Mathematical and Physical Journal for Secondary Schools

KöMaL

Volume 1

Number 1

December 2002

Journal of the János Bolyai Mathematical Society
and Roland Eötvös Physical Society

The History of the Bolyai-Prize

"There are two relevant issues concerning the revitalization of the Prize. The Hungarian Academy of Sciences is resuming this magnificent tradition of recognizing high quality scientific achievement on an international level. The other one nonetheless important is that we are looking out into the world again."

Academician Dénes Berényi
Academic News 1992/3, p. 9

The János Bolyai International Mathematical Prize of the Hungarian Academy of Sciences (MTA) consists of a medal and an award of $25,000.

This award was founded in 1903 by the Hungarian Academy of Sciences in the honour of János Bolyai, co-discoverer of non-Euclidean geometry. It went for the first time to H. Poincaré in 1905 and to D. Hilbert afterwards in 1910. Then, however, due to various historical events, World War I included, it ceased to exist.

The Academy decided to relaunch this award, and Professor Shelah has been the first recipient in modern times. In accordance with the original project, the prize will be issued every five years to the author of the best mathematical monograph expanding original research, that has been published in the previous ten years.

Henri Poincaré (1905)

David Hilbert (1910)

Saharon Shelah (2000)

details:
BARNA SZÉNÁSSY: Contributions to the History of the Bolyai-Prize
www.kfki.hu/~tudtor/tallozo1/contrib.html

MATHEMATICAL AND PHYSICAL JOURNAL FOR SECONDARY SCHOOLS
FOUNDED BY **DÁNIEL ARANY** IN 1894

Volume 1, Number 1. Budapest, 2003. November

Appeared 2 times per year. Price: 8 USD

CONTENTS

Supported by:

HUNGARIAN MINISTRY OF EDUCATION

IPAR MŰSZAKI FEJLESZTÉSÉÉRT ALAPÍTVÁNY

ELTE

INDEX: 25 450 ISSN 1215-9247

This journal can be ordered from abroad at
Roland Eötvös Physical Society,
Bp., P.O.B. 433, H-1371, HUNGARY.
Address of Publisher:
H-1027, Budapest, Fő u. 68. II. 241.
Telephone, fax: (36-1)-201-8682
Address of Editorial office: H-1117, Budapest,
Pázmány Péter sétány 1/A. V. 5.106.
Telephone: (36-1)-372-2850, (36-1)-209-0555/6541
Postal address: Budapest 112, P.O.B. 32, H-1518
Subscription fee: 15 USD.
E-mail: `editors@komal.hu`
Internet: `http://www.komal.hu`

What is KöMaL?

It was more than a hundred years ago that Dániel Arany, a high school teacher from the city of Győr, decided to found a mathematical journal for high school students. His goal was "to give a wealth of examples to students and teachers". The journal's first edition appeared on January 1, 1894.

From that time several generations of mathematicians and scientists developed their problem-solving skills through KöMaL. The best solutions with the names of the 14–18 year-old authors are printed in the periodical. KöMaL regularly reports on national and international competitions, prints articles on interesting results in mathematics and physics, and includes book reviews. For more than 30 years all the new problems have appeared in English as well as Hungarian in the journal. This means thousands of mathematics and physics problems and exercises in English. At present the journal is published by the János Bolyai Mathematical Society and the Roland Eötvös Physical Society with the financial support of the Ministry of Education in 5000 copies. The periodical "KöMaL — Középiskolai Matematikai és Fizikai Lapok" appears in Hungarian language 64 pages a month 9 times a year. This periodical "KöMaL", that you are reading now, appears in English language two times a year. This is the first edition. The most interesting problems end articles from the homepage of KöMaL are collected and printed. The main goal of the periodical KöMaL to show the content that is open for students. We are waiting for you. Let us think.

On János Bolyai's Bicentennial

János Bolyai is one of the greatest figures of Hungarian and universal science. When mentioning his name, one always thinks of his inventive achievements in geometry. This is wholly legitimate, because with the creation of absolute geometry and non-Euclidean geometry in particular, he opened up a new chapter in the history of science. One can rightly assert that few inventions had so great an impact on the development of scientific world-view as that of Bolyai's geometrical invention. His only work published during his lifetime, *The Absolutely True Science of Space,* was enough to eternally inscribe his name in the history of mathematics. Until recently we used to think that we had a complete knowledge about his life-work. However, the research works of the last decade have shown that concerning the wide problematics of number theory and the question of solubility of algebraic equations Bolyai's works were in the front line of mathematical research, sometimes preceding by decades other great scientists' discoveries.

János Bolyai's 26 pages long work *The Absolutely True Science of Space,* was issued as an addendum to his father's book entitled *Tentamen,* therefore, it is often referred to simply as the *Appendix.* Written in Latin with a remarkable precision and conciseness, it is one of the oustanding achievements in the world history of mathematics and it has been translated into several languages. Bolyai's discovery is not only the first step in the development of modern mathematics, but his ideas had a significant impact on the shaping of natural sciences in general. According to Erik Temple Bell (1883–1960) the developments of hyperbolic geometry revolutionized universal thinking to an even greater degree than the ideas of Copernicus [2]. Bolyai's influence can also be detected in the latest developments of mathematics. It is reflected in his theory of space and in his widespread concepts in modern mathematics.

The Appendix is not the only work János Bolyai left to posterity. Even after the completion of his great work, he studied and took notes continuously. It resulted in his vast legacy of manuscripts, fourteen thousand pages of which are kept in the Teleki–Bolyai Library of Marosvásárhely. These notes contain the "treasures" (it was Bolyai's way of naming his newly discovered theorems) that have been brought to light by the research works of recent years.

1. János Bolyai's Course of Life

János Bolyai was born on the 15$^{\text{th}}$ of December, 1802 in Kolozsvár [currently Cluj, in Romania]. His father, Farkas Bolyai (1775–1856), became later the erudite professor of the college of Marosvásárhely, whereas his mother, Zsuzsanna Benkő (1782–1821) was the daughter of a surgeon from Kolozsvár.

His later notes and his father's letters provide a detailed account of the first section of his life. He spent his childhood and youth in Domáld [now part of Viişoara-Mureş county in Romania] and Marosvásárhely [now Târgu-Mureş in Romania]. His father gave very careful attention to his son's physical and intellectual education. The nimble, wholesome child showed from the very beginning outstanding intellectual capabilities combined with a sharp perception and an implacable sense of justice. He learned to read and write very easily, as a five years old child he could already distinguish various geometrical figures, he was familiar with the sine function, and recognized the main constellations. He was also unusually talented in learning languages and music. His father imposed on János systematic studying from the age of nine, many subjects were taught to him by his father's more gifted students, but it was his father who taught him mathematics from the very beginning. The extremely talented child shortly became familiar with Euclides's six books, Leonhard Euler's (1707–1783) algebra and even the main part of George Vega's (1754–1802) four-volume handbook.

Farkas Bolyai intended that János continue his studies in Göttingen with his friend of youth, Gauss. He wrote to Gauss in this matter, but his friend did not answer to his letter. Therefore, after due consideration he decided to send his son to the Royal Engineering College of Vienna. In August 1818 János successfully passed the entrance examination and began his career as a soldier.

While staying in Vienna, János was seriously interested in mathematical problems. The seeds of his original ideas are already present in these notes. The illustrations found in his booklet containing solutions to mechanical problems attest to the fact that around the year 1820 he had already began to ponder the unprovability of the axiom of parallelism. In the same year, he experimented with one of the famous, ancient problems, namely, the trisection of angles.

After he had finished his studies, in September 1823 he was appointed second lieutenant to Temesvár (now Timişoara in Romania). It was the place where his more than three years' cogitation, which had started in Vienna, reached a conclusive stage. On a winter night in 1823 he determined the relation holding between the so-called angle of parallels (u) and the distance of parallels (x), which was later written down in §.29 of his Appendix:

$$\cot \frac{u}{2} = e^{\frac{x}{k}} \tag{1}$$

where $e = 2.718\ldots$.

In April 1826 Bolyai was transferred to Arad (now Arad in Romania). In 1831 Bolyai was commanded to go to Lemberg (today Lviv in Ukraine), then in 1832 another order called him to Olmütz (now Olomouc in the Czech Republic). In the previous years he had suffered many times from various diseases, very often from malaria and supposedly also from the infection of the joints. In this period he was especially restless and irritable and he openly manifested his indifference towards military career. The direct consequence of all these was that from the 16$^{\text{th}}$ of June 1833 he was sent to retirement.

Meanwhile, János Bolyai's pioneering work, *The Absolutely True Science of Space,* was published in 1832. This important work [5] was published as an appendix to the first volume of Farkas Bolyai's *Tentamen* [3], but its off-print had already been ready the previous year, in April 1831 [4]. The latter was the version which, together with a letter, was sent to Gauss by Farkas Bolyai on the 20$^{\text{th}}$ of June 1831. Gauss got the letter but János's work was lost on the way. On the 16$^{\text{th}}$ of January 1832 Farkas sent the Appendix to his friend again with another letter in which he wrote: "My son appreciates Your critique more than that of whole Europe and it is the only thing he is waiting for" [14].

After twenty-three years of silence, Gauss replied to his "old, unforgettable friend" on the 6$^{\text{th}}$ of March 1832. One of his well-known sentences was: "if I praised your son's work I would praise myself". The letter deeply afflicted and upset János Bolyai, although it reflects appreciation, too: "... I am very glad that it is my old friend's son who so splendidly preceded me" [14].

After his retirement János Bolyai returned to Marosvásárhely in June 1833. He lived at his father's place for one year, and then he moved to Domáld in 1834. There he lived in seclusion until 1846, when he returned to Marosvásárhely again. His stay at Domáld was not unfruitful in mathematical research either, as former biographers have argued. It was at this time that he wrote his other manuscript, the *Responsio,* but he was also interested in the solvability of algebraic equations of higher degree and made inquiries into number theory. In the last twenty-seven years of his life he did not publish anything, mainly because of his bad finacial situation, but this does not mean that he was not working.

On the 20$^{\text{th}}$ of November 1856 his father died at the age of eighty-one. Farkas Bolyai's death took away from János the only person he could really talk to. From the autumn of 1857 he was ill and confined to bed almost all the time. In January 1860 he got pneumonia and on the 27$^{\text{th}}$ he passed away.

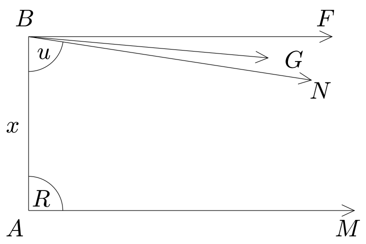
Had he lived eight more years, he would have learned that several western mathematicians showed keen interest in his life and significant work. In 1867 the French version [7], and in 1868 the Italian translation [8] of the *Appendix* are published. At the same time the Grunerts Archiv der Math. und Phys issues the biography of Farkas and János Bolyai [13]. These writings mark the beginning of the vast literature written on the two Bolyais.

2. The Absolutely True Science of Space

Ancient geometry reached its apex in Euclid's work, the *Elements.* It is a work in which Euclid sets up geometry on the basis of certain fundamental notions and simple assertions called axioms or postulates, while any further concept or theorem is logically deduced from these axioms. Euclid's Postulate V. (in some versions axiom IX.) aroused the interest of mathematicians already in ancient times. Early mathematicians regarded that it was not "simple" and "clear" enough to satisfy the requirements of an axiom. Thus, they first tried to substitute it with simpler axioms. Later, the idea occured that Postulate V. might not be a fundamental truth at all, just a consequence of other axioms. Proving Postulate V. posed an important question, which concerned for centuries various mathematicians of the world.

János Bolyai was the first to build up a geometry, which neither affirms nor negates Postulate V., but it rather puts it aside: he interpreted parallelism in a way which can intertwine the possibilities of affirming and negating Postulate V. Accordingly, both Euclidean (the Σ-system) and non-Euclidean geometry, or in other words hyperbolic geometry (the S-system) are special cases of the more general geometry Bolyai called absolute geometry. Bolyai's great merit consisted in his invention of absolute geometry and, within it, hyperbolic geometry.

János Bolyai preserves all Euclides's postulates except Postulate V. Just as in common perception, all those basic assumptions which underlie the connecting of points with the help of lines and planes, the transfer of distances and angles with the same extent or the congruence of triangles etc. are also requirements of the S-system. The difference is with regard to the question of parallelism, which Bolyai elucidated in §1. of the *Appendix.* He defines parallelism not with lines but



with half-lines: the directed half-line $\overrightarrow{BN}$ is parallel with the directed half-line $\overrightarrow{AM}$ if the counterclockwise rotation of the half-lines from BA around B results in the half-line $\overrightarrow{BN}$, which does not intersect AM. According to János Bolyai it is clear that from any point B outside line AM there is only one such $\overrightarrow{BN}$ and that

$$\angle BAM + \angle ABN \leqslant 2R \tag{2}$$

(R refers to the right angle).

Parallelism defined in such a way is called absolute parallelism, and if in case (2) we only allow the use of sign $<$ then we talk about hyperbolic parallelism. In the latter case there are two — oppositely directed — parallels to AM through point B. In the hyperbolic definition there are several half-lines $\overrightarrow{BG}$ which are neither parallel with $\overrightarrow{AM}$ nor do they intersect it. Thus, while on the Euclidean plane two distinct lines either intersect or are parallel to each other, on the hyperbilic plane there are lines which neither intersect nor are they parallels.

Both in its content and in its form János Bolyai's *Appendix* is one of the basic works in the history of mathemetics. Absolute geometry widely and deeply influenced further investigations. It opened up the way for new developments, which, in turn, extended their scope beyond mathematics, influencing physics and other related sciences. However, its immediate influence was on the development of mathematics.

The birth of Bolyai's geometry is a turning point in the history of the axiomatic method. His work put an end to all those axiomatic investigations, which — for thousands of years — had attempted to tackle the problem of parallelism. At the same time, these investigations opened up the way for a whole row of modern inquiries connected with the axiomatic method. The questions of independence and compatibility of the axiomatic systems rose for the first time in a close relation to non-Euclidean geometry.

Finally, I would like to emphasize that the invention of absolute geometry is solely János Bolyai's merit. He was the first to think of its creation, which was not done with the help of non-Euclidean geometry. For him, non-Euclidean geometry was a kind of gift resulting from absolute geometry.

3. Number Theory

All Bolyai-monographs unanimously assert: although János Bolyai tried his hand at a few problems in number theory, his investigations were not particularly successful. However, his manuscripts attest the opposite of all this. Bolyai had a keen interest in questions of number theory and he had several original ideas, with which he preceded many other mathematicians of later ages.

Among the very first theorems found in Bolyai's legacy is the following: If p and q are prime numbers, and a is an integer divisible neither by p nor by q, and if $a^{p-1} \equiv 1 \pmod{q}$ and $a^{q-1} \equiv 1 \pmod{p}$, then

$$a^{pq-1} \equiv 1 \pmod{pq} \tag{3}$$

[11].

We can readily observe that it is the same theorem which James Hopwood Jeans (1877–1946) published decades later in 1898. Since we can definitely affirm that this relation was first recognized and demonstrated by János Bolyai, I propose that in the future it should be called Bolyai–Jeans Theorem.

At a time János Bolyai thought that he could find the formula of prime numbers by means of Fermat's little theorem. This is why he tried to prove its converse. As a result, he reached conclusion (3). By substituting $a = 2$ in this relation, with repeated attempts he got the numbers $p = 11$, $q = 31$, and thus Bolyai found the smallest pseudoprime number with respect to 2, that is, 341, for which

$$2^{340} \equiv 1 \pmod{341}.$$

Thus, he showed that the converse of the so-called "little theorem" of Pierre de Fermat (1601–1665) was not true. We can remark that the only one who found the number 341 in Bolyai's time was an anonymous scientist [1], but Bolyai was not aware of this.

Bolyai's further observations concerning the Fermat's little theorem can be found in [11].

János Bolyai's inquiries concerning Fermat's two-square theorem are very valuable. The theorem goes as follows: every prime of the form $4k + 1$ ($k \in \mathbb{N}$) can be written as a sum of two squares. The theorem had been formulated by Fermat but it was demonstrated by Leonhard Euler (1707–1783) at about one hundred years later. Euler's proof reached the Teleki Téka of Marosvásárhely, where Farkas Bolyai read it. The proof seemed too long and complicated to him. Therefore, he asked his son to provide him with the "simplest" demonstration of the theorem. Within a short period of time János sent his father a two-page letter with four possible solutions to the problem. His solutions were so simple, because he deployed his achievements regarding the question of complex integers. One of his solutions is especially simple [12]. We feel, that nobody has provided a more brilliant solution to this theorem than Bolyai.

In addition to these theorems János Bolyai dealt with several other number theoretical problems too, namely, with the Pell equation. Since he did not know that the converse of the Wilson's theorem — if $(n-1)! \equiv -1 \pmod{n}$, then n is prime — had already been demonstrated by Lagrange, he, just as his father, sought a solution to this problem. In his own words: "both my father and I solved the converse of the so beautiful and important Wilson's theorem" [6].

We mention, that one can find in his manuscripts even a magic square:

x	y	$3b - x - y$
$4b - 2x - y$	b	$2x + y - 2b$
$x + y - b$	$2b - y$	$2b - x$

János Bolyai constructs his magic square in a general way, using letters.

Bolyai got the bulk of his knowledge concerning number theory from Gauss's *Disquisitiones Arithmeticae* (1801). Including the most important and most recent problems, Gauss had sent a copy of his *Disquisitiones,* dedicated to his friend, Farkas Bolyai (Amico suo de Bolyai per curam Pauli Vada, auctor) as early as 1803. János could have read it in his early childhood, because at the age of 13 he already spoke Latin. But later, he definitely bought some of Gauss's work in Vienna. The latter copy, accompanied by Bolyai's glosses can be found in the Library of the Hungarian Academy of Sciences. Farkas Bolyai's book is in the Teleki–Bolyai Library of Marosvásárhely.

We used to think [15] that Hungarian mathematics did not have significant achievements in number theory up to the last quarter of the 19$^{\text{th}}$ century. If we take into consideration János Bolyai's ideas mentioned above, then it turns out that the first investigations in number theory started half a century earlier. Indeed, János Bolyai was the first to do such inquiries in Hungary. We can assert that the first Hungarian mathematician to produce significant achievements in the field of number theory was János Bolyai.

4. Algebraic Investigations

János Bolyai was also greatly interested in the solvability of algebraic equations. We can infer from his notes that for a long time he had tried in vain to prove the solubility of the equation of fifth degree, but later, realizing his error, also he got to the Ruffini–Abel theorem. He found the problem in the works of Gauss, Andreas von Ettingshausen (1796–1887), Joseph Luis Lagrange (1736–1813) and Farkas Bolyai. He often mentions in his notes Ettinghausen's work published [9] in 1827 in Vienna, in which the author mentions Paolo Ruffini's (1765–1822) "demonstration" of the solvability of algebraic eqations higher than fourth degree, dating from 1799. Bolyai was quick to realize the flaw of Ruffini's paper. His manuscripts attest to the fact that he successfully corrected Ruffini's mistake and proved that such equations cannot be solved. He asserts: "the general equation of fifth degree is unsolvable … the easiest correct way is Ruffini's 'solution' modified by myself" [6]. However, before Bolyai put down his ideas in this topic, mathematicians had already been familiar with Niels Abel's (1802–1829) flawless demonstration from 1826. Bolyai did not know about either Abel's or his contemporary's, Evariste Galois's (1811–1832) works. The history of mathematics, in its turn, did not know that in the middle of the 19$^{\text{th}}$ century there was a Hungarian mathematician, who solved one of the most important algebraic problems.

5. Conclusions

There are very few scientists whose work is appreciated in their lifetime. The inventors of non-Euclidean geometry did not have the opportunity to enjoy the triumph of their discovery. Above all, János Bolyai would have deserved much better recognition. His demonstration that the Euclidean axiom of parallelism was independent of other axioms brought an end to a period of development of two millennia. He solved one of the most lasting problems of geometry and thus created the concept of modern geometry. At the same time, he also obtained significant results in other branches of mathematics.

Now, on the occasion of his bicentennial it is necessary to evoke his course of life, his ideas and his mathematical activity in the light of the most recent examinations. Thus, we can get a more detailed and colourful portrait of the great inventor of geometry.

Acknowledgments. I thank the Domus Hungarica Scientarium et Artium and Arany János Közalapítvány for their support, which made the writing of this paper possible.

References

[1] Anonymus, Théorèmes et problèmes sur les nombres, *Journal für die reine und angewandte Mathematik,* **6** (1830), 100–106.

[2] Erik Temple Bell, *The Development of Mathematics,* Dover Publication, INC. New York (is an unabridged and unaltered publication of the second edition, 1945).

[3] Farkas Bolyai, *Tentamen juventutem studiosam in elementa puraem, . . .* Timus I–II, Marosvásárhely, 1832–33.

[4] János Bolyai, *Appendix prima scientia spatti . . . ,* Marosvásárhely, 1831 április.

[5] János Bolyai, *Appendix. Scientiam spatii absolute veram . . . ,* Marosvásárhely, 1832. (Attached to Farkas Bolyai's Tentamen).

[6] János Bolyai's manuscripts, Târgu-Mureş: Teleki–Bolyai Library.

[7] Jeans Bolyai, La science absolute de l'espace . . . , Traduit par Guillame-Jules Hoüel, *Memoires de la Société des sciences physiques et naturelles de Bordeaux,* V. Bordeaux, 1867.

[8] Giovanni Bolyai, Sulla scienza dello spazio assolutamente vera . . . , Versione dal latino per Giuseppe Battaglini, *Giornale di Matematica,* **6** (1868), Napoli, 97–116.

[9] Andreas von Ettingshausen, *Vorlesungen über die höhere Mathematik,* Wien, 1827.

[10] Elemér Kiss, *Mathematical Gems from the Bolyai Chests,* Budapest: Akadémiai Kiadó, 1999.

[11] Elemér Kiss, Notes on János Bolyai's Researches in Number Theory, *Historia Mathematica* **26**, (1999), 68–76.

[12] Elemér Kiss, A Short Proof of Fermat's Two-Square Theorem Given by János Bolyai, *Mathematica Pannonica,* **8** (2) (1997), 293–295.

[13] Franz Schmidt, Aus dem Leben zweier ungarischer Mathematiker, Johann und Wolfgang Bolyai von Bolya, *Grunerts Archiv der Math. und Phys.,* **48** (1868), 217–228.

[14] Franz Schmidt and Paul Stäckel, *Briefwechsel zwischen Carl Friderich Gauss und Wolfgang Bolyai,* Leipzig: Teubner, 1899.

[15] Barna Szénássy, *History of Mathematics in Hungary until the 20th Century,* Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo Hong Kong Barcelona Budapest, 1992.

Elemér Kiss

Cardan and cryptography The mathematics of encryption grids

To the 500th anniversary of the Girolamo Cardano

Introduction

The 16th century had just begun when Girolamo Cardano (1501–1576), Italian mathematician, physicist, philosopher, physician (a real renaissance scholar) was born. His 1545 publication titled *Ars Magna* contains general formulae for the roots of the cubic equation. Today, it is these formulae that Cardan's name is most often associated with, though it is still uncertain whether these discoveries were his own.[1]

Very few of us recognize Cardan as one of the most outstanding figures of 16th-century cryptography. This is not so surprising, as it is natural that cryptography should be pursued inconspicuously. The strictly confidential correspondence of kings and warlords used various cipher systems. As the more complicated cipher techniques, and especially the decryption of messages often require advanced mathematical skills, it can be expected that the theoretical background should be established in a large part by famous mathematicians.

Cardan developed a cipher system, then completely unknown, that is now called Cardan's screen. The success of Cardan's encryption screen is best proved

[1] According to historians, Scipione del Ferro (1465–1526) had found the general solution for cubic equations and showed it to his colleagues. That probably happened around 1515, when mathematical competitions were fashionable in Italy. A colleague of Ferro suggested to Niccolo Tartaglia (1500–1557), a mathematician of great learning, that they should solve cubic equations. Tartaglia solved the equations by the set deadline, but he did not reveal his technique. Cardan asked him so persistently for the method that finally, he confided the solution to Cardan, but he made Cardan swear to secrecy. Cardan broke his word and published the method in his *Ars Magna,* in 1545. A bitter dispute started between Tartaglia and Cardan, and it remains unsettled to this day.

by the fact that is was still used 400 years later, in the middle of the 20th century, by the West-German intelligence service (BND = Federal Information Service.)

In this paper, after a short historical overview, we illustrate the principle of Cardan's encryption screen, and then discuss several generalizations and a few mathematical properties of the grid.

Torch telegraphy and interval cipher

Cardan conducted a thorough research of the cipher systems of the past, back to antiquity. He found a text by Polybius, a Greek historian of the 2nd century BC, in which the author describes an interesting and completely unusual technique.

Torch telegraphy by Polybius

Consider the 5 by 5 table in *Figure 1.*

The sender of the message needs 10 torches, 5 for each hand. He sends the message letter by letter, by holding up as many torches with his left hand as the number of the row, and with his right hand as the number of the column containing the letter to be sent. For example, in the case of the letter "s", he holds 3 torches in his left hand and 4 in his right hand. Polybius was very proud of his method:

	1.	2.	3.	4.	5.
1.	a	f	l	q	v
2.	b	g	m	r	x
3.	c	h	n	s	y
4.	d	i	o	t	z
5.	e	k	p	u	

Figure 1

"This method was invented by Cleoxenus and Democritus but it was enhanced by me", he wrote.

He was proud with good reason. Though the idea of sending messages by means of torches was known and used by the ancient Chinese[2] a lot before Polybius, his cipher was the first to apply a table. The great advantage of a table is that the alphabet or the arrangement of the letters in the table can be changed any time without changing the method itself.

Question: *In how many different ways can the* 24 *letters of the alphabet be arranged in Figure 1? What if all the* 25 *fields are filled up?*

Cardan further improved this method by reducing the number of torches to two, one in each hand. The letters of the alphabet were coded by the respective positions of the torches. This method may have given Cardan the idea of two new types of cipher systems.

One type is "interval cipher" in which the message is coded by distances between letters. For simplicity, let us illustrate the method by an example. Prepare a table identical to that *Figure 2.*

[2]As early as 2000 years ago, the Chinese were able to transmit messages very quickly (and accurately) along the Great Wall with torches held up by men positioned at 100-m intervals.

Let the message be *"piglet"*. (The steps of the procedure can be followed in *Figures 3*(*a*) and *3*(*b*).) Take a blank sheet of paper. In the upper left corners, write any one of letters A, B, C (we choose C). This will only mark the beginning of the text. Take the table of *Figure 2,* and place the blank field onto the beginning letter.

A	a	e	r	n	c	b
B	i	o	d	l	g	q
C	u	s	m	f	p	t

Figure 2

Locate the first letter of *"piglet"* (p) in the table, and write the symbol of the row (C) directly above the letter p (*Figure 3*(*a*)).

C					C	B					B				B		A						C
	a	e	r	n	c	a	a	e	r	n	c	a	e	r	n	a	e	a	e	r	n	c	b
	i	o	d	l	g	i	i	o	d	l	g	i	o	d	l	i	o	i	o	d	l	g	q
	u	s	m	f	p	u	u	s	m	f	p	u	s	m	f	u	s	u	s	m	f	p	t

Figure 3(*a*)

C E L T I **C** **B** I K E R **B** E G S **B** E **A** V E R T O **C** U T W O O D
↑ ↑ ↑ ↑ ↑ ↑ ↑
begin mark (p) (i) (g) (l) (e) (t)

Figure 3(*b*)

Now place the blank square of the table onto the last capital letter written over the table, and locate the next letter (i) of the message. Repeat the previous procedure: Write the symbol (B) of the row over the letter i of the table. The procedure is continued until there is no more room left in the current row of the sheet. Then the first step is repeated and another row is opened. And so on, until the message is over. We can make the task of decryption even harder by filling up the spaces with arbitrary letters different from A, B, C (*Figure 3*(*b*).) (It is even better to complete the cipher to a meaningful text, but that is not necessary.)

The receiver of the message holds an identical table to that used by the sender. Thus by carrying out the above procedure starting at the begin mark, the receiver is able to read the message.

The modern reader might find this an interesting technique but it seems impractical, as the use of the table is complicated, and it requires too much space for its relatively small amount of information content. Cardan's method was also criticized by his contemporaries for being hard to follow. They did not realize that Cardan was far ahead of his age by establishing what is now called a non-symmetrical cipher. As opposed to other methods in use at that time, the above procedure is more than a simple substitution cipher.[3] It is a one-to-many rather than a one-to-one assignment, as the three capital letters code 6 lowercase letters each. Extra information is needed to decrypt the message (the position of the

[3] In cryptography, "substitution cipher" means that by some rule, there is one particular (different) letter of an alphabet assigned to the letters of the message. The distribution of letters in the ciphertext will thus be the same as in the plain text.

letter in the line, i.e. its distance from the reference letter). Consequently, unlike in simple substitution, the frequencies of the letters in the ciphertext do not match the frequencies in the plain text.

Cardan's screen

The other type of cipher system invented by Cardan, which bears his name to this day, uses the so-called Cardan grid (screen). The encryption grid is a matrix of letters. For illustration, let us cite Cardan's own words.[4]

"Take two sheets of parchment of the same size, ruled for writing, and on the lines of both make slits at various places. These slits are to be small, but of proper size for the size or height of letters of the alphabet. Some of the slits will hold seven, some three, some eight or ten letters, so that all the slits together will hold 120 letters, counting all the letters which can be inserted in them. One of these sheets of parchment you will give to your correspondent. When occasion arises, first write your message as briefly as possible, in such a way that the message may consist of a smaller number of letters than the slits will hold. Then write your message on a sheet of parchment placed beneath the slits, and again on a second sheet, and on still a third. Then fill the spaces of the first sheet by completing sentences, erasing, and filling in until connected sense results. Next, on the second sheet, finish the message which you now have in such a way that the words and sentences may appear coherent. Arrange it again on the third sheet of parchment in such a way that, without disturbing the original letters, the entire sense and the number and size of the words may hang together and retain a harmony of style. When this is completed, lay the sheet containing the slits upon a sheet of the same size, and place minute dots at the ends of the slits to mark the limits of the letters which you wish to insert. Then take the third sheet of parchment [i.e., the final draft of the three which have been made] and copy the message from it with the words in regular order and with a proper arrangement of spaces and size of the letters, so that the original [i.e., the secret] message and its words may be contained within the limits marked by the dots. No suspicion of any deception will now remain. Your correspondent, when he receives your communication, places his slitted sheet of parchment over it and reads what you wish to convey. Although this method entails no slight labor, none equally good can be devised for conveying information to friends in dangerous times."

The encryption screen became remarkably popular in cryptography. The success of the technique may have been due to its simplicity and versatility together. Such a success occurs very rarely in the history of science, especially in cryptography. With the development of technical skills, cryptanalysis usually catches up with cryptography. Though Cardan's name did not become widely known in this area, his cipher screen remained in use for 450 years. It has even found its way to fiction: In *Jules Verne's Mathias Sandorf,* the villains Torontal and Sarcany intercept Sandorf's coded message and decipher it by getting hold of a copy of the

[4] Quoted from Cardan on cryptography, [6], by Charles J. Mendelssohn.

screen. The screen appears right at the beginning of the novel, and becomes an important factor of the plot. The example below illustrates a 6×6 grid. The table of *Figure 4* has been filled in with the sentence "(O) how sweet to be a cloud floating in the blue." It is interesting to see how many different messages may be hidden in this ciphertext. The bold numbers in *Figures 5, 6, 7* stand for the windows in Cardan's screen. If the screen is placed over the table of *Figure 4,* the letters shown in the windows reveal the encrypted message (when read left to right, row by row.)

The ciphertext in *Figure 4:* O HOW SWEET TO BE A CLOUD FLOATING IN THE BLUE.

The message revealed by the screen of

Figure 5: WET TOAD LOATHE.

Figure 6: HOT COD FAT HUE.

Figure 7: WEE TOE OF ANNE.

O	H	O	W	S	W
E	E	T	T	O	B
E	A	C	L	O	U
D	F	L	O	A	T
I	N	G	I	N	T
H	E	B	L	U	E

Figure 4

1	2	3	**4**	5	6
7	8	**9**	**10**	**11**	12
13	**14**	15	16	17	18
19	20	**21**	**22**	**23**	24
25	26	27	28	29	**30**
31	32	33	34	35	**36**

Figure 5

1	**2**	**3**	4	5	6
7	8	9	**10**	11	12
13	14	**15**	16	**17**	18
19	**20**	21	22	**23**	24
25	26	27	28	29	**30**
31	32	33	34	**35**	**36**

Figure 6

1	2	3	4	5	**6**
7	**8**	9	**10**	**11**	12
13	14	15	16	**17**	18
19	**20**	21	22	**23**	24
25	**26**	27	28	**29**	30
31	32	33	34	35	**36**

Figure 7

The text written in an $n \times n$ table (n rows and n columns) can be n^2 letters long. If the length of the message is k letters (where obviously $k < n^2$) then the number of grids containing k windows is

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

To see how large this number is, consider the grid of *Figure 6.* Here $n = 6$, $k = 12$, the number of possible grids is therefore

$$\frac{36!}{12! \cdot 24!} = 31 \cdot 29 \cdot 28 \cdot 25 \cdot 17 \cdot 13 \cdot 9 = 1\,251\,677\,700.$$

The number of grids can be calculated in a similar way for *Figure 5* (where $n = 6$, $k = 13$).

Let us rotate the grid

In the *simple Cardan screen* described above, the choice of the positions of the windows was arbitrary. Let us consider now another technique for preparing the screen and filling out the table: the rotating screen. The rotating screen is an encryption device that can be rotated through 90 degrees about the center of the corresponding letter matrix, revealing each field in exactly one of the four positions.

The choice of the window positions is not arbitrary any more, as no field can be revealed by more than one window during the rotations. Each window has to have a different position after every rotations. It is clear that, for a rotating screen, n, the size of the matrix has to be even, as $k = \frac{n^2}{4}$ is the number of windows needed for revealing each field in exactly one of the four positions of the screen.

Let us illustrate the rotating screen with an example. Let $n = 6$ be the size of the grid. Thus we need 9 windows.

Step 1: Divide the 6×6 matrix into four zones as shown in *Figure 8.*

Step 2: Select k_1 fields from zone I, where $1 \leqslant k_1 \leqslant 9$. We have $k_1 = 2$, and fields 4 and 6 are selected. (See *Figure 9.*)

Step 3: Rotate the grid through 90 degrees and mark those fields of zone II that the chosen fields (4 and 6) cover. Then go on rotating the grid through 90 and mark the covered fields in each position. (See *Figure 9.*) Thus the choice of k_1 windows makes $4k_1$ fields covered.

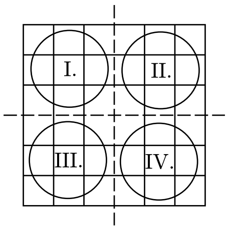


Figure 8

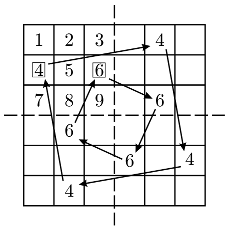


Figure 9

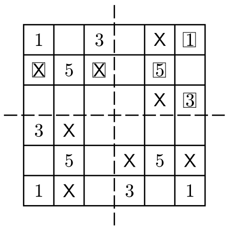


Figure 10

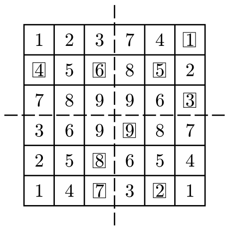


Figure 11

Step 4: Now select $k_2 = 3$ fields, still uncovered, from zone II. We have selected fields 1, 3 and 5. (See *Figure 10* where X marks the covered fields, the boxes around the numbers mark the windows, and the numbering of the fields of the zone corresponds to the rotated positions of the fields of zone I.) With the four rotations $4k_2$ more fields are covered.

Step 5: Repeat the above procedure in zones III and IV, too. Then $4k_1 + 4k_2 + 4k_3 + 4k_4 = n^2$, and we get $k = k_1 + k_2 + k_3 + k_4 = 9$ for the number of windows.[5] (See *Figure 11* where the boxed numbers represent the windows.)

Note that we are free to choose each of the k windows from any of the zones I–IV, and the number of all possible rotating $n \times n$ screens (with the maximum number of windows) is therefore $4^k = 4^{\frac{n^2}{4}}$. In our example, that is $4^9 = 262\,144$.

Question: *For a given grid size n and window number k, are there more simple screens or more rotating screens?*

[5]The number of windows can of course be less than that, but then the screen will not reveal all the fields during the rotation, and we cannot use the whole matrix for encryption.

The answer that the Reader will certainly find is as follows.

For the same grid size, there are much more simple screens than rotating screens. This comparison however is misleading from the cryptographical point of view, as the rotating screen makes it possible to write the letters of the plain text in the whole matrix[6], whereas the simple screen only uses a part of it.

As an illustration, see the *Figures 12, 13, 14, 15* for the encryption of the plain text in *Figure 3* using the screen of *Figure 11.*

	1	2	3	4	5	6
1						**O**
2	**H**		**O**		**W**	
3						**S**
4				**W**		
5			**E**			
6			**E**		**T**	

Figure 12

	1	2	3	4	5	6
1					**T**	O
2	H		O		W	
3	**O**	**B**			**E**	S
4			**A**	W		
5	**C**		E		**L**	
6			E	**O**	T	**U**

Figure 13

	1	2	3	4	5	6
1		**D**		**F**	T	O
2	H		O	**L**	W	
3	O	B	**O**		E	S
4	**A**		A	W		
5	C	**T**	E	**I**	L	**N**
6	**G**		E	O	T	U

Figure 14

	1	2	3	4	5	6
1	**I**	D	**N**	F	T	O
2	H	**T**	O	L	W	**H**
3	O	B	O	**E**	E	S
4	A	**B**	A	W	**L**	**U**
5	C	T	E	I	L	N
6	G	**E**	E	O	T	U

Figure 15

Step 1: On a blank sheet, draw a grid of the same size as the screen, and place the screen on the grid.

Step 2: Fill in the windows with the first nine letters of the plain text, proceeding left to right, row by row.

Step 3: Rotate the screen through 90 degrees, and repeat Step 2.

Step 4: Repeat Step 3 two more times.

The result is the letter matrix of *Figure 15* that is sent to the recipient, who can decrypt the message with an identical screen following Steps 1–4.

(Another interesting feature of our example is that with the simple screens of *Figures 5, 6, 7,* further hidden messages can be revealed from the decrypted text.)

It is an interesting historical addition to Cardan's screen that exactly 250 years after Cardan's *Ars Magna,* the German mathematician Carl Friedrich Hindenburg published a book[7] in which the entire Chapter VI focuses on cryptography, and on encryption screens in particular. He does not even mention Cardan's name (which is not unusual in the history of science and technology). Besides providing a detailed description of Cardan's screen, Hindenburg's book also shows possible improvements. It points out that if the sides of the screen are labelled by the letters a, b, c, d then the rotations of the screen can be represented by permutations of the four letters. This increases the number of possibilities by a factor of $4! = 24$.

[6]Encryption with a simple screen does not change the order of the letters of the plain text, while the rotating screen mixes the letters. Cryptography uses two kinds of encryption: substitution and transposition, and a cipher may use one of the two methods or a combination of them. The great cryptographical advantage of the rotating screen is the combination of the two methods. It should be noted, therefore, that quantity is not the only factor to consider when comparing ciphers.

[7]*Carl Friedrich Hindenburg:* Urchid der Reinenen und Angewandten Mathematic herausgegeben von Carl Friedrich Hindenburg, Leipzig, 1795.

Question: *How does the permutation change the encryption algorithm?*

As we shall see below, apart from their use in the process of preparing the grid permutations also play a role in the selection of the windows of the screen.

Permutations, Latin squares and encryption screens

A Latin square is an $n \times n$ square matrix whose rows and columns are permutations of the numbers $1, 2, \ldots, n$.

An $n \times n$ matrix is a permutation matrix if it contains exactly n 1's such that there is exactly one 1 in each row and column, and the remaining entries are all zeros. The following simple result is important from the point of view of encryption grids:

Every $n \times n$ Latin square $L(n)$ can be represented in one unique way in terms of n permutation matrices as follows:

$$L(n) = 1 \cdot P_1 + 2 \cdot P_2 + \ldots + n \cdot P_n, \tag{1}$$

Moreover, the 1's in the permutation matrix P_k appear in the positions where the Latin square $L(n)$ contains the number k.

(The operation of matrix addition as well as the multiplication of a matrix by a number is performed entry by entry.)

The permutation matrices obtained in this way can be used as encryption screens. The technique is illustrated by the following example:

$$L(4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 1 & 2 \end{bmatrix}$$

$$P_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad P_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad P_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad P_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Each permutation matrix P_i represents an encryption screen whose windows are in the positions of the 1's. Now, instead of rotation, one should place the permutation matrices as encryption screens over the letter matrix in order to encrypt or decrypt the message. As the theorem above ensures that the resolution into permutation matrices is unique, the windows of the screens thus produced reveal each of the n^2 fields exactly once, and therefore the entire letter matrix can be filled with the plain text, just like with rotating screens. As a further advantage, the uniqueness of the resolution of the Latin square remains valid if the order of the permutation matrices (screens) is changed. Thus the number of possibilities is $n!$ times the number of resolutions.[8]

[8] For lack of space, we can but briefly mention that every Latin square represents an operation table, which operations, under certain conditions, possess favorable properties

The problem with the practical application of encryption screens is that they require a lot of space, as the entire permutation matrix is needed for writing n characters into the letter matrix. This, being a binary matrix, takes n^2 bytes to be stored. If the permutation matrices are numbered, i.e. every $n \times n$ permutation matrix is assigned to a permutation of the numbers $1, 2, \ldots, n$ then the required memory space is reduced.

This kind of numbering only requires the positions of the 1's, as all the other entries are zeros. Suppose the entry in the i-th row and j-th column is 1. Then set the i-th element of the corresponding permutation equal to j. Since there is a single 1 entry in each row of the matrix the result is a permutation indeed.

We can apply an appropriate algorithm to assign numbers 1 to $n!$ to the permutations. If the permutation matrix is used as an encryption screen, then, instead of the actual matrix and the corresponding permutation it is enough to send its number along with the ciphertext.

Storing a permutation of the numbers $1, 2, \ldots, n$ requires $c(n)$ characters where[9]

$$c(n) = \big([\log n] + 1\big)n \tag{2}$$

The number of digits of the number $n!$ (denoted by $j(n)$) is

$$j(n) = [\log n! + 1]. \tag{3}$$

Hence

$$\frac{j(n)}{c(n)} = \frac{[\log n! + 1]}{n\big([\log n] + 1\big)} = \frac{\sum_{i=1}^{n} \log i + 1}{n\big([\log n] + 1\big)}, \tag{4}$$

and thus

$$\lim_{n\to\infty} \frac{j(n)}{c(n)} = 1. \tag{5}$$

However, for typical values of n, the above assignment is still useful in practice. The table below shows the values of $j(n)$ and $c(n)$ and that we can save 25–50% of memory space by storing and sending the number of the permutation instead of the permutation itself.

for encryption (non-commutative, non-associative). In a future paper we are going to discuss these properties and compare them to the number theoretical cipher systems that are so fashionable today.

[9] where $[x]$ denotes the greatest integer less than or equal to x.

n	$j(n)$	$c(n)$	$\dfrac{j(n)}{c(n)}$
10	7	20	.35
100	158	300	.526
200	375	600	.625
300	615	900	.683
400	869	1200	.724
500	1134	1500	.756

Table 1

A generalization of Cardan's screen: the k-screen (cobweb screen)

Both Cardan and Hindenburg used square screens. Now we show that the technique can be extended to arbitrary regular n-sided polygons.

Consider the construction in *Figure 16.* It is a regular polygon of k sides. Each side is $\frac{N}{2}$ units long, that is, the outermost layer of each sector consists of $N-1\left(=\frac{N}{2}+\frac{N}{2}-1\right)$ cells. There are $\frac{N}{2}$ layers in a sector, and $N-(2i-1)$ cells in the i-th layer. Hence the total number of cells in each layer is $\sum_{i=1}^{\frac{N}{2}} N-(2i-1)=\frac{N^2}{4}$. Thus the number of cells in the entire k-grid is $k\frac{N^2}{4}$. (In the case of Cardan's grid, $k=4$, and the result is the same as the number of cells in the square grid.)

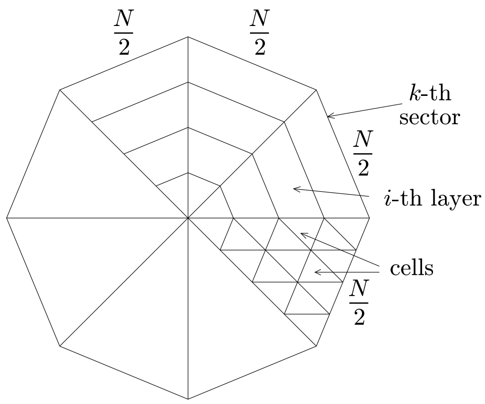


Figure 16

	1	2	3	4	...	.	.	.	$N-2i+1$
1	.	X	.	X	...	.	.	.	.
2	.	.	.	.	...	.	.	.	X
3	.	.	.	.	...	.	.	.	.
.	X	.	.	.	...	.	.	.	.
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
.	.	.	.	.	...	.	.	X	.
$k-1$	.	.	.	.	...	.	.	.	.
k	.	.	X	.	...	X	.	.	.

Figure 17

Obviously, the angle of rotation of the k-grid is not $90°$ any more, but $\frac{360°}{k}$. The real problem is how to choose the positions of the windows in the screen. Consider the matrix below (*Figure 17*) that has k rows (corresponding to the sectors of the k-grid) and $N-2i+1$ columns (the number of cells in the i-th layer). The X marks in *Figure 17* represent the windows. According to the rules of the rotating screen, there must be exactly one window in each column of the matrix. Hence the number of window combinations in the i-th layer is k^{N-2i+1}.

As the positions of windows in different layers are independent of each other, the total number of window combinations in the k-screen is

$$SC_k^N = \prod_{i=1}^{\frac{N}{2}} k^{N-2i+1} = k^{\sum\limits_{i=1}^{\frac{N}{2}} N-2i+1} = k^{\frac{N^2}{4}}. \tag{6}$$

It can be seen that for $k = 4$ this equals the number of possible Cardan screens. Hindenburg's permutations can also be applied here, which increases the number of possibilities by a factor of $k!$. The table below illustrates the number of possible k-screens for a few grid sizes.

k	N	SC_k^N	k	N	SC_k^N
3	4	81	4	10	1 125 899 906 842 624
3	6	19 683	5	4	625
3	8	43 046 720	5	6	1 953 125
3	10	847 288 598 528	5	8	152 587 894 784
4	4	256	6	4	1 296
4	6	262 144	6	6	10 077 696
4	8	4 294 967 296	6	8	2 821 109 841 920

Table 2

Finally, *Figure 18* shows a complete ciphertext matrix and *Figure 19* provides the corresponding Cardan screen (where the squares represent the windows). The decryption is left to the reader as an exercise, and the reader can use the screen for producing his own encrypted messages.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Y	O	H	T	N	C	E	.	E			M	U	P
2	,	O	T	N	S	A		A	T	Y		T	A	R
3	T	H	E	I	E		M	E	D	I		T	H	
4	E		M	R	E			G	W	A	T	O		O
5	R	G	O	E		S		O		A	A		W	N
6	T		B	H	E	D	O		I	S	E		M	E
7	K	E	R		H	Y		I	S	T	H		F	
8	A	R	I	N	D	E	R	Y	O	.	S	O	R	O
9		T	U	T	H		E	U	Y	N	E	,	A	.
10		O	N	W	S	K	E	E	E	H	E	N	T	
11	M	,	B	O	D			Y	T	H	E	E	T	
12	M	C	A	T	O		.	Y	R	A	E		A	N
13	D		S	,	N	C	S	A	I	A	I		D	C
14		T	N	T	H	E	G	.		B			O	A

Figure 18

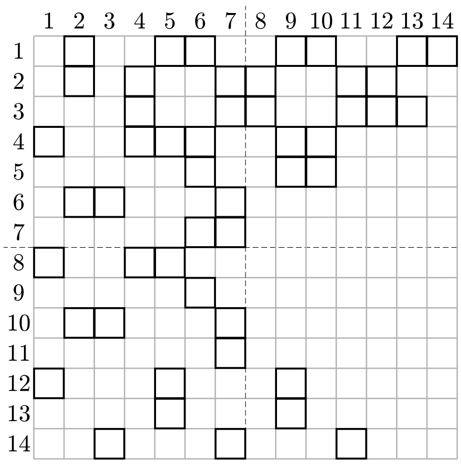


Figure 19

Tamás Dénes

Poncelet's theorem

The prisoner

J. V. Poncelet, a 24-year-old soldier of Napoléon was taken prisoner by Kutuzov's army while retreating from Moscow. In the severe winter of 1812–13, he and his fellows were marched 800 km across the Russian steppe to the prisoner camp of Saratov. In captivity, Poncelet recalled his studies completed recently, and the memories started to live a new life in his mind. With no access to a library, without any spiritual companion and tormented by physical pain, the young military engineer discovered new areas of geometry. He developed the concept of ideal points, he dreamed about a special mapping called polarity, and polygons were dancing around in his mind. Poncelet's theorem, the topic of this article, was also born there.

The prisoners who survived, including Poncelet, were released in the September of 1814. The engineer-mathematician's thoughts bred in captivity were published in 1822. His book was called "Treatise on the Projective Properties of Figures." The following theorem is from that book.

Poncelet's Theorem: *Let the circle a lie in the interior of a circle e, not touching it. Starting at an arbitrary point A_0 on e, the points $A_1, A_2, \dots$ of circle e can be successively constructed, such that the chords $A_0A_1, A_1A_2, \dots$ are all tangent to the circle a, and any two consecutive lines should be different.*

It may happen that we get back to A_0 in a finite number of steps, that is, $A_n = A_0$. In that case, we always end up at the starting point, no matter how it is chosen on the circle e, and the number of steps required will always be the same (n).

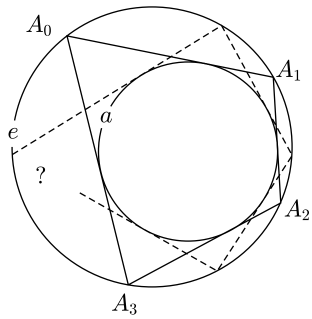


Figure 1

The theorem does not claim that this will always happen, but that whether or not we will get back depends on the size and mutual position of the two circles only and not on the particular choice of the starting point.

For concentric circles, the statement is obvious. In the general case, however, the proof is quite complicated. This innocent-looking theorem is not only interesting because of its romantic birth, but also because it leads us into the thick of 19th-century mathematics. Poncelet's result, to be stated in its general form two chapters below, is equivalent to the group property of cubic curves and to the addition theorems of elliptic functions, the generalizations of trigonometric functions.

Poncelet did formulate his theorem for arbitrary irreducible second order curves (see Problem 6) rather than circles. It is unnecessary for one curve to be inside the other one, but that kind of generalization would make the elementary treatment very difficult.

Pencils of circles

The (affine) equation of a circle a of radius r_1 centered at $O_a(u_a, v_a)$ is

$$(x-u_a)^2+(y-v_a)^2-r_a^2=0. \tag{1}$$

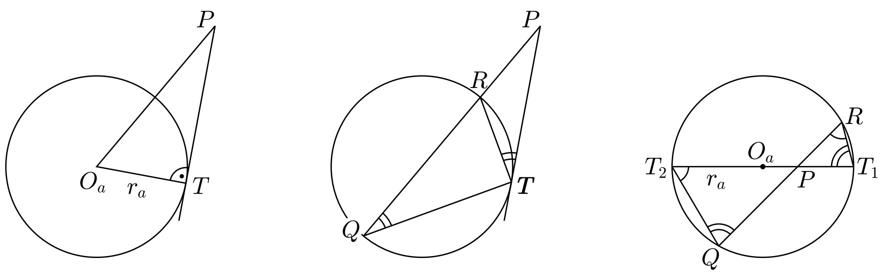
Let $a(x,y)$ denote the polynomial on the left-hand side as a function of x and y. If a point $P(\xi,\eta)$ lies on this circle then

$$a(\xi,\eta)=0,$$

and if not, then

$$a(\xi,\eta)\neq 0.$$

In the latter case, the value of $a(\xi,\eta)$ not only shows that P does not lie on the circle, but also the way it does not lie on it.



$O_aP^2-r_a^2=PT^2$ $\qquad$ $PR\cdot PQ=PT^2$ $\qquad$ $PR\cdot PQ=PT_1\cdot PT_2=O_aP^2-r_a^2$

Figure 2

The part $(\xi-u_1)^2+(\eta-v_a)^2$ of the expression $a(\xi,\eta)$ computes the square of the length of segment O_aP. If $a(\xi,\eta)$ is negative, it means that $O_AP^2<r_a^2$, that is, P lies in the interior of the circle a. If it is positive, then P lies outside the circle and $a(\xi,\eta)$ is equal to the square of the tangent drawn to the circle from P (*Figure 2*).

We can say a little more that that. It is true in both the positive and the negative case that for all secants drawn to the circle from P intersecting the circle at R and Q, the value of $PR\cdot PQ$ is constant, that is, independent of the choice of the secant. This can be proved with the help of similar triangles arising from the equal angles subtended by the chord at the points of a segment of a circle and the angle enclosed between the chord and the tangent drawn at its endpoints.

This constant value[1] of $PR \cdot PQ$ is also called the *power of the point P with respect to the circle a,* and it is equal to $O_aP^2 - r_a^2 = a(\xi, \eta)$.

Thus we can say that the equation

$$a(x, y) = t$$

is satisfied by those points whose power with respect to the circle a is t. For $t > 0$, these are the points for which the square of the tangent is t.

Let b be a circle different from a, with the equation

$$b(x, y) = (x - u_b)^2 + (y - v_b)^2 - r_b^2 = 0.$$

Consider the points for which the ratio of the tangents drawn to a and b is constant. Generally speaking, let c be the locus of those points in the plane whose power with respect to a and power with respect to b are in the ratio α to β. The equation of the set c is

$$\beta a(x, y) - \alpha b(x, y) = 0. \qquad (2)$$

This equation also represents a circle (or a point, or the empty set, or a line if $\alpha = \beta$), as it is an equation in two variables where the coefficients of x^2 and y^2 are equal (zero if $\alpha = \beta$) and there is no term in xy.

The set of curves of the form (2) is called the *pencil generated by a and b.* From any two elements of the pencil, every element can be obtained by means of a *linear combination.* Thus the pencil is generated by any two of its elements, that is, any two elements determine the system.

If a and b are two arbitrary circles of the pencil, and c is any element of the system, then the ratios of the powers of all points of c with respect to a and are the same.

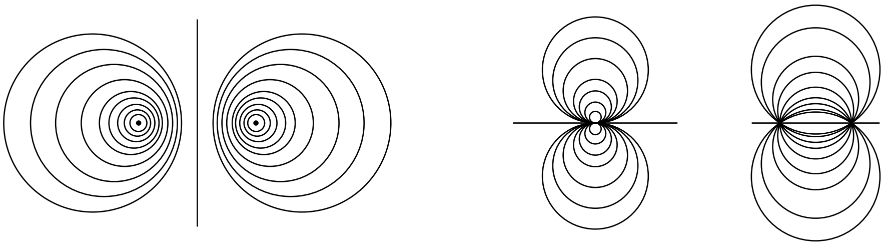


Figure 3

It is not hard to show that there are three kinds of pencils of circles: *non-intersecting, touching* and *intersecting.* In the first case, no two circles of the system share a common point, in the second case all the circles touch at one point, and in the third case they all pass through two common points. (See also Problems 1 and 2.)

[1] If PR and PQ are considered oriented segments then for interior points the product $PR \cdot PQ$ will be negative, as R and Q lie on opposite sides of R.

Poncelet's reasoning

In this chapter, there will be very little proof, it is rather an outline of Poncelet's reasoning. All the more, so, as the proof of the last chapter will also shed light to some of the details here.

A famous theorem by *L. Euler* establishes a relationship between the radii r and R of the inscribed and circumscribed circles of a triangle and the distance d of their centres:

$$R^2 - d^2 = 2Rr. \tag{3}$$

The proof can be found in Geometry Revisited by *H. S. M. Coxeter* and *S. L. Greitzer* (Theorem 2.1.2), but Problem 3 also provides some help.

Assume now that the task is to construct a triangle, given the radii of the circumscribed and inscribed circles and the distance between their centres. It follows from the theorem that if the three data do not satisfy condition (3) then there is no such triangle but there are infinitely many solutions if they do.

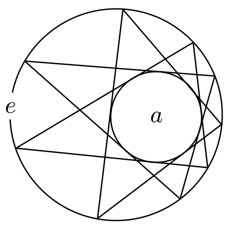


Figure 4

This is similar to constructing a triangle when the three angles are given. The solution only exists if the sum of the angles is 180°, but then there are infinitely many of them. In the latter case, one can even choose one side of the triangle arbitrarily, and still get a solution. Similarly, if the radii R and r of the circles e and a satisfy equation (3), then any point of e can be chosen as one vertex of the triangle circumscribed about a. Obviously, this statement requires a proof, see Problem 3 for a hint. From the statement and Euler's theorem, Poncelet's theorem follows for $n = 3$: the polygon will only close up in three steps if the condition (3) holds, but then it will close up wherever the starting point is.

Let us investigate *how the "imaginary" triangles corresponding to data not satisfying equation* (3) *fail to exist.* The steps of Poncelet's proof and the way he complains about the lack of constructing tools in the foreword of his book suggest that this was the question the imprisoned engineer wanted to answer.

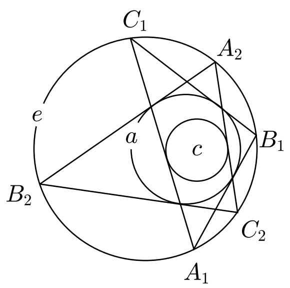


Figure 5

Figure 5 shows an attempt to construct a triangle when the data are inconsistent. The circles e and a correspond to such a situation. From an arbitrary point A of the circle e, a tangent is drawn to a. The tangent intersects e at the next vertex B of the triangle. C is obtained by drawing the other tangent to a from B. As the line AC does not touch a, it is clear that the construction was not successful. After a number of similar attempts, Poncelet must have noticed (as that is what he has proved) that although none of the lines AC obtained by the construction touch the circle a, they all do touch a certain other circle c.

What is more, this circle c belongs to the pencil generated by e and a. This is particularly apparent in the case of intersecting circles a, e, when the construction of the triangle is obviously hopeless.

Thus the triangles do not exist "by following a very regular pattern." It has turned out that beyond triangles and their two circles Euler's theorem has also something to say about the polygon that snakes its way between the circles of a pencil.

The observations lead to the following generalization of the above construction problem:

Let a given circle e and the circles a, b, c in its interior all belong to the same pencil. Construct a triangle, such that its circumscribed circle is e, and its sides AB, BC, AC touch that the circles a, b, c, respectively.

There are two tangents to a circle from an exterior point. In order to eliminate the ambiguity as to which tangent to draw in the construction, let us define a fixed sense of rotation for each of the circles a, b, c, and require that the directions of $\overrightarrow{AB}$, $\overrightarrow{BC}$, $\overrightarrow{CA}$ on the sides of the triangle ABC to be constructed should all have the same orientation that the circles they touch.

The solution of the construction problem is similar to that of the above problem, but now the proof is even more difficult. As before, the difficulty does not lie in the construction itself, but in the discussion of whether there are solutions in various cases: For appropriate circles e, a, b, c (and appropriate orientation on a, b, c) the construction will always produce a unique triangle, whichever point of e is chosen as a starting point. In general, furthermore, one can notice again that the lines AC always touch a certain element c' of the pencil, and they always touch it in the same orientation. This circle c', however, is different from the given c in most of the cases. Now we are not investigating when does this circle c' coincide with c, as it is surprising enough that such a c' should exist at all.

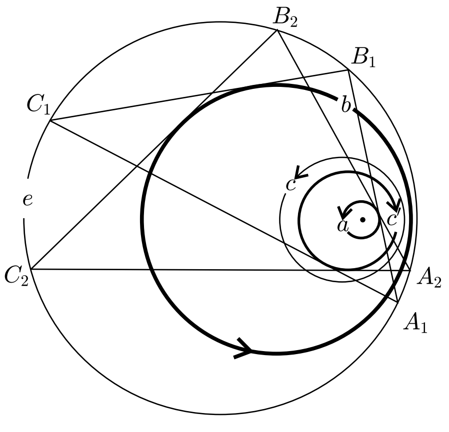


Figure 6

Consider now the mapping defined on the set of points of the circle e that maps the point $X \in e$ onto the point where the tangent drawn from X in the appropriate direction to the (directed) circle a intersects the circle e again. If the circle a coincides with e, then this mapping is defined to be the identity that maps the points of e onto themselves. If they are concentric but not identical, the mapping is a simple rotation. In any other case, it is not a rotation, only similar to it. That kind of mapping is called an "oblique rotation". The composition of two consecutive rotations about the same point is equivalent to a single rotation through an angle equal to the sum of the two angles of rotation.

According to the above observation, the first part of this statement can be generalized: The composition of the oblique rotations with respect to the directed circle a and then with respect to the directed circle b is also an oblique rotation, the one determined by the circle c' above. Jacobi's proof will show what is the number, or measure that corresponds to the angle of rotation in the general case. As if on the set $\mathbb{P}$ comprising the circle e and the oriented circles of the pencil lying in its interior, including the one point circle (see Problem 2) there were an operation $\circledast$ that corresponds to the composition of oblique rotations:

$$a \circledast b = c'.$$

What Poncelet actually did, although he did not even mention such abstract algebraic concepts, was to show that this operation was associative and commutative. Thus the set $\mathbb{P}$ is a commutative group, in other words an Abelian group, with respect to the above operation, as the remaining group axioms also hold: e is the identity element, and the inverse of a given circle is the very same circle but oriented in the opposite way.

As a result of his argument, Poncelet arrived at a much more general statement than the one stated above:

Poncelet's General Theorem: *Let e be a circle of a non-intersecting pencil and let $a_1, a_2, \dots, a_n$ be (not necessarily different) oriented circles in the interior of e that belong to the same pencil. Starting at an arbitrary point A_0 of the circle e, the points $A_1, A_2, \dots, A_n$ are constructed on the same circle, such that the lines $A_0A_1, A_1A_2, \dots, A_{n-1}A_n$ touch the circles $a_1, a_2, \dots, a_n$, respectively, in the appropriate direction. It may happen that at the end of the construction, we get back to the starting point, that is, $A_n = A_0$. The theorem states that in that case, we will always get back to the starting point in the n-th step, whichever point of e we start from. We do not even need to take care to draw the tangents to the circles in a fixed order.*

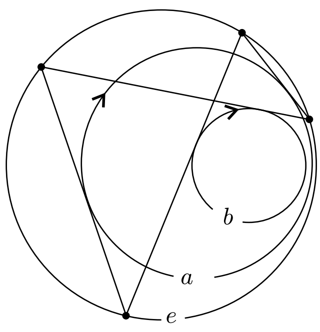


Figure 7

Proof. The composition of the oblique rotations of the circle e with respect to the circles $a_1, a_2, \dots, a_n$ is equivalent to the oblique rotation determined by the directed circle

$$b = a_1 \circledast a_2 \circledast \cdots \circledast a_n$$

of the pencil. This transformation maps the point A_0 onto itself, thus the tangent drawn to the directed circle b from A_0 cannot intersect the circle e, it must be tangent to e, too. Hence $b = e$, as all other elements of the pencil lie inside e, and cannot touch it either. The oblique rotation corresponding to e is the identity, therefore if we start at any other point instead of A_0, we will get back to that point again. As the group is commutative, the order of the tangents drawn to the given circles does not matter either.

The case of $a_1 = a_2 = \cdots = a_n = a$ gives Poncelet's theorem as stated above. In that case it is not necessary to assign a direction to the circles, as the reversal of the orientation of the circle a (or any one of $a_1, a_2, \ldots, a_n$ in the general case) only results in the very same tangents drawn, but in reverse order and in opposite direction.

Elliptic integrals

In 1827, J. Steiner set the following problem in the *Journal für die reine und angewandte Mathematik*[2]:

If a pentagon is both cyclic and circumscribed, what is the relationship between the radii of the two circles and the distance between their centres? Solve the same problem for polygons of 6, 7, 8, 9 *and* 10 *sides, too.*

Based on Poncelet's theorem, Steiner asked for the algebraic condition for the polygon to close up. Steiner knew the solution in these cases, but he did not set the problem in vain. It raised Jacobi's interest, and Jacobi found a new and extraordinary proof for Poncelet's theorem.

Jacobi was working on elliptic integrals at the time. The problem of elliptic integrals was born out of the investigations of Prince G. Fagnano into the properties of the *ellipse* and the *lemniscate.* Fagnano wanted to determine the length of the arc that belongs to a chord of length t drawn from the origin in the lemniscate $(x^2+y^2)^2 = x^2 - y^2$. J. Bernoulli and L. Euler also faced an equivalent question in their studies of elasticity. Neither of them managed to find the function $I(t)$ expressing the length of the lemniscate arc.

What Fagnano achieved was finding the length of the chord that belongs to an arc twice as long as the arc that belongs to t. Euler generalized the method by providing an *addition formula* to express the length of the chord that belongs to the arc whose length is the sum of the lengths of the arcs that belong to the chords of lengths t_1 and t_2. He even went beyond that: He described a wide collection of arc length and area problems (*integrals,* in general) where such an addition formula can be found. These are called elliptic integrals.

Jacobi also had remarkable results in this area. In competition with N. H. Abel, they published one article after another in the above mentioned journal. For a change, Jacobi also tried Steiner's problem. He constructed a diagram, drew a few lines in it, expressed their lengths, and to his surprise, he obtained formulae that were strikingly similar to the addition formulae of elliptic integrals. The formulae

[2] The *Journal for Pure and Applied Mathematics* was founded by the Prussian engineer A. L. Crelle, encouraged by Abel and Steiner himself.

showed that there was a quantity, an integral that increases by the same amount with each additional side of the Poncelet polygon. In the case of concentric circles, this quantity is the central angle corresponding to the polygon. In that special case, each “tangent chord” between the two circles has the same length, and thus the corresponding central angles are also equal. If n times the central angle is 360° or a multiple of it, the polygon will close up in n steps, and otherwise it will not.

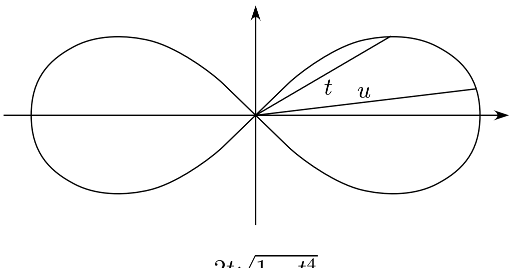


Figure 9. If $u = \dfrac{2t\sqrt{1-t^4}}{1+t^4}$ then $I(u) = 2I(t)$

Jacobi concluded from the formulae that there is a measure analogous to the central angle in the general case, too. As far as the proof was concerned, it did not matter what the geometrical meaning of the measure was. This is important to emphasize, as however logical the following proof is, and however easy to follow, Jacobi discovered it by an entirely different logic, with an entirely different approach.

Jacobi's proof

The task is to introduce a measure on the circle e of Poncelet's theorem that assigns the same number to the arcs PP' and QQ' if the lines PP' and QQ' both touch the circle a.

Let us try arcs lying close to each other first. It would also be good if the measures of the arcs PQ and $P'Q'$ were equal. Those small arcs have almost the same length as the segments PQ and $P'Q'$. The segments are, unfortunately, not equal in length, but there is a simple relationship between them. Since the angles subtended at the circumference of circle e are equal, the triangles PQT and $Q'P'T$ are similar. Thus

$$\frac{PQ}{PT} = \frac{P'Q}{Q'T}. \tag{4}$$

The denominators approach the lengths of the tangents drawn to the circle a from the points of the arcs PQ and $P'Q'$. Therefore, if the opposite arcs PQ and $P'Q'$ are to be assigned the same measure then each of them should be weighted with the reciprocal of the tangent drawn from its points to the circle a.

This idea is easy to visualize. Surround the circle e with a surface perpendicular to the plane of the circle, like the lateral surface of a cylinder. The base of the surface is the circle itself, but its height should vary pointwise. At a point P of the circle, set the height of the surface equal to the reciprocal of the length of the tangent drawn from P to the circle a. The area of the surface is the measure required.

We claim that the areas corresponding to the arcs PQ and $P'Q'$ are equal. Each side of equation (4) is an approximation of those areas. The lengths of the

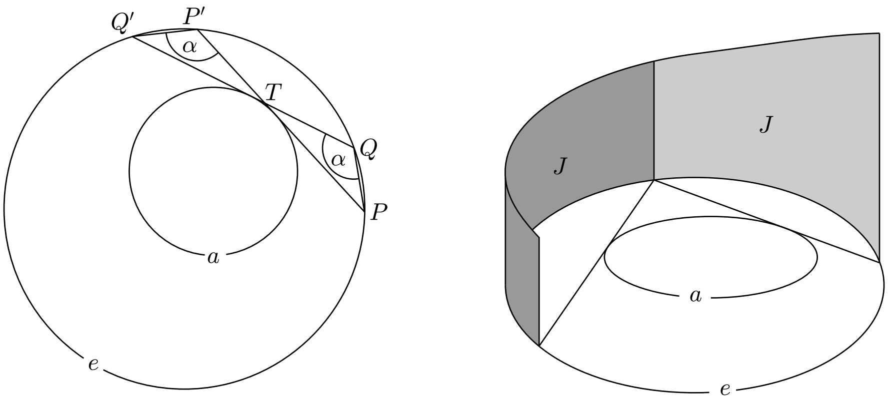


Figure 10

segments PQ and $P'Q'$ approach the lengths of the arcs PQ and $P'Q'$, respectively, and the values of $\dfrac{1}{PT}$ and $\dfrac{1}{Q'T}$ approach the heights of the surface over the arcs. A better approximation of these areas is obtained if the arc PQ and the arc $P'Q'$ opposite are divided into smaller pieces, and each of the smaller pieces is estimated separately with the product of the chord and the corresponding approximate height. If this is always done according to the formula corresponding to the two sides of equation (4), then the areas obtained for the surfaces over the arcs PQ and $P'Q'$ will always be equal. With this technique, the areas over the two arcs can be approached by equal quantities to any desired precision, which is only possible if the two areas themselves are equal.

It follows now that the areas over the arcs PP' and QQ' are also equal. Let the points P and P' move along the circle e so that the chord PP' should remain tangent to the circle a. It follows from the above considerations that the area over the arc PP' will also remain constant. Let the value of that constant area be J, and let the area of the whole surface be I.

Poncelet's polygon will close up in n steps going around e m times if and only if $mI = nJ$. This condition is independent of the choice of the starting point A_0. This completes the proof of Poncelet's theorem. Note that Poncelet's polygon will close up if and only if the quotient $\dfrac{J}{I}$ is rational, and the number of steps required for getting back to the starting point is the denominator of this rational number.

The area of the Jacobi surface has the same property as the arc length of the lemniscate. The arc is a transcendent function of the length of chords from a given point, that is, it cannot be expressed with a finite number of elementary functions. But it is possible to generalize Fagnano's duplication formula and set up a formula for multiplying the arc by n, and that will solve the generalized Steiner problem. This work, however, was only completed 25 years later by A. Cayley.

With a little modification, Jacobi's method can also be used for proving the generalized Poncelet theorem. In order to do so, fix a point E on the circle e and define the height of the lateral surface at the point P as the ratio of the tangents drawn to the circle a from the points E and P: $h(P) = \dfrac{EE_A}{PP_A}$, which differs only by the constant factor EE_A from the above defined height. The motivation for this definition is that it makes the height universal, that is each element of the pencil determines the same surface. This is explained by one of the results obtained above. We have seen that if a, b, e are three elements of a pencil of circles then the ratios of the powers of different points of e with respect to a and b (i.e. the ratios of the tangents, in our case) are equal:

$$\frac{EE_A}{EE_B} = \frac{PP_A}{PP_B}, \quad \text{that is,} \quad \frac{EE_A}{PP_A} = \frac{EE_B}{PP_B}.$$

If I is the area of the whole surface and $J_1, J_2, \dots, J_n$ are the areas over the arcs determined by the tangents drawn to the elements $a_1, a_2, \dots, a_n$ of the pencil then the condition for the polygon to close up is described by the equation

$$J_1 + J_2 + \dots + J_n = mI.$$

The validity of this equation is clearly independent of the choice of the starting point.

Problems

1. *a*) Show that the centres of the members of any pencil of circles are collinear.

b) Let the radius of one circle of a pencil be R, let the radius of another, smaller circle be r, and let d be the distance of their centres. Prove that the value of

$$k = \sqrt{\frac{4Rd}{(R+d)^2 - r^2}}$$

is independent of the choice of the smaller circle.

c) Show that the pencil is concentric, non-intersecting, tangent and intersecting, respectively if $k = 0$; $0 < k < 1$; $k = 1$; $1 < k$.

2. Prove that in non-intersecting, tangent and intersecting pencils, respectively there are 2; 1; 0 *one point circles,* i.e. figures of equation

$$(x-u)^2 + (y-v)^2 = 0.$$

3. The circumscribed circle of a triangle ABC is e and its incircle is a. Their radii are R and r, respectively, and the distance of their centres is d. The points of tangency on the incircle are X, Y, Z.

a) Prove that the inversion of the circle e with respect to the circle a maps e onto a circle of radius $R' = \dfrac{Rr^2}{R^2 - d^2}$, and its centre's distance from the centre of a is $d' = \dfrac{dr^2}{R^2 - d^2}$.

b) Prove that the inversion with respect to the circle a maps the points A, B, C onto the midpoints of the sides of the triangle XYZ.

c) Prove Euler's theorem.

d) Prove Poncelet's theorem for $n = 3$.

4. Find the formula corresponding to Euler's theorem for the circumscribed and *escribed* circles of the triangle.

5. *a*) Prove that the equation of the element of the pencil generated by the circles $a(x,y) = 0$, $b(x,y) = 0$ that passes through the point $P(\xi,\eta)$ is

$$b(\xi,\eta)a(x,y) - a(\xi,\eta)b(x,y) = 0.$$

b) Prove that the equation of the line touching the circle of equation (1) at its point $P(\xi,\eta)$ is

$$(\xi - u_a)(x - \xi) + (\eta - v_a)(y - \eta) = 0.$$

c) Prove that the points of tangency on the tangents drawn form a point to the elements of a pencil of circles form a cubic curve.

6. *a*) Express the equation corresponding to (1) in homogeneous coordinates, and show that the ideal and imaginary points $(1, i, 0)$ and $(1, -i, 0)$, where $i^2 = -1$, lie on the circle.

b) Prove that a nonempty irreducible quadratic curve of real coefficients is a circle if and only if it contains the points $(1, i, 0)$ and $(1, -i, 0)$.[3]

Bibliography

[1] H. S. M. Coxeter and S. L. Greitzer: *Geometry Revisited,* Random House (New York, 1967).

[2] M. Berger: *Géométrie* (chapter 16.6); CEDIC/Fernand Nathan (Paris, 1977).

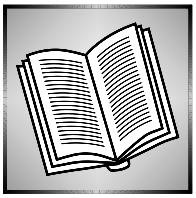
[3] A. Shen: Mathematical entertainments, Poncelet Theorem Revisited; *The Mathematical Intelligencer,* vol. 20, n. 4 (1998), page 31.

[4] R. Ayoub: The lemniscate and Fagnano's contribution to elliptic integrals; *Archive for history of Exact Sciences,* vol. 29, n. 2 (1984), pages 131–149.

[5] H. J. M. Bos, C. Kers, F. Oort and D. W. Raven: Poncelet's closure theorem; *Expositiones Mathematicae,* vol. 5 (1987), pages 289–364.

András Hraskó

[3]The introduction of complex numbers into geometry is also a result of Poncelet's considerations. He pointed out that if complex coordinates are allowed then any two quadratic curves have two common points. If those two points are projected to the points $(1, i, 0)$ and $(1, -i, 0)$ then the two curves are mapped onto two circles. Thus it is enough to prove Poncelet's theorem for two circles.



Remarks to the Olympiad

We investigate Problem 6 of the International Mathematical Olympiad of this year. This article presents two solutions.

The first one, like the solution of Problem 2, does not make use of any special idea, and does not require anything beyond high-school mathematics, but it starts with a surprising step that might look discouraging at the first sight.

The second solution requires much more mathematical background. It uses as extension of the set of integers, the theory of the so-called Eulerian integers. This is the price for revealing the most probable origin of the problem.

Problem 6. *Let a, b, c, d be integers, such that $a > b > c > d > 0$. Given that*

$$ac + bd = (b + d + a - c)(b + d - a + c), \tag{6}$$

show that $ab + cd$ is not a prime number.

By rearranging equation (6), we have

$$a^2 - ac + c^2 = b^2 + bd + d^2. \tag{7}$$

Let us use this form from now on.

Solution 1: Substitute.

The proof is indirect. Assume that $ab + cd = p$, where p is a prime. We have the simultaneous equations

$$a^2 - ac + c^2 = b^2 + bd + d^2, \quad ab + cd = p. \tag{8}$$

The number of unknowns and equations can be reduced by expressing some appropriate expression out of one equation and substituting it into the other. In order to make calculations more convenient, let us consider everything modulo p.

According to the second equation, $ab \equiv -cd \pmod{p}$. Multiply equation (7) by b^2, and substitute $-cd$ for ab:

$$0 = b^2(b^2 + bd + d^2 - a^2 + ac - c^2) = b^4 + b^3d + b^2d^2 - (ab)^2 + ab \cdot bc - b^2c^2 \equiv$$

$$\equiv b^4 + b^3d + b^2d^2 - (cd)^2 - cd \cdot bc - b^2c^2 = (b + c)(b - c)(b^2 + bd + d^2) \pmod{p}.$$

The resulting expression is a product of three factors, one of which is equal to the quantity in equation (7). It follows from the congruence that one of the three factors $b + c$, $b - c$ and $b^2 + bd + d^2$ is divisible by p, as we assumed that p was a prime. The numbers $b + c$ and $b - c$ are positive and less than $ab + cd = p$, and thus cannot be divisible by p. There remains the only possibility that b^2+bd+d^2 is divisible by p. As

$$0 < b^2+bd+d^2 < ab+ab+cd < 2(ab+cd) = 2p,$$

the number b^2+bd+d^2 can only be divisible by p if it equals p. Hence the simultaneous equations to solve are

$$a^2-ac+c^2 = b^2+bd+d^2 = ab+cd = p. \tag{9}$$

No it is easy to show the contradiction. Consider equation (9) modulo a (as a is the largest one of the unknowns). It follows that $c(c-d) = ab+ac-a^2$ is divisible by a. But that is impossible, as a and c are relative primes (or otherwise $ab+cd$ could not be a prime), and $0 < c-d < a$.

Solution 2: With a little help form Euler.

It is clear to anyone who has read about them that equation (7) is closely related to Eulerian integers.

Let ϱ be a complex third root of unity. The complex numbers of the form $x+y\varrho$, where x and y are integers, are called Eulerian integers. Eulerian integers form a lattice of regular triangles in the complex plane (*Figure 1*).

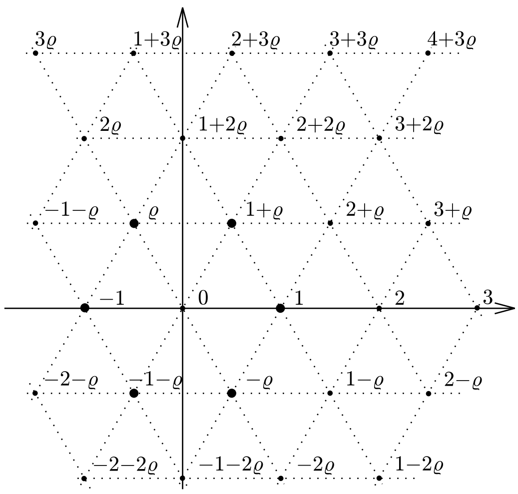


Figure 1

This number set has several remarkable and useful properties. Leonhard Euler also used these numbers when he proved Fermat's last theorem for the exponent 3. Let us briefly summarize the most important concepts and theorems related to Eulerian integers that will be needed in the proof.

Addition, subtraction and multiplication of Eulerian integers are defined in the natural way. Remember that $\varrho^2 = -\varrho - 1$:

$$(x+y\varrho) \pm (u+v\varrho) = (x \pm u) + (y \pm v)\varrho;$$

$$(x+y\varrho)(u+v\varrho) = xu + (xv+yu)\varrho + yv\varrho^2 = (xu-yv) + (xv+uy-yv)\varrho.$$

The commutative, associative and distributive properties of addition and multiplication of integers or real numbers are also valid for Eulerian integers. The properties of the numbers 0 and 1 also remain valid: for example if 0 is added to any Eulerian integer, the sum equals the original number, or 0 times any Eulerian integer is 0.

The *conjugate* of an Eulerian integer $\alpha = x + y\varrho$ is the number $\overline{\alpha} = x + y\varrho^2 = (x - y) - y\varrho$.

There is a very important quantity called the norm of an Eulerian integer. The norm of an Eulerian integer $\alpha = x + y\varrho$ is denoted by $N(\alpha)$ and defined as follows:

$$N(\alpha) = \alpha \cdot \overline{\alpha} = x^2 - xy + y^2.$$

The norm is always a non-negative integer, and 0 is the only number whose norm is 0.

The norm is clearly equal to the square of the modulus of the complex number. Thus the norm of a product is the product of the norms of the factors:

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta).$$

An Eulerian integer α is a *factor* of an Eulerian integer β if there exists an Eulerian integer γ such that $\alpha\gamma = \beta$. It follows from the multiplicativity of the norm that if $\alpha \mid \beta$ then $N(\alpha) \mid N(\beta)$. (The latter divisibility is meant in the set of rational integers.)

There are six Eulerian integers whose norm is 1. They are called *units* and marked in *Figure 1.* The units divide all Eulerian integers.

Two Eulerian integers are said to be associate if they are obtained from each other by multiplication with a unit, that is, by rotation about 0 through a multiple of 60°.

A non-unit Eulerian integer π is said to be *irreducible* if its only factors are the units and itself.

A non-unit and non-zero Eulerian integer π is said to be a *prime* if $\pi \mid \alpha\beta$ implies $\pi \mid \alpha$ or $\pi \mid \beta$ for any Eulerian integers α, β. In order to distinguish the primes in the system of Eulerian integers from real primes, let us call them *Eulerian primes.*

The most important theorems of the theory of Eulerian integers are the following

1. Irreducible Eulerian integers are the same as Eulerian primes.
2. The fundamental theorem of number theory is valid for Eulerian integers, too: Every non-zero and non-unit Eulerian integer can be expressed as a product of Eulerian primes and units, and the representation is unique up to associates, that is, in any two representations, the corresponding factors are associates of each other.
3. The real primes of the form $3k + 2$ are also Eulerian primes. The primes of the form $3k + 1$ can be reduced to the product of two non-associate Eulerian primes (e.g. $7 = (3 + \varrho)(2 - \varrho)$). The prime factor decomposition of 3 is $3 = -\varrho^2(1 - \varrho)^2$.

The theorems show that there is a close relationship between the prime factors of an Eulerian integer α and the prime factors of $N(\alpha)$. The square of each prime factor $3k + 2$ of α occurs in the prime factor decomposition of $N(\alpha)$, and so do the norms of all the other prime factors, which are either 3 or primes of the form $3k+1$.

For example, let $\alpha = 10 + 8\varrho$. Its resolution into Eulerian primes is $2\cdot(2+\varrho)(3+\varrho)$ and that of its norm is $N(\alpha) = N(2)\cdot N(2+\varrho)\cdot N(3+\varrho) = 2^2\cdot 3\cdot 7$.

Conversely, the prime factors of $N(\alpha)$ "almost determine" the prime factors of α. All prime factors $3k+2$ of $N(\alpha)$ are also prime factors of α (with half the exponent), and each factor of 3 in the resolution of $N(\alpha)$ is the norm of the Eulerian prime $1-\varrho$. The prime factors $3k+1$ of $N(\alpha)$ are also norms of prime factors of α, but there are two possible Eulerian primes in each case, even if associates are not considered different.

Back to the problem: let $\alpha = a + c\varrho$ and $\beta = b - d\varrho$. According to the given condition, $a^2 - ac + c^2 = b^2 + bd + d^2$, that is, $N(\alpha) = N(\beta)$. We have to prove that $ab+cd$, that is, the "real part" of $\alpha\beta = (ab+cd) + (bc+cd-ad)\varrho$, cannot be a prime.

As $N(\alpha) = N(\beta)$, the prime factors of the two Eulerian integers are "almost the same". They have some prime factors in common, and the remaining factors are pairwise conjugate. This can be put as follows:

$$\alpha = \varepsilon_1 \cdot \pi_1 \cdots \pi_k \cdot \mu_1 \cdots \mu_l \quad \text{and} \quad \beta = \varepsilon_2 \cdot \pi_1 \cdots \pi_k \cdot \overline{\mu}_1 \cdots \overline{\mu}_l, \tag{10}$$

where $\pi_1, \ldots, \pi_k$ and $\mu_1, \ldots, \mu_l$ are Eulerian primes and ε_1, ε_2 are units.

Let $\gamma = \pi_1 \cdot \ldots \cdot \pi_k$ and $\delta = \mu_1 \cdot \ldots \cdot \mu_l$ as above. Then

$$\alpha = \varepsilon_1\gamma\delta \quad \text{and} \quad \beta = \varepsilon_2\gamma\overline{\delta}.$$

(It may happen that there are only common or only different prime factors in α and β; then, of course $\gamma = 1$, or $\delta = 1$.)

Consider now the number

$$\alpha\beta = (ab+cd) + (bc+cd-ad)\varrho = \varepsilon_1\varepsilon_2\gamma^2 \cdot N(\delta). \tag{11}$$

This number is divisible by $N(\delta)$, and thus $ab+cd$ and $bc+cd-ad$ are also divisible by $N(\delta)$. What remains to prove is that neither $N(\delta) = 1$ nor $ab+cd = N(\delta)$ is possible.

If $N(\delta) = 1$, that is $\delta = 1$, then α and β are associates, which means that they can be obtained from each other by a few 60° rotations about 0. The number of these rotations is determined by the arguments of α and β.

It follows from the condition $a > b > c > d > 0$ that the argument of α is between 0° and 60°, and that of β is between -30° and 0° (*Figure 2*). Thus the difference of the arguments is between 0° and 90°, and hence the angle of rotation is exactly 60°, that is $\alpha = (1+\varrho)\beta$. But then,

$$\alpha = a + c\varrho = (1+\varrho)(b - d\varrho) = (b+d) + b\varrho,$$

which is impossible, as $b > c$. Thus the assumption $N(\delta) = 1$ leads to a contradiction.

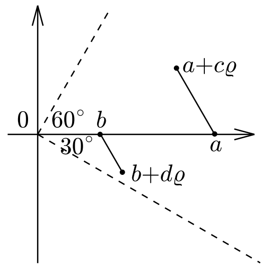


Figure 2

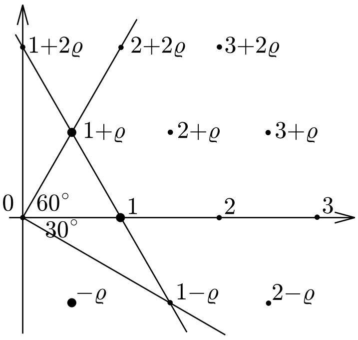


Figure 3

If $ab+cd=N(\delta)$, then by dividing equation (11) by $N(\delta)$ we get

$$\frac{\alpha\beta}{N(\delta)}=\frac{ab+cd}{N(\delta)}+\frac{ad+bc-cd}{N(\delta)}\cdot\varrho=\varepsilon_1\varepsilon_2\cdot\gamma^2.$$

This number, as shown by the right-hand side, is an Eulerian integer. Its argument is the sum of the arguments of α and β, which is between $-30°$ and $60°$, and its "real part" is $\dfrac{ab+cd}{N(\delta)}=1$, by assumption. The only Eulerian integer satisfying this requirement is 1 (*Figure 3*), hence $\varepsilon_1\varepsilon_2\gamma^2=1$ and $\alpha\beta=N(\delta)$.

Thus the product of the numbers α and β is the positive real number $N(\delta)$. As $N(\alpha)=N(\beta)$, it follows that the two numbers are conjugates. But then

$$\alpha=a+c\varrho=\overline{\beta}=\overline{b-d\varrho}=b+d(1+\varrho)=(b+d)+d\varrho,$$

which is impossible, as $c>d$. The assumption $ab+cd=N(\delta)$ also leads to a contradiction. This completes the proof.

Solution 2 not only proves the statement of the problem, but also provides a construction for finding appropriate numbers a, b, c, d with $a>b>c>d$ and

$$a^2-ac+c^2=b^2+bd+d^2.$$

All we need to do is find Eulerian integers of the appropriate arguments.

For example, setting

$$\alpha=a+c\varrho=(4+\varrho)(3+\varrho)=11+6\varrho,\quad \beta=b-d\varrho=(4+\varrho)\overline{(3+\varrho)}=9-\varrho,$$

$a=11$, $b=9$, $c=6$ and $d=1$, with

$$a^2-ac+c^2=b^2+bd+d^2=91.$$

(Obviously, $ab+cd=105$ is not a prime.)

Géza Kós

Solutions to the problems of the Kürschák Competition, 2001

1. *Given $3n-1$ points in the plane, no three of which are collinear, show that it is possible to select $2n$ points, such that their convex hull should not be a triangle.*

Solution 1. The claim is obvious if $n=1$. For $n>1$, we have to prove that there exist $2n$ among the given points, such that their convex hull has at least 4 vertices. If we manage to find $m \geqslant 2n$ points whose convex hull has at least 4 vertices, then $m-2n$ of them can be deleted so that the convex hull of the remaining points should still have at least 4 vertices.

Thus if the convex hull of the set $\mathcal{P}$ of the points is not a triangle then we are done. Therefore we can assume that the convex hull of $\mathcal{P}$ is a triangle $A_1B_1C_1$. Assume that for some $i<n$, we have already defined the points $A_1,\dots,A_i$, such that for all $j \leqslant i$ the convex hull of the set $\mathcal{P}\setminus\{A_1,\dots,A_{j-1}\}$ is the triangle $A_jB_1C_1$. The set $\mathcal{P}\setminus\{A_1,\dots,A_i\}$ has at least $2n$ elements, thus by the previous argument we can assume that the convex hull of that set is also a triangle. Two vertices of that triangle are clearly B_1 and C_1. Let A_{i+1} denote the third vertex.

Thus we have shown that if it is not possible to select $2n$ points whose convex hull is not a triangle, then there exists a sequence $A_1,A_2,\dots,A_n$ of points in $\mathcal{P}$, such that for all $i \leqslant n$, the convex hull of $\mathcal{P}\setminus\{A_1,\dots,A_{i-1}\}$ is the triangle $A_iB_1C_1$. The point sequences $B_1,B_2,\dots,B_n$ and $C_1,C_2,\dots,C_n$ can be constructed in the same way. Among the $3n$ points hence obtained, there must be two points that coincide. Without the loss of generality we can assume that $A_j=B_k$. Then the set

$$\mathcal{P}\setminus\{A_1,A_2,\dots,A_n\}\setminus\{B_1,B_2,\dots,B_n\}\setminus\{C_1\}$$

has at least $n-1 \geqslant 1$ elements, all of which are interior points of both triangles $A_jB_1C_1$ and $B_kA_1C_1$. But that is impossible, as the two triangles have no common interior points. This contradiction proves the claim.

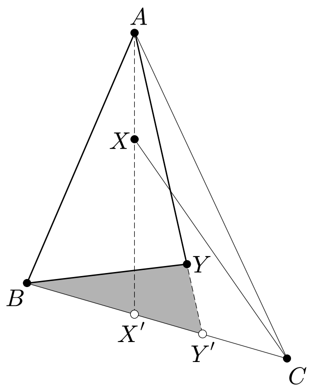
Remarks. 1. It is not hard to show that the number of points in the problem cannot be decreased to $3n-2$: Let $A_1B_1C_1$ be an equilateral triangle with centre O, and let A, B, C be the midpoints of OA_1, OB_1, OC_1, respectively. Let k_A, k_B, k_C be circular arcs of radius R that connect A_1 and A, B_1 and B, C_1 and C, respectively. Finally, let the points $A_2,\dots,A_n$, $B_2,\dots,B_{n-1}$, $C_2,\dots,C_{n-1}$ lie on the arcs k_A, k_B, k_C. If $n \geqslant 2$ and R is big enough then it is not possible to select $2n$ points of the $(3n-2)$-element set $\mathcal{P}=\{A_1,\dots,A_n,B_1,\dots,B_{n-1},C_1,\dots,C_{n-1}\}$, such that their convex hull should not be a triangle. This is true because if R is big enough then each line A_iA_j separates the points B_k and C_ℓ. Thus if A_i and A_j are both vertices of the convex hull of a subset of $\mathcal{P}$, then it may contain at most $n-1$ points other than $A_1,\dots,A_n$, and therefore the subset itself may contain at most $2n-1$ points. Similar reasoning applies if the convex hull contains at least two of the points B_i or the points C_i as vertices. Therefore, the convex hull of every $2n$-element subset may only contain one A_i, one B_i and one C_i as vertices, and that makes it necessarily a triangle.

2. For any real number x denote the smallest integer not smaller than x by $\lceil x \rceil$. It can be shown that the claim can be improved as follows:

Let $n \neq 3$. Given $\lceil 3n/2 \rceil - 1$ points in the plane, no three of which are collinear, it is possible to select n of them, such that their convex hull is not a triangle.

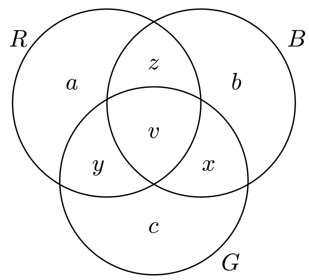
The two solutions below prove this stronger statement. Note that the condition makes sense for positive integer n only, and that for $n \leqslant 2$ the claim obviously holds. Thus, in what follows, n is greater than 3. If n is odd, then a minor adjustment of the previous counterexample shows that the claim fails to hold if the number of points is reduced to $\lceil 3n/2 \rceil - 2$.

Solution 2. Assume that $\mathcal{P}$ is a set of at least $\lceil 3n/2 \rceil - 1$ points that does not contain n points whose convex hull is not a triangle. Let the convex hull of $\mathcal{P}$ be the triangle ABC, and let $A_1 = A$. As in Solution 1, construct the sequence $A_1, A_2, \ldots, A_{\lceil n/2 \rceil}$ such that for all $i \leqslant \lceil n/2 \rceil$, the convex hull of $\mathcal{P} \setminus \{A_1, \ldots, A_{i-1}\}$ is the triangle A_iBC.



Consider the points $A_2, \ldots, A_{\lceil n/2 \rceil}$ in counterclockwise order as seen from the point A. Let X and Y denote the first and last of them, respectively. Let X' and Y' be the intersections of lines AX and AY with the segment BC. We can assume, without loss of generality, that the order of points on the line BC is B, X', Y', C. One of the triangles BCX and BCY contains the other one. The smaller one of the two triangles, which is covered by the union of triangles BYY' and CXX', contains the set $\mathcal{P}' = \mathcal{P} \setminus \big\{A_1, A_2, \ldots, A_{\lceil n/2 \rceil}, B, C\big\}$. $\mathcal{P}'$ has at least $n-3$ elements. We can clearly assume that at least half of these points lie inside the triangle BYY' (*figure*). Select $\big\lceil (n-3)/2 \big\rceil$ ones out of these points and denote this set by $\mathcal{P}''$. Finally, let $\mathcal{Q} = \mathcal{P}'' \cup \Big\{A_1, A_2, \ldots, A_{\lceil n/2 \rceil}, B\Big\}$. $\mathcal{Q}$ has $\big\lceil (n-3)/2 \big\rceil + \lceil n/2 \rceil + 1 = n$ elements, each of which lies either inside the triangle $AY'B$ or on its boundary. Thus the points A, Y, B lie on the convex hull of Q. However, the convex hull of Q must also contain at least one point of the set $\mathcal{P}''$, contradicting the assumption that $\mathcal{P}$ does not contain n points whose convex hull is not a triangle.

Solution 3 (by *G. Lippner*). As explained in Solution 1, we can assume that the convex hull of the points is a triangle ABC. Consider the points lying in the interior of this triangle ABC. Colour the segments connecting any two of the given points red, blue or green, depending on which side of the triangle they do not intersect: AB, BC, or CA, respectively. Let R, B, G, denote the sets of points incident to red, blue, green segments, respectively. Since $n \geqslant 4$, there must be at least 2 points in the interior of triangle ABC, therefore the set $R \cup B \cup G$ is the same as the set of points inside the triangle, and thus it has $\lceil 3n/2\rceil - 4$ elements. We show that one of the sets R, B, G must have at least $n-2$ elements.



Let us represent the sets on a Venn diagram. The letters denote the number of elements in the corresponding subsets.

If, say, $a \neq 0$, then there is a point in the interior of the triangle that is connected to each of the other points with a red segment. Then

$$|P| = \lceil 3n/2\rceil - 4 \geqslant n-2,$$

as $n \geqslant 4$. Therefore, we can assume that $a = b = c = 0$. Hence

$$|R \cup B \cup G| = x + y + z + v.$$

Now if each of

$$|R| = y + z + v, \quad |B| = z + x + v \quad \text{and} \quad |G| = x + y + v$$

were smaller than $n-2$, then this would imply the inequality

$$3n - 8 \leqslant 2\big(\lceil 3n/2\rceil - 4\big) = 2(x+y+z+v) \leqslant |R| + |B| + |G| \leqslant 3(n-3) = 3n-9,$$

a contradiction.

Therefore, it is true that one of the sets has at least $n-2$ elements. Assume that $|R| \geqslant n-2 \geqslant 2$. Consider the set $R' = R \cup \{A, B\}$. R' has at least n elements, and its convex hull contains the vertices A and B. Let $D \in R$, and let E be a point in R for which the segment DE is red. As the line DE does not intersect the segment AB, E cannot be in the interior of triangle ABD. Hence the convex hull of R' cannot be a triangle. Now it is clearly possible to select a subset of at least $n \geqslant 4$ elements from R', such that their convex hull is not a triangle either.

2. *Let $k \geqslant 3$ be an integer, and $n > \binom{k}{3}$. Prove that if a_i, b_i, c_i $(1 \leqslant i \leqslant n)$ are $3n$ distinct real numbers then there are at least $k+1$ different numbers among the numbers $a_i + b_i$, $a_i + c_i$, $b_i + c_i$. Show that the statement is not necessarily true for $n = \binom{k}{3}$.*

Solution 1. Assume that the statement is not true, that is, there are at most k different numbers among the sums $a_i + b_i$, $a_i + c_i$, $b_i + c_i$. Let T denote the set of these numbers. It is obvious that for every $1 \leqslant i \leqslant n$, the numbers $a_i + b_i$, $a_i + c_i$, $b_i + c_i$ are pairwise different, and thus form a 3-element subset of T. Furthermore, if $a_i + b_i = x$, $a_i + c_i = y$, $b_i + c_i = z$ then $a_i = (x+y-z)/2$, $b_i = (x+z-y)/2$, $c_i = (y+z-x)/2$, and thus, the set $\{x, y, z\}$ uniquely determines the set $\{a_i, b_i, c_i\}$. As

$$\binom{|T|}{3} \leqslant \binom{k}{3} < n,$$

there exist indices $1 \leqslant i < j \leqslant n$, such that $\{a_i, b_i, c_i\} = \{a_j, b_j, c_j\}$, contradicting to the condition.

For the second part, consider the set $T = \{t_1, t_2, \ldots, t_k\}$, where $t_i = 4^i$. Let $n = \binom{k}{3}$, and let $T_1, T_2, \ldots, T_n$ denote the 3-element subsets of T. If $T_i = \{4^u, 4^v, 4^w\}$, where $1 \leqslant u < v < w \leqslant k$ are integers, then let

$$a_i = (4^u + 4^v - 4^w)/2, \quad b_i = (4^u + 4^w - 4^v)/2 \quad \text{and} \quad c_i = (4^v + 4^w - 4^u)/2.$$

Clearly $a_i + b_i, a_i + c_i, b_i + c_i \in T$. Hence it is enough to show that the numbers a_i, b_i, c_i $(1 \leqslant i \leqslant n)$ are all different.

$a_i = b_j$ or $a_i = c_j$ are not possible for any i, j, as the numbers a_i are all negative, whereas b_j and c_j are all positive. $b_i = c_j$ is not possible either, as each b_i lies in some interval $(2^{2s-2}, 2^{2s-1})$, while each c_i lies in an interval of the form $(2^{2s-1}, 2^{2s})$ where $3 \leqslant s \leqslant k$ is an integer.

Now let $T_i = \{4^u, 4^v, 4^w\}$ and $T_j = \{4^x, 4^y, 4^z\}$, where $1 \leqslant u < v < w \leqslant k$ and $1 \leqslant x < y < z \leqslant k$ are integers. Suppose that $c_i = c_j$. Then

$$4^v + 4^w - 4^u = 4^y + 4^z - 4^x.$$

As $4^w < 4^v + 4^w - 4^u < 4^{w+1}$, and $4^z < 4^y + 4^z - 4^x < 4^{z+1}$, this can happen only if $w = z$, and thus $4^v - 4^u = 4^y - 4^x$. Here $4^{v-1} < 4^v - 4^u < 4^v$ and $4^{y-1} < 4^y - 4^x < 4^y$, and therefore equality can hold only if $v = y$ and then necessarily $u = x$ and $i = j$. Thus the numbers c_i are all different. A similar reasoning shows that the numbers a_i and the numbers b_i are all different. That completes the proof.

Solution 2. This is a different proof for the first part of the problem, by *D. Kiss.* Assume again, to the contrary, that there are at most k different numbers among the $3n$ sums. Then there is a sum that occurs at least $\frac{3n}{k} > \binom{k-1}{2}$ times. Let a denote that sum. If two of the sums $a_i + b_i$, $b_i + c_i$ and $a_i + c_i$ were equal to a for some i, then there would be two equal numbers among a_i, b_i and c_i. Thus we can assume that for all $1 \leqslant i \leqslant \binom{k-1}{2} + 1$, exactly one of the sums $a_i + b_i$, $b_i + c_i$ and $a_i + c_i$ equals a. Now the remaining $2\left(\binom{k-1}{2} + 1\right)$ sums can assume only $k - 1$ different values. Therefore, there is a value, some b, that occurs at least

$$2\left(\binom{k-1}{2} + 1\right) \Big/ (k-1) > k - 2$$

times. By the previous argument, we can assume that for all $1 \leqslant i \leqslant k - 1$, one of the sums $a_i + b_i$, $b_i + c_i$, $a_i + c_i$ is a and another one is b. The $k - 1$ sums still remaining can only assume $k - 2$ different values, and hence two of them are equal. But then the corresponding numbers a_i, b_i, c_i are also equal. This contradiction proves the statement.

In what follows there are further constructions for the second part of the problem.

Solution 3. Consider the set $T = \{t_1, t_2, \dots, t_k\}$, where $t_i = 3^i$. Let $\{x, y, z\}$ and $\{u, v, w\}$ be two 3-element subsets of the set $\{1, 2, \dots, k\}$. As in Solution 1, it is enough to show that if

$$\frac{3^x + 3^y - 3^z}{2} = \frac{3^u + 3^v - 3^w}{2},$$

then the two subsets are necessarily equal, and $z = w$. It follows from the equality that

$$3^x + 3^y + 3^w = 3^u + 3^v + 3^z = A.$$

If A is written in base-3 notation, then its non-zero digits contain either three 1's, or one 1 and one 2, as $x = y = w$ is not possible. The base-3 notation of a number is unique, thus in the first case, $\{x, y, w\}$ and $\{u, v, z\}$ are the same 3-element subsets of the set $\{1, 2, \dots, k\}$. Since $x, y \neq z$, this yields $w = z$ and hence $\{x, y\} = \{u, v\}$, indeed. In the second case we have that $\{x, y, w\}$ and $\{u, v, z\}$ are identical 2-element subsets of $\{1, 2, \dots, k\}$. As $x \neq y$, this subset must be identical to the set $\{x, y\}$ and this would imply $z \in \{x, y\}$ which is impossible.

Solution 4. As also suggested by the above solutions, it is enough to show that for every positive integer k, there exists a set $T_k = \{t_1, t_2, \dots, t_k\}$ for which $t_x + t_y + t_z = t_u + t_v + t_w$ is true if and only if the numbers x, y, z are identical to the numbers u, v, w in some order. Then it is easy to show that the $3\binom{k}{3}$ numbers of the form $(t_x + t_y - t_z)/2$ (where $\{x, y, z\}$ is an arbitrary 3-element subset of the set $\{1, 2, \dots, k\}$) are all different.

If $k = 1$, then $t_1 = 1$ is obviously a good choice. It is enough to show that there exists an infinite sequence $t_1, t_2, \dots, t_i, \dots$, such that for all $i \geqslant 2$, t_i cannot be expressed in the form $r_1 t_1 + \dots + r_{i-1} t_{i-1}$, where $r_1, \dots, r_{i-1}$ are rational numbers. Indeed, assuming that such a sequence exists, consider the set T_k, and suppose that $t_x + t_y + t_z = t_u + t_v + t_w$ for some $1 \leqslant x, y, z, u, v, w \leqslant k$. Let i be the greatest one of the indices x, y, z, u, v, w. Now if t_i does not occur the same number of times on both sides of the equality, then rearrangement yields an equality of the form $t_i = r_1 t_1 + \dots + r_{i-1} t_{i-1}$. Thus i occurs the same numbers of times among x, y, z as among u, v, w. Cancelling the terms equal to t_i on both sides, and repeating the above procedure, one finally concludes that the numbers x, y, z indeed coincide with u, v, w in some order.

Assume, therefore, that $k > 1$ and the numbers $t_1, \dots, t_{k-1}$ have already been determined according to the above requirement. Then the infinite set of numbers that can be expressed in the form $r_1 t_1 + \dots + r_{k-1} t_{k-1}$ is denumerable, while the set of all real numbers is not. Thus, there exists a real number t_k that cannot be expressed in the form $r_1 t_1 + \dots + r_{k-1} t_{k-1}$. Hence the existence of a sequence of the required property follows directly from the principle of mathematical induction.

Remark. 1. The last solution uses a non-constructive method to prove the existence of an appropriate sequence $t_1, t_2, \dots, t_i, \dots$. It can be shown that the choice $t_i = \sqrt{p_i}$, for example, yields a suitable sequence. (p_i denotes the i-th positive prime number.) The proof, however, is beyond the scope of this article.

2. As observed by *A. T. Kocsis,* the problem can be generalized as follows. Let $k \geqslant t \geqslant 3$ be integers and $n > \binom{k}{t}$. If $a_{i1}, a_{i2}, \ldots, a_{it}$ $(1 \leqslant i \leqslant n)$ are tn different real numbers then there are at least $k+1$ different numbers among the sums $\sum_{j=1}^{t} a_{ij} - a_{ik}$ $(1 \leqslant i \leqslant n,\ 1 \leqslant k \leqslant t)$, but this is not necessarily so if $n = \binom{k}{t}$. The proof is left to the reader as an exercise as it does not require any new idea.

3. The story is entirely different if we ask about two term sums. It is clear that if $k \geqslant 3$ is an integer, $n > \binom{k}{3}$, and a_i, b_i, c_i, d_i $(1 \leqslant i \leqslant n)$ are $4n$ different real numbers, then there are at least $k+1$ different numbers among the sums $a_i + b_i$, $a_i + c_i$, $a_i + d_i$, $b_i + c_i$, $b_i + d_i$, $c_i + d_i$. Surprisingly enough this cannot be improved significantly. You can think about the following problem: for every integer $k \geqslant 3$, there exist $4\binom{k}{3}$ different real numbers a_i, b_i, c_i, d_i $\left(1 \leqslant i \leqslant \binom{k}{3}\right)$, such that there are at most $2k$ different numbers among the sums $a_i + b_i$, $a_i + c_i$, $a_i + d_i$, $b_i + c_i$, $b_i + d_i$, $c_i + d_i$.

3. *In a square lattice, consider any triangle of minimum area that is similar to a given triangle. Prove that the centre of its circumscribed circle is not a lattice point.*

Solution 1 (by *B. Gerencsér*) Consider a lattice triangle whose circumcentre is also a lattice point. We can assume, without loss of generality, that one vertex (A) is the origin. Let the coordinates of the other two vertices be $B = (a, b)$ and $C = (c, d)$, and let the circumcentre be $O = (x, y)$.

From the equality of the segments OA and OB, the Pythagorean theorem yields $x^2 + y^2 = (a-x)^2 + (b-y)^2$. Hence $a^2 + b^2$ is even, and thus so are $a+b$ and $a-b$. By a similar argument, $c+d$ and $c-d$ are also even numbers.

Consider now the lattice triangle $A_1B_1C_1$, where

$$A_1 = A, \quad B_1 = \left(\frac{a+b}{2}, \frac{a-b}{2}\right) \quad \text{and} \quad C_1 = \left(\frac{c+d}{2}, \frac{c-d}{2}\right).$$

In this triangle,

$$A_1{B_1}^2 = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{a^2+b^2}{2} = \frac{AB^2}{2},$$

$$A_1{C_1}^2 = \left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = \frac{AC^2}{2}$$

and

$$B_1{C_1}^2 = \left(\frac{a+b-c-d}{2}\right)^2 + \left(\frac{a-b-c+d}{2}\right)^2 = \frac{(a-c)^2 + (b-d)^2}{2} = \frac{BC^2}{2}.$$

Hence the lengths of the sides of the triangle $A_1B_1C_1$ are $\frac{1}{\sqrt{2}}$ times the corresponding sides of the triangle ABC, and thus we have found a lattice triangle similar to the triangle ABC, but of smaller area. This proves the statement.

Solution 2. Assume that the circumcentre O of a lattice triangle H is also a lattice point. Let (x, y) be the coordinates of one of the side vectors, and let (a, b) and (c, d) be the coordinates of the position vectors of the endpoints of that side. Then a, b, c, d, x, y are integers, and from the Pythagorean theorem,

$$x^2 + y^2 = (a - c)^2 + (b - d)^2 = (a^2 + b^2) + (c^2 + d^2) - 2(ac + bd).$$

As $a^2 + b^2 = c^2 + d^2$ (the square of the radius of the circumscribed circle), $x^2 + y^2$ and thus also $(x + y)^2$ is an even number. It follows that $x + y$ and $x - y$ are also even.

By rotating the vector (x, y) through an angle of $45°$ about the origin in the positive direction, we get the vector $\left(\frac{x-y}{\sqrt{2}}, \frac{x+y}{\sqrt{2}}\right)$. An enlargement of scale factor $\frac{1}{\sqrt{2}}$ yields the vector $\left(\frac{x-y}{2}, \frac{x+y}{2}\right)$ which is a vector of integer coordinates.

Thus we have shown that by a rotation through $45°$ and an enlargement of scale factor $\frac{1}{\sqrt{2}}$, H is mapped onto a similar but smaller triangle. This proves the statement.

Remark. The diagonals drawn from one vertex of a cyclic polygon divide the polygon into triangles. As all these triangles have a common circumcentre, the statement of the problem is also valid for any cyclic polygon not just a triangle.

Gyula Károlyi

Mathematics and physics quiz

(from the Conference of KöMaL*)

1. The foci of an ellipse are $F_1(9, 20)$ and $F_2(49, 55)$. The ellipse touches the x-axis. How long is the major axis? 53 (1); 72 (2); 85 (X).

2. How many data are needed to determine the elastic behaviour of a single crystal? Two (e.g. the Young modulus and the torsional modulus) (1); six (two for each axis of the crystal) (2); more than twenty (X).

3. Consider the sequence $1001, 1004, 1009, \ldots$ where $a_n = 1000+n^2$. Let d_n denote the greatest common terms of neighbouring divisor of the sequence, that is $d_n = (a_n, a_{n+1})$. What is the maximum of the numbers d_n? 2001 (1); 4001 (2); the sequence d_n is not bounded (X).

*The questions are based on the suggestions of I. Varga and J. Pataki.

4. The diameter of a 4.5-cm-long string of liquid is 0.2 mm. If the string falls apart 'by itself" into identical spherical droplets, what is the maximum possible number of droplets formed? 100 (1); 200 (2); 300 (X).

5. How many multiplications are needed for calculating 2001^{2001}? 1000 (1); at least 17 (2); 16 (X).

6. A spherical raindrop is falling at a rate of $2\ \frac{\mathrm{m}}{\mathrm{s}}$. What will be the falling speed of a single spherical drop formed out of two such drops? $2^{\frac{7}{6}}\ \frac{\mathrm{m}}{\mathrm{s}}$ (1); $2^{\frac{5}{6}}\ \frac{\mathrm{m}}{\mathrm{s}}$ (2); $4^{\frac{1}{3}}\ \frac{\mathrm{m}}{\mathrm{s}}$ (X).

7. If $f(n)$ denotes the number of zeros in the decimal notation of the number n then the value of

$$S = 2^{f(1)} + 2^{f(2)} + \cdots + 2^{f(999\,999)}$$

is 1 594 404 (1); 1 495 404 (2); 1 595 440 (X).

8. Two point-like objects of different masses are attached to the ends of a massless rigid rod. The rod is placed on the table in vertical position and released. The rod will fall over. In which case will the upper end of the rod hit the table at greater speed? If the large mass is at the upper end (1); if the smaller mass is at the upper end (2); the speed is the same in both cases (X).

9. If A is the smallest multiple of 27 that only contains ones and zeros in decimal notation then the number of digits of A is 27 (1); 9 (2); 10 (X).

10. A tetrahedron of uniform mass distribution is placed onto a horizontal tabletop. At most how many such faces may it have that it should fall over if placed onto that face? At most one (1); at most two (2); at most three (X).

11. How many positive even numbers are there that cannot be expressed as the sum of two positive odd composite numbers? 13 (1); 14 (2); 43 (X).

12. In the gym, there is a rigid rod and a rope hanging from the ceiling. They have the same length and mass and they are free to rotate about their upper ends. The lower end of each object is pulled by a horizontal force of the same magnitude until equilibrium is reached. The lower end of which object will rise higher? The rod (1); the rope (2); they will both rise to the same height (X).

13. How many numbers out of the first 2001 positive integers can be expressed in the form

$$[x] + [2x] + [4x] + [8x]$$

(where $[x]$ denotes the greatest integer not greater than x)? 1001 (1); 1067 (2); 1113 (X).

13 + 1. Three identical compass needles are placed at the vertices of an equilateral triangle. They can rotate in the plane of the triangle. There is no external magnetic field. What will be the equilibrium position of the needles? The north (or south) pole of each needle will point towards the centre of the triangle (1); each needle will be parallel to the opposite side of the triangle (2); neither of the above (they will be in some different position) (X).

Preparatory problems for the entrance exam of high school

1. Solve the following equation on the set of real numbers:

$$\frac{2x+2}{7}=\frac{(x^2-x-6)(x+1)}{x^2+2x-3}.$$

2. For what positive integers a is the value of the following expression also an integer?

$$\left(\frac{a+1}{1-a}+\frac{a-1}{a+1}-\frac{4a^2}{a^2-1}\right):\left(\frac{2}{a^3+a^2}-\frac{2-2a+2a^2}{a^2}\right)$$

3. Given that the second coordinates of the points $A(1,a)$, $B(3,b)$, $C(4,c)$ are

$$a=-\frac{\sin 39^\circ+\sin 13^\circ}{\sin 26^\circ\cdot\cos 13^\circ},\qquad b=\sqrt{10^{2+\log_{10}25}},\qquad c=\left(\frac{1}{\sqrt{5}-2}\right)^3-\left(\frac{1}{\sqrt{5}+2}\right)^3$$

determine whether the three points are collinear.

4. What is more favourable:
I. If the bank pays 20% annual interest, and the inflation rate is 15% per year, or
II. if the bank pays 12% annual interest, and the inflation rate is 7% per year?

5. The first four terms of an arithmetic progression of integers are a_1, a_2, a_3, a_4. Show that $1\cdot a_1^2+2\cdot a_2^2+3\cdot a_3^2+4\cdot a_4^2$ can be expressed as the sum of two perfect squares.

6. In an acute triangle ABC, the circle of diameter AC intersects the line of the altitude from B at the points D and E, and the circle of diameter AB intersects the line of the altitude from C at the points F and G. Show that the points D, E, F, G lie on a circle.

7. The base of a right pyramid is a triangle ABC, the lengths of the sides are $AB=21$ cm, $BC=20$ cm and $CA=13$ cm. A', B', C' are points on the corresponding lateral edges, such that $AA'=5$ cm, $BB'=25$ cm and $CC'=4$ cm. Find the angle of the planes of triangle $A'B'C'$ and triangle ABC.

8. Let $f(x)=2x^6-3x^4+x^2$. Prove that $f(\sin\alpha)+f(\cos\alpha)=0$.

László Számadó

Solution of exercises for practice C

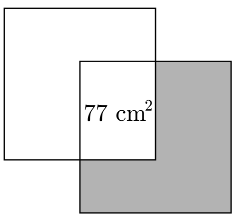
C. 607. *The sides of a square are* 12 cm *long. If the square is rotated through* 90° *about the point* P*, the total area covered by the two squares is* 211 cm^2*. If the rotated square is rotated again through* 90° *about* P*, a third square is obtained. The total area covered by the three squares is* 287 cm^2*. Where is the point* P*?*

Suggested by *G. Bakonyi,* Budapest

Solution. The result of the second rotation is the reflection of the original square in the point P. If P is not inside the original square, then the mirror image has no common point with the original one and thus the total area of the three squares must be greater than $2 \cdot 144~\mathrm{cm}^2 = 288~\mathrm{cm}^2$.

Assume that there is a point P in the interior of the square, such that if the square is rotated through 90° about P, the total area is 211 cm^2. The area of one square is 144 cm^2, and the area of the overlapping part is $2 \cdot 144~\mathrm{cm}^2 - 211~\mathrm{cm}^2 = 77~\mathrm{cm}^2$. By subtracting the overlapping area from the area of the square, we get $144~\mathrm{cm}^2 - 77~\mathrm{cm}^2 = 67~\mathrm{cm}^2$.

The first rotation increased the area by this amount (the shaded region in the *figure*). The 2nd square is now rotated about P through 90°. As the rotated image of the 1st square is the 2nd one, and the rotated image of the 2nd square is the 3rd one, the rotated image of the common part of the 1st and 2nd squares is necessarily the common part of the 2nd and 3rd squares. Thus the total covered area may increase by at most the same amount as the previous time, that is, the covered area cannot exceed $211~\mathrm{cm}^2 + 67~\mathrm{cm}^2 = 278~\mathrm{cm}^2$, as opposed to the given 287 cm^2. Therefore, no such point P exists.



B. Udvari, Baja

Solutions of problems B

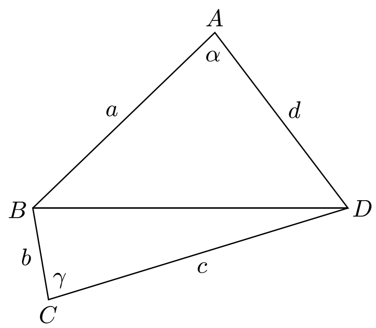
B. 3416. *A convex polyhedron is bounded by quadrilateral faces, its surface area is* A*, and the sum of the squares of its edges is* Q*. Prove that* $Q \geqslant 2A$*.*

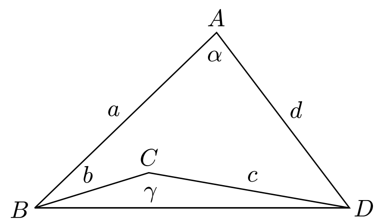
Proposed by *Á. Besenyei,* Tatabánya

Solution. First we prove that the sum of the squares of the sides of any quadrilateral is at least four times its area. Using the notations of the *figure,* the area of the quadrilateral is

$$A_{ABCD} = A_{ABD} \pm A_{BCD} \leqslant A_{ABD} + A_{BCD} = \frac{a \cdot d \cdot \sin\alpha}{2} + \frac{b \cdot c \cdot \sin\gamma}{2} \leqslant \frac{ad + bc}{2}.$$

From the inequality between the arithmetic and geometric means, $ad \leqslant \dfrac{a^2 + d^2}{2}$ and $bc \leqslant \dfrac{b^2 + c^2}{2}$, and thus $4A_{ABCD} \leqslant a^2 + b^2 + c^2 + d^2$, as stated above.





If the corresponding inequality is set up for each face of the polyhedron, and the inequalities are summed, the left-hand side will be $4A$, and the right-hand side will be $2Q$, as each edge belongs to two faces of the convex polyhedron. Therefore, $4A \leqslant 2Q$, and hence $2A \leqslant Q$, and we are done.

Based on the solution by *A. Babos,* Budapest

B. 3429. *Let* $q = \dfrac{1 + \sqrt{5}}{2}$, *and let* $f\colon \mathbb{N} \to \mathbb{N}$ *be a function, such that for all positive integers* n,

$$\big|f(n) - qn\big| < \frac{1}{q}.$$

Prove that $f\big(f(n)\big) = f(n) + n$.

Solution. As $\dfrac{1}{q} > \big|f(0)\big|$, obviously $f(0) = 0$. For any other n, the value of f is a positive integer, otherwise $f(n) = 0 < n$ would imply $\dfrac{1}{q} > \big|f(n) - qn\big| = |-qn|$ and hence $n < \dfrac{1}{q^2} < 1$, which is impossible. It is easy to check, furthermore, that $q(q-1) = \dfrac{\sqrt{5}+1}{2} \cdot \dfrac{\sqrt{5}-1}{2} = 1$. Thus for any natural number n,

$$\begin{aligned}\Big|f\big(f(n)\big) - f(n) - n\Big| &= \Big|f\big(f(n)\big) - qf(n) + (q-1)f(n) - q(q-1)n\Big| = \\ &= \Big|f\big(f(n)\big) - qf(n) + (q-1)\big(f(n) - qn\big)\Big|.\end{aligned}$$

As the inequality $|a+b| \leqslant |a|+|b|$ holds for all real numbers a, b, the above absolute value can be at most

$$\left|f\big(f(n)\big)-qf(n)\right|+\left|(q-1)\big(f(n)-qn\big)\right|=\left|f\big(f(n)\big)-qf(n)\right|+(q-1)\left|f(n)-qn\right|,$$

which is less than $\dfrac{1}{q}+(q-1)\dfrac{1}{q}=1$ according to the condition. Hence

$$\left|f\big(f(n)\big)-f(n)-n\right|<1,$$

which can only happen if $f\big(f(n)\big)-f(n)-n=0$, as $f\big(f(n)\big)$, $f(n)$ and n are integers.

G. Bóka, Szolnok

B. 3463. *The diameter of a semicircular sponge is* 20 cm *long. Find the area wiped by the sponge in the corner of the floor of a room if the endpoints of the diameter slide along the two walls enclosing a right angle.*

Solution. The sponge is a semicircular disc of diameter AB. If A is moving along the x-axis and B is moving along the y-axis then the circle of diameter AB passes through O. Therefore, no point of the wiped region is farther away from the point O than 20 cm, no points outside the quadrant of radius 20 cm centred at O can be reached by the sponge.

The points of the quadrant of radius 10 cm centred at O are covered by the semicircles whose diameters lie along the x and y axes (*Figure 2*).

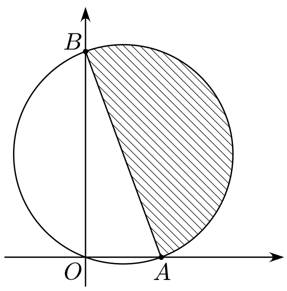


Figure 1

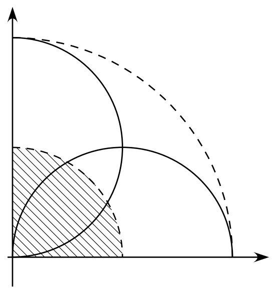


Figure 2

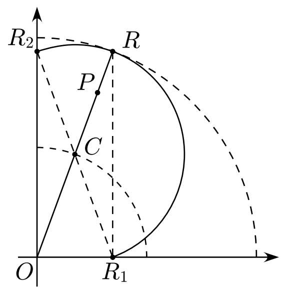


Figure 3

If P is a point of the "ring" bounded by the two arcs and OP intersects the larger arc at R, let R_1 and R_2 denote the projections of R onto the axes. Then OR_1RR_2 is a rectangle with diagonals $RO=R_1R_2=20$ cm. If C is the centre of the rectangle, then $OC=10$ cm, C lies on the smaller arc, and P lies on the segment CR. The point P is thus contained in the right-angled triangle R_1RR_2, which is entirely contained in the semicircle of diameter R_1R_2 passing through R. Thus the point P is wiped by the sponge.

Therefore, the area wiped by the sponge consists of the points of the closed quadrant of radius 20 cm centred at O, and hence the area wiped is

$$\frac{1}{4}\cdot 20^2\pi = 100\pi \text{ cm}^2.$$

B. 3470. *Find the equation of the line that touches the curve $y = 3x^4 - 4x^3$ at two different points.*

Solution 1. *Figure 1* shows the graph of the function $f(x) = 3x^4 - 4x^3$. The dotted line is the line whose equation is needed.

Notice that if $x + \frac{1}{3}$ is substituted[1] for x in the polynomial, which means shifting the graph by $-\frac{1}{3}$ parallel to the axis, then the resulting fourth-degree polynomial $f_1(x) = f\left(x + \frac{1}{3}\right)$ contains no cubic term:

$$f_1(x) = 3\left(x + \frac{1}{3}\right)^4 - 4\left(x + \frac{1}{3}\right)^3 = 3x^4 - 2x^2 - \frac{8}{9}x - \frac{1}{9}.$$

By forming a perfect square out of the terms of even degree in f_1, we get

$$f_1(x) = 3\left(x^2 - \frac{1}{3}\right)^2 - \frac{8}{9}x - \frac{4}{9}.$$

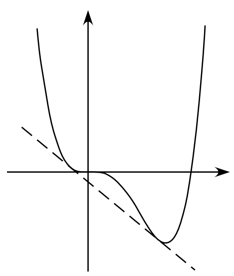


Figure 1

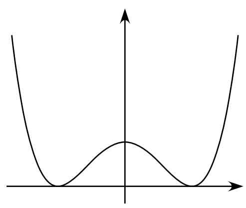


Figure 2

The line that touches the graph of $y = 3\left(x^2 - \frac{1}{3}\right)^2$ (*Figure 2*) is obviously the x-axis, and thus $y = -\frac{8}{9}x - \frac{4}{9}$ is a double tangent to the graph of $f_1(x)$. Hence the solution is obtained by applying the inverse substitution. If $x - \frac{1}{3}$ is substituted for x, the equation of the line will be

$$y = -\frac{8}{9}\left(x - \frac{1}{3}\right) - \frac{4}{9} = -\frac{8}{9}x - \frac{4}{27}.$$

Solution 2. The line $y = ax + b$ touches the graph of the function $y = 3x^4 - 4x^3$ at most two points if and only if the graph of the polynomial

[1]This substitution, called the Tschirnhaus substitution, is also used as the first step of solving a general fourth-degree equation. It eliminates the cubic term.

$p(x)=3x^4-4x^3-ax-b$ touches the x-axis at two points, that is, it has two multiple roots. The degree of the curve is four, thus the multiplicity of each multiple root is two, and there are no other roots. If the roots are x_1 and x_2, $p(x)$ can be factorised as follows:

$$p(x)=3(x-x_1)^2(x-x_2)^2. \tag{$*$}$$

By carrying out the operations on the right-hand side, we have

$$3x^4-4x^3-ax-b=$$
$$=3x^4-6(x_1+x_2)x^3+3(x_1^2+4x_1x_2+x_2^2)x^2-6x_1x_2(x_1+x_2)x+3x_1^2x_2^2.$$

As the corresponding coefficients must be equal,

$$x_1+x_2=\frac{2}{3}, \tag{1}$$

$$x_1^2+4x_1x_2+x_2^2=0, \tag{2}$$

$$6x_1x_2(x_1+x_2)=a, \tag{3}$$

$$-3x_1^2x_2^2=b. \tag{4}$$

By rearranging (2), we get $(x_1+x_2)^2=-2x_1x_2$, and with (1), $x_1x_2=-\frac{2}{9}$. Then it follows from (3) that $a=-\frac{8}{9}$, and from (4) that $b=-\frac{4}{27}$.

Hence the equation of the line can only be $y=-\frac{8}{9}x-\frac{4}{27}$. This line is really a solution, as the roots of the simultaneous equations (1) and (2) are real numbers $\left(x_1=\frac{1}{3}-\frac{\sqrt{3}}{3}\text{ and }x_2=\frac{1}{3}+\frac{\sqrt{3}}{3}\right)$, and thus all the above steps can be retraced and the factors of the product $(*)$ will be polynomials of real coefficients.

B. A. Rácz, Budapest

Solution 3. If a is an arbitrary real number, the equation of the line touching the curve at the point $\big(a,f(a)\big)$ is $y=f'(a)(x-a)+f(a)$. If $b\neq a$ then this is identical to the tangent at $\big(b,f(b)\big)$ if and only if

$$f'(a)=f'(b) \tag{1}$$

$$f(a)-a\cdot f'(a)=f(b)-b\cdot f'(b). \tag{2}$$

From (1), division by $a-b\neq 0$ yields

$$a^2+ab+b^2-a-b=0, \tag{3}$$

and from (2), in the same way,

$$9(a+b)(a^2+b^2)-8(a^2+ab+b^2)=0. \tag{4}$$

As it follows from (3) that $a^2 + ab + b^2 = a + b$, by substitution into (4) we get

$$a^2 + b^2 = \frac{8}{9}. \tag{5}$$

Substituting this into (3),

$$a + b - ab = \frac{8}{9}. \tag{6}$$

As the simultaneous equations (5), (6) lead to a fourth-degree equation, let us introduce the new unknowns $u = a + b$ and $v = ab$. Thus the simultaneous equations are

$$u^2 - 2v = \frac{8}{9}, \qquad u - v = \frac{8}{9}.$$

Substituting $v = u - \frac{8}{9}$, we get $u^2 - 2u + \frac{8}{9} = 0$. The roots of this equation are $u_1 = \frac{2}{3}$ and $u_2 = \frac{4}{3}$. The corresponding values of v are $v_1 = -\frac{2}{9}$ and $v_2 = \frac{4}{9}$.

Now the values of a and b are the solutions of the equations $t^2 - u_1 t + v_1 = 0$ and $t^2 - u_2 t + v_2 = 0$. In the first case, $a = \frac{1}{3} - \frac{\sqrt{3}}{3}$ and $b = \frac{1}{3} + \frac{\sqrt{3}}{3}$, while in the second case the two roots are equal, $a = b = \frac{2}{3}$. As $a \neq b$, by definition, the second case does not represent a solution.

If $a = \frac{1}{3} - \frac{\sqrt{3}}{3}$ then $f'(a) = -\frac{8}{9}$ and $f(a) - a \cdot f'(a) = -\frac{4}{27}$ thus the equation of the tangent at $\big(a, f(a)\big)$ is

$$y = -\frac{8}{9}x - \frac{4}{27}.$$

As all the steps are reversible, the same equation is obtained for the tangent at $\big(b, f(b)\big)$.

Remarks. 1. $a = b = \frac{2}{3}$ is one of the points of inflection of the curve $y = 4x^3 - 3x^2$. Strictly speaking, the second case also represents a double tangent but the points of tangency also coincide.

2. The condition (3) $\left(\dfrac{f'(a) - f'(b)}{a - b} = 0\right)$ obtained in Solution 3 yields an ellipse if a and b are represented on the coordinate axes (*Figure 3*). This ellipse consists of the points $P(a, b)$ for which the tangents drawn to the curve $y = 4x^3 - 3x^2$ at $\big(a, f(a)\big)$ and $\big(b, f(b)\big)$ are parallel. The axes of the ellipse are parallel to the angle bisectors of the coordinate axes, and its centre is the point $C\left(\frac{1}{3}, \frac{1}{3}\right)$.

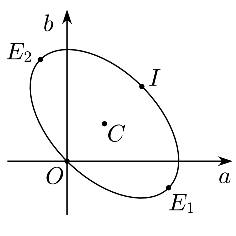


Figure 3

The endpoints of the minor axis are O and $I\left(\frac{2}{3}, \frac{2}{3}\right)$, and $E_1\left(\frac{1}{3} + \frac{1}{\sqrt{3}}, \frac{1}{3} - \frac{1}{\sqrt{3}}\right)$, $E_2\left(\frac{1}{3} - \frac{1}{\sqrt{3}}, \frac{1}{3} + \frac{1}{\sqrt{3}}\right)$ represent the points of tangency on the double tangent. This relationship becomes clear if one considers the "symmetry" of the fourth-degree curve about the point $x=\frac{1}{3}$. This is the abscissa of the centre of symmetry in the graph of the third-degree derivative function representing the slopes of the tangents. If the equation of the double tangent is subtracted from the fourth degree polynomial then the resulting fourth-degree curve will indeed be symmetrical about the line $x=\frac{1}{3}$. (This is a reason for the substitution in Solution 1.) Thus the abscissas of the points of tangency on the double tangent are symmetric about the point $x=\frac{1}{3}$. The corresponding point of *Figure 3* lies on the line $a+b=\frac{2}{3}$, the major axis of the ellipse.

It is easy to check that all fourth-degree curves with a double tangent have this property, that is, more precisely, $\frac{f'(a)-f'(b)}{a-b}=0$ will represent a real ellipse in exactly that case. All the ellipses obtained in this way are similar, their eccentricity is $\frac{\sqrt{3}}{3}$, and they are all obtained as shown in *Figure 3.* The endpoints of their minor axes represent the points of inflection of the corresponding fourth-degree curves, and the endpoints of their major axes represent the points of tangency on the double tangent.

B. 3471. *An ant is walking about in the region bounded by the curve of equation $x^2+y^2+xy=6$. Its path consists of segments parallel to the coordinate axes. Starting at an arbitrary point of the curve it walks straight ahead inside the curve until it hits the boundary again. Then it makes a 90° turn and goes on walking inside the curve. It only stops if it either arrives at a point of the boundary where it has been before, or if it cannot continue its walk by the above rules. Prove that wherever the starting point is, the walk of the ant will always terminate.*

Gillis–Turán Mathematics Competition, 2000

Solution 1. If the ant is at a point $P(a,b)$ of the curve, then the equations $x^2+bx+b^2-6=0$ and $y^2+ay+a^2-6=0$ have real roots: a and b, respectively. Thus the discriminants $D_b=24-3b^2$ and $D_a=24-3a^2$ are non-negative. If either of them is zero, for example $D_a=0$, that is $|a|=2\sqrt{2}$ (hence $b=-\frac{a}{2}$) then the ant cannot continue its walk parallel to the y-axis. This happens at the points $Y_1\big(2\sqrt{2},-\sqrt{2}\,\big)$ and $Y_2\big(-2\sqrt{2},\sqrt{2}\,\big)$. Similarly, when $D_b=0$, that is, the ant is at the points $X_1\big(\sqrt{2},-\sqrt{2}\,\big)$ or $X_2\big(-\sqrt{2},2\sqrt{2}\,\big)$, it cannot continue its walk parallel to the x-axis.

This is all clearly seen if one considers that the curve $x^2+y^2+xy=6$ is an ellipse (*Figure 1*), and the points X_i, Y_i are the points where the tangents parallel to the coordinate axes touch the curve.

If the ant is at a point $P(a,b)$ different from these four points then it can walk in either allowed direction. If P is not the starting point, then it can obviously walk in one direction only, as it must have come from the other direction.

For example, if the ant is walking parallel to the x-axis, and it arrives at a point $Q(c,b)$ of the curve then with the above reasoning $c\neq a$, and the two numbers a and c are the two real roots of the equation $x^2+bx+b^2-6=0$. Thus $a+c=-b$.

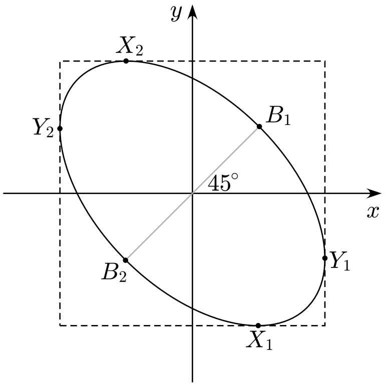


Figure 1

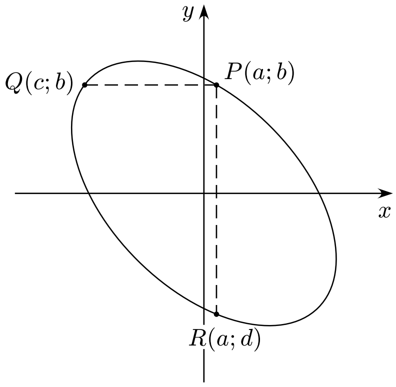


Figure 2

Similarly, if the ant is walking parallel to the y-axis and arrives at a point $R(a,d)$ from P then $d+b=-a$ (*Figure 2*).

It follows that the endpoints of any segment of the ant's walk are such points of the curve that two out of the 4 coordinates altogether are equal, and the sum of this coordinate and the remaining two is 0: $a+b+c=0$ and $a+b+d=0$.

For example, if the ant starts out at $P_0(a,b)$ parallel to the x-axis, its path will pass through the following points of the curve:

$$P_0(a,b) \to P_1(-a-b,b) \to P_2(-a-b,a) \to P_3(b,a) \to$$
$$\to P_4(b,-a-b) \to P_5(a,-a-b) \to P_6(a;b),$$

Thus if the ant never arrives at any of the points X_i, Y_i then its walk terminates at the end of exactly the sixth segment. If it does arrive at one of those points, then its walk may terminate even sooner.

A. Babos, Budapest

Remarks. 1. It is easy to see that the ant can only arrive at the point X_i if it is walking parallel to the y-axis: to X_1 from $B_1\left(\sqrt{2},\sqrt{2}\right)$ and to X_2 from $B_2\left(-\sqrt{2},-\sqrt{2}\right)$. These are the same points, with their coordinates equal, from where the ant can reach Y_1 and Y_2.

To summarize the results, we can state that if the starting position of the ant is different from the points X_i, Y_i, B_i then its walk will terminate in six steps, if it starts from B_i then it will terminate in one step, and if it starts from X_i or Y_i then two steps. All principally correct solutions used more or less the same reasoning, but it eluded almost everyone to examine the special cases.

2. With the notation $c=-a-b$, the path of the ant (with the exception of the special cases) touches the boundary at the points (a,b), (c,b), (c,a), (b,a), (b,c), (a,c), (a,b). The coordinates of the points are all a, b or c where $a+b+c=0$ (*Figure 3*). The path, just like the curve itself, is symmetrical in the line $y=x$.

The number triples of this kind are in an interesting relationship to a possible approach of problem B. 3470. (See the Remark to Problem B. 3470 on page 51.) If

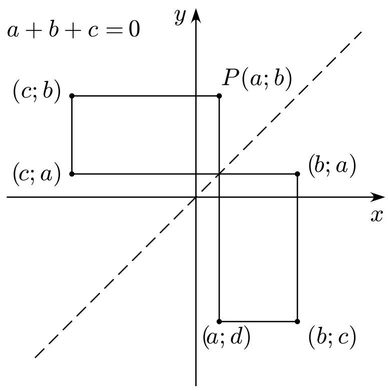


Figure 3

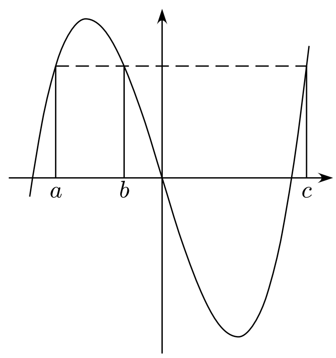


Figure 4

the original polynomial is the third-degree polynomial $f(x) = x^3 - 6x$ (*Figure 4*) then the equation of the ellipse of this problem is $\dfrac{f(x)-f(y)}{x-y} = 0$, and the coordinates of the points of the ellipse are number pairs (a, b) for which $f(a) = f(b)$.

Each value of f other than the local extrema is assumed at three points, and the path of the ant corresponds to a number triple of this kind. With this interpretation, the statement of the problem is obvious.

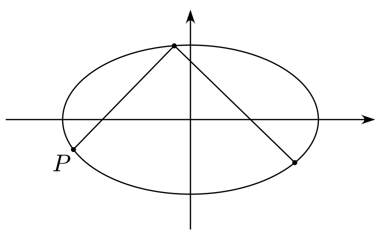


Figure 5

Solution 2. Let us rotate the curve, as well as the path of the ant, through $-45°$. Then the equation of the curve will be

$$\frac{x^2}{12} + \frac{y^2}{4} = 1$$

(*Figure 5*).

The rotated path consist of segments enclosing $45°$ with the coordinate axes. The eccentricity of the ellipse is $\dfrac{b}{a} = \dfrac{1}{\sqrt{3}}$, therefore an orthogonal axial affinity with a scale factor of $\sqrt{3}$ applied to the ellipse and the ant's path will map the ellipse onto a circle centred at the origin, and the path of the ant onto a polygon of segments enclosing $+60°$ and $-60°$ with the x-axis alternately (*Figure 6*).

Thus the position of the ant on the curve after two steps can be obtained by rotating the starting point through $120°$ about the origin. The direction of the rotation depends on the direction of the ant's walk, and since the direction stays the same all through the ant's journey, the ant will necessarily return to its starting position in six consecutive steps, and that terminates its walk.

This is true for almost all starting points, with the exception of six points. Four of these are the points where the tangents enclose angles of $60°$ or $-60°$ with the x-axis. If the ant arrives at these points, it must stop. The other two are the

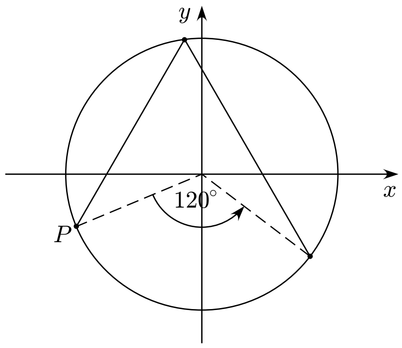


Figure 6

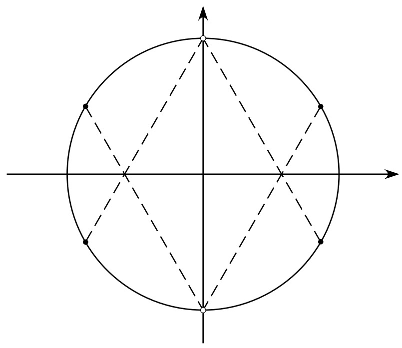
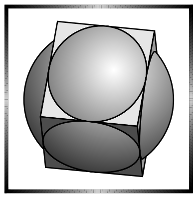


Figure 7

endpoints of the vertical diameter, the points from where the ant can reach those points of tangency (*Figure 7*).

Solutions of advanced problems A



A. 269. *A circular hole is to be completely covered with two square boards. The sides of the squares are* 1 *metre. In what interval may the diameter of the hole vary?*

It is easy to see that a hole of radius $2-\sqrt{2}$ (and all smaller holes) can be covered by two unit squares, see *Figure 1.*

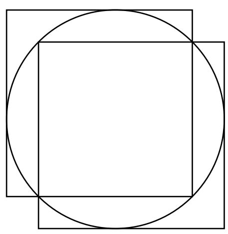


Figure 1

We will prove that if a unit square covers at least half of the perimeter of a circle of radius r, then $r \leqslant 2-\sqrt{2}$. This implies that the diameter of the hole cannot exceed

$$4-2\sqrt{2} \approx 1.17 \text{ metre.}$$

Let K be a circle of radius r, and N be a unit square, which covers at least the half of K. If $r \geqslant 1/2$, then N can be translated such that each side of N or its extension has at least one common point with K and the covered part of the curve is increasing, see *Figure 2.*

So, it can be assumed that $r > 1/2$ and (the extension of) each side of N has a common point with K.

First, assume that a vertex of N is inside K. Let the vertices of N be A, B, C, D and suppose that A is inside K. Denote the intersection of K and the half-lines AB and AD by P and Q, respectively. (*Figure 3.*)

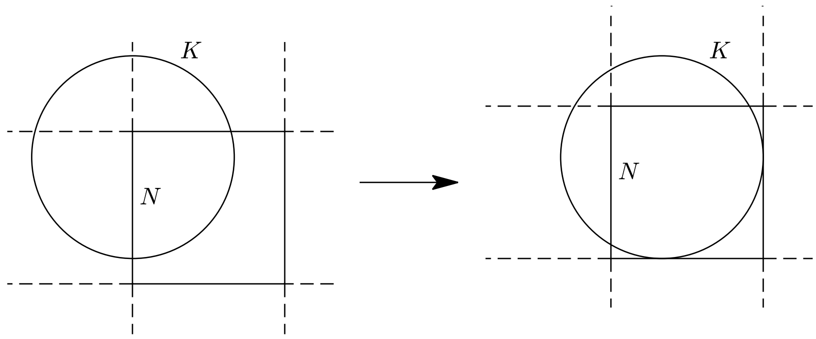


Figure 2

Because $PAQ\sphericalangle = 90^\circ$, the centre of K and vertex A are on the same side of line PQ. This implies that the uncovered arc PQ is longer than the half of K. This is a contradiction, thus this case is impossible.

We are left to deal with the case when there are no vertices of N inside K and each side or its extension has a common point with K. It is easy to check that these common points cannot be on the extension of the sides of N; they must lie on the perimeter of N.

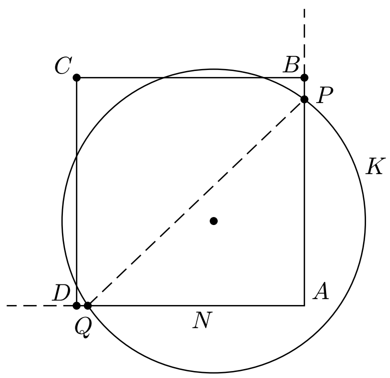


Figure 3

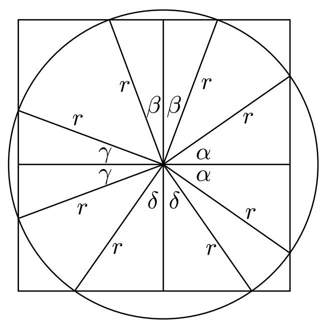


Figure 4

Denote by α, β, γ and δ the angles drawn on *Figure 4*.

The total of the uncovered arcs is at most the half of K, so $\alpha+\beta+\gamma+\delta \leqslant 90^\circ$. By symmetry, it can be assumed that $\alpha + \gamma \leqslant 45^\circ$.

As can be read from the Figure, $r(\cos\alpha + \cos\gamma) = r(\cos\beta + \cos\delta) = 1$. The concavity of the cosine function yields

$$1 = r(\cos\alpha + \cos\gamma) \geqslant r\big(1 + \cos(\alpha+\gamma)\big) \geqslant r(1 + \cos 45^\circ) = r\left(1 + \frac{\sqrt{2}}{2}\right),$$

and hence $r \leqslant \dfrac{1}{1+\sqrt{2}/2} = 2 - \sqrt{2}$.

Thus, the radius of the hole can be at most $2-\sqrt{2}$; its diameter can be at most $4-2\sqrt{2}\approx 1.17$ metre.

A. 274. *Let a, b, c be positive integers for which $ac=b^2+b+1$. Prove that the equation*

$$ax^2-(2b+1)xy+cy^2=1$$

has an integer solution.

Polish competition problem

Solution 1. The proof is by induction on b. If $b=0$, then $a=c=1$, and $x=y=1$ is a solution.

Now suppose that b is positive, and the statement is true for all smaller values of b. The numbers a and c cannot be both greater than b, since if $a,c\geqslant b+1$, then $ac\geqslant(b+1)^2>b^2+b+1$. As the statement remains the same interchanging a and c, we can assume, without loss of generality, that $a\leqslant b$.

Let $A=a$, $B=b-a$, $C=a-2b+c-1$. These are integers, satsifying

$$\begin{aligned}B^2+B+1&=(b-a)^2+(b-a)+1=\\&=(b^2+b+1)-2ab+a^2-a=\\&=ac-2ab+a^2-a=a(a-2b+c-1)=AC,\end{aligned}$$

and furthermore, $A>0$, $0\leqslant B<b$, and $C=(B^2+B+1)/A>0$. Hence the induction hypothesis applied to the numbers A, B, C, yields integers X and Y, such that

$$AX^2-(2B+1)XY+CY^2=1.$$

By substituting the definitions of A, B and C, we get

$$\begin{aligned}1&=AX^2-(2B+1)XY+CY^2=\\&=aX^2-(2b-2a+1)XY+(a-2b+c-1)Y^2=\\&=a(X+Y)^2-(2b+1)(X+Y)Y+cY^2.\end{aligned}$$

Therefore, the number pair $x=X-Y$, $y=Y$ is a solution of the equation.

Solution 2. Consider the set of points in the Cartesian system for which $ax^2-(2b+1)xy+cy^2<2$. Simple calculation shows that they form an ellipse whose area is $\dfrac{4\pi}{\sqrt{3}}$ units.

The elliptical disc is symmetric about the origin, it is convex, and its area is greater than 4 units. Thus, according to Minkowski's theorem there is a lattice point other than the origin in its interior. At that point, the value of $ax^2-(2b+1)xy+cy^2$ is between 0 and 2, therefore it is 1.

Remark. In Solution 1, we are actually using the area preserving transformation $(x,y)\mapsto(x-y,y)$ to map the elliptical disc onto another ellipse of equal area with smaller coefficients. By repeating the transformation several times, we will always obtain the ellipse $x^2 - xy + y^2 < 2$. This ellipse contains six lattice points different from the origin, they are $(\pm 1, 0)$, $(0, \pm 1)$ and $(\pm 1, \pm 1)$. Therefore, the equation always has six solutions.

A. 284. *Let f be a function defined on the subsets of a finite set S. Prove that if $f(S \setminus A) = f(A)$ and $\max\big(f(A), f(B)\big) \geqslant f(A \cup B)$ for all subsets A, B of S, then f assumes at most $|S|$ distinct values.*

(Miklós Schweitzer Memorial Competition, 2001)

Solution 1. If $S = \emptyset$, the statement is not true. Assume from now on that S is not empty.

The proof is by induction. For $|S| = 1$ and $|S| = 2$ the number of complementary pairs of subsets is exactly 1 and 2, respectively, thus the function can have no other values. Now let $|S| > 2$, and assume that the statement is true for smaller numbers of elements.

Let the m be the largest value of f. First we prove that S has a one-element subset $X = \{x\}$, such that $f(X) = m$. Consider the subsets assigned the number m by the function f. It follows from the complementary property that there is a nonempty set among these subsets. Thus consider the smallest nonempty subset X, such that $f(X) = m$. If X had at least two elements, it could be expressed as the union of two smaller sets: $X = X_1 \cup X_2$, but then, as

$$\max\big(f(X_1), f(X_2)\big) \geqslant f(X_1 \cup X_2) = f(X) = m,$$

one of $f(X_1)$ and $f(X_2)$ would also be m. Therefore, the set X has one element.

Let $R = S \setminus X$, and define the function $g : P(R) \to R$ as follows: for all $A \subset R$, let

$$g(A) = \min\big(f(A), f(A \cup X)\big) = \min\big(f(A), f(R \setminus A)\big).$$

Note that for any $A \subset R$, $\max\big(f(A), f(A \cup X)\big) = m$, as

$$m = f(X) = f(S \setminus X) = f\big(A \cup (R \setminus A)\big) \leqslant \max\big(f(A), f(R \setminus A)\big) =$$

$$= \max\big(f(A), f\big(S \setminus (R \setminus A)\big)\big) = \max\big(f(A), f(A \cup X)\big).$$

There remains to prove that the assumption of the induction is true for the function g, that is, $g(R \setminus A) = g(A)$ and $g(A \cup B) \leqslant \max\big(g(A), g(B)\big)$ for all $A, B \subset R$. Then, by the induction hypothesis, g may assume at most $\big(|S| - 1\big)$ different values. For any set $A \subset R$, one of $f(A)$ and $f(A \cup X)$ is m, and the other is $g(A)$. Hence the range of f can only exceed the range of g by the single element m.

The property $g(R \setminus A) = g(A)$ can be deduced from the definition of g.

If either of $g(A)$ or $g(B)$ is m, then $g(A \cup B) \leqslant \max\big(g(A), g(B)\big)$ follows trivially. Assume, therefore, that $g(A)$ and $g(B)$ are both smaller than m, that is, one of $f(A)$ and $f(A \cup X)$, and one of $f(B)$ and $f(B \cup X)$ are smaller than m. If $f(A) < m$, then let $C = A$, otherwise let $C = A \cup X$. Similarly, for $f(B) < m$ let $D = B$, otherwise $D = B \cup X$. Then $f(C) = g(A)$ and $f(D) = g(B)$, and the set $C \cup D$ is either $A \cup B$ or $A \cup B \cup X$. Therefore,

$$\max\big(g(A), g(B)\big) = \max\big(f(C), f(D)\big) \geqslant f(C \cup D) \geqslant$$

$$\geqslant \min\big(f(A \cup B), f(A \cup B \cup X)\big) = g(A \cup B).$$

Thus the function g satisfies the conditions, indeed.

Solution 2 (by *E. Csóka*). The solution is based on the following lemma:

Lemma. *For any real number v, let S_v be the set of those subsets of the set S for which the value assigned by the function f is not greater than v:*

$$S_v = \big\{X \subset S : \ f(X) \leqslant v\big\}.$$

Then $|S_v|$ is either 0, or a power of 2 that is different from 1.

Proof for the lemma. First observe that S_v is closed for complement, union, intersection and difference, that is, for all sets X, Y in S_v, $S \setminus X$, $X \cap Y$, $X \cup Y$ and $X \setminus Y$ are also in S_v. The first two are true because $f(S \setminus X) = f(X) \leqslant v$, and $f(X \cup Y) \leqslant \max\big(f(X), f(Y)\big) \leqslant \max(v, v) = v$; and both intersection and difference can be expressed in terms of complement and union.

It follows from the closeness under union and complement that if S_v is not empty, then $S \in S_v$.

It follows from the closeness under complement that if S_v has at least one element then the complement of that element also belongs to S. Thus the elements of S_v can be matched, and thus S_v cannot be a one-element set.

Let the *atoms* of S_v be its nonempty subsets with the minimum number of elements. Thus a nonempty set $A \in S_v$ is an atom if and only if for all $X \subset A$, $X \in S_v$ it is true that either $X = \emptyset$ or $X = A$.

Two important consequences are immediate: One of them is that if $A \in S_v$ is an atom and $X \in S_v$ is arbitrary, then A is a subset of either X or $(S \setminus X)$. They contrary would imply that $A \setminus X$ is a proper subset of A, which contradicts to A being an atom. The other important consequence is that atoms are pairwise disjoint. If there were two non-disjoint atoms, then they would contain each other for the above reason, that is, the two atoms would be identical.

Now we shall prove that every element of the set S is contained in exactly one atom of S_v. As the atoms are pairwise disjoint, x can belong to at most one atom, and all we need to prove is that such an atom exists. Let $x \in S$ be an arbitrary element. Consider a set in S_v that contains x and has the minimum number of elements, and call it A. If A is not an atom then it is not minimal, that is, it has a subset $X \subset A$ that is not empty but not equal to A either. Then X and $A \setminus X$ are both in S_v, they are proper subsets of A, and one of them contains x. This contradicts to A being minimal among the sets in S_v containing x. Therefore, A is indeed an atom.

It follows that any set in $X \in S_v$ can be uniquely expressed as the union of atoms in S_v. For any element $x \in S$, let A_x be the atom for which $x \in A_x$. The unique representation of the set X is then:

$$X = \bigcup_{x \in X} A_x.$$

For a proof, observe that all atoms are subsets of X and thus the right-hand side is a subset of X, and that the right-hand side contains all elements of X as the set A_x containing x occurs among the terms for each $x \in X$. All there remains to prove is that the above representation is unique. If $x \in X$, then a representation of X must contain the atom A_x as that is the only atom that contains x. On the other hand, if X and a particular atom are disjoint, it cannot occur in the representation of X.

Let the atoms of S_v be $A^1, \ldots, A^k$. By the above reasoning, for each set X in S_v there exists a unique index set $I \subset \{1, 2, \ldots, k\}$, such that $X = \cup_{i \in I} A^i$, and vice versa, for any index set I the set $\cup_{i \in I} A^i$ is in S_v. Thus there is a one-to-one correspondence between the sets in S_v and the subsets of the set $\{1, 2, \ldots, k\}$. The number of such subsets is 2^k, therefore $|S_v| = 2^k$. This completes the proof of the lemma.

Now there remains to prove the statement of the problem. Let the values of the function f be $v_1 < v_2 < \cdots < v_n$. Consider the sets $S_{v_1}, S_{v_2}, \ldots, S_{v_n}$. These sets form a chain getting larger and larger: $S_{v_1} \subset S_{v_2} \subset \cdots \subset S_{v_n}$.

These sets are not empty, and no two of them are identical. It follows from the lemma that $|S_{v_1}| < |S_{v_2}| < \cdots < |S_{v_n}|$ are different powers of 2, greater than 1, and thus $|S_{v_n}| \geqslant 2^n$. On the other hand, S_{v_n} consists of all the subsets of S, thus $|S_{v_n}| = 2^{|S|}$. Hence, $n \leqslant |S|$.

Remark. It is not hard to construct an example where the range of f has exactly $|S|$ elements. Let $S = \{1, 2, \ldots, n\}$, $f(S) = f(\emptyset) = 0$, and for any subset X different from S and the empty set, let $f(X)$ be the largest number in S, such that exactly one of $f(X)$ and $f(X) - 1$ is an element of X. For example, in the case of $n = 6$, let $f(\{1, 2, 5\}) = 5$.

Problem Solving Competition: 2002/2003

The competitions start annually and last from September to May, but you can enter any time during the academic year.

In Mathematics, there are three different contests, in Physics there are two. Additionally, a new contest in Informatics is launched. The conditions of the respective contests are slightly different. See below for details.

Every primary or secondary school student is eligible to participate in the competitions. Students in different grades might find the same problems but in most cases their work is evaluated within their age group, they compete with students of the same age only. Therefore, it is essential that *the paper should indicate the 1 to 12 grade of the contestant* in the current school year. The KöMaL contests are individual competitions, solutions produced by a group are not accepted. If two papers turn out to be practically identical, none of them will be marked.

Mathematics

C *contest:* exercises for practice, easier than those in the **B** contest; 5 each month. Correct solutions worth 5 marks.

Age groups:

- up to 10th grade students
- 11 to 12th grade students (preferably those not studying mathematics in a special advanced class. Those in advanced classes are advised to take part in the **B** contest).

B *contest:* 10 problems each month. You can send any number of solutions, but only the highest six scores are entered.

Age groups:

- up to the 8th grade
- 9th grade
- 10th grade
- 11th grade
- 12th grade

A *contest:* advanced problems, 3 each month. More demainding than the **B** contest, for those who are preparing for national or international competitions. Here there are no separate age groups.

Physics

M *contest:* Experimental problems: One measuring task is set each month. Each of them is worth 6 points. The report must contain a description of the method, the data obtained sufficient in quantity and quality, the analysis of the data, and the estimation of the error. There are no separate age groups.

P *contest:* 10 theoretical problems each month.

Age groups:

- up to the 8th grade;
- 9th grade;
- 10th grade;
- 11th grade;
- 12th grade.

Every age group may send solutions to all kinds of problems. In the **P** contest we evaluate only 3 problems up to the 8th grade and 5 problems from 9th–12th grade.

Informatics

Three programming problems are set each month. The solutions should be written as working programs in any high level programming language, preferably Pascal or C. Do not send .exe files! There are no separate age groups, competition is opened for everyone.

Deadlines, adresses

The deadline of mailing or e-mailing the solutions is indicated in every issue next to the new exercises and problems. Deadlines: in Physics: 11th of the month following the publication of the current issue; in Informatics: 13th of the month following the publication of the current issue; in Mathematics: 15th of the month following the publication of the current issue. Should that be a weekend or bank holiday, the deadline is the next workday.

Send your solutions to the following address:
KöMaL Szerkesztőség (KöMaL feladatok), Budapest Pf. 47. 1255, Hungary or by e-mail to: `solutions@komal.hu`.

Informatics solutions are accepted via e-mail only and should be sent to the following address: `infotech@komal.hu`.

The actual state of the contests appears on our web-site
(`http://www.komal.hu/eredm/index.e.shtml`)
and it is updated regularly. These data are not official, only for your information. The final results will appear in August on our Internet home page and in the September issue of the following academic year. The cca 10 top contestans are rewarded by a certificate in each category and this is going to be mailed to their schools, and their portraits, additionally, will be presented in the December issue and the Internet.

Entry Form for the contests
The layout of the papers:

By ordinary mail:

- Write the solutions to different problems on separate A4 sheets of paper. (This is important because different people are responsible for the marking.)
- The header of every sheet must contain the following in the upper left corner (see sample 1):
  — the letter code (A, B, C, M, P) and number of the problem in red
  — the full name and the grade of the sender
  — the name of the school and the town (and country)
  — the e-mail adress of the sender
- Fold each sheet into four separatly so that the header should appear in the front side.
- Solutions to geometry problems should include diagrams.

- Enclose with your solutions a separate sheet listing your data and the contents of your mail. See sample 2.

Sample 1. Header of a sheet

C. 593.

Varga 163 Róbert, 9th grade

Révai High School, Győr

e-mail: robi@revai.hu

Denote the age of the captain by C, the age of the ship by S. When the age of the ship was C, the age of the captain was C-$(S-C)$=$2C-S$. When the ship was $2C-S$ ...

Sample 2. Enclosed list

Varga 163 Róbert, 9th grade
Révai High School, Győr
I send the following 3 papers in:
C. 591., C. 593., B. 3389.

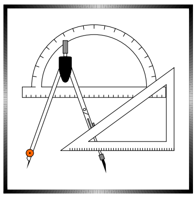
By e-mail:

- Send the solutions of different problems as separate e-mail messages.
- The "subject" field of the e-mail message should contain the letter code and number of the problem.
- Additional requirements concerning the Informatics solutions
  - The solutions should be mailed separately to the following address: `infotech@komal.hu`.
  - In the first few comment lines of each program do enter the following information:
    — your name and class
    — your school.
    — your town (country)

The content of the papers

It is not enough to state the answer. Results with detailed explanations only will receive full credit. (Reference to standard school math is accepted without proof.)

New exercises for practice – competition C (690–694.)



C. 690. Is it possible for the sum of the volumes of three cubes of integer edges to be 2002 units?

C. 691. Express in mm^2 the area of Hungary on a globe of radius 25 cm.

C. 692. For the real numbers x, y, z,

$$x + 2y + 4z \geqslant 3 \qquad \text{and} \tag{1}$$

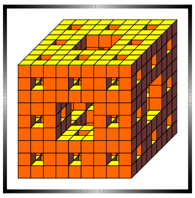
$$y - 3x + 2z \geqslant 5. \tag{2}$$

Prove that $y - x + 2z \geqslant 3$.

C. 693. In what interval may the apex angle of an isosceles triangle vary if a triangle can be constructed out of its altitudes?

C. 694. Evaluate the sum $[\log_2 1] + [\log_2 2] + [\log_2 3] + \cdots + [\log_2 2002]$.

Suggested by *Ádám Besenyei,* Budapest



New problems – competition B (3582–3591.)

B. 3582. Solve the equation $3xyz - 5yz + 3x + 3z = 5$ on the set of natural numbers.

(*3 points*)

B. 3583. The incentre of a triangle ABC is connected to the vertices. One of the resulting three triangles is similar to the original triangle ABC. Find the angles of the triangle ABC.

(*3 points*)

B. 3584. Write down all the integers from 1 to 10^{n-1}, and let A denote the number of digits hence written down. Now write down all the integers from 1 to 10^n, and let B denote the number of zeros written down this time. Prove that $A = B$.

(*4 points*)

B. 3585. Find the possible values of the parameter a, such that the inequality $\sqrt{1+x^4} > 1 - 2ax + x^2$ holds for all positive x.

(*3 points*) 11th International Hungarian Mathematics Competition

B. 3586. For what values of the parameter a does the equation

$$\log(ax) = 2\log(x+1)$$

have exactly one root?

(*4 points*)

B. 3587. A truncated right pyramid with a square base is circumscribed about a sphere. Find the range for the ratio of the volume and the surface area of the solid.

(*4 points*)

B. 3588. M is a point in the interior of a given circle. The vertex of a right angle is M and its arms intersect the circle at the points A and B. What is the locus of the midpoint of the line segment AB as the right angle is rotated about the point M?

(*4 points*)

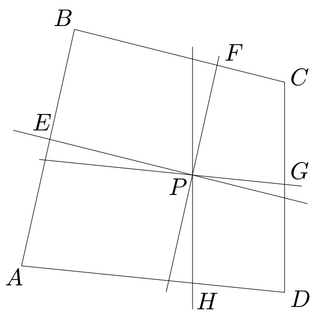
B. 3589. Prove that there are infinitely many odd positive integers n, such that $2^n + n$ is a composite number.

(*4 points*)

B. 3590. The roots of the equation $x^3 - 10x + 11 = 0$ are u, v and w. Determine the value of

$$\arctan u + \arctan v + \arctan w.$$

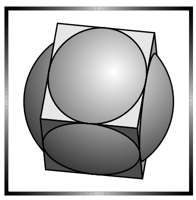
(*5 points*)



B. 3591. The area of the convex quadrilateral $ABCD$ is T, and P is a point in its interior. The parallel through the point P to the line segment BC intersects the side BA at E, the parallel to the line segment AB intersects the side BC at$F$, the parallel to AD intersects CD at G, and the parallel to CD intersects AD at the point H. Let t_1 denote the area of the quadrilateral $AEPH$, and let t_2 denote the area of the quadrilateral $PFCG$. Prove that $\sqrt{t_1} + \sqrt{t_2} \leqslant \sqrt{T}$.

(*5 points*)

New advanced problems – competition A (302–304.)



A. 302. Given the unit square $ABCD$ and the point P on the plane, prove that

$$3AP + 5CP + \sqrt{5}(BP + DP) \geqslant 6\sqrt{2}.$$

A. 303. x, y are non-negative numbers, and $x^3 + y^4 \leqslant x^2 + y^3$. Prove that

$$x^3 + y^3 \leqslant 2.$$

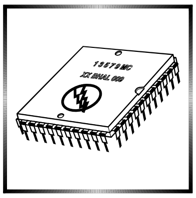
A. 304. Find all functions $R^+ \mapsto R^+$, such that

$$f(x+y) + f(x) \cdot f(y) = f(xy) + f(x) + f(y)?$$

❄

New problems: `http://www.komal.hu/verseny/2002-10/mat.e.shtml`

❄



Solution of the problems for information technology November 2001

I. 7. *The function* Factorial(N) *increases very rapidly. While* $5! = 120$, 4*-byte integers are needed for storing* $10! = 3628800$. *A computer can store* $100!$ *neither as a* 4*-byte nor as an* 8*-byte integer. We know however, that every natural number has its prime factorization. For example* $5! = 2^3 \cdot 3 \cdot 5$, *or* $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$. *Your program should read the number* N $(1 \leqslant N \leqslant 10000)$ *from the keyboard, then print the prime factorization of its factorial* N!

(*10 points*)

We solve the problem by giving two algorithms producing the same results.

First solution. Read the number. If it is 1, then the factorization is done, otherwise we begin the calculation. The first prime is 2 with exponent 1 in the beginning. Then we compute the prime factorizations of the numbers from 3 to N. The exponents from the prime factorization of the new element should be added to the exponents we already have.

Every new prime number is added to the list. (This happens if the new number is a prime number, hence the number of primes in a step can increase only by 1.)

Finally, we print all the elements in the factorization of the factorial.

We use the function `PRIME` to decide whether the number is prime or not. We look for divisors from 2 to the square root of the number. Because if it divides, then it is not prime, otherwise it is (its root is dropped). The first prime with exponent 1 in the beginning is 2. We go on until the prime is less than or equal to the number.

If j divides i, then the exponent is increased, otherwise, we look for the next (not greater) prime divisor.

If a prime is detected, then we have one more prime which will be j with exponent 0. (It will be 1 in the beginning of the next loop when increased.)

The last 0 exponent does not count.

Second solution. We use the Legendre's formula in the following form. If p is an arbitrary prime and N is a positive integer, then the exponent of p in the prime factorization of $N!$ is given by ...

Of course, this is only a finite sum, since the integer parts are zero if $N < p^i$.

The number is read. If the number is 1, then the factorization is done. The smallest prime is 2. If 2 is not greater than N, then 2 and its exponent is printed.

The next prime is 3. While the prime is not greater than the number, the prime number and its exponent is printed. Then we look for the next prime.

Computing the exponent of a prime using Legendre's formula. The exponent contains the computed sum which is 0 in the beginning.

`pp` contains the powers of p, which is p in the beginning. We go on until every power of p is less than or equal to N. The exponent is increased, and the next power is computed.

Determining the next prime after p. We use the function `PRIME` to decide whether the number is prime number. We look for divisors from 2 to the square root of the number. If it divides, then it is not prime, otherwise it is (its root is dropped).

2 steps forward can safely be done, since the only even prime is 2. This makes our program faster and more effective. Separating 2 and the subsequent primes served this purpose also. We increase the number by 2 while it is not a prime.

The Pascal programs are finding on

`http://www.komal.hu/verseny/2001-11/l.e.shtml`.

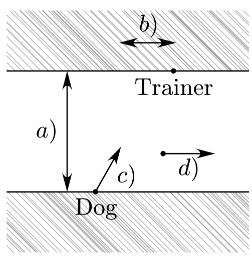
I. 8. *A dog swims across the river, always heading for its trainer standing on the opposite riverside. The approximate path of the dog in the river is to be modelled and displayed on the screen. One should be able to input the following real parameters from the keyboard:*

a) the width of the river in meters

b) the distance (in meters) of the trainer from the starting position of the dog projected onto the opposite riverside. (The distance is positive if it is in the same direction as the streamline of the river and negative otherwise.)

c) the constant velocity of the dog (in $\frac{\mathrm{m}}{\mathrm{s}}$*).*

d) the constant velocity of the river (in $\frac{\mathrm{m}}{\mathrm{s}}$*).*



e) the accuracy of approximation, that is the length of the time interval (in seconds) in which your program can replace the actual motion by a straight line segment.

The two riversides are considered as parallel lines. Simulation should stop when the dog has approached the opposite riverside within 1 *meter.*

The dog's motion depends on its direction, its velocity and the river velocity. Remember that these are constant velocities. However, the direction of the motion and the x- and y-components of the dog's velocity (depending on its direction) can be considered constant only in a time interval. The dog's direction can be computed by the following formula:

Draw the two sides of the river as parallel lines, the starting position of the dog and the trainer, and the path of the dog derived from the above formulation.

(*10 points*)

Solution. Displaying this simulation uses a simple conversion between the real system of coordinates and the axes on the computer screen. On pixel corresponds to 1 meter, and values along the x-axis increase rightwards, while values along the y-axis increase — counter to the usual case — downwards. Explanation of the code.

The variables according to the original problem read as follows. The riversides are drawn. One did not need to draw the velocity vector, so it is drawn now in blue, then red colour is set back.

The new x- (and the y-components also) can be computed by considering a straight and uniform motion and the formula given in the Problem.

We draw a straight line to the new coordinates. The time elapses in the small interval.

The result is displayed.

The Pascal program implements our algorithm is finding on

`http://www.komal.hu/verseny/2001-11/l.e.shtml`.

I. 9. *Binomial coefficients can be arranged in the usual Pascal's triangle as in the figure. Except for the outermost entries in each row, every number is the sum of its upper and upper-left neighbours.*

1					$N=6$	
1	1					
1	2	1				
1	3	3	1			
1	4	6	4	1		
1	5	10	10	5	1	
1	6	15	20	15	6	1

Prepare your Excel sheet capable of displaying the first $N+1$ rows of Pascal's triangle in this arrangement. Let the value of N $(1 \leqslant N \leqslant 20)$ be entered in the 7^{th} cell of the first row. The sheet should contain exactly $N+1$ rows in every case.

(*10 points*)

Solution. The solution is simple taking into account the well-known properties of the Pascal's triangle: any element is the sum of its upper neighbours. But our table is on a tilt now, so its upper and upper-left neighbours are to be summed.

The solution itself reads:

In column

A:=IF(ROW()<=$H$1+1;1;""),

there is everywhere either 1's or nothing, corresponding to the $N+1$ rows to be displayed, that is depending on the number of the row.

The other cells will contain

=IF(ROW()<=$H$1+1;C5+D5;""),

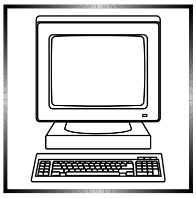
since only those rows are to be printed here in which the number of the row is at most $N+1$ (the value of N is at `$H$1`). In our example, according to the formula in cell `D6`, the values of cell `D5` and `C5` should be added.

Filling of the table is also simple, because Excel automatically increases the row and column identifiers of the cells upon filling. One has to take care not to put anything into cells from the sixth one in the second row, otherwise the whole triangle will be incorrect: we can not carry out addition using only one character.

You can download the solution from here:

`http://www.komal.hu/verseny/2001-11/l.e.shtml`.

Problems in information technology (34–36.)



I. 34. Binomial coefficients can be used to represent natural numbers in the so-called *binomial base.* For a fixed m ($2 \leqslant m \leqslant 50$) every natural number n ($0 \leqslant n \leqslant 10000$) can uniquely be represented as

$$n = \binom{a_1}{1} + \binom{a_2}{2} + \dots + \binom{a_m}{m}, \quad \text{where} \quad 0 \leqslant a_1 < a_2 < \ldots < a_m.$$

Your program (I34.pas, ...) should read the numbers n and m, then display the corresponding sequence $a_1, a_2, \ldots, a_m$.

Example. Let $n = 41$, then $a_1 = 1$, $a_2 = 2$, $a_3 = 4$, $a_4 = 7$, because

$$41 = \binom{1}{1} + \binom{2}{2} + \binom{4}{3} + \binom{7}{4} = 1 + 1 + 4 + 35.$$

(*10 points*)

I. 35. We put an ant close beside the base of a cylinder-jacket with radius R and height H. In every minute the ant creeps upwards M centimetres. The cylinder

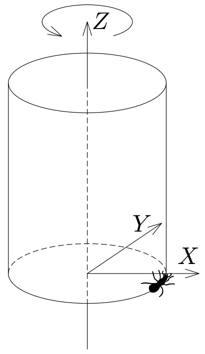


Figure 1

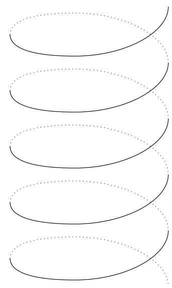


Figure 2

is rotated around its axis (which is just the Z-axis) anticlockwise completing T turns per minute. The ant starts from the point $(R, 0, 0)$, and we are watching it at an angle of $ALPHA$ degree relative to the Y-axis, see *Figure 1.*

Write your program (I35.pas, ...) which reads the values of R ($1 \leqslant R \leqslant 50$), H ($1 \leqslant H \leqslant 200$), M ($1 \leqslant M \leqslant H$), T ($1 \leqslant T \leqslant 100$) and $ALPHA$ ($0 \leqslant ALPHA < 90$), then displays the axonometric projection to the plane $Y = 0$ of the path of the ant using continuous line on the visible side of the cylinder and dotted line on the back side.

Example. *Figure 2* shows the path of the ant with $R = 50$, $H = 200$, $M = 1$, $T = 40$, $ALPHA = 30$.

(*10 points*)

I. 36. According to the trinomial theorem

$$(x+y+z)^n = \sum_{\substack{0 \leqslant a,b,c \leqslant n \\ a+b+c=n}} \binom{a+b+c}{a,b,c} x^a y^b z^c.$$

The trinomial coefficients can be computed, for example, by the formula

$$\binom{a+b+c}{a,b,c} = \frac{(a+b+c)!}{a!b!c!}.$$

However, these factorials can be very large, thus their direct computation is not always feasible. Nevertheless, writing trinomial coefficients as a product of binomial coefficients can settle this problem.

Prepare your sheet (I36.xls) which, if n ($n = a+b+c$, $n \leqslant 20$) is entered into a given cell, displays a table of trinomial coefficients, similar to the one below.

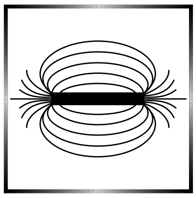
The example shows the coefficients when $n = 5$.

a/b	**0**	**1**	**2**	**3**	**4**	**5**
0	1	5	10	10	5	1
1	5	20	30	20	5	0
2	10	30	30	10	0	0
3	10	20	10	0	0	0
4	5	5	0	0	0	0
5	1	0	0	0	0	0

(*10 points*)

New problems: `http://www.komal.hu/verseny/2002-10/inf.e.shtml`

Interesting new characteristics of the electrostatic field



There are many important and interesting characteristics of the electrostatic field, such as the spherical symmetry of the field of a point charge or the theorem which states that outside a homogeneously charged spherical shell an electrostatic field generated by it is the same as that of a point charge having the same overall electric charge, and the electric field strength inside the shell is zero. Beyond these well-known features there arose a question in my mind of which I have not heard or read in any book, neither of the proposal nor of the solution of the problem. This problem — mainly after having been considered thoroughly — cast a new light on the characteristics of electrostatic fields (and also of those fields that can be described with similar equations, such as magnetostatic and gravitational fields) for me.

A problem of averaging

The question I was concerned with was: what result do we get in an arbitrary electrostatic field (not necessarily having a spherical symmetry) if we average the electric field strength vector and the electric potential on the surface of an imaginary sphere?

My guess was that the average electric field vector would be the same as the electric field vector in the centre of the sphere and the average potential would be the same as the electric potential in the centre of the sphere. As we will see, the guess is *not* correct in general, but is not too far from the truth and with a slight modification a true statement can be given.

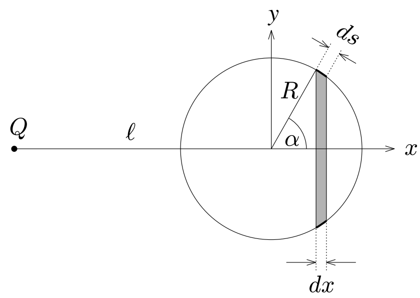
The 'brute force' method

Let us calculate the average of the potential mechanically, that is let us call upon the help of the integral calculus. (If the Reader is inexperienced in this chapter of mathematics, do not put away this paper just skip this section, because in the latter sections there is also an elementary solution offered to this problem!)

Let us first take a field where there is only one point charge and it is in ℓ distance of the centre of the imaginary sphere of radius R. Under the 'average' of the U potential we mean the quantity of:

$$U_{\text{average}} = \frac{\sum_i U_i \cdot df_i}{\sum_i df_i} \tag{1}$$

Interpretation: the surface of the sphere is divided into df_i surface elements (i is an appropriately chosen index of the elements) and the average of the electric potentials detectable on the surface weighted with the size of the surface elements is calculated. (We must emphasize here that df_i means the *size* of a surface element, a scalar quantity, and it should not be mixed up with the 'directional surface element' a vector used in calculating fluxes).



Let us get down to calculation. Take the co-ordinate frame as seen in the *figure*. The point charge resides on axis x, and let us take the centre of the sphere as the origin. Let us divide the surface of the sphere into belts of width dx. The first step is to determine the size of these surface belts.

$$df = 2\pi y \cdot ds = 2\pi R \sin\alpha \cdot \frac{dx}{\sin\alpha} = 2\pi R \cdot dx.$$

That is, we got that the size of the spherical belts depend only on dx and that makes our further task quite simple. With the above equation the whole surface of the sphere can easily be calculated:

$$F = \sum df = 2\pi R \cdot \sum_{x=-R}^{+R} dx = 2\pi R \cdot 2R = 4\pi R^2. \tag{2}$$

In the next step let us calculate the potential in the surface points with x co-ordinates.

$$U = \frac{kQ}{r},$$

where

$$r = \sqrt{(\ell + x)^2 + y^2} = \sqrt{(\ell + x)^2 + R^2 - x^2} = \sqrt{\ell^2 + 2\ell x + R^2}.$$

Now, we can do the integration itself. Since the surface elements with the same distance from the point charge are on a thin spherical belt, it is sensible to divide the sphere into such belts or zones and make the averaging according to these.

$$\begin{aligned} U_{\text{average}} &= \frac{1}{F} \int U \cdot df = \frac{1}{4\pi R^2} 2R\pi \cdot kQ \cdot \int_{-R}^{R} \frac{1}{\sqrt{\ell^2 + 2\ell x + R^2}}\, dx = \\ &= \frac{kQ}{2\ell R}\big(|\ell + R| - |\ell - R|\big) = \begin{cases} \dfrac{kQ}{\ell}, & \text{if } \ell \geqslant R, \\[2mm] \dfrac{kQ}{R}, & \text{if } \ell \leqslant R. \end{cases} \end{aligned} \tag{3}$$

We have arrived at a strange formula. Firstly, its form is peculiar, since in the final formula only one is present of the two quantities, R and ℓ, and in a symmetric way. Secondly, the physical interpretation is also interesting, because the same formula describes the potential derived from a homogeneously charged spherical shell of charge Q in distance ℓ. The present problem under investigation is quite different to that, as it appears, but we will see that there is a close connection between the two (and that can be well exploited).

An elementary solution resulting from energetic considerations

Now let us think that the so far imaginary (or 'virtual') spherical shell is an existing (insulator) body which is charged homogeneously with $q = 1$ total charge. What is the *interaction energy* of this homogeneously charged spherical shell and a point charge of magnitude Q residing in ℓ distance from its centre?

This energy can be determined in two ways. On the one hand, we can calculate the potential derived from the spherical shell in the place where the point charge is located (this can easily be done since the charge distribution has a spherical symmetry) and multiply it with the magnitude of the point charge (Q). The result is well-known, it is exactly the same as the final form of equation (3).

But there is another way. In the spherical symmetric (Coulomb) field of the point charge Q we can calculate the potential energy of the homogeneously distributed charge of the spherical shell. In theory it can be done by dividing the spherical shell into small parts in thought, multiplying the quantities of charge of the surface elements (df), that is $df/(4\pi R^2)$, by the potentials resulting from the Q point charge at the place of the given surface elements, and summing up these energies.

The second method is technically much more difficult than the first one. But fortunately we do not have to go through the complicated summing procedure since its result is obviously the same as that of the first calculation.

N.B. the quantity resulted by the second method is the average potential on the sphere of radius R originated from charge Q. Benefiting from the fact that the two calculations have identical results, the average value in question can be determined with an *elementary* method leaving out the integral calculus:

$$U_{\text{average}} = \begin{cases} \dfrac{kQ}{\ell}, & \text{if } \ell \geqslant R, \\ \dfrac{kQ}{R}, & \text{if } \ell \leqslant R. \end{cases} \tag{4}$$

The average of the electric field strength vector

The next problem is the averaging of the *electric field vector.* On the basis of our foregoing results this can be done in two ways. The first method is based on the idea that the field vector is in close connection with the potential, or more exactly with the rate of its spatial variation. This connection can be described in a mathematical form: if from a location where the electric field vector is E we move on with a small Δx displacement vector, the change in the potential will be:

$$\Delta U = -\overrightarrow{E} \cdot \overrightarrow{\Delta x}. \tag{5}$$

(In the above expression the dot between the two vector quantities means the dot-product of the two vectors, and the negative sign expresses that going in the direction of $\overrightarrow{E}$ the potential energy *decreases.*)

From all these it follows that if we know the potential in every location in an electrostatic field, we can calculate the field vector with (5) as well. In a given place the components of the field vector can be calculated by moving out from the given location in the direction of all three co-ordinate axes by Δs displacement and divide the change in the potential with Δs. The resulting three quantities are just the field vector components (except for the sense).

It is not the field vector in a point we would like to determine now but rather the field vector *average.* Since the components of the average field vector are equal with the average of those consequent components and these can be expressed by the energy variation of the whole sphere due to displacement we can achieve our aim with equations (4) and (5). The x component of the average field vector can be calculated by displacing the sphere along the axis x by Δs, calculating the variation of the average potential in this position and dividing it by Δs. (We exploit here the fact that the change in the average and the average change in the potential are identical.)

Let us see what equation (4) and the above procedure tells us of the average field vector. If the point charge is inside the sphere, we can move the sphere in any direction but the average potential will not change, since it depends only on R and independent of ℓ. For this reason, the average field vector on the surface of the sphere is nil. If the charge Q is outside the sphere, the situation is a bit more difficult. However, in this case we can exploit the fact that the average potential is independent of R, so the sphere can be point-like as well. But in this case, the potential energy would be the well known interaction energy of two point charges and the field vector derived by its variation would be equal with the Coulomb filed in the centre of the sphere. Summarizing briefly: The average of the field vector of a point charge on a sphere can be calculated as:

$$\overrightarrow{E}_{\text{average}} = \begin{cases} \dfrac{kQ}{\ell^2} \cdot \dfrac{\overrightarrow{\ell}}{\ell}, & \text{if } \ \ell > R, \\ 0, & \text{if } \ \ell < R. \end{cases} \tag{6}$$

Superposition

So far we have dealt with one point charge and the average of its electric field on an imaginary sphere. What is the case if the electrostatic field is generated by several point charges (or a continuous distribution of electric charge)? The resultant electric field is the vector sum (superposition) of the field of the single point-like charges and the average of the sum is the sum of the average of the single constituent fields.

In the previous section we saw that — in the case of a point charge — the average field vector is equal with the field vector detectable in the centre of the sphere. From the superposition principle it follows that the average of the resultant field vector of an arbitrarily complex electrostatic field is equal with the electric field vector in the centre of the sphere generated by the charges residing outside of the sphere. The charges residing inside the sphere do not add to the average. This is the small modification that was not included in the guess-based first form of our theorem. It is interesting that summing according to directed (considered as vector quantities) surface elements (averaging) the situation is just the opposite: the addition of the charges outside of the sphere is nil and the result depends only on the charges inside the sphere, and only these determine the electric flux going through the surface.

Action-reaction

As a conclusion we show that the result obtained for the average of the electric field vector could have been determined more simply without any reference of the potential, with a straight method valid for the most general fields without any symmetry.

Let us suppose that there is an actually existing, evenly charged spherical surface and its overall charge equals the unit charge. In this case, the average of the field vector just equals the force exerted on the sphere by the whole charge system. This force is — according to the action-reaction law — the same as the force exerted on the charge system by the electrostatic field of the sphere with opposite direction. As the sphere is evenly charged, its field corresponds to the field of a point charge (outside of the sphere). So the force is that of a point charge of unit charge exerted on the charges outside of the sphere.

Let us apply the action-reaction principle again: the resultant force exerted on the charges outside of the sphere is equal with the force exerted on a point-like unit charge in the centre of the sphere (apart from the sense), and this equals the electric field vector derived from the outer charges in the centre of the sphere. What is the case with the inner charges? We leave this matter to the reader.

Throughout these considerations we exploited only the inverse square law of the field of a point charge and the superposition principle. The Newtonian gravitational field also possesses these characteristics. And with some further considerations the results are also valid in a magnetic field (Although there is no magnetic pole in Nature, the magnetic field can be describe *as if there were* separate magnetic poles, and the same kind of laws are valid as in electrostatics). Therefore all of our statements are valid in the same form for the gravitational and magnetostatic fields and also applicable for all 'Coulomb-like' vector fields that may be discovered in the future.

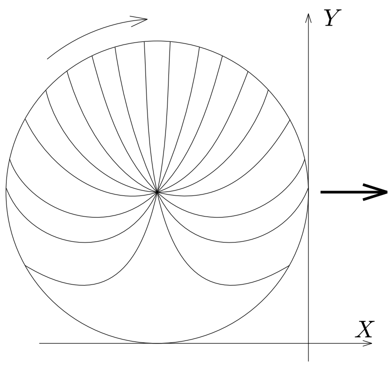
Balázs Pozsgay

Solutions of problems for physics P

P. 3425. *What is the picture of the spoked wheel of a bicycle like on a photo-finish? (The photo finish is made the following way: pictures of a very narrow band around the finish line are made in very short time intervals using electronic camera. These are then placed next to each other at distances corresponding to the expected speed of the bicycle.)*

(*6 points*) Submitted by: *Bodor András,* Budapest

Solution. For the sake of simplicity let us take the radius and velocity of the wheel both as 1 unit (in this case the angular velocity is also 1 unit). Let us choose a co-ordinate system where axis x lies in the direction of the horizontal motion of the bicycle and axis y points vertically upwards.



When the axle of the wheel is in point $(-1, 1)$ (when the forefront of the wheel touches the finish line where $x = 0$), the equation of a spoke including an α angle with axis x is: $y-1 = \tan\alpha \cdot (x+1)$. (We neglected the size of the wheel hub, that is all the lengthened spokes are supposed to go through the axis of the wheel.) After a certain t time the spoke turns by $-t$ angle and the wheel moves t distance in the direction of the positive axis x, so the equation of the spoke will be: $y - 1 = \tan(\alpha - t) \cdot (x - t + 1)$. In the photo-finish those points can be seen that are on axis y, that is those that correspond to the condition $x = 0$ and they are positioned in the height of:

$$Y = y(t)_{x=0} = 1 + \tan(\alpha - t) \cdot (1 - t),$$

and their horizontal co-ordinate (corresponding the 1 unit horizontal speed) is $X = -t$. (Those co-ordinates that give the 'virtual reality' of the photo-finish are denoted by capital letters and they are not to be mixed up with the real co-ordinates of the spokes denoted by lower case letters!)

Let us make a graph of the function $Y(X) = 1 + \tan(\alpha + X) \cdot (X + 1)$ with different *alpha* angles (choose values in 20° steps)! The rim of the wheel looks like a circle in the photo-finish too since a rotation maps a circle into a circle and the proper amount of 'electronic displacement' of the points takes their translational motion proportionally into account.

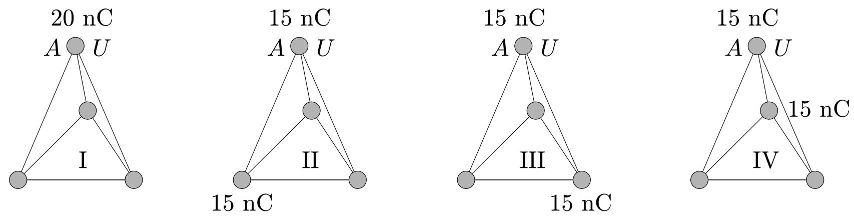
The problem of spokes is not so simple. As can be seen in the figure they are very distorted in these images, and their shape corresponds well to the shape of the spokes on the real electronic photo-finishes (After important bicycle events these can be found and studied on the Internet as well.) (Such a photo-finish can be seen on the home page of KöMaL at the preliminary short solution of the recent problem. The editor.)

Based on the paper of *Dőry Magdolna*
(10th form student of Ferences Secondary Grammar School, Szentendre)

P. 3432. *Identical metal spheres are placed into the vertices of a regular tetrahedron. The spheres do not touch. When a single sphere* (A) *is given a charge of* 20 nC *it reaches the same potential as when A and another sphere are given* 15 nC *each. What equal charge should be given to A and to two other spheres, and what equal charge to all four spheres so that the potential of sphere A is always the same?*

(*6 points*) Submitted by: *Bihary Zsolt,* Irvine, California

Solution. If, in a certain tetrahedral arrangement, the electric charges are in equilibrium on the metal spheres, then increasing the charges proportionally (say λ times) the equilibrium will not change but the original values of the field strengths and potentials will increase λ times. It is also true that if we add together two equilibrium arrangements then the result is also an equilibrium arrangement in which the field strengths and the potentials at every point are the sum of the original vectors or scalars. The two above-mentioned characteristics can together be described as the *principle of superposition.*



Let us term the first arrangement (with only one charged sphere) I, and the second (where A and an other sphere is charged) II. Turn by 120° arrangement II around a line connecting the centre of sphere A and the centre of the tetrahedron (let us call this arrangement III), and turn it by $-120°$ (let us call this arrangement IV).

After this let us take the superposition of the λ_1-fold value of arrangement I and the λ_2-fold values of arrangements II and III and let us choose the coefficients in a way that there are three spheres of the same charge and the potential of sphere A is exactly the same (U) as in arrangement I. These requirements are fulfilled if

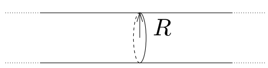
$$20\lambda_1 + 15\lambda_2 + 15\lambda_2 = 15\lambda_2, \quad \text{and} \quad \lambda_1 U + \lambda_2 U + \lambda_2 U = U.$$

The solution of the above equation system is $\lambda_1 = -\frac{3}{5}$, $\lambda_2 = \frac{4}{5}$ and, accordingly, the three charged spheres will have 12 nC charge each.

Similarly, taking the proper superposition of arrangement I and arrangement II + III + IV, an arrangement can be obtained where all four spheres have the same charge and the potential of A is U. In this case the charge of the spheres are 10 nC each.

Based on the paper of *Pápai Tivadar*
(11th form student of Dráva Völgye Secondary School, Barcs)

Note. If the distance of the spheres were much greater than the radii of the spheres, their electrostatic field could be obtained in the point charge approximation. In this case (with the numbers given) this is not feasible, the size of the spheres and their distances are commeasurable and therefore the spheres polarize each other. The calculation of the charge distributions and the electric field is very difficult, but fortunately they are not needed — if we follow the above considerations.



P. 3436. *One of the planets of star Noname is long and cylindrical. The average density of the planet is identical to that of the Earth, its radius equals that of the Earth and the period of its rotation is exactly* 1 *day.*

a) *What is the first cosmic speed for this planet?*

b) *How high above the surface of the planet do the synchronous telecommunications satellites orbit?*

c) *What is the second cosmic speed for this planet?*

(*5 points*) Submitted by: *Horányi Gábor,* Budapest

Solution. The gravitational field around a very long cylinder shows cylindrical symmetry, and the direction of the field strength (sufficiently far from the ends) is radial, which means that it is perpendicular to the axis of the cylinder and its magnitude depends solely on the distance from that axis.

Using the analogy of gravitational and Coulomb fields we can make the statement that the number of the gravitational field lines (the product of the **g** gravitational acceleration and the surface perpendicular to it) 'leaving' the body of mass m is $4\pi f \cdot m$ where f is the Newtonian gravitation constant. Therefore, the connection between the g-lines leaving a cylinder of length L and radius r and the mass inside the cylinder is:

$$g \cdot 2r\pi L = 4\pi f R^2 \pi L \varrho, \quad \text{that is} \quad g(r) = \frac{2\pi f R^2 \varrho}{r}.$$

a) According to the above law of force (and motion equation $mg = mv^2/r$) the velocity of a body revolving in a circular orbit, independently of the radius of the orbit (so on the surface of the planet as well), is:

$$v = \sqrt{2fR^2\pi\varrho},$$

accordingly, this is the value of the first cosmic speed. This is $\sqrt{3/2}$ times higher than the value valid for the Earth

$$v_F = \sqrt{\frac{fM_{\text{Earth}}}{R}} = \sqrt{\frac{4}{3}R^2\pi f\varrho} = 7.9 \text{ km/s}$$

that is about $9,7$ km/s.

b) The period of a satellite revolving in an orbit of radius r is $T_r = 2\pi r/v$. If one 'day' is T_0 long, then the orbiting radius of a synchronous satellite is

$$r_0 = \frac{T_0 v}{2\pi} = R\sqrt{\frac{T_0^2 f\varrho}{2\pi}}.$$

In the case of the Earth this radius is $r^* = R\sqrt[3]{T_0^2 f\varrho/3\pi}$, that is

$$r_0 = \sqrt{\frac{2r^{*3}}{3R}} \approx 1.33 \cdot 10^8 \text{ m}.$$

Synchronous telecommunications satellites therefore orbit at an

$$r_0 - R = 1.27 \cdot 10^8 \text{ m}$$

height above the surface of the cylinder shaped planet.

c) The second cosmic speed, which is the escape velocity from the planet, is very high, and its exact value depends on the length of the planet. If it is endless, the escape velocity is also endless because with finite energy there is *no escape* from a force field, which decreases in the order of the $1/r$ law. To prove this, let us consider a series of distances in geometrical progression: $r_n = \alpha^n r_0$ (where $\alpha > 1$ and $r_0 = R$). The energy $E(r_{n-1} \to r_n)$ that is needed to get from the height of r_{n-1} to the height of r_n is independent of n, that is with increasing n the force decreases the same rate as the distance increases. The required energy to get from r_0 to r_N is $E(r_0 \to r_N) = NE(r_0 \to r_1)$. It is clear even from this that while putting in finite energy one can get only to a finite height.

If the planet is not endless (its length is H), then as long as we are far from its ends and $r \ll H$, the $1/r$ force law holds, but if $r \simeq H$, the characteristics of the force law change, and if $r \gg H$ the usual $1/r^2$ rule takes over. From a planet like this an escape is possible at a certain finite velocity.

Based on the papers of
Dolgos Gergely (11th form student of Árpád Secondary Grammar School, Budapest) and *Siroki László* (11th form student of Fazekas M. Secondary Grammar School, Debrecen)

Note. Using the means of the integral calculus it can be shown that the second cosmic speed equals the $\sqrt{2} \cdot \ln(H/R)$-fold value of the first cosmic speed (In Earth's case it is $\sqrt{2}$.) This logarithmic factor doesn't get too big even if $H \gg R$ (when $H = 10\,R$ $v_{\text{II}}/v_{\text{I}}$ is about 3, and at the value of $H = 1000\,R$ it is still lower than 10).

(G. P.)

Solution of measuring problem M

M. 222. *The angle of refraction of a puck bouncing back from a board is usually not identical to its angle of incident. (The motion of a puck can be modelled using the lid of a jar.) How does the angle of refraction depend on the speed of the puck (lid) and on the angle of incidence?*

Solution. For an adequate measurement one needs a 'puck launching device' which can repeat puck launches at the same initial speed (within measurement error). This technical problem was resolved by most competitors, using a spring or rubber operated 'catapult'. *Biró István* (10th form student of Bolyai Farkas Secondary School, Marosvásárhely) constructed a clever device, which, in addition to the repeatable launches, solved the problem of recording the path of the puck (*Fig. 1*). He bore a hole into the middle of the puck, into which he put a toothpick wrapped in sewing thread. He had black ink permeated into the thread, and so the end of the sewing thread, just touching a glass plate, draw the path of the centre of mass of the puck.

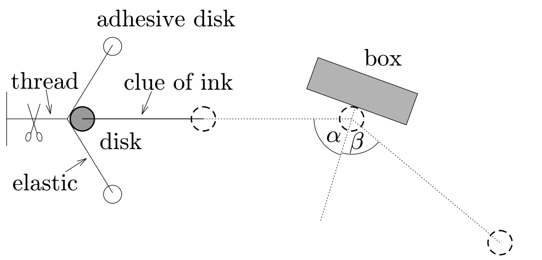


Figure 1

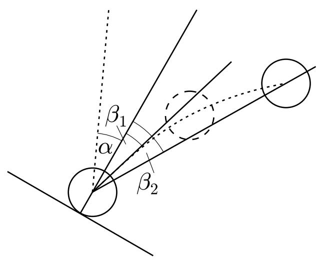


Figure 2

Two competitors, *Nagy Ádám* (12th form student of Szent István Secondary Grammar School, Budapest) and Biró István, noticed that the reflected path of the puck 'bends', but they did not use this fact in the determination of the reflection angle. All of the competitors calculated the β_2 reflection angle from the position of the puck after it had stopped, but this differs slightly from angle β_1 which characterizes the collision better though it is more difficult to measure (*Fig. 2*).

A crucial point in the completion of the measurement is the selection of the sliding surface. Most competitors chose a smooth surface. In the velocity measurement they had to take friction into account. *Jurányi Zsófia* (12th form student of Leöwey Klára Secondary Grammar School, Pécs) carried out her measurements on a panel board oiled with co-oking oil. She stated that on a board like that friction is negligibly small. *Geresdi Attila* (11th form student of Árpád Fejedelem Secondary Grammar School, Pécs) made his experiments on a 1 m^2 air-cushioned table. The competitors usually used rulers and bevels for measuring the angles, but there were other methods as well: *Sükösd Zsuzsanna* (7th form student of Orsolya Rendi Szent Angéla Elementary and Secondary Grammar School, Budapest,) used 'chequered' floor-plates as a coordinate system to define the position and the motion of the puck. Almost all the competitors got a result where the reflection angle was greater than the angle of incidence, but the difference was small and decreased while approaching the perpendicular direction. This was demonstrated by the graph drawn by *Szilágyi Péter* (9th form student of Kossuth L. Secondary Grammar School, Debrecen) containing the data for 3 different velocities (*Figure 3*). Nagy Ádám plotted the *ratio* of the reflection and incidence angles as a function of the incidence angle (*Figure 4*).

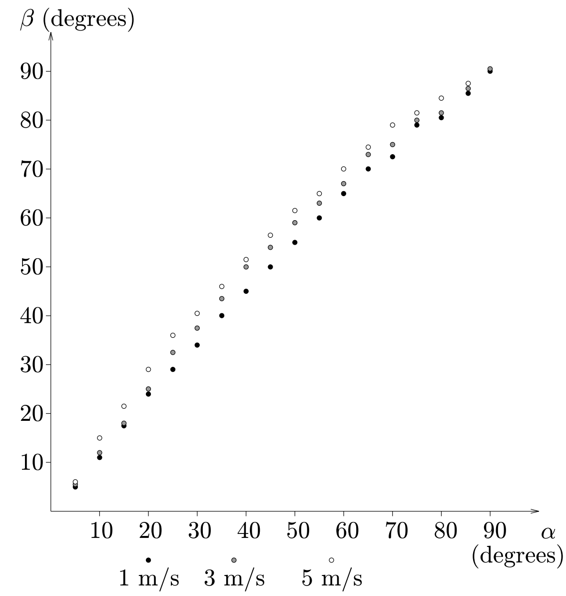


Figure 3

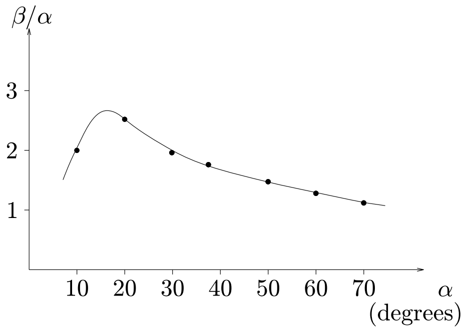


Figure 4

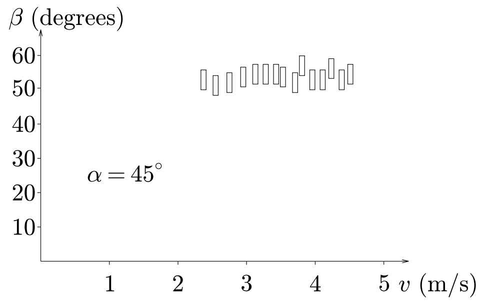


Figure 5

The experimental examination of velocity dependence is more difficult than measuring the angles. Using slopes the attainable velocity differences of the pucks started from different heights are not big enough — with considerable measurement errors — to find a definite connection between the angles and velocities. (Using catapult devices the velocity of the impact can be greater, but the measurement of velocity becomes more inaccurate.) The data measured by Jurányi Zsófia is shown in *Figure 5.* She plotted the β reflection angle (the accuracy of the measurement is also indicated) against different v impact velocities at fixed $\alpha = 45^\circ$ incidence angle. It can be seen that in the investigated interval β is independent of v.

Problems in Physics

M. 237. Make a 1.5 m-long line pendulum using a table-tennis ball as the weight. How does the work done by the aerodynamic drag (the energy lost) depend on the starting height h? What is the average power of the aerodynamic force during a half swing?

(*6 points*) Suggested by: *Varga István,* Békéscsaba

P. 3561. According to a car safety advertisement a 50 km/h collision into a wall has the same result as falling off the top of a four-storey building. What storey height did they think of?

(*3 points*) Suggested by: *Kopcsa József,* Debrecen

P. 3562. In a fruit farm the crates are conveyed on steel plates dragged by tractors. The mass of a steel plate is 20 kg and 400 kg of fruit is piled on it. The friction coefficient between the plate and the soil is 0.6. To what extent does the steel plate heat up on a 100 meter road if the internal energy of the steel plate is increased by 40% of the work done by the friction?

(*3 points*) *"Keresd a megoldást!"* competition, Szeged

P. 3563. There are two cars following each other on a narrow straight road. Their speed is 72 km/h each. The leading one begins to brake and stops with constant deceleration while his velocity decreases 5 m/s a second. The response time of the other driver is 1 second, and he can decrease his velocity by 4 m/s a second.

a) What distance should there be at least between the two cars to avoid a collision?

b) If they keep the minimally safe distance, how long will it take them to be at a 22 m distance of each other after the fist one begins to brake?

(*4 points*) Suggested by: *Szegedi Ervin,* Debrecen

P. 3564. How many balloons of a 25 cm diameter can be inflated from a 0.1 m^3 volume gas cylinder filled with helium at a pressure of 1.5×10^7 Pa? The gas pressure in a balloon rises to 1.02×10^5 Pa when the temperature of the gas reaches the temperature of the environment. The gas cylinder has been in the place where the balloons are filled for days.

(*4 points*) Suggested by: *Hilbert Margit,* Szeged

P. 3565. We want to cool down 15 l of 80 °C water to 25 °C by putting 0 °C ice into it. What minimum volume should the vessel have to prevent the water from overflowing at the rim?

(*3 points*) Suggested by: *Holics László,* Budapest

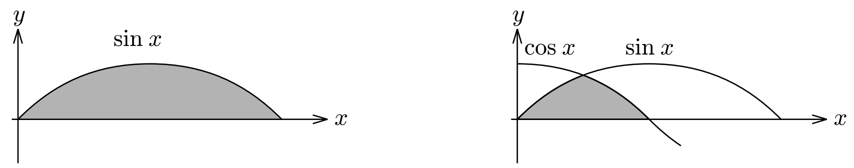
P. 3566. We want to throw a weight of 5 kg over a 1.5 m high wall, starting from ground level at a 2 m distance from the wall.

a) what should the direction of the 8 m/s initial velocity be to throw the weight the furthest beyond the wall? What is this distance?

b) What is the lowest energy to use for throwing the weight over the wall? What is the direction of the initial velocity in this case?

(*5 points*) Suggested by: *Szűcs József,* Pécs

P. 3567. Determine the size of the two hatched areas in the *figure* without using the integral calculus, by some simple physical reasoning.



(*5 points*) Suggested by: *Sári Péter,* Budapest

P. 3568. We fix a line pendulum with a pointlike weight of mass m to a horizontal metal ceiling. The period of the pendulum for small amplitudes is T_1. Then we put some electric charge on the weight and make it swing with a small amplitude again. The line is insulating. The period now is T_2. What is the charge put on the weight? (*The data:* $m = 5$ g, $T_1 = 2.02$ s, $T_2 = 2.03$ s, $g = 9.81$ m/s^2.)

(*5 points*) Suggested by: *Légrádi Imre,* Sopron

P. 3569. There is a 1.12 A electric current going through a working discharge tube filled with hydrogen gas. How many electrons pass the cross-section of the tube in one second if the number of electrons leaving the cathode is 3×10^{18} a second?

(*4 points*) Suggested by: *Radnai Gyula,* Budapest

P. 3570. We connect an R resistance, an L inductor device and a C capacitor after a sinusoidal generator of voltage U in a serial arrangement. The inductivity is adjustable. When it is increased, the current first increases then it begins to decrease. The highest current reached is I_0, and then the voltage of the coil is U_0.

Increasing the inductivity further, the voltage of the coil reaches a maximum of $U_{\max}$, and then begins to decrease. Determine the $U_{\max}/U_0$ ratio and calculate its value when $R = 2\sqrt{2}X_C$.

(*5 points*) Suggested by: *Veres Zoltán,* Margitta (Romania)

New problems: `http://www.komal.hu/verseny/2002-10/fiz.e.shtml`

KöMaL

It was more than a hundred years ago that Dániel Arany, a high school teacher from the city of Győr, decided to found a mathematical journal for high school students. His goal was "to give a wealth of examples to students and teachers". The journal's first edition appeared on January 1, 1894.

The foundation of the Journal had close connections with the boom in scientific life at the turn of the century. The Mathematical and Physical Society was founded in 1891, and in the autumn of 1894 the first Eötvös Competition in mathematics was organised for students that just graduated from high school.

From that time several generations of mathematicians and scientists developed their problem-solving skills through KöMaL. The best solutions with the names of the 14–18 year-old authors are printed in the periodical.

KöMaL regularly reports on national and international competitions, prints articles on interesting results in mathematics and physics, and includes book reviews.

For more than 30 years all the new problems have appeared in English as well as Hungarian. This means thousands of mathematics and physics problems and exercises in English.

The Journal is published today by the János Bolyai Mathematical Society and the Roland Eötvös Physical Society with the financial support of the Ministry of Education in 6000 copies.

Periodical "KöMaL — Középiskolai Matematikai és Fizikai Lapok" appears in Hungarian language 64 pages a month 9 times a year.

Every issue contains the English translation of 5 new exercises for practice (C), 10 problems (B) and 3 advanced problems (A) in mathematics; an experimental problem (M) and 10 problems (P) in physics; 3 problems (I) in Information Technology.

This journal (Hungarian language) can be ordered for 35 USD in a school year (postal costs are included). Those who want to send us solutions from September month to month in English should pay a 35 USD entry fee, the problem of the competition can be find on the web page of the KöMaL: `http://www.komal.hu`. If they subscribe KöMaL (in English, two issues per year), subscription plus entry fee is only 50 USD for a school year.

Please return this Order Form (Subscription Form) to

Roland Eötvös Physical Society,

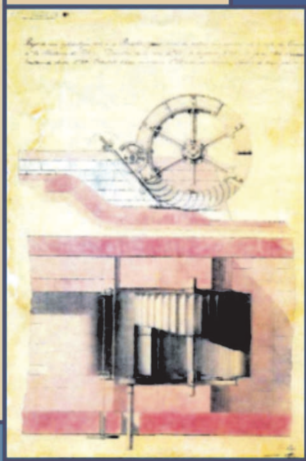
Budapest, P.O.B. 433, H-1371, Hungary

E-mail: `szerk@komal.hu` Telefax: +36 (1) 201-8682.

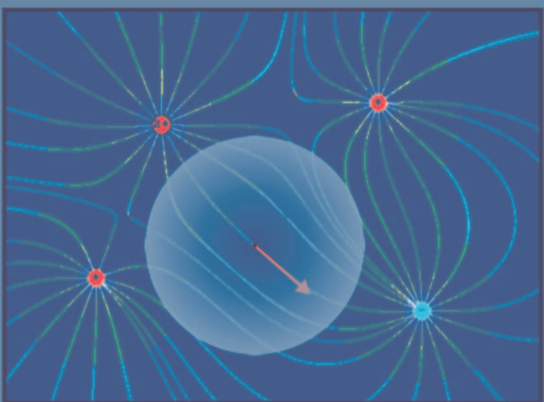
Jean-Victor Poncelet (1788-1867)

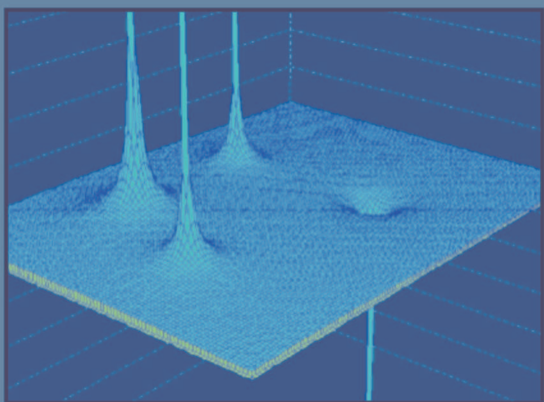
Jean Victor Poncelet was born in Metz in 1788. As an officer of Bonaparte's Grand Army he partook in the campaign against Russia and he was taken a prisoner during the retreat in 1812. Still in prison he had produced an essay in geometry. In 1826 he published a book on mechanics and another one water mills. The latter one included his new design of the traditional undershot waterwheel. He has proposed to reshape the blades so that the fluid could enter the wheel tangentially. After this it dropped into a trench with a minimum of kinetic energy. A breastwork at the front increased the head of water that resulted the water contact the wheel about 15 degrees over the vertical position. Poncelet was awarded the "Prix de Mechanique" by the French Academy for his design in recognition of his wheel having achieved an efficiency of 30 percent, double that of the older wheels. Steam power was still a few years ahead on the way and many of the 60,000 water wheels in France had been quickly retrofitted with this efficient new wheel.

A side view and top view drawing of Poncelet's Wheel (Turin, Madonna del Pilone watermills, 1844)



The average of the electric field vector on the surface of an uncharged sphere is the same as the electric field vector in the centre of the sphere.

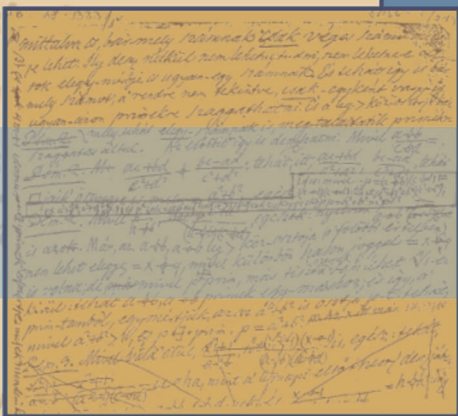




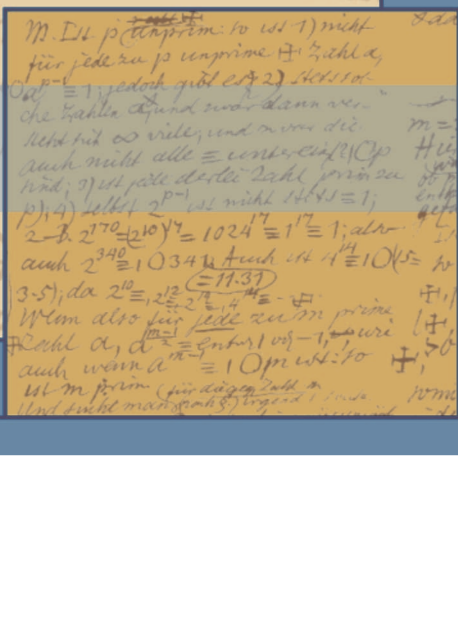
200 years from the birth of Bolyai János

János Bolyai (1802-1860)

The house in Kolozsvár (Cluj, Romania) where Bolyai was born.



János Bolyai's short, elegant and simple proof for Fermat's famous Christmas Theorem, that would deserve an entry in the Great Book of Paul Erdős.



One of Bolyai's (so far unpublished) manuscript on number theory, in German.

The background shows a page of the Appendix