Wolfgang Goethe–Universität Frankfurt am Main
Senckenberganlage 9–11
60054 Frankfurt am Main 11
Germany

Series Editor:
Paul R. Halmos
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

Mathematics Subject Classification (1991): 00A07

Library of Congress Cataloging-in-Publication Data

Engel, Arthur.
Problem-solving strategies/Arthur Engel.
p. cm. — (Problem books in mathematics)
Includes index.
ISBN 0-387-98219-1 (softcover: alk. paper)
1. Problem solving. I. Title. II. Series.
QA63.E54 1997
510'.76—dc21 97-10090

ISBN 0–387–98219–1 Springer-Verlag New York Berlin Heidelburg SPIN 10557554

Preface

This book is an outgrowth of the training of the German IMO team from a time when we had only a short training time of 14 days, including 6 half-day tests. This has forced upon us a training of enormous compactness. "Great Ideas" were the leading principles. A huge number of problems were selected to illustrate these principles. Not only topics but also ideas were efficient means of classification.

For whom is this book written?

- For trainers and participants of contests of all kinds up to the highest level of international competitions, including the IMO and the Putnam Competition.
- For the regular high school teacher, who is conducting a mathematics club and is looking for ideas and problems for his/her club. Here, he/she will find problems of any level from very simple ones to the most difficult problems ever proposed at any competition.
- For high school teachers who want to pose *the problem of the week, problem of the month,* and *research problems of the year.* This is not so easy. Many fail, but some persevere, and after a while they succeed and generate a creative atmosphere with continuous discussions of mathematical problems.
- For the regular high school teacher, who is just looking for ideas to enrich his/her teaching by some interesting nonroutine problems.
- For all those who are interested in solving tough and interesting problems.

The book is organized into chapters. Each chapter starts with typical examples illustrating the main ideas followed by many problems and their solutions. The

solutions are sometimes just hints, giving away the main idea leading to the solution. In this way, it was possible to increase the number of examples and problems to over 1300. The reader can increase the effectiveness of the book even more by trying to solve the examples.

The problems are almost exclusively competition problems from all over the world. Most of them are from the former USSR, some from Hungary, and some from Western countries, especially from the German National Competition. The competition problems are usually variations of problems from journals with problem sections. So it is not always easy to give credit to the originators of the problem. If you see a beautiful problem, you first wonder at the creativity of the problem proposer. Later you discover the result in an earlier source. For this reason, the references to competitions are somewhat sporadic. Usually no source is given if I have known the problem for more than 25 years. Anyway, most of the problems are results that are known to experts in the respective fields.

There is a huge literature of mathematical problems. But, as a trainer, I know that there can never be enough problems. You are always in desperate need of new problems or old problems with new solutions. Any new problem book has some new problems, and a big book, as this one, usually has quite a few problems that are new to the reader.

The problems are arranged in no particular order, and especially not in increasing order of difficulty. We do not know how to rate a problem's difficulty. Even the IMO jury, now consisting of 75 highly skilled problem solvers, commits grave errors in rating the difficulty of the problems it selects. The over 400 IMO contestants are also an unreliable guide. Too much depends on the previous training by an ever-changing set of hundreds of trainers. A problem changes from impossible to trivial if a related problem was solved in training.

I would like to thank Dr. Manfred Grathwohl for his help in implementing various LaTeX versions on the workstation at the institute and on my PC at home. When difficulties arose, he was a competent and friendly advisor.

There will be some errors in the proofs, for which I take full responsibility, since none of my colleagues has read the manuscript before. Readers will miss important strategies. So do I, but I have set myself a limit to the size of the book. Especially, advanced methods are missing. Still, it is probably the most complete training book on the market. The gravest gap is the absence of new topics like probability and algorithmics to counter the conservative mood of the IMO jury. One exception is Chapter 13 on games, a topic almost nonexistent in the IMO, but very popular in Russia.

Frankfurt am Main, Germany Arthur Engel

Contents

Abbreviations and Notations

Abbreviations

ARO	Allrussian Mathematical Olympiad
ATMO	Austrian Mathematical Olympiad
AuMO	Australian Mathematical Olympiad
AUO	Allunion Mathematical Olympiad
BrMO	British Mathematical Olympiad
BWM	German National Olympiad
BMO	Balkan Mathematical Olympiad
ChNO	Chinese National Olympiad
HMO	Hungarian Mathematical Olympiad (Kűrschak Competition)
IIM	International Intellectual Marathon (Mathematics/Physics Competition)
IMO	International Mathematical Olympiad
LMO	Leningrad Mathematical Olympiad
MMO	Moskov Mathematical Olympiad
PAMO	Polish-Austrian Mathematical Olympiad

PMO	Polish Mathematical Olympiad
RO	Russian Olympiad (ARO from 1994 on)
SPMO	St. Petersburg Mathematical Olympiad
TT	Tournament of the Towns
USO	US Olympiad

Notations for Numerical Sets

$\mathbb{N}$ or $\mathbb{Z}^+$	the positive integers (natural numbers), i.e., $\{1,2,3,\dots\}$
$\mathbb{N}_0$	the nonnegative integers, $\{0,1,2,\dots\}$
$\mathbb{Z}$	the integers
$\mathbb{Q}$	the rational numbers
$\mathbb{Q}^+$	the positive rational numbers
$\mathbb{Q}_0^+$	the nonnegative rational numbers
$\mathbb{R}$	the real numbers
$\mathbb{R}^+$	the positive real numbers
$\mathbb{C}$	the complex numbers
$\mathbb{Z}_n$	the integers modulo n
$1\,..\,n$	the integers $1,\ 2,\ \dots,\ n$

Notations from Sets, Logic, and Geometry

$\iff$	iff, if and only if
$\implies$	implies
$A \subset B$	A is a subset of B
$A \setminus B$	A without B
$A \cap B$	the intersection of A and B
$A \cup B$	the union of A and B
$a \in A$	the element a belongs to the set A
$\lvert AB\rvert$	also AB, the distance between the points A and B
box	parallelepiped, solid bounded by three pairs of parallel planes

1

The Invariance Principle

We present our first *Higher Problem-Solving Strategy*. It is extremely useful in solving certain types of difficult problems, which are easily recognizable. We will teach it by solving problems which use this strategy. In fact, **problem solving can be learned only by solving problems.** But it must be supported by strategies provided by the trainer.

Our first strategy is the *search for invariants*, and it is called the **Invariance Principle**. The principle is applicable to algorithms (games, transformations). Some task is repeatedly performed. **What stays the same? What remains invariant?** Here is a saying easy to remember:

If there is repetition, look for what does not change!

In algorithms there is a starting state S and a sequence of legal steps (moves, transformations). One looks for answers to the following questions:

1. Can a given end state be reached?

2. Find all reachable end states.

3. Is there convergence to an end state?

4. Find all periods with or without tails, if any.

Since the Invariance Principle is a *heuristic principle*, it is best learned by experience, which we will gain by solving the key examples **E1** to **E10**.

E1. *Starting with a point $S = (a, b)$ of the plane with $0 < b < a$, we generate a sequence of points (x_n, y_n) according to the rule*

$$x_0 = a, \quad y_0 = b, \quad x_{n+1} = \frac{x_n + y_n}{2}, \quad y_{n+1} = \frac{2x_n y_n}{x_n + y_n}.$$

Here it is easy to find an *invariant*. From $x_{n+1}y_{n+1} = x_n y_n$, for all n we deduce $x_n y_n = ab$ for all n. This is the *invariant* we are looking for. Initially, we have $y_0 < x_0$. This relation also remains invariant. Indeed, suppose $y_n < x_n$ for some n. Then x_{n+1} is the midpoint of the segment with endpoints y_n, x_n. Moreover, $y_{n+1} < x_{n+1}$ since the harmonic mean is strictly less than the arithmetic mean. Thus,

$$0 < x_{n+1} - y_{n+1} = \frac{x_n - y_n}{x_n + y_n} \cdot \frac{x_n - y_n}{2} < \frac{x_n - y_n}{2}$$

for all n. So we have $\lim x_n = \lim y_n = x$ with $x^2 = ab$ or $x = \sqrt{ab}$.

Here the invariant helped us very much, but its recognition was not yet the solution, although the completion of the solution was trivial.

E2. *Suppose the positive integer n is odd. First Al writes the numbers $1, 2, \ldots, 2n$ on the blackboard. Then he picks any two numbers a, b, erases them, and writes, instead, $|a - b|$. Prove that an odd number will remain at the end.*

Solution. Suppose S is the sum of all the numbers still on the blackboard. Initially this sum is $S = 1 + 2 + \cdots + 2n = n(2n + 1)$, an odd number. Each step reduces S by $2\min(a, b)$, which is an even number. So the parity of S is an *invariant*. During the whole reduction process we have $S \equiv 1 \bmod 2$. Initially the parity is odd. So, it will also be odd at the end.

E3. *A circle is divided into six sectors. Then the numbers $1, 0, 1, 0, 0, 0$ are written into the sectors (counterclockwise, say). You may increase two neighboring numbers by 1. Is it possible to equalize all numbers by a sequence of such steps?*

Solution. Suppose $a_1, \ldots, a_6$ are the numbers currently on the sectors. Then $I = a_1 - a_2 + a_3 - a_4 + a_5 - a_6$ is an *invariant*. Initially $I = 2$. The goal $I = 0$ cannot be reached.

E4. *In the Parliament of Sikinia, each member has* **at most three enemies.** *Prove that the house can be separated into two houses, so that each member has* **at most one enemy** *in his own house.*

Solution. Initially, we separate the members in any way into the two houses. Let H be the total sum of all the enemies each member has in his own house. Now suppose A has at least two enemies in his own house. Then he has at most one enemy in the other house. If A switches houses, the number H will decrease. This decrease cannot go on forever. At some time, H reaches its absolute minimum. Then we have reached the required distribution.

Here we have a new idea. We construct a positive integral function which decreases at each step of the algorithm. So we know that our algorithm will terminate. There is no strictly decreasing infinite sequence of positive integers. H is not strictly an invariant, but decreases monotonically until it becomes constant. Here, the monotonicity relation is the invariant.

E5. *Suppose not all four integers a, b, c, d are equal. Start with (a, b, c, d) and repeatedly replace (a, b, c, d) by $(a - b, b - c, c - d, d - a)$. Then at least one number of the quadruple will eventually become arbitrarily large.*

Solution. Let $P_n = (a_n, b_n, c_n, d_n)$ be the quadruple after n iterations. Then we have $a_n + b_n + c_n + d_n = 0$ for $n \geq 1$. We do not see yet how to use this invariant. But geometric interpretation is mostly helpful. A very important function for the point P_n in 4-space is the square of its distance from the origin $(0, 0, 0, 0)$, which is $a_n^2 + b_n^2 + c_n^2 + d_n^2$. If we could prove that it has no upper bound, we would be finished.

We try to find a relation between P_{n+1} and P_n:

$$\begin{aligned} a_{n+1}^2 + b_{n+1}^2 + c_{n+1}^2 + d_{n+1}^2 &= (a_n - b_n)^2 + (b_n - c_n)^2 + (c_n - d_n)^2 + (d_n - a_n)^2 \\ &= 2(a_n^2 + b_n^2 + c_n^2 + d_n^2) \\ &\quad - 2a_nb_n - 2b_nc_n - 2c_nd_n - 2d_na_n. \end{aligned}$$

Now we can use $a_n + b_n + c_n + d_n = 0$ or rather its square:

$$0 = (a_n+b_n+c_n+d_n)^2 = (a_n+c_n)^2+(b_n+d_n)^2+2a_nb_n+2a_nd_n+2b_nc_n+2c_nd_n. \tag{1}$$

Adding (1) and (2), for $a_{n+1}^2 + b_{n+1}^2 + c_{n+1}^2 + d_{n+1}^2$, we get

$$2(a_n^2 + b_n^2 + c_n^2 + d_n^2) + (a_n + c_n)^2 + (b_n + d_n)^2 \geq 2(a_n^2 + b_n^2 + c_n^2 + d_n^2).$$

From this invariant inequality relationship we conclude that, for $n \geq 2$,

$$a_n^2 + b_n^2 + c_n^2 + d_n^2 \geq 2^{n-1}(a_1^2 + b_1^2 + c_1^2 + d_1^2). \tag{2}$$

The distance of the points P_n from the origin increases without bound, which means that at least one component must become arbitrarily large. Can you always have equality in (2)?

Here we learned that the distance from the origin is a very important function. Each time you have a sequence of points you should consider it.

E6. *An algorithm is defined as follows:*

$$\begin{aligned} &\textit{Start:} \quad (x_0, y_0) \textit{ with } 0 < x_0 < y_0. \\ &\textit{Step:} \quad x_{n+1} = \frac{x_n + y_n}{2}, \qquad y_{n+1} = \sqrt{x_{n+1}y_n}. \end{aligned}$$

Some more trials suggest that, even for all nonnegative real quadruples, we always end up with $(0, 0, 0, 0)$. But with $t > 1$ and $S = (1, t, t^2, t^3)$ we have

$$T(S) = [t - 1, (t - 1)t, (t - 1)t^2, (t - 1)(t^2 + t + 1)].$$

If $t^3 = t^2 + t + 1$, i.e., $t = 1.8392867552\ldots$, then the process never stops because of the second observation. This t is unique up to a transformation $f(t) = at + b$.

(b) Start with $S = (a_0, a_1, \ldots, a_{n-1})$, a_i nonnegative integers. For $n = 2$, we reach $(0, 0)$ after 2 steps at most. For $n = 3$, we get, for 011, a pure cycle of length 3: $011 \mapsto 101 \mapsto 110 \mapsto 011$. For $n = 5$ we get $00011 \mapsto 00101 \mapsto 01111 \mapsto 10001 \mapsto 10010 \mapsto 10111 \mapsto 11000 \mapsto 01001 \mapsto 11011 \mapsto 01100 \mapsto 10100 \mapsto 11101 \mapsto 00110 \mapsto 01010 \mapsto 11110 \mapsto 00011$, which has a pure cycle of length 15.

1. Find the periods for $n = 6$ ($n = 7$) starting with 000011 (0000011).

2. Prove that, for $n = 8$, the algorithm stops starting with 00000011.

3. Prove that, for $n = 2^r$, we always reach $(0, 0, \ldots, 0)$, and, for $n \neq 2^r$, we get (up to some exceptions) a cycle containing just two numbers: 0 and evenly often some number $a > 0$. Because of observation 2, we may assume that $a = 1$. Then $| a - b | = a + b \bmod 2$, and we do our calculations in GF(2), i.e., the finite field with two elements 0 and 1.

4. Let $n \neq 2^r$ and $c(n)$ be the cycle length. Prove that $c(2n) = 2c(n)$ (up to some exceptions).

5. Prove that, for odd n, $S = (0, 0, \ldots, 1, 1)$ always lies on a cycle.

6. *Algebraization.* To the sequence $(a_0, \ldots, a_{n-1})$, we assign the polynomial $p(x) = a_{n-1} + \cdots + a_0 x^{n-1}$ with coefficients from GF(2), and $x^n = 1$. The polynomial $(1 + x)p(x)$ belongs to $T(S)$. Use this algebraization if you can.

7. The following table was generated by means of a computer. Guess as many properties of $c(n)$ as you can, and prove those you can.

n	3	5	7	9	11	13	15	17	19	21	23	25
$c(n)$	3	15	7	63	341	819	15	255	9709	63	2047	25575

n	27	29	31	33	35	37	39	41	43
$c(n)$	13797	47507	31	1023	4095	3233097	4095	41943	5461

Problems

1. Start with the positive integers $1, \ldots, 4n - 1$. In one move you may replace any two integers by their difference. Prove that an even integer will be left after $4n - 2$ steps.

2. Start with the set $\{3, 4, 12\}$. In each step you may choose two of the numbers a, b and replace them by $0.6a - 0.8b$ and $0.8a + 0.6b$. Can you reach the goal (a) or (b) in finitely many steps:

   (a) $\{4, 6, 12\}$, (b) $\{x, y, z\}$ with $|x - 4|, |y - 6|, |z - 12|$ each less than $1/\sqrt{3}$?

3. Assume an 8×8 chessboard with the usual coloring. You may repaint all squares (a) of a row or column (b) of a 2×2 square. The goal is to attain just one black square. Can you reach the goal?

4. We start with the state (a, b) where a, b are positive integers. To this initial state we apply the following algorithm:

   while $a > 0$, **do if** $a < b$ **then** $(a, b) \leftarrow (2a, b - a)$ **else** $(a, b) \leftarrow (a - b, 2b)$.

   For which starting positions does the algorithm stop? In how many steps does it stop, if it stops? What can you tell about periods and tails?

   The same questions, when a, b are positive reals.

5. Around a circle, 5 ones and 4 zeros are arranged in any order. Then between any two equal digits, you write 0 and between different digits 1. Finally, the original digits are wiped out. If this process is repeated indefinitely, you can never get 9 zeros. Generalize!

6. There are a white, b black, and c red chips on a table. In one step, you may choose two chips of different colors and replace them by a chip of the third color. If just one chip will remain at the end, its color will not depend on the evolution of the game. When can this final state be reached?

7. There are a white, b black, and c red chips on a table. In one step, you may choose two chips of different colors and replace each one by a chip of the third color. Find conditions for all chips to become of the same color. Suppose you have initially 13 white 15 black and 17 red chips. Can all chips become of the same color? What states can be reached from these numbers?

8. There is a positive integer in each square of a rectangular table. In each move, you may double each number in a row or subtract 1 from each number of a column. Prove that you can reach a table of zeros by a sequence of these permitted moves.

9. Each of the numbers 1 to 10^6 is repeatedly replaced by its digital sum until we reach 10^6 one-digit numbers. Will these have more 1's or 2's?

10. The vertices of an n-gon are labeled by real numbers $x_1, \ldots, x_n$. Let a, b, c, d be four successive labels. If $(a - d)(b - c) < 0$, then we may switch b with c. Decide if this switching operation can be performed infinitely often.

11. In Fig. 1.5, you may switch the signs of all numbers of a row, column, or a parallel to one of the diagonals. In particular, you may switch the sign of each corner square. Prove that at least one -1 will remain in the table.

1	1	1	1
1	1	1	1
1	1	1	1
1	-1	1	1

Fig. 1.5

Prove that there is a limiting point with $x = y$. Find this limit.

58. Consider any binary word $W = a_1a_2\cdots a_n$. It can be transformed by inserting, deleting or appending any word XXX, X being any binary word. Our goal is to transform W from 01 to 10 by a sequence of such transformations. Can the goal be attained (LMO 1988, oral round)?

59. Seven vertices of a cube are marked by 0 and one by 1. You may repeatedly select an edge and increase by 1 the numbers at the ends of that edge. Your goal is to reach (a) 8 equal numbers, (b) 8 numbers divisible by 3.

60. Start with a point $S(a, b)$ of the plane with $0 < b < a$, and generate a sequence of points $S_n(x_n, y_n)$ according to the rule

$$x_0 = a, \quad y_0 = b, \quad x_{n+1} = \frac{2x_ny_n}{x_n + y_n}, \quad y_{n+1} = \frac{2x_{n+1}y_n}{x_{n+1} + y_n}.$$

Prove that there is a limiting point with $x = y$. Find this limit.

Solutions

1. In one move the number of integers always decreases by one. After $(4n - 2)$ steps, just one integer will be left. Initially, there are $2n$ even integers, which is an even number. If two odd integers are replaced, the number of odd integers decreases by 2. If one of them is odd or both are even, then the number of odd numbers remains the same. Thus, the number of odd integers remains even after each move. Since it is initially even, it will remain even to the end. Hence, one even number will remain.

2. (a) $(0.6a-0.8b)^2+(0.8a+0.6b)^2 = a^2+b^2$. Since $a^2+b^2+c^2 = 3^2+4^2+12^2 = 13^2$, the point (a, b, c) lies on the sphere around O with radius 13. Because $4^2+6^2+12^2 = 14^2$, the goal lies on the sphere around O with radius 14. The goal cannot be reached.
(b) $(x - 4)^2 + (y - 6)^2 + (z - 12)^2 < 1$. The goal cannot be reached.
The important invariant, here, is the distance of the point (a, b, c) from O.

3. (a) Repainting a row or column with b black and $8 - b$ white squares, you get $(8 - b)$ black and b white squares. The number of black squares changes by $|(8 - b) - b| = |8 - 2b|$, that is an even number. The parity of the number of black squares does not change. Initially, it was even. So, it always remains even. One black square is unattainable. The reasoning for (b) is similar.

4. Here is a solution valid for natural, rational and irrational numbers. With the invariant $a + b = n$ the algorithm can be reformulated as follows:

   If $a < n/2$, replace a by $2a$.

   If $a \geq n/2$, replace a by $a - b = a - (n - a) = 2a - n \equiv 2a \pmod{n}$.

   Thus, we double a repeatedly modulo n and get the sequence

$$a, 2a, 2^2a, 2^3a, \ldots \pmod{n}. \tag{1}$$

   Divide a by n in base 2. There are three cases.
   (a) The result is terminating: $a/n = 0.d_1d_2d_3\ldots d_k, \quad d_i \in \{0, 1\}$. Then $2^k \equiv 0$

2
Coloring Proofs

The problems of this chapter are concerned with the partitioning of a set into a finite number of subsets. The partitioning is done by *coloring* each element of a subset by the same color. The prototypical example runs as follows.

In 1961, the British theoretical physicist M.E. Fisher solved a famous and very tough problem. He showed that an 8×8 chessboard can be covered by 2×1 dominoes in $2^4 \times 901^2$ or 12,988,816 ways. Now let us cut out two diagonally opposite corners of the board. In how many ways can you cover the 62 squares of the mutilated chessboard with 31 dominoes?

The problem looks even more complicated than the problem solved by Fisher, but this is not so. The problem is trivial. There is no way to cover the mutilated chessboard. Indeed, each domino covers one black and one white square. If a covering of the board existed, it would cover 31 black and 31 white squares. But the mutilated chessboard has 30 squares of one color and 32 squares of the other color.

The following problems are mostly ingenious impossibility proofs based on coloring or parity. Some really belong to Chapter 3 or Chapter 4, but they use coloring, so I put them in this chapter. A few also belong to the closely related Chapter 1. The mutilated chessboard required two colors. The problems of this chapter often require more than two colors.

29. Each element of a 25×25 matrix is either $+1$ or -1. Let a_i be the product of all elements of the ith row and b_j be the product of all elements of the jth column. Prove that $a_1 + b_1 + \cdots + a_{25} + b_{25} \neq 0$.

30. Can you pack 53 bricks of dimensions $1 \times 1 \times 4$ into a $6 \times 6 \times 6$ box? The faces of the bricks are parallel to the faces of the box.

31. Three pucks A, B, C are in a plane. An ice hockey player hits the pucks so that any one glides through the other two in a straight line. Can all pucks return to their original spots after 1001 hits?

32. A 23×23 square is completely tiled by 1×1, 2×2 and 3×3 tiles. What minimum number of 1×1 tiles are needed (AUO 1989)?

33. The vertices and midpoints of the faces are marked on a cube, and all face diagonals are drawn. Is it possible to visit all marked points by walking along the face diagonals?

34. There is no closed knight's tour of a $(4 \times n)$ board.

35. The plane is colored with two colors. Prove that there exist three points of the same color, which are vertices of a regular triangle.

36. A sphere is colored in two colors. Prove that there exist on this sphere three points of the same color, which are vertices of a regular triangle.

37. Given an $m \times n$ rectangle, what minimum number of cells (1×1 squares) must be colored, such that there is no place on the remaining cells for an L-tromino?

38. The positive integers are colored black and white. The sum of two differently colored numbers is black, and their product is white. What is the product of two white numbers? Find all such colorings.

Solutions

1. Color the floor as in Fig. 2.7. A 4×1 tile always covers 0 or 2 black squares. A 2×2 tile always covers one black square. It follows immediately from this that it is impossible to exchange one tile for a tile of the other kind.

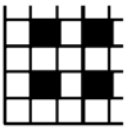


Fig. 2.7

2. Any rectangle with 20 squares can be colored like a chessboard with 10 black and 10 white squares. Four of the tetrominoes will cover 2 black and 2 white squares each. The remaining 2 black and 2 white squares cannot be covered by the T-tetromino. A T-tetromino always covers 3 black and one white squares or 3 white and one black squares.

3. A T-tetromino either covers one white and three black squares or three white and one black squares. See Fig. 2.8. To cover it completely, we need equally many tetrominoes of each kind. But 25 is an odd number. Contradiction!

3

The Extremal Principle

A successful research mathematician has mastered a dozen general heuristic principles of large scope and simplicity, which he/she applies over and over again. These principles are not tied to any subject but are applicable in all branches of mathematics. He usually does not reflect about them but knows them subconsciously. One of these principles, *the invariance principle* was discussed in Chapter I. It is applicable whenever a transformation is given or can be introduced. **If you have a transformation, look for an invariant!** In this chapter we discuss the **extremal principle**, which has truly universal applicability, but is not so easy to recognize, and therefore must be trained. It is also called *the variational method*, and soon we will see why. It often leads to extremely short proofs.

We are trying to prove the existence of an object with certain properties. The *extremal principle* tells us to pick an object which *maximizes* or *minimizes* some function. The *resulting object* is then shown to have the desired property by showing that a slight perturbation (variation) would further increase or decrease the given function. If there are several optimizing objects, then it is usually immaterial which one we use. In addition, the *extremal principle* is mostly constructive, giving an algorithm for constructing the object.

We will learn the use of the *extremal principle* by solving 17 examples from geometry, graph theory, combinatorics, and number theory, but first we will remind the reader of three well known facts:

(a) Every *finite* nonempty set A of nonnegative integers or real numbers has a minimal element $\min A$ and a maximal element $\max A$, which need not be unique.

(b) Every nonempty subset of positive integers has a smallest element. This is called the *well ordering principle*, and it is equivalent to the *principle of mathematical induction.*

(c) An infinite set A of real numbers need not have a minimal or maximal element. If A is bounded above, then it has a smallest upper bound $\sup A$. Read: supremum of A. If A is bounded below, then it has a largest lower bound $\inf A$. Read: infimum of A. If $\sup A \in A$, then $\sup A = \max A$, and if $\inf A \in A$, then $\inf A = \min A$.

E1. *(a) Into how many parts at most is a plane cut by n lines? (b) Into how many parts is space divided by n planes in general position?*

Solution. We denote the numbers in (a) and (b) by p_n and s_n, respectively. A beginner will solve these problems recursively, by finding $p_{n+1} = f(p_n)$ and $s_{n+1} = g(s_n)$. Indeed, by adding to n lines (planes) another line (plane) we easily get

$$p_{n+1} = p_n + n + 1, \qquad s_{n+1} = s_n + p_n.$$

There is nothing wrong with this approach since recursion is a fundamental idea of large scope and applicability, as we will see later. An experienced problem solver might try to solve the problems in his head.

In (a) we have a counting problem. A fundamental counting principle is one-to-one correspondence. The first question is: Can I map the p_n parts of the plane bijectively onto a set which is easy to count? The $\binom{n}{2}$ intersection points of the n lines are easy to count. But each intersection point is the deepest point of exactly one part. (Extremal principle!) Hence there are $\binom{n}{2}$ parts with a deepest point. The parts without deepest points are not bounded below, and they cut a horizontal line h (which we introduce) into $n + 1$ pieces (Fig. 3.1). The parts can be uniquely assigned to these pieces. Thus there are $n + 1$, or $\binom{n}{0} + \binom{n}{1}$ parts without a deepest point. So there are altogether

$$p_n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} \quad \text{parts of the plane.}$$

(b) Three planes form a vertex in space. There are $\binom{n}{3}$ vertices, and each is a deepest point of exactly one part of space. Thus there are $\binom{n}{3}$ parts with a deepest point. Each part without a deepest point intersects a horizonal plane h in one of p_n plane parts. So the number of space parts is

$$s_n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3}.$$

Fig. 3.1

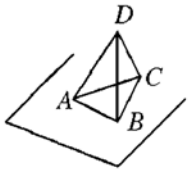


Fig. 3.2

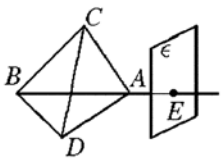


Fig. 3.3

E2. Continuation of 1b. *Let $n \geq 5$. Show that, among the s_n space parts, there are at least $(2n-3)/4$ tetrahedra* (HMO 1973).

Telling the result simplifies the problem considerably. An experienced problem-solver can often infer the road to the solution from the result.

Let t_n be the number of tetrahedra among the s_n space parts. We want to show that $t_n \geq (2n-3)/4$.

Interpretation of the numerator: On each of the n planes rest at least two tetrahedra. Only one tetrahedron need rest on each of three exceptional planes.

Interpretation of the denominator: Each tetrahedron is counted four times, once for each face. Hence, we must divide by four.

Using these guiding principles we can easily find a proof. Let ϵ be any of the n planes. It decomposes space into two half-spaces H_1 and H_2. At least one half-space, e.g., H_1 , contains vertices. In H_1, we choose a vertex D with smallest distance from ϵ (extremal principle). D is the intersection point of the planes $\epsilon_1, \epsilon_2, \epsilon_3$. Then $\epsilon, \epsilon_1, \epsilon_2, \epsilon_3$ define a tetrahedron $T = ABCD$ (Fig. 3.2). None of the remaining $n-4$ planes cuts T, so that T is one of the parts, defined by the n planes. If the plane ϵ' would cut the tetrahedron T, then ϵ' would have to cut at least one of the edges AD, BD, CD in a point Q having an even smaller distance from ϵ than D. Contradiction.

This is valid for any of the n planes. If there are vertices on both sides of a plane, at least two tetrahedra then must rest on this plane.

It remains to be shown that among the n planes there are at most three, so that all vertices lie on the same side of these planes.

We show this by *contradiction.* Suppose there are four such planes ϵ_1, ϵ_2, ϵ_3, ϵ_4. They delimit a tetrahedron $ABCD$ (Fig. 3.3). Since $n \geq 5$, there is another plane ϵ. It cannot intersect all six edges of the tetrahedron $ABCD$ simultaneously. Suppose it cuts the continuation of AB in E. Then B and E lie on different sides of the plane $\epsilon_3 = ACD$. *Contradiction!*

E3. *There are n points given in the plane. Any three of the points form a triangle of area ≤ 1. Show that all n points lie in a triangle of area ≤ 4.*

Solution. Among all $\binom{n}{3}$ triples of points, we choose a triple A, B, C so that $\triangle ABC$ has maximal area F. Obviously $F \leq 1$. Draw parallels to the opposite sides through A, B, C. You get $\triangle A_1B_1C_1$ with area $F_1 = 4F \leq 4$. We will show that $\triangle A_1B_1C_1$ contains all n points.

Suppose there is a point P outside $\triangle A_1B_1C_1$. Then $\triangle ABC$ and P lie on different sides of at least one of the lines A_1B_1, B_1C_1, C_1A_1. Suppose they lie on different sides of B_1C_1. Then $\triangle BCP$ has a larger area than $\triangle ABC$. This contradicts the maximality assumption about ABC (Fig. 3.4).

E4. *$2n$ points are given in the plane, no three collinear. Exactly n of these points are farms $F = \{F_1, F_2, \ldots, F_n\}$. The remaining n points are wells: $W = \{W_1, W_2, \ldots, W_n\}$. It is intended to build a straight line road from each*

farm to one well. Show that the wells can be assigned bijectively to the farms, so that none of the roads intersect.

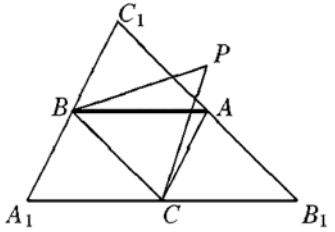


Fig. 3.4

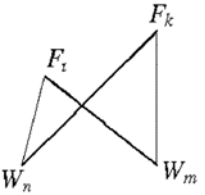


Fig. 3.5

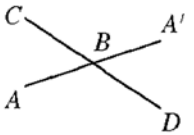


Fig. 3.6

Solution. We consider any bijection: $f : F \mapsto W$. If we draw from each F_i a straight line to $f(F_i)$, we get a road system. Among all $n!$ road systems, we choose one of minimal total length.Suppose this system has intersecting segments F_iW_m and F_kW_n (Fig. 3.5). Replacing these segments by F_kW_m and F_iW_n, the total road length becomes shorter because of the triangle inequality. Thus it has no intersecting roads.

E5. *Let Ω be a set of points in the plane. Each point in Ω is a midpoint of two points in Ω. Show that Ω is an infinite set.*

First proof. Suppose Ω is a finite set. Then Ω contains two points A, B with maximal distance $|AB| = m$. B is a midpoint of some segment CD with $C, D \in \Omega$. Fig. 3.6 shows that $|AC| > |AB|$ or $|AD| > |AB|$.

Second proof. We consider all points in Ω farthest to the left, and among those the point M farthest down. M cannot be a midpoint of two points $A, B \in \Omega$ since one element of $\{A, B\}$ would be either left of M or on the vertical below M.

E6. *In each convex pentagon, we can choose three diagonals from which a triangle can be constructed.*

Solution. Fig. 3.7 shows a convex pentagon $ABCDE$. Let BE be the longest of the diagonals. The triangle inequality implies $|BD| + |CE| > |BE| + |CD| > |BE|$, that is, we can construct a triangle from BE, BD, CE.

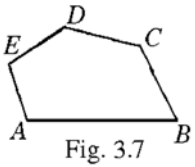


Fig. 3.7

E7. *In every tetrahedron, there are three edges meeting at the same vertex from which a triangle can be constructed.*

Solution. Let AB be the *longest* edge of the tetrahedron $ABCD$. Since $(|AC| + |AD| - |AB|) + (|BC| + |BD| - |BA|) = (|AD| + |BD| - |AB|) + (|AC| + |BC| -$

$|AB|) > 0$ then, either $|AC| + |AD| - |AB| > 0$, or $|BC| + |BD| - |BA| > 0$. In each case, we can construct a triangle from the edges at some vertex.

E8. *Each lattice point of the plane is labeled by a positive integer. Each of these numbers is the arithmetic mean of its four neighbors (above, below, left, right). Show that all the labels are equal.*

Solution. We consider a smallest label m. Let L be a lattice point labeled by m. Its neighbors are labeled by a, b, c, d. Then $m = (a + b + c + d)/4$, or

$$a + b + c + d = 4m. \tag{1}$$

Now $a \geq m, b \geq m, c \geq m, d \geq m$. If any of these inequalities would be strict, we would have $a + b + c + d > 4m$ which contradicts (1). Thus $a = b = c = d = m$. It follows from this that all labels are equal to m.

This is a very simple problem. By replacing positive integers by positive reals, it becomes a very difficult problem. The trouble is that positive reals need not have a smallest element. For positive integers, this is assured by the *well ordering principle*. The theorem is still valid, but I do not know an elementary solution.

E9. *There is no quadruple of positive integers (x, y, z, u) satisfying*

$$x^2 + y^2 = 3(z^2 + u^2).$$

Solution. Suppose there is such a quadruple. We choose the solution with the smallest $x^2 + y^2$. Let (a, b, c, d) be the chosen solution. Then

$$a^2 + b^2 = 3(c^2 + d^2) \Rightarrow 3|a^2 + b^2 \Rightarrow 3|a, 3|b \Rightarrow a = 3a_1, b = 3b_1,$$
$$a^2 + b^2 = 9(a_1^2 + b_1^2) = 3(c^2 + d^2) \Rightarrow c^2 + d^2 = 3(a_1^2 + b_1^2).$$

We have found a new solution (c, d, a_1, b_1) with $c^2 + d^2 < a^2 + b^2$. *Contradiction.*

We have used the fact that $3|a^2 + b^2 \Rightarrow 3|a, 3|b$. Show this yourself. We will return to similar examples when treating *infinite descent.*

E10. The Sylvester Problem, posed by Sylvester in 1893, was solved by T. Gallai 1933 in a very complicated way and by L.M. Kelly in 1948 in a few lines with the extremal principle.

A finite set S of points in the plane has the property that any line through two of them passes through a third. Show that all the points lie on a line.

Solution. Suppose the points are not collinear. Among pairs (p, L) consisting of a line L and a point not on that line, choose one which minimizes the distance d from p to L. Let f be the foot of the perpendicular from p to L. There are (by assumption) at least three points a, b, c on L. Hence two of these, say, a and b are on the same side of f (Fig. 3.8). Let b be nearer to f than a. Then the distance from b to the line ap is less than d. *Contradiction.*

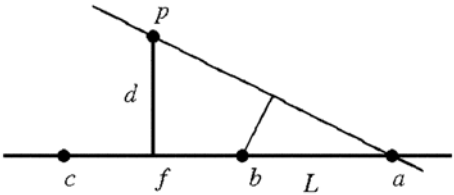


Fig. 3.8

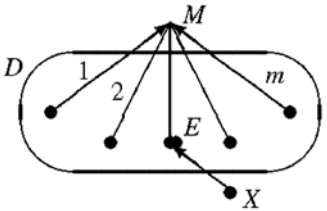


Fig. 3.9

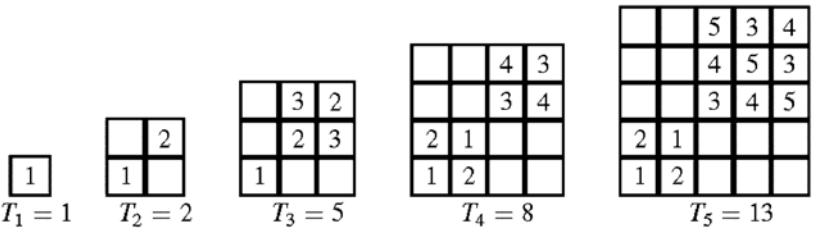
E11. *Every road in Sikinia is one-way. Every pair of cities is connected exactly by one direct road. Show that there exists a city which can be reached from every city directly or via at most one other city.*

Solution. Let m be the *maximum* number of direct roads leading into any city, and let M be a city for which this maximum is attained. Let D be the set of m cities with direct connections into M. Let R be the set of all cities apart from M and the cities in D. If $R = \emptyset$, the theorem is valid. If $X \in R$, then there is an $E \in D$ with connection $X \to E \to M$. If such an E did not exist, then X could be reached directly from all cities in D and from M, that is, $m + 1$ roads would lead into X, which contradicts the assumption about M. Thus, every city with the maximum number of entering roads satisfies the conditions of the problem (Fig. 3.9).

E12. *Rooks on an $n \times n \times n$ chessboard. Obviously n is the smallest number of rooks which can dominate an $n \times n$ chessboard. But what is the number R_n of rooks, which can dominate an $n \times n \times n$-chessboard?*

Solution. We try to guess the result for small values of n. But first we need a good representation for placing rooks in space. We place n layers of size $n \times n \times 1$ over an $n \times n$ square, and we number them $1, 2, \ldots, n$. Each rook is labeled with the number of the layer on which it is located. Fig. 3.10 suggests the conjecture

$$R_n = \begin{cases} \frac{n^2}{2} & : \quad n \equiv 0 \bmod 2, \\ \frac{n^2+1}{2} & : \quad n \equiv 1 \bmod 2. \end{cases}$$



$T_1 = 1$ $T_2 = 2$ $T_3 = 5$ $T_4 = 8$ $T_5 = 13$

Fig. 3.10

Now comes the proof. Suppose R rooks are so placed on the n^3 cubes of the board, that they dominate all cubes. We choose a layer L, which contains the *minimum* number of rooks. We may assume that it is parallel to the x_1x_2-plane. Suppose that L contains t rooks. Suppose these t rooks dominate t_1 rows in the

x_1-direction and t_2 rows in the x_2-direction. We may further assume that $t_1 \geq t_2$. Obviously $t \geq t_1$ and $t \geq t_2$. In the layer L, these rooks fail to dominate $(n-t_1)(n-t_2)$ cubes, which must be dominated in the x_3-direction. We consider all n layers parallel to the x_1x_3-plane. In $n-t_1$ of these not containing a rook from L, there must be at least $(n-t_1)(n-t_2)$ rooks. In each of the remaining t_1 layers are at least t rooks (by the choice of t). Hence, we have

$$R \geq (n-t_1)(n-t_2) + tt_1 \geq (n-t_1)^2 + t_1^2 = \frac{n^2}{2} + \frac{(2t_1-n)^2}{2}.$$

The right side assumes its minimum $n^2/2$ for even n and $(n^2+1)/2$ for odd n. It is easy to see that this necessary number is also sufficient. Fig. 3.11 gives a hint for a proof (MMO 1965, AUO 1971, IMO 1971).

Remark. The exact number of rooks which dominate an $n \times n \times n \times n$ board and other higher dimensional boards does not seem to be known. Here good bounds would be welcome.

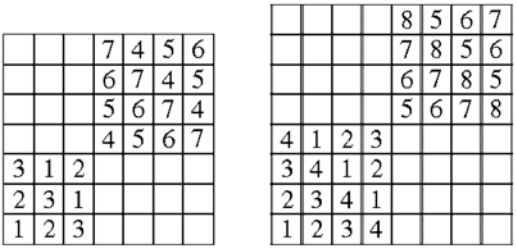


Fig. 3.11

E13. *Seven dwarfs are sitting around a circular table. There is a cup in front of each. There is milk in some cups, altogether 3 liters. One of the dwarfs shares his milk uniformly with the other cups. Proceeding counter-clockwise, each of the other dwarfs, in turn, does the same. After the seventh dwarf has shared his milk, the initial content of each cup is restored. Find the initial amount of milk in each cup (AUO 1977, grade 8).*

Solution. Every 8th grader, 53 altogether, guessed the correct answer 6/7, 5/7, 4/7, 3/7, 2/7, 1/7, 0 liters. The answer is easy to guess because of an invariance property. Each sharing operation merely rotates the answer. But only 9 students could prove that the answer is unique. The solutions were quite ingenious and required just a few lines. We prefer, instead, a solution based on a general principle, in this case, the *extremal principle.*

Suppose the dwarf *#i* has the (maximal) amount x_i before starting to share his milk. The dwarf Max has the maximum amount x to share. The others to the right of him have $x_1, x_2, \ldots, x_6$ to share. Max gets $x_i/6$ from dwarf *#i*. Thus, we have

$$x = \frac{x_1+x_2+x_3+x_4+x_5+x_6}{6}, \tag{1}$$

where $x_i \leq x$ for $i = 1, \ldots, 6$. If the inequality would be strict only once, we could not have equality in (1). Thus $x_1 = x_2 = x_3 = x_4 = x_5 = x_6 = x$, that is, each dwarf shares the same amount of milk. We easily infer from this that, initially, the milk distribution is 0, $x/6$, $2x/6$, $3x/6$,$4x/6$, $5x/6$, $6x/6$. From the sum 3 liters, we get $x = 6/7$.

E14. *The Sikinian Parliament consists of one house. Every member has three enemies at most among the remaining members. Show that one can split the house into two houses so that every member has one enemy at most in his house.*

Solution. We consider all partitions of the Parliament into two houses and, for each partition, we count the total number E of enemies each member has in his house. The partition with minimal E has the required property. Indeed, if some member would have *at least two enemies* in his house, then he would have *one enemy at most* in the other house. By placing him in the other house, we could decrease the minimal E, which is a contradiction.

We have solved this problem already in Chapter 1 by a variation of the invariance principle which we call the **Principle of the Finiteness of a Decreasing Sequence of Nonnegative Integers**. So the Extremal Principle is related to the Invariance Principle.

E15. *Can you choose* 1983 *pairwise distinct positive integers* < 100000, *such that no three are in arithmetic progression* (IMO 1983)?

All hints to the solution are eliminated in this problem. So we must recover them. We need some strategic idea to get the first clues. Let us construct a tight sequence with no three terms in arithmetic progression. Here, the extremal principle helps in finding an algorithm. We use the so-called *greedy algorithm*: Start with the smallest nonnegative integer 0. At each step, add the smallest integer which is not in arithmetic progression with two preceding terms. We get

- 0, 1 (translate this by 3),
- 0, 1, 3, 4 (translate this by 9),
- 0, 1, 3, 4, 9, 10, 12, 13 (translate this by 27), and
- 0, 1, 3, 4, 9, 10, 12, 13, 27, 28, 30, 31, 36, 37, 39, 40 (translate this by 81).

We get a sequence with many regularities. The powers of 3 are a hint to use the ternary system. So we rewrite the sequence in the ternary system, getting

$$0,\ 1,\ 10,\ 11,\ 100,\ 101,\ 110,\ 111,\ 1000, \ldots.$$

This is a hint to the binary system. We conjecture that the constructed sequence consists of those ternary numbers, which miss the digit 2, i.e., they are written in the binary system. Our next conjecture is that if we read the terms of the sequence

a_n in the binary system, we get n. Read in the ternary system, we get a_n. The solution to our problem is

$$a_{1983} = a_{11110111111_2} = 11110111111_3 = 87844.$$

It is quite easy to finish the problem. Five of our six team members gave this answer, probably, because in training I briefly treated the greedy algorithm as a construction principle for good but not necessarily optimal solutions. This is one of the innumerable versions of the *Extremal Principle*.

E16. *There exist three consecutive vertices A, B, C in every convex n-gon with $n \geq 3$, such that the circumcircle of $\triangle ABC$ covers the whole n-gon.*

Among the finitely many circles through three vertices of the n-gon, there is a **maximal circle**. Now we split the problem into two parts:

(a) the maximal circle covers the n-gon, and
(b) the **maximal circle** passes through three consecutive vertices.

We prove (a) indirectly. Suppose the point A' lies outside the maximal circle about $\triangle ABC$ where A, B, C are denoted such that A, B, C, A' are vertices of a convex quadrilateral. Then the circumcircle of $\triangle A'BC$ has a larger radius then that of $\triangle ABC$. Contradiction.

We also prove (b) indirectly. Let A, B, C be vertices on the **maximal circle**, and let A' lie between B and C and not on the maximal circle. Because of (a), it lies inside that circle, but then the circle about $\triangle A'BC$ is larger than the maximal circumcircle. Contradiction.

E17. *$n\sqrt{2}$ is not an integer for any positive integer n.*

We use a proof method of wide applicability based on the **extremal principle**. Let S be the set of those positive integers n, for which $n\sqrt{2}$ is an integer. If S is not empty, it would have a **least element** k. Consider $(\sqrt{2}-1)k$. Then

$$(\sqrt{2}-1)k\sqrt{2} = 2k - k\sqrt{2},$$

and, since $k \in S$, both $(\sqrt{2}-1)k$ and $2k - k\sqrt{2}$ are positive integers. So, by definition, $(\sqrt{2}-1)k \in S$. But $(\sqrt{2}-1)k < k$, contradicting the assumption that k is the least element of S. Hence S is empty, which means that $\sqrt{2}$ is irrational.

Problems

1. Prove that there are at least $(2n-2)/3$ triangles among the p_n parts of the plane in Example #1.
2. In the plane, n lines are given ($n \geq 3$), no two of them parallel. Through every intersection of two lines there passes at least an additional line. Prove that all lines pass through one point.

3. If n points of the plane do not lie on the same line, then there exists a line passing through exactly two points.
4. Start with several piles of chips. Two players move alternately. A move consists in splitting every pile with more than one chip into two piles. The one who makes the last move wins. For what initial conditions does the first player win and what is his winning strategy?
5. Does there exist a tetrahedron, so that every edge is the side of an obtuse angle of a face?
6. Prove that every convex polyhedron has at least two faces with the same number of sides.
7. $(2n+1)$ persons are placed in the plane so that their mutual distances are different. Then everybody shoots his nearest neighbor. Prove that

   (a) at least one person survives; (b) nobody is hit by more then five bullets;

   (c) the paths of the bullets do not cross; d) the set of segments formed by the bullet paths does not contain a closed polygon.
8. Rooks are placed on the $n \times n$ chessboard satisfying the following condition: If the square (i, j) is free, then at least n rooks are on the ith row and jth column together. Show that there are at least $n^2/2$ rooks on the board.
9. All plane sections of a solid are circles. Prove that the solid is a ball.
10. A closed and bounded figure Φ with the following property is given in a plane: Any two points of Φ can be connected by a half circle lying completely in Φ. Find the figure Φ (West German proposal for IMO 1977).
11. Of n points in space, no four lie in a plane. Some of the points are connected by lines. We get a graph G with k edges.

    (a) If G does not contain a triangle, then $k \leq \lfloor n^2/4 \rfloor$.

    (b) If G does not contain a tetrahedron, then $k \leq \lfloor n^2/3 \rfloor$.
12. There are 20 countries on a planet. Among any three of these countries, there are always two with no diplomatic relations. Prove that there are at most 200 embassies on this planet.
13. Every participant of a tournament plays with every other participant exactly once. No game is a draw. After the tounament, every player makes a list with the names of all players, who

    (a) were beaten by him and (b) were beaten by the players beaten by him.

    Prove that the list of some player contains the names of all other players.
14. Let O be the point of intersection of the diagonals of the convex quadrilateral $ABCD$. Prove that, if the perimeters of the triangles ABO, BCO, CDO and DAO are equal, then $ABCD$ is a rhombus.
15. There are n identical cars on a circular track. Together they have just enough gas for one car to complete a lap. Show that there is a car which can complete a lap by collecting gas from the other cars on its way around.
16. Let M be the largest distance among six distinct points of the plane, and let m be the smallest of their mutual distances. Prove that $M/m \geq \sqrt{3}$.
17. A cube cannot be divided into several pairwise distinct cubes.

35. Six circles have a common point A. Prove that there is one among these circles which contains the center of another circle.

36. We choose n points on a circle and draw all chords joining these n points. Find the number of parts into which the circular disk is cut.

37. Each of 30 students in a class has the same number of friends among his class mates. What is the highest possible number of students, who learn better than the majority of their friends? Of any two students one can tell which one is better (RO 1994).

38. A set S of persons has the following property. Any two with the same number of friends in S have no common friends in S. Prove that there is a person in S with exactly one friend in S.

39. The sum of several nonnegative reals is 3, and the sum of their squares is > 1. Prove that you may choose three of these numbers with sum > 1.

40. Several positive reals are written on paper. The sum of their pairwise products is 1. Prove that you can cross out one number, so that the sum of the remaining numbers is less than $\sqrt{2}$.

41. m chips ($m > n$) are placed at the vertices of a convex n-gon. In one move, two chips at a vertex are moved in opposite directions to neighboring vertices. Prove that, if the original distribution is restored after some moves, then the number of moves is a multiple of n.

42. It is known that the numbers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are both permutations of $1, 1/2, \ldots, 1/n$. In addition, we know that $a_1 + b_1 \geq a_2 + b_2 \geq \cdots \geq a_n + b_n$. Prove that $a_m + b_m \leq 4/m$ for all m from 1 to n.

43. Fifty segments are given on a line. Prove that some eight of the segments have a common point, or eight of the segments are pairwise disjoint (AUO 1972).

44. There are n students in each of three schools. Any student has altogether $n + 1$ acquaintances from the other two schools. Prove that one can select one student from each school, so that the three selected students know each other.

Solutions

1. Use the ideas of **E2**, which treats the more complicated space analogue.

2. Suppose not all lines pass through one point. We consider all intersection points, and we choose the smallest of the distances from these points to the lines. Suppose the smallest distance is from the point A to the line l. At least three lines pass through A. They intersect l in B, C, D. From A drop the perpendicular AP to l. Two of the points B, C, D lie on the same side of P. Suppose these are C and D. Suppose $|CP| < |DP|$. Then the distance from C to AD is smaller than the distance from A to l, contradicting the choice of A and l. (This argument is exactly the one used by L.M. Kelly.)

3. Again, this is a variation of Sylvester's problem.

4. It is my move. *It all depends on the largest pile.* Suppose it contains M chips. As long as $M > 1$, I can move. Trying small numbers shows that I must occupy the

4

The Box Principle

The simplest version of Dirichlet's box principle reads as follows:

If $(n + 1)$ *pearls are put into n boxes, then at least one box has more than one pearl.*

This simple combinatorial principle was first used explicitly by Dirichlet (1805–1859) in number theory. In spite of its simplicity it has a huge number of quite unexpected applications. It can be used to prove deep theorems. F.P. Ramsey made vast generalizations of this principle. The topic of *Ramsey Numbers* belongs to the deepest problems of combinatorics. In spite of huge efforts, progress in this area is very slow.

It is easy to recognize if the box principle is to be used. Every existence problem about finite and, sometimes, infinite sets is usually solved by the box principle. The principle is a pure existence assertion. It gives no help in finding a multiply occupied box. The main difficulty is the identification of the *pearls* and the *boxes*.

For a warmup, we begin with a dozen simple problems without solutions:

1. Among three persons, there are two of the same sex.

2. Among 13 persons, there are two born in the same month.

3. Nobody has more than 300,000 hairs on his head. The capital of Sikinia has 300,001 inhabitants. Can you assert with certainty that there are two persons with the same number of hairs on their heads?

4. How many persons do you need to be sure that 2 (3, q) persons have the same birthday?

5. If $qs + 1$ pearls are put into s boxes, then at least one box has more than q pearls.

6. A line l in the plane of the triangle ABC passes through no vertex. Prove that it cannot cut all sides of the triangle.

7. A plane does not pass through a vertex of a tetrahedron. How many edges can it intersect?

8. A target has the form of an equilateral triangle with side 2.

   (a) If it is hit 5 times, then there will be two holes with distance ≤ 1.

   (b) It is hit 17 times. What is the minimal distance of two holes at most?

9. The decimal representation of a/b with coprime a, b has at most period $(b-1)$.

10. From 11 infinite decimals, we can select two numbers a, b so that their decimal representations have the same digits at infinitely many corresponding places.

11. Of 12 distinct two-digit numbers, we can select two with a two-digit difference of the form aa.

12. If none of the numbers $a, a+d, \ldots, a+(n-1)d$ is divisible by n, then d and n are coprime.

The next eleven examples show typical applications of the box principle.

E1. *There are n persons present in a room. Prove that among them there are two persons who have the same number of acquaintances in the room.*

Solution. A person (pearl) goes into box #i if she has i acquaintances. We have n persons and n boxes numbered $0, 1, \ldots, n-1$. But the boxes with the numbers 0 and $n-1$ cannot both be occupied. Thus, there is at least one box with more then one pearl.

E2. *A chessmaster has 77 days to prepare for a tournament. He wants to play at least one game per day, but not more then 132 games. Prove that there is a sequence of successive days on which he plays exactly 21 games.*

Solution. Let a_i be the number of games played until the ith day inclusive. Then

$$1 \leq a_1 < \ldots < a_{77} \leq 132 \Rightarrow 22 \leq a_1 + 21 < a_2 + 21 < \ldots < a_{77} + 21 \leq 153.$$

Among the 154 numbers $a_1, \ldots, a_{77}, a_1 + 21, \ldots, a_{77} + 21$ there are two equal numbers. Hence there are indices i, j, so that $a_i = a_j + 21$. The chessmaster has played exactly 21 games on the days $\#j+1, j+2, \ldots, i$.

E3. *Let $a_1, a_2, \ldots, a_n$ be n not necessarily distinct integers. Then there always exists a subset of these numbers with sum divisible by n.*

Solution. We consider the n integers

$$s_1 = a_1, \quad s_2 = a_1 + a_2, \quad s_3 = a_1 + a_2 + a_3, \ldots, \quad s_n = a_1 + a_2 + \cdots + a_n.$$

If any of these integers is divisible by n, then we are done. Otherwise, all their remainders are different modulo n. Since there are only $n-1$ such remainders, two of the sums, say s_p and s_q with $p < q$, are equal modulo n, that is, the following difference is divisible by n.

$$s_q - s_p = a_{p+1} + \ldots + a_q.$$

This proof contains an important motive with many applications in number theory, group theory, and other areas.

E4. *One of $(n+1)$ numbers from $\{1, 2, \ldots, 2n\}$ is divisible by another.*

Solution. We select $(n+1)$ numbers $a_1, \ldots, a_{n+1}$ and write them in the form $a_i = 2^k b_i$ with b_i odd. Then we have $(n+1)$ odd numbers $b_1, \ldots, b_{n+1}$ from the interval $[1, 2n-1]$. But there are only n odd numbers in this interval. Thus two of them p, q are such that $b_p = b_q$. Then one of the numbers a_p, a_q is divisible by the other.

E5. *Let $a, b \in \mathbb{N}$ be coprime. Then $ax - by = 1$ for some $x, y \in \mathbb{N}$.*

Solution. Consider the remainders mod b of the sequence $a, \ldots, (b-1)a$. The remainder 0 does not occur. If the remainder 1 would not occur either, then we would have positive integers p, q, $0 < p < q < b$, so that $pa \equiv qa \pmod{b}$. But a and b are coprime. Hence we have $b|q-p$. This is a contradiction since $0 < q - p < b$. Thus there exists an x so that $ax \equiv 1 \pmod{b}$, that is, ax=1+by, or $ax - by = 1$.

E6. Erdős and Szekeres. *The positive integers 1 to 101 are written down in any order. Prove that you can strike 90 of these numbers, so that a monotonically increasing or decreasing sequence remains.*

Solution. We prove a generalization: For $n \geq (p-1)(q-1)+1$ every sequence of n integers contains either a monotonically increasing subsequence of length p or a monotonically decreasing subsequence of length q.

We assign the maximal length L_m of a monotonically increasing sequence with last element m and the maximal length R_m of a monotonically decreasing sequence beginning with m to any number m in the sequence.

This assignment has the property that, for two different numbers m and k there must be $L_m \neq L_k$ or $R_m \neq R_k$. This follows easily from the fact that either $m > k$ or $m < k$. All pairs (L_m, R_m) with $m = 1, 2, \ldots, n$ are distinct. Assuming that no such subsequences exist, L_m can assume only the values $1, 2, \ldots, p-1$ and R_m only the values $1, 2, \ldots, q-1$. This gives $(p-1)(q-1)$ different boxes for the pairs. But $n \geq (p-1)(q-1)+1$ and the box principle leads to a contradiction.

E7. *Five lattice points are chosen in the plane lattice. Prove that you can always choose two of these points such that the segment joining these points passes through*

another lattice point. (The plane lattice consists of all points of the plane with integral coordinates.)

Solution. Let us consider the parity patterns of the coordinates of these lattice points. There are only four possible patterns: (e,e),(e,o), (o,e), (o,o). Among the five lattice points, there will be two points, say $A = (a, b)$ and $B = (c, d)$ with the same parity pattern. Consider the midpoint L of AB,

$$L = \left(\frac{a+c}{2}, \frac{b+d}{2} \right).$$

a and c as well as b and d have the same parity, and so L is a lattice point.

E8. *In the sequence* $1, 1, 2, 3, 5, 8, 3, 1, 4, \ldots$ *each term starting with the third is the sum of the two preceding terms. But addition is done mod 10. Prove that the sequence is purely periodic. What is the maximum possible length of the period?*

Solution. Any two consecutive terms of the sequence determine all succeeding terms and all preceding terms. Thus the sequence will become periodic if any pair (a, b) of successive terms repeats, and the first repeating pair will be $(1, 1)$.

Consider 101 successive terms $1, 1, 2, 3, 5, 8, 3, \ldots$. They form 100 pairs $(1, 1)$, $(1, 2)$, $(2, 3)$, $\ldots$. Since the pair $(0, 0)$ cannot occur, there are only 99 possible distinct pairs. Thus two pairs will repeat, and the period of the sequence is at most 99.

E9. *Consider the Fibonacci sequence defined by*

$$a_1 = a_2 = 1, \quad a_{n+1} = a_{n-1} + a_n, \ n > 1.$$

Prove that, for any n, there is a Fibonacci number ending with n zeros.

Solution. A term a_p ends in n zeros if it is divisible by 10^n, or, if $a_p \equiv 0 \bmod 10^n$. Thus we consider the Fibonacci sequence modulo 10^n, and we prove that the term 0 will occur in the sequence. Take $(10^{2n} + 1)$ terms of the sequence $a_1, a_2, \ldots \bmod 10^n$. They form 10^{2n} pairs $(a_1, a_2), (a_2, a_3), \ldots$, but the pair $(0, 0)$ cannot occur. Thus there are only $(10^{2n} - 1)$ possible pairs. Hence one pair will repeat. So the period length is at most $(10^{2n} - 1)$. As in **E8**, the first pair to repeat is $(1, 1)$.

$$\underbrace{1, 1, 2, 3, \ldots, a_p}_{\text{period}}, 1, 1.$$

Then $a_p = 1 - 1 = 0$. Thus, the term 0, will occur in the sequence. In fact, it is the last term of the period.

E10. *Suppose a is prime to* 2 *and* 5. *Prove that for any n there is a power of a ending with* $\underbrace{000\ldots01}_{n}$.

Solution. Consider the 10^n terms $a, a^2, a^3, \ldots, a^{10^n}$. Take their remainders modulo 10^n. The remainder 0 cannot occur since a and 10 are coprime. Thus there are

only $(10^n - 1)$ possible remainders

$$1, 2, 3, \ldots, 10^n - 1.$$

Hence, two of the terms a_i, $a_k (i < k)$ will have the same remainder, and so their difference will be divisible by 10^n:

$$10^n | a^k - a^i \iff 10^n | a^i (a^{k-i} - 1).$$

Since $\gcd(10^n, a^i) = 1$, we have $10^n | a^{k-i} - 1$ or $a^{k-i} - 1 = q * 10^n$, or $a^{k-i} = q * 10^n + 1$. Thus, a^{k-i} ends in $000 \ldots 01$ (n digits).

E11. *Inside a room of area 5, you place 9 rugs, each of area 1 and an arbitrary shape. Prove that there are two rugs which overlap by at least* $1/9$.

Suppose every pair of rugs overlaps by less than $1/9$. Place the rugs one by one on the floor. We note how much of the yet uncovered area each suceeding rug will cover. The first rug will cover area 1 or $9/9$. The 2nd, 3rd, . . ., 9th rug will cover area greater than $8/9, \ldots, 1/9$. Since $9/9 + \ldots + 1/9 = 5$, all nine rugs cover area greater than five. Contradiction!

Ramsey Numbers, Sum-Free Sets, and a Theorem of I. Schur

We consider four related competition problems:

E12. *Among six persons, there are always three who know each other or three who are complete strangers.*

This problem was proposed in 1947 in the Kürschak Competition and in 1953 in the Putnam Competition. Later, it was generalized by R.E. Greenwood and A.M. Gleason.

E13. *Each of* 17 *scientists corresponds with all the others. They correspond about only three topics and any two treat exactly one topic. Prove that there are at least three scientists, who correspond with each other about the same subject.*

E14. *In space, there are given* $p_n = \lfloor en! \rfloor + 1$ *points. Each pair of points is connected by a line, and each line is colored with one of n colors. Prove that there is at least one triangle with sides of the same color.*

E15. *An international society has members from six different countries. The list of members contains* 1978 *names, numbered* $1, 2, \ldots, 1978$. *Prove that there is at least one member whose number is the sum of the numbers of two members from his own country or twice as large as the number of one member from his own country* (IMO 1978).

The first two problems are special cases of the third with $n = 2$ and $n = 3$. One represents the persons by points. In the first problem, each pair of points is

In problem 43, we will prove

$$f(n) \geq \frac{3^n - 1}{2}.$$

Thus, we have

$$\frac{3^n + 3}{2} \leq R_n(3) \leq \lfloor en! \rfloor + 1,$$

that is,

$$3 \leq R_1(3) \leq 3, \quad 6 \leq R_2(3) \leq 6, \quad 15 \leq R_3(3) \leq 17, \quad 42 \leq R_4(3) \leq 66.$$

Because of Baumert's result, we know that even $44 \leq R_4(3) \leq 66$. The first three upper bounds are exact. The fourth is not. For about 20 years, it has been known that $R_4(3) \leq 65$, that is,

$$44 \leq R_4(3) \leq 65.$$

Problems

13. n persons meet in a room. Everyone shakes hands with everyone else. Prove that during the greeting ceremony there are always two persons who have shaken the same number of hands.

14. In a tournament with n players, everybody plays with everybody else exactly once. Prove that during the game there are always two players who have played the same number of games.

15. Twenty pairwise distinct positive integers are all < 70. Prove that among their pairwise differences there are four equal numbers.

16. Let $P_1, \ldots, P_9$ be nine lattice points in space, no three collinear. Prove that there is a lattice point L lying on some segment $P_iP_k, i \neq k$.

17. Fifty-one small insects are placed inside a square of side 1. Prove that at any moment there are at least three insects which can be covered by a single disk of radius 1/7.

18. Three hundred forty-two points are selected inside a cube with edge 7. Can you place a small cube with edge 1 inside the big cube such that the interior of the small cube does not contain one of the selected points?

19. Let n be a positive integer which is not divisible by 2 or 5. Prove that there is a multiple of n consisting entirely of ones.

20. S is a set of n positive integers. None of the elements of S is divisible by n. Prove that there exists a subset of S such that the sum of its elements is divisible by n.

21. Let S be a set of 25 points such that, in any 3-subset of S, there are at least two points with distance less than 1. Prove that there exists a 13-subset of S which can be covered by a disk of radius 1.

22. In any convex hexagon, there exists a diagonal which cuts off a triangle with area not more then one sixth of the hexagon.

23. If each diagonal of a convex hexagon cuts off a triangle not less than one sixth of its area, then all diagonals pass through one point, are divided by this point in the same ratio, and are parallel to the sides of the hexagon.

24. Among $n+1$ integers from $\{1, 2, \ldots, 2n\}$ there are two which are coprime.

25. From ten distinct two-digit numbers, one can always choose two disjoint nonempty subsets, so that their elements have the same sum (IMO 1972).

26. Let k be a positive integer and $n = 2^{k-1}$. Prove that, from $(2n-1)$ positive integers, one can select n integers, such that their sum is divisible by n.

27. Let $a_1, \cdots, a_n$ $(n \geq 5)$ be any sequence of positive integers. Prove that it is always possible to select a subsequence and add or subtract its elements such that the sum is a multiple of n^2.

28. In a room with $(m-1)n+1$ persons, there are m mutual strangers (in the room) or there is a person who is acquainted with n persons.

    Does the theorem remain valid, if one person leaves the room?

29. Of k positive integers with $a_1 < a_2 < \ldots < a_k \leq n$ and $k > \lfloor (n+1)/2 \rfloor$, there is at least one pair a_i, a_r such that $a_i + a_1 = a_r$.

30. Among $(ab+1)$ mice, there is either a sequence of $(a+1)$ mice of which one is descended from the preceding, or there are $(b+1)$ mice of which none descends from the other.

31. Let a, b, c, d be integers. Show that the product of the differences $b-a, c-a, d-a, c-b, d-b, d-c$ is divisible by 12.

32. One of the positive reals $a, 2a, \ldots, (n-1)a$ has at most distance $1/n$ from a positive integer.

33. Two of six points placed into a 3×4 rectangle will have distance $\leq \sqrt{5}$.

34. In any convex $2n$-gon, there is a diagonal not parallel to any side.

35. From 52 positive integers, we can select two such that their sum or difference is divisible by 100. Is the assertion also valid for 51 positive integers?

36. Each of ten segments is longer than 1 cm but shorter than 55 cm. Prove that you can select three sides of a triangle among the segments.

37. The vertices of a regular 7-gon are colored white or black. Prove that there are vertices of the same color, which form an isosceles triangle. What about a regular 8-gon? For what regular n-gons is the assertion valid?

38. Each of nine lines partitions a square into two quadrilaterals of areas in the ratio 2:3. Then at least three of the nine lines pass through one point.

39. Among nine persons, there are three who know each other or four persons who do not know each other. The number nine cannot be replaced by a smaller one.

40. $R(4,4) = 18$ yields the problem: Among 18 persons, there are four who know each other or four persons who do not know each other. For 17 persons this need not be true.

41. $R(3,6) = 18$ gives the problem: Among 18 persons, there are three who know each other, or six who do not know each other. Try to get an estimate of $R(6,3)$ from below and above.

80. A positive integer is placed on each square of an 8×8 board. You may select any 3×3 or 4×4 subboard and add 1 to each number on its squares. The goal is to get 64 multiples of 10. Can the goal always be reached?

81. The numbers from 1 to 81 are written on the squares of a 9×9 board. Prove that there exist two neighbors which differ by at least 6.

82. Each of m cards is labeled by one of the numbers $1, \ldots, m$. Prove that if the sum of the labels of any subset of the cards is not a multiple of $m+1$, then each card is labeled by the same number.

83. Two of 70 distinct positive integers ≤ 200 have differences of 4, 5, or 9.

84. A $20 \times 20 \times 20$ cube is built of $1 \times 2 \times 2$ bricks. Prove that one can pierce it by a needle without damaging one of the bricks.

Solutions

13. The solution is the same as for **E1**.

14. The same problem as problem 13. Handshakes are replaced by contests.

15. Denote the 20 integers a_1 to a_{20}. Then $0 < a_1 < \cdots < a_{20} < 70$. We want to prove that there is a k, so that $a_j - a_i = k$ has at least four solutions. Now

$$0 < (a_2 - a_1) + (a_3 - a_2) + \cdots + (a_{20} - a_{19}) = a_{20} - a_1 \leq 68.$$

We will prove that, among the differences $a_{i+1} - a_i$, $i = 1, \ldots, 19$, there will be four equal ones. Suppose there are at most three differences equal. Then

$$3 \cdot 1 + 3 \cdot 2 + 3 \cdot 3 + 3 \cdot 4 + 3 \cdot 5 + 3 \cdot 6 + 7 \leq 68,$$

that is, $70 \leq 68$. Contradiction!

16. Generalization of **E7**. Consider the three coordinates mod 2. There are $2^3 = 8$ possible binary 3-words. Since there are nine words altogether, at least two sequences must be identical. Thus there are two points (a, b, c) and (r, s, t) with integral midpoint $M = ((a+r)/2, (b+s)/2, (c+t)/2)$.

17. Subdivide the unit square into 25 small squares of side $1/5$. There will be three insects in one of these squares of side $1/5$ and diagonal $\sqrt{2}/5$. A circumcircle of this square has radius $\sqrt{2}/10 < 1/7$. If we circumscribe a concentric circle with radius $1/7$, it will cover this square completely.

18. Subdivide the cube into $7^3 = 343$ unit cubes. Since there are altogether only 342 points inside the large cube, the interior of at least one unit cube must remain empty.

19. Consider the n integers $1, 11, \ldots, 11\cdots1 \bmod n$. There are n possible remainders $0, 1, \ldots, n-1$. If 0 occurs, we are finished. If not, two of the numbers have the same remainder mod n. Their difference $111\cdots100\cdots0$ is divisible by n. Since n is not divisible by 2 or 5, we can strike the zeros at the end and get the number consisting of ones and divisible by n.

6

Number Theory

Number Theory requires extensive preparation, but the prerequisites are very finite. One usually can use the prerequisites 1 to 19 without proof. Here all variables stand for integers. The strategies are acquired by **massive problem solving**. At first the problems are far below a hard competitive level. But if you do most of the problems you are fit for any competition.

1. If $b = aq$ for some $q \in \mathbb{Z}$, then a **divides** b, and we write $a|b$.
2. **Fundamental Properties of the Divisibility Relation**

   I. $a \mid b,\ b \mid c \Rightarrow a \mid c$.

   II. $d \mid a,\ d \mid b \Rightarrow d \mid ax + by$. Especially $d \mid a + b,\ d \mid a - b$.

   III. If any two terms in $a + b = c$ are divisible by d, the third will also be divisible by d.
3. **Division with Remainder.** Every integer a is uniquely representable by the positive integer b in the form

   $$a = bq + r,\ 0 \leq r < b.$$

   q and r are called **quotient** and **remainder** upon division of a by b.
4. **GCD and Euclidean Algorithm.** Let a and b be nonnegative integers, not both 0. Their *greatest common divisor* and *least common multiple* will be denoted by $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$, respectively. Then

   $$\gcd(a, 1) = 1,\ \gcd(a, a) = a,\ \gcd(a, 0) = a,\ \gcd(a, b) = \gcd(b, a).$$

a and b will be called *relatively prime* or *coprime*, if $\gcd(a, b) = 1$. With

$$\gcd(a, b) = \gcd(b, a - b), \tag{4}$$

we can compute $\gcd(a, b)$ by subtracting repeatedly the smaller of the two numbers from the larger one. The following example shows this:

$$\gcd(48, 30) = \gcd(30, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 6) = 6.$$

The Euclidean algorithm is a speedup of this algorithm, and it is based on

$$a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r) = \gcd(b, a - bq). \tag{5}$$

Theorem. *The* $\gcd(a, b)$ *can be represented by a linear combination of* a *and* b *with integral coefficients, that is, there are* $x, y \in \mathbb{Z}$, *so that* $\gcd(a, b) = ax + by$.

Special case: *If* a *and* b *are coprime, then the equation* $ax + by = 1$ *has integral solutions.*

5. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$.

6. A positive integer is called a prime if it has exactly two divisors.

7. **Euclid's Lemma.** *If* p *is a prime,* $p \mid ab \Rightarrow p \mid a$ *or* $p \mid b$.

8. **Fundamental Theorem of Arithmetic.** *Every positive integer can be uniquely represented as a product of primes.*

9. There are infinitely many primes since $p \nmid (n! + 1)$ for any prime $p \leq n$.

10. $n! + 2, n! + 3, \ldots, n! + n$ are $(n - 1)$ consecutive composite integers.

11. The smallest prime factor of a nonprime n is $\leq \sqrt{n}$.

12. All primes $p > 3$ have the form $6n \pm 1$.

13. All pairwise prime triples of integers satisfying $x^2 + y^2 = z^2$ are given by

$$x = |u^2 - v^2|,\ y = 2uv,\ z = u^2 + v^2, \quad \gcd(u, v) = 1,\ u \neq v \bmod 2.$$

14. **Congruences.** $a \equiv b \bmod m \Leftrightarrow m \mid a - b \Leftrightarrow a - b = qm \Leftrightarrow a = b + qm \Leftrightarrow a$ and b have the same remainder upon division by m. Congruences can be added, subtracted, and multiplied.

Suppose $a \equiv b \bmod m$ and $c \equiv d \bmod m$. Then

$$a \pm c \equiv b \pm d \bmod m, \text{ and } ac \equiv bd \bmod m,$$

This has several consequences:

$$a \equiv b \bmod m \Rightarrow a^k \equiv b^k \bmod m \qquad \text{and}$$
$$a \equiv b \bmod m \Rightarrow f(a) \equiv f(b) \bmod m,$$

where

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in \mathbb{Z}.$$

In general we cannot divide, but we have the following **cancellation rule:**

$$\gcd(c, m) = 1,\ ca \equiv cb \bmod m \Rightarrow a \equiv b \bmod m.$$

15. **Fermat's Little Theorem (1640).** *Let a be a positive integer and p be a prime. Then*

$$a^p \equiv a \bmod p.$$

The cancellation rule tells us that we can divide by a if $\gcd(a, p) = 1$, getting

$$\gcd(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \bmod p.$$

16. Fermat's theorem is the first nontrivial theorem. So we give three proofs.

First proof by induction. The theorem is valid for $a = 1$, since $p|1^p - 1$. Suppose it is valid for some value of a, that is,

$$p|a^p - a. \tag{6}$$

We will also show that $p|(a+1)^p - (a+1)$. Indeed,

$$(a+1)^p - (a+1) = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} + 1 - (a+1) \tag{7}$$

or

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i}. \tag{8}$$

Now $p|\binom{p}{i}$ for $1 \le i \le p-1$. Also since $p|a^p - a$, we have $p|(a+1)^p - (a+1)$.

Second proof with congruences. We may multiply congruences, that is, from $c_i \equiv d_i \bmod p$ for $i = 1, \ldots, n$ follows

$$c_1 \cdot c_2 \cdot \cdots \cdot c_n \equiv d_1 \cdot d_2 \cdot \cdots \cdot c_n \bmod p. \tag{9}$$

Now, suppose that $\gcd(a, p) = 1$. We form the sequence

$$a, 2a, 3a, \ldots, (p-1)a. \tag{10}$$

No two of its terms are congruent mod p, since

$$i \cdot a \equiv k \cdot a \pmod{p} \Rightarrow i \equiv k \bmod p \Rightarrow i = k.$$

Hence, each of the numbers in (7) is congruent to exactly one of the numbers

$$1, 2, 3, \ldots p-1. \tag{11}$$

Applying (6) to (7) and (8) gives

$$a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv 1 \cdot 2 \cdot \cdots \cdot (p-1) \bmod p.$$

We may cancel with $(p-1)!$ since $(p-1)!$ and p are coprime. Thus,

$$a^{p-1} \equiv 1 \bmod p.$$

Third proof by combinatorics. We have pearls with a colors. From these we make necklaces with exactly p pearls. First, we make a string of pearls. There are a^p different strings. If we throw away the a one-colored strings $a^p - a$ strings will remain. We connect the ends of each string to get necklaces. We find that two strings that differ only by a cyclic permutation of its pearls result in indistinguishable necklaces. But there are p cyclic permutations of p pearls on a string. Hence the number of distinct necklaces is $(a^p - a)/p$. Because of its interpretation this is an integer. So

$$p \mid a^p - a.$$

17. The converse theorem is not valid. The smallest counterexample is

$$341 \mid 2^{341} - 2,$$

where 341=31 · 11 is not a prime. Indeed, we have

$$2^{341} - 2 = 2(2^{340} - 1) = 2((2^{10})^{34} - 1^{34}) = 2(2^{10} - 1)(\cdots) = 2 \cdot 3 \cdot 341 \cdot (\cdots).$$

18. **The Fermat–Euler Theorem.** Euler's ϕ-function is defined as follows:

$$\phi(m) = \text{number of elements from } \{1, 2, \ldots, m\} \text{ which are prime to } m.$$

$$\gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \bmod m.$$

19. **The Function Integer Part.** $\lfloor x \rfloor$ = greatest integer $\leq x$ = integer part of x. $x \bmod 1 = x - \lfloor x \rfloor = \{x\}$ = fractional part of x.

(a) $\lfloor x + y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor$. We have equality only if $x \bmod 1 + y \bmod 1 < 1$.

(b) $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$. This is an important special case of the formula $\lfloor (x+m)/n \rfloor = \lfloor (\lfloor x \rfloor + m)/n \rfloor$. Here m and n are integers.

(c) $\lfloor x + 1/2 \rfloor$ = the integer, which is nearest to x. More precisely, $n \leq x < n + 1/2 \Rightarrow \lfloor x + 1/2 \rfloor = n$, $n + 1/2 \leq x < n + 1 \Rightarrow \lfloor x + 1/2 \rfloor = n + 1$.

(d) The prime p divides $n!$ with multiplicity $e = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$.

Divisibility

The most useful formula in competitions is the fact that $a-b \mid a^n-b^n$ for all n, and $a+b \mid a^n+b^n$ for odd n. The second of these is a consequence of the first. Indeed, $a^n+b^n = a^n-(-b)^n$ for odd n, which is divisible by $a-(-b) = a+b$. In particular, a difference of two squares can always be factored. We have $a^2-b^2 = (a-b)(a+b)$. But a sum of two squares such as $x^2 + y^2$ can only be factored if $2xy$ is also a square. Here you must add and subtract $2xy$. The simplest example is the identity of Sophie Germain:

$$\begin{aligned} a^4 + 4b^4 &= a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2 \\ &= (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab). \end{aligned}$$

Some difficult Olympiad problems are based on this identity. For instance, in the 1978 Kürschak Competition, we find the following problem which few students solved.

E1. $n > 1 \Rightarrow n^4 + 4^n$ *is never a prime.*

If n is even, then $n^4 + 4^n$ is even and larger than 2. Thus it is not a prime. So we need to show the assertion only for odd n. But for odd $n = 2k + 1$, we can make the following transformation, getting Sophie Germain's identity:

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4,$$

which has the form $a^4 + 4b^4$.

This problem first appeared in the *Mathematics Magazine* 1950. It was proposed by A. Makowski, a leader of the Polish IMO-team.

Quite recently, the following problem was posed in a Russian Olympiad for 8th graders:

E2. *Is* $4^{545} + 545^4$ *a prime?*

Only few saw the solution, although all knew the identity of Sophie Germain and some competitions problems based on it. In fact, it is almost trivial to see that

$$4^{545} + 545^4 = 545^4 + 4 \cdot (4^{138})^4,$$

which is the left side of Sophie Germain's identity.

Now, consider the following recent competition problem from the former USSR:

E3. $n \in \mathbb{N}_0 \Rightarrow f(n) = 2^{2^n} + 2^{2^{n-1}} + 1$ *has at least n different prime factors.*

Here, we use the lemma $x^4+x^2+1 = (x^2+1)^2-x^2 = (x^2-x+1)(x^2+x+1)$. With $x = 2^{2^{n-1}}$, we get

$$2^{2^{n+1}} + 2^{2^n} + 1 = (2^{2^n} - 2^{2^{n-1}} + 1)(2^{2^n} + 2^{2^{n-1}} + 1).$$

Both right-hand side factors are prime to each other. If they had an odd divisor $q > 1$, then their difference $2 \cdot 2^{2^{n-1}} = 2^{2^{n-1}+1}$ would have the same factor. If we

already know that $2^{2^n} + 2^{2^{n-1}} + 1$ has at least n prime factors, then by induction $2^{2^{n+1}} + 2^{2^n} + 1$ has at least $n + 1$ prime factors.

Remarks. For $n > 4$, the number has at least $n + 1$ different prime factors, since

$$2^{2^4} - 2^{2^3} + 1 = 97 \cdot 673, \qquad 2^{2^4} + 2^{2^3} + 1 = 3 \cdot 7 \cdot 13 \cdot 241.$$

The product of the last two terms is $f(5)$. Thus $f(5)$ has six factors and $f(n)$ has at least $n + 1$ factors. The problem also shows that there are infinitely many primes.

We can solve the following competition problem with the same paradigm.

E4. *Find all primes of the form* $n^n + 1$, *which are less then* 10^{19}.

For $n = 1$ and $n = 2$, we get primes. An odd $n > 1$ yields an even $n^n + 1 > 2$. So n must be even, i.e., $n = 2^{2^t(2k+1)}$. Since

$$2^{2^t} + 1 | 2^{2^t(2k+1)} + 1,$$

the exponent of n cannot have an odd divisor. Thus $n = 2^{2^t}$, or

$$n^n = \left(2^{2^t}\right)^{2^{2^t}}.$$

For $t = 0,\ 1,\ 2$ we get $n^n + 1 = 5,\ 257,\ 16^{16} + 1 = 2^{64} + 1 > 16 \cdot 1000^6 + 1 > 10^{19}$. So there are no other primes besides 2, 5, and 257.

Let us consider some more competition problems.

E5. *Can the number A consisting of* 600 *sixes and some zeros be a square?*

Solution. If A is a square, then it ends in an even number of zeros. By canceling them we get a square $2B$, B consisting of 300 threes and some zeros, with B ending in 3. Since B is odd, $2B$ cannot be a square. It has only one factor 2.

E6. *The equation* $15x^2 - 7y^2 = 9$ *has no integer solutions.*

Solution. $15x^2 - 7y^2 = 9 \Rightarrow y = 3y_1 \Rightarrow 15x^2 - 63y_1^2 = 9 \Rightarrow 5x^2 - 21y_1^2 = 3 \Rightarrow x = 3x_1 \Rightarrow 45x_1^2 - 21y_1^2 = 3 \Rightarrow 15x_1^2 - 7y_1^2 = 1 \Rightarrow y_1^2 \equiv -1 \bmod 3$. This is a contradiction since $y_1^2 \equiv 0$ or $1 \bmod 3$.

E7. *A nine-digit number, in which every digit except zero occurs and which ends in 5, cannot be a square.*

Solution. Suppose there is such a nine-digit number D, so that $D = A^2$. $A = 10a + 5 \Rightarrow A^2 = 100a^2 + 100a + 25 = 100a(a + 1) + 25$. Consequences:

(a) The next to last digit is 2.

(b) The third digit from the right in D is one, which can be the final digit in $a(a + 1)$, that is 0, 2, or 6. See the table below:

a	0	1	2	3	4	5	6	7	8	9
$a(a+1) \bmod 10$	0	2	6	2	0	0	2	6	2	0

But 0 cannot occur, and 2 has already occurred. Hence, the third digit is a 6. From $D = 1000B + 625$ follows that $125|D$. Since $D = A^2$ we have $5^4|D$. Thus the fourth digit from the right in D must be 0 or 5. But 0 cannot occur, and 5 has already occurred.

E8. *There is no polynomial $f(x)$ with integer coefficients, so that $f(7) = 11$, $f(11) = 13$.*

Solution. Let $f(x) = \sum_{i=1}^{n} a_i x^i$, $a_i \in Z$. Then $a - b \mid f(a) - f(b)$, that is, $f(11) - f(7)$ is divisible by $11 - 7 = 4$. But $f(11) - f(7) = 2$. Contradiction!

E9. *For every positive integer p, we consider the equation*

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{p}. \tag{1}$$

We are looking for its solutions (x, y) in positive integers, with (x, y) and (y, x) being considered different. Show that if p is prime, then there are exactly three solutions. Otherwise, there are more then three solutions.

Solution. We have $x > p$, $y > p$. Hence, we set $x = p + q$, $y = p + r$ in (1) and get

$$\frac{1}{p+q} + \frac{1}{p+r} = \frac{1}{p} \Rightarrow p^2 = qr.$$

If p is a prime, the only solutions will be $(1, p^2)$, (p, p), $(p^2, 1)$, that is, for (x, y), there are the three pairs of solutions $(p+1, p(p+1))$, $(2p, 2p)$, $(p(p+1), p+1)$. If p is composite, then there will be obviously more solutions.

E10. *I start with any multidigit number a_1 and generate a sequence $a_1, a_2, a_3 \ldots$. Here a_{n+1} comes from a_n by attaching a digit $\neq 9$. Then I cannot avoid the fact that a_n is infinitely often a composite number.*

Solution. My strategy is to attach digits so as to get only finitely many composite digits. I cannot use 9 at all, and I can use 0, 2, 4, 6, 8, 5 only finitely often. Of the other digits 1, 3, 7, I may use 1 and 7 but finitely often because they change the remainder mod 3. Each time I attach 1 or 7 three times I get a number divisible by 3. So I am forced from a place upward to attach only threes. If at some moment I have a prime p, then after attaching at most p threes, again I get a multiple of p. I know that $\gcd(10, p) = 1$. Hence, among $1, 11, 111, \ldots, \underbrace{111\ldots11}_{p}$ there is at least one multiple of p.

Remark. If I could use 3 and 9, then I could not tell if I could get only primes from some n upwards. For instance, with $a_1 = 1$, I get the following primes of length 9: 1979339333, 1979339339.

E11. *In the sequence 1, 9, 7, 7, 4, 7, 5, 3, 9, 4, 1, . . ., every digit from the fifth on is the sum of the preceding digits mod 10. Does one of the following words ever occur in the sequence.*

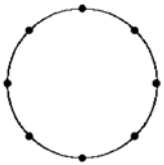
(a) 1234 (b) 3269 (c) 1977 (d) 0197?

Solution. We reduce all digits mod 2 and get 111101111011110.... To the words 1234 and 3269 correspond 1010 and 1001. Both patterns do not occur in the reduced sequence. For (c) we observe that there are only finitely many possible 4-words. Hence, some word $abcd$ will repeat for the first time:

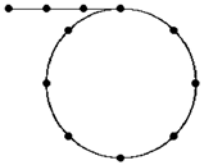
$$1977\ldots\underbrace{abcd\ldots}_{\text{period p}}abcd.$$

Four successive digits determine the next digit, but they also determine the preceding digit. Hence the sequence can be extended indefinitely in both directions. This extended sequence is purely periodic. In each period of length p lies one word 1977. This word is the first one to repeat, if you start with 1977.

This is an important observation. First, we show that the sequence must repeat. Then we show invertibility, which garantees a pure cycle (Fig. 6.1). For (d) we extend the sequence to the left by one term and get 0197.



(a) Pure cycle for invertible operation



(b) Noninvertible operation

Fig. 6.1. The two types of behavior of iterates $x \to f(x)$.

Remark. Computer experimentation shows that if we start with four odd digits, the period length will be $p = 1560 = 5 \cdot 312$. Starting with four even digits, we get period $p = 312$. If we start with at least one 5 and only zeros, the period will be $p = 5$.

E12. *The equation*

$$x^2 + y^2 + z^2 = 2xyz \tag{0}$$

has no integral solutions except $x = y = z = 0$. *Show this.*

First Solution. Let $(x, y, z) \neq (0, 0, 0)$ be an integral solution. If $2^k, k \geq 0$ is the highest power of 2, which divides x, y, z, then

$$x = 2^k x_1, \quad y = 2^k y_1, \quad z = 2^k z_1, \quad 2^{2k}x_1^2 + 2^{2k}y_1^2 + 2^{2k}z_1^2 = 2^{3k+1}x_1y_1z_1,$$
$$x_1^2 + y_1^2 + z_1^2 = 2^{k+1}x_1y_1z_1. \tag{1}$$

The right side of (1) is even. Hence, the left side is also even. All three terms on the left cannot be even because of the choice of k. Hence, exactly one term is even. Suppose $x_1 = 2x_2$, while y_1 and z_1 are odd. Hence,

$$y_1^2 + z_1^2 = 2^{k+2}x_2y_1z_1 - 4x_2^2 \equiv 0 \bmod 4.$$

Third Solution: By third roots of unity. Let ω be the third root of unity, i.e., $\omega^3 = 1$. Then $\omega^2 + \omega + 1 = 0$. Since $\omega^5 + \omega^4 + 1 = \omega^2 + \omega + 1$, we see that $\omega^2 + \omega + 1$ is a factor of the polynomial. So $n^2 + n + 1 | n^5 + n^4 + 1$. By long division of $n^5 + n^4 + 1$ by $n^2 + n + 1$, we get the second factor $n^3 - n + 1$.

The next two problems are among the most difficult ever proposed at any competition.

E14. *If $n \geq 3$, then 2^n can be represented in the form $2^n = 7x^2 + y^2$ with odd x, y.*

Solution. This is a very interesting and exceedingly tough problem which was proposed at the MMO 1985. It is due to Euler, who never published it. It was taken from his notebook by the proposers. No participant could solve it. It became a subject of controversy among mathematicians. A prominent number theorist wrote in the Russian journal *Mathematics in School* that it was well beyond the students and required algebraic number theory. I proposed it to our Olympiad team. One student Eric Müller gave a solution after some time, which I did not understand. I asked him to write it down, so that I could study it in detail. It took him some time to write it down, since he solved not only this problem but along with it also over a thousand other problems on 434 pages, all the problems posed by the trainers in three years. I found the solution of our problem. It was correct.

Figure 6.2 shows the first 8 solutions, which can easily be found by guessing. Now study this table closely. Before reading on, try to find the pattern behind the table.

n	3	4	5	6	7	8	9	10
x	1	1	1	3	1	5	7	3
y	1	3	5	1	11	9	13	31

Fig. 6.2

Our hypothesis is that one column somehow determines the next one. How can I get the next pair x_1, y_1 from the current x, y? This conjecture is supported by similar equations, for instance the Pell–Fermat equation where we get from one pair (x, y) to the next by a linear transformation. Let us start with x_1. How can I get from (x, y) to x_1? We get x_1 from the first pair (1,1) by taking the arithmetic mean. From the second pair (1,3), the mean 2 is not an odd integer. So let us take the difference $|x - y|/2 = 1$. Again we are successful. Some more trials convince us that we should take $(x + y)/2$ if that number is odd. If that number is even, we should take $|x - y|/2$. After guessing the pattern behind x, we will try to guess the pattern behind y. There is a 7 before x^2 in the equation. So we could try $(7x + y)/2$ and $|7x - y|/2$. The pattern seems to hold for the table above.

To support our conjecture, we observe that exactly one of

$$\frac{x+y}{2} \quad \text{or} \quad \frac{|x-y|}{2} \quad \text{is odd since} \quad \frac{x+y}{2} + \frac{|x-y|}{2} = \max(x, y).$$

Exactly one of

$$\frac{7x+y}{2} \quad \text{or} \quad \frac{|7x-y|}{2} \quad \text{is odd since} \quad \frac{7x+y}{2} + \frac{|7x-y|}{2} = \max(7x, y).$$

A counting argument similar to the one in the preceding example shows, that exactly the triangular numbers are omitted.

Problems

1. $a-c \mid ab+cd \Rightarrow a-c \mid ad+bc$.
2. $a \equiv b \equiv 1 \bmod 2 \Rightarrow a^2+b^2$ not a square.
3. (a) $6 \mid n^3+5n$. (b) $30 \mid n^5-n$. (c) For which n is $120 \mid n^5-n$?
4. (a) $3 \mid a,\ 3 \mid b \Leftrightarrow 3 \mid a^2+b^2$. (b) $7 \mid a,\ 7 \mid b \Leftrightarrow 7 \mid a^2+b^2$. (c) $21 \mid a^2+b^2 \Rightarrow 441 \mid a^2+b^2$.
5. $n \equiv 1 \bmod 2 \Rightarrow n^2 \equiv 1 \bmod 8 \Leftrightarrow 8 \mid n^2-1$.
6. $6 \mid a+b+c \Leftrightarrow 6 \mid a^3+b^3+c^3$.
7. Derive divisibility criteria for 9 and 11.
8. Let $A = 3^{105}+4^{105}$. Show that $7 \mid A$. Find $A \bmod 11$ and $A \bmod 13$.
9. Show that $3n-1,\ 5n \pm 2,\ 7n-1,\ 7n-2,\ 7n+3$ are not squares.
10. If n is not a prime, then 2^n-1 is not a prime.
11. If n has an odd divisor, then 2^n+1 is not prime.
12. $641 \mid 2^{32}+1$. No calculator allowed!
13. (a) $n>2 \Rightarrow 2^n-1$ is not a power of 3. (b) $n>3 \Rightarrow 2^n+1$ is not a power of 3.
14. A number with 3^n equal digits is divisible by 3^n.
15. Find all primes p, q, so that $p^2-2q^2=1$.
16. If $2n+1$ and $3n+1$ are squares, then $5n+3$ is not a prime.
17. If p is prime, then $p^2 \equiv 1 \bmod 24$.
18. $9 \mid a^2+b^2+c^2 \Rightarrow 9 \mid a^2-b^2$ or $9 \mid b^2-c^2$ or $9 \mid a^2-c^2$.
19. $n \equiv 0 \bmod 2 \Rightarrow 323 \mid 20^n+16^n-3^n-1$.
20. $121 \nmid n^2+3n+5$.
21. If p and p^2+2 are primes, then p^3+2 is also prime.
22. $2^n \nmid n!$.
23. How many zeros are at the end of 1000!?
24. Among five integers, there are always three with sum divisible by 3.
25. Using $x^2+y^2+z^2 \not\equiv 7 \bmod 8$, find numbers which are not sums of 3 squares.
26. The four-digit number $aabb$ is a square. Find it.
27. Can the digital sum of a square be (a) 3, (b) 1977?
28. $1000\cdots001$ with 1961 zeros is composite (not prime).
29. Let $Q(n)$ be the digital sum of n. Show that $Q(n)=Q(2n) \Rightarrow 9 \mid n$.
30. The sum of squares of five successive positive integers is not a square.
31. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, p_i be distinct primes. Then n has $(a_1+1)\cdots(a_n+1)$ divisors.

32. Among $n+1$ positive integers$\leq 2n$, there are two which are coprime.
33. Among $n+1$ positive integers $\leq 2n$, there are $p,\ q$ such that $p|q$.
34. $(12n+1)/(30n+2)$ and $(21n+4)/(14n+3)$ are irreducible.
35. Show that $\gcd(2n+3, n+7) = 1$ for $n \not\equiv 4 \bmod 11$, and $= 11$ for $n \equiv 4 \bmod 11$.
36. $\gcd(n, n+1) = 1$, $\gcd(2n-1, 2n+1) = 1$, $\gcd(2n, 2n+2) = 2$, $\gcd(a, b) = \gcd(a, a+b)$, $\gcd(5a+3b, 13a+8b) = \gcd(a, b)$.
37. (a) $\gcd(2^a-1, 2^b-1) = 2^{\gcd(a,b)}-1$. (b) $n = ab \Rightarrow 2^a-1 \mid 2^n-1$.
38. (a) $\gcd(6, n) = 1 \Rightarrow 24 \mid n^2-1$. (b) p, q primes > 3 implies $24 \mid p^2-q^2$.
39. (a) $p,\ p+10,\ p+14$ are primes, (b) $p,\ p+4,\ p+14$ are primes. Find p.
40. (a) $p, 2p+1, 4p+1$ are primes (b) p and $8p^2+1$ are primes. Find p.
41. $13 \mid a+4b \Rightarrow 13 \mid 10a+b$. $19 \mid 3x+7y \Rightarrow 19 \mid 43x+75y$. $17 \mid 3a+2b \Rightarrow 17 \mid 10a+b$.
42. If $p > 5$ is a prime, then $p^2 \equiv 1$ or $p^2 \equiv 19 \bmod 30$.
43. $x^2+y^2 = x^2y^2$ has no integral solutions besides $x = y = 0$.
44. $120 \mid n^5-5n^3+4n$. $9 \mid 4^n+15n-1$.
45. Let $m > 1$. Then exactly one of the integers $a, a+1, \ldots, a+m-1$ is divisible by m.
46. Find all integral solutions of $x^2+y^2+z^2 = x^2y^2$.
47. Find the integral solutions of (a) $x+y = xy$ (b) $x^2-y^2 = 2xyz$.
48. Find all integral solutions of (a) $x^2-3y^2 = 17$, (b) $2xy+3y^2 = 24$.
49. Find the integral solutions of $x^2+xy+y^2 = x^2y^2$ and $x^2+y^2+z^2+u^2 = 2xyzu$.
50. Find all integral solutions of $x+y = x^2-xy+y^2$.
51. Let $p = p_1p_2\cdots p_n, n > 1$ be the product of the first n primes. Show that $p-1$ and $p+1$ are not squares.
52. $a_1a_2+a_2a_3+\cdots+a_{n-1}a_n+a_na_1 = 0$ with $a_i \in \{1, -1\}$. Show that $4 \mid n$.
53. Three brothers inherit n gold pieces weighing $1, 2, \ldots, n$. For what n can they be split into three equal heaps?
54. Find the smallest positive integer n, so that $999999 \cdot n = 111\cdots11$.
55. Find the smallest positive integer with the property that, if you move the first digit to the end, the new number is 1.5 times larger than the old one.
56. With the digits 1 to 9, construct two numbers with (a) maximal (b) minimal product.
57. Which smallest positive integer becomes 57 times smaller by striking its first digit.
58. If $ab = cd$, then $a^2+b^2+c^2+d^2$ is composite. Generalize (BWM 1970/71).
59. Find the four-digit number $abcd$ such that $4 \cdot abcd = dcba$.
60. Find the five-digit number $abcde$ such that $4 \cdot abcde = edcba$.
61. If $n > 2$, p a prime, and $2n/3 < p < n$, then $p \not\mid \binom{2n}{n}$.
62. The sequence $a_n = \sqrt{24n+1}, n \in \mathbb{N}$, contains all primes except 2 and 3.

156. Several different positive integers lie strictly between two successive squares. Prove that their pairwise products are also different (AUO 1983).

157. Find the integral solutions of $19x^3 - 84y^2 = 1984$ (MMO 1984).

158. Start with some positive integers. In one step you may take any two numbers a, b and replace them by $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$. Prove that, eventually, the numbers will stop changing.

159. The powers 2^n and 5^n start with the same digit d. What is this digit?

160. If $n = a^2 + b^2 + c^2$, then $n^2 = x^2 + y^2 + z^2$, where $a, b, c, x, y, z \in \mathbb{N}$.

161. For infinitely many composite n, we have $n | 3^{n-1} - 2^{n-1}$ (MMO 1995).

162. The equation $x^2 + y^2 + z^2 = x^3 + y^3 + z^3$ has infinitely many integer solutions (MMO 1994).

163. Prove that there exist infinitely many positive integers n such that 2^n ends with n, i.e., $2^n = \cdots n$ (MMO 1978).

164. There are white and black balls in an urn. If you draw two balls at random, the probability is $1/2$ to get a mixed couple. What can you conclude about the contents of the urn?

165. A multidigit number contains the digit 0. If you strike it the number becomes 9 times smaller. At which position is this 0 located? Find all such numbers.

166. If you are condemned to die in Sikinia, you are put into Death Row until the last day of the year. Then all prisoners from Death Row are arranged in a circle and numbered $1, 2, \ldots, n$. Starting with #2 every second one is shot until only one remains who is immediately set free. How do you find the place of the sole survivor?

167. (a) Find a number divisible by 2 and 9 which has exactly 14 divisors.

(b) Replacing 14 by 15 there will be several solutions, replacing 14 by 17 there will be none.

168. The positive integer k has the property: for all $m \in \mathbb{N} : k \mid m \Rightarrow k \mid m_r$. Here m and m_r are mutual reflections like 1234 and 4321. Show that $k \mid 99$.

169. Let p and q be fixed positive integers. The set $\mathbb{Z}$ of integers is to be partitioned into three subsets A, B, C such that, for every $n \in \mathbb{Z}$, the three integers n, $n + p$, and $n + q$ belong to different subsets. What relationships must p and q satisfy?

170. A positive integer is the product of n distinct primes. In how many ways can it be represented as the difference of two squares?

Solutions

1. $(ab + cd) - (ad + bc) = a(b - d) - c(b - d) = (a - c)(b - d)$.

2. An even square is divisible by 4.

3. (a) $n^3 + 5n = n^3 - n + 6n = (n - 1)n(n + 1) + 6n$. (b) The three first factors of $n^5 - n = n(n - 1)(n + 1)(n^2 + 1)$ are successive integers. Divisibility by 5 follows from Fermat's theorem. (c) If n is odd, $n^5 - n$ is divisible by 120.

7

Inequalities

Means

Let x be a real number. The most basic inequalities are

$$x^2 \geq 0, \tag{1}$$

$$\sum_{i=1}^{n} x_i^2 \geq 0. \tag{2}$$

We have equality only if $x = 0$ in (1) or $x_i = 0$ for all i in (2). One strategy for proving inequalities is to transform them into the form (1) or (2). This is usually a long road. So we derive some consequences equivalent to (1). With $x = a - b$, $a > 0, b > 0$, we get the following equivalent inequalities:

$$a^2 + b^2 \geq 2ab \Leftrightarrow 2(a^2 + b^2) \geq (a + b)^2 \Leftrightarrow \frac{a}{b} + \frac{b}{a} \geq 2$$

$$\Leftrightarrow x + \frac{1}{x} \geq 2,\ x > 0 \Leftrightarrow \frac{a + b}{2} \leq \sqrt{\frac{a^2 + b^2}{2}}.$$

Replacing a, b by $\sqrt{a}$, $\sqrt{b}$, we get

$$a + b \geq 2\sqrt{ab} \Leftrightarrow \frac{a + b}{2} \geq \sqrt{ab} \Leftrightarrow \sqrt{ab} \geq \frac{2ab}{a + b}.$$

In particular, we have the inequality chain

$$\min(a, b) \leq \frac{2ab}{a + b} \leq \sqrt{ab} \leq \frac{a + b}{2} \leq \sqrt{\frac{a^2 + b^2}{2}} \leq \max(a, b).$$

This is the *harmonic-geometric-arithmetic-quadratic mean inequality,* or the HM-GM-AM-QM inequality. By repeated use of the inequalities above, we can already prove a huge number of other inequalities. Every contestant in any competition must be able to apply these inequalities in any situation that may arise. Here are a few very simple examples.

E1. $\frac{x^2+2}{\sqrt{x^2+1}} \geq 2$ for all x. This can be transformed as follows.

$$\frac{x^2+2}{\sqrt{x^2+1}} = \frac{x^2+1}{\sqrt{x^2+1}} + \frac{1}{\sqrt{x^2+1}} = \sqrt{x^2+1} + \frac{1}{\sqrt{x^2+1}} \geq 2.$$

E2. For $a,\ b,\ c,\ \geq 0$, we have $(a+b)(b+c)(c+a) \geq 8abc$. Indeed,

$$\frac{a+b}{2} \cdot \frac{b+c}{2} \cdot \frac{c+a}{2} \geq \sqrt{ab} \cdot \sqrt{bc} \cdot \sqrt{ca} = abc.$$

E3. If $a_i > 0$ for $i = 1, \ldots, n$ and $a_1 a_2 \cdots a_n = 1$, then

$$(1+a_1)(1+a_2)\cdots(1+a_n) \geq 2^n.$$

Dividing by 2^n we get

$$\frac{1+a_1}{2} \cdot \frac{1+a_2}{2} \cdots \frac{1+a_n}{2} \geq \sqrt{a_1}\sqrt{a_2}\cdots\sqrt{a_n} = \sqrt{a_1 a_2 \cdots a_n} = 1.$$

E4. For $a,\ b,\ c,\ d \geq 0$, we have $\sqrt{(a+c)(b+d)} \geq \sqrt{ab} + \sqrt{cd}$. Squaring and simplifying, we get $ad + bc \geq 2\sqrt{abcd}$, which is $x + y \geq 2\sqrt{xy}$.

E5. *Show that, for real $a,\ b,\ c$,*

$$a^2 + b^2 + c^2 \geq ab + bc + ca. \tag{3}$$

First proof. Multiplying by 2, we reduce (3) to (2):

$$2a^2 + 2b^2 + 2c^2 - 2ab - 2bc - 2ca \geq 0 \Leftrightarrow (a-b)^2 + (b-c)^2 + (c-a)^2 \geq 0.$$

Second proof. We have $a^2 + b^2 \geq 2ab,\ b^2 + c^2 \geq 2bc,\ c^2 + a^2 \geq 2ca$. Addition and division by 2 yields (3).

Third proof. *Introduce ordering or assume that some element is extremal.* Since the inequality is *symmetric* in $a,\ b,\ c$, assume $a \geq b \geq c$. Then

$$\begin{aligned} a^2 + b^2 + c^2 \geq ab + bc + ca &\Leftrightarrow a(a-b) + b(b-c) - c(a-c) \\ &\geq 0 \Leftrightarrow a(a-b) + b(b-c) \\ -c(a-b+b-c) \geq 0 &\Leftrightarrow a(a-b) + b(b-c) - c(a-b) - c(b-c) \\ &\geq 0 \Leftrightarrow (a-c)(a-b) + (b-c)^2 \geq 0. \end{aligned}$$

The last inequality is obviously correct. Here it is enough to assume that a is the maximal or minimal element. *Note also the replacement of* $-c(a-c)$ *by* $-c(a-b+b-c)$. *This idea has many applications.*

Fourth proof. Let $f(a,b,c) = a^2+b^2+c^2-ab-bc-ca$. Then we have $f(ta,tb,tc) = t^2 f(a,b,c)$. Hence, f is homogeneous of degree two. For $t \neq 0$, we have $f(a,b,c) \geq 0 \Leftrightarrow f(ta,tb,tc) \geq 0$. Therefore, we may make various *normalizations*. For example, we may set $a=1$, $b=1+x$, $c=1+y$ and get $x^2+y^2-xy = (x-y/2)^2+3y^2/4 \geq 0$. More proofs will be given later.

E6. We start with the classic factorization

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca). \tag{4}$$

Because of (3), for nonnegative a, b, c, we have

$$a^3+b^3+c^3 \geq 3abc \Leftrightarrow a+b+c \geq 3\sqrt[3]{abc} \Leftrightarrow \frac{a+b+c}{3} \geq \sqrt[3]{abc}. \tag{5}$$

This is the AM-GM inequality for three nonnegative reals.

Generally, for n positive numbers a_i, we have the following inequalities:

$$\min(a_i) \leq \frac{n}{\frac{1}{a_1}+\cdots+\frac{1}{a_n}} \leq \sqrt[n]{a_1\cdots a_n} \leq \frac{a_1+\cdots+a_n}{n} \leq \sqrt{\frac{a_1^2+\cdots+a_n^2}{n}} \leq \max(a_i).$$

The equality sign is valid only if $a_1 = \cdots = a_n$. We will prove these later. At the IMO, they need never be proved, just applied.

E7. Let us apply (5) to Nesbitt's inequality (England 1903):

$$\frac{a}{b+c}+\frac{b}{a+c}+\frac{c}{a+b} \geq \frac{3}{2}. \tag{6}$$

It has many instructive proofs and generalizations and is a favorite Olympiad problem. Let us transform the left-hand side $f(a,b,c)$ as follows.

$$\begin{aligned} &\tfrac{a+b+c}{b+c}+\tfrac{a+b+c}{a+c}+\tfrac{a+b+c}{a+b}-3 \\ &\qquad = (a+b+c)\left(\tfrac{1}{a+b}+\tfrac{1}{b+c}+\tfrac{1}{a+c}\right)-3, \\ &\tfrac{1}{2}\left[(a+b)+(b+c)+(c+a)\right]\left(\tfrac{1}{a+b}+\tfrac{1}{b+c}+\tfrac{1}{a+c}\right)-3. \end{aligned} \tag{7}$$

First proof. In (7), we set $a+b=x$, $b+c=y$, $a+c=z$ and get

$$\begin{aligned} 2f(a,b,c) &= (x+y+z)\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)-6 \\ &= \underbrace{\frac{x}{y}+\frac{y}{x}}_{\geq 2}+\underbrace{\frac{x}{z}+\frac{z}{x}}_{\geq 2}+\underbrace{\frac{y}{z}+\frac{z}{y}}_{\geq 2}-3 \geq 3. \end{aligned}$$

We have equality for $x = y = z$, that is, $a = b = c$.

Second proof. The AM-HM Inequality can be transformed as follows:

$$\frac{u+v+w}{3} \geq \frac{3}{\frac{1}{u}+\frac{1}{v}+\frac{1}{w}} \Leftrightarrow (u+v+w)(\frac{1}{u}+\frac{1}{v}+\frac{1}{w}) \geq 9.$$

From (7), we get

$$f(a,b,c) \geq \frac{1}{2} \cdot 9 - 3 = \frac{3}{2}.$$

Let us prove the product form of the AM-HM inequality

$$(a_1 + \cdots + a_n)\left(\frac{1}{a_1} + \cdots \frac{1}{a_n}\right) \geq n^2.$$

Multiplying the LHS, we get n times 1 and $\binom{n}{2}$ pairs $x_i/x_j + x_j/x_i$, each pair being at least 2. Hence the LHS is at least $n + 2\binom{n}{2} = n^2$.

Third proof. We apply the inequality $u + v + w \geq 3\sqrt[3]{uvw}$ to both parentheses of (7) and get

$$f(a,b,c) \geq \frac{1}{2} \cdot 3\sqrt[3]{(a+b)(b+c)(c+a)} \cdot 3\sqrt[3]{\frac{1}{(a+b)(b+c)(c+a)}} - 3 = \frac{3}{2}.$$

Fourth proof. We have $f(a,b,c) = f(ta,tb,tc)$ for $t \neq 0$, that is, f is *homogeneous* in a, b, c of degree 0. We may normalize to $a + b + c = 1$. Then, from the AM-HM inequality, we get

$$f(a,b,c) = \frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} - 3 \geq \frac{9}{2} - 3 = \frac{3}{2}.$$

E8. Inequalities for the sides a, b, c of a triangle are very popular. In this case, the *Triangle Inequality* plays a central role. During the proof you must use the triangle inequality or else the inequality is valid for all triples (a,b,c) of positive reals. That includes all triangles, of course.

The triangle inequality occurs in four equivalent forms:

I. $a + b > c, \quad b + c > a, \quad c + a > b.$

II. $a > |b - c|, \quad b > |a - c|, \quad c > |a - b|.$

III. $(a + b - c)(b + c - a)(c + a - b) > 0.$

IV. $a = y + z, \quad b = z + x, \quad c = x + y$, where x, y, z are positive.

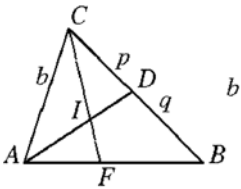
If we know that $c = \max(a, b, c)$, then $a + b > c$ alone suffices. The other two inequalities in I are automatically satisfied. We prove the equivalence of I and III. If I is valid, then III is also valid. Suppose III is valid. Then all three factors are positive, which is I, or exactly two factors are negative. Suppose the first and second factor are negative. Adding $a + b - c < 0$ and $b + c - a < 0$, we get $2b < 0$, which is a contradiction.

E9. *In a triangle ABC, the bisectors AD, BE, and CF meet at the point I. Show that*

$$\frac{1}{4} < \frac{IA}{AD} \cdot \frac{IB}{BE} \cdot \frac{IC}{CF} \leq \frac{8}{27}. \tag{1}$$

Solution. This was the first problem of IMO 1991. To avoid trigonometry, we use the following simple geometric theorem (Fig. 7.1):

A bisector of a triangle divides the opposite side in the ratio of the other two sides.



$b : c = p : q.$

Fig. 7.1

Hence, $p = CD = (ab)/(b + c)$, $q = DB = (ac)/(b + c)$. Thus, we have

$$\frac{AI}{ID} = b : p = \frac{b + c}{a}, \quad \frac{AI}{AD} = \frac{AI}{AI + ID} = \frac{b + c}{a + b + c}.$$

Similarly,

$$\frac{BI}{BE} = \frac{a + c}{a + b + c}, \quad \frac{CI}{CF} = \frac{a + b}{a + b + c}.$$

Applying the GM-AM inequality to the numerator,we get $f(a, b, c) =$

$$\frac{AI}{AD} \cdot \frac{BI}{BE} \cdot \frac{CI}{CF} = \frac{(a + b)(b + c)(c + a)}{(a + b + c)^3} \leq \frac{8}{(a + b + c)^3} \left(\frac{a + b + c}{3} \right)^3,$$

which is $8/27$. This is the right side of the inequality chain. To prove the left side, we use the triangle inequality

$$(a + b - c)(a + c - b)(b + c - a) > 0. \tag{2}$$

For a more economical evaluation, we introduce the elementary symmetric functions

$$u = a + b + c, \quad v = ab + bc + ca, \quad w = abc. \tag{3}$$

E19. *Prove the inequality* $a^4 + b^4 + c^4 \geq a^2bc + b^2ca + c^2ab$.

We use an extension of the scalar product to three sequences:

$$\begin{bmatrix} a^2 & b^2 & c^2 \\ a & b & c \\ a & b & c \end{bmatrix} \geq \begin{bmatrix} a^2 & b^2 & c^2 \\ b & c & a \\ c & a & b \end{bmatrix}.$$

In the first matrix, the three sequences are sorted the same way, in the second, not.

Recently, the following inequality was posed in the *Mathematics Magazine*.

E20. *Let* $x_1, \ldots, x_n$ *be positive real numbers. Show that*

$$x_1^{n+1} + x_2^{n+1} + \cdots + x_n^{n+1} \geq x_1x_2 \ldots x_n\,(x_1 + x_2 + \cdots + x_n).$$

The proof is immediate. Rewrite the preceding inequality as follows:

$$\begin{bmatrix} x_1 & \cdots & x_n \\ x_1 & \cdots & x_n \\ \cdots & \cdots & \cdots \\ x_1 & \cdots & x_n \end{bmatrix} \geq \begin{bmatrix} x_1 & \cdots & x_n \\ x_2 & \cdots & x_1 \\ \cdots & \cdots & \cdots \\ x_1 & \cdots & x_n \end{bmatrix}.$$

E21. Triangular Inequalities. In this section we discuss inequalities for a triangle. Our students acquire all their knowledge about the geometry and trigonometry of the triangle from **E21/22**.

We will denote the sides of a triangle by a, b, c. The opposite angles will be denoted by α, β, γ. The area will be denoted by A, the inradius by r and the circumradius by R. Two indispensable theorems are *the Cosine Law*:

$$c^2 = a^2 + b^2 - 2ab\cos\gamma \quad \text{(and cyclic permutations)}.$$

and *the Sine Law:*

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R.$$

The area of the triangle is

$$A = \frac{1}{2}ab\sin\gamma = \frac{1}{2}bc\sin\alpha = \frac{1}{2}ac\sin\beta.$$

We start with an inequality, which we will prove and sharpen in many ways.

Prove that, for any triangle with sides a, b, c *and area* A,

$$a^2 + b^2 + c^2 \geq 4\sqrt{3}A \quad \text{(IMO 1961)}.$$

The inequality is due to Weitzenböck, *Math. Z.* 5, 137–146, (1919).

Main idea: We conjecture that we have equality exactly for the equilateral triangle. This conjecture is the guide to most of our proofs.

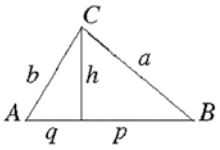


Fig. 7.3

First proof. An equilateral triangle with side c has altitude $\frac{c}{2}\sqrt{3}$. Any triangle with side c will have an altitude perpendicular to c of length $\frac{c}{2}\sqrt{3}+y$. It splits c into parts $\frac{c}{2}-x$ and $\frac{c}{2}+x$. Here $x,\ y$ are the deviations from an equilateral triangle. Then we have (see Fig. 7.3)

$$\begin{aligned} a^2+b^2+c^2-4\sqrt{3}A &= \left(\frac{c}{2}-x\right)^2+\left(\frac{c}{2}+x\right)^2+2\left(y+\frac{c}{2}\sqrt{3}\right)^2+c^2-2\sqrt{3}c\left(y+\frac{c}{2}\sqrt{3}\right) \\ &= 2x^2+2y^2\geq 0. \end{aligned}$$

We have equality iff $x=y=0$, i.e., for the equilateral triangle.

Second proof. This is a more geometric version of the preceding solution. Let $a\leq b\leq c$. We erect the equilateral triangle ABC' on AB and introduce $p=|CC'|$ as the deviation from an equilateral triangle. The Cosine Law yields

$$\begin{aligned} p^2 &= a^2+c^2-2ac\cos(\beta-60^\circ) \\ &= a^2+c^2-2ac\left(\cos\beta\cos 60^\circ+\sin\beta\sin 60^\circ\right), \\ p^2 &= a^2+c^2-ac\cos\beta-\sqrt{3}ac\sin\beta \\ &= a^2+b^2-2\sqrt{3}A-\frac{1}{2}\underbrace{(2ac\cos\beta)}_{a^2+c^2-b^2}, \\ p^2 &= \frac{a^2+b^2+c^2}{2}-2\sqrt{3}A=\frac{a^2+b^2+c^2-4\sqrt{3}A}{2}\geq 0, \end{aligned}$$

since the square p^2 is not negative. We have equality exactly if $p=0$, that is, $a=b=c$.

Third proof. This is a proof by contradiction. We assume $4A\sqrt{3}>a^2+b^2+c^2$ and by equivalence transformations we get

$$4A\sqrt{3}>a^2+b^2+c^2 \Leftrightarrow 2bc\sin\alpha>\frac{1}{\sqrt{3}}\left(a^2+b^2+c^2\right).$$

Now we use the Cosine Law $2bc\cos\alpha=b^2+c^2-a^2$. Square and add the last two relations. We get the contradiction

$$a^2b^2+b^2c^2+c^2a^2>a^4+b^4+c^4 \Leftrightarrow \left(a^2-b^2\right)^2+\left(b^2-c^2\right)^2+\left(c^2-a^2\right)^2<0.$$

Fourth proof. Using Heron's formula and the AM-GM inequality, we get

$$\begin{aligned} 16A^2 &= (a+b+c)(-a+b+c)(a-b+c)(a+b-c) \\ &\le (a+b+c)\left(\frac{a+b+c}{3}\right)^3, \\ 4A &\le \frac{(a+b+c)^2}{3\sqrt{3}} = \sqrt{3}\left(\frac{a+b+c}{3}\right)^2 \le \sqrt{3}\frac{a^2+b^2+c^2}{3}, \end{aligned}$$

or $a^2+b^2+c^2 \ge 4A\sqrt{3}$. We have equality exactly for $a=b=c$.

Fifth proof.

$$a^2+b^2+c^2 \ge ab+bc+ca = 2A\left(\frac{1}{\sin\alpha}+\frac{1}{\sin\beta}+\frac{1}{\sin\gamma}\right).$$

Now we use the fact that $f(x) = 1/\sin x$ is convex. Convexity implies that

$$f(\alpha)+f(\beta)+f(\gamma) \ge 3f(\frac{\alpha+\beta+\gamma}{3}) = 3f(60^\circ) = \frac{3}{\sin 60^\circ} = 2\sqrt{3},$$

that is,

$$a^2+b^2+c^2 \ge 4A\sqrt{3}.$$

Sixth proof. We prove a slight generalization.

$$\begin{aligned} 2a^2+2b^2+2c^2 &= (a-b)^2+(b-c)^2+(c-a)^2+2ab+2bc+2ca \\ &= \underbrace{(a-b)^2+(b-c)^2+(c-a)^2}_{Q} \\ &\quad + 4A\underbrace{\left(\frac{1}{\sin\alpha}+\frac{1}{\sin\beta}+\frac{1}{\sin\gamma}\right)}_{\ge 2\sqrt{3}}. \end{aligned}$$

We get a generalization

$$a^2+b^2+c^2 \ge \frac{Q}{2}+4A\sqrt{3}.$$

Seventh proof. We replace a^2 in $a^2+b^2+c^2$ by $b^2+c^2-2bc\cos\alpha$ and get

$$\begin{aligned} a^2+b^2+c^2-4A\sqrt{3} &= 2(b^2+c^2)-2bc\cos\alpha-2bc\sqrt{3}\sin\alpha = 2(b^2+c^2) \\ &\quad -4bc\left(\frac{1}{2}\cos\alpha+\frac{\sqrt{3}}{2}\sin\alpha\right) \\ &= 2[b^2+c^2-4bc\cos(60^\circ-\alpha)] \\ &\ge 2(b^2+c^2)-4bc = 2(b-c)^2. \end{aligned}$$

We have equality exactly for $b = c$ and $\alpha = 60°$. In this case $a = b = c$.

Eighth proof. The Hadwiger–Finsler inequality (1937). This is a strong generalization.

$$\begin{aligned} a^2 &= b^2 + c^2 - 2bc\cos\alpha \\ &= (b-c)^2 + 2bc(1-\cos\alpha) \\ &= (b-c)^2 + 4A\frac{1-\cos\alpha}{\sin\alpha} \\ &= (b-c)^2 + 4A\tan\frac{\alpha}{2}. \end{aligned}$$

Here we used $1 - \cos\alpha = 2\sin^2\frac{\alpha}{2}$, $\sin\alpha = 2\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}$, that is,

$$a^2 + b^2 + c^2 = (a-b)^2 + (b-c)^2 + (c-a)^2 + 4A\left(\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2}\right).$$

Since $\alpha/2,\ \beta/2,\ \gamma/2 < \pi/2$, the function tan is convex. Thus, we have

$$\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2} \geq 3\tan\frac{\alpha+\beta+\gamma}{6} = 3\tan 30° = \sqrt{3}.$$

We have equality for $\alpha = \beta = \gamma = 60°$. Then we have

$$a^2 + b^2 + c^2 \geq (a-b)^2 + (b-c)^2 + (c-a)^2 + 4A\sqrt{3}.$$

Ninth proof. We have the following equivalence transformations:

$$\begin{gathered} a^2 + b^2 + c^2 \geq 4A\sqrt{3}, \\ \left(a^2 + b^2 + c^2\right)^2 \geq 3(a+b+c)(a-b+c)(-a+b+c)(a+b-c), \\ (a^2 + b^2 + c^2)^2 \geq 3\left(2a^2b^2 + 2c^2a^2 + 2a^2b^2 - a^4 - b^4 - c^4\right), \\ 4a^4 + 4b^4 + 4c^4 - 4a^2b^2 - 4b^2c^2 - 4a^2c^2 \geq 0, \\ \left(a^2 - b^2\right)^2 + \left(b^2 - c^2\right)^2 + \left(c^2 - a^2\right)^2 \geq 0. \end{gathered}$$

Tenth proof. We try to invent a triangular inequality which becomes an exact equality for the equilateral triangle. Such an inequality is

$$(a-b)^2 + (b-c)^2 + (c-a)^2 \geq 0.$$

Squaring, we get

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

We decide to introduce the area of the triangle. We use

$$ab = \frac{2A}{\sin\gamma}, \quad bc = \frac{2A}{\sin\alpha}, \quad ca = \frac{2A}{\sin\beta}.$$

We transform into the form

$$\sqrt{\frac{a}{a+d}\cdot\frac{b}{b+c}}+\sqrt{\frac{c}{b+c}\cdot\frac{d}{a+d}}\le 1.$$

Setting $a/(a+d)=\sin^2\alpha$, $b/(b+c)=\sin^2\beta$ $(0<\alpha,\beta<\frac{\pi}{2})$, the inequality takes the form $\sin\alpha\sin\beta+\cos\alpha\cos\beta\le 1$, i.e., $\cos(\alpha-\beta)\le 1$.

Strategies for Proving Inequalities

1. Try to transform the inequality into the form $\sum p_i$, $p_i>0$, e.g., $p_i=x_i^2$.
2. Does the expression remind you of the AM, GM, HM, or QM?
3. Can you apply the Cauchy–Schwarz inequality? This is especially tricky. You can apply this inequality far more often than you think.
4. Can you apply the Rearrangement inequality? Again, this theorem is much underused. You can apply it in most unexpected circumstances.
5. Is the inequality symmetric in its variables a, b, c, ...? In that case, assume $a\le b\le c\le\dots$. Sometimes one can assume that a is the maximal or minimal element. It may be advantageous to express the inequality by elementary symmetric functions.
6. An inequality homogeneous in its variables can be **normalized.**
7. If you are dealing with an inequality for the sides a, b, c of a triangle, think of the triangle inequality in its many forms. Especially, think of setting $a=x+y$, $b=y+z$ and $c=z+x$ with $x, y, z>0$.
8. Bring the inequality into the form $f(a,b,c,\dots)\ge 0$. Is f quadratic in one of its variables? Can you find its discriminant?
9. If the inequality is to be proved for all positive integers $n\ge n_0$, then use induction.
10. Try to make estimates by telescoping series or products:

$$(a_2-a_1)+(a_3-a_2)+\cdots+(a_n-a_{n-1})=a_n-a_1,\qquad \frac{a_2}{a_1}\frac{a_3}{a_2}\cdots\frac{a_n}{a_{n-1}}=\frac{a_n}{a_1}.$$

11. If $a_1x_1+\cdots+a_nx_n=c$, then $x_1\cdots x_n$ is maximal for $a_1x_1=\cdots=a_nx_n$.
12. If $x_1\cdots x_n=c$, then $a_1x_1+\cdots+a_nx_n$ is minimal for $a_1x_1=\cdots=a_nx_n$.
13. Max $x_i>d$ if the mean of the x_i is $>d$.
14. One of several numbers is positive if their sum or mean is positive.

15. A powerful idea for proving inequalities is **convexity** or **concavity**.

16. To prove an inequality $T(a, b, c, \ldots) \geq 0$ or $T(a, b, c, \ldots) \leq 0$ one often solves an optimization problem: find the values $a, b, c, \ldots$ such that $T(a, b, c, \ldots)$ is a minimum or maximum.

17. Does trigonometric substitution simplify the inequality?

18. If none of these methods is immediately applicable then transform the inequality into a simpler form with some aims in view until a standard method is applicable. If you have no success, continue transforming and try to interpret the intermediate results.

Problems

1. $a, b, c \in \mathbb{R}$, $a^2 + b^2 + c^2 = 1 \Rightarrow -\frac{1}{2} \leq ab + bc + ca \leq 1$.

2. Prove that, for $a, b, c > 0$,

$$\text{(a)}\ \frac{a^2+b^2}{a+b} \geq \frac{a+b}{2}, \quad \text{(b)}\ \frac{a^3+b^3+c^3}{a^2+b^2+c^2} \geq \frac{a+b+c}{3},$$

$$\text{(c)}\ \frac{a+b+c}{3} \geq \sqrt{\frac{ab+bc+ca}{3}} \geq \sqrt[3]{abc}.$$

3. For $a, b, c, d > 0$,

$$\sqrt{\frac{a^2+b^2+c^2+d^2}{4}} \geq \sqrt[3]{\frac{abc+abd+acd+bcd}{4}}.$$

4. Prove that, for $a, b > 0$, we have $\sqrt[n+1]{ab^n} \leq (a + nb)/(n + 1)$.

5. The spinner in Fig. 7.5 has circumference 1. It is spun 6 times. For what values of x, y, z for the probabilities of O, A, B, respectively, is the probability of the word $BAOBAB$ maximal?

6. Let a, b, c be the sides of a triangle. Then $ab + bc + ca \leq a^2 + b^2 + c^2 \leq 2(ab + bc + ca)$.

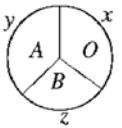


Fig. 7.5

7. If a, b, c are sides of a triangle, then $2(a^2 + b^2 + c^2) < (a + b + c)^2$.

8. If a, b, c are sides of a triangle, then so are $1/(a + b)$, $1/(b + c)$, $1/(c + a)$.

9. Let $a, b, c, d > 0$. Find all possible values of the sum

$$S = \frac{a}{a+b+d} + \frac{b}{a+b+c} + \frac{c}{b+c+d} + \frac{d}{a+c+d} \qquad \text{(IMO 1974)}.$$

10. Prove the triangle inequality

$$\sqrt{a_1^2+\cdots+a_n^2}+\sqrt{b_1^2+\cdots+b_n^2}\geq\sqrt{(a_1+b_1)^2+\cdots+(a_n+b_n)^2}.$$

11. Let $a,\ b,\ c>0$. Show that

$$\frac{a+b+c}{abc}\leq\frac{1}{a^2}+\frac{1}{b^2}+\frac{1}{c^2}.$$

12. Let $x_i,\ y_i,\ 1\leq i\leq n$ be real numbers such that

$$x_1\geq x_2\geq\cdots\geq x_n \quad\text{and}\quad y_1\geq y_2\geq\cdots\geq y_n \qquad \text{(IMO 1975)}$$

Let $z_1,\ z_2,\ \ldots,\ z_n$ be any permutation of $y_1,\ y_2,\ \ldots,\ y_n$. Show that

$$\sum_{i=0}^{n}(x_i-y_i)^2\leq\sum_{i=1}^{n}(x_i-z_i)^2.$$

13. Let $\{a_k\}\quad(k=1,2,\ldots,n,\ldots)$ be a sequence of pairwise distinct positive integers. Show that for all positive integers n

$$\sum_{k=1}^{n}\frac{a_k}{k^2}\geq\sum_{k=1}^{n}\frac{1}{n}\qquad\text{(IMO 1978)}.$$

14. (Telescoping product.) Prove that

$$\frac{1}{15}<\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdot\frac{7}{8}\cdots\frac{99}{100}<\frac{1}{10}.$$

Hint:

$$(1)\quad A=\frac{1}{2}\cdot\frac{3}{4}\cdots\frac{99}{100},\quad (2)\quad A<\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdots\frac{100}{101},\quad (3)\quad A>\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdots\frac{98}{99}.$$

Multiply (1) with (2) and (1) with (3).

15. (Telescoping series.) Let $Q_n=1+1/4+1/9+\cdots+1/n^2$. Then, for $n\geq 3$,

$$\frac{19}{12}-\frac{1}{n+1}<Q_n<\frac{7}{4}-\frac{1}{n}.$$

16. By induction, prove the sharp inequality

$$\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdots\frac{2n-1}{2n}\leq\frac{1}{\sqrt{3n+1}},\quad n\geq 1.$$

Replace $3n+1$ by $3n$ on the right side, and try to prove this weaker inequality by induction. What happens?

17. $a,\ b,\ c>0\Rightarrow abc(a+b+c)\leq a^3b+b^3c+c^3a$.

18. $1/2<1/(n+1)+1/(n+2)+\cdots+1/2n<3/4,\ n>1$.

19. The Fibonacci sequence is defined by $a_1=a_2=1,\ a_{n+2}=a_n+a_{n+1}$. Prove that

$$\frac{1}{2}+\frac{1}{2^2}+\frac{2}{2^3}+\frac{3}{2^4}+\frac{5}{2^5}+\cdots+\frac{a_n}{2^n}<2.$$

20. Prove that, for real numbers $x,\ y,\ z$

$$|x| + |y| + |z| \le |x + y - z| + |x - y + z| + |-x + y + z|.$$

21. If $a,\ b,\ c > 0$, then $a(1-b) > 1/4,\ b(1-c) > 1/4,\ c(1-a) > 1/4$ cannot be valid simultaneously.

22. If $a,\ b,\ c,\ d > 0$, then at least one of the following inequalities is wrong:

$$a + b < c + d, \quad (a+b)(c+d) < ab + cd, \quad (a+b)cd < ab(c+d).$$

23. The product of three positive reals is 1. Their sum is greater than the sum of their reciprocals. Prove that exactly one of these numbers is > 1.

24. Let $x_1 = 1$, $x_{n+1} = 1 + n/x_n$ for $n \ge 1$. Show that $\sqrt{n} \le x_n \le \sqrt{n} + 1$.

25. If a, b, and c are sides of a triangle, then

$$\frac{3}{2} \le \frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} < 2.$$

26. If a, b, c are sides of a triangle with $\gamma = 90°$, then

$$c^n > a^n + b^n \quad \text{for } n \in \mathbb{N}, n > 2.$$

27. If $x,\ y,\ z$ are sides of a triangle, then $|x/y + y/z + z/x - y/x - z/y - x/z| < 1$. Can you replace 1 by a smaller number?

28. A point is chosen on each side of a unit square. The four points are sides of a quadrilateral with sides a, b, c, d. Show that

$$2 \le a^2 + b^2 + c^2 + d^2 \le 4 \quad \text{and} \quad 2\sqrt{2} \le a + b + c + d \le 4.$$

29. Let $a_i \ge 1$ for $i = 1, \ldots, n$. Show that

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \ge \frac{2^n}{n+1}(1 + a_1 + a_2 + \cdots + a_n).$$

30. Let $0 < a \le b \le c \le d$. Then $a^b b^c c^d d^a \ge b^a c^b d^c a^d$.

31. If $a,\ b > 0$ and m is an integer, then $(1 + a/b)^m + (1 + b/a)^m \ge 2^{m+1}$.

32. Let $0 < p \le a,\ b,\ c,\ d,\ e \le q$. Show that

$$(a+b+c+d+e)\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{d} + \frac{1}{e}\right) \le 25 + 6\left(\sqrt{\frac{p}{q}} - \sqrt{\frac{q}{p}}\right)^2.$$

This is a problem of the US Olympiad 1977. It is a special case of a general theorem. Also, prove this more general theorem.

33. The diagonals of a convex quadrilateral intersect in O. What is the smallest area this quadrilateral can have, if the triangles AOB and COD have areas 4 and 9, respectively?

34. Let $x,\ y > 0$, and let s be the smallest of the numbers $x,\ y + 1/x,\ 1/y$. Find the greatest possible value of s. For which $x,\ y$ is this value assumed?

35. Let $x_i > 0$, $x_1 + \cdots + x_n = 1$, and let s be the greatest of the numbers

$$\frac{x_1}{1+x_1}, \frac{x_2}{1+x_1+x_2}, \frac{x_3}{1+x_1+x_2+x_3}, \ldots, \frac{x_n}{1+x_1+x_2+\cdots+x_n}.$$

Find the smallest value of s. For which $x_1, \ldots, x_n$ will it be assumed?

36. Find a point P inside the triangle ABC, such that the product $PL \cdot PM \cdot PN$ is maximal. Here L, M, N are the feet of the perpendiculars from P onto BC, CA, AB (BrMO 1978).

37. If $x_i > 0$ and $x_i y_i - z_i^2 > 0$ for $i \leq n$, then

$$\frac{n^3}{\left(\sum_{i=1}^n x_i\right)\left(\sum_{i=1}^n y_i\right) - \left(\sum_{i=1}^n z_i\right)^2} \leq \sum_{i=1}^n \frac{1}{x_i y_i - z_i^2}.$$

Prove this inequality for $n = 2$ (IMO 1969), and then also generally.

38. The vectors $\vec{a}$, $\vec{b}$, $\vec{c}$, $\vec{d}$ with sum $\vec{o}$ are given in a plane. Prove the inequality

$$|\vec{a}| + |\vec{b}| + |\vec{c}| + |\vec{d}| \geq |\vec{a} + \vec{d}| + |\vec{b} + \vec{d}| + |\vec{c} + \vec{d}|.$$

Prove this also for one and three dimensions (AUO 1976).

39. Show that $(n+1)^n \geq 2^n \cdot n!$ for $n = 1, 2, 3, \ldots$.

40. (MMO 1975.) Which of the two numbers is larger:
(a) An exponential tower of n 2's or an exponential tower of $(n-1)$ 3's?
(b) An exponential tower of n 3's or an exponential tower of $(n-1)$ 4's?

41. Fifty watches, all showing correct time, are on a table. Prove that at a certain moment the sum of the distances from the center O of the table to the endpoints of the minute hands is greater than the sums of the distances from O to the centers of the watches (AUO 1976).

42. Let $x_1 = 2$, $x_{n+1} = (x_n^4 + 1)/5x_n$ for $n > 0$. Show that $1/5 \leq x_n < 2$ for all $n > 1$.

43. Let a, b, $c > 0$. Show that

(a) $abc \geq (a+b-c)(a+c-b)(b+c-a)$, (b) $a^3 + b^3 + c^3 \geq a^2 b + b^2 c + c^2 a$.

44. Let $x_i > 0$, $s = x_1 + \cdots, +x_n$. Show that

$$\frac{s}{s-x_1} + \frac{s}{s-x_2} + \cdots + \frac{s}{s-x_n} \geq \frac{n^2}{n-1}.$$

45. For x, y, $z > 0$,

(a) $\dfrac{x^2}{y^2} + \dfrac{y^2}{z^2} + \dfrac{z^2}{x^2} \geq \dfrac{y}{x} + \dfrac{z}{y} + \dfrac{x}{z}$, (b) $\dfrac{x^2}{y^2} + \dfrac{y^2}{z^2} + \dfrac{z^2}{x^2} \geq \dfrac{x}{y} + \dfrac{y}{z} + \dfrac{z}{x}$.

46. Write each rational number from $(0, 1]$ as a fraction a/b with $\gcd(a, b) = 1$, and cover a/b with the interval

$$\left[\frac{a}{b} - \frac{1}{4b^2}, \frac{a}{b} + \frac{1}{4b^2}\right].$$

Prove that the number $\sqrt{2}/2$ is not covered.

91. Prove that, for real numbers $x_1 \geq x_2 \geq \cdots \geq x_n > 0$,

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} \leq \frac{x_2}{x_1} + \frac{x_3}{x_2} + \cdots + \frac{x_n}{x_{n-1}} + \frac{x_1}{x_n}.$$

92. Prove that, if the numbers a, b, and c satisfy the inequalities $|a-b| \geq |c|, |b-c| \geq |a|$, $|c-a| \geq |b|$, then one of these numbers is the sum of the other two (MMO 1996).

93. The positive integers a, b, c are such that $a^2+b^2-ab = c^2$. Prove that $(a-c)(b-c) \leq 0$ (MMO 1996).

94. If x, y, z are reals from $[0, 1]$, then $2(x^3 + y^3 + z^3) - x^2y - y^2z - z^2x \leq 3$.

95. If a, b, c are real numbers such that $0 \leq a, b, c \leq 1$, then

$$\frac{a}{1+bc} + \frac{b}{1+ac} + \frac{c}{1+ab} \leq 2.$$

96. Prove that, for any distribution of signs $+$ and $-$ in the odd powers of x,

$$x^{2n} \pm x^{2n-1} + x^{2n-2} \pm x^{2n-3} + \cdots + x^4 \pm x^3 + x^2 \pm x + 1 > \frac{1}{2}.$$

97. Given are any eight real numbers a, b, c, d, e, f, g, and h. Prove that at least one of the six numbers $ac + bd$, $ae + bf$, $ag + bh$, $ce + df$, $cg + dh$, $eg + fh$ is not negative.

98. Let $n > 2$ and $x_1, \ldots, x_n$ be nonnegative reals. Prove the inequality

$$(x_1x_2 \cdots x_n)^{1/n} + \frac{1}{n} \sum_{i<j} |\, x_i - x_j \,| \geq \frac{x_1 + \cdots + x_n}{n}.$$

99. Let $a, b \in \mathbb{R}$ and $f(x) = a\cos x + b\cos 3x$. It is known that $f(x) > 1$ has no solutions. Prove that $|\, b \,| \leq 1$.

100. Let a, b, c be the sides of a triangle. Prove that

$$\frac{a}{b+c-a} + \frac{b}{c+a-b} + \frac{c}{a+b-c} \geq 3.$$

Solutions

1. The right side follows from $ab + bc + ca \leq a^2 + b^2 + c^2$. The left side follows from $0 \leq (a+b+c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca) = 1 + 2(ab + bc + ca)$.

2. (a) This is a slight transformation of the QM-AM and an example of the Chebyshev inequality $2(a^2 + b^2) \geq (a+b)^2$.

   (b) This is the Chebyshev inequality $3(a^3 + b^3 + c^3) \geq (a+b+c)(a^2 + b^2 + c^2)$.

   (c) The right side is $\sqrt{(ab+bc+ca)/3} \geq \sqrt{\sqrt[3]{ab \cdot bc \cdot ca}} = \sqrt[3]{abc}$. We get the left side easily by squaring $a^2 + b^2 + c^2 \geq ab + bc + ca$.

9

Sequences

Difference Equations. A *sequence* is a function f defined for every nonnegative integer n. For sequences one mostly sets $x_n = f(n)$. Usually we are given an equation of the form

$$x_n = F(x_{n-1}, x_{n-2}, x_{n-3}, \ldots).$$

Sometimes we are expected to find a 'closed expression' for x_n. Such an equation is called a *functional equation*. A functional equation of the form

$$x_n = px_{n-1} + qx_{n-2} \quad (q \neq 0) \tag{1}$$

is a (homogeneous) *linear difference equation of order 2* (with constant coefficients.) To find the general solution of (1), first we try to find a solution of the form $x_n = \lambda^n$ for a suitable number λ. To find λ, we plug λ^n into (1) and get $\lambda^n = p\lambda^{n-1} + q\lambda^{n-2}$, $\lambda^2 = p\lambda + q$, or

$$\lambda^2 - p\lambda - q = 0. \tag{2}$$

This is the *characteristic equation* of (1). For distinct roots λ_1 and λ_2,

$$x_n = a\lambda_1^n + b\lambda_2^n$$

is the general solution. a and b can be found from the initial values x_0, x_1.

If $\lambda_1 = \lambda_2 = \lambda$, the general solution has the form

$$x_n = (a + bn)\lambda^n. \tag{3}$$

E1. *A sequence x_n is given by means of $x_0 = 2$, $x_1 = 7$, and $x_{n+1} = 7x_n - 12x_{n-1}$. Find a closed expression for x_n.*

The characteristic equation $\lambda^2 - 7\lambda + 12 = 0$ has roots $\lambda_1 = 3$, $\lambda_2 = 4$. The general solution $x_n = a \cdot 3^n + b \cdot 4^n$ yields $a + b = 2$, $3a + 4b = 7$ with solutions $a = b = 1$ for $x_0 = 2$ and $x_1 = 7$. Thus, $x_n = 3^n + 4^n$.

E2. *For all $x \in \mathbb{R}$, a function f satisfies the functional equation*

$$f(x+1) + f(x-1) = \sqrt{2} f(x). \tag{1}$$

Show that it is periodic.

With $a = f(x-1)$, $b = f(x)$, we get $f(x+1) = \sqrt{2}b - a$, $f(x+2) = b - \sqrt{2}a$, $f(x+3) = -a$, $f(x+4) = -b$, i.e, $f(x+4) = -f(x)$ for all x, and $f(x+8) = f(x)$ for all x. Thus 8 is a period of f.

E3. *Can we replace $\sqrt{2}$ in (1) so that the period has any preassigned value, e.g., 12?*

Replacing $\sqrt{2}$ by the golden section $t = (\sqrt{5}+1)/2$ with the property $t > 0$, $t^2 = t+1$ we get $a = f(x-1), b = f(x)$, $f(x+1) = tb - a$, $f(x+2) = t(b-a)$, $f(x+3) = b - ta$, $f(x+4) = -a$, $f(x+5) = -f(x)$, $f(x+10) = f(x)$. Now f has period 10.

Replacing $\sqrt{2}$ by the positive root of $t^3 = t^2 + t + 1$, no periodicity was in sight after many steps. Whenever t^3 turned up, I replaced it by $t^2 + t + 1$. Is f not periodic in this case?

A second look shows that (1) is a linear difference equation of second order. But the discrete variable n is replaced by the continuous variable x. So we try to find solutions $f(x) = \lambda^x$. For the value of λ, we get $\lambda^2 - t\lambda + 1 = 0$ with solutions

$$\lambda = \frac{t}{2} \pm \sqrt{\frac{t^2}{4} - 1}.$$

For $t < 2$ we have the solutions

$$\lambda = \frac{t}{2} + i\sqrt{1 - \frac{t^2}{4}}, \qquad \overline{\lambda} = \frac{t}{2} - i\sqrt{1 - \frac{t^2}{4}}, \qquad \text{and} \qquad |\lambda| = |\overline{\lambda}| = 1.$$

So λ and its conjugate $\overline{\lambda}$ are unit vectors in the complex plane, that is,

$$\lambda = \cos\phi + i\sin\phi,$$
$$\overline{\lambda} = \cos\phi - i\sin\phi.$$

Thus, λ has period n if $\lambda^n = 1$ or $\lambda = \cos(2\pi/n) + i\sin(2\pi/n)$. In particular, it has period 12, if $t/2 = \cos(\pi/6)$, $t = 2\cos(\pi/6) = \sqrt{3}$. The period is exactly n, if $t/2 = \cos(2\pi/n)$ or $t = 2\cos(2\pi/n)$. The positive solution of $t^3 = t^2 + t + 1$ is $t = 1.854\ldots < 2$. Yet it is unlikely that this irrational number gives a rational multiple of π for the angle ϕ, the only way to secure periodicity.

10
Polynomials

1. The terms

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0,\ a_n \neq 0,\ b_m \neq 0$$

are *polynomials* of *degrees* n and m: $\deg f = n, \deg g = m$. The coefficients a_i, b_i can be from $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{Z}_n$.

2. **Division with Remainder**. For polynomials f and g there exist unique polynomials q and r so that

$$f(x) = g(x)q(x) + r(x), \quad \deg r < \deg g \text{ or } r(x) = 0.$$

$q(x)$ and $r(x)$ are *quotient* and *remainder* on division of f by g. If $r(x) = 0$, then we say that $g(x)$ divides $f(x)$, and we write $g(x) | f(x)$.

E1. With $f(x) = x^7 - 1,\ g(x) = x^3 + x + 1$ the grade school method of division yields

$$x^7 - 1 = (x^3 + x + 1)(x^4 - x^2 - x + 1) + 2x^2 - 2.$$

Here $q(x) = x^4 - x^2 - x + 1,\ r(x) = 2x^2 - 2$.

3. Let f be a polynomial of degree n and $a \in \mathbb{R}$. Division by $x - a$ yields

$$f(x) = (x - a)q(x) + r, \quad r \in \mathbb{R}, \quad \deg q = n - 1. \tag{1}$$

Setting $x = a$ in (1), we get $f(a) = r$, and hence

$$f(x) = (x - a)q(x) + f(a). \tag{2}$$

If $f(a) = 0$, then a is a *root* or *zero* of f. It follows from (2)

$$f(a) = 0 \Leftrightarrow f(x) = (x - a)q(x) \text{ for some polynomial } q(x). \tag{3}$$

If a_1, a_2 are distinct zeros of f, then $f(x) = (x - a_1)q(x)$ with $q(a_2) = 0$, that is, $q(x) = (x - a_2)q_1(x)$. Thus,

$$f(x) = (x - a_1)(x - a_2)q_1(x), \ \deg q_1 = n - 2.$$

If $\deg f = n$ and $f(a_i) = 0$ for $a_1, \ldots, a_n$, then

$$f(x) = c(x - a_1)(x - a_2)\cdots(x - a_n), \quad c \in \mathbb{R}.$$

4. If there exists an $m \in \mathbb{N}$ and a polynomial q so that

$$f(x) = (x - a)^m q(x), \quad q(a) \neq 0, \tag{4}$$

then the root a of f has multiplicity m. (4) implies that a has multiplicity m if and only if

$$f(a) = f'(a) = f''(a) = \cdots = f^{(m-1)}(a) = 0, \quad f^m(a) \neq 0. \tag{5}$$

5. Let $f(x) = a_n x^n + \cdots + a_0$ have integer coefficients, and let $z \in \mathbb{Z}$. Then

$$f(z) = 0 \Leftrightarrow z | a_0.$$

Indeed, $a_n z^n + \cdots + a_1 z + a_0 = 0 \Leftrightarrow a_0 = -z(a_n z^{n-1} + \cdots + a_1)$. If $a_n = 1$, then each *rational* root of f is an *integer*. Indeed, let p/q be a root, $p, q \in \mathbb{Z}$, $\gcd(p, q) = 1$. Then

$$\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1\frac{p}{q} + a_0,$$

$$\frac{p^n}{q} = -a_{n-1}p^{n-1} - a_{n-2}p^{n-2}q - \cdots - a_1 pq^{n-2} - a_0 q^{n-1}.$$

The RHS is an integer. Hence, $q = 1$.

If the highest degree coefficient $a_n = 1$, then the polynomial is called a *monic polynomial*.

6. **Vieta's Theorem.** (a) If the polynomial $x^2 + px + q$ has roots x_1, x_2, then $x^2 + px + q = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$, that is,

$$p = -(x_1 + x_2), \ q = x_1x_2.$$

(b) Let x_1, x_2, x_3 be the roots of $x^3 + px^2 + qx + r$. By expanding

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_2x_3 + x_3x_1)x - x_1x_2x_3$$

and comparing coefficients, we get

$$p = -(x_1 + x_2 + x_3), \ q = x_1x_2 + x_2x_3 + x_3x_1, \ r = -x_1x_2x_3.$$

Similar relations exist for higher degree monic polynomials.

E2. *Let* $x_1,\ x_2,\ x_3$ *be the roots of* x^3+3x^2-7x+1. *Find* $x_1^2+x_2^2+x_3^2$.

Solution. $x_1+x_2+x_3=-3,\ x_1x_2+x_2x_3+x_3x_1=-7,\ 9=(x_1+x_2+x_3)^2=x_1^2+x_2^2+x_3^2+2(x_1x_2+x_2x_3+x_3x_1)=x_1^2+x_2^2+x_3^2-2\cdot 7,\ x_1^2+x_2^2+x_3^2=23.$

7. If $a\in\mathbb{R}$, then $f(x)=a_nx^n+\cdots+a_0$ can be written in the form

$$f(x)=c_n(x-a)^n+\cdots+c_1(x-a)+c_0.$$

To prove this, we set $x=a+(x-a)$ for x in f.

8. **Fundamental Theorem of Algebra.** *Every polynomial* $f(z)=a_nz^n+\cdots+a_0,\ a_i\in\mathbb{C},\ n\geq 1,\ a_n\neq 0$ *has at least one root in* $\mathbb{C}$.

From this theorem it easily follows that each polynomial of degree n can be written in the form

$$f(x)=c(x-x_1)(x-x_2)\cdots(x-x_n),\ x_i\in\mathbb{C},$$

where the x_i are not necessarily distinct.

9. **Roots of Unity**. Let $\omega=e^{i\frac{2\pi}{n}}=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$. The polynomial x^n-1 has the roots $\omega,\ \omega^2,\cdots,\omega^n=1$. They are called *roots of unity* and they are the vertices of a regular n-gon inscribed in the unit circle with center O. If $\gcd(k,n)=1$, then the powers of ω^k also give all nth roots of unity. We have the decomposition

$$x^n-1=(x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{n-1}).$$

In particular, the roots of $x^3-1=0$, or $(x-1)(x^2+x+1)=0$ are the third roots of unity. Denoting by $\overline{z}$ the conjugate of z, we get

$$\omega=\frac{-1+i\sqrt{3}}{2},\quad \omega^2=\overline{\omega}=\frac{1}{\omega},\quad \omega^3=1,\quad 1+\omega+\omega^2=0. \tag{6}$$

We can solve the general cubic equation with third unit roots. We start with the classic decomposition

$$x^3+a^3+b^3-3abx=(x+a+b)(x^2+a^2+b^2-ax-bx-ab).$$

The last factor has the roots $x_2=-a\omega-b\omega^2,\ x_3=-a\omega^2-b\omega$. Thus,

$$x^3+a^3+b^3-3abx=(x+a+b)(x+a\omega+b\omega^2)(x+a\omega^2+b\omega).$$

Hence, the cubic equation $x^3-3abx+a^3+b^3=0$ has the solutions

$$x_1=-a-b,\ x_2=-a\omega-b\omega^2,\ x_3=-a\omega^2-b\omega. \tag{7}$$

Comparing this with $x^3+px+q=0$. we get $p=-3ab,\ q=a^3+b^3$, or

$$a^3b^3=-p^3/27,\quad a^3+b^3=q. \tag{8}$$

From (8) we infer that a^3, b^3 are roots of the quadratic

$$z^2 - qz - p^3/27 = 0.$$

Thus,

$$a = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad b = \sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}. \tag{9}$$

Inserting (9) into (7) we get the three solutions of $x^3 + px + q = 0$. Any cubic can be transformed into this form by translation and division by a constant.

Now we use the fifth roots of unity to construct the regular pentagon.

$$x^5 - 1 = (x - 1)(x^4 + x^3 + x^2 + x + 1).$$

This factoring shows that the fifth unit root ω satisfies the equation

$$\begin{aligned} \omega^4 + \omega^3 + \omega^2 + \omega + 1 &= 0, \\ \omega^2 + \tfrac{1}{\omega^2} + \omega + \tfrac{1}{\omega} + 1 &= 0, \\ (\omega + \tfrac{1}{\omega})^2 + (\omega + \tfrac{1}{\omega}) - 1 &= 0, \\ \omega + \tfrac{1}{\omega} &= \tfrac{\sqrt{5}-1}{2}. \end{aligned}$$

For $a = \cos 72°$ in Fig. 10.1, we have

$$a = \frac{\sqrt{5} - 1}{4}.$$

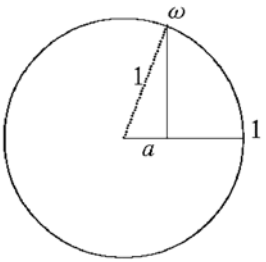


Fig. 10.1

The segment a is easy to construct with ruler and compass.

Now we solve some typical examples with polynomials.

E3. (a) *For which* $n \in \mathbb{N}$ *is* $x^2 + x + 1 | x^{2n} + x^n + 1$? (b) *For which* n *is* $37 | 10\underbrace{\ldots 0}_{n}10\underbrace{\ldots 0}_{n}1$?

First Solution. By straightforward transformation using the relations

$$x^3 - 1 = (x - 1)(x^2 + x + 1) \quad \text{and} \quad x^3 - 1 | x^{3m} - 1.$$

(i) $n = 3k \Leftrightarrow x^{6k} + x^{3k} + 1 = (x^{6k} - 1) + (x^{3k} - 1) + 3 = (x^2 + x + 1)Q(x) + 3$.

(ii) $n = 3k+1 \Leftrightarrow x^{6k+2} + x^{3k+1} + 1 = x^2(x^{6k} - 1) + x(x^{3k} - 1) + x^2 + x + 1 = (x^2 + x + 1)R(x)$.

(iii) $n = 3k+2 \Leftrightarrow x^{6k+4} + x^{3k+2} + 1 = x^4(x^{6k} - 1) + x^2(x^{3k} - 1) + x^4 + x^2 + 1 = x^4(x^{6k} - 1) + x^2(x^{3k} - 1) + x(x^3 - 1) + x^2 + x + 1 = (x^2 + x + 1)S(x)$.

Answer: $x^2 + x + 1 | x^{2n} + x^n + 1 \Leftrightarrow 3 \not| n$.

(b) $x = 10$ yields $x^2 + x + 1 = 111$, $x^{2(n+1)} + x^{n+1} + 1 = 1\underbrace{0\ldots0}_{n}1\underbrace{0\ldots0}_{n}1$, $111 = 3 \cdot 37$. The number is divisible by 3 since the digit sum is 3. Hence

$$37 | 1\underbrace{0\ldots0}_{n}1\underbrace{0\ldots0}_{n}1 \text{ if } n = 0 \bmod 3 \text{ or } n = 1 \bmod 3.$$

Second Solution of (a). $x^2 + x + 1 = 0$ has solutions ω and ω^2. By using the relationships $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$, we get

$$\begin{aligned} n = 3k &\Rightarrow \omega^{6k} + \omega^{3k} + 1 = 1 + 1 + 1 = 3, \\ n = 3k+1 &\Rightarrow \omega^{6k+2} + \omega^{3k+1} + 1 = \omega^2 + \omega + 1 = 0, \\ n = 3k+2 &\Rightarrow \omega^{6k+4} + \omega^{3k+2} + 1 = \omega^4 + \omega^2 + 1 = \omega + \omega^2 + 1 = 0. \end{aligned}$$

E4. *If $P(x)$, $Q(x)$, $R(x)$, $S(x)$ are polynomials so that*

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x), \qquad (*)$$

then $x - 1$ is a factor of $P(x)$. Show this (USO 1976).

Solution. Let $\omega = e^{2\pi i/5}$, so that $\omega^5 = 1$. We set for x in (*), ω, ω^2, ω^3, ω^4 successively, and get the following equations 1 to 4. If we multiply 1 to 4 by $-\omega$, $-\omega^2$, $-\omega^3$, $-\omega^4$, then we get the last 4 equations.

$$\begin{aligned} P(1) + \omega Q(1) + \omega^2 R(1) &= 0, \\ P(1) + \omega^2 Q(1) + \omega^4 R(1) &= 0, \\ P(1) + \omega^3 Q(1) + \omega R(1) &= 1, \\ P(1) + \omega^4 Q(1) + \omega^3 R(1) &= 0, \\ -\omega P(1) - \omega^2 Q(1) - \omega^3 R(1) &= 0, \\ -\omega^2 P(1) - \omega^4 Q(1) - \omega R(1) &= 0, \\ -\omega^3 P(1) - \omega Q(1) - \omega^4 R(1) &= 0, \\ -\omega^4 P(1) - \omega^3 Q(1) - \omega^2 R(1) &= 0. \end{aligned}$$

Using $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$, we get the sum $5P(1) = 0$, that is, $x - 1 | P(x)$.

E5. *Let $P(x)$ be a polynomial of degree n, so that $P(k) = k/(k+1)$ for $k = 0..n$. Find $P(n+1)$* (USO 1975).

Solution. Let $Q(x) = (x+1)P(x) - x$. Then the polynomial $Q(x)$ vanishes for $k = 0, \ldots, n$, that is,

$$(x+1)P(x) - x = a \cdot x \cdot (x-1)(x-2)\cdots(x-n).$$

To find a we set $x = -1$ and get $1 = a(-1)^{n+1}(n+1)!$. Thus,

$$P(x) = \frac{(-1)^{n+1}x(x-1)\cdots(x-n)/(n+1)! + x}{x+1},$$

and

$$P(n+1) = \begin{cases} 1 & \text{for odd } n, \\ n/(n+2) & \text{for even } n. \end{cases}$$

E6. *Let a, b, c be three distinct integers, and let P be a polynomial with integer coefficients. Show that in this case the conditions*

$$P(a) = b, \quad P(b) = c, \quad P(c) = a$$

cannot be satisfied simultaneously (USO 1974).

Solution. Suppose the conditions are satisfied. We derive a contradiction.

$$P(x) - b = (x-a)P_1(x), \tag{1}$$
$$P(x) - c = (x-b)P_2(x), \tag{2}$$
$$P(x) - a = (x-c)P_3(x). \tag{3}$$

Among the numbers a, b, c, we choose the pair with maximal absolute difference. Suppose this is $|a-c|$. Then we have

$$|a-b| < |a-c|. \tag{4}$$

If we replace x by c in (1), then we get

$$a - b = (c-a)P_1(c).$$

Since $P_1(c)$ is an integer, we have $|a-b| \geq |c-a|$, which contradicts (4).

10. Reciprocal Equations

Definition. The polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$ is called reciprocal, if $a_i = a_{n-i}$ for $i = 0, \ldots, n$.

Examples $x^n + 1$, $x^5 + 3x^3 + 3x^2 + 1$, $5x^8 - 2x^6 + 4x^5 + 4x^3 - 2x^2 + 5$. The equation $f(x) = 0$ with $f(x)$ being a reciprocal polynomial is called a *reciprocal equation*.

Theorem. *Any reciprocal polynomial $f(x)$ of degree $2n$ can be written in the form $f(x) = x^n g(z)$, where $z = x + \frac{1}{x}$, and $g(z)$ is a polynomial in z of degree n.*

Proof.

$$f(x) = a_0x^{2n} + a_1x^{2n-1} + \cdots + a_1x + a_0,$$
$$f(x) = x^n\left(a_0x^n + a_1x^{n-1} + \cdots + \frac{a_1}{x^{n-1}} + \frac{a_0}{x^n}\right),$$
$$f(x) = x^n\left(a_0\left(x^n + \frac{1}{x^n}\right) + a_1\left(x^{n-1} + \frac{1}{x^{n-1}}\right) + \cdots + a_n\right).$$

We show how to express $x^k + 1/x^k$ by $z = x + 1/x$:

$$x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2 = z^2 - 2,$$
$$x^3 + \frac{1}{x^3} = \left(x + \frac{1}{x}\right)^3 - 3x - \frac{3}{x} = z^3 - 3z,$$
$$x^4 + \frac{1}{x^4} = \left(x + \frac{1}{x}\right)^4 - 4x^2 - 6 - \frac{4}{x^2} = z^4 - 4\left(z^2 - 2\right) - 6 = z^4 - 4z^2 + 2,$$
$$x^5 + \frac{1}{x^5} = \left(x + \frac{1}{x}\right)^5 - 5x^3 - 10x - \frac{10}{x} - \frac{5}{x^3} = z^5 - 5z^3 + 5z.$$

Without proof we state some properties of reciprocal polynomials. They are easy to prove and are left to the reader as exercises:

(a) Every polynomial $f(x)$ of degree n with $a_0 \neq 0$ is reciprocal iff

$$x^n f\left(\frac{1}{x}\right) = f(x).$$

(b) Every reciprocal polynomial $f(x)$ of odd degree is divisible by $x + 1$ and the quotient is a reciprocal polynomial of even degree.

(c) If a is a zero of the reciprocal equation $f(x) = 0$, then $\frac{1}{a}$ is also a zero of this equation.

11. Symmetric Polynomials

A polynomial $f(x, y)$ is symmetric, if $f(x, y) = f(y, x)$ for all x, y. Examples:
(a) The elementary symmetric polynomials in x, y

$$\sigma_1 = x + y, \quad \sigma_2 = xy.$$

(b) The power sums

$$s_i = x^i + y^i \quad i = 0, 1, 2, \ldots.$$

A polynomial symmetric in x, y can be represented as a polynomial in σ_1, σ_2. Indeed,

$$s_n = x^n + y^n = (x + y)(x^{n-1} + y^{n-1}) - xy\left(x^{n-2} + y^{n-2}\right) = \sigma_1 s_{n-1} + \sigma_2 s_{n-2}.$$

Thus, we have the recursion

$$s_0 = 2, \quad s_1 = \sigma_1, \quad s_n = \sigma_1 s_{n-1} - \sigma_2 s_{n-2}, \quad n \geq 2.$$

Now the proof for any symmetric polynomial is simple. Terms of the form $ax^k y^k$ cause no trouble since $ax^k y^k = a\sigma_2^k$. With the term $bx^i y^k$ $(i < k)$, it must also contain $bx^k y^i$. We collect these terms:

$$bx^i y^k + bx^k y^i = bx^i y^i \left(x^{k-i} + y^{k-i}\right) = b\sigma_2^i s_{k-i}.$$

But s_{k-i} can be expressed through σ_1, σ_2.

Nonlinear systems of symmetric equations in two variables x, y can mostly be simplified by the substitution $\sigma_1 = x + y$, $\sigma_2 = xy$. The degree of these equations will be reduced since $\sigma_2 = xy$ is of second degree in x, y. As soon as we have found σ_1 and σ_2 we find the solutions z_1, z_2 of the quadratic equation

$$z^2 - \sigma_1 z + \sigma_2 = 0.$$

Then we have the system of equations

$$x + y = \sigma_1, \quad xy = \sigma_2.$$

E7. *Solve the system*

$$x^5 + y^5 = 33, \quad x + y = 3.$$

We set $\sigma_1 = x + y$, $\sigma_2 = xy$. Then the system becomes

$$\sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2 = 33, \quad \sigma_1 = 3.$$

Substituting $\sigma_1 = 3$ in the first equation, we get $\sigma_2^2 - 9\sigma_2 + 14 = 0$ with two solutions $\sigma_2 = 2$ and $\sigma_2 = 7$. Now we must solve $x + y = 3$, $xy = 2$, and $x + y = 3$, $xy = 7$ resulting in

$$(2, 1),\ (1, 2),\ (x_3, y_3) = \left(\frac{3}{2} + \frac{\sqrt{19}}{2}i, \frac{3}{2} - \frac{\sqrt{19}}{2}i\right),\ (x_4, y_4) = (y_3, x_3).$$

E8. *Find the real solutions of the equation*

$$\sqrt[4]{97 - x} + \sqrt[4]{x} = 5.$$

We set $\sqrt[4]{x} = y$, $\sqrt[4]{97 - x} = z$ and get $y^4 + z^4 = x + 97 - x = 97$. Hence,

$$y + z = 5, \quad y^4 + z^4 = 97.$$

Setting $\sigma_1 = y + z$, $\sigma_2 = yz$, we get the system of equations

$$\sigma_1 = 5, \quad \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 = 97$$

resulting in $\sigma_2^2 - 50\sigma_2 + 264 = 0$ with solutions $\sigma_2 = 6,\ \sigma_2 = 44$. We must solve the system $y + z = 5,\ yz = 6$ with solutions $(y_1, z_1) = (2, 3),\ (y_2, z_2) = (3, 2)$. Now $x_1 = 16,\ x_2 = 81$. The solutions $y + z = 5,\ yz = 4$ give complex values.

E9. *What is the relationship between $a,\ b,\ c$ if the system*

$$x + y = a, \quad x^2 + y^2 = b, \quad x^3 + y^3 = c$$

is compatible (has solutions)?

Solution. We eliminate $x,\ y$: $\sigma_1 = a,\ \sigma_1^2 - 2\sigma_2 = b,\ \sigma_1^3 - 3\sigma_1\sigma_2 = c$ with the result $a^3 - 3ab + 2c = 0$.

(c) Polynomials with three variables have the elementary symmetric polynomials

$$\sigma_1 = x + y + z, \quad \sigma_2 = xy + yz + zx, \quad \sigma_3 = xyz.$$

The power sums $s_i = x^i + y^i + z^i,\ i = 0, 1, 2, \cdots$ can be represented by $\sigma_1,\ \sigma_2,\ \sigma_3$. Show that the following identities are valid:

$$\begin{aligned} s_0 &= x^0 + y^0 + z^0,\ s_1 = x + y + z = \sigma_1, \\ s_2 &= x^2 + y^2 + z^2 = \sigma_1^2 - 2\sigma_2, \\ s_3 &= x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3, \\ s_4 &= \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3, \\ x^2y + xy^2 + x^2z + xz^2 + y^2z + yz^2 &= \sigma_1\sigma_2 - 3\sigma_3,\ x^2y^2 + y^2z^2 + z^2x^2 \\ &= \sigma_2^2 - 2\sigma_1\sigma_3. \end{aligned}$$

Systems of equations which are symmetric in $x,\ y,\ z$ can be expressed through $\sigma_1,\ \sigma_2,\ \sigma_3$. As soon as we have $\sigma_1,\ \sigma_2,\ \sigma_3$, we find the solutions $u_1,\ u_2,\ u_3$ of the cubic equation $u^3 - \sigma_1 u^2 + \sigma_2 u - \sigma_3 = 0$. Then $(x_1, y_1, z_1) = (u_1, u_2, u_3)$ is one solution. We get the others by permuting the variables.

E10. *Solve the system of equations*

$$x + y + z = a, \quad x^2 + y^2 + z^2 = b^2, \quad x^3 + y^3 + z^3 = a^3.$$

We set $x + y + z = \sigma_1,\ xy + yz + zx = \sigma_2,\ xyz = \sigma_3$ and get

$$\begin{gathered} \sigma_1 = a, \quad \sigma_2 = \tfrac{1}{2}\left(a^2 - b^2\right), \quad \sigma_3 = \tfrac{1}{2}a\left(a^2 - b^2\right), \\ u^3 - au^2 + \tfrac{1}{2}\left(a^2 - b^2\right)u - \tfrac{1}{2}a\left(a^2 - b^2\right) = 0, \\ (u - a)\left[u^2 - \tfrac{1}{2}\left(b^2 - a^2\right)\right] = 0, \\ u_1 = a, \quad u_2 = \sqrt{\tfrac{b^2 - a^2}{2}}, \quad u_3 = -\sqrt{\tfrac{b^2 - a^2}{2}}. \end{gathered}$$

There are six solutions (u_1, u_2, u_3) and its permutations.

E11. *Find all real solutions of the system $x + y + z = 1,\ x^3 + y^3 + z^3 + xyz = x^4 + y^4 + z^4 + 1$.*

Introducing elementary symmetric polynomials yields $\sigma_1 = 1$, $x^3 + y^3 + z^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, $x^4 + y^4 + z^4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3$. For $\sigma_1 = 1$, the second equality becomes $2\sigma_2^2 - \sigma_2 + 1 = 0$, which has no solutions.

E12. *Given $2n$ distinct numbers $a_1, \ldots, a_n, b_1, \ldots, b_n$, an $n \times n$ table is filled as follows: into the cell in the ith row and jth column is written the number $a_i + b_j$. Prove that if the product of each column is the same, then also the product of each row is the same* (AUO 1991).

Consider the polynomial

$$f(x) = \prod_{i=1}^{n}(x + a_i) - \prod_{j=1}^{n}(x - b_j)$$

of degree less than n. If

$$f(b_j) = \prod_{i=1}^{n}(a_i + b_j) = c$$

for all $j = 1, \ldots, n$ then the polynomial $f(x) - c$ has at least n distinct roots. This implies $f(x) - c = 0$ for all x. But then

$$c = f(-a_i) = -\prod_{j=1}^{n}(-a_i - b_j) = (-1)^{n+1}\prod_{j=1}^{n}(a_i + b_j), \quad \text{QED.}$$

Problems

1. Factor $x^3 + y^3 + z^3 - 3xyz$ by elementary symmetric functions.
2. For which $a \in \mathbb{R}$ is the sum of the squares of the zeros of $x^2 - (a-2)x - a - 1$ minimal?
3. If x_1, x_2 are the zeros of the polynomial $x^2 - 6x + 1$, then for every nonnegative integer n, $x_1^n + x_2^n$ is an integer and not divisible by 5.
4. Given a monic polynomial $f(x)$ of degree n over $\mathbb{Z}$ and k, $p \in \mathbb{N}$, prove that if none of the numbers $f(k)$, $f(k+1), \ldots, f(k+p)$ is divisible by $p+1$, then $f(x) = 0$ has no rational solution.
5. The polynomial $x^{2n} - 2x^{2n-1} + 3x^{2n-2} - \cdots - 2nx + 2n + 1$ has no real roots.
6. $a, b, c \in \mathbb{R}$, $a + b + c > 0$, $bc + ca + ab > 0$, $abc > 0 \Rightarrow a, b, c > 0$.
7. A polynomial $f(x, y)$ is *antisymmetric*, if $f(x, y) = -f(y, x)$. Prove that every antisymmetric polynomial $f(x, y)$ has the form $f(x, y) = (x - y)g(x, y)$, where $g(x, y)$ is symmetric.
8. The polynomial $f(x, y, z)$ is antisymmetric if the sign changes on switching any two variables. Prove that every antisymmetric polynomial $f(x, y, z)$ can be written in the form $f(x, y, z) = (x - y)(x - z)(y - z)g(x, y, z)$, where $g(x, y, z)$ is symmetric.
9. If $f(x, y)$ is symmetric and $x - y | f(x, y)$, then $(x - y)^2 | f(x, y)$.

11

Functional Equations

Equations for unknown functions are called *functional equations*. We dealt with these already in the chapters on sequences and polynomials. Sequences and polynomials are just special functions.

Here are five examples of functional equations of a single variable:

$$f(x) = f(-x), \quad f(x) = -f(-x), \quad f \circ f(x) = x, \quad f(x) = f\left(\tfrac{x}{2}\right);$$
$$f(x) = \cos\tfrac{x}{2} f\left(\tfrac{x}{2}\right), \quad f(0) = 1, \quad f \text{ continuous.}$$

The first three properties characterize even functions, odd functions, and involutions, respectively. Many functions have the fourth property. On the other hand, the last condition makes the solution unique.

Here are examples of famous functional equations in two variables:

$$f(x+y) = f(x) + f(y), \quad f(x+y) = f(x)f(y), \quad f(xy) = f(x) + f(y),$$

and $f(xy) = f(x)f(y)$. These are *Cauchy's functional equations.*

$f\left(\frac{x+y}{2}\right) = \frac{f(x)+f(y)}{2}$. This is Jensen's functional equation.

$f(x+y) + f(x-y) = 2f(x)f(y)$. This is d'Alambert's functional equation.

$$g(x+y) = g(x)f(y) + f(x)g(y), \quad f(x+y) = f(x)f(y) - g(x)g(y),$$
$$g(x-y) = g(x)f(y) - g(y)f(x), \quad f(x-y) = f(x)f(y) + g(x)g(y).$$

The last four functional equations are the addition theorems for the trigonometric functions $f(x) = \cos x$ and $g(x) = \sin x$.

Usually a functional equation has many solutions, and it is quite difficult to find all of them. On the other hand it is often easy to find all solutions with

some additional properties, for example, all continuous, monotonic, bounded, or differentiable solutions.

Without additional assumptions, it may be possible to find only certain properties of the functions. We give some examples:

E1. First we consider the equation

$$f(xy) = f(x) + f(y). \tag{1}$$

One solution is easy to guess: $f(x) = 0$ for all x. This is the only solution which is defined for $x = 0$. If $x = 0$ belongs to the domain of f, then we can set $y = 0$ in (1), and we get $f(0) = f(x) + f(0)$, implying $f(x) = 0$ for all x. Let $x = 1$ be in the domain of f. With $x = y = 1$, we get $f(1) = 2f(1)$, or

$$f(1) = 0. \tag{2}$$

If both 1 and -1 belong to the domain, then f is an even function, i.e., $f(-x) = f(x)$ for all x. To prove this, we set $x = y = -1$ in (1), and because of (2), we get

$$f(1) = 2f(-1) = 0 \Rightarrow f(-1) = 0.$$

Setting $y = -1$ in (1), we get $f(-x) = f(x) + f(1)$, or

$$f(-x) = f(x) \quad \text{for all } x.$$

Assume that f is differentiable for $x > 0$. We keep y fixed and differentiate for x. Then we get $yf'(xy) = f'(x)$. For $x = 1$, one gets $yf'(y) = f'(1)$. Change of notation leads to $f'(x) = f'(1)/x$, or

$$f(x) = \int_1^x \frac{f'(1)}{t}\, dt = f'(1) \ln x.$$

If the function is also defined for $x < 0$, then we have $f(x) = f'(1) \ln |x|$.

E2. A famous classical functional equation is

$$f(x + y) = f(x) + f(y). \tag{1}$$

First, we try to get out of (1) as much information as possible without any additional assumptions. $y = 0$ yields $f(x) = f(x) + f(0)$, that is,

$$f(0) = 0. \tag{2}$$

For $y = -x$, we get $0 = f(x) + f(-x)$, or

$$f(-x) = -f(x). \tag{3}$$

Now we can confine our attention to $x > 0$. For $y = x$, we get $f(2x) = 2f(x)$, and by induction,

$$f(nx) = nf(x) \quad \text{for all } n \in \mathbb{N}. \tag{4}$$

For rational $x = \frac{m}{n}$, that is, $n \cdot x = m \cdot 1$, by (4) we get $f(n \cdot x) = f(m \cdot 1)$, $nf(x) = mf(1)$, and

$$f(x) = \frac{m}{n} f(1). \tag{5}$$

If we set $f(1) = c$, then, from (2), (3), (5), we get $f(x) = cx$ for rational x. That is all we can get without additional assumptions.

(a) Suppose f is continuous. If x is irrational, then we choose a rational sequence x_n with limit x. Because of the continuity of f, we have

$$f(x) = \lim_{x_n \to x} f(x_n) = \lim_{x_n \to x} cx_n = cx.$$

Then we have $f(x) = cx$ for all x.

(b) Let f be monotonically increasing. If x is irrational, then we choose an increasing and a decreasing sequence r_n and R_n of rational numbers, which converge toward x. Then we have

$$cr_n = f(r_n) \leq f(x) \leq f(R_n) = cR_n.$$

For $n \to \infty$, both cr_n and cR_n converge to cx. Thus $f(x) = cx$ for all x.

(c) Let f be bounded on $[a, b]$, that is,

$$|f(x)| < M \quad \text{for all } x \in [a, b].$$

We show that f is also bounded on $[0, b - a]$. If $x \in [0, b - a]$, then $x + a \in [a, b]$. From $f(x) = f(x + a) - f(a)$, we get

$$|f(x)| < 2M.$$

If we set $b - a = d$, then f is bounded on $[0, d]$. Let $c = f(d)/d$ and $g(x) = f(x) - cx$. Then

$$g(x + y) = g(x) + g(y).$$

Furthermore, we have $g(d) = f(d) - cd = 0$ and

$$g(x + d) = g(x) + g(d) = g(x),$$

that is, g is periodic with period d. As the difference of two bounded functions, g is also bounded on $[0, d]$. From the periodicity, it follows that g is bounded on the whole number line. Suppose there is an x_0, so that $g(x_0) \neq 0$. Then $g(nx_0) = ng(x_0)$. By choosing n sufficiently large, we can make $|ng(x_0)|$ as large as we want. This contradicts the boundedness of g. Hence, $g(x) = 0$ for all x, that is,

$$f(x) = cx \quad \text{for all } x.$$

In 1905 G. Hamel discovered "wild" functions that are nowhere bounded and also satisfy the functional equation $f(x + y) = f(x) + f(y)$. We are looking for "tame"

solutions. If we succeed in finding a solution for all rationals, then we can extend them to reals by continuity or monotonicity, etc.

E3. Another classical equation is

$$f(x+y) = f(x)f(y). \tag{1}$$

If there is an a such that $f(a) = 0$, then $f(x+a) = f(x)f(a) = 0$ for all x, that is, f is identically zero. For all other solutions, $f(x) \neq 0$ everywhere. For $x = y = t/2$, we get

$$f(t) = f^2\left(\frac{t}{2}\right) > 0.$$

The solutions we are looking for are everywhere positive. For $y = 0$, we get $f(x) = f(x)f(0)$ from (1), that is, $f(0) = 1$. For $x = y$, we get $f(2x) = f^2(x)$, and by induction

$$f(nx) = f^n(x). \tag{2}$$

Let $x = \frac{m}{n}$ $(m, n \in \mathbb{N})$, that is, $n \cdot x = m \cdot 1$. Applying (2), we get $f(nx) = f(m \cdot 1) \Rightarrow f^n(x) = f^m(1) \Rightarrow f(x) = f^{\frac{m}{n}}(1)$. If we set $f(1) = a$, then

$$f\left(\frac{m}{n}\right) = a^{\frac{m}{n}},$$

that is, $f(x) = a^x$ for rational x. With a weak additional assumption (continuity, monotonicity, boundedness), as in **E2**, we can show that

$$f(x) = a^x \quad \text{for all } x.$$

The following procedure is simpler: Since $f(x) > 0$ for all x, we can take logarithms in (1):

$$\ln \circ f(x+y) = \ln \circ f(x) + \ln \circ f(y).$$

Let $\ln \circ f = g$. Then $g(x+y) = g(x) + g(y) \Rightarrow g(x) = cx \Rightarrow \ln \circ f(x) = cx$, and

$$f(x) = e^{cx}.$$

E4. We treat the following equation more generally:

$$f(xy) = f(x) + f(y), \quad x, y > 0. \tag{1}$$

We set $x = e^u$, $y = e^v$, $f(e^u) = g(u)$. Then (1) is transformed into $g(u+v) = g(u) + g(v)$ with solution $g(u) = cu$, and $f(x) = c \ln x$, as in **E1**, where we used differentiability.

E5. Next we consider the last Cauchy equation

$$f(xy) = f(x)f(y). \tag{1}$$

We assume $x > 0$ and $y > 0$. Then we set $x = e^u$, $y = e^v$, $f(e^u) = g(u)$ and get $g(u + v) = g(u) + g(v)$ with the solution $g(u) = e^{cu} = (e^u)^c = x^c$.

$$f(x) = x^c$$

and with the trivial solution $f(x) = 0$ for all x.

If we require (1) for all $x \neq 0,\ y \neq 0$, then $x = y = t$ and $x = y = -t$ give

$$f^2(t) = f(t^2) = f(-t)f(-t)$$

and

$$f(-t) = \begin{cases} f(t) = t^c \quad (\text{or } 0), \\ -f(t) = -t^c. \end{cases}$$

In this case the general continuous solutions are

$$(a) \quad f(x) = |x|^c, \quad (b) \quad f(x) = \operatorname{sgn} x \cdot |x|^c, \quad (c) \quad f(x) = 0.$$

E6. Now we come to Jensen's functional equation

$$f\left(\frac{x+y}{2}\right) = \frac{f(x) + f(y)}{2}. \tag{1}$$

We set $f(0) = a$ and $y = 0$ and get $f\left(\frac{x}{2}\right) = \frac{f(x)+a}{2}$. Then

$$\frac{f(x) + f(y)}{2} = f\left(\frac{x+y}{2}\right) = \frac{f(x+y) + a}{2},$$
$$f(x + y) = f(x) + f(y) - a.$$

With $g(x) = f(x) - a$, we get $g(x + y) = g(x) + g(y)$, $g(x) = cx$, and

$$f(x) = cx + a.$$

E7. Now we come to our last and most complicated example

$$f(x + y) + f(x - y) = 2f(x)f(y). \tag{1}$$

We want to find the continuous solutions of (1). First we eliminate the trivial solution $f(x) = 0$ for all x. Now

$$y = 0 \Rightarrow 2f(x) = 2f(x)f(0) \Rightarrow f(0) = 1,$$
$$x = 0 \Rightarrow f(y) + f(-y) = 2f(0)f(y) \Rightarrow f(-y) = f(y),$$

that is, f is an even function. For $x = ny$, we get

$$f[(n + 1)y] = 2f(y)f(ny) - f[(n - 1)y]. \tag{2}$$

For $y = x$, we get $f(2x) + f(0) = 2f^2(x)$. From this we conclude with $t = 2x$ that

$$f^2\left(\frac{t}{2}\right) = \frac{f(t)+1}{2}. \tag{3}$$

(2) and (3) are satisfied by the functions cos and cosh. Since $f(0) = 1$ and f is continuous, we have $f(x) > 0$ in $[-a, a]$ for sufficiently small $a > 0$. Thus, $f(a) > 0$.

(a) *First case.* $0 < f(a) \leq 1$. Then there will be a c from $0 \leq c \leq \frac{\pi}{2}$, so that $f(a) = \cos c$. We show that, for any number of the form $x = (n/2^m)a$,

$$f(x) = \cos \frac{c}{a}x. \tag{4}$$

For $x = a$, this is valid by definition of c. Because of (3), for $x = a/2$,

$$f^2\left(\frac{a}{2}\right) = \frac{f(a)+1}{2} = \frac{\cos c + 1}{2} = \cos^2 \frac{c}{2}.$$

Because of $f(a/2) > 0$, $\cos \frac{c}{2} > 0$, we conclude that

$$f\left(\frac{a}{2}\right) = \cos \frac{c}{2}. \tag{5}$$

Suppose (5) is valid for $x = a/2^m$. Then (3) implies

$$f^2\left(\frac{a}{2^{m+1}}\right) = \frac{f\left(\frac{a}{2^m}\right)+1}{2} = \cos^2 \frac{c}{2^{m+1}}$$

or

$$f\left(\frac{a}{2^{m+1}}\right) = \cos \frac{c}{2^{m+1}},$$

that is, $f(a/2^m) = \cos(c/2^m)$ for every natural number m. Because of (2) for $n = 2$,

$$\begin{aligned} f\left(\frac{3}{2^m}a\right) = f\left(3 \cdot \frac{a}{2^m}\right) &= 2f\left(\frac{a}{2^m}\right) f\left(\frac{a}{2^{m-1}}\right) - f\left(\frac{a}{2^m}\right) \\ &= 2\cos \frac{c}{2^m} \cos \frac{c}{2^{m-1}} - \cos \frac{c}{2^m} = \cos \frac{3}{2^m} c. \end{aligned}$$

Since (4) is valid for $x = [(n-1)/2^m]a$ and $x = (n/2^m)a$, we conclude from (2) for $x = [(n-1)/2^m]a$ and $x = (n/2^m)a$, that

$$f\left(\frac{n+1}{2^m}a\right) = \cos \frac{n+1}{2^m} c.$$

Hence, we have

$$f\left(\frac{n}{2^m}a\right) = \cos \frac{n}{2^m} c \quad \text{for } n,\ m \in \{0, 1, 2, 3, \ldots\}.$$

Since f is continuous and even, we have

$$f(x) = \cos \frac{c}{a} x \quad \text{for all } x.$$

Second case. If $f(a) > 1$, then there is a $c > 0$, so that

$$f(a) = \cosh c.$$

One can show exactly as in the first case that

$$f(x) = \cosh \frac{c}{a} x \quad \text{for all } x.$$

Thus, the functional equation (1) has the following continuous solutions:

$$f(x) = 0, \quad f(x) = \cos bx, \quad f(x) = \cosh bx.$$

This list also contains $f(x) = 1$ for $b = 0$.

(b) We want to find all differentiable solutions of (1). Since differentiability is a far more powerful property than continuity, it will be quite easy to find all solutions of $f(x+y) + f(x-y) = 2f(x)f(y)$. We differentiate twice with respect to each variable:

With respect to x: $f''(x+y) + f''(x-y) = 2f''(x)f(y)$.
With respect to y: $f''(x+y) + f''(x-y) = 2f(x)f''(y)$.

From both equations we conclude that

$$f''(x) \cdot f(y) = f(x) \cdot f''(y) \Rightarrow \frac{f''(x)}{f(x)} = \frac{f''(y)}{f(y)} = c \Rightarrow f''(x) = cf(x),$$
$$c = -\omega^2 \Rightarrow f(x) = a \cos \omega x + b \sin \omega x,$$
$$c = \omega^2 \Rightarrow f(x) = a \cosh \omega x + b \sinh \omega x.$$

$f(0) = 1$ and $f(-x) = f(x)$ result in $f(x) = \cos \omega x$ and $f(x) = \cosh \omega x$, respectively.

Problems

1. Find some (all) functions f with the property $f(x) = f\left(\frac{x}{2}\right)$ for all $x \in \mathbb{R}$.
2. Find all continuous solutions of $f(x+y) = g(x) + h(y)$.
3. Find all solutions of the functional equation $f(x+y) + f(x-y) = 2f(x)\cos y$.
4. The function f is periodic, if, for fixed a and any x,

$$f(x+a) = \frac{1 + f(x)}{1 - f(x)}.$$

5. Find all polynomials p satisfying $p(x+1) = p(x) + 2x + 1$.

6. Find all functions f which are defined for all $x \in \mathbb{R}$ and, for any $x,\ y$, satisfy

$$xf(y) + yf(x) = (x + y)f(x)f(y).$$

7. Find all real, not identically vanishing functions f with the property

$$f(x)f(y) = f(x - y) \quad \text{for all } x,\ y.$$

8. Find a function f defined for $x > 0$, so that $f(xy) = xf(y) + yf(x)$.
9. The rational function f has the property $f(x) = f(1/x)$. Show that f is a rational function of $x + 1/x$.

   Remark. A rational function is the quotient of two polynomials.
10. Find all "tame" solutions of $f(x + y) + f(x - y) = 2[f(x) + f(y)]$.
11. Find all "tame" solutions of $f(x + y) - f(x - y) = 2f(y)$.
12. Find all "tame" solutions of $f(x + y) + f(x - y) = 2f(x)$.
13. Find all tame solutions of

$$f(x + y) = \frac{f(x)f(y)}{f(x) + f(y)}.$$

14. Find all tame solutions of $f^2(x) = f(x + y)f(x - y)$. Note the similarity to 11.
15. Find the function f which satisfies the functional equation

$$f(x) + f\left(\frac{1}{1 - x}\right) = x \quad \text{for all } x \neq 0,\ 1.$$

16. Find all continuous solutions of $f(x - y) = f(x)f(y) + g(x)g(y)$.
17. Let f be a real-valued function defined for all real numbers x such that, for some positive constant a, the equation

$$f(x + a) = \frac{1}{2} + \sqrt{f(x) - f^2(x)}$$

   holds for all x.

   (a) Prove that the function f is periodic, i.e., there exists a positive number b such that $f(x + b) = f(x)$ for all x.

   (b) For $a = 1$, give an example of a nonconstant function with the required properties (IMO 1968).
18. Find all continuous functions satisfying $f(x + y)f(x - y) = [f(x)f(y)]^2$.
19. Let $f(n)$ be a function defined on the set of all positive integers and with all its values in the same set. Prove that if

$$f(n + 1) > f[f(n)]$$

   for each positive integer n, then $f(n) = n$ for each n (IMO 1977).
20. Find all continuous functions in 0 which satisfy the relations

$$f(x + y) = f(x) + f(y) + xy(x + y), \quad x,\ y \in \mathbb{R}.$$

21. Find all functions f defined on the set of positive real numbers which take positive real values and satisfy the conditions:

$$\text{(i)} \quad f[xf(y)] = yf(x) \quad \text{for all positive } x,\ y;$$
$$\text{(ii)} \quad f(x) \to 0 \quad \text{as} \quad x \to \infty \quad \text{(IMO 1983)}.$$

22. Find all functions f, defined on the nonnegative real numbers and taking nonnegative real values, such that

$$\text{(i)} \quad f[xf(y)]\, f(y) = f(x+y) \quad \text{for all } x,\ y \geq 0;$$
$$\text{(ii)} \quad f(2) = 0;$$
$$\text{(iii)} \quad f(x) \neq 0 \quad \text{for } 0 \leq x < 2 \quad \text{(IMO 1986)}.$$

23. Find a function $f : \mathbb{Q}^+ \mapsto \mathbb{Q}^+$, which satisfies, for all $x,\ y \in \mathbb{Q}^+$, the equation

$$f(xf(y)) = f(x)/y \quad \text{(IMO 1990)}.$$

24. Find all functions $f : \mathbb{R} \mapsto \mathbb{R}$ such that

$$f\left[x^2 + f(y)\right] = y + [f(x)]^2 \quad \text{for all } x,\ y \in \mathbb{R} \quad \text{(IMO 1992)}.$$

25. Does there exist a function $f : \mathbb{N} \mapsto \mathbb{N}$ such that

$$f(1) = 2,\ f[f(n)] = f(n)+n,\ f(n) < f(n+1) \quad \text{for all } n \in \mathbb{N} \text{ (IMO 1993)?}$$

26. Find all continuous functions $f : \mathbb{R} \mapsto \mathbb{R}_+$ which transform three terms of the arithmetic progression $x,\ x+y,\ x+2y$ into corresponding terms $f(x),\ f(x+y),\ f(x+2y)$ of a geometric progression, that is,

$$[f(x+y)]^2 = f(x) \cdot f(x+2y).$$

27. Find all continuous functions f satisfying $f(x+y) = f(x) + f(y) + f(x)f(y)$.
28. Guess a simple function f satisfying $f^2(x) = 1 + xf(x+1)$.
29. Find all continuous functions which transform three terms of an arithmetic progression into three terms of an arithmetic progression.
30. Find all continuous functions f satisfying $3f(2x+1) = f(x) + 5x$.
31. Which function is characterized by the equation $xf(x) + 2xf(-x) = -1$?
32. Find the class of continuous functions satisfying $f(x+y) = f(x) + f(y) + xy$.
33. Let $a \neq \pm 1$. Solve $f(x/(x-1)) = af(x) + \phi(x)$, where $\phi(x)$ is a given function, which is defined for $x \neq 1$.
34. The function f is defined on the set of positive integers as follows:

$$f(1) = 1, \quad f(3) = 3, \quad f(2n) = f(n),$$
$$f(4n+1) = 2f(2n+1) - f(n), \quad f(4n+3) = 3f(2n+1) - 2f(n).$$

Find all values of n with $f(n) = n$ and $1 \leq n \leq 1988$ (IMO 1988).

12

Geometry

12.1 Vectors

12.1.1 Affine Geometry

We consider the space with any number of dimensions. For competitions only 2 or 3 dimensions will be relevant. Points of the space will be denoted by capital letters A, B, C .... One point will be distinguished and will be denoted by O (for origin). The most important mappings of the space are the *translations* or *vectors*. A translation T is determined by any point X and its map $T(X) = Y$. The translation taking point A into B is denoted by $\overrightarrow{AB}$. It is usual practice to use O as the first point. The translation taking O to A is then $\overrightarrow{OA}$. Since O is always the same point, we drop it and get $\vec{A}$. After a while one also drops the arrow on A and gets the point A. We simply identify points A and their vectors beginning in O and ending in A. We need not distinguish between points and vectors since all that is valid for points is also valid for vectors.

Now we define *addition* of two points A, B and *multiplication* of a point A by a real number t.

$$A + B = \text{reflection of the origin } O \text{ at the midpoint } M \text{ of } (A, B).$$

The point tA lies on the line OA. Its distance from O is $|t|$ times the distance of A. For $t < 0$ both A and tA are separated by O. For $t > 0$ they lie on the same side of O. For this reason multiplication with a real number is also called a *stretch* from O by the factor t. For the points (vectors) of the space, we have the following

properties (vector space axioms):

$$(A + B) + C = A + (B + C) \quad \text{for all } A,\ B,\ C, \tag{1}$$
$$A + O = A \quad \text{for all } A, \tag{2}$$
$$A + (-A) = O \quad \text{for all } A, \tag{3}$$
$$A + B = B + A \quad \text{for all } A,\ B, \tag{4}$$

and

$$(st)A = (ts)A \quad \text{for all real } s, t, \text{ and all } A, \tag{5}$$
$$t(A + B) = tA + tB, \tag{6}$$
$$(s + t)A = sA + tA, \tag{7}$$
$$1 \cdot A = A. \tag{8}$$

Let A be a fixed point. The function $T : Z \mapsto A + Z$ is a translation by A. Fig. 12.1 shows that $2M = A + B$, that is, the midpoint of (A, B) is

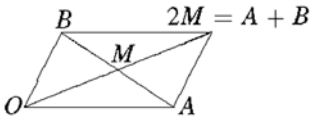


Fig. 12.1

$$M = \tfrac{A+B}{2}.$$
$$(A, B, C, D) \quad \text{a parallelogram} \iff \tfrac{A+C}{2} = \tfrac{B+D}{2} \iff A + C = B + D.$$

We note the fundamental rule

$$\overrightarrow{AB} = B - A.$$

Indeed, apply to (A, B) the translation which sends A to O. It will send B to $B - A$. Thus, $\overrightarrow{AB}$ is the same translation as $B - A$.

$$A \text{ is the midpoint of } (Z, Z') \iff \frac{Z + Z'}{2} = A \iff Z' = 2A - Z.$$

The function $H_A : Z \mapsto 2A - Z$ is a *reflection* at A or a *half-turn* about A. We have

$$Z \overset{H_A}{\longmapsto} 2A - Z \overset{H_B}{\longmapsto} 2B - (2A - Z) = 2(B - A) + Z.$$

So $H_A \circ H_B = 2\overrightarrow{AB}$, and

$$H_A \circ H_B \circ H_C : Z \overset{H_C}{\longmapsto} 2C - (2B - 2A + Z),$$

or $H_A \circ H_B \circ H_C = H_D$ where H_D is the half-turn about $D = A - B + C$. Since $A + C = B + D$, the quadruple (A, B, C, D) is a parallelogram.

E1. *The midpoints P, Q, R, S of any quadrilateral in plane or space are vertices of a parallelogram.*

Indeed,

$$P = \frac{A+B}{2}, \quad R = \frac{C+D}{2} \Rightarrow P + R = \frac{A+B+C+D}{2},$$
$$Q = \frac{B+C}{2}, \quad S = \frac{A+D}{2} \Rightarrow Q + S = \frac{A+B+C+D}{2}.$$

Thus, $P + R = Q + S \iff (P, Q, R, S)$ a parallelogram.

E2. *Reconstruct a pentagon from the midpoints P, Q, R, S, T of its sides.*

We denote H_A simply by A. Then $P \circ Q \circ R = X$, where X is the fourth parallelogram vertex to the triple (P, Q, R). Furthermore $X \circ S \circ T = A$. Thus, we have constructed A. The remaining vertices can be found by reflections in P, Q, R, S. This construction works for any polygon with $(2n + 1)$ vertices, but not for polygons with $2n$ vertices. Successive reflections in the midpoints leave the first vertex A_1 fixed. But the product of $2n$ reflections is a translation. Since it has a *fixed point*, it must be the identity mapping. So, any point of the plane can be chosen for vertex A_1.

Suppose C lies on line AB.Then $\overrightarrow{AC} = t \cdot \overrightarrow{AB}$, or $C - A = t(B - A)$, or

$$C = A + t(B - A), \quad \text{and all real } t.$$

In $\triangle ABC$, let $D = (A + B)/2$ be the midpoint of AB, and let S be such that $\overrightarrow{CS} = 2\overrightarrow{CD}/3$. Then

$$S - C = \frac{2}{3}(D - C) = \frac{2}{3} \cdot \frac{A+B}{2} - \frac{2}{3}C \Rightarrow S = \frac{A+B+C}{3}.$$

S is called the *centroid* of ABC. Since it is symmetric with respect to A, B, C, we conclude that the medians of a triangle intersect in S and are divided by S in the ratio $2 : 1$.

E3. *Let $ABCDEF$ be any hexagon, and let $A_1B_1C_1D_1E_1F_1$ be the hexagon of the centroids of the triangles ABC, BCD, CDE, DEF, EFA, FAB. Then the $A_1B_1C_1D_1E_1F_1$ has parallel and equal opposites sides.*

Solution. We want to prove that $\overrightarrow{A_1B_1} = \overrightarrow{E_1D_1} \iff B_1 - A_1 = D_1 - E_1$, that is, $A_1 + D_1 = B_1 + E_1$. Indeed, we have

$$A_1 = \frac{A+B+C}{3}, \quad D_1 = \frac{D+E+F}{3},$$
$$B_1 = \frac{B+C+D}{3}, \quad E_1 = \frac{E+F+A}{3}.$$

This implies that

$$A_1 + D_1 = B_1 + E_1 = \frac{A+B+C+D+E+F}{3}.$$

E4. *Let $ABCD$ be a quadrilateral, and let $A'B'C'D'$ be the quadrilateral of the centroids of BCD, CDA, DAB, ABC. Show that $ABCD$ can be transformed into $A'B'C'D'$ by a stretch from some point Z. Find Z and the stretch factor t.*

Solution. We have

$$\overrightarrow{A'B'} = B' - A' = \frac{A+C+D}{3} - \frac{B+C+D}{3} = \frac{A-B}{3} = -\frac{\overrightarrow{AB}}{3}.$$

Similarly, we get $\overrightarrow{B'C'} = -\overrightarrow{BC}/3$, $\overrightarrow{C'D'} = -\overrightarrow{CD}/3$, $\overrightarrow{D'A'} = -\overrightarrow{DA}/3$.

For the center Z, we get $\overrightarrow{ZA'} = -\overrightarrow{ZA}/3$, or $A' - Z = -(A - Z)/3$, or $A + 3A' = 4Z$, or

$$Z = \frac{A+B+C+D}{4}.$$

Because of the symmetry of Z with respect to A, B, C, D we always get the same point Z.

E5. *Find the centroid S of n points $A_1, \ldots, A_n$ defined by*

$$\sum_{i=1}^{n} \overrightarrow{SA_i} = \overrightarrow{O}.$$

Solution. From this equation, we get $(A_1 - S) + \cdots + (A_n - S) = O$ and

$$S = \frac{A_1 + \cdots + A_n}{n}.$$

12.1.2 Scalar or Dot Product

Let us introduce rectangular coordinates in space. The points A and B are now

$$A = (a_1, \cdots, a_n), \quad B = (b_1, \ldots, a_n).$$

We define the *scalar* or *dot product* as follows:

$$A \cdot B = \sum_{i=1}^{n} a_i b_i,$$

which is a real number. This definition implies

S1. $A \cdot B = B \cdot A$.

S2. $A \cdot (B + C) = A \cdot B + A \cdot C, \quad (tA) \cdot B = A \cdot (tB) = t(A \cdot B)$.

S3. $A = 0 \Rightarrow A \cdot A = 0$, otherwise $A \cdot A > 0$.

We define the *norm* or *length* of the vector A by

$$|A| = \sqrt{A \cdot A} = \sqrt{a_1^2 + \cdots, +a_n^2}$$

and the *distance* of the points A and B by

$$|A - B| = \sqrt{(A - B) \cdot (A - B)}.$$

For 2 and 3 dimensions, it is easy to show that

$$A \cdot B = |A| \cdot |B| \cdot \cos(\hat{AB}).$$

For $n > 3$, this becomes the definition of $\cos(\hat{AB})$. Now we have

$$A \perp B \iff A \cdot B = 0.$$

With the scalar product, we prove some classical geometric theorems.

E6. *The diagonals of a quadrilateral are orthogonal if and only if the sums of the squares of opposite sides are equal.*

We can write the theorem in the form

$$C - A \perp B - D \iff (B - A)^2 + (C - D)^2 = (B - C)^2 + (A - D)^2.$$

Prove this by transforming, equivalently, the right side into the left.

A *median* of a triangle connects a vertex with the midpoint of the opposite side. A *median* of a quadrilateral connects the midpoints of two opposite sides.

E7. *The diagonals of a quadrilateral are orthogonal iff its medians have equal length.*

Solution. Let MK and NL be the medians. Then we can express this theorem as follows: $\overrightarrow{AC} \perp \overrightarrow{BD} \Leftrightarrow |MK|^2 = |NL|^2$.

To prove the theorem, we apply a sequence of equivalence transformations to the right-hand side (RHS) until we get the left-hand side (LHS).

$$\left(\frac{C + D}{2} - \frac{A + B}{2}\right)^2 - \left(\frac{A + D}{2} - \frac{B + C}{2}\right)^2 = (C - A) \cdot (D - B)$$
$$= \overrightarrow{AC} \cdot \overrightarrow{BD} = 0.$$

E8. *Let A, B, C, D be four points in space. Then we always have*

$$|AB|^2 + |CD|^2 - |BC|^2 - |AD|^2 = 2\overrightarrow{AC} \cdot \overrightarrow{DB}.$$

To prove this, we transform the LHS equivalently to get the RHS:

$$\begin{aligned}(B - A)^2 + (D - C)^2 - (B - C)^2 - (A - D)^2 \\ = 2(B \cdot C + A \cdot D - A \cdot B - C \cdot D) \\ = 2(C - A) \cdot (B - D) = 2\overrightarrow{AC} \cdot \overrightarrow{DB}.\end{aligned}$$

Some consequences of this theorem are the following:

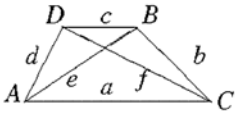


Fig. 12.2

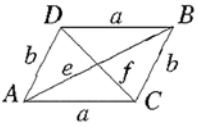


Fig. 12.3

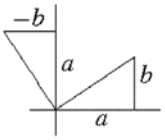


Fig. 12.4

- In a tetrahedron $AC \perp BD \iff |AB|^2 + |CD|^2 = |BC|^2 + |AD|^2$.
- Application of the theorem to the trapezoid in Fig. 12.2 yields

$$e^2 + f^2 = b^2 + d^2 + 2ac.$$

- The application to the parallelogram in Fig. 12.3 yields $e^2 + f^2 = 2(a^2 + b^2)$, that is, *in a parallelogram, the sum of the squares of the diagonals is equal to the sum of the squares of the sides*. We will show later that this property characterizes parallelograms.
- With the last theorem, we can easily express the length s_a of the median of a triangle ABC. Reflect A at the midpoint of BC to D. You get parallelogram $ABDC$ with diagonals $2s_a$ and a. The main parallelogram theorem gives

$$a^2 + 4s_a^2 = 2b^2 + 2c^2 \quad \text{or} \quad s_a^2 = \frac{1}{4}\left(2b^2 + 2c^2 - a^2\right).$$

  Similarly,

$$s_b^2 = \frac{1}{4}\left(2a^2 + 2c^2 - b^2\right), \quad s_c^2 = \frac{1}{4}\left(2a^2 + 2b^2 - c^2\right).$$

- Let S be the centroid of $\triangle ABC$. From the last theorem, one easily proves that $AS \perp BS \iff a^2 + b^2 = 5c^2$.

12.1.3 *Complex Numbers*

Now we restrict ourselves to the plane. In the plane we will call points *complex numbers*, and we denote them by small letters like a, b, c, ... Point z in the plane can be represented in the form $z = xe_1 + ye_2$, where e_1 and e_2 are unit points on the axes. Now e_1 is our real unit, nothing new. But what about e_2? Multiplication by e_2 should have a geometric meaning. Since $e_2e_1 = e_2$, we conclude that e_2 rotates e_1 by 90°. We simply define that e_2 also rotates the vector e_2 by 90°. Thus, $e_2 \cdot e_2 = -e_1$. Now we want to see what happens if $z = xe_1 + ye_2$ is multiplied by e_2:

$$e_2 z = e_2(xe_1 + ye_2) = xe_2 + ye_2e_2 = -ye_1 + xe_2.$$

Fig. 12.4 shows that multiplication by e_2 rotates the vector z by 90° counterclockwise.

From now on, we set $e_1 = 1$ and $e_2 = i$. Then $z = x + iy$, $i^2 = -1$. It is easy to show that complex numbers are a field with respect to addition and multiplication.

This means that you can calculate with them as with real numbers. But you may not compare them with respect to order. $a < b$ cannot be defined if you want the usual ordering properties to be satisfied.

We know that multiplication by i is a rotation of the plane by 90°. We can find the formula for the rotation about any point a by 90°. In fact,

$$z' = a + i(z - a).$$

Indeed, translate a to the origin. Then z goes to $z - a$. Rotate by 90° to get $i(z - a)$. Now translate back to get $z' = a + i(z - a)$. We can use this result to solve a simple classical problem:

E9. *Someone found in his attic an old description of a pirate, who died long ago. It read as follows: Go to the island X, start at the gallows, go to the elm tree, and count the steps. Then turn left by 90°, and go the same number of steps until point g'. Again, go from the gallows to the fig tree, and count the steps. Then turn right by 90°, and go the same number of steps to the point g''. A treasure is buried in the midpoint t of $g'g''$.*

A man went to the island and found the elm tree e and the fig tree f. But the gallows could not be traced. Find the treasure point t.

Fig. 12.5 tells us that

$$g' = e + i(e - g),\ g'' = f + i(g - f),\ t = \frac{g' + g''}{2} = \frac{e + f}{2} + i\frac{e - f}{2}.$$

This is easy to interpret geometrically. $m = (e + f)/2$ is the midpoint of the segment ef. Furthermore, $\overrightarrow{me} = (e - f)/2$. This vector must be rotated by 90° counterclockwise to get $\overrightarrow{mt}$. The location of the gallows does not matter.

Multiplication $z \mapsto az$ is a rotation about the origin O combined with a stretch from O with factor $|a|$. The rotational angle is the angle of vector a with the positive x-axis. This is easy to prove. If we do it without using trigonometry, then we get trigonometry for nothing.

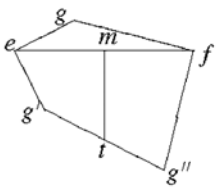


Fig. 12.5

Let $e(\alpha)$ be the unit vector in the direction α, $|e(\alpha)| = 1$. Then

$$e(\alpha) \cdot e(\beta) = e(\alpha + \beta). \tag{1}$$

Now we can define the trigonometric functions sin and cos as follows:

$$e(\alpha) = \cos\alpha + i\sin\alpha, \tag{2}$$

$$e(-\alpha) = \cos\alpha - i\sin\alpha = \overline{e(\alpha)} = 1/e(\alpha). \tag{3}$$

Now we prove some classical theorems with complex numbers.

E10. Napoleonic Triangles. *If one erects regular triangles outwardly (inwardly) on the sides of a triangle, then their centers are vertices of a regular triangle (outer and inner Napoleonic triangles).*

Let $\epsilon = e(60°) = (1 + \sqrt{3}i)/2$ be the sixth unit root, i.e., $\epsilon^6 = 1$ and

$$1 - \epsilon + \epsilon^2 = 0, \quad \epsilon^2 = \epsilon - 1, \quad \epsilon^3 = -1,$$
$$\overline{\epsilon} = e(-60°) = \tfrac{1-i\sqrt{3}}{2}, \quad \epsilon + \overline{\epsilon} = 1.$$

In Fig. 12.6, we have $b_0 = a + (c - a)\epsilon$, $c_0 = b + (a - b)\epsilon$, $a_0 = c + (b - c)\epsilon$.

$$\begin{aligned} 3(a_1 - c_1) &= c_0 - b_0 + c - a = 2c - a - b + (2b - a - c)\epsilon, \\ 3(b_1 - c_1) &= a_0 - b_0 + c - b = a + c - 2b + (b + c - 2a)\epsilon, \\ 3(a_1 - c_1)\epsilon &= \epsilon(2c - a - b) + (\epsilon - 1)(2b - a - c) \\ &= a + c - 2b + \epsilon(b + c - 2a) = 3(b_1 - c_1). \end{aligned}$$

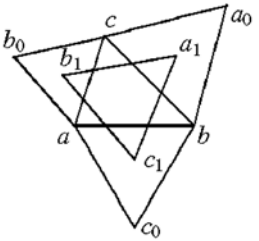


Fig. 12.6. Napoleonic triangles.

E11. *Squares are erected outwardly on the sides of a quadrilateral. If the centers of the squares are x, y, z, u, then the segments xz and yu are perpendicular and of equal length.*

$$x = \frac{a+b}{2} + i\frac{a-b}{2}, \quad y = \frac{b+c}{2} + i\frac{b-c}{2},$$
$$z = \frac{c+d}{2} + i\frac{c-d}{2}, \quad u = \frac{d+a}{2} + i\frac{d-a}{2}.$$
$$z - x = \frac{c+d-a-b}{2} + i\frac{c-d-a+b}{2},$$
$$u - y = \frac{a+d-b-c}{2} + i\frac{c+d-a-b}{2}, \quad u - y = i(z - x).$$

The last equation tells us that we get $\overrightarrow{yu}$ by rotating $\overrightarrow{xz}$ by 90°.

E12. *Squares $cbqp$ and $acmn$ are erected outwardly on the sides bc and ac of the triangle abc. Show that the midpoints d, e of these squares, the midpoint g of ab, and the midpoint f of mp are vertices of a square.*

This is a routine problem. Indeed, $gefd$ is a parallelogram since its vertices are midpoints of the sides of the quadrilateral $abpm$. We have just to show that eg and gd are perpendicular and of equal length. Indeed

$$g = \frac{a+b}{2}, \quad d = \frac{b+c}{2} + i\frac{b-c}{2}, \quad e = \frac{a+c}{2} + i\frac{c-a}{2},$$
$$d - g = \frac{c-a}{2} + i\frac{b-c}{2}, \quad e - g = \frac{c-b}{2} + i\frac{c-a}{2},$$
$$(d-g)i = \frac{c-b}{2} + i\frac{c-a}{2} = e - g.$$

E13. *Let $a_1b_1c_1$ and $b_1b_2b_3$ be two, positively oriented, regular triangles and let c_i be the midpoint of a_ib_i. Then $c_1c_2c_3$ is a regular triangle.*

Let $a_1 = a$, $b_1 = b$, $c_1 = a + \epsilon(b-a)$. The fact that $a_1b_1c_1$ is regular has already been incorporated. We do the same with $b_1b_2b_3$: $b_1 = c$, $b_2 = d$, $b_3 = c + \epsilon(d-c)$. Now

$$c_1 = \frac{a+c}{2}, \quad c_2 = \frac{b+d}{2}, \quad c_3 = \frac{a+c}{2} + \epsilon\frac{b+d-a-c}{2}.$$

Furthermore,

$$c_2 - c_1 = \frac{b+d-a-c}{2}, \quad c_3 - c_1 = \epsilon\frac{b+d-a-c}{2}, \quad c_3 - c_1 = \epsilon(c_2 - c_1).$$

E14. *Let A, B, C, D be four points in a plane. Then*

$$|AB| \cdot |CD| + |BC| \cdot |AD| \geq |AC| \cdot |BD| \quad \textit{(Ptolemy's inequality).}$$

There is equality iff A, B, C, D in this order lie on a circle or on a straight line.

Proof. For any four points z_1, z_2, z_3, z_4 in the plane, we have the identity

$$(z_2 - z_1)(z_4 - z_3) + (z_3 - z_2)(z_4 - z_1) = (z_3 - z_1)(z_4 - z_2).$$

The triangle inequality $|z_1| + |z_2| \geq |z_1 + z_2|$ implies that

$$|z_2 - z_1| \cdot |z_4 - z_3| + |z_3 - z_2| \cdot |z_4 - z_1| \geq |z_3 - z_1| \cdot |z_4 - z_2|$$

or

$$|AB| \cdot |CD| + |BC| \cdot |AD| \geq |AC| \cdot |BD|.$$

We have equality iff $(z_2 - z_1)(z_4 - z_3)$ and $(z_3 - z_2)(z_4 - z_1)$ have the same direction, i.e., their quotient is real and positive. Denote the arguments of $(z_2 - z_1)/(z_4 - z_1)$ and $(z_4 - z_3)/(z_3 - z_2)$ by α and μ, respectively. Then

$$\frac{z_2 - z_1}{z_4 - z_1} \cdot \frac{z_4 - z_3}{z_3 - z_2} \quad \text{is a positive real} \Rightarrow \alpha + \mu = 0°,$$

- *The sum of the lengths of a space diagonal starting at some point and the edges is greater then the sum of the face diagonals starting at the same point.*
- $|\vec{a}+\vec{b}+\vec{c}|+|\vec{a}|+|\vec{b}|+|\vec{c}| > |\vec{a}+\vec{b}|+|\vec{b}+\vec{c}|+|\vec{c}+\vec{a}|$ (ATMO 1972).

42. Equilateral triangles are erected to the outside on the sides of a convex quadrilateral. Prove that the segment PQ joining the vertices of ABP and CDQ is perpendicular to the segment RS joining the centers of the two other triangles, and, in addition, $|PQ| = \sqrt{3}|RS|$.

43. A point P_0 and a triangle $A_1A_2A_3$ are given in a plane. Let us set $A_s = A_{s-3}$ for all $s \geq 4$. We construct the sequence $P_0, P_1, P_2, \ldots$ of points, so that the point P_{k+1} is the map of P_k rotated around A_{k+1} by 120° clockwise (mathematically negative sense) ($k = 0, 1, 2, \ldots$). Show that if $P_{1986} = P_0$, then triangle $A_1A_2A_3$ is regular (IMO 1986).

44. Construct regular hexagons on the sides of a centrally symmetric hexagon. Their centers form the vertices of a regular hexagon. (A special case of a theorem of A. Barlotti.)

45. Equilateral triangles ABK, BCL, CDM, DAN are constructed inside the square $ABCD$. Prove that the midpoints of the four segments KL, LM, MN, NK and the midpoints of the eight segments AK, BK, BL, CL, CM, DM, DN, AN are the twelve vertices of a regular dodecagon.

Solutions

1. Expanding and collecting terms in the LHS of the equivalence yields $(A+C-B-D)^2 = 0$, or $A+C = B+D$, i.e., $ABCD$ is a parallelogram.

2. Routine transformation yields $A^2+C^2-B^2-D^2 = 2X(A+C-B-D)$. This is valid for all points X of the plane iff

$$A+C = B+D, \tag{1}$$

and

$$A^2+C^2 = B^2+D^2. \tag{2}$$

From (1) we get

$$(A+C)^2 = (B+D)^2 \iff A^2+C^2+2A\cdot C = B^2+D^2+2B\cdot D. \tag{3}$$

Subtracting (2) from (3), we get

$$2A\cdot C = 2B\cdot D. \tag{4}$$

Subtracting (4) from (2), we get $(A-C)^2 = (B-D)^2$, i.e., the parallelogram has equal diagonals. Hence it is a rectangle. We have shown that this property characterizes rectangles. This will be useful in several later problems, e.g., the next one.

37. Let P, Q and R be the midpoints of BD, BE, and AC, respectively. Then

$$r = \frac{a+c}{2}, \quad p = \frac{2b+(a-b)\epsilon}{2}, \quad q = \frac{b+c+(b-c)\epsilon}{2},$$
$$p - r = \frac{2b-a-c+(a-b)\epsilon}{2}, \quad q - r = \frac{b-a+(b-c)\epsilon}{2},$$
$$(p-r)\epsilon = \frac{b-a+(b-c)\epsilon}{2}.$$

Since $q - r = (p - r)\epsilon$, the triangle pqr is regular.

38. Assign the complex numbers a, b, c, o to A, B, C, D, respectively. Then setting

$$s = \frac{|AC|}{|AD|} = \frac{|BC|}{|BD|}, \quad \angle CAD = \alpha,$$

we get $a - c = se^{i\alpha}a$, $c - b = sie^{i\alpha}b$, and hence $c = a(1 - e^{i\alpha}) = b(1 + ise^{i\alpha})$, $(a-b)c = s(e^{i\alpha}ac + ie^{i\alpha}bc) = sab\left[e^{i\alpha}(1 + sie^{i\alpha}) + ie^{i\alpha}(1 - se^{i\alpha})\right] = sabe^{i\alpha}(1 + i)$. Thus, $|AB| \cdot |CD| = |a - b| \cdot |c| = s|a| \cdot |b|\sqrt{2} = |AC| \cdot |BD| \cdot \sqrt{2}$, that is,

$$\frac{|AB| \cdot |CD|}{|AC| \cdot |BD|} = \sqrt{2}.$$

12.2 Transformation Geometry

In this section *isometries* and *similarities* and their concatenations are used to prove theorems or to solve problems. Problems solvable by vectors or complex numbers are usually good examples for transformation geometric methods. In fact, vectors are translations, a simple type of isometry. Multiplication by a complex number is a stretch from O combined with a rotation about O.

Isometries are one-to-one transformations of a plane (or space) which *preserve distance*. In a plane, *direct* isometries preserve *sense*. They are *translations* and *rotations*. The *opposite* isometries are not sense-preserving. They are *line reflections* and *glide reflections*. The last one is hardly ever used in competitions. A translation has no fixed point except the identity, which has nothing but fixed points. A rotation has just one fixed point. Among the opposite isometries the line reflection has a whole line of fixed points. The glide reflection has none if it is not a reflection. Every direct isometry is the concatenation of two line reflections. An opposite isometry can be represented as a composition of one or three line reflections.

Rotation around point P with angle 2ϕ is the concatenation of two line reflections with the lines passing through P and forming angle ϕ. A translation is the product of two line reflections in parallel mirrors. The direction of the translation is orthogonal to the lines, and its distance is twice the distance of the parallel lines. A product of two half-turns about A and B is the translation $2\overrightarrow{AB}$.

We give some examples of the use of transformation geometry.

E1. Napoleonic Triangles. *Erect outwardly (inwardly) isosceles triangles with vertices P, Q, R and vertex angles* 120° *on the sides AC, BC, AB of a triangle. Prove that* $\triangle PQR$ *is regular.*

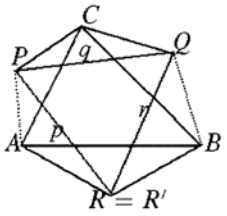


Fig. 12.15

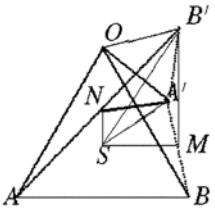


Fig. 12.16

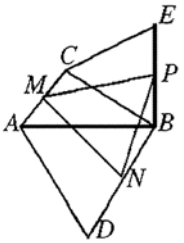


Fig. 12.17

Look at Fig. 12.15. $P_{120^\circ} \circ Q_{120^\circ} \circ R_{120^\circ} = I$, since it is a translation with fixed point A, i.e., the identity mapping. Hence $P_{120^\circ} \circ Q_{120^\circ} = R_{-120^\circ}$. Now construct the regular triangle with base PQ and vertex R'. Then

$$P_{120^\circ} \circ Q_{120^\circ} = p \circ q \circ q \circ r = p \circ r = R'_{-120^\circ}.$$

Thus, $R_{-120^\circ} = R'_{-120^\circ}$, which is the same rotation with the same fixed point, that is, $R = R'$.

E2. Again we solve problem 31, Chapter 12.2 (IMO jury 1977). In Fig. 12.16, dilatation from B with factor 2 and then rotation about O by 60° moves M to B' and leaves S fixed. Hence $\angle MSB' = 60^\circ$ and $SM : SB' = 1/2$. Similarly $\angle NSA' = 60^\circ$, $SN : SA' = 1/2$. Hence $\triangle SMB' \sim \triangle SNA'$.

E3. Let us look at another problem we already solved by complex numbers. *On the sides AB and BC of $\triangle ABC$ are erected outwardly regular triangles with vertices D and E. Show that the midpoints of AC, BD, BE are vertices of a regular triangle.*

We must show in Fig. 12.17 that $\triangle MNP$ is regular. The idea is to move N by a sequence of transformations to P. The product must be a rotation about M by 60°. Such a sequence is easy to find: dilatation with center B by factor 2, rotation about B by -60°, a half turn about M, rotation about B by -60°, and a stretch from B by factor $1/2$. It moves $N \mapsto D \mapsto A \mapsto C \mapsto E \mapsto P$. Now we show that M is a fixed point. Indeed, $M \mapsto M_1 \mapsto M_2 \mapsto M_3 \mapsto M_1 \mapsto M$. Since the stretches by 2 and $1/2$ give an isometry, this is a rotation by $+60^\circ$ since $-60^\circ + 180^\circ - 60^\circ = 60^\circ$.

E4. *The trapezoid $ABCD$ in Fig. 12.18 has $AB \parallel CD$. An arbitrary point P on the line BC, which does not coincide with B or C, is joined with D and the midpoint M of the segment AB. Let $X \in PD \cup AB$, $Q \in PM \cup AC$, $Y \in DQ \cup AB$. Show that M is the midpoint of XY.*

Consider the following homotheties:

$$H_Q : A \mapsto C, \quad H_P : C \mapsto B.$$

Obviously, $H_Q \circ H_P$ maps A to B and leaves M fixed. Since M is the midpoint of AB, the composite mapping $H_Q \circ H_P = H_M$ is a half turn about M. But $H_Q : Y \mapsto D$, $H_P : D \mapsto X$. Thus $H_M : Y \mapsto X$, and $|MX| = |MY|$.

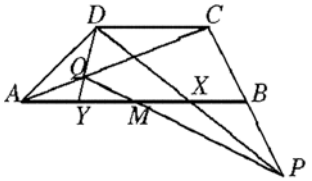


Fig. 12.18

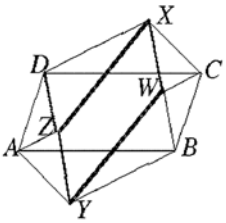


Fig. 12.19

E5. *On the sides AB, BC, CD, DA of a quadrilateral $ABCD$, we construct, alternately to the outside and inside, regular triangles with vertices Y, W, X, Z, respectively. Show that $YWXZ$ is a parallelogram.*

A parallelogram is generated by translation. So we try to find some mappings which give a translation as a product. Such a product is easy to find. $A_{60°} \circ C_{-60°}$ is a translation which takes Y to W and Z to X. Thus, $\overrightarrow{YW} = \overrightarrow{WX}$. Indeed,

$$Y \overset{A_{60°}}{\longmapsto} B \overset{C_{-60°}}{\longmapsto} W, \qquad Z \overset{A_{60°}}{\longmapsto} D \overset{C_{-60°}}{\longmapsto} X.$$

E6. *This is a generalization of the preceding example. Suppose, we replace the regular triangles with directly similar triangles. See Fig. 12.19. The result still seems to be a parallelogram.*

Indeed, with $|AY|/|AB| = r$, we have

$$A_\alpha \circ A\left(\frac{1}{r}\right) \circ C(r) \circ C_{-\alpha} = f, \quad \text{a translation.}$$

$$Y \overset{f}{\longmapsto} W, \quad Z \overset{f}{\longmapsto} X \Rightarrow \overrightarrow{YW} = \overrightarrow{ZX}.$$

E7. *Construct a parallelogram, given two opposite vertices A, C, if the other two vertices lie on a given circle.*

A parallelogram is a centrally symmetric figure. The center M is the midpoint of AC. A half turn about M interchanges the other two vertices, but they must lie on the reflected circle. So they are the intersections of the given circle and its reflection.

E8. *Construct a parallelogram $ABCD$, given the vertices A, C and the distances r and s of the points B and D from a given point E.*

Reflect E at the midpoint M of AC to E'. Now B is constructible from EE' and circles with radii r and s and centers E and E', respectively.

E9. *Construct a parallelogram $ABCD$ from C, D and the distances r and s of A and B from a given point E.*

The translation $\overrightarrow{AD}$ takes E to E'. Now $\triangle DE'C$ is constructible from the three sides $|CD|$, $|DE'| = r$, $|E'C| = s$. Now translate DC by $\overrightarrow{E'E}$. The image of DC is AB.

E10. *Two circles α and α_1 and a point P are given. Find a circle which is tangent to α and α_1, such that the line through the two points of tangency passes through P.*

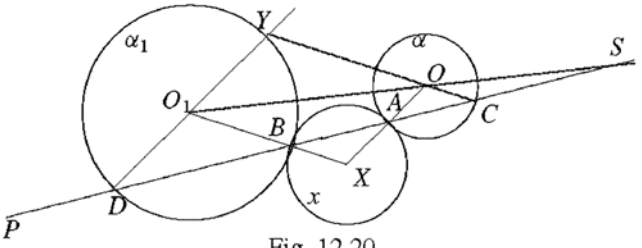


Fig. 12.20

The circle x to be constructed touches α and α_1 (with centers O, O_1) in A and B, where $P \in AB$. We consider the homothety with center A, which maps α to x, and the homothety with center B, which maps x to α_1. Their product maps α onto α_1 and has center $S \in AB \cup OO_1$, that is, AB is determined by P and S, where S is a similarity center of the circles α and α_1. If α, α_1 are not congruent, there will be two similarity centers S, S_1, such that $\alpha \to \alpha_1$. There will be solutions, if at least one of the lines SP, SP_1 intersects the given circles. At most there are four solutions: two circles x, y for SP and two for S_1P (with a negative stretch factor). See Fig. 12.20, which shows the two solutions for S. The second solution is not actually drawn, but its center Y and its points C and D of tangency are constructed.

E11. *A circle and one of its diameters AB are given as well as one point P in the plane. Construct the perpendicular to AB through P by ruler alone. With a ruler, you can connect two points.*

The problem is almost automatic for most positions of P. In Fig. 12.21 you must draw AP and BP. Then two new points C, D arise. So you draw AC and BD. They intersect in H. But $AC \perp BP$ and $BD \perp AP$. So H is the orthocenter of the triangle ABP. Thus $PH \perp AB$. For a point P inside the circle, the lines to be drawn are exactly the same, but this time P is the orthocenter. The case in Fig. 12.22 is not much different. But suppose P lies on the circle as in Fig. 12.23. The new idea is to choose a point Q outside the circle. We can drop a perpendicular from this point to AB which intersects the circle at R, S. We can drop perpendicular from P, if we can reflect P at AB. Now we have two symmetric points R, S. With their help, we can easily reflect P. Draw SP. It intersects AB in T. Draw RT. It intersects the circle in P', the image of P. Now $PP' \perp AB$.

Now suppose that $P \in AB$ as in Fig. 12.24. We want to draw the perpendicular to AB through P. This is a considerably more difficult problem. Now we must draw two perpendiculars to AB. The first intersects AB in Q and the circle in S, S'. The other intersects AB in R. Draw SP and $S'P$. They intersect the second perpendicular in T and T'. The simplest way to proceed now is to use a *shear* with fixed line SS' which takes $T'R$ to RT. Shears preserve areas and take lines into lines. Now the trapezoids $S'T'RQ$ and $S'RTQ$ have the same area, $S'T'$ goes to $S'R$, and QR goes to QT. Since $\triangle S'PQ$ and $S'P'Q$ have the same area and the

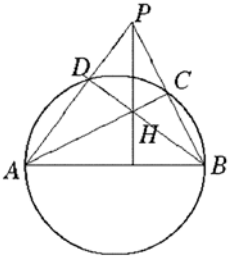


Fig. 12.21

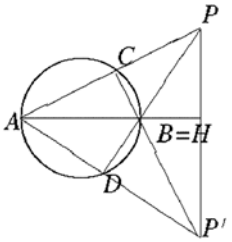


Fig. 12.22

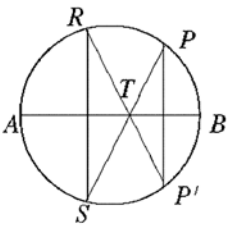


Fig. 12.23

same base $S'Q$, they will have the same altitude. Thus P and P' are equidistant from $S'Q$. Hence, $PP' \perp AB$.

E12. *Construct a quadrilateral $ABCD$ from its sides and the median MN joining the midpoints of AB and CD, respecively.*

Reflect the whole quadrangle $ABCD$ at M to $ABD'C'$. N will go to N_1. Translate DN by $\overrightarrow{DA}$ to AA_1. Similarly, translate CN by $\overrightarrow{CB}$ to BB_1. $\triangle A_1N_1N$ can be constructed from its sides. Now $\triangle MAA_1$ can also be constructed from its sides. The rest is trivial. See Fig. 12.25.

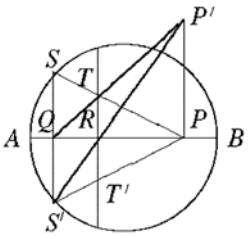


Fig. 12.24

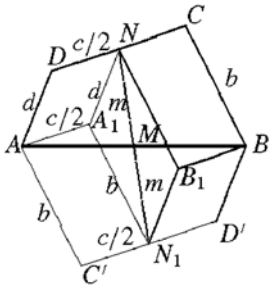


Fig. 12.25

Problems

1. ABC and $A'B'C$ are regular triangles with the same orientation. Let P, Q, R be the midpoints of the segments AB', BC, $A'C$, respectively. Show that $\triangle PQR$ is regular.

2. Let M, N be the midpoints of the bases of trapezoid $ABCD$. Show that the line MN passes through the intersection point O of the diagonals and the point S where the extensions of the legs intersect.

3. A point P is joined to the vertices of triangle ABC. The straight lines $AP = y$, $BP = z$, $CP = x$ are reflected at the angle bisectors passing through A, B, C to v, w, u, respectively. Prove that u, v, w pass through one point Q.

4. Three lines x, y, z are incident with a point P and are orthogonal to the sides c, a, b of a triangle ABC. Now x, y, z are reflected at the midpoints of c, a, b to u, v, w, respectively. Prove that u, v, w also pass through a point Q.
5. Take a point A inside an acute angle. Construct the triangle ABC of minimum perimeter if B and C lie on the legs of the angle.
6. Two circles are tangent internally at point A. A secant intersects the circles in M, N, P, Q. Prove that $\angle MAP = \angle NAQ$.
7. A chord MN is drawn in a circle ω. In one of the circular segments, the circles ω_1, ω_2 are inscribed touching the arc in A and C and the chord in B and D. Show that the point of intersection of AB and CD is independent of the choice of ω_1, ω_2.
8. Consider n circles C_i ($C_{n+1} = C_1$) with C_i touching C_{i+1} externally at T_i for $i = 1$ to n. Start at any point A_1 on C_1, and, for $i = 1$ to n, draw straight lines A_iT_i intersecting C_{i+1} a second time in A_{i+1}. What is the relative position of A_1 and A_{n+1} on C_1? Generalize.
9. Assume a line a and a point P. Using as few lines as possible (circles or segments), construct the line perpendicular to a which passes through P. If $P \notin a$ the problem is well known to every high school student of geometry. But suppose $P \in a$. The minimal construction is hardly known. See the solution for a proof of our contention.
10. A, B, C, D are four points on a line. Through A and B, draw a pair (a, b) of parallels and, through C and D, another pair (c, d) of parallels so that $(a, b) \cup (c, d) = PQRS$ is a square.
11. Draw through a point P inside an angle a segment, which cuts off a triangle of minimum area.
12. On the sides CA and CB of $\triangle ABC$, squares $CAMN$ and $CBPQ$ with centers O_1 and O_2 are constructed to the outside. The points D and F are the midpoints of the segments MP and NQ. Prove that the triangles ABD and O_1O_2F are rectangular and isosceles.
13. What can you say about lines a and b if $a \circ b \circ a = b \circ a \circ b$. Here we identify a line a with the reflection in a.
14. What is the relative position of a, b, c, d if $a \circ b \circ c \circ d = b \circ a \circ d \circ c$?
15. In a quadrilateral $ABCD$, we reflect A at B to A_1, B at C to B_1, C at D to C_1, D at A to D_1. Suppose, only A_1, B_1, C_1, D_1 are given. Reconstruct $ABCD$. Compare the areas of $ABCD$ and $A_1B_1C_1D_1$.
16. In a quadrilateral $ABCD$, reflect A at C to A_1, B at D to B_1, C at A to C_1, D at B to D_1. Compare the areas of $ABCD$ and $A_1B_1C_1D_1$.
17. On the sides BC, CA, and AB of triangle ABC, regular triangles with vertices D, E, and F are erected. Reconstruct ABC from D, E, F.
18. On the sides AB and DA of a parallelogram $ABCD$, regular triangles with vertices E and F are erected. Prove that E, C, F are vertices of a regular triangle.
19. On the sides of $\triangle ABC$, the points P, Q, R are chosen, such that $AP = 2PB$, $BQ = 2QC$, $CR = 2RA$. Reconstruct the triangle from P, Q, R.
20. Construct a triangle ABC from two sides b, c, if it is known that the median AD divides the angle at A in the ratio $1 : 2$, so that $\angle BAD = \alpha$, $\angle DAC = 2\alpha$, α being unknown.

Problems

17. Along a circle are written 4 ones and 5 zeros. Then between two equal numbers we write a one and between two distinct numbers zero. Finally the original numbers are wiped out. This step is repeated. In this way can we ever reach 9 ones?
18. There are n weights on a table with weights $m_1 > m_2 > \cdots > m_n$ and a two-pan scale. The weights are put on the pans one-by-one. To each weighing we assign a word from the alphabet $\{L, R\}$. The kth letter of the word is L or R if the left or right pan outweighs the other, respectively. Prove that any word from $\{L, R\}$ can be realized.
19. In n glasses with sufficient volume, there is initially the same amount of water. In one step you may empty as much water from any glass into any other glass as there is in the second glass. For what n can you pour all the water into one glass?
20. Starting with 1, 9, 9, 3, we construct the sequence 1, 9, 9, 3, 2, 3, 7, ..., where each new digit is the mod 10 sum of the preceding four terms. Will the 4-tuple 7, 3, 6, 7 ever occur?
21. The integers $1, 2, \ldots, n$ are placed in order, so that each value is either bigger than all preceding values or is smaller than all preceding values. In how many ways can this be done?

14.4 Conjugate Numbers

Let a, b, r be rational, but $\sqrt{r}$ be irrational. Then $a + b\sqrt{r}$ and $a - b\sqrt{r}$ are called *conjugate numbers*. They often occur simultaneously.

Often it is helpful to switch between $a + b\sqrt{r}$ and $a - b\sqrt{r}$.

We rationalize the denominator as often as we rationalize the numerator:

$$\frac{1}{a + b\sqrt{r}} = \frac{a - b\sqrt{r}}{a^2 - b^2 r}, \quad a + b\sqrt{r} = \frac{a^2 - b^2 r}{a - b\sqrt{r}}.$$

To rationalize the denominator in

$$\frac{1}{1 + \sqrt{2} + \sqrt{3}},$$

we multiply denominator and numerator so that we get the denominator

$$(1 + \sqrt{2} + \sqrt{3})(1 + \sqrt{2} - \sqrt{3})(1 - \sqrt{2} + \sqrt{3})(1 - \sqrt{2} - \sqrt{3}).$$

The mapping $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto -\sqrt{3}$ leaves this term unchanged. Thus, the term is rational. To rationalize the denominators in

$$\frac{1}{1 + \sqrt[3]{2} + 2\sqrt[3]{4}}, \qquad \frac{1}{1 - \sqrt[4]{2} + 2\sqrt{2} + \sqrt[4]{8}},$$

it is useful to know that the sets $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} | a, b, c \in \mathbb{Q}\}$ and $\{a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} | a, b, c, d \in \mathbb{Q}\}$ are fields, i.e., algebraic systems which are closed with respect to the operations $+, -, \cdot, :$.

As a typical example, we use the problem from the "Ersatz"-IMO 1980.

E1. *Find the first digit before and after the decimal point in* $\left(\sqrt{2}+\sqrt{3}\right)^{1980}$.

The base $\sqrt{2}+\sqrt{3}$ does not have the form $a+b\sqrt{n}$ for which we have a theory. Hence we transform it into this form by squaring the base and halving the exponent. We get $x=(5+2\sqrt{6})^{990}$. This is almost an integer. Indeed, by adding the tiny number $y=(5-2\sqrt{6})^{990}$ we get the integer

$$a=(5+2\sqrt{6})^{990}+(5-2\sqrt{6})^{990}=x+y=p+q\sqrt{6}+p-q\sqrt{6}=2p,$$

where p is an integer. We need only the last digit of $2p$, i.e., $2p \bmod 10$. We can find $2p \bmod 10$ by the binomial theorem. We get

$$2p=2\left[5^{990}+\binom{990}{2}5^{988}\cdot 2^2\cdot 6+\binom{990}{4}5^{986}\cdot 2^4\cdot 6^2+\cdots\right]+2\cdot 2^{990}\cdot 6^{495}.$$

All of the terms except the last one are divisible by 10. The last one is easy to find mod 10 since $6^n \bmod 10 = 6$. Thus it remains to find $2^{991} \bmod 10$, which is 8, since the last digit of powers of 2 has period 2, 4, 8, 6. Finally $8\cdot 6\equiv 8 \bmod 10$.

Now we have the last digit 8 of $x+y$. Subtracting the tiny number y, we get $x=\ldots 7,9\ldots$.

Alternate solution: We embed the problem into a more general one. Let

$$\begin{aligned}
u_n&=(5+2\sqrt{6})^n+(5-2\sqrt{6})^n=x_n+y_n\sqrt{6}+x_n-y_n\sqrt{6}=2x_n,\\
u_{n+1}&=(x_n+y_n\sqrt{6})(5+2\sqrt{6})+(x_n-y_n\sqrt{6})(5-2\sqrt{6})=10x_n+24y_n,\\
u_{n+2}&=10x_{n+1}+24y_{n+1}=10(5x_n+12y_n)+24(2x_n+5y_n)=98x_n+240y_n,\\
u_{n+2}&+u_n=100x_n+240y_n=10u_{n+1}\equiv 0 \bmod 10.
\end{aligned}$$

From $u_1=10,\ u_2=98$ we get $0,\ 8,\ 0,\ 2,\ldots$ with period 4 for the last digit of u_n. Thus the 990th term is 8. The remainder can be finished as above.

Problems

22. Prove that $(a+b\sqrt{r})^n=p+q\sqrt{r} \iff (a-b\sqrt{r})^n=p-q\sqrt{r}$.
23. $(x+y\sqrt{5})^4+(z+t\sqrt{5})^4=2+\sqrt{5}$ has no rational solutions $x,\ y,\ z,\ t$.
24. Let $(1+\sqrt{2})^n=x_n+y_n\sqrt{2}$, where $x_n,\ y_n$ are integers. Prove that

    (a) $x_n^2-2y_n^2=(-1)^n$; (b) $x_{n+1}=x_n+2y_n,\ y_n=x_n+y_n$.

25. Which number is larger: (a) $\sqrt{1979}+\sqrt{1980}$ or $\sqrt{1978}+\sqrt{1981}$?
    (b) $a_n=\sqrt{n}+\sqrt{n+1}$ or $b_n=\sqrt{n-1}+\sqrt{n+2}$?
26. Let $a_n=n\left(\sqrt{n^2+1}-n\right)$. Find $\lim_{n\to\infty}a_n$.
27. $a_n=\sqrt{n+1}+\sqrt{n},\ b_n=\sqrt{4n+2}\Rightarrow 0<b_n-a_n<1/16n\sqrt{n}$.

28. Find the first 100 decimals of $\left(\sqrt{50}+7\right)^{100}$.
29. If $p > 2$ is a prime, then $p \mid \lfloor (2+\sqrt{5})^p \rfloor - 2^{p+1}$.
30. $\lfloor (2+\sqrt{3})^n \rfloor$ is odd.
31. Find the highest power of 2 which divides $\lfloor \left(1+\sqrt{3}\right)^n \rfloor$.
32. (a) For every $n \in \mathbb{N}$, we have $n\sqrt{2} - \lfloor n\sqrt{2} \rfloor > 1/(2n\sqrt{2})$.
    (b) For every $\epsilon > 0$ there is an $n \in \mathbb{N}$ such that $n\sqrt{2} - \lfloor n\sqrt{2} \rfloor < (1+\epsilon)/(2n\sqrt{2})$.
33. Find the equation of lowest degree with integral coefficients and one solution $x_1 = 1+\sqrt{2}+\sqrt{3}$. Give the other solutions without computation.
34. Decide if $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ is rational or irrational.
35. If $a,\ b,\ \sqrt{a}+\sqrt{b}$ are rational, then so are $\sqrt{a},\ \sqrt{b}$.
36. If $a,\ b,\ c,\ \sqrt{a}+\sqrt{b}+\sqrt{c}$ are rational, then so are $\sqrt{a},\ \sqrt{b},\ \sqrt{c}$.
37. $\sqrt[3]{2}$ cannot be represented in the form $a + b\sqrt{r}$ with $a,\ b,\ r \in \mathbb{Q}$.
38. $\left(\sqrt{2}-1\right)^n,\ n \in \mathbb{N}$ has the form $\sqrt{m} - \sqrt{m-1},\ m \in \mathbb{N}$.
39. Find the sixth decimal in $\left(\sqrt{1978} + \lfloor \sqrt{1978} \rfloor\right)^{20}$.
40. Rationalize the denominator in

$$\text{(a)}\ \frac{1}{1+\sqrt[3]{2}+2\cdot\sqrt[3]{4}}, \qquad \text{(b)}\ \frac{1}{1-\sqrt[4]{2}+2\cdot\sqrt{2}+\sqrt[4]{8}}.$$

41. Let $m,\ n \in \mathbb{N}$ and $\frac{m}{n} < \sqrt{2}$. Prove that $\sqrt{2} - \frac{m}{n} > \frac{1}{2\cdot\sqrt{2}\cdot n^2}$.
42. (a) Prove that there exist integers $a,\ b,\ c$ not all zero and each of absolute value less than one million, such that $|a + b\sqrt{2} + c\sqrt{3}| < 10^{-11}$.
    (b) Let $a,\ b,\ c$ be integers, not all zero and each of absolute value less than one million. Prove that $|a + b\sqrt{2} + c\sqrt{3}| > 10^{-21}$ (Putnam 1980).
43. Simplify the expression $L = 2/\sqrt{4 - 3\sqrt[4]{5} + 2\sqrt{5} - \sqrt[4]{125}}$ (MMO 1982).

14.5 Equations, Functions, and Iterations

In this section we collect some nonlinear systems of equations, which are of geometric origin or which originate in functional iterations.

E1. *The positive reals $x,\ y,\ z$ satisfy the equations*

$$x^2 + xy + \frac{y^2}{3} = 25, \quad \frac{y^2}{3} + z^2 = 9, \quad z^2 + zx + x^2 = 16.$$

Find $xy + 2yz + 3zx$ (AUO 1984).

In a training session I gave this to one member our team, and I told him to give a detailed account of all ideas he had during the solution. Here is a short version: