# GAZETA MATEMATICĂ

## SERIA A

ANUL XXX(CIX) Nr. 1 – 2/ 2012

## ARTICOLE

### Functions with the Intermediate Value Property

Beniamin Bogoşel[1)]

**Abstract**. The article presents the construction of some real functions which have the intermediate value property and other interesting properties. A new approach in finding a discontinuous solution for the Cauchy functional equation which has the intermediate value property is presented in the second part, along with a theorem regarding the structure of the solutions of the same equation in terms of solutions with intermediate value property.

**Keywords:** Intermediate value property, Cauchy functional equation.

**MSC:** 26A30, 39B22, 26B35, 03E75

## 1. Introduction

In this article we construct some unusual and unintuitive functions which have interesting properties. We will concentrate our attention on the intermediate value property. In the first part we prove the existence of functions which map any open real interval onto a certain subset of $\mathbb{R}$. Next we present Sierpiński's theorem which states that every function $f : \mathbb{R} \to \mathbb{R}$ can be written as the sum of two functions with the intermediate value property, and a theorem regarding the existence of a function $f : [0,1] \to [0,1]$ for which there exist non-empty sets $A, B$ which partition the interval $[0,1]$ with $f(A) \subset B$ and $f(B) \subset A$. In the third section we give a very simple example of a function which is a discontinuous solution for the Cauchy functional equation and has the intermediate value property. In the end we present a variant of Sierpiński's theorem for the solutions of the Cauchy functional equation.

[1)]Faculty of Mathematics and Informatics, West University, Timişoara, Romania, beni22sof@yahoo.com

**Definition 1.1.** *If $f : I \to \mathbb{R}$ is a function, and $I \subset \mathbb{R}$ is an interval, $f$ has the* intermediate value property *if for any $a, b \in I,\ a < b$ and for any $\lambda$ between $f(a)$ and $f(b)$, there is $c \in (a, b)$ such that $f(c) = \lambda$.*

In applications, one of the following equivalent definitions is easier to use:

- $f$ has the intermediate value property if and only if $f(J)$ is an interval for any interval $J \subset I$.
- $f$ has the intermediate value property if and only if $f([c, d])$ is an interval for any $c, d \in I,\ c < d$.

**Definition 1.2.** *If $f : I \to \mathbb{R}$ is a function, and $I \subset \mathbb{R}$ is an interval, $f$ has the* weak intermediate value property *if $\overline{f(J)}$ is an interval, for any interval $J \subset I$.*

For $x, y \in \mathbb{R}$ define $x \sim y$ if and only if $x - y \in \mathbb{Q}$. This is obviously an equivalence relation and for any $x \in \mathbb{R}$ we will denote by $[x] = \{y \in \mathbb{R} : y \sim x\}$ the equivalence class which contains $x$. It is obvious that $\mathbb{R} = \bigcup_{x \in \mathbb{R}} [x]$ and $y \notin [x] \Rightarrow [x] \cap [y] = \emptyset$. In the following, we denote by $\mathcal{A} = \{[x] : x \in \mathbb{R}\}$ the set of the equivalence classes, and we will find its cardinal number. In the sequel, we denote $\aleph = \mathrm{card}\mathbb{R}$.

**Proposition 1.1.** $\mathrm{card}\mathcal{A} = \mathrm{card}\mathbb{R}$.

*Proof.* Set $C = \mathrm{card}\mathcal{A}$. Since every equivalence class has $\aleph_0$ elements, taking cardinals in the relation $\mathbb{R} = \bigcup_{[x] \in \mathcal{A}} [x]$, we obtain

$$\aleph = C\aleph_0 = C,$$

since $C$ is infinite. □

## 2. Some strange functions with intermediate value property

We state some results about the existence of some interesting real functions which have the intermediate value property.

**Theorem 2.1.** *There exist non-constant functions $f : \mathbb{R} \to \mathbb{R}$ which map any open interval onto a closed one.*

Another surprising result is given in the following

**Theorem 2.2.** *There exist functions $f : \mathbb{R} \to \mathbb{R}$ which have the intermediate value property and take any real value in any neighborhood of any point in $\mathbb{R}$.*

A slight generalization is the following

**Theorem 2.3.** *Given $T \subseteq \mathbb{R}$, there exists a function $f : \mathbb{R} \to \mathbb{R}$ such that $f$ maps any open interval onto $T$.*

*Proof.* Because $\mathrm{card}T \leq \mathrm{card}\mathbb{R} = \mathrm{card}\mathcal{A}$, there exists a surjection $\phi : \mathcal{A} \to T$. Considering the function $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \phi([x])$ we have the requested function. □

**Remark 2.1.** Note that if $\mathrm{card}T > 1$, any function which satisfies the condition of Theorem 2.3 is a function which has intermediate value property and is everywhere discontinuous.

If we denote $\mathcal{E} = \{f : \mathbb{R} \to \mathbb{R}\}$ and $\mathcal{D} = \{f \in \mathcal{E} : f$ has the intermediate value property$\}$ there are not many obvious set relations between $\mathcal{E}$ and $\mathcal{D}$ (apart from the obvious $\mathcal{D} \subset \mathcal{E}$). Still, if we consider for two subsets $A, B$ of $\mathcal{E}$ the operation $A + B = \{f + g : f \in A, g \in B\}$ we will find that $\mathcal{D} + \mathcal{D} = \mathcal{E}$. This result is due to Wacław Sierpiński.

**Theorem 2.4.** (Sierpiński) *For any function $f : \mathbb{R} \to \mathbb{R}$ there exist two functions $f_1, f_2 : \mathbb{R} \to \mathbb{R}$ having the intermediate value property and being discontinuous at any point in $\mathbb{R}$ such that $f = f_1 + f_2$.*

The proof of Sierpiński's theorem uses the equivalence relation defined above and the set of equivalence classes $\mathcal{A}$. The proof is somewhat classical, and will not be included here. Proofs can be found in [4], [5]. Also, the ideas used in proving Theorem 3.3 can easily lead to the proof of Sierpiński's theorem. The proof of the above theorem inspired the following result, proposed as a problem in a Romanian mathematical contest[1)] in 2003:
*Let us define*

$$\mathcal{F} = \{f : [0,1] \to [0,1] : \text{ there exist non-empty sets } A, B \subset [0,1]$$
$$\text{with } \; A \cap B = \emptyset, A \cup B = [0,1], \; f(A) \subset B, \; f(B) \subset A\}.$$

*Study if $\mathcal{F}$ contains continuous functions, functions which have antiderivatives, and functions which have the intermediate value property.*

The answer to the first two questions is obvious. If a function $f \in \mathcal{F}$ is continuous or has antiderivatives, then the function $g(x) = f(x) - x$, $\forall\, x \in [0,1]$ has antiderivatives. It is well known that any function which has antiderivatives necessarily has the intermediate value property. Since $g(0)g(1) \leq 0$ and $g$ has the intermediate value property, we conclude that $g$ has at least one zero in $[0,1]$. This yields that $f$ has a fixed point which contradicts $f \in \mathcal{F}$.

The third part is way harder than the first two, since in fact there exists a function $f \in \mathcal{F}$ with the intermediate value property, and the task becomes finding such an example. The fixed point argument used before does not work in the case of functions with the intermediate value property, since it

[1)] „Traian Lalescu“

is known that there exist functions $f : [0,1] \to [0,1]$ having the intermediate value property and without fixed points (see for example [6]).

**Theorem 2.5.** *There exist functions $f \in \mathcal{F}$ having the intermediate value property.*

*Proof.* We choose a bijection $\phi : \mathcal{A} \to \mathbb{R}$ and denote $Y = \phi^{-1}((\infty, 0])$, $Z = \phi^{-1}((0,\infty))$. Take $A = \{x \in [0,1] : [x] \in Y\}$, $B = \{x \in [0,1] : [x] \in Z\}$. $A$ and $B$ are disjoint and non-empty because $Y$ and $Z$ are disjoint and non-empty. We have $Y \cup Z = \mathcal{A}$, so $A \cup B = \{x \in [0,1] : [x] \in \mathcal{A}\} = [0,1]$. Because $A$ and $B$ contain all the elements from $[0,1]$ which are in the same equivalence class, $A$ and $B$ are dense in $[0,1]$.

From their definitions, $\mathrm{card}Y = \mathrm{card}Z = \mathrm{card}A = \mathrm{card}B = \aleph$. Therefore, we can find two bijections $\mu : Y \to B$ and $\nu : Z \to A$. We define the function $f : [0,1] \to [0,1]$ by

$$f(x) = \begin{cases} \mu([x]), & x \in A \\ \nu([x]), & x \in B. \end{cases}$$

From the definition of $f$ and of the sets $A, B, Y, Z$ we find that $f(A) \subset B$ and $f(B) \subset A$. Let's prove that $f$ has the intermediate value property. We take $I$ an interval contained in $[0,1]$. Then $I$ intersects all the classes from $\mathcal{A}$ (because any of these is dense in $\mathbb{R}$), which means that $I$ intersects all the classes from $Y$ and $Z$. Hence $f(I) = \mu(Y) \cup \nu(Z) = B \cup A = [0,1]$. Therefore $f \in \mathcal{F}$ and $f$ has the intermediate value property. □

From the theorem above we have the following

**Corollary 2.1.** *If $a, b \in \mathbb{R}$, $a < b$ then we can find functions $f : [a,b] \to [a,b]$ which have the intermediate value property and have no fixed points.*

## 3. Cauchy functional equation and the intermediate value property

A function $f : \mathbb{R} \to \mathbb{R}$ satisfies the *Cauchy functional equation* if

$$f(x+y) = f(x) + f(y) \tag{C}$$

holds for any $x, y \in \mathbb{R}$.

Here are a few facts about the Cauchy functional equation:

i) A function which satisfies (C) also satisfies $f(qx) = qf(x)$, $\forall\, q \in \mathbb{Q}$, $\forall\, x \in \mathbb{R}$.

ii) Any function of the form $f(x) = ax$, $a \in \mathbb{R}$, satisfies the equation (C). We will call these functions the *trivial solutions* of equation (C). It is well known that any continuous solution of the equation (C) is trivial.

iii) If we consider $\mathbb{R}$ as vector space over $\mathbb{Q}$, then, according to (C) and i), $f$ is a linear map. This implies that $f$ is well and uniquely defined if we know its values on a $\mathbb{Q}$-basis of $\mathbb{R}$.

The proof of the above facts is straightforward, and for any details we refer the reader to [2], pg. 193. The next result allows us to talk about the nontrivial solutions of (C).

**Proposition 3.1.** *There exist nontrivial solutions of the equation* (C).

*Proof.* Using iii) we can take a basis $\mathcal{B}$ which contains 1 and consider $f(1) = 1$, $f(b) = 0$, $\forall\, b \in \mathcal{B} \setminus \{1\}$. Thus $f(x)$ will be the coefficient of 1 in the representation of $x$ in the basis $\mathcal{B}$. Because $f(\mathbb{R}) = \mathbb{Q}$, $f$ is not a trivial solution for (C). □

Once we established the existence of nontrivial solutions for (C), we can give the following theorem which states that the nontrivial solutions of the Cauchy functional equation have an unusual graph:

**Theorem 3.1.** *If $f$ is a nontrivial solution for* (C)*, then its graph*

$$G_f = \{(x, y) \in \mathbb{R}^2 : y = f(x)\}$$

*is everywhere dense in* $\mathbb{R}^2$.

*Proof.* Assume that $f$ is a nontrivial solution of (C) such that $G_f$ is not dense in $\mathbb{R}^2$. Then there exist $a, b, c, d \in \mathbb{R}$ such that $D = (a, b) \times (c, d)$ and $D \cap G_f = \emptyset$. We prove now that at least one of the following is true:

i) $f(x) \leq c,\ \forall x \in (a, b)$;
ii) $f(x) \geq d,\ \forall x \in (a, b)$.

Assume that there exist $x, y \in (a, b)$ such that $f(x) \leq c$ and $f(y) \geq d$. Then there exist $q, r \in \mathbb{Q}_+$ with $q + r = 1$ such that

$$f(qx + ry) = qf(x) + rf(y) \in (c, d),$$

because $[0, 1] \cap \mathbb{Q} \ni t \mapsto (1 - t)f(x) + tf(y)$ maps densely into $[f(x), f(y)] \supset$ $\supset (c, d)$. This contradicts the fact that $D \cap G_f = \emptyset$.

Without loss of generality assume that i) holds. There exist $\delta > 0$ and $h \in \mathbb{R}$ such that $(-\delta, \delta) + h \subset (a, b)$. Using the additivity of the function $f$ and i) we obtain that $f$ has an upper bound on $(-\delta, \delta)$. Because $f(x) = -f(-x)$, for every $x \in \mathbb{R}$ we conclude that $f$ is bounded on $(-\delta, \delta)$.

Because of the additivity, continuity in 0 is equivalent to global continuity, therefore $f$ is not continuous in 0. Then there exists a sequence $(y_n)$ which tends to 0 such that $f(y_n) \to \ell \in (0, \infty]$ (if $\ell < 0$, then replace $(y_n)$ by $(-y_n)$). Because almost all terms of the sequence are in $(-\delta, \delta)$, we deduce that $(f(y_n))$ is bounded. There exists $n_0$ with the property that $f(y_n) > \min\{\ell/2, 1\}$ whenever $n \geq n_0$. Take $m \in \mathbb{N}$. Then there exists an integer $k_m \geq \max\{n_0, k_{m-1}\}$ such that $|my_{k_m}| < \delta$. For $k_m$ we have $f(my_{k_m}) = mf(y_{k_m}) > \dfrac{ml}{2}$. This procedure builds a subsequence $(y_{k_m})$ of $(y_n)$ for which $f(y_{k_m}) \to \infty$, which contradicts the fact that $f$ is bounded on $(-\delta, \delta)$. □

**Remark 3.1.** We can see from the results above that the solutions of the equation (C) have a common property: If $f$ is a solution for (C), then $f$ has the *weak intermediate value property*, that is, $\overline{f(J)}$ is an interval whenever $J \subset I$ is an interval.

Thinking about the connection between the solutions of the Cauchy functional equation and the intermediate value property, we may ask a few questions:

1) Does every solution of the Cauchy functional equation have the intermediate value property?
   *Answer:* No. An example occured in the proof of Theorem 3.1.
2) Since continuity forces a solution to be trivial, we may ask if the intermediate value property forces a solution to be trivial.
   *Answer:* No. An example can be found in the next theorem.

**Theorem 3.2.** *There exist nontrivial solutions for equation* (C) *which have the intermediate value property.*

*Proof.* We use iii) and choose a basis $\mathcal{B}$ of $\mathbb{R}$ over $\mathbb{Q}$ which contains 1. Take a bijection $\phi : \mathcal{B} \setminus \{1\} \to \mathbb{R}^*$, and then define $f(1) = 0$ and $f(b) = \phi(b)$, $\forall b \in \mathcal{B} \setminus \{1\}$.

It is clear that $f(q) = 0$, $\forall q \in \mathbb{Q}$. Considering the equivalence relation $\sim$ we get that $x \in [y] \Rightarrow f(x) = f(y) + f(x - y) = f(y)$. Let $y \in \mathbb{R}$. Then we can find $b \in \mathcal{B}$ such that $f(b) = \phi(b) = y$. We take $b_0 \in [b] \cap I$ which is non-empty. We have $f(b_0) = f(b) = y$, so $y \in f(I)$, and because $y$ was chosen arbitrarily, it follows that $f(I) = \mathbb{R}$. Therefore $f$ has the intermediate value property. We see that $f(\mathbb{Q}) = \{0\}$ and $f(\mathbb{R}) \neq \{0\}$, which proves that $f$ is a nontrivial solution for (C). □

The example in the last theorem gives us a solution of the Cauchy functional equation which is non-trivial, has the intermediate value property and is surjective. The next result provides an interesting connection between these concepts.

**Proposition 3.2.** *If $f$ is a solution of the Cauchy functional equation which is surjective but not injective, then $f$ has the intermediate value property.*

*Proof.* First note that $f$ must be non-trivial. If $f$ would be trivial, then $f(x) = cx$ for some $c \in \mathbb{R}$. The hypothesis $f$ surjective proves that $c \neq 0$, but then $f$ is injective, a contradiction.

Since $f$ is not injective, there exists $b \neq 0$ such that $f(b) = 0$, and using the properties of $f$ we have that $f(qb) = 0$ for every $q \in \mathbb{Q}$.

Pick an interval $I \subset \mathbb{R}$ and a value $y_0 \in \mathbb{R}$. Since $f$ is surjective, there exists $x_0 \in \mathbb{R}$ such that $f(x_0) = y_0$. Since the set $\{x_0 + bq : q \in \mathbb{Q}\}$ is dense in $\mathbb{R}$, there exists $q_0$ such that $x_0 + bq_0 \in I$. Therefore $f(x_0 + bq_0) = f(x_0) = y_0$ and $y_0 \in f(I)$. This proves that $f(I) = \mathbb{R}$. Since this happens for every interval $I$, it follows that $f$ has the intermediate value property. □

If we denote

$$\mathcal{E}_C = \{f : \mathbb{R} \to \mathbb{R} : f \text{ is a solution of (C)}\}$$

and

$$\mathcal{D}_C = \{f \in \mathcal{E}_C : f \text{ has the intermediate value property}\},$$

then an analogous result to the Sierpiński theorem holds, namely $\mathcal{D}_C + \mathcal{D}_C = \mathcal{E}_C$. The theorem below can be found in [3], problem P.3.23, pg. 106, and was pointed out to me by the authors. The solution presented here is a simplified version of the solution given in the reference.

**Theorem 3.3.** *For every solution $f$ of the Cauchy functional equation there exist two non-trivial solutions $f_1, f_2$ of the same equation such that $f_1$ and $f_2$ have the intermediate value property and $f = f_1 + f_2$.*

*Proof.* Consider a $\mathbb{Q}$-basis $\mathcal{B}$ of $\mathbb{R}$ and $b_1, b_2 \in \mathcal{B}$. Since $\text{card}(\mathcal{B} \setminus \{b_1, b_2\}) = \text{card}\mathbb{R}$ there exists a bijection $g : \mathbb{R} \to B \setminus \{b_1, b_2\}$. Set $A = g((-\infty, 0))$ and $C = g([0, \infty))$. Therefore we have partitioned $B \setminus \{b_1, b_2\}$ into two uncountable sets $A$ and $C$. This allows us to construct another two bijections $g_1 : A \to \mathbb{R}$ and $g_2 : C \to \mathbb{R}$.

Now we can define two functions $f_1, f_2$ with the required properties. As we have already noticed, a solution of the Cauchy functional equation is well and uniquely defined if we know the values of the solution on a $\mathbb{Q}$-basis of $\mathbb{R}$. We can define $f_1$ and $f_2$ by their values on $\mathcal{B}$ as follows:

$$f_1(b) = \begin{cases} 0, & b = b_1 \\ f(b_2), & b = b_2 \\ g_1(b), & b \in A \\ f(b) - g_2(b), & b \in C \end{cases}$$

and

$$f_2(b) = \begin{cases} f(b_1), & b = b_1 \\ 0, & b = b_2 \\ f(b) - g_1(b), & b \in A \\ g_2(b), & b \in C. \end{cases}$$

Note that $f_1, f_2$ are solutions of the Cauchy functional equation. Moreover, it is easy to see that $f_1(b) + f_2(b) = f(b)$ for every $b \in \mathcal{B}$, which implies $f_1 + f_2 = f$.

Since $g_1$ is a bijection from $A$ to $\mathbb{R}$ it follows that $f_1$ is surjective, and because $f(b_1) = 0,\ b_1 \neq 0$ we see that $f_1$ is not injective. Using Proposition 3.2 we conclude that $f_1$ is nontrivial and has the intermediate value property. By a similar argument $f_2$ is nontrivial and also has the intermediate value property. $\square$

**Acknowledgments.** The author thanks to the referee for his careful reading of the manuscript and his helpful suggestions concerning the aspect and content of this paper.

## REFERENCES

[1] N. Jacobson, *Lectures in Abstract Algebra, vol. II, Linear Algebra*, D. Van Nostrand Company, Inc., 1953.
[2] A. B. Kharazishvili, *Strange Functions in Real Analysis*, Chapman & Hall/CRC, 2006.
[3] M. Megan, A.L. Sasu, B. Sasu, *Calcul diferenţial în $\mathbb{R}$ prin exerciţii şi probleme*, Ed. Mirton, Timişoara, 2003.
[4] M. Megan, *Bazele Analizei Matematice*, Ed. Eurobit, Timisoara, 1997.
[5] W. Sierpiński, *Sur une propriete des fonctions reelles quelconques*, Matematiche (Catania) 8(1953), 43-48.
[6] Z. Grande, *An example of a Darboux function having no fixed points*, Real Anal. Exchange 28(2002), 375-380.

# Arithmetical Properties of the Image of a Polynomial with Integer Coefficients

VLAD MATEI[1)]

**Abstract**. In this article we present some results on the set of prime divisors of the numbers in the image of a polynomial with integer coefficients, and we look at the image of such polynomials restricted to the set of prime numbers.

**Keywords:** Polynomials with integer coefficients.
**MSC:** 11C08, 11T06, 13B25

In the first part of this article we present some results on the set of prime divisors of the numbers in the image of a polynomial, which are classical but worthy of being noted. In the second section, which is our main contribution, we look at the image of the polynomials restricted to the set of prime numbers.

The most famous problem motivating the study of the set of prime divisors of the numbers in the image of a polynomial is a conjecture that states that if we have given an irreducible polynomial with integer coefficients and the greatest common divisor of the numbers in the set is 1, then this set must contain at least one prime number. This conjecture is due to Bunyakovsky. Schinzel generalized the conjecture of Bunyakovsky to a finite number of polynomials, asking if they could take simultaneously prime values.

An interesting illustrative example of a connected problem with this one is the famous Euler polynomial $n^2+n+41$ which takes prime values for $n=0,\ldots,39$. It is natural to ask whether for arbitrary $N$ we could find a

[1)]University of Cambridge, Cambridge, UK.

polynomial which takes prime values for at least $N$ consecutive values. This is also a conjecture.

## 1. Schur's Lemma and connected results

We define for a polynomial $f \in \mathbb{Z}[X]$ the following sets:

$$\mathbb{P}(f) = \{p \text{ prime} \mid \exists\, n \in \mathbb{N}^*, p \mid f(n)\}$$

and

$$\mathbf{P}(f) = \{p \text{ prime} \mid \exists\, q \in \mathbb{N}^*, q \text{ prime}, p \mid f(q)\}.$$

Note that $\mathbf{P}(f) \subset \mathbb{P}(f)$.

It is well-known that for $f \in \mathbb{Z}[X]$ we have $a - b \mid f(a) - f(b)$, for any $a, b \in \mathbb{Z}$, and we refer to as the "fundamental lemma".

We begin with a simple result.

**Proposition 1.1.** *For $f \in \mathbb{Z}[X]$ a non-constant polynomial, we have*

$$\mathbb{P}(f) = \mathbf{P}(f).$$

*Proof.* Let $p \in \mathbb{P}(f)$ and $p \nmid f(0)$. Then there exists $n \in \mathbb{N}$ with $(n, p) = 1$ and $p \mid f(n)$. According to Dirichlet's theorem, the arithmetic progression $n + pr$, with $r \in \mathbb{N}^*$, contains infinitely many primes. Let $q$ be a prime from this progression. Then, using the „fundamental lemma“, we have $p \mid f(q)$, so $p \in \mathbf{P}(f)$. For $p \mid f(0)$, it follows $p \mid f(p)$. Thus $\mathbb{P}(f) = \mathbf{P}(f)$. □

We proceed with the first classical result due to Schur.

**Theorem 1.1.** *(Schur's Lemma) For $f \in \mathbb{Z}[X]$ a non-constant polynomial, $\mathbb{P}(f)$ is an infinite set.*

*Proof.* We assume that $\mathbb{P}(f)$ is finite and let $\{p_1, \ldots, p_k\}$ denote its elements. We first note that $f(0) \neq 0$, otherwise $X \mid f(X)$, and thus $p \mid f(p)$ for any prime number $p$, a contradiction with our assumption.

Let $f(X) = a_nX^n + \cdots + a_1X + a_0$. We look at the value of $f$ on numbers of the type $Ma_0p_1 \cdots p_k$. We observe that

$$f(Ma_0p_1 \cdots p_k) = a_0[a_nM^na_0^{n-1}(p_1 \cdots p_k)^n + \cdots + a_1Mp_1 \cdots p_k + 1] = a_0t,$$

where $t \equiv 1 \pmod{p_1p_2 \cdots p_k}$. If $t \neq 1$, then there is a prime $q$ with $q \notin \{p_1, \ldots, p_k\}$ and $q \mid f(Ma_0p_1 \cdots p_k)$ for some $M$, a contradiction. Thus $f(Ma_0p_1 \cdots p_k) = a_0$ for any $M$. It follows that $f - a_0$ has infinitely many roots, so it is the zero polynomial, which leads to $f$ constant, a contradiction with the hypothesis. □

Since we have proven that $\mathbb{P}(f)$ is infinite, we can ask whether it could be the whole set of prime numbers. This obviously holds for linear polynomials. We can prove that these are the only irreducible polynomials for which this assertion holds.

**Theorem 1.2.** *The only irreducible polynomials $f \in \mathbb{Z}[X]$ for which $\mathbb{P}(f)$ contains all the primes, except a finite number, are the linear ones.*

*Proof.* A celebrated result, due to Frobenius (see [1]), states that the density of primes $p$ for which $f$ has a given decomposition of type $n_1, n_2, \ldots, n_t$ over $\mathbb{F}_p$ exists and is equal to $\dfrac{1}{|G|}$ times the number of $\sigma \in G$ with cycle pattern $n_1, \ldots, n_t$. (Here we denoted by $G$ the Galois group of the polynomial $f$, which can be identified with a group of permutations of the set $X$ of roots of $f$.) In particular, the density of primes where $f$ has a root, i.e. a factor of degree 1, equals $\dfrac{1}{|G|}$ times the number of elements of $G$ that have at least one cycle of length 1, i.e. a fixed point. By the hypothesis this density is equal to 1, so all elements of $G$ must have a fixed point.

We shall prove that this is not possible for $\deg(f) \geq 2$. In order to prove this we make use of Burnside's lemma (see [2]), which states that if $X$ is a finite $G$-set, and $|X^g|$ is the number of elements of $X$ fixed by $g$, then the number of $G$-orbits of $X$ is equal to $\dfrac{1}{|G|}\displaystyle\sum_{g \in G} |X^g|$. A corollary of this is that if $X$ is a finite transitive set with $|X| > 1$, then there is $g \in G$ with $|X^g| = 0$. The statement is immediate, since the number of $G$-orbits is 1, so $|G| = \displaystyle\sum_{g \in G} |X^g|$. We note that $|X^e| = |X| > 1$, so if for every $g \neq e$ we would have $|X^g| \geq 1$, then the number in the right-hand side would be too large.

We apply this to the case of the set $X$ of roots of the polynomial $f$, and $G$ taken as the Galois group of $f$. It follows that for $\deg(f) \geq 2$, or equivalently $|X| \geq 2$, since $f$ has no multiple roots, there is an automorphism $\sigma \in G$ with no fixed points. This contradicts our hypothesis. $\square$

The following result extends Schur's lemma to an arbitrary number of polynomials.

**Theorem 1.3.** *If $f_1, \ldots, f_n \in \mathbb{Z}[X]$ are non-constant polynomials, then $\displaystyle\bigcap_{i=1}^{n} \mathbb{P}(f_i)$ is an infinite set.*

*Proof.* First of all let us prove that there exists $z \in \mathbb{C}$ an algebraic number and the polynomials $h_1, h_2, \ldots, h_n \in \mathbb{Q}[X]$ such that $f_i(h_i(z)) = 0$, $\forall i = 1, \ldots, n$.

To prove this claim, for each $f_i$ we take $x_i$ one of its roots. The field extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(x_1, x_2, \ldots, x_n)$ is finite and separable. We deduce, from the primitive element theorem, that there exists $z \in \mathbb{C}$ with $\mathbb{Q}(z) = \mathbb{Q}(x_1, x_2, \ldots, x_n)$. Thus we can find $h_1, h_2, \ldots, h_n \in \mathbb{Q}[X]$ such that $h_i(z) = x_i$, and thus $f_i(h_i(z)) = f_i(x_i) = 0$.

We note that for each $h_i$ there is $N_i \in \mathbb{Z}^*$ such that $N_i h_i \in \mathbb{Z}[X]$. Thus the polynomials $N_i^{d_i} f \circ h_i$ have integer coefficients, where $d_i$ is the degree of $f_i$, $i = 1, \ldots, n$.

Since all these polynomials have in common the root $z$ which is an algebraic number, each of the polynomials $f \circ h_i$ is divisible by the minimal polynomial of $z$, denoted by $g$. We know that $g \in \mathbb{Q}[X]$, thus we consider $M \in \mathbb{Z}^*$ such that $Mg \in \mathbb{Z}[X]$.

We observe that $Mg \mid MN_i^{d_i} f \circ h_i$, $\forall i = 1, \ldots, n$. Since $Mg$ is a non-constant polynomial with integer coefficients, from Schur's lemma we know that $\mathbb{P}(Mg)$ is infinite. Now the set of prime divisors of the number $M \prod_{i=1}^{n} N_i$ is finite, and thus we deduce that $\mathbb{P}(Mg) \subset \mathbb{P}(f_i)$, $\forall\, i = 1, \ldots, n$, except a finite number of primes.

We conclude that $\mathbb{P}(Mg) \subset \bigcap_{i=1}^{n} \mathbb{P}(f_i)$, except a finite set, and thus the theorem is proved. □

## 2. The image of a polynomial restricted to prime numbers

In this section we present two results about the number of prime divisors and the exponent of a prime in numbers of the type $f(p)$, with $p$ prime.

**Theorem 2.1.** *The only polynomials $f \in \mathbb{Z}[X]$ for which there exists $k \in \mathbb{N}^*$ such that for any prime number $q$, $f(q)$ has at most $k$ distinct prime divisors, are $f(X) = cX^i$, where $c \in \mathbb{Z}^*$ and $i \in \mathbb{N}^*$.*

*Proof.* Let us prove that $f(0) = 0$. We proceed by contradiction and assume $f(0) \neq 0$.

We prove by induction on $j \in \mathbb{N}^*$ the following statement: there is a prime $p > |f(0)|$ such that $f(p)$ has at least $j$ distinct prime divisors.

For $j = 1$ there exists a prime $p_1 > |f(0)|$ such that $p_1$ is not a root of the polynomial $f^2 - 1$, since $f$ is non-constant. Then $p_1$ satisfies our statement.

Now, for $j \to j + 1$, let $p_j$ be a prime with the property $p_j > |f(0)|$ and $f(p_j)$ has at least $j$ distinct prime divisors. If $f(p_j)$ has at least $j+1$ distinct prime divisors, then we choose $p_{j+1} = p_j$. Otherwise, let us notice that $(p_j, f(p_j)) = 1$ since from the "fundamental lemma" we have $f(p_j) \equiv f(0) \pmod{p_j}$ and the conclusion follows since $p_j$ is prime and greater that $|f(0)|$. According to Dirichlet's theorem, there are infinitely many primes in the arithmetic progression $rf^2(p_j) + p_j$. Let $p_{j+1} = sf^2(p_j) + p_j$ be such a prime. From the "fundamental lemma" we have that $f(p_{j+1}) \equiv f(p_j) \pmod{f^2(p_j)}$ and thus there is $t$ such that $f(p_{j+1}) = f(p_j)(1 + tf(p_j))$. From this it is obvious that $f(p_{j+1})$ has at least one prime divisor more than $f(p_j)$. Since

$f(p_j)$ has $j$ distinct prime divisors it follows that $f(p_{j+1})$ has at least $j+1$ prime factors.

Thus the statement is proved and we get that $f(0) \neq 0$ is false. This implies $f(0) = 0$, so $f(X) = X^i g(X)$ with $g(0) \neq 0$, and if $g$ would be nonconstant, arguing the same way as above, we obtain again a contradiction.

We can now conclude that the only possibility is $f(X) = cX^i$ with $i \in \mathbb{N}^*$ and $c \in \mathbb{Z}^*$. $\square$

**Theorem 2.2.** *The polynomials $f \in \mathbb{Z}[X]$ such that $f(p)$ is $k$-th power free for all primes $p$, where $k \geq 2$ is an integer, are $dX^i$, where $1 \leq i < k$, and every prime factor of $d$ occurs in its prime factors decomposition at a power less than or equal to $k-i-1$.*

*Proof.* First of all let $f = g_1 \cdots g_r$ be the decomposition of $f$ in irreducibile factors over $\mathbb{Z}[X]$. It follows from the hypothesis that $g_1, \ldots, g_r$ satisfy the condition that they are $k$-th power free on prime values. Thus we can assume that $f$ is a nonconstant irreducible polynomial.

Next let us prove that $f(0) = 0$. Assume the contrary, $f(0) \neq 0$.

Since $\deg(f') < \deg(f)$ and $f$ is irreducibile over $\mathbb{Q}[X]$, it follows that $(f', f) = 1$, and thus there are polynomials $g, h \in \mathbb{Q}[X]$ such that $f'g + fh = 1$. Now there is $c \in \mathbb{Z}$ such that $cg$ and $ch$ are both polynomials in $\mathbb{Z}[X]$, thus there are $g_1, h_1 \in \mathbb{Z}[X]$ with

$$f'g_1 + fh_1 = c. \tag{1}$$

From Schur's lemma we can choose infinitely many primes $q$ such that there is $p$ with $p > |c|$, $p > |f(0)|$, and $p^a \mid f(q)$, $1 \leq a < k$. We know from Taylor expansion for polynomials that

$$f(q+tp^a) = f(q)+f'(q)\cdot tp^a+f''(q)\cdot\frac{(tp^a)^2}{2!}+\ldots \equiv f(q)+f'(q)\cdot tp^a \pmod{p^{a+1}}.$$

If we have $p \mid f'(q)$, then from (1) we get $p \mid c$, a contradiction with $p > |c|$. Thus we can pick $t$ with the property that $f(q) + f'(q) \cdot tp^a \equiv$ $\equiv 0(\mathrm{mod}\ p^{a+1})$, so $p^{a+1} \mid f(q+tp^a)$. Since $f(0) \neq 0$, we get $(q+tp^a, p^{a+1}) = 1$. Assuming the contrary, it would follow that $p = q$, and this would imply $p \mid f(q) = f(p)$, thus $p \mid f(0)$, a contradiction with the choice $p > |f(0)|$. So $(q + tp^a, p^{a+1}) = 1$ and by Dirichlet's theorem there is a prime $m$ in the arithmetic progression $np^{a+1} + q + tp^a$ with $m \nmid f(0)$.

We have found a prime $m$ such that $p^{a+1} \mid f(m)$. We can repeat the same argument in order to increase the power of $p$ and finally reach a contradiction with the fact that the exponent of $p$ is bounded by $k$.

Thus $f(0) = 0$ and since $f$ is irreducible it follows that $f = \pm X$. We can conclude from here that the only required polynomials are of the form $dX^i$ with $1 \leq i < k$ and every prime factor of $d$ occurs at a power less than $k - i - 1$. $\square$

References

[1] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2000.
[2] J. Rotman, *An introduction to the Theory of Groups*, Springer, 1995.


# Seria lui Euler

Mircea Olteanu[1)]

**Abstract**. The purpose of this note is to present one of the most celebrated problems of the XVII-th century, known as the "Basel Problem", i.e. the computation of the sum of the series $\sum_{n\geq 1}\frac{1}{n^2}$. The first part of the paper contains the "history" of the problem, including Euler's original approach and some further developments, e.g. the connections with the Prime Number Theorem. In the second part, few rigorous "modern solutions" are presented.

**Keywords:** Euler series, Riemann zeta function.
**MSC:** 40A05, 97I30

Calculele implicând sume infinite au apărut încă din antichitate. Paradoxul dihotomiei al lui Zenon (care conduce la seria geometrică de raţie $\frac{1}{2}$) sau aria mărginită de parabolă şi de o secantă a ei (calculată de Arhimede folosind suma seriei geometrice cu raţia $\frac{1}{4}$) sunt exemple celebre. În secolul al XIV-lea, Nicolas Oresme a arătat divergenţa seriei armonice, iar ulterior, în secolul al XVII-lea, Gregory, Newton, Leibniz ş.a. au rezolvat probleme devenite clasice (de exemplu, seria lui Leibniz: $\sum_{n\geq 1}\frac{(-1)^{n-1}}{2n-1}=\frac{\pi}{4}$). Desigur, demonstraţiile nu întruneau standardele actuale de rigoare, lucru explicabil ţinând cont de lipsa unor definiţii riguroase pentru noţiunile fundamentale ale analizei matematice: convergenţă, limită, derivată, integrală, convergenţă uniformă etc.

În această notă vrem să ilustrăm dificultăţile, dar şi implicaţiile profunde ale unor probleme ridicate de teoria seriilor. Vom face acest lucru prezentând o problemă celebră: calculul sumei seriei lui Euler

$$\sum_{n\geq 1}\frac{1}{n^2}=\frac{\pi^2}{6}$$

(numită, datorită fraţilor Jakob şi Johann Bernoulli, ,,problema de la Basel").

Textul care urmează are caracter elementar şi nu prezintă întreaga complexitate a consecinţelor care au avut ca punct de plecare problema de la

1) Department of Mathematical Methods and Models, University Politehnica of Bucharest

Basel. Scopul este de a ilustra câteva din subtilităţile pe care le ridică teoria seriilor şi de a prezenta o parte din ideile şi raţionamentele care l-au condus pe Euler la rezolvarea problemei. În plus, contactul cu metodele folosite de marii clasici ai matematicii poate avea astăzi valoare didactică, în sensul ideilor lui Courant şi Robbins din prefaţa la [2].

Revenim acum la seria lui Euler. Problema pare a fi fost enunţată pentru prima dată în 1644 de Pietro Mengoli (acesta a calculat în 1650 suma seriei armonice alternate, $\sum_{n\geq 1} \frac{(-1)^n}{n} = \ln 2$) şi aproape toţi marii matematicieni ai vremii au încercat să o rezolve (printre alţii: Wallis în 1655, Leibniz, Jakob şi Johann Bernoulli după 1691), ajungând cea mai cunoscută problemă a timpului respectiv. În anul 1734, Euler publică rezultatul (dând trei demonstraţii), după ce, în prealabil, începând cu 1730, obţinuse aproximări din ce în ce mai bune ale sumei seriei (6 zecimale exacte în 1731, 20 de zecimale exacte în 1733). Într-o serie de articole ulterioare (până în 1748), Euler a reluat problema, publicând mai multe soluţii, extinzând o serie de rezultate şi îmbunătăţind rigoarea argumentelor. În continuare vom prezenta ideile lui Euler, urmate şi de soluţii riguroase conforme cu standardele actuale.

Convergenţa seriei este asigurată de majorarea:

$$\sum_{n\geq 1} \frac{1}{n^2} \leq 1 + \sum_{n\geq 2} \frac{1}{n(n-1)} = 1 + \sum_{n\geq 2} \left( \frac{1}{n-1} - \frac{1}{n} \right) = 2.$$

Vom nota în continuare cu $\mathcal{S}$ suma seriei lui Euler.

## Aproximarea sumei

Trebuie observat că o primă dificultate a problemei constă în faptul că seria $\sum_{n\geq 1} \frac{1}{n^2}$ converge foarte încet, deci nu se pot obţine aproximări ale sumei adunând un număr acceptabil de termeni. Mai precis, din inegalităţile

$$\frac{1}{k} - \frac{1}{k+1} = \frac{1}{k(k+1)} < \frac{1}{k^2} < \frac{1}{(k-1)k} = \frac{1}{k-1} - \frac{1}{k},\ k = 2, 3, \ldots,$$

obţinem următoarea evaluare a restului seriei:

$$\frac{1}{m+1} < \sum_{n\geq m+1} \frac{1}{n^2} < \frac{1}{m},\ m = 1, 2, 3, \ldots.$$

De aici rezultă că pentru a calcula primele 6 zecimale exacte ale sumei seriei trebuie însumaţi cel puţin primii $10^6$ termeni. Pentru a obţine aproximări cât mai bune ale sumei, Euler a construit o serie care converge rapid la aceeaşi sumă ca şi $\sum\limits_{n\geq 1}\dfrac{1}{n^2}$. Seria obţinută de Euler este

$$\ln^2 2 + 2\sum_{n\geq 1}\frac{1}{n^2\cdot 2^n}. \tag{1}$$

Pentru aproximarea lui $\ln 2$ s-a folosit seria

$$\ln 2 = \sum_{n\geq 1}\frac{1}{n\cdot 2^n},$$

obţinută din seria de puteri a funcţiei $-\ln(1-x)$ pentru $x = 2^{-1}$. În acest fel Euler a obţinut valoarea aproximativă cu 6 zecimale exacte: $\mathcal{S}\approx 1,644944$.

Nu intrăm aici în detaliile descoperirii de către Euler a seriei (1); pe scurt, a considerat seria de puteri $\sum\limits_{n\geq 1}\dfrac{x^n}{n^2}$, $|x|\leq 1$ (de fapt funcţia generatoare a şirului $\dfrac{1}{n^2}$). Suma acestei serii este funcţia dilogaritmică, notată $\mathrm{Li}_2(x)$; evident, $\mathrm{Li}_2(1) = \mathcal{S}$. Are loc următoarea reprezentare integrală:

$$\mathrm{Li}_2(x) = \int_0^x -\frac{\ln(1-t)}{t}\mathrm{d}t.$$

Pentru $x = 1$, rezultă

$$\mathrm{Li}_2(1) = \int_0^s -\frac{\ln(1-t)}{t}\mathrm{d}t + \int_s^1 -\frac{\ln(1-u)}{u}\mathrm{d}u.$$

De aici, schimbând în a doua integrală variabila $1-u = y$ şi aplicând formula de integrare prin părţi, se obţine ecuaţia funcţională

$$\mathrm{Li}_2(x) + \mathrm{Li}_2(1-x) = -\ln x\cdot\ln(1-x) + \mathrm{Li}_2(1),\ \ |x| < 1.$$

Pentru $x = 2^{-1}$, rezultă

$$\mathcal{S} = \ln^2 2 + 2\sum_{n\geq 1}\frac{1}{n^2\cdot 2^n}.$$

## Metodele lui Euler pentru calculul sumei

În continuare vom prezenta câteva din soluţiile propuse de Euler. Ideea lui Euler a fost să extrapoleze relaţii între rădăcinile şi coeficienţii unui polinom la serii de puteri. În legătură cu utilizarea metodei analogiei în matematică recomandăm [4].

Prima soluţie (care are include şi un raţionament geometric) pe care Euler o prezintă în articolul din 1734 este descrisă în detaliu în [6].

Vom începe însă cu a treia soluţie din acel articol. Fie $P$ un polinom de gradul $2n$ cu coeficienţi reali, având numai termeni de grad par, scris sub forma

$$P(x) = a_0 - a_1 x^2 + a_2 x^4 + \cdots + (-1)^n a_n x^{2n}.$$

Presupunem că toate rădăcinile $x_1, -x_1, x_2, -x_2, \ldots, x_n, -x_n$ ale polinomului $P$ sunt reale, nenule şi simple. Din relaţiile dintre rădăcini şi coeficienţi rezultă

$$\sum_{k=1}^{n} \frac{1}{x_k^2} = \frac{a_1}{a_0}. \tag{2}$$

În continuare, Euler face o analogie între acest rezultat din teoria polinoamelor şi seria de puteri (pare) asociate funcţiei $\dfrac{\sin x}{x}$:

$$\frac{\sin x}{x} = 1 - \frac{1}{3!}x^2 + \frac{1}{5!}x^4 - \cdots$$

şi extrapolează (fără o justificare riguroasă) formula (2) în acest caz. Soluţiile ecuaţiei $\dfrac{\sin x}{x} = 0$ sunt $\pi, -\pi, 2\pi, -2\pi, \ldots$ şi deci din (2) rezultă

$$\sum_{n \geq 1} \frac{1}{(n\pi)^2} = \frac{1}{3!},$$

ceea ce încheie demonstraţia.

Desigur, Euler era conştient de punctele slabe ale raţionamentelor sale: nu toate rezultatele adevărate pentru polinoame sunt adevărate pentru serii de puteri, şi, în plus, nu se ştia în acel moment dacă $n\pi, n \in \mathbb{Z}$, sunt singurele zerouri ale funcţiei sinus. Totuşi, Euler era sigur că rezultatul este corect pentru că el concorda cu aproximările obţinute anterior (folosind seria (1)). În plus, el verificase proprietăţi de tipul (2) şi pentru alte serii de puteri utilizate în calculul unor sume infinite. Trebuie totuşi menţionat că există serii de puteri care nu satisfac relaţii de tipul (2). Un exemplu simplu în acest sens este dat de seria geometrică. Fie funcţia

$$f(x) = 2 - \frac{1}{1-x} = 1 - x - x^2 - x^3 - \cdots, \ |x| < 1.$$

Ecuaţia $f(x) = 0$ are o singură soluţie: $x = 2^{-1}$. Pe de altă parte, dacă încercăm să extrapolăm formula pentru suma inverselor rădăcinilor unui polinom (aceasta este în fapt relaţia (2)) la seria de puteri a funcţiei $f$, obţinem o contradicţie: $2 = 1$.

Prezentăm acum o altă soluţie (dată tot în articolul din 1734) care i-a permis ulterior lui Euler să obţină generalizări şi alte rezultate interesante. Fie $P$ un polinom de gradul $n$ având rădăcini nenule (eventual multiple)

$x_1, x_2, \ldots, x_n$ pe care-l scriem sub forma

$$P(x) = \left(1 - \frac{x}{x_1}\right)\left(1 - \frac{x}{x_2}\right) \cdots \left(1 - \frac{x}{x_n}\right).$$

Atunci, dacă polinomul $P$ are forma canonică

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

rezultă

$$a_0 = 1,$$

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = -a_1, \tag{3}$$

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = a_1^2 - 2a_2, \tag{4}$$

$$\frac{1}{x_1^3} + \frac{1}{x_2^3} + \cdots + \frac{1}{x_n^3} = -a_1^3 - 3a_1 a_2 - 3a_3,$$

$$\cdots\cdots\cdots\cdots\cdots$$

Euler a extrapolat (fără justificare riguroasă) acest rezultat de la polinoame la seria de puteri a funcţiei $1 - \sin x$:

$$1 - \sin x = 1 - \sum_{n \geq 0} \frac{(-1)^n}{(2n+1)!} x^{2n+1} = 1 - x + \frac{x^3}{3!} + \ldots, \ \forall x \in \mathbb{R}.$$

Funcţia $1 - \sin x$ se anulează în

$$\frac{\pi}{2}, -\frac{3\pi}{2}, \frac{5\pi}{2}, -\frac{7\pi}{2}, \ldots.$$

În plus, toate aceste rădăcini sunt duble (aici iarăşi se extrapolează noţiuni de la polinoame la serii de puteri).

Aplicând acum relaţia (3) seriei de puteri a funcţiei $1 - \sin x$, Euler regăseşte rezultatul lui Leibniz:

$$\frac{4}{\pi} \sum_{n \geq 1} \frac{(-1)^{n-1}}{2n-1} = 1.$$

În acelaşi mod, din relaţia (4), rezultă

$$\frac{8}{\pi^2} \sum_{n \geq 1} \frac{1}{(2n-1)^2} = 1.$$

Pentru a încheia demonstraţia mai este nevoie de următoarea observaţie simplă:

$$\sum_{n \geq 1} \frac{1}{(2n)^2} = \frac{1}{4} \sum_{n \geq 1} \frac{1}{n^2} = \frac{1}{4} \mathcal{S}.$$

Rezultă că

$$\mathcal{S} = \frac{4}{3} \sum_{n \geq 1} \frac{1}{(2n-1)^2} = \frac{4}{3} \cdot \frac{\pi^2}{8} = \frac{\pi^2}{6}.$$

Dacă introducem acum funcţia zeta a lui Riemann,

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}, s \in \mathbb{C}, s = \sigma + it,$$

definită de Euler pentru $s$ natural, prelungită de Chebyshev la numere reale $s > 1$ şi extinsă (prin prelungire analitică) de Riemann în 1859 la numere complexe, rezultatul de mai sus se scrie

$$\zeta(2) = \mathcal{S} = \frac{\pi^2}{6}.$$

Tot cu metoda de mai sus, rezultă

$$\zeta(4) = \sum_{n\geq 1} \frac{1}{n^4} = \frac{\pi^4}{90}.$$

Continuând raţionamentele, Euler a reuşit să calculeze valorile funcţiei $\zeta$ pentru orice număr natural par, exprimându-le cu ajutorul numerelor lui Bernoulli (introduse mai înainte de Jakob Bernoulli şi publicate postum în 1713):

$$\zeta(2k) = \frac{(-1)^{k-1}2^{2k-1}B_{2k}}{(2k)!} \cdot \pi^{2k},\ k = 1, 2, \ldots.$$

Euler este cel care, cu ocazia publicării acestei formule, a propus denumirea de „numerele lui Bernoulli“. Nu intrăm în detalii, doar reamintim o definiţie elementară a numerelor lui Bernoulli (notate $B_k$):

$$\sum_{k=1}^{n} k^m = \frac{1}{m+1} \sum_{k=0}^{m} C_{m+1}^k \cdot B_k \cdot n^{m+1-k},\ m, n = 1, 2, 3, \ldots.$$

În anul 1737, Euler demonstrează formula care face legătura între numerele prime şi funcţia $\zeta$:

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p \text{ prim}} \frac{1}{1 - p^{-s}}.$$

În scopul estimării numărului numerelor prime mai mici decât un număr dat $x$ (număr notat $\pi(x)$), în 1859, Bernhard Riemann prelungeşte funcţia $\zeta$ la întreg planul complex şi demonstrează că „zerourile netriviale“ ale funcţiei $\zeta$ se găsesc în „banda critică“ $0 \leq \sigma \leq 1$ şi sunt poziţionate simetric faţă de axa reală şi faţă de „axa critică“ $\sigma = \dfrac{1}{2}$ (vezi [5]). Reamintim că „zerourile triviale“ ale funcţiei $\zeta$ sunt numerele negative pare. Tot în articolul amintit, Riemann face celebra conjectură cu privire la „zerourile netriviale“ ale funcţiei $\zeta$: acestea sunt toate pe axa critică $\sigma = \dfrac{1}{2}$. Afirmaţia este încă nedemonstrată, ea constituind probabil cea mai celebră problemă ce îşi aşteaptă rezolvarea. Zerourile netriviale al e funcţiei zeta sunt legate de repartiţia numerelor prime.

În 1896, Hadamard şi de la Valleé-Poussin au demonstrat (în mod independent) legea de repartiţie asimptotică a numerelor prime (enunţată de Gauss în 1792):

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1,$$

folosind faptul că zerourile netriviale ale funcţiei zeta nu se găsesc pe dreapta $\sigma = 1$. În 1951, N. Wiener a arătat că teorema numerelor prime este de fapt echivalentă cu această proprietate. Demonstraţia conjecturii lui Riemann ar duce la enunţuri mai precise pentru repartiţia numerelor prime.

Revenind la seria lui Euler, acesta a publicat în 1744 celebra formulă-produs pentru funcţia sinus, formulă ce i-a permis să obţină riguros suma seriei $\sum\limits_{n\geq 1} \frac{1}{n^2}$:

$$\frac{\sin x}{x} = \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2\pi^2}\right). \tag{5}$$

Pentru demonstraţia formulei (5), Euler a pornit de la relaţia

$$\frac{\sin x}{x} = \frac{e^{ix} - e^{-ix}}{2ix}$$

şi a exprimat exponenţialele ca limite ale unor polinoame

$$\frac{\sin x}{x} = \lim_{n\to\infty} \frac{\left(1 + \frac{ix}{n}\right)^n - \left(1 - \frac{ix}{n}\right)^n}{2ix}.$$

Apoi a descompus în factori polinoamele

$$\frac{\left(1 + \frac{ix}{n}\right)^n - \left(1 - \frac{ix}{n}\right)^n}{2ix} = \prod_{k=1}^{p} \left(1 - \frac{x^2}{n^2} \cdot \frac{1 + \cos\frac{2k\pi}{n}}{1 - \cos\frac{2k\pi}{n}}\right), \quad n = 2p + 1.$$

Formula (5) se obţine prin trecere la limită şi comutând limita cu produsul:

$$\frac{\sin x}{x} = \lim_{n\to\infty} \prod_{k=1}^{p} \left(1 - \frac{x^2}{n^2} \cdot \frac{1 + \cos\frac{2k\pi}{n}}{1 - \cos\frac{2k\pi}{n}}\right) = \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2\pi^2}\right).$$

Euler nu justifică trecerea la limită factor cu factor, dar acest lucru se poate face uşor folosind noţiunea de convergenţă uniformă şi majorarea uniformă (în raport cu $n$):

$$\left|\frac{1+\cos\dfrac{2k\pi}{n}}{1-\cos\dfrac{2k\pi}{n}}\right| \leq \frac{M}{k^2\pi^2},$$

$M$ fiind o constantă rezultată din mărginirea funcţiei $\dfrac{x}{\sin x}$ în jurul originii. Folosind formula (5), suma seriei lui Euler se poate calcula identificând coeficientul lui $x^2$ din dezvoltarea

$$\frac{\sin x}{x} = 1 - \frac{1}{3!}x^2 + \frac{1}{5!}x^4 - \cdots$$

cu coeficientul lui $x^2$ din produsul 5; rezultă că

$$-\frac{1}{3!} = -\left(\frac{1}{\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \cdots\right),$$

ceea ce încheie demonstraţia.

## Exerciţiu

Înainte de a continua cu alte soluţii pentru problema de la Basel, propunem cititorului să demonstreze formula urmând metoda lui Euler (analogia polinoame - serii de puteri), folosind dezvoltarea în serie de puteri a funcţiei $\dfrac{\sin\sqrt{x}}{\sqrt{x}}$:

$$\frac{\sin\sqrt{x}}{\sqrt{x}} = 1 - \frac{1}{3!}x + \frac{1}{5!}x^2 - \frac{1}{7!}x^3 + \cdots$$

şi observând că funcţia $\dfrac{\sin\sqrt{x}}{\sqrt{x}}$ se anulează în $n^2\pi^2,\ n = 1, 2, 3, \ldots.$

## Metode moderne pentru calculul sumei

În continuare vom prezenta alte demonstraţii (numite de obicei moderne) ale rezultatului obţinut de Euler.

O primă metodă (elementară) foloseşte şirul de integrale

$$I_n = \int_0^{\frac{\pi}{2}} x^2 \cos^n x \, \mathrm{d}x,\ n = 0, 1, 2, \ldots.$$

Presupunem cunoscut rezultatul următor (pe care-l propunem ca exerciţiu):

$$\int_0^{\frac{\pi}{2}} \cos^{2n} x \, \mathrm{d}x = \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdot \ldots \cdot (2n)} \cdot \frac{\pi}{2}.$$

Pe de altă parte, integrând succesiv prin părţi, obţinem:

$$\int_0^{\frac{\pi}{2}} \cos^{2n} x\,\mathrm{d}x = 2n\int_0^{\frac{\pi}{2}} x\cos^{2n-1} x\cdot \sin x\,\mathrm{d}x = -n\int_0^{\frac{\pi}{2}} x^2(\cos^{2n-1} x\,\sin x)'\,\mathrm{d}x =$$

$$= n(2n-1)\int_0^{\frac{\pi}{2}} x^2\cos^{2n-2} x - 2n^2\int_0^{\frac{\pi}{2}} x^2\cos^{2n} x\,\mathrm{d}x = n(2n-1)I_{2n-2} - 2n^2 I_{2n}.$$

Folosind şi valoarea integralei $\int_0^{\frac{\pi}{2}} \cos^{2n} x\,\mathrm{d}x$ de mai sus, rezultă relaţia de recurenţă

$$2n^2 I_{2n} - n(2n-1)I_{2n-2} = -\frac{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot (2n)}\cdot\frac{\pi}{2}.$$

Înmulţind ultima egalitate cu $\frac{2\cdot 4\cdot 6\cdot \ldots\cdot (2n)}{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-1)}\cdot\frac{1}{2n^2}$, rezultă

$$\frac{2\cdot 4\cdot 6\cdot \ldots\cdot (2n)}{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-1)}\cdot I_{2n} - \frac{2\cdot 4\cdot 6\cdot \ldots\cdot (2n-2)}{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-3)}\cdot I_{2n-2} = -\frac{\pi}{4}\cdot\frac{1}{n^2}.$$

Scriem acum relaţia de mai sus pentru $1, 2, 3, l\ldots, n$ (pentru $n = 1$ luăm relaţia de recurenţă înainte de înmulţire) şi însumând obţinem

$$\frac{2\cdot 4\cdot 6\cdot \ldots\cdot (2n)}{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-1)}\cdot I_{2n} = I_0 - \frac{\pi}{4}\left(1+\frac{1}{2^2}+\frac{1}{3^2}+\ldots+\frac{1}{n^2}\right).$$

Prin calcul direct, $I_0 = \frac{\pi^3}{24}$ şi deci demonstraţia se încheie dacă arătăm egalitatea

$$\lim_{n\to\infty}\frac{2\cdot 4\cdot 6\cdot \ldots\cdot (2n)}{1\cdot 3\cdot 5\cdot \ldots\cdot (2n-1)}\cdot I_{2n} = 0.$$

Din inegalitatea elementară (exerciţiu !)

$$\frac{2}{\pi}\cdot x \le \sin x,\ \forall x\in\left[0,\frac{\pi}{2}\right],$$

rezultă

$$I_{2n} = \int_0^{\frac{\pi}{2}} x^2\cos^{2n} x\,\mathrm{d}x \le \frac{\pi^2}{4}\cdot\int_0^{\frac{\pi}{2}} \sin^2 x\cos^{2n} x\,\mathrm{d}x =$$

$$= \frac{\pi^2}{4}\left(\int_0^{\frac{\pi}{2}} \cos^{2n} x\,\mathrm{d}x - \int_0^{\frac{\pi}{2}} \cos^{2n+2} x\,\mathrm{d}x\right) =$$

$$= \frac{\pi^3}{8}\left(\frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}{2\cdot 4\cdot 6\cdot \ldots \gamma(2n)} - \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n+1)}{2\cdot 4\cdot 6\cdot \ldots \cdot (2n+2)}\right) =$$

$$= \frac{\pi^3}{8}\cdot \frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}{2\cdot 4\cdot 6 \ldots \cdot (2n+2)}.$$

Obţinem că

$$0 \le \frac{2\cdot 4\cdot 6\cdot \ldots \cdot (2n)}{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}\cdot I_{2n} \le \frac{\pi^3}{8}\cdot \frac{1}{2n+2},$$

ceea ce încheie demonstraţia.

O altă demonstraţie (tot cu caracter elementar) se obţine plecând de la identităţile trigonometrice:

$$\sum_{k=1}^{n} \mathrm{ctg}^2 \frac{k\pi}{2n+1} = \frac{n(2n-1)}{3},\ n = 1, 2, 3, \ldots$$

$$\sum_{k=1}^{n} \mathrm{cosec}^2 \frac{k\pi}{2n+1} = \frac{n(2n+2)}{3},\ n = 1, 2, 3, \ldots .$$

Inegalitatea (cunoscută)

$$\sin x < x < \mathrm{tg}\, x,\ \ \forall\, x \in \left(0, \frac{\pi}{2}\right),$$

se poate scrie sub forma

$$\mathrm{ctg}^2 x < \frac{1}{x^2} < \mathrm{cosec}^2 x,\ \forall\, x \in \left(0, \frac{\pi}{2}\right),$$

şi deci

$$\mathrm{ctg}^2 \frac{k\pi}{2n+1} < \left(\frac{2n+1}{k\pi}\right)^2 < \mathrm{cosec}^2 \frac{k\pi}{2n+1},\ k = 1, 2, \ldots, n.$$

Însumând inegalităţile de mai sus pentru $k = 1, 2, 3, \ldots, n$ şi aplicând cele două identităţi trigonometrice menţionate, rezultă

$$\frac{n(2n-1)}{3} < \frac{(2n+1)^2}{\pi^2}\sum_{k=1}^{n}\frac{1}{k^2} < \frac{n(2n+3)}{3},$$

sau, echivalent,

$$\frac{\pi^2}{(2n+1)^2}\cdot \frac{n(2n-1)}{3} < \sum_{k=1}^{n}\frac{1}{k^2} < \frac{\pi^2}{(2n+1)^2}\cdot\frac{n(2n+3)}{3}.$$

Pentru $n \to \infty$ se obţine rezultatul lui Euler.

Ultima soluţie pe care o prezentăm foloseşte serii trigonometrice. În continuare vom presupune că cititorul este familiarizat cu dezvoltarea în serie trigonometrică a unei funcţii periodice.

Vom dezvolta în serie Fourier funcţia (continuă)

$$f(x) = x^2,\ x \in (-\pi, \pi].$$

Calculăm coeficienţii Fourier:

$$a_0 = \frac{1}{\pi}\int\limits_{-\pi}^{\pi} x^2\,\mathrm{d}x = \frac{2}{3}\pi^2,$$

$$a_n = \frac{1}{\pi}\int\limits_{-\pi}^{\pi} x^2\cos nx\,\mathrm{d}x = \frac{2}{n\pi}x^2\sin nx\Big|_0^{\pi} - \frac{4}{n\pi}\int\limits_0^{\pi} x\sin nx\,\mathrm{d}x =$$

$$= \frac{4}{n^2\pi}x\cos nx\Big|_0^{\pi} - \frac{4}{n^2\pi}\int\limits_0^{\pi}\sin nx\,\mathrm{d}x = 4\frac{(-1)^n}{n^2},\ \forall\, n \geq 1.$$

$$b_n = \frac{1}{\pi}\int\limits_{-\pi}^{\pi} x^2\sin nx\,\mathrm{d}x = 0,\ \forall\, n \geq 1.$$

Obţinem dezvoltarea

$$x^2 = \frac{a_0}{2} + \sum_{n\geq 1}(a_n\cos nx + b_n\sin nx) =$$

$$= \frac{\pi^2}{3} + \sum_{n\geq 1} 4\frac{(-1)^n}{n^2}\cos nx,\ \forall x \in (-\pi, \pi].$$

În particular, pentru $x = \pi$, obţinem rezultatul lui Euler.

Există multe alte soluţii pentru problema de la Basel. O parte dintre ele, însoţite de diverse dezvoltări şi comentarii interesante, se pot găsi în lucrările de mai jos.

## REFERENCES


[1] R. Chapman, *Evaluating* $\zeta(2)$, available at
`http://www.math.uiuc.edu/~reznick/zeta2.pdf`

[2] R. Courant, H. Robbins, *Ce este matematica*, Ed. Ştiinţifică, 1969.

[3] D. Kalman, *Six ways to sum a series*, available at
`http://scipp.ucsc.edu/~haber/ph116A/Sixways.pdf`

[4] A. Pease, M. Guhe, A. Smaill, *Using analogies to find and evaluate mathematical conjectures*. Proceedings of the 1st International Conference on Computational Creativity, Lisbon, 7–9 January 2010, pp. 60–64.

[5] B. Riemann, *On the Number of Prime Numbers less than a Given Quantity (Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse)*, Monatsberichte der Berliner Akademie, November 1859. Translated by D. R. Wilkins, 1998.

[6] E. Sandifer, *Euler's Solution of the Basel Problem – The Longer Story*, available at
`http://www.math.uiuc.edu/~reznick/sandifer.pdf`

[7] The Euler Archive, *The works of Leonhard Euler on line*, available at
`http://www.math.dartmouth.edu/edu/~euler/`

[8] V.S. Varadarajan, *Euler and his work on infinite Series*, Bull. Amer. Math. Soc., 44 (2007), 515—539.

# Olimpiada de Matematică a studenţilor din sud-estul Europei, SEEMOUS 2012

Cornel Băeţica şi Gabriel Mincu[1)]

**Abstract**. This note deals with the problems of the 6th South Eastern European Mathematical Olympiad for University Students, SEEMOUS 2012, organized by the Union of Bulgarian Mathematicians in Blagoevgrad, Bulgaria, between March 6 and March 11, 2012.

**Keywords:** Determinants, dominated convergence theorem, eigenvalues, Gamma function, Leibniz product rule.

**MSC:** 11C20, 15A18, 33D05, 40A30

Cea de-a şasea ediţie a Olimpiadei de Matematică a studenţilor din sud-estul Europei, SEEMOUS 2012, a fost organizată de Uniunea Matematicienilor din Bulgaria şi de Societatea de Matematică din Sud-Estul Europei în localitatea Blagoevgrad din Bulgaria, în perioada 6-11 martie 2012. Au participat 97 de studenţi de la universităţi din Bulgaria, Grecia, Macedonia, România, Turcia şi Ucraina.

Concursul a avut o singură probă constând în patru probleme. Prezentăm mai jos cele patru probleme însoţite de soluţii, unele dintre acestea fiind preluate din lucrările concurenţilor. Pentru soluţiile oficiale facem trimitere la `http://seemous2012.swu.bg`.

**Problema 1.** Fie matricea $A = (a_{ij})_{i,j} \in \mathcal{M}_n(\mathbb{Z})$, $a_{ij}$ fiind restul împărţirii la 3 a numărului $i^j + j^i$. Găsiţi valoarea maximă a lui $n \in \mathbb{N}^*$ pentru care $\det A \neq 0$.

**Volodimir Braiman**, Ucraina

*Aceasta a fost considerată de juriu drept o problemă uşoară. Majoritatea studenţi-lor care au rezolvat problema au procedat în spiritul primei soluţii pe care o prezentăm. Aceasta şi soluţia oficială.*

*Soluţia* 1. Notăm cu $m$ valoarea maximă cerută. Remarcăm că pentru orice $i, j \in \mathbb{N}^*$ avem $i^{j+2} \equiv i^j \pmod 3$ şi $(i+3)^j \equiv i^j \pmod 3$. Prin urmare, $(i+6)^j + j^{i+6} \equiv i^j + j^i \pmod 3$. Rezultă că în cazul $n \geq 7$ linia a şaptea a matricei $A$ coincide cu prima. Deducem că în acest caz $\det A = 0$, deci $m \leq 6$. Se constată prin calcul direct că pentru $n = 6$ avem $\det A = 0$, iar pentru $n = 5$ avem $\det A = 12 \neq 0$. În concluzie, $m = 5$. $\square$

*Soluţia* 2. Fie $n \geq 6$. Considerăm matricele $B = (b_{ij})_{i,j}, C = (c_{ij})_{i,j} \in \in \mathcal{M}_n(\mathbb{Z})$, unde $b_{ij}$, respectiv $c_{ij}$, sunt resturile împărţirii la 3 ale lui $i^j$, respectiv $j^i$. Evident, $A = B + C$. Notăm cu $c_k^M$ coloana $k$ a unei matrice arbitrare $M$. Este imediat (folosind observaţiile făcute în cadrul primei soluţii) că pentru orice $k \in \{1, 2, \ldots, n-2\}$ avem $c_{k+2}^B = c_k^B$ şi că pentru orice

[1)]University of Bucharest, Faculty of Mathematics and Informatics, Bucharest, Romania, `cornel.baetica@fmi.unibuc.ro`, `gamin@fmi.unibuc.ro`

$k \in \{1, 2, \dots, n-3\}$ avem $c^C_{k+3} = c^C_k$. Prin urmare, din orice trei coloane ale matricei $B$ cel puţin două coincid, iar din orice patru coloane ale matricei $C$ cel puţin două coincid. Pentru fiecare $1 \leq i_1 < i_2 < \dots < i_k \leq n$, desemnăm prin $B^{i_1, i_2, \dots, i_k}$ matricea obţinută din $B$ înlocuind coloanele $i_1, i_2, \dots, i_n$ cu cele corespunzătoare ale lui $C$. Folosind în mod repetat aditivitatea determinantului în raport cu coloanele sale, obţinem că

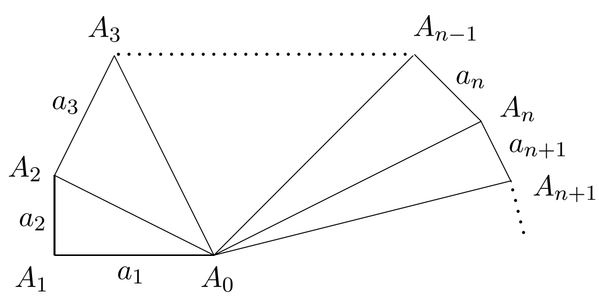
$$\det A = \det(B + C) = \det B + \sum_{k=1}^{n} \left( \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \det B^{i_1, i_2, \dots, i_k} \right).$$

Se constată că fiecare determinant din membrul drept al relaţiei anterioare are fie cel puţin trei coloane ale matricei $B$, fie cel puţin patru coloane ale matricei $C$. De aici rezultă că matricea $A$ are cel puţin două coloane egale, deci $\det A = 0$.

În consecinţă, $m \leq 5$. Pentru $n = 5$ se constată prin calcul direct că $\det A = 12 \neq 0$. În concluzie, $m = 5$. $\square$

(*Această soluţie a fost dată în concurs de către Theodor Munteanu.*)

**Problema 2.** Considerăm triunghiurile dreptunghice $\triangle A_0 A_n A_{n+1}$, $n \in \mathbb{N}^*$, cu $\mathrm{m}(\sphericalangle A_0 A_n A_{n+1}) = 90^0$ şi astfel încât pentru fiecare $n \geq 2$ dreapta $A_0 A_n$ să separe punctele $A_{n-1}$ şi $A_{n+1}$.

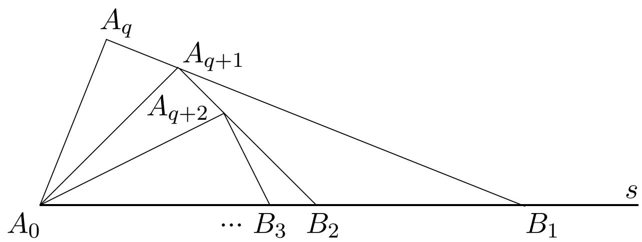



Este posibil ca şirul de puncte $(A_n)_{n \geq 1}$ să fie nemărginit, dar seria $\sum_{n \geq 1} \mathrm{m}(\sphericalangle A_0 A_n A_{n+1})$ să fie convergentă?

**Volodimir Braiman**, Ucraina

*Aceasta a fost considerată de juriu drept o problemă de dificultate medie. Studenţii care au rezolvat problema au procedat în spiritul uneia dintre cele două soluţii oficiale.*

*Soluţia* 1. Presupunem că seria din enunţ este convergentă. Există atunci $q \in \mathbb{N}^*$ astfel încât $\alpha \overset{\text{not}}{=} \sum_{n \geq q} m(\sphericalangle A_n A_0 A_{n+1}) < \frac{\pi}{2}$. În semiplanul determinat de dreapta $A_0 A_q$ şi punctul $A_{q+1}$ considerăm semidreapta $s$ cu originea $A_0$ care formează cu $[A_0A_q$ un unghi de măsură $\alpha$. Notăm cu $B_1$ intersecţia dintre $s$ şi $[A_qA_{q+1}$ şi arătăm inductiv că pentru orice $k \in \mathbb{N}^*$ semidreapta $[A_{q+k-1}A_{q+k}$ intersectează $s$ (într-un punct pe care îl notăm cu $B_k$).




Fie $k \in \mathbb{N}^*$. Presupunem construit $B_k$. Dreapta $A_0A_{q+k}$ separă atât $A_{q+k-1}$ şi $A_{q+k+1}$, cât şi $A_{q+k-1}$ şi $B_k$; prin urmare, ea nu separă $A_{q+k+1}$ şi $B_k$. Cum $\mathrm{m}(\sphericalangle A_{q+k}A_0A_{q+k+1}) < \mathrm{m}(\sphericalangle A_{q+k}A_0B_k)$, iar $\mathrm{m}(\sphericalangle A_0A_{q+k}B_k) > \dfrac{\pi}{2} = \mathrm{m}(\sphericalangle A_0A_{q+k}A_{q+k+1})$, rezultă $A_{q+k+1} \in \mathrm{Int}(\triangle A_0A_{q+k}B_k)$, deci $[A_{q+k}A_{q+k+1}$ şi $[A_0B_k] \subset s$ au un punct comun. Notând cu $B_{k+1}$ acest punct, încheiem pasul de inducţie. Din cele precedente se obţine pentru fiecare $k \in \mathbb{N}^*$ şi incluziunea $\mathrm{Int}(\triangle A_0A_{q+k+1}B_{k+1}) \subset \mathrm{Int}(\triangle A_0A_{q+k}B_k)$.

Folosind inductiv aceste relaţii, constatăm că pentru orice $k \geq 2$ avem $A_{q+k} \in \mathrm{Int}(\triangle A_0A_{q+k-1}B_{k-1}) \subset \mathrm{Int}(\triangle A_0A_qB_1)$, de unde deducem că şirul $(A_n)_{n\geq 1}$ este mărginit.

În concluzie, răspunsul la întrebarea problemei este negativ. $\square$

*Soluţia* 2. Notăm $a_n = A_{n-1}A_n$, $n \in \mathbb{N}^*$. Observăm că pentru orice $n \in \mathbb{N}^*$ avem $A_0A_n = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$, iar

$$\mathrm{m}(\sphericalangle A_nA_0A_{n+1}) = \mathrm{arctg}\frac{a_{n+1}}{\sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}}.$$

Notând $s_n = a_1^2 + a_2^2 + \cdots + a_n^2$, întrebarea problemei se poate reformula astfel: „Există şiruri strict crescătoare şi nemărginite $(s_n)_{n\geq 1}$ de numere pozitive pentru care seria $\sum\limits_{n\geq 1} \mathrm{arctg}\sqrt{\dfrac{s_{n+1} - s_n}{s_n}}$ este convergentă?“.

Presupunem că există un astfel de şir $(s_n)_{n\geq 1}$.

Cum $\sum\limits_{n\geq 1} \mathrm{arctg}\sqrt{\dfrac{s_{n+1} - s_n}{s_n}}$ este convergentă, rezultă că

$$\lim_{n\to\infty} \sqrt{\frac{s_{n+1} - s_n}{s_n}} = 0,$$

de unde $\lim_{n\to\infty} \dfrac{\operatorname{arctg}\sqrt{\dfrac{s_{n+1}-s_n}{s_n}}}{\sqrt{\dfrac{s_{n+1}-s_n}{s_n}}} = 1$, deci seria $\sum_{n\geq 1}\sqrt{\dfrac{s_{n+1}-s_n}{s_n}}$ este la rândul său convergentă. Notăm $t_n = \sqrt{\dfrac{s_{n+1}-s_n}{s_n}}$. Atunci, pentru orice $k \in \mathbb{N}^*$ avem $\dfrac{s_{k+1}}{s_k} = 1 + t_k^2$, deci $\ln s_{k+1} = \ln s_k + \ln(1+t_k^2)$. Adunând aceste relaţii pentru $k \in \{1, 2, \ldots, n-1\}$, obţinem

$$\ln s_n = \ln s_1 + \sum_{k=1}^{n-1} \ln(1+t_k^2). \tag{1}$$

Întrucât $\lim_{n\to\infty} t_n^2 = \left(\lim_{n\to\infty} t_n\right)^2 = 0$, avem $\lim_{n\to\infty} \dfrac{\ln(1+t_n^2)}{t_n^2} = 1$, deci seriile $\sum_{n\geq 1} \ln(1+t_n^2)$ şi $\sum_{n\geq 1} t_n^2$ au aceeaşi natură. Cum însă seria $\sum_{n\geq 1} t_n$ este convergentă şi $t_n > 0$ pentru orice $n \in \mathbb{N}^*$, rezultă că şi $\sum_{n\geq 1} t_n^2$ este serie convergentă. Prin urmare, $\sum_{n\geq 1} \ln(1+t_n^2)$ este convergentă. De aici şi din relaţia (1) deducem că şirul $(\ln s_n)_{n\geq 1}$ este mărginit, contradicţie. Prin urmare, răspunsul la întrebarea din enunţ este negativ. $\square$

**Problema 3.** a) Arătaţi că dacă numărul $k \in \mathbb{N}^*$ este par, iar $A \in \mathcal{M}_n(\mathbb{R})$ este o matrice simetrică cu proprietatea că $(\mathrm{tr}A^k)^{k+1} = (\mathrm{tr}A^{k+1})^k$, atunci $A^n = (\mathrm{tr}A)A^{n-1}$.

b) Rămâne afirmaţia de la a) adevărată pentru $k$ impar?

**Vasile Pop**, România

*Aceasta a fost considerată de juriu drept o problemă de dificultate medie. Concurenţii au dat mai multe soluţii, dar în linii mari s-a mers pe două idei: aducerea matricei A la forma diagonală sau folosirea teoremei Hamilton-Cayley.*

a) Notăm $k = 2t$, $t \in \mathbb{N}^*$. Matricea $A$ fiind simetrică, ea are toate valorile proprii reale. Notăm cu $\lambda_1, \lambda_2, \ldots, \lambda_n$ aceste valori. Relaţia dată se rescrie

$$(\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t})^{2t+1} = (\lambda_1^{2t+1} + \lambda_2^{2t+1} + \cdots + \lambda_n^{2t+1})^{2t}. \tag{2}$$

Dacă $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$, atunci polinomul caracteristic al lui $A$ este $X^n$, deci, conform teoremei Hamilton-Cayley, $A^n = 0 = (\mathrm{tr}A)A^{n-1}$.

Dacă măcar una dintre valorile proprii ale lui $A$ este nenulă, constatăm (împărţind prin $(\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t})^{2t+1}$ şi notând

$$\mu_j = \frac{\lambda_j}{(\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t})^{\frac{1}{2t}}}\ ,\ \ j \in \{1, 2, \ldots, n\}),$$

că relaţia (2) este echivalentă cu

$$1 = (\mu_1^{2t+1} + \mu_2^{2t+1} + \cdots + \mu_n^{2t+1})^{2t}. \tag{3}$$

Întrucât $\mu_1^{2t} + \mu_2^{2t} + \cdots + \mu_n^{2t} = 1$, avem $|\mu_j| \leq 1$, deci $\mu_j^{2t+1} \leq \mu_j^{2t}$, $j \in \{1, 2, \ldots, n\}$, cu egalitate dacă şi numai dacă $\mu_j \in \{0, 1\}$. Se obţine deci $1 = (\mu_1^{2t+1} + \mu_2^{2t+1} + \cdots + \mu_n^{2t+1})^{2t} \leq (\mu_1^{2t} + \mu_2^{2t} + \cdots + \mu_n^{2t})^{2t} = 1$, de unde deducem că $\mu_j^{2t+1} = \mu_j^{2t}$, deci $\mu_j \in \{0, 1\}$, pentru fiecare $j \in \{1, 2, \ldots, n\}$. Cum însă $\mu_1^{2t} + \mu_2^{2t} + \cdots + \mu_n^{2t} = 1$, rezultă că unul dintre numerele $\mu_j$ este 1, iar celelalte sunt nule.

În concluzie, după o eventuală renumerotare vom avea $\lambda_2 = \lambda_3 = \ldots = \lambda_n = 0$. Prin urmare polinomul caracteristic al lui $A$ este $X^n - \lambda_1 X^{n-1}$, de unde, conform teoremei Hamilton-Cayley, $A^n = \lambda_1 A^{n-1} = (\mathrm{tr}A)A^{n-1}$. $\square$

**Observaţii.** 1) Matricea $A$ fiind diagonalizabilă, faptul că ea are cel mult o valoare proprie nenulă conduce la un rezultat mai tare decât cel din enunţul problemei, anume $A^{s+1} = (\mathrm{tr}A)A^s$ pentru orice $s \in \mathbb{N}^*$.

2) Calcule similare celor prezentate mai sus se folosesc pentru a demonstra următorul rezultat: dacă $x_1, x_2, \ldots, x_n$ sunt numere reale nenegative iar $0 < p < q$, atunci $(x_1^p + x_2^p + \cdots + x_n^p)^{\frac{1}{p}} \geq (x_1^q + x_2^q + \cdots + x_n^q)^{\frac{1}{q}}$, egalitatea având loc dacă şi numai dacă cel mult unul dintre numerele $x_1, x_2, \ldots, x_n$ este nenul (a se vedea, de exemplu, [1, Theorem 19]).

Acest rezultat a apărut citat în lucrarea unui concurent grec şi utilizarea lui rezolvă imediat problema.

3) Am prezentat raţionamentul prin care am dedus din relaţia (2) faptul că avem cel mult o valoare $\lambda_j$ nenulă în forma în care este el întâlnit în texte standard. Laurian Filip a găsit în concurs următoarea manieră elegantă de a proba această implicaţie: dacă are loc relaţia (2), atunci fie $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$, fie cel puţin una dintre aceste valori este nenulă. În această ultimă situaţie vom considera, după o eventuală renumerotare, că $|\lambda_1| \geq |\lambda_j|$ pentru orice $j \in \{1, 2, \ldots, n\}$. Obţinem

$$(\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t})^{2t+1} = (\lambda_1^{2t+1} + \lambda_2^{2t+1} + \cdots + \lambda_n^{2t+1})^{2t} \leq$$

$$\leq (|\lambda_1|^{2t+1} + |\lambda|_2^{2t+1} + \cdots + |\lambda_n|^{2t+1})^{2t} \leq \lambda_1^{2t}(\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t})^{2t}.$$

De aici rezultă $\lambda_1^{2t} + \lambda_2^{2t} + \cdots + \lambda_n^{2t} \leq \lambda_1^{2t}$, de unde $\lambda_2 = \lambda_3 = \ldots = \lambda_n = 0$.

Remarcăm că putem folosi un raţionament similar pentru demonstrarea cazului de egalitate al inegalităţii menţionate în observaţia 2.

b) Dacă luăm $k = 1$, $n = 3$ şi $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{2} \end{pmatrix}$, avem

$(\mathrm{tr}A)^2 = \dfrac{9}{4} = \mathrm{tr}A^2$, dar $A^3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\frac{1}{8} \end{pmatrix} \neq \dfrac{3}{2}\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{4} \end{pmatrix} = (\mathrm{tr}A)A^2$.

Prin urmare, afirmaţia de la punctul a) al problemei nu rămâne valabilă pentru $k$ impar. □

**Observaţii.** 1) Putem găsi contraexemple de tipul celui din soluţia punctului b) pentru orice $k = 2t+1$, $t \in \mathbb{N}$, astfel: se consideră funcţia $f : \mathbb{R} \to \mathbb{R}$, $f(x) = (2x^{2t+1}-1)^{2t+2} - (2x^{2t+2}+1)^{2t+1}$ şi se vede că $f(1) < 0$ şi $\lim\limits_{x\to\infty} f(x) = \infty$. Prin urmare, ecuaţia $(2x^{2t+1}-1)^{2t+2} - (2x^{2t+2}+1)^{2t+1} = 0$ are cel puţin o rădăcină în intervalul $(1,\infty)$. Notăm cu $\lambda$ o astfel de rădăcină. Atunci, pentru matricea

$$A = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

avem $(\mathrm{tr}A^{2t+1})^{2t+2} = (2\lambda^{2t+1}-1)^{2t+2} = (2\lambda^{2t+2}+1)^{2t+1} = (\mathrm{tr}A^{2t+2})^{2t+1}$. Dar

$$A^n = \begin{pmatrix} \lambda^n & 0 & 0 \\ 0 & \lambda^n & 0 \\ 0 & 0 & (-1)^n \end{pmatrix}$$

iar

$$(\mathrm{tr}A)A^{n-1} = (2\lambda-1)\begin{pmatrix} \lambda^{n-1} & 0 & 0 \\ 0 & \lambda^{n-1} & 0 \\ 0 & 0 & (-1)^{n-1} \end{pmatrix},$$

deci $A^n \neq (\mathrm{tr}A)A^{n-1}$.

2) Lăsăm ca exerciţiu cititorului faptul că pentru $n = 2$ nu putem găsi contraexemple la afirmaţia de la punctul a).

**Problema 4.** a) Calculaţi $\lim\limits_{n\to\infty} n \displaystyle\int_0^1 \left(\frac{1-x}{1+x}\right)^n \mathrm{d}x$.

b) Calculaţi $\lim\limits_{n\to\infty} n^{k+1} \displaystyle\int_0^1 \left(\frac{1-x}{1+x}\right)^n x^k \mathrm{d}x$, unde $k \in \mathbb{N}$, $k \geq 1$.

**Ovidiu Furdui**, România

*Aceasta a fost considerată de juriu drept o problemă dificilă. Aprecierea s-a dovedit a fi corectă, doar un singur concurent obţinând punctajul maxim. Soluţia acestuia, diferită de cea oficială, a primit premiul special al juriului.*

*Soluţie.* a) Facem schimbarea de variabilă $x = \dfrac{1-t}{1+t}$, $t \in [0,1]$ şi obţinem

$$\lim_{n\to\infty} n \int_0^1 \left(\frac{1-x}{1+x}\right)^n \mathrm{d}x = 2 \lim_{n\to\infty} n \int_0^1 \frac{t^n}{(1+t)^2}\mathrm{d}t.$$

Integrând prin părţi, membrul drept al acestei relaţii devine

$$\frac{1}{2} + 4 \lim_{n\to\infty} \int_0^1 \frac{t^{n+1}}{(1+t)^3}\mathrm{d}t.$$

Cum pentru orice $t \in [0,1]$ au loc relaţiile $0 \le \dfrac{t^{n+1}}{(1+t)^3} \le t^{n+1}$, obţinem $0 \le \displaystyle\int_0^1 \frac{t^{n+1}}{(1+t)^3} \le \frac{1}{n+2}$, deci $\displaystyle\lim_{n\to\infty} \int_0^1 \frac{t^{n+1}}{(1+t)^3}\mathrm{d}t = 0$, iar

$$\lim_{n\to\infty} n \int_0^1 \left(\frac{1-x}{1+x}\right)^n \mathrm{d}x = \frac{1}{2}.$$

b) *Soluţia* 1. Folosind schimbarea de variabilă de la punctul a), obţinem

$$\lim_{n\to\infty} n^{k+1} \int_0^1 \left(\frac{1-x}{1+x}\right)^n x^k \mathrm{d}x = 2 \lim_{n\to\infty} n^{k+1} \int_0^1 t^n \frac{(1-t)^k}{(1+t)^{k+2}}\mathrm{d}t.$$

Definim $\varphi : [0,1] \to \mathbb{R}$, $\varphi(t) = \frac{(1-t)^k}{(1+t)^{k+2}}$. Limita cerută este deci egală cu

$$2 \lim_{n\to\infty} n^{k+1} \int_0^1 t^n \varphi(t)\mathrm{d}t.$$

Folosind formula lui Leibniz referitoare la calculul derivatelor unui produs de funcţii derivabile, obţinem că $\varphi^{(j)}(1) = 0$ pentru $0 \le j < k$ şi $\varphi^{(k)}(1) = \dfrac{(-1)^k k!}{2^{k+2}}$.

Integrând în mod repetat prin părţi, constatăm că

$$n^{k+1} \int_0^1 t^n \varphi(t)\mathrm{d}t = -\frac{n^{k+1}}{n+1} \int_0^1 t^{n+1}\varphi'(t)\mathrm{d}t = \frac{n^{k+1}}{(n+1)(n+2)} \int_0^1 t^{n+2}\varphi''(t)\mathrm{d}t =$$

$$= \ldots = \frac{(-1)^k n^{k+1}}{(n+1)(n+2)\cdots(n+k)} \int_0^1 t^{n+k}\varphi^{(k)}(t)\mathrm{d}t =$$

$$= \frac{(-1)^k n^{k+1}}{(n+1)(n+2)\cdots(n+k+1)} \left( t^{n+k+1}\varphi^{(k)}(t)\Big|_0^1 - \int_0^1 t^{n+k+1}\varphi^{(k+1)}(t)\mathrm{d}t \right).$$

Dar $\varphi^{(k+1)}$ este continuă pe $[0,1]$, deci există $M > 0$ astfel încât $|\varphi^{(k+1)}(t)| \le M$ pentru orice $t \in [0,1]$. Rezultă că

$$0 \le \left| \int_0^1 t^{n+k+1}\varphi^{(k+1)}(t)\mathrm{d}t \right| \le M \int_0^1 t^{n+k+1}\mathrm{d}t = \frac{M}{n+k+2},$$

de unde deducem că $\lim\limits_{n\to\infty} \int_0^1 t^{n+k+1}\varphi^{(k+1)}(t)\mathrm{d}t = 0$. În consecinţă

$$\lim_{n\to\infty} n^{k+1} \int_0^1 \left(\frac{1-x}{1+x}\right)^n x^k \mathrm{d}x = 2(-1)^k\varphi^{(k)}(1) = \frac{k!}{2^{k+1}}.$$

b) *Soluţia* 2. Aplicând schimbarea de variabilă $x = \frac{t}{n}$, $t \in [0,n]$, obţinem

$$\lim_{n\to\infty} n^{k+1} \int_0^1 \left(\frac{1-x}{1+x}\right)^n x^k \mathrm{d}x = \lim_{n\to\infty} \int_0^n \left(\frac{n-t}{n+t}\right)^n t^k \mathrm{d}t =$$

$$= \lim_{n\to\infty} \int_0^\infty \left(\frac{n-t}{n+t}\right)^n t^k \chi_{[0,n]}(t)\mathrm{d}t.$$

Pentru orice $t \ge 0$ au loc relaţiile

$$\left| \left(\frac{n-t}{n+t}\right)^n t^k \chi_{[0,n]}(t) \right| = \left| \left(1 - \frac{2t}{n+t}\right)^n t^k \chi_{[0,n]}(t) \right| \le$$

$$\le t^k e^{-\frac{2nt}{n+t}} \chi_{[0,n]}(t) \le t^k e^{-t}.$$

Cum funcţia $t \mapsto t^k e^{-t}$ este integrabilă Lebesgue pe $[0,\infty)$, putem aplica teorema de convergenţă dominată. Deducem că

$$\lim_{n\to\infty} \int_0^\infty \left(\frac{n-t}{n+t}\right)^n t^k \chi_{[0,n]}(t)\mathrm{d}t = \int_0^\infty \lim_{n\to\infty} \left[ \left(\frac{n-t}{n+t}\right)^n t^k \chi_{[0,n]}(t) \right] \mathrm{d}t =$$

$$= \int_0^\infty t^k e^{-2t}\mathrm{d}t = \frac{1}{2^{k+1}} \int_0^\infty u^k e^{-u}\mathrm{d}u = \frac{\Gamma(k+1)}{2^{k+1}} = \frac{k!}{2^{k+1}}.$$

(*Această soluţie a fost dată în concurs de către Konstantinos Tsouvalas din Grecia.*)

References

[1] G. H. Hardy, J. E. Littlewood, G. Pólya, *Inequalities*, Cambridge University Press, 1934.


# NOTE MATEMATICE

## Linear Recursive Sequences in Arbitrary Characteristics

Constantin-Nicolae Beli[1]

**Abstract**. In this note we obtain a new formula for the general term of a linearly recursive sequence which holds regardless of the characteristic of the field.

**Keywords:** Fields with positive characteristic, linear recurrences, sequences.

**MSC:** 65Q30, 14G17

The sequences satisfying linear recurrences have been studied for a long time. There is a well known formula for the general term of these sequences and it involves the roots of the characteristic polynomial and their multiplicities. We usually assume that these are sequences of real or complex numbers but the theory works for arbitrary fields of characteristic zero. However, when the characteristic is $p > 0$ and the characteristic polynomial has a root with multiplicity greater than $p$, the general formula no longer works.

Let $K$ be an algebraically closed field,

$$f = X^k + a_{k-1}X^{k-1} + \cdots + a_0 \in K[X]$$

with $a_0 \neq 0$, and let $\alpha_1, \ldots, \alpha_s$ be the roots of $f$ with multiplicities $k_1, \ldots, k_s$.

We want to determine all sequences $(x_n)_{n\geq 0}$ with $x_n \in K$ satisfying the linear recurrence of rank $k$

$$x_{n+k} + a_{k-1}x_{n+k-1} + \cdots + a_0 x_n = 0 \ \forall n \geq 0.$$

This problem and its solution are well known when $K = \mathbb{C}$. Namely, the sequences satisfying the recurrence above are precisely the linear combinations of the sequences $\left(n^j \alpha_i^n\right)_{n\geq 0}$ with $1 \leq i \leq s$ and $0 \leq j \leq k_i - 1$.

This answer holds for arbitrary fields of characteristic 0 and in many cases (e.g. when all the roots are simple) in positive characteristics but not when $\operatorname{char} K = p$ and there is a multiplicity $k_i \geq p + 1$. In a field $K$ of positive characteristic $p$ we have $n^p = n$ for any integer $n$, so $n^{p+1} = n^2$, $n^{p+2} = n^3$, and so on. Therefore the sequence $(n\alpha_i^n)_{n\geq 0}$ coincides with $(n^p \alpha_i^n)_{n\geq 0}$, $\left(n^2 \alpha_i^n\right)_{n\geq 0}$ with $\left(n^{p+1}\alpha_i^n\right)_{n\geq 0}$, and so on.

[1]Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania

In this note we give another basis for the space of sequences satisfying a linear recurrence which works regardless of characteristic. Namely, we prove that such a basis is made of

$$\left(\binom{n}{j}\alpha_i^n\right)_{n\geq 0}$$

with $1 \leq i \leq s$ and $0 \leq j \leq k_i - 1$. This result is not essentially new. It is the subject of [1], a PhD thesis from 1967. The author uses a different method and restricts himself to the case when $K$ is a finite field. In a footnote he mentions that the result can be extended to arbitrary fields of positive characteristic.

We denote $V := \{(x_n)_{n\geq 0} : x_n \in K\ \forall n \geq 0\}$. Then $V$ is a $K$-vector space.

On $V$ we define the linear operator $T$ given by $(x_n)_{n\geq 0} \mapsto (x_{n+1})_{n\geq 0}$. Then for any integer $k \geq 0$ the operator $T^k$ is given by $(x_n)_{n\geq 0} \mapsto (x_{n+k})_{n\geq 0}$. (When $k = 0$ $T^0 := 1_V$, the identity on $V$.)

**Lemma 1.** *If $f = a_kX^k + \cdots + a_0 \in K[X]$, then $f(T)$ is given by*

$$(x_n)_{n\geq 0} \mapsto (a_kx_{n+k} + \cdots + a_0x_n)_{n\geq 0}.$$

*Proof.* Let $x = (x_n)_{n\geq 0} \in V$. If $i \geq 0$ then $T^i(x) = (x_{n+i})_{n\geq 0}$. Hence

$$f(T)(x) = \left(\sum_{i=0}^{k} a_iT^i\right)(x) = \sum_{i=0}^{k} a_i(x_{n+i})_{n\geq 0} = \left(\sum_{i=0}^{k} a_ix_{n+i}\right)_{n\geq 0},$$

as claimed. □

We denote $V_f := \ker f(T)$. Then our problem can be restated:

*Find a basis for $V_f$, where $f = X^k + a_{k-1}X^{k-1} + \cdots + a_0 \in K[X]$.*

**Remark 2.** If $f$ is a monic polynomial of degree $k$, as above, then the sequences from $V_f$ satisfy a linear recurrence of order $k$, so they are uniquely defined by the first $k$ elements. In other words, the mapping $(x_n)_{n\geq 0} \mapsto$ $\mapsto (x_0, \ldots, x_{k-1})$ is an isomorphism of vector spaces from $V_f$ to $K^k$. It follows that $\dim V_f = k = \deg f$.

**Remark 3.** If $g \mid f$, then $V_g \subseteq V_f$.

*Proof.* Let $f = gh$. For any $x \in V_g$ we have $f(T)(x) = gh(T)(x) =$ $= h(T)(g(T)(x)) = h(T)(0) = 0$ so $x \in V_f$. Thus $V_g \subseteq V_f$. □

**Lemma 4.** *Let $f, g \in K[X]$ with $(f, g) = 1$. Then $V_{fg} = V_f \oplus V_g$.*

*Proof.* Since $(f, g) = 1$ there are $P, Q \in K[X]$ such that $Pf + Qg = 1$. For any $x \in V_{fg}$ we have $x = 1_V(x) = (Pf + Qg)(T)(x) = Pf(T)(x) + Qg(T)(x)$. But $f(T)(Qg(T)(x)) = Q(T)(fg(T)(x)) = Q(T)(0) = 0$, so $Qg(T)(x) \in V_f$. Similarly $Pf(T)(x) \in V_g$ and so $x \in V_f + V_g$. Thus $V_{fg} \subseteq V_f + V_g$. The reverse inclusion follows from Remark 3 (we have $V_f, V_g \subseteq V_{fg}$), so $V_{fg} = V_f + V_g$. Since also by Remark 2 $\dim V_f + \dim V_g = \deg f + \deg g = \deg fg = \dim V_{fg}$, we have $V_f \cap V_g = \{0\}$, and therefore $V_{fg} = V_f \oplus V_g$.

(Alternatively, if $x \in V_f \cap V_g$ then $f(T)(x) = g(T)(x) = 0$, so $Pf(T)(x) = = Qg(T)(x) = 0$, which implies $x = Pf(T)(x) + Qg(T)(x) = 0$.) $\square$

By induction one gets:

**Corollary 5.** *If $f_1, \dots, f_s \in K[X]$ are pairwise coprime, then*

$$V_{f_1 \cdots f_s} = V_{f_1} \oplus \cdots \oplus V_{f_s}.$$

**Lemma 6.** *For any $k \geq 1$ the sequences $x^j = \left(\binom{n}{j}\right)_{n\geq 0}$ with $0 \leq j \leq k-1$ are a basis for $V_{(X-1)^k}$.*

*Proof.* For any $x = (x_n)_{n\geq 0} \in V$ we have $(T-1)(x) = (x_{n+1} - x_n)_{n\geq 0}$. We have $x^0 = \left(\binom{n}{0}\right)_{n\geq 0} = (1)_{n\geq 0}$, so $x^0 \neq 0$ and $(T-1)(x^0) = (1-1)_{n\geq 0} = 0$. If $j \geq 1$ then $(T-1)(x^j) = \left(\binom{n+1}{j} - \binom{n}{j}\right)_{n\geq 0} = \left(\binom{n}{j-1}\right)_{n\geq 0} = x^{j-1}$. These imply that $(T-1)^l(x^j) = x^{j-l}$ for $j \geq l \geq 1$ and $(T-1)^{j+1}(x^j) = 0$.

We now prove our statement by induction on $k$. If $k = 1$ then $x^0 \neq 0$ and $(T-1)(x^0) = 0$, so $x^0 \in V_{X-1}$. But by Remark 2 $\dim V_{X-1} = 1$, so $x^0$ is a basis for $V_{X-1}$. Let now $k > 1$. We have $(T-1)^{k-1}(x^{k-1}) = x^0 \neq 0$ and $(T-1)^k(x^{k-1}) = 0$ (see above), so $x^{k-1} \in V_{(X-1)^k} \setminus V_{(X-1)^{k-1}}$. But by Remark 3 $V_{(X-1)^{k-1}} \subseteq V_{(X-1)^k}$ and by Remark 2 $\dim V_{(X-1)^k} = k = = \dim V_{(X-1)^{k-1}} + 1$. These imply $V_{(X-1)^k} = V_{(X-1)^{k-1}} \oplus Kx^{k-1}$. By the induction hypothesis $x^0, \dots, x^{k-2}$ is a basis for $V_{(X-1)^{k-1}}$, so $x^0, \dots, x^{k-1}$ is a basis for $V_{(X-1)^k} = V_{(X-1)^{k-1}} \oplus Kx^{k-1}$. $\square$

**Lemma 7.** *Let $\alpha \in K^*$. If $f = \sum_{i=0}^{k} a_i X^i \in K[X]$ and $g = \alpha^k f(\alpha^{-1}X) = = \sum_{i=0}^{k} a_i \alpha^{k-i} X^i$, then $\phi_\alpha : V \to V$ given by $(x_n)_{n\geq 0} \mapsto (x_n \alpha^n)_{n\geq 0}$ defines an isomorphism between $V_f$ and $V_g$.*

*Proof.* Notice that $\phi_\alpha \in \mathrm{Aut}(V)$, $\phi_\alpha^{-1} = \phi_{\alpha^{-1}}$. The mapping $\phi_\alpha T \phi_\alpha^{-1}$ is given by $(x_n)_{n\geq 0} \mapsto (x_{n+1}\alpha^{-1})_{n\geq 0}$ so we have $\phi_\alpha T \phi_\alpha^{-1} = \alpha^{-1}T$. Therefore $\phi_\alpha f(T) \phi_\alpha^{-1} = \sum_{i=1}^{k} a_i \phi_\alpha T^i \phi_\alpha^{-1} = \sum_{i=0}^{k} a_i (\alpha^{-1}T)^i = f(\alpha^{-1}T)$. It follows that $g(T) = \alpha^k \phi_\alpha f(T) \phi_\alpha^{-1}$, which implies $\ker g(T) = \ker(\phi_\alpha f(T) \phi_\alpha^{-1}) = = \phi_\alpha(\ker f(T))$, i.e. $V_g = \phi_\alpha(V_f)$. $\square$

**Corollary 8.** *If $\alpha \in K^*$ and $k \geq 1$ then* $\left(\binom{n}{j}\alpha^n\right)_{n\geq 0}$ *with* $0 \leq j \leq k-1$ *are a basis for* $V_{(X-\alpha)^k}$.

*Proof.* We apply Lemma 7 to $f = (X-1)^k$. We have $g = \alpha^k f(X/\alpha) = (X-\alpha)^k$. Then $\phi_\alpha$ is an isomorphism between $V_f$ and $V_g$. By Lemma 6 $x^0, \dots, x^{k-1}$ is a basis for $V_f$, so $\phi_\alpha(x^0), \dots, \phi_\alpha(x^{k-1})$ is a basis for $V_g$. But $\phi_\alpha(x^j) = \phi_\alpha\left(\left(\binom{n}{j}\right)_{n\geq 0}\right) = \left(\binom{n}{j}\alpha^n\right)_{n\geq 0}$. Hence the conclusion. □

We are now in a position to state and prove the main result.

**Theorem.** *Let $f = X^k + a_{k-1}X^{k-1} + \dots + a_0 \in K[X]$ with $a_0 \neq 0$ and let $\alpha_1, \dots, \alpha_s$ be the roots of $f$ with multiplicities $k_1, \dots, k_s$. Then the sequences*

$$\left(\binom{n}{j}\alpha_i^n\right)_{n\geq 0}$$

*with $1 \leq i \leq s$ and $0 \leq j \leq k_i - 1$ are a basis for the space $V_f$ of all sequences $(x_n)_{n\geq 0}$ satisfying the recurrence relation*

$$x_{n+k} + a_{k-1}x_{n+k-1} + \dots + a_0 x_n = 0 \ \forall n \geq 0.$$

*Proof.* We have $f = (X-\alpha_1)^{k_1} \cdots (X-\alpha_s)^{k_s}$. By Corollary 5 we have

$$V_f = V_{(X-\alpha_1)^{k_1}} \oplus \dots \oplus V_{(X-\alpha_s)^{k_s}}.$$

By Corollary 8 for $1 \leq i \leq s$ the set

$$\left\{\left(\binom{n}{j}\alpha_i^n\right)_{n\geq 0} : 0 \leq j \leq k_i - 1\right\}$$

is a basis for $V_{(X-\alpha_i)^{k_i}}$. By putting together these bases we obtain the basis

$$\left\{\left(\binom{n}{j}\alpha_i^n\right)_{n\geq 0} : 1 \leq i \leq s,\ 0 \leq j \leq k_i - 1\right\}$$

for $V_f$. □

**Note.** The powers $n^j$ which appear in the solution when the characteristic is 0 are replaced by the binomial coefficients $\binom{n}{j}$. While $1, \dots, X^{k-1}$ are a $\mathbb{Z}$-basis for $\{P \in \mathbb{Z}[X] : \deg P < k\}$, the polynomials $\binom{X}{0}, \dots, \binom{X}{k-1}$ are a $\mathbb{Z}$-basis for $\{P \in \mathbb{Q}[X] : P(\mathbb{Z}) \subseteq \mathbb{Z},\ \deg P < k\}$.

## REFERENCES

[1] R.J. McEliece, *Linear recurring sequences over finite fields*, PhD thesis, California Institute of Technology (1967). Available at
http://thesis.library.caltech.edu/3856/1/McEliece_rj_1967.pdf

# Effective Error Bounds

GEORGE STOICA[1)]

**Abstract**. Using the error estimates in the Moivre-Laplace approximation of the binomial distribution, we obtain effective error bounds for the binomial coefficients.

**Keywords:** Binomial coefficients, Moivre-Laplace approximation.
**MSC:** 97H30

Given an even natural number $n$, it is easy to deduce using Stirling's formula, that

$$2^{-n}\binom{n}{n/2} \sim \frac{1}{\sqrt{\pi n/2}}, \tag{1}$$

where the sign $\sim$ is used to indicate that the ratio of the two sides tends to 1 as $n \to \infty$ (see [1], Chapter II, section 9).

Using the following double inequality

$$\sqrt{2\pi}n^{n+1/2}\mathrm{e}^{-n}\mathrm{e}^{(12n+1)^{-1}} < n! < \sqrt{2\pi}n^{n+1/2}\mathrm{e}^{-n}\mathrm{e}^{(12n)^{-1}}$$

valid for any $n \geq 1$ (not necessarily even), one obtains the error estimate in (1):

$$\exp\left(\frac{-9n-1}{3n(12n+1)}\right)\frac{1}{\sqrt{\pi n/2}} \leq 2^{-n}\binom{n}{n/2} \leq \frac{1}{\sqrt{\pi n/2}}\exp\left(\frac{-18n+1}{12n(6n+1)}\right). \tag{2}$$

The purpose of this note is to obtain a double inequality similar to (2), in which $\binom{n}{n/2}$ is replaced by $\binom{n}{k}$, and that holds true within a certain range of values $k \in \{0, 1, \ldots, n\}$ around the center $\frac{n}{2}$.

Let us start with the following result (in which one no longer assumes that $n$ is even).

**Proposition.** *There exist universal constants $C_1, C_2 > 0$ with the following property: if $a \geq 0$ and $(a_n)_{n\geq 1}$ is a sequence of real numbers such that $a_n \searrow 0$ as $n \to \infty$ then, for any $n \geq 1$ and $k \in \{0, 1, \ldots, n\}$ satisfying*

$$\sqrt{an\log n} \leq \left|k - \frac{n}{2}\right| \leq a_n n^{2/3}, \tag{3}$$

[1)] University of New Brunswick, Saint John, Canada

*one has*

$$\frac{C_1}{\sqrt{n}}\exp(-2a_n^2 n^{1/3}) \leq 2^{-n}\binom{n}{k} \leq \frac{C_2}{n^{2a+1/2}}. \tag{4}$$

*Proof.* We shall use the error estimate in the classical Moivre-Laplace approximation of the binomial distribution (see [1], Chapter VII, section 3, or [2], pg. 36), namely: under the assumption $\left|k - \frac{n}{2}\right| \leq a_n n^{2/3}$ we have

$$2^{-n}\binom{n}{k} = \frac{1+\varepsilon_n(k)}{\sqrt{\pi n/2}}\exp\left(-\frac{2(k-n/2)^2}{n}\right), \tag{5}$$

where

$$\lim_{n\to\infty} \sup_{|k-n/2|\leq a_n n^{2/3}} |\varepsilon_n(k)| = 0. \tag{6}$$

It follows that for all $n \geq 1$ and all $k$ satisfying $\left|k - \frac{n}{2}\right| \leq a_n n^{2/3}$, one has

$$\frac{C_1}{\sqrt{n}}\exp\left(-\frac{2\left(k-\frac{n}{2}\right)^2}{n}\right) \leq 2^{-n}\binom{n}{k} \leq \frac{C_2}{\sqrt{n}}\exp\left(-\frac{2\left(k-\frac{n}{2}\right)^2}{n}\right) \tag{7}$$

for some $C_1, C_2 > 0$ independent of $n$ (due to the uniform limit in (6)).

As $\left|k - \frac{n}{2}\right| \leq a_n n^{2/3}$ , the left-hand side inequality in (7) is greater than or equal to

$$\frac{C_1}{\sqrt{n}}\exp(-2a_n^2 n^{1/3}).$$

On the other hand, as $\sqrt{an\log n} \leq \left|k - \frac{n}{2}\right|$, the right-hand side inequality in (7) is smaller than or equal to

$$\frac{C_2}{\sqrt{n}}\exp\left(-2a\log n\right) = \frac{C_2}{n^{2a+1/2}},$$

and the proof is complete.

For instance, choosing $a_n = \sqrt{b\log n}\cdot n^{-1/6}$ for some $b \geq 0$, one obtains from (3) and (4) the following effective error bounds, similar to (2):

**Corollary.** *There exist universal constants $C_1, C_2 > 0$ with the following property: if $n \geq 1$ and $k \in \{0, 1, \ldots, n\}$ satisfying*

$$\sqrt{an\log n} \leq \left|k - \frac{n}{2}\right| \leq \sqrt{bn\log n}$$

*for some $b \geq a \geq 0$, then*

$$\frac{C_1}{n^{2b+1/2}} \leq 2^{-n}\binom{n}{k} \leq \frac{C_2}{n^{2a+1/2}}.$$

**Remark.** Note that, from (5) and (6), it follows that both $C_1$ and $C_2$ are very close to $\sqrt{\frac{2}{\pi}}$ as $n \to \infty$.

## References

[1] W. Feller, *An introduction to probability theory and its applications*, Vol. 1, 3rd ed., John Wiley, New York, 1971.
[2] E. Lesigne, *Pile ou face: une introduction au calcul des probabilités*, Ellipse, Paris, 2001.

# Determinanţi Gram şi minime integrale

VASILE POP[1)]

**Abstract**. This note shows how to use the Gram determinant in order to find the minimum value of some integrals.
**Keywords:** Gram determinant.
**MSC:** 11C20

Deoarece la concursurile pentru studenţi apar numeroase probleme legate de determinarea minimelor unor integrale, pe lângă un rezultat teoretic clasic prezentăm câteva probleme semnificative care ajută la înţelegerea noţiunilor şi la pregătirea pentru concursuri.

Pentru notaţiile şi definiţiile noţiunilor folosite în această notă recomandăm [1].

**Teorema 1.** *Fie $(V, \langle\cdot,\cdot\rangle)$ un spaţiu euclidian de dimensiune finită, $x \in V$, $V_1 \subset V$ subspaţiu, $x_1 \in V_1$ proiecţia ortogonală a lui $x$ pe $V_1$ şi $x_1^\perp$ componenta ortogonală a lui $x$ relativă la subspaţiul $V_1$.*

*Atunci distanţa de la $x$ la $V_1$ este*

$$d(x, V_1) = \|x_1^\perp\| = \sqrt{\frac{G(v_1, \ldots, v_k, x)}{G(v_1, \ldots, v_k)}},$$

*unde $\{v_1, \ldots, v_k\}$ este o bază în $V_1$ iar*

$$G(v_1, \ldots, v_k) = \det[\langle v_i, v_j\rangle]_{i,j=\overline{1,k}}$$

*este determinantul Gram al vectorilor $v_1, v_2, \ldots, v_k$.*

*Demonstraţie.* Pentru a arăta că $d(x, V_1) = d(x, x_1)$ este suficient să arătăm că $\|x - y_1\| \geq \|x - x_1\|$ pentru orice $y_1 \in V_1$. Aceasta rezultă imediat din relaţia $\|x - y_1\|^2 = \|x_1 - y_1\|^2 + \|x_1^\perp\|^2$, deci

$$d(x, V_1) = \|x - x_1\| = \|x_1^\perp\|.$$

[1)] Technical University of Cluj-Napoca, Cluj-Napoca, Romania.

Dacă $x \in V_1$, atunci este evident că $x = x_1$ şi distanţa este zero. Dacă $x \notin V_1$, atunci vectorii $v_1, \ldots, v_k, x$ sunt liniar independenţi şi prin ortogonalizare Gram-Schmidt se transformă în vectorii ortogonali $e_1, \ldots, e_k, e_{k+1}$, unde $e_1, \ldots, e_k$ formează tot o bază în $V_1$ iar

$$e_{k+1} \perp V_1,\ e_{k+1} = x - \sum_{i=1}^{k} \frac{\langle x, e_i\rangle}{\langle e_i, e_i\rangle} e_i,$$

deci

$$x_1 = \sum_{i=1}^{k} \frac{\langle x, e_i\rangle}{\langle e_i, e_i\rangle} e_i \text{ şi } x_1^{\perp} = e_{k+1}.$$

Pe de altă parte se arată uşor că

$$G(v_1, \ldots, v_k) = G(e_1, \ldots, e_k) = \|e_1\|^2 \cdot \ldots \cdot \|e_k\|^2,$$

$$G(v_1, \ldots, v_k, x) = G(e_1, \ldots, e_k, e_{k+1}) = \|e_1\|^2 \cdot \ldots \cdot \|e_k\|^2 \cdot \|e_{k+1}\|^2$$

şi atunci $\|x_1^{\perp}\| = \|e_{k+1}\| = \sqrt{\dfrac{G(v_1, \ldots, v_k, x)}{G(v_1, \ldots, v_k)}}$. □

**Observaţia 2.** Din Teorema 1 se obţin în spaţiile euclidiene $\mathbb{R}^2$ şi $\mathbb{R}^3$ distanţele de la un punct la o dreaptă $D$ sau la un plan $P$:

$$d(\overline{x}, D) = \frac{\|\overline{x} \times \overline{d}\|}{\|\overline{d}\|},$$

unde $\overline{d} \neq \overline{0}$ este vector director al dreptei $D$, respectiv

$$d(\overline{x}, P) = \frac{|(\overline{x}, \overline{d}_1, \overline{d}_2)|}{\|\overline{d}_1 \times \overline{d}_2\|},$$

unde $\overline{d}_1, \overline{d}_2$ sunt vectori necoliniari din planul $P$ iar $(\overline{x}_1, \overline{d}_1, \overline{d}_2) = \overline{x} \cdot (\overline{d}_1 \times \overline{d}_2)$ reprezintă produsul mixt al vectorilor $\overline{x}, \overline{d}_1, \overline{d}_2$.

(În general avem $\|\overline{v}_1 \times \overline{v}_2\|^2 = G(v_1, v_2)$ şi $(\overline{v}_1, \overline{v}_2, \overline{v}_3)^2 = G(\overline{v}_1, \overline{v}_2, \overline{v}_3)$.)

În cele ce urmează vom nota cu $C([a,b])$ spaţiul euclidian al funcţiilor reale continue definite pe intervalul $[a,b]$ cu produsul scalar

$$\langle f, g\rangle = \int_a^b f(x)g(x)\mathrm{d}x.$$

**Problema 3.** Să se determine valoarea minimă a integralei

$$\int_0^{2\pi} (a_1 + a_2 \cos x + \cdots + a_n \cos^n x + \cos^{n+1} x)^2 \mathrm{d}x,\ \text{pentru } a_1, a_2, \ldots, a_n \in \mathbb{R}.$$

*Soluţie.* Considerăm spaţiul euclidian $C([0,2\pi])$. Distanţa între două funcţii $f$ şi $g$ este

$$d(f,g) = \|f-g\| = \sqrt{\int_0^{2\pi} (f(x)-g(x))^2 \mathrm{d}x}.$$

Luăm $f(x) = \cos^{n+1} x$ şi atunci funcţia de minimizat este

$$\phi(g) = d^2(f,g),$$

cu

$$g(x) = -(a_1 + a_2 \cos x + \cdots + a_n \cos^n x), \quad a_1, a_2, \ldots, a_n \in \mathbb{R}.$$

Mulţimea funcţiilor $g$ formează subspaţiul

$$V_1 = \mathrm{Span}\{1, \cos x, \cos^2 x, \ldots, \cos^n x\}$$

generat de funcţiile $1, \cos x, \cos^2 x, \ldots, \cos^n x$. Un exerciţiu (util) arată că funcţiile $1, \cos x, \cos 2x, \ldots, \cos nx$ formează o bază în $V_1$ şi

$$\cos^{n+1} x = \frac{1}{2^n}\cos(n+1)x + f_1(x),$$

unde $f_1 \in V_1$.

Avem:

$$\min \phi(g) = d^2(\cos^{n+1} x, V_1) = d^2\left(\frac{1}{2^n}\cos(n+1)x, V_1\right)$$

$$= \frac{G\left(1, \cos x, \ldots, \cos nx, \dfrac{1}{2^n}\cos(n+1)x\right)}{G(1, \cos x, \ldots, \cos nx)} = \frac{\pi}{2^{2n}}$$

(matricele Gram care apar sunt matrice diagonale căci $\langle \cos kx, \cos px\rangle = 0$ pentru $k \neq p$ şi $\langle \cos kx, \cos kx\rangle = \pi,\ k \geq 1$).

În concluzie valoarea minimă a integralei este $\dfrac{\pi}{2^{2n}}$.

**Problema 4.** Să se determine valoarea minimă a integralei $\displaystyle\int_{-1}^{1} (f(x))^2 \mathrm{d}x$, unde $f$ este un polinom monic de grad $n$ cu coeficienţi reali.

*Soluţie.* Considerăm spaţiul euclidian $C([-1,1])$ şi avem de calculat minimul funcţiei

$$\phi(a_1, a_2, \ldots, a_n) = \int_{-1}^{1} \left(a_1 + a_2 x + \cdots + a_n x^{n-1} + x^n\right)^2 \mathrm{d}x,$$

care reprezintă pătratul distanţei de la funcţia $x^n$ la spaţiul polinoamelor de grad $\leq n-1$, notat $\mathbb{R}_{n-1}[x]$. Ortogonalizând în $\mathbb{R}_n[x]$ baza $1, x, \ldots, x^{n-1}, x^n$ obţinem polinoamele lui Legendre

$$P_n(x) = \frac{n!}{(2n)!}[(x^2-1)^n]^{(n)}$$

şi din Teorema 1 rezultă că

$$d^2(x^n, \mathbb{R}_{n-1}[x]) = \|P_n\|^2 = \frac{n!^2}{(2n)!^2}\int_{-1}^{1}[(x^2-1)^n]^{(n)}[(x^2-1)^n]^{(n)}\mathrm{d}x.$$

Integrăm prin părţi ţinând cont că polinomul $(x^2-1)^n$ şi derivatele sale până la ordinul $n-1$ se anulează în 1 şi $-1$ şi obţinem:

$$\|P_n\|^2 = \frac{(-1)^n n!^2}{(2n)!^2}\int_{-1}^{1}(x^2-1)^n\mathrm{d}x = \frac{(-1)^n n!^2}{(2n)!}\int_{-1}^{1}(x-1)^n(x+1)^n\mathrm{d}x.$$

Integrăm din nou succesiv prin părţi şi obţinem

$$\|P_n\|^2 = \frac{n!^2}{(2n)!^2}\cdot\frac{n(n-1)\ldots 1}{(n+1)(n+2)\ldots(2n)}\int_{-1}^{1}(x+1)^{2n}\mathrm{d}x = \frac{n!^4}{(2n)!^3}\cdot\frac{2^{2n+1}}{2n+1}.$$

**Problema 5.** Să se determine valoarea minimă a integralei $\displaystyle\int_0^1 (f(x))^2\mathrm{d}x$, unde $f$ este polinom monic de grad $n$ cu coeficienţi reali.

*Soluţie.* În spaţiul euclidian $C([0,1])$, minimul căutat este pătratul distanţei de la $x^n$ la $\mathbb{R}_{n-1}[x]$ care, conform Teoremei 1, este

$$\frac{G(1, x, \ldots, x^{n-1}, x^n)}{G(1, x, \ldots, x^{n-1})} = \frac{G_1}{G_2}.$$

Deoarece $\langle x^k, x^p\rangle = \displaystyle\int_0^1 x^{k+p}\mathrm{d}x = \frac{1}{k+p+1}$, determinanţii $G_1$ şi $G_2$ sunt determinanţi Cauchy:

$$G_1 = C(0,1,\ldots,n; 1,2,\ldots,n+1) = \frac{V(0,1,\ldots,n)\cdot V(1,2,\ldots,n+1)}{\prod\limits_{k,p=0}^{n}(k+p+1)}$$

$$\frac{G_1}{G_2} = \frac{n!^2}{(n+1)^2\cdots(2n+2)^2(2n+3)} = \frac{n!^4}{(2n)!^2}\cdot\frac{1}{2n+3}. \qquad \square$$

## References

[1] V. Pop, *Algebră liniară*, Ed. Mediamira, Cluj-Napoca, 2003.

# PROBLEMS

Authors should submit proposed problems to gmaproblems@rms.unibuc.ro. Files should be in PDF or DVI format. Once a problem is accepted and considered for publication, the author will be asked to submit the TeX file also. The referee process will usually take between several weeks and two months. Solutions may also be submitted to the same e-mail address. For this issue, solutions should arrive before **15th of July 2012**.

## PROPOSED PROBLEMS

**351.** Let $(a_n)_{n\geq 1}$ be a sequence of positive integers and let $\alpha > \dfrac{1}{2}$ such that $\sum\limits_{n\geq 1} a_n^{-\alpha} = \infty$. Prove that for any $k \geq 2$ there is an integer that can be represented in at least $k$ ways as a sum of two elements of the sequence.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

**352.** Let $K$ be a field and let $m$, $n$, $k$ be positive integers. Find necessary and sufficient conditions the integers $a$, $b$, $c$ should satisfy such that there exist some matrices $A \in M_{m,n}(K)$ and $B \in M_{n,k}(K)$ with $\operatorname{rank}(A) = a$, $\operatorname{rank}(B) = b$ and $\operatorname{rank}(AB) = c$.

Proposed by Nicolae Constantin Beli, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

**353.** Let $f : [-1, 1] \to \mathbb{R}$ be a continuous function which is differentiable at 0. Denote

$$I(h) = \int_{-h}^{h} f(x)\mathrm{d}x, \quad h \in [0, 1].$$

Show that

$$\lim_{n\to\infty} \frac{1}{n^2} \sum_{k=1}^{n} \varphi(k)k|I(1/k)| = \frac{6}{\pi^2}|f(0)|.$$

(Here $\varphi$ is the Euler's totient function.)

Proposed by Cezar Lupu, University of Pittsburgh, Pittsburgh, PA, USA, and Călin Popescu, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

**354.** For $x > 1$, define the function $f(x) = \displaystyle\int_{1}^{\infty} e^{it^x}\,\mathrm{d}t$. Prove that there exists $L \in \mathbb{C}^*$ such that $\lim\limits_{x\to\infty} xf(x) = L$.

Proposed by Moubinool Omarjee, Jean Lurçat High School, Paris, France.

**355.** Let $p$ be an odd prime number and $\alpha \in \left[0; \frac{\pi}{2}\right]$ such that $\cos\alpha = \frac{1}{p}$. Prove that for any $n \in \mathbb{N}^*$, $n > 1$, there is no $m \in \mathbb{N}^*$ such that $\cos(n\alpha) = \frac{1}{m}$.

Proposed by Vlad Matei, University of Cambridge, Cambridge, UK.

**356.** Let $\{b_n\}_{n\geq 0}$ be a sequence of positive real numbers. The following statements are equivalent:

i) $\displaystyle\sum_{n=0}^{\infty} \frac{|b_{n+1}^r - b_n^r|}{b_n} < \infty$ for all $r \in \mathbb{R}$;

ii) $\displaystyle\sum_{n=0}^{\infty} \frac{|b_{n+1} - b_n|}{b_n} < \infty$;

iii) $\displaystyle\sum_{n=0}^{\infty} |b_{n+1} - b_n| < \infty$ and $\lim b_n > 0$;

iv) $\displaystyle\sum_{n=0}^{\infty} \frac{|b_{n+1} - b_n|}{b_{n+1}} < \infty$;

v) $\displaystyle\sum_{n=0}^{\infty} \frac{|b_{n+1}^r - b_n^r|}{b_{n+1}} < \infty$ for all $r \in \mathbb{R}$.

Proposed by Alexandru Kristaly, Babeş-Bolyai University, Cluj-Napoca, Romania, and Gheorghe Moroşanu, Central European University, Budapest, Hungary.

**357.** Find all functions $\varphi : \mathbb{R} \to \mathbb{R}$ with $\varphi(0) = 0$ such that the set of functions $\{\varphi + y \mid y \in \mathbb{R}\}$ is a semigroup with respect to the operation „$\circ$", the composition of functions. Prove that this semigroup is a monoid if and only if $\varphi$ is the identity map.

Proposed by Dan Schwarz, Bucharest and Marcel Ţena, Sfântul Sava National College, Bucharest, Romania.

**358.** Prove that for any coloring of the latticial points of the plane with a finite number of colors and for any triangle $ABC$ having angles with rational tangents there is a triangle with latticial vertices of the same color which is similar to $ABC$.

Proposed by Beniamin Bogoşel, West University of Timişoara, Timişoara, Romania.

**Editors' note.** Do not use the plane van der Waerden theorem, try a direct solution.

**359.** Determine how many permutations of the 81 squares of the Sudoku grid have the property that for any solution of the Sudoku game, if we apply the permutation to the 81 squares we obtain another solution of the Sudoku game.

Proposed by Nicolae Constantin Beli, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

**360.** Let $M_n(\mathbb{C})$ be the ring of square matrices of size $n$ and $A \in M_n(\mathbb{C})$. Show that if for all $k \in \mathbb{N}$, $k \geq 1$, we have $\det((\mathrm{adj}(A))^k + I_n) = 1$, then $(\mathrm{adj}(A))^2 = 0_n$.

(Here $\mathrm{adj}(A)$ denotes the classical adjoint of $A$, defined as follows: the $(i, j)$-minor $M_{ij}$ of $A$ is the determinant of the $(n-1) \times (n-1)$ matrix obtained by deleting row $i$ and column $j$ of $A$, and the $(i, j)$ cofactor of $A$ is $C_{ij} = (-1)^{i+j} M_{ij}$. The classical adjoint of $A$ is the transpose of the "cofactor matrix" $C_{ij}$ of $A$.)

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania, and Cezar Lupu, University of Pittsburgh, Pittsburgh, PA, USA.

**361.** 88% of the surface of a sphere is colored in red. Prove that there is a cube inscribed in the sphere with all vertices red.

Proposed by George Stoica, University of New Brunswick in Saint John, Saint John, NB, Canada.

**362.** Given a function $f : X \to X$, we will denote

$$f_0(X) := X,\ f_n(X) := f(f_{n-1}(X)) \text{ for } n \geq 1,$$
$$f_\omega(X) := \bigcap_{n \geq 0} f_n(X).$$

i) Prove that $f(f_\omega(X)) \subseteq f_\omega(X)$.

ii) Prove that for $X = \mathbb{R}$ and $f$ a continuous mapping, $f_\omega(\mathbb{R})$ is $\mathbb{R}$, a half-line, a bounded segment, a singleton, or the empty set.

Moreover, let it now be given that $f(f_\omega(\mathbb{R})) = f_\omega(\mathbb{R})$.

iii) Prove that if $f_\omega(\mathbb{R})$ is bounded, then it is a closed interval (possibly degenerate – a singleton or the empty set). Give examples for each of these cases.

iv) Give an example for $f_\omega(\mathbb{R})$ being an open half-line.

Proposed by Dan Schwarz, Bucharest, Romania.

**363.** For a given sequence $(x_n)_{n \geq 1}$ of real numbers and $n_0$ a fixed positive integer, consider the following conditions:

$(C_1)$: $n^2(x_{n+1} - x_n) - (2n+1)x_n$ has the same sign for all $n \geq n_0$;

$(C_2)$: $x_{n+m} \leq x_n + x_m$ for all $n, m \neq n_0$;

$(C_3)$: $\displaystyle\sum_{n=1}^{\infty} n^{-2} x_n < \infty$;

$(C_4)$: $\displaystyle\lim_{n \to \infty} \frac{x_n}{n} = 0$.

Prove that:

(a) none of $(C_1)$, $(C_2)$, $(C_3)$ implies $(C_4)$;

(b) $(C_4)$ follows from $(C_3)$ and either $(C_1)$ or $(C_2)$;

(c) the converse of b) is false.

Proposed by Arpad Benyi, Western Washington University, Bellingham, WA and Kasso Okoudjou, University of Maryland, College Park, Washington DC, WA, USA.

**364.** Let $(x_n)_{n\geq 1}$ be a sequence of real numbers such that
$$\limsup_{n\to\infty}((1-x_n)\log n) < \infty.$$
Show that if the series of positive reals $\sum\limits_{n\geq 1} a_n$ converges, then the series $\sum\limits_{n\geq 1} a_n^{x_n}$ also converges.

Proposed by Cristian Ghiu, Politehnica University of Bucharest, Bucharest, Romania.

## SOLUTIONS

**323.** Let $\mathcal{C}$ be the set of the circles in the plane and $\mathcal{L}$ be the set of the lines in the plane. Show that there exist bijective maps $f, g : \mathcal{C} \to \mathcal{L}$ such that for any circle $C \in \mathcal{C}$, the line $f(C)$ is tangent at $C$ and the line $g(C)$ contains the center of $C$.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

*Solution by the author.* If $A$ is an well ordered set and $\alpha \in A$ we denote $A_\alpha := \{a \in A \mid a < \alpha\}$. We prove that there is an well ordered set $A$ of cardinal $\mathbf{c} := |\mathbb{R}|$ such that $|A_\alpha| < \mathbf{c}\ \forall \alpha \in A$. To do this we take a well-ordered set $M$ with $|M| = \mathbf{c}$. If there is $\alpha \in M$ with $|M_\alpha| = \mathbf{c}$ then let $M' = \{\alpha \in A \mid |M_\alpha| = \mathbf{c}\}$ and let $\alpha_0$ be the smallest element of $M'$. Then $|M'_{\alpha_0}| = \mathbf{c}$ and if we denote $M'' = M'_{\alpha_0}$ then for any $\alpha \in M''$ we have $\alpha < \alpha_0$, so $|M''_\alpha| = |M_\alpha| < \mathbf{c}$ and we may take $A = M''$.

Let $\mathcal{C}$ be the set of all circles in the plane and let $\mathcal{L}$ be the set of all lines in the plane. Since $|\mathcal{C}| = |\mathcal{L}| = \mathbf{c}$, the order relation from $A$ may be transported to $\mathcal{C}$ and $\mathcal{L}$. The function $f$ will be constructed by transfinite induction. First we take $c_0 = \min \mathcal{C}$ and we define $f(c_0)$ as the smallest element $l_0$ of $\mathcal{L}$ that is tangent to $c_0$.

Assumed that for some $c \in \mathcal{C}$ we have already defined $f(c')\ \forall c' < c$. Since $N := \mathcal{C}_c$ has a cardinal which is smaller than $\mathbf{c}$, there are lines tangent to $c$ that are not contained in $N$. Let $l$ be the smallest of these lines and define $f(c) = l$. Obviously $f$ is injective.

To prove the surjectivity, assume that $\mathcal{L} \setminus \operatorname{Im} f \neq \emptyset$ and let $l \in \mathcal{L} \setminus \operatorname{Im} f$. Since the set of the circles tangent to $l$ has cardinal $\mathbf{c}$ and $|\mathcal{L}_l| < \mathbf{c}$, there is some $c \in \mathcal{C}$ which is tangent to $l$ such that $f(c) \notin \mathcal{L}_l$, i.e., $f(c) \geq l$. On the other hand, $f(c)$ is the smallest element of $X := \{d \in \mathcal{L} \mid d \text{ tangent to } c\} \setminus f(\mathcal{C}_c)$. Since $l \notin \operatorname{Im} f \supseteq f(\mathcal{C}_c)$ and $l$ is tangent to $c$, we have $l \in X$ and so $f(c) \leq l$. It folows that $f(c) = l$, so $c \in \operatorname{Im} f$. Contradiction.

The function $g$ is constructed the same way but with the property "a line is tangent to a circle" replaced by the property "the line contains the center of the circle".

**324.** Consider the set
$$K := \{\, f(\sqrt[4]{20}\,, \sqrt[6]{500}\,) \mid f(X,Y) \in \mathbb{Q}[X,Y]\,\}.$$

(a) Show that $K$ is a field with respect to the usual addition and multiplication of real numbers.

(b) Find all the subfields of $K$.

(c) If one considers $K$ as a vector space ${}_{\mathbb{Q}}K$ over the field $\mathbb{Q}$ in the usual way, find the dimension of ${}_{\mathbb{Q}}K$.

(d) Exhibit a vector space basis of ${}_{\mathbb{Q}}K$.

Proposed by Toma Albu, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.

*Solution by the author.* (a) Note that $K$ is exactly the subring $\mathbb{Q}[\sqrt[4]{20}\,, \sqrt[6]{500}\,]$ of $\mathbb{R}$ obtained by adjoining to $\mathbb{Q}$ the algebraic elements $\sqrt[4]{20}$ and $\sqrt[6]{500}$ over $\mathbb{Q}$, so as it is well known from any undergraduate General Algebra course, $K$ is a subfield of $\mathbb{R}$, and the field extension $\mathbb{Q} \subseteq K$ is finite, in other words, the vector space ${}_{\mathbb{Q}}K$ is finite dimensional. The dimension $[\,K : \mathbb{Q}\,]$ of this vector field will be determined in (c).

(b) For simplicity, denote $a := \sqrt[6]{500}$, $b := \sqrt[4]{20}$, $c := \sqrt[12]{500}$. Then $a = \sqrt[12]{2^4 \cdot 5^6}$, $b = \sqrt[12]{2^6 \cdot 5^3}$, $c = \sqrt[12]{2^2 \cdot 5^3}$. Easy calculations show that $a = c^2$, $b = 10c{\cdot}a^{-2}$, so $a \in \mathbb{Q}[c]$, and then, also $b \in \mathbb{Q}[c]$. It follows that $K = \mathbb{Q}[a, b] \subseteq \mathbb{Q}[c]$. Since $c = 10^{-1}a^2b$, we have $c \in \mathbb{Q}[a, b]$, and hence $\mathbb{Q}[c] \subseteq \mathbb{Q}[a, b]$. We deduce that $K = \mathbb{Q}[c]$.

In the sequel we will freely refer to some basic results of Cogalois Theory, as exposed in [1]. First, observe that the field extension $\mathbb{Q} \subseteq K$ is a Cogalois extension with Cogalois group $\mathrm{Cog}(K/\mathbb{Q}) = \mathbb{Q}^*\langle c\,\rangle/\mathbb{Q}^*$, where

$$\mathbb{Q}^*\langle c\,\rangle := \{\, a \cdot c^n \mid a \in \mathbb{Q}^*,\, n \in \mathbb{Z}\},$$

see Examples 3.2.1 (1) in [1]. By Theorem 3.2.3 in [1], all the intermediate fields of the Cogalois extension $\mathbb{Q} \subseteq K$, that is to say, all the subfields of the field $K$, are exactly $\mathbb{Q}[H]$, where $H/\mathbb{Q}^*$ is a subgroup of $\mathrm{Cog}(K/\mathbb{Q})$.

Clearly $\mathrm{Cog}(K/\mathbb{Q}) = \mathbb{Q}^*\langle c\,\rangle/\mathbb{Q}^* = \langle \widehat{c}\,\rangle$ is a cyclic group of order 12 generated by the coset $\widehat{c} = c\,\mathbb{Q}^*$ of $c$ in the quotient group $\mathbb{Q}^*\langle c\,\rangle/\mathbb{Q}^*$, so its subgroups are precisely the following ones:

$$\langle \widehat{c}\,\rangle,\ \langle \widehat{c^2}\,\rangle,\ \langle \widehat{c^3}\,\rangle,\ \langle \widehat{c^4}\,\rangle,\ \langle \widehat{c^6}\,\rangle,\ \langle \widehat{c^{12}}\,\rangle\,.$$

Consequently, all the subfields of $E$ are:

$$\mathbb{Q},\ \mathbb{Q}[c],\ \mathbb{Q}[c^2],\ \mathbb{Q}[c^3],\ \mathbb{Q}[c^4],\ \mathbb{Q}[c^6],$$

where $c = \sqrt[12]{500}$.

(c) Since the extension $\mathbb{Q} \subseteq K$ is Cogalois, we have

$$[\,K : \mathbb{Q}\,] = |\mathrm{Cog}(K/\mathbb{Q})| = 12.$$

(d) By basic properties of Kneser field extensions, a vector space basis for the Cogalois extension $\mathbb{Q} \subseteq K$ is easily obtained as soon as we have listed, with no repetition, all the elements of its cyclic Cogalois group $\mathbb{Q}^*\langle c\,\rangle/\mathbb{Q}^* = \langle \widehat{c}\,\rangle$ of order 12: any set of representatives of the cosets from this list is a basis of the extension. Consequently such a basis is the set $\{\, \sqrt[12]{500}^{\,i} \mid 0 \leqslant i \leqslant 11\}$.

**Remarks.** More generally, let

$$E := \mathbb{Q}\,[\,\sqrt[n_1]{a_1}\,, \ldots, \sqrt[n_r]{a_r}\,]$$

and

$$G := \mathbb{Q}^*\langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r} \rangle$$
$$= \{ a \cdot \sqrt[n_1]{a_1}^{k_1} \cdot \ldots \cdot \sqrt[n_r]{a_r}^{k_r} \mid a \in \mathbb{Q}^*,\, 0 \leqslant k_i < n_i,\, \forall\, 1 \leqslant i \leqslant r\},$$

where $r$, $n_1, \ldots, n_r$ are nonzero natural numbers and $a_1, \ldots, a_r$ are positive rational numbers. Then, by the Kneser Criterion (see Theorem 2.2.1 in [1]), the extension $\mathbb{Q} \subseteq E$ is $G$-Kneser extension, so

$$[\,\mathbb{Q}\,[\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\,] : \mathbb{Q}\,] = |\,\mathbb{Q}^*\langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\rangle/\mathbb{Q}^*|.$$

Moreover, this extension is $G$-Cogalois, so, by Theorem 4.3.2 in [1], all the intermediate fields of the $G$-Cogalois extension $\mathbb{Q} \subseteq E$, i.e., all the subfields of the field $E$, are exactly $\mathbb{Q}[H]$, where $H/\mathbb{Q}^*$ is a subgroup of its Kneser group $G/\mathbb{Q}^*$. So, knowing all the subgroups of this Kneser group, we can completely describe all the subfields of $\mathbb{Q}\,[\sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\,]$.

As in the particular case considered above, a vector space basis for the extension $\mathbb{Q} \subseteq E$ is easily obtained as follows. List, with no repetition, all the elements of its Kneser group $\mathbb{Q}^*\langle \sqrt[n_1]{a_1}, \ldots, \sqrt[n_r]{a_r}\rangle/\mathbb{Q}^*$; then any set of representatives of the cosets from this list is a basis of the extension.

## References

[1] T. Albu, *Cogalois Theory*, A Series of Monographs and Textbooks, Vol. 252, Marcel Dekker, Inc., New York and Basel, 2003.

**325.** We call *toroidal chess board* a regular chess board (of arbitrary dimension) in which the opposite sides are identified in the same direction. Show that the maximum number of kings on a toroidal chess board of dimensions $m \times n$ $(m, n \in \mathbb{N})$ such that each king attacks no more than six other kings is less than or equal to $\dfrac{4mn}{5}$ and the inequality is sharp.

`Proposed by Eugen Ionaşcu, Columbus State University, Columbus, GA, USA.`

*Solution by the author.* Let us denote by $x_{i,j}$ $(i = 0, \ldots, m-1,\, j = 0, \ldots, n-1)$ $mn$ variables for each square of the board. These variables take the value 1 if a king is placed on the $(i, j)$ position or 0 otherwise. The condition that we required in this problem is equivalent to

$$2x_{i,j} + x_{i-1,j-1} + x_{i,j-1} + x_{i+1,j-1} + x_{i-1,j} + x_{i+1,j} + x_{i-1,j+1} + x_{i,j+1} + x_{i+1,j+1} \le 8$$

for all possible $i, j$ and the operations are done modulo $m$ on the first component and modulo $n$ for the second component of the indices of $x_{k,l}$. Let us put $k = \sum\limits_{i,j} x_{i,j}$.

Adding all these inequalities gives $2k + 8k \le 8mn$. Therefore $k \le \dfrac{4mn}{5}$. An example that shows that this estimate is sharp when $5 \mid m$ and $5 \mid n$ is given in the figure below. (In our case $m = 10$, $n = 15$.)

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 |

## References

[1] E.J. Ionaşcu, D. Pritikin and S.E. Wright, *k-Dependence and domination in king's graphs*, Amer. Math. Monthly 115 (2008), 820–836.

[2] T. Howard, E.J. Ionaşcu and D. Woolbright, *Introduction to the prisoners vs guards puzzle*, J. Integer Sequences, vol. 12, Article 09.1.3, (2009).

[3] E.J. Ionaşcu, *Bounds on the cardinality of a minimum $\frac{1}{2}$-dominating set in the king's graph*, in progress.

**326.** For $t > 0$ define $H(t) = \sum_{n=0}^{\infty} \frac{t^n}{n!(n+1)!}$. Show that

$$\lim_{t\to\infty} \frac{t^{3/4}H(t)}{\exp(2\sqrt{t})} = \frac{1}{2\sqrt{\pi}}.$$

`Proposed by Moubinool Omarjee, Jean Lurçat High School, Paris, France.`

*Solution by the author.* As a first step we prove that

$$H(t) = \frac{1}{\pi\sqrt{t}} \int_0^{\pi} \cos u \exp(2\sqrt{t}\cos u)\mathrm{d}u \text{ for } t > 0.$$

Indeed, we have

$$\frac{1}{\pi\sqrt{t}} \int_0^{\pi} \cos u \exp(2\sqrt{t}\cos u)\mathrm{d}u = \sum_{n=0}^{\infty} h_n(u),$$

where $h_n(u) = \dfrac{2^n(\sqrt{t})^{n-1}\cos^{n+1} u}{\pi n!}$ and we have

$$||h_n|| = \sup_{u\in[0,2\pi]} |h_n(u)| = \frac{2^n(\sqrt{t})^{n-1}}{\pi n!}.$$

Then

$$\frac{1}{\pi\sqrt{t}} \int_0^{\pi} \cos u \exp(2\sqrt{t}\cos u)\mathrm{d}u = \sum_{n=0}^{\infty} \frac{2^n(\sqrt{t})^{n-1}}{\pi n!} I_{n+1},$$

where

$$I_m = \int_0^\pi \cos^m u \mathrm{d}u = \begin{cases} 0 & \text{if } m \text{ is odd} \\ \pi 2^{-2k}\binom{2k}{k} & \text{if } m = 2k. \end{cases}$$

This leads to

$$\sum_{n=0}^{\infty} \frac{2^n(\sqrt{t})^{n-1}}{\pi n!} I_{n+1} = \sum_{n=0}^{\infty} \frac{2^{2n+1}t^n}{\pi(2n+1)!} \cdot \pi 2^{-2n-2}\binom{2n+2}{n+1} = \sum_{n=0}^{\infty} \frac{t^n}{n!(n+1)!},$$

as claimed.

Next we note that $\cos u \leq 0$ when $\frac{\pi}{2} \leq u \leq \pi$, so

$$\left| \frac{1}{\pi\sqrt{t}} \int_{\frac{\pi}{2}}^{\pi} \cos u \exp(2\sqrt{t}\cos u)\mathrm{d}u \right| \leq \frac{1}{\pi\sqrt{t}} \int_{\frac{\pi}{2}}^{\pi} |\cos u| \mathrm{d}u \to 0 \text{ when } t \to \infty.$$

For the integral $A(t) = \int_0^{\frac{\pi}{2}} \cos u \exp(2\sqrt{t}\cos u)\mathrm{d}u$ the change of variables $\nu = 1 - \cos u$ gives

$$A(t) = e^{2\sqrt{t}} \int_0^1 \frac{1-\nu}{\sqrt{1-\frac{\nu}{2}}} \cdot \frac{e^{-2\nu\sqrt{t}}}{\sqrt{2\nu}} \mathrm{d}\nu.$$

After two more changes of variables, $y = 2\nu\sqrt{t}$ and $w = \sqrt{y}$ one gets

$$\int_0^1 \frac{1-\nu}{\sqrt{1-\frac{\nu}{2}}} \cdot \frac{e^{-2\nu\sqrt{t}}}{\sqrt{2\nu}} \mathrm{d}\nu = \frac{1}{t^{\frac{1}{4}}} \int_0^{\sqrt{2}t^{\frac{1}{4}}} \frac{1 - \frac{w^2}{2\sqrt{t}}}{\sqrt{1 - \frac{w^2}{4\sqrt{t}}}} \cdot e^{-w^2} \mathrm{d}w.$$

By Lebesgue dominated convergence theorem one gets

$$t^{\frac{1}{4}} \int_0^1 \frac{1-\nu}{\sqrt{1-\frac{\nu}{2}}} \cdot \frac{e^{-2\nu\sqrt{t}}}{\sqrt{2\nu}} \mathrm{d}\nu \to \int_0^\infty e^{-w^2} \mathrm{d}w = \frac{\sqrt{\pi}}{2} \text{ when } t \to \infty,$$

so

$$A(t) \sim e^{2\sqrt{t}} \cdot \frac{\sqrt{\pi}}{2t^{\frac{1}{4}}}$$

and, finally

$$H(t) \sim \frac{1}{\pi\sqrt{t}} \cdot e^{2\sqrt{t}} \cdot \frac{\sqrt{\pi}}{2t^{\frac{1}{4}}}.$$

**327.** (Correction) Let $f : [a, b] \to \mathbb{R}$ be a convex and continuous function. Prove that:

a) $\mathcal{M}(a; b) + f\left(\frac{a+b}{2}\right) \geq 2\mathcal{M}\left(\frac{3a+b}{4}; \frac{3b+a}{4}\right)$;

b) $3\mathcal{M}\left(\frac{2a+b}{3}; \frac{2b+a}{3}\right) + \mathcal{M}(a; b) \geq 4\mathcal{M}\left(\frac{3a+b}{4}; \frac{3b+a}{4}\right)$.

Here $\mathcal{M}(x,y) = \dfrac{1}{y-x}\int\limits_x^y f(t)\mathrm{d}t.$

Proposed by Cezar Lupu, Politehnica University of Bucharest, Bucharest, Romania, and Tudorel Lupu, Decebal High School, Constanţa, Romania.

*Solution by the authors.* a) We use Popoviciu's inequality from [1]. (See also [2], pag. 12.) It states that for any convex function $f$ defined on an interval $[a,b]$ and any $x$, $y$, $z \in [a,b]$ we have

$$f(x)+f(y)+f(z)+3f\left(\frac{x+y+z}{3}\right) \geq 2f\left(\frac{x+y}{2}\right)+2f\left(\frac{x+z}{2}\right)+2f\left(\frac{y+z}{2}\right).$$

By applying Popoviciu's inequality to $x$, $\dfrac{a+b}{2}$, $a+b-x \in [a,b]$, we get

$$f(x)+f\left(\frac{a+b}{2}\right)+f(a+b-x)+3f\left(\frac{a+b}{2}\right) \geq$$

$$\geq 2f\left(\frac{a+b+2x}{4}\right)+2f\left(\frac{a+b}{2}\right)+2f\left(\frac{3a+3b-2x}{4}\right).$$

We integrate on $[a,b]$ and after suitable changes of variables we obtain

$$2(b-a)f\left(\frac{a+b}{2}\right)+2\int\limits_a^b f(x)\mathrm{d}x \geq 8\int\limits_{\frac{3a+b}{4}}^{\frac{a+3b}{4}} f(x)\mathrm{d}x,$$

which is a).

For b) we use again Popoviciu's inequality but this time for $x, \dfrac{a+b}{2}, \dfrac{a+b}{2} \in [a,b]$. We have

$$f(x)+2f\left(\frac{a+b}{2}\right)+3f\left(\frac{a+b+x}{3}\right) \geq 4f\left(\frac{2x+a+b}{4}\right)+2f\left(\frac{a+b}{2}\right).$$

After we integrate on $[a,b]$ and make the suitable changes of variable we get

$$9\int\limits_{\frac{2a+b}{3}}^{\frac{a+2b}{3}} f(x)\mathrm{d}x+\int\limits_a^b f(x)\mathrm{d}x \geq 8\int\limits_{\frac{3a+b}{4}}^{\frac{a+3b}{4}} f(x)\mathrm{d}x,$$

i.e. we have b).

## References

[1] T. Popoviciu, *Sur certaines inégalités qui caractérisent les fonctions convexes*, Analele ştiinţifice Univ. „Al.I. Cuza“ Iaşi, Secţia I a Mat. 11 (1965), 155–164.

[2] C. Niculescu, L.E. Persson, *Convex functions and their applications: a contemporary approach*, Springer Science & Business (2006).

**328.** Given any positive integers $m$, $n$, prove that the set

$$\{1, 2, 3, \ldots, m^{n+1}\}$$

can be partitioned into $m$ subsets $A_1, A_2, \ldots, A_m$, each of size $m^n$, such that

$$\sum_{a_1 \in A_1} a_1^k = \sum_{a_2 \in A_2} a_2^k = \ldots = \sum_{a_m \in A_m} a_m^k, \quad \text{for all} \quad k = 1,\ 2,\ \ldots,\ n.$$

Proposed by Cosmin Pohoaţă, student Princeton University, Princeton, NJ, USA.

*Solution by Marian Tetiva.* This is an immediate consequence of Prouhet's theorem, old since 1851. It has the same statement as the present problem but with $\{1, \ldots, m^{n+1}\}$ replaced by $A := \{0, \ldots, m^{n+1} - 1\}$, i.e., the set of natural numbers with at most $n+1$ digits when written in base $m$.

Basically the set $A_j$ will contain precisely those numbers in $A$ whose sum of base $m$ digits is congruent to $j$ modulo $m$. A solution can be found in *The American Mathematical Monthly* from April 2009, pages 366–368 (solution of problem 11266). In addition, there one can find many references on this and related topics, such as Tarry-Escott problem.

To obtain our result one only has to note that if $A = A_1 \cup \cdots \cup A_m$ is a partition with the property that $|A_j|$ is the same for all $j$ and for $1 \le k \le n$ $\sum_{a \in A_j} a^k$ is the same for all $j$ then for any $x$ the set $a + A := \{x + a \mid a \in A\}$ has a similar partition. Namely $x + A = (x + A_1) \cup \cdots \cup (x + A_m)$. Indeed, if $|A_j| = S_0$ and $\sum_{a \in A_j} a^k = S_k$ for all $j$ and for $1 \le k \le n$ then for every $1 \le j \le n$ we have $|x + A_j| = S_0$, and if $1 \le k \le n$ then

$$\sum_{b \in x + A_j} b^k = \sum_{a \in A_j} (x + a)^k = \sum_{a \in A_j} \sum_{l=0}^{k} \binom{k}{l} x^{k-l} a^l = \sum_{l=0}^{k} \binom{k}{l} x^{k-l} S_l,$$

which is independent of $j$.

**329.** Let $p \ge 11$ be a prime number. Show that, if

$$\sum_{j=1}^{(p-1)/2} \frac{1}{j^6} = \frac{a}{b}$$

with $a$, $b$ relatively prime, then $p$ divides $a$.

Proposed by Marian Tetiva, Gheorghe Roşca Codreanu National College, Bârlad, Romania.

*Solution by the author.* The inverses modulo $p$ of the quadratic residues $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are precisely the same quadratic residues, in some order. For proving this claim one can observe that the inverse of a quadratic residue is a quadratic residue, too, and the inverses of the $\frac{p-1}{2}$ nonzero quadratic residues are mutually distinct.

Denote, for every $j$ from 1 to $\frac{p-1}{2}$, by $k_j$ the unique integer with the properties $1 \le k_j \le \frac{p-1}{2}$ and $j^2k_j^2 \equiv 1 \pmod{p}$. Then, by the above observation,

$$\left\{k_1^2, k_2^2, \ldots, k_{(p-1)/2}^2\right\} = \left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}.$$

We thus have

$$\sum_{j=1}^{(p-1)/2} \frac{1}{j^6} - \sum_{j=1}^{(p-1)/2} k_j^6 = \sum_{j=1}^{(p-1)/2} \frac{1-j^6k_j^6}{j^6} \equiv 0 \pmod{p}$$

and

$$\sum_{j=1}^{(p-1)/2} k_j^6 = \sum_{j=1}^{(p-1)/2} j^6 \equiv 0 \pmod{p}.$$

The last congruence follows by using the formula

$$\sum_{j=1}^{n} j^6 = \frac{n(n+1)(2n+1)(3n^4+6n^3-3n+1)}{42}$$

according to which (for $n = \frac{p-1}{2}$) $\sum_{j=1}^{(p-1)/2} j^6$ is divisible by $2\frac{p-1}{2}+1 = p$, unless $p$ is one of the primes that divide 42, hence the divisibility is true for either $p = 5$ or $p \ge 11$. The two congruences above solve our problem.

Actually one can see that the property is true if and only if $p = 5$ or $p \ge 11$.

**330.** Determine all nonconstant monic polynomials $f \in \mathbb{Z}[X]$ such that $\varphi(f(p)) = f(p-1)$ for all natural prime numbers $p$. (Here $\varphi$ is the Euler totient function.)

`Proposed by Vlad Matei, student University of Bucharest, Bucharest, Romania.`

*Solution by the author.* We will use the following property of polynomials with integer coefficients:

$$(C) \text{ for all } a, b \in \mathbb{Z}, a-b \text{ divides } f(a)-f(b).$$

First we prove that $f(0) = 0$. Let us assume the contrary, $f(0) \ne 0$. Then for a fixed prime $p > |f(0)|$ we deduce from $(C)$ that $f(p) \equiv f(0) \pmod{p}$, so $\gcd(f(p), p) = 1$. According to Dirichlet's theorem, there are infinitely many primes in the arithmetic progression $p + rf(p)$. Let $p_k$ be the $k$th prime in this sequence.

Again from $(C)$ we deduce that $f(p+rf(p)) \equiv f(p) \pmod{f(p)}$ for any integer $r$, so $f(p) \mid f(p_k)$. From the fact that $\frac{\varphi(a)}{a} = \prod_{\substack{q \text{ prime} \\ q|a}} \left(1 - \frac{1}{q}\right)$ we can easily deduce that for $c \mid a$ we have $\dfrac{\varphi(a)}{a} \le \dfrac{\varphi(c)}{c}$. This implies $\dfrac{\varphi(f(p_k))}{f(p_k)} \le \dfrac{\varphi(f(p))}{f(p)}$, that is,

$$\frac{f(p_k-1)}{f(p_k)} \le \frac{\varphi(f(p))}{f(p)}. \tag{1}$$

Let us note that $\lim\limits_{k\to\infty} p_k = \infty$. Putting $h(X) = f(X-1)$, we observe that $h$ and $f$ have the same degree and both are monic polynomials, so $\lim\limits_{x\to\infty} \dfrac{h(x)}{f(x)} = 1$. This means that $\lim\limits_{k\to\infty} \dfrac{f(p_k-1)}{f(p_k)} = 1$. Passing to limit in (1), we obtain $1 \le \dfrac{\varphi(f(p))}{f(p)}$, so $f(p) \le \varphi(f(p))$. We conclude that $f(p) = 1$. But this can not hold for infinitely many primes $p$, since then $f$ would be a constant polynomial, which contradicts the hypothesis.

So $f(0) = 0$. Let $f(X) = X^i g(X)$ with $g(0) \ne 0$ and $i$ a positive integer.

The hypothesis gives that $\left(\dfrac{p}{p-1}\right)^{i-1} \varphi(g(p)) = g(p-1)$ for all primes $p$ not dividing $g(0)$. We assume that $g$ is nonconstant, and arguing as above we get an infinite sequence of prime numbers $p'_k$ such that $\dfrac{g(p'_k-1)}{g(p'_k)} \le \dfrac{\varphi(g(p))}{g(p)} \cdot \left(\dfrac{p'_k}{p'_k-1}\right)^{i-1}$. Again we pass to limit as $k \to \infty$ and obtain $1 \le \dfrac{\varphi(g(p))}{g(p)}$.

Thus $g(p) = 1$ for infinitely many primes $p$, so $g \equiv 1$, a contradiction with the assumption that $g$ is not constant. So $g(X) = c$ and from the fact that $f$ is monic we get $c = 1$. We are left with $\left(\dfrac{p}{p-1}\right)^{i-1} = 1$ for all prime numbers $p$, so $i = 1$.

This means that the only solution is $f(X) = X$.

**331.** Let $\mathcal{B}_n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid x_i \le x_{i+2} \text{ for } 1 \le i \le n-2\}$ and let $\mathcal{B} = \bigcup\limits_{n\ge1} \mathcal{B}_n$. On $\mathcal{B}$ we define the relation $\le$ as follows. If $x, y \in \mathcal{B}$, $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$, we say that $x \le y$ if $m \ge n$ and for any $1 \le i \le n$ we have either $x_i \le y_i$ or $1 < i < m$ and $x_i + x_{i+1} \le y_{i-1} + y_i$. Prove that $(\mathcal{B}, \le)$ is a partially ordered set.

`Proposed by Nicolae Constantin Beli, Simion Stoilow Institute of Mathematics of the Romanian Academy, Bucharest, Romania.`

*Solution by the author.* Let $x, y, z \in \mathcal{B}$, $x = (x_1, \ldots, x_m)$, $y = (y_1, \ldots, y_n)$ and $z = (z_1, \ldots, z_k)$.

We first prove that if $x \le y$ then $x_i + x_{i+1} \le y_i + y_{i+1}$ for any $1 \le i \le n-1$. We have three cases.

If $x_i \le y_i$ and $x_{i+1} \le y_{i+1}$ then $x_i + x_{i+1} \le y_i + y_{i+1}$.

If $x_i > y_i$ then $x_i + x_{i+1} \le y_{i-1} + y_i \le y_i + y_{i+1}$.

If $x_{i+1} > y_{i+1}$ then $x_i + x_{i+1} \le x_{i+1} + x_{i+2} \le y_i + y_{i+1}$.

Similarly if $y \le z$ then $y_i + y_{i+1} \le z_i + z_{i+1}$ for $1 \le i \le k-1$.

We now prove that $\le$ is an order relation.

To prove the transitivity, assume that $x \le y$ and $y \le z$. We want to prove that $x \le z$. We have $m \ge n$ and $n \ge k$, so $m \ge k$. We have to prove that for any $1 \le i \le k$ we have $x_i \le z_i$ or $x_i + x_{i+1} \le z_{i-1} + z_i$. There are three cases.

If $x_i \le y_i$ and $y_i \le z_i$ then $x_i \le z_i$ and we are done.

If $x_i > y_i$ then $x_i + x_{i+1} \le y_{i-1} + y_i \le z_{i-1} + z_i$.

If $y_i > z_i$ then $x_i + x_{i+1} \le y_i + y_{i+1} \le z_{i-1} + z_i$.

The reflexivity is trivial. We have $m \ge m$ and $x_i \le x_i$ for $1 \le i \le m$ so $x \le x$.

To prove the antisymmetry, assume that $x \le y$ and $y \le x$. Then $m \ge n$ and $n \ge m$ so $m = n$. For any $1 \le i \le m-1$ we have $x_i + x_{i+1} \le y_i + y_{i+1}$ and $y_i + y_{i+1} \le x_i + x_{i+1}$, so $x_i + x_{i+1} = y_i + y_{i+1}$. The condition at $i = 1$ from the definition of $x \le y$ is $x_1 \le y_1$. Similarly $y_1 \le x_1$ so $x_1 = y_1$. From $x_1 = y_1$, $x_1 + x_2 = y_1 + y_2$, $x_2 + x_3 = y_2 + y_3, \ldots, x_{m-1} + x_m = y_{m-1} + y_m$ one gets $x_i = y_i$ for $1 \le i \le m$ so $x = y$.

**332.** For a positive integer $n = \displaystyle\prod_{i=1}^{s} p_i^{\alpha_i}$ denote by $\Omega(n) := \displaystyle\sum_{i=1}^{s} \alpha_i$ the total number of prime factors of $n$ (counting multiplicities). Of course, by default $\Omega(1) = 0$. Define now $\lambda(n) := (-1)^{\Omega(n)}$, and consider the sequence $\mathfrak{S} := (\lambda(n))_{n\ge 1}$. Prove the following claims on $\mathfrak{S}$:

a) It contains infinitely many terms $\lambda(n) = -\lambda(n+1)$.

b) It is not ultimately periodic.

c) It is not ultimately constant over an arithmetic progression.

d) It contains infinitely many pairs $\lambda(n) = \lambda(n+1)$.

e) It contains infinitely many terms $\lambda(n) = \lambda(n+1) = 1$.

f) It contains infinitely many terms $\lambda(n) = \lambda(n+1) = -1$.

`Proposed by Dan Schwarz, Bucharest, Romania.`

*Solution by the author.* Notice that $\Omega(mn) = \Omega(m) + \Omega(n)$ for all positive integers $m, n$ ($\Omega$ is a completely additive arithmetic function), translating into $\lambda(mn) = \lambda(m) \cdot \lambda(n)$ ($\lambda$ is a completely multiplicative arithmetic function), hence $\lambda(p) = -1$ for any prime $p$, and $\lambda(k^2) = \lambda(k)^2 = 1$ for positive integers $k$.

The start (first 100 terms) of the sequence $\mathfrak{S}$ is

$1, -1, -1, 1, -1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1, -1, -1,$
$1, 1, -1, 1, 1, 1, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, 1, 1, 1, 1, -1, 1, 1, 1,$
$-\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, -\mathbf{1}, 1, -1, -1, 1, -1, 1, -1, -1, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, -1, 1,$
$-1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, -1, -1,$
$1, 1, -1, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1.$

a) According with the preliminaries, $\mathfrak{S}$ is therefore not ultimately constant, hence the thesis.

b) Assume there exist $t, k$ such that $\lambda(n+t) = \lambda(n)$ for all $n \ge k$. Take $n = mt \ge k$; then $\lambda((m+1)t) = \lambda(mt)$, so $\lambda(m+1) \cdot \lambda(t) = \lambda(m) \cdot \lambda(t)$, hence $\lambda(m+1) = \lambda(m)$ for all large enough $m$, at odds with part a).

c) We have to prove that, given $a \in \mathbb{N}$, $b \in \mathbb{Z}$, then $\lambda(an+b)$ is not constant for $n > n_0$ (a stronger result than that of point b)). Take first $M \in \mathbb{N}$ large enough so $b' = aM + b > 0$; also take $n = kb' + M$. Then

$$\lambda(an+b) = \lambda((ak+1)b') = \lambda(ak+1) \cdot \lambda(b').$$

But $\lambda(ak+1) = -1$ when $ak+1$ is a prime, infinitely often for $k \in \mathbb{N}$ (by Dirichlet's theorem), while $\lambda(ak+1) = 1$ when $ak+1$ is a perfect square, and it is enough to this purpose to take $k = a\ell^2 + 2\ell$, so then $ak + 1 = (a\ell + 1)^2$.

d) Take one of the subsequences $(\lambda(k), \lambda(k+1)) = (1, -1)$. Then we have $\lambda(2k) = \lambda(2) \cdot \lambda(k) = -1$, and $\lambda(2k+2) = \lambda(2) \cdot \lambda(k+1) = 1$; we will call this the "doubling" of the subsequence $(1, -1)$, producing $(-1, ?, 1)$. Now, both $? = \lambda(2k+1) = 1$ and $? = \lambda(2k+1) = -1$ create a pair of consecutive terms of same value, hence the thesis.

e) The Pell equation $x^2 - 6y^2 = 1$ has infinitely many solutions in positive integers; all solutions are given by $(x_n, y_n)$, where $x_n + y_n\sqrt{6} = (5 + 2\sqrt{6})^n$. Since $\lambda(6y^2) = 1$ and $\lambda(6y^2+1) = \lambda(x^2) = 1$, the thesis is proven (an alternative approach is to do like in what comes next).

*Alternative Solution.* Take any existing pair $\lambda(n) = \lambda(n+1) = 1$. Then

$$\lambda((2n+1)^2 - 1) = \lambda(4n^2 + 4n) = \lambda(4) \cdot \lambda(n) \cdot \lambda(n+1) = 1,$$

and also $\lambda((2n+1)^2) = \lambda(2n+1)^2 = 1$, so we have built a larger $(1, 1)$ pair.

f) The Pell-like equation $3x^2 - 2y^2 = 1$ has infinitely many solutions in positive integers, given by $(x_n, y_n)$, where $x_n\sqrt{3} + y_n\sqrt{2} = (\sqrt{3} + \sqrt{2})^{3^{n-1}}$. Since $\lambda(2y^2) = -1$ and $\lambda(2y^2 + 1) = \lambda(3x^2) = -1$, the thesis is proven (an alternative approach is to do like in what comes next). Next, assume $(\lambda(n-1), \lambda(n))$ is the largest $(-1, -1)$ pair, therefore $\lambda(n+1) = 1$ and $\lambda(n^2 + n) = \lambda(n) \cdot \lambda(n+1) = -1$, therefore again $\lambda(n^2 + n + 1) = 1$. But then $\lambda(n^3 - 1) = \lambda(n-1) \cdot \lambda(n^2 + n + 1) = -1$, and also $\lambda(n^3) = \lambda(n)^3 = -1$, so we found a yet larger such pair, contradiction. Assume the pairs of consecutive terms $(-1, -1)$ in $\mathfrak{S}$ are finitely many. Then from some rank on we only have subsequences $(1, -1, 1, 1, \dots, 1, -1, 1)$. By "doubling" such a subsequence (like at point b)), we produce

$$(-1, ?, 1, ?, -1, ?, -1, ?, \dots, ?, -1, ?, 1, ?, -1).$$

According with our assumption, all ?-terms ought to be 1, hence the produced subsequence is

$$(-1, 1, 1, 1, -1, 1, -1, 1, \dots, 1, -1, 1, 1, 1, -1),$$

and so the "separating packets" of 1's contain either one or three terms. Now assume some far enough $(1, 1, 1, 1)$ or $(-1, 1, 1, -1)$ subsequence of $\mathfrak{S}$ were to exist. Since it lies within some "doubled" subsequence, it contradicts the structure described above, which thus is the only prevalent from some rank on. But then all the positions of the $(-1)$-terms will have the same parity. However though, we have $\lambda(p) = \lambda(2p^2) = -1$ for all odd primes $p$, and these terms have different parity of their positions. A contradiction has been reached.[1)]

We have thus proved the existence in $\mathfrak{S}$ of infinitely many occurences of all possible subsequences of length 1, viz. $(1)$ and $(-1)$, and of length 2, viz. $(1, -1)$, $(-1, 1)$, $(1, 1)$ and $(-1, -1)$.[2)]

---

[1)] Using the same procedure for point e), we only need notice that $\lambda((2k+1)^2) = \lambda((2k)^2) = 1$, and these terms again are of different parity of their position.

[2)] Is this true for subsequences of all lengths $\ell = 3, 4$, etc.? If no, up to which length $\ell \geq 2$?

**Remark.** See Sloane's Online Encyclopædia of Integer Sequences (OEIS), sequence A001222 for $\Omega$ and sequence A008836 for $\lambda$, which is called Liouville's function. Its summatory function $\sum_{d|n} \lambda(d)$ is equal to 1 for a perfect square $n$, and 0 otherwise. Pólya conjectured that $L(n) := \sum_{k=1}^{n} \lambda(k) \leq 0$ for all $n$, but this has been proven false by Minoru Tanaka, who in 1980 computed that for $n = 906, 151, 257$ its value was positive. Turán showed that if $T(n) := \sum_{k=1}^{n} \frac{\lambda(k)}{k} \geq 0$ for all large enough $n$, that will imply Riemann's Hypothesis; however, Haselgrove proved it is negative infinitely often.

*Solution by Marian Tetiva.* Evidently, any of the parts e) and f) implies d); yet, part c) implies b), since if $S$ is ultimately periodic there exist $n_0 \in \mathbb{N}^*$ and $p \in \mathbb{N}^*$ such that $\lambda(n+p) = \lambda(n)$ for all $n \geq n_0$, therefore $S$ is constant over the arithmetic progression $(n_0 + kp)_{k \geq 1}$. So we will prove parts a), c), e), f) — in order f), a), e), c).

First, let $(u_k, v_k)$ be the general solution of the Pell equation $u^2 - 6v^2 = 1$, that is $u_k^2 - 6v_k^2 = 1$ for all $k \in \mathbb{N}$ ($u_0 = 1, v_0 = 0, u_1 = 5, v_1 = 2$ and so on; $u_k + v_k\sqrt{6} = (5 + 2\sqrt{6})^k$ for all $k$) and let $x_k = u_k + 2v_k$, $y_k = u_k + 3v_k$ for all $k \in \mathbb{N}$. We then have

$$3x_k^2 - 2y_k^2 = 3(u_k + 2v_k)^2 - 2(u_k + 3v_k)^2 = u_k^2 - 6v_k^2 = 1$$

for all $k \in \mathbb{N}$.

Consider $n_k = 2y_k^2$, hence $n_k + 1 = 3x_k^2$. Clearly, $\lambda(n_k) = \lambda(n_k + 1) = -1$ (as each of $2y_k^2$ and $3x_k^2$ has an odd number of prime factors), thus part f) is solved.

A similar argument with the solutions of the Pell equation $x^2 - 2y^2 = 1$ proves that there are infinitely many $n$ with $\lambda(n) = -1$ and $\lambda(n+1) = 1$ (take $n = 2y^2$, hence $n + 1 = x^2$, for such a solution $(x, y)$). On the other hand, with $n = x^2$ and $n + 1 = 2y^2$ for a solution $(x, y)$ of $x^2 - 2y^2 = -1$, we find infinitely many $n$ for which $\lambda(n) = 1$ and $\lambda(n+1) = -1$. This solves part a) (in two ways).

Now let $n_1 = 9$ and $n_{k+1} = 4n_k(n_k + 1)$. We have $\lambda(n_1) = \lambda(n_1 + 1) = 1$ and inductively we see that $\lambda(n_k) = \lambda(n_k + 1) = 1$. Indeed, if this is true for $k$, then it is true for $k + 1$, too, because $n_{k+1} = 4n_k(n_k + 1)$ has also an even number of prime factors (as $n_k$ and $n_{k+1}$ have), and $n_{k+1} + 1 = (2n_k + 1)^2$ obviously has an even number of prime of factors. This sequence $(n_k)_{k \geq 1}$ solves part e).

Now for part c) let us suppose by contradiction that there exist $a, b \in \mathbb{N}^*$ such that $\lambda(a + nb) = \lambda(a)$ for all $n \in \mathbb{N}$. Consider the greatest common divisor $d = \gcd(a, b)$ of $a$ and $b$, and let $a = da_1$, $b = db_1$ with $a_1$ and $b_1$ relatively prime positive integers. According to Dirichlet's theorem, there is an $s$ such that $a_1 + sb_1 = p$ is a prime, and from [1, Problem 16, Chapter 13] there exists $t$ such that $a_1 + tb_1 = qr$ is a product of two primes $q$ and $r$ (actually this is also an immediate consequence of Dirichlet's theorem). Then

$$\lambda(dp) = \lambda(d(a_1 + sb_1)) = \lambda(a + sb) = \lambda(a)$$

and $\lambda(dqr) = \lambda(d(a_1+tb_1)) = \lambda(a+tb) = \lambda(a)$, therefore $\lambda(dp) = \lambda(dqr)$, which is definitely false. Thus our assumption is wrong, and the sequence $S$ cannot be constant over any arithmetic progression. The problem is completely solved.

A slightly different form for the proof of this part can be found in [2].

## REFERENCES

[1] L. Panaitopol, A. Gica, *Probleme de aritmetică şi teoria numerelor. Idei şi metode de rezolvare*, Gil, 2006.

[2] P. Borwein, S. Choi and H. Ganguli, *Sign Changes of the Liouville Function on Quadratics*, available at `http://www.sfu.ca/~hganguli/papers/quadratic.pdf`

**333.** Show that there do not exist polynomials $P, Q \in \mathbb{R}[X]$ such that

$$\int\limits_0^{\log\log n} \frac{P(x)}{Q(x)}\mathrm{d}x = \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}, n \geq 1,$$

where $p_n$ is the $n$th prime number.

`Proposed by Cezar Lupu, Politehnica University of Bucharest, Bucharest, Romania, and Cristinel Mortici, Valahia University of Târgovişte, Târgovişte, Romania.`

*Solution by the authors.* Let us denote by $p_n$ the $n$th prime number. From the prime number theorem we know that

$$\pi(x) \sim \frac{x}{\log x}.$$

Now, if we put $x = p_n$, we have $n \sim \dfrac{p_n}{\log p_n}$ and by taking the logarithm we deduce $\log n \sim \log p_n - \log\log p_n$. On the other hand, we have

$$\frac{\log n}{\log p_n} \sim 1 - \frac{\log\log p_n}{\log p_n},$$

and since $\lim\limits_{x\to\infty} \dfrac{\log\log x}{\log x} = 0$, we finally obtain $\log n \sim \log p_n$. Combining this with the fact that $n \sim \dfrac{p_n}{\log p_n}$, we obtain that $p_n \sim n \log n$. It is obvious that the sequence $(P_n)_{n\geq 1}$ defined by

$$P_n = \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

diverges because $\sum\limits_{n=1}^{\infty} \dfrac{1}{p_n} \sim \sum\limits_{n=2}^{\infty} \dfrac{1}{n\log n}$, which is the celebrated Bertrand serie.

Now we shall prove that the sequence $(M_n)_{n\geq 2}$ defined by

$$M_n = P_n - \log\log n$$

is convergent. We have $M_{n+1} - M_n = \dfrac{1}{p_{n+1}} - (\log\log(n+1) - \log\log n)$. On the other hand, it is well-known that $p_n > n\log n, \forall n \geq 1$, and by the mean value theorem applied to the function $\log\log x$, we infer the inequality

$$\frac{1}{(n+1)\log(n+1)} < \log\log(n+1) - \log\log n < \frac{1}{n\log n}, \forall n \geq 1.$$

From these inequalities we derive that the sequence $M_n$ is strictly decreasing. However, as it is shown in [1], there exists $\lim\limits_{n\to\infty} M_n = B$, where $B$ is called the Brun constant.

We also have $M_n - M_{n-1} \sim -\dfrac{\log\log n}{n\log^2 n}$. One the other hand,

$$M_n - M_{n-1} = \int\limits_{\log\log(n-1)}^{\log\log n} \frac{P(x)}{Q(x)}\mathrm{d}x - (\log\log n - \log\log(n-1)).$$

By the mean value theorem, there exists $a_n \in (\log\log(n-1), \log\log n)$ such that

$$M_n - M_{n-1} = (\log\log n - \log\log(n-1))\left(\frac{P(a_n)}{Q(a_n)} - 1\right) \sim -\frac{\log\log n}{n\log^2 n},$$

which is equivalent to

$$n\log n(\log\log n - \log\log(n-1))\left(\frac{P(a_n)}{Q(a_n)} - 1\right) \sim -\frac{\log\log n}{\log n}.$$

But after some computations one finds

$$x_n = n\log n(\log\log n - \log\log(n-1)) \to 1$$

and $\dfrac{\log\log n}{\log n} \to 0$ as $n \to \infty$.

We obtain $\dfrac{P(a_n)}{Q(a_n)} \to 1$. Since $a_n \to \infty$ this implies that $\deg(P) = \deg(Q) =: p$ and, if $P(x) = \alpha_p x^p + \cdots + \alpha_1 x + \alpha_0$ and $Q(x) = \beta_p x^p + \cdots + \beta_1 x + \beta_0$, then $\alpha_p = \beta_p$. We finally obtain

$$x_n \cdot \frac{P_1(a_n)}{Q(a_n)} \sim -\frac{\log\log n}{\log n},$$

where $\deg(P_1) = r < p = \deg(Q)$ Therefore

$$y_n = x_n \cdot \frac{P_1(a_n)}{Q(a_n)} \cdot {a_n}^{p-r} \sim -\frac{(\log\log n)^{p-r+1}}{\log n} \cdot \left(\frac{a_n}{\log\log n}\right)^{p-r} = z_n.$$

Obviously $y_n \to 1 \cdot L \neq 0$ and $z_n \to -0 \cdot 1 = 0$, which gives a contradiction. The last limit follows from $\dfrac{(\log\log n)^{p-r+1}}{\log n} = \dfrac{u^{p-r+1}}{e^u} \to 0$ for $u = \log\log n \to \infty$.

## REFERENCES

[1] C. E. Froberg, *On the sum of inverses of prime and twin primes*, BIT Numerical Mathematics, **1**(1961), 15–20.

**334.** (Correction) Let $a$, $b$ be two positive integers with $a$ even and $b \equiv 3 \pmod 4$. Show that $a^m + b^m$ does not divide $a^n - b^n$ for any odd $m, n \geq 3$.

Proposed by Octavian Ganea, student École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland.

*Solution by the author.* Since $m$ is odd and $\geq 3$ we have $a^m + b^m \equiv 0 + 3 = = 3 \pmod 4$. It follows that $a^m + b^m$ has a prime factor $r \equiv 3 \pmod 4$.

We have $a^m \equiv -b^m \pmod r$ so $\left(\dfrac{a}{r}\right) = \left(\dfrac{a^m}{r}\right) = \left(\dfrac{-b^m}{r}\right) = -\left(\dfrac{b}{r}\right)$ because $r \equiv 3 \pmod 4$.

If $a^m + b^m \mid a^n - b^n$, then we also have $r \mid a^n - b^n$ and by the same reasoning as above we get $\left(\dfrac{a}{r}\right) = \left(\dfrac{b}{r}\right)$, a contradiction.

**335.** Let $m$ and $n$ be positive integers with $m \leq n$ and $A \in \mathcal{M}_{m,n}(\mathbb{R})$, $B \in \mathcal{M}_{n,m}(\mathbb{R})$ such that $\operatorname{rank} A = \operatorname{rank} B = m$. Show that there exists $C \in \mathcal{M}_n(\mathbb{R})$ such that $ACB = I_m$, where $I_m$ denotes the $m$ by $m$ unit matrix.

Proposed by Vasile Pop, Technical University Cluj-Napoca, Cluj-Napoca, Romania.

*Solution by Marian Tetiva.* If $m = n$ there is nothing to prove (just choose $C = A^{-1}B^{-1}$), so we consider further that $m < n$.

Let $P$ be an $n \times n$ permutation matrix such that the determinant of the submatrix of $AP$ with entries at the intersections of its $m$ rows and first $m$ columns is nonzero. Let $M$ be the $(n - m) \times n$ matrix consisting of two blocks as follows:

$$M = \begin{pmatrix} O_{n-m,m} & I_{n-m} \end{pmatrix}$$

and let $A_1$ be the $n \times n$ matrix

$$A_1 = \begin{pmatrix} AP \\ M \end{pmatrix}.$$

Using Binet's rule for computing determinants, one sees that $\det A_1 \neq 0$, hence $A_1$ is invertible in $M_n(\mathbb{R})$.

Similarly, because $B$ has rank $m$, there exists an $n \times n$ permutation matrix $Q$ such that $QB$ has a nonsingular submatrix with entries at the intersections of its first $m$ rows and its $m$ columns. Putting

$$N = \begin{pmatrix} O_{m,n-m} \\ I_{n-m} \end{pmatrix} \quad \text{and} \quad B_1 = \begin{pmatrix} QB & N \end{pmatrix},$$

one sees that $B_1$ is an invertible $n \times n$ matrix.

We consider $C_1 = A_1^{-1}B_1^{-1}$, thus we have

$$I_n = A_1C_1B_1 = \begin{pmatrix} AP \\ M \end{pmatrix} C_1 \begin{pmatrix} QB & N \end{pmatrix} = \begin{pmatrix} APC_1QB & APC_1N \\ MC_1QB & MC_1N \end{pmatrix},$$

whence (by reading the equality for the upper left $m \times m$ corner) $I_m = APC_1QB$ follows. Now, for $C = PC_1Q$ (which is an $n \times n$ matrix), we get $ACB = I_m$ and finish the proof.

**Remark.** The solution shows that we can find a matrix $C$ with the required property which is invertible.

**336.** (Correction) Show that the sequence $(a_n)_{n\geq 1}$ defined by

$$a_n = [2^n\sqrt{2}] + [2^n\sqrt{3}],\ n \geq 1,$$

contains infinitely many odd numbers and infinitely many even numbers. Here $[x]$ is the integer part of $x$.

Proposed by Marius Cavachi, Ovidius University of Constanţa, Constanţa, Romania.

*Solution by the author.* We write $\sqrt{2}$, $\sqrt{3}$ in base 2 as $\sqrt{2} = 0.x_1x_2\ldots$ and $\sqrt{3} = 0.y_1y_2\ldots$. Assume that there is an integer $N \geq 1$ such that $a_n$ is odd for $n \geq N$. Since in base 2 it holds $a_n = x_1\ldots x_n + y_1\ldots y_n$, we have $(x_n, y_n) \in$ $\in \{(0,1),(1,0)\}$ for $n \geq N$. It follows that the base 2 expansion of $\sqrt{2}+\sqrt{3}$ has the form $1.z_1\ldots z_{N-1}111\ldots$, so the number $\sqrt{2}+\sqrt{3}$ is rational, which is false.

Similarly, if we assume that $a_n$ is even for all sufficiently large $n$, we get $(x_n, y_n) \in \{(0,0),(1,1)\}$ for $n \geq N$. Therefore, the base 2 expansion of $\sqrt{3}-\sqrt{2}$ has the form $0.t_1\ldots t_{N-1}000\ldots$, whence $\sqrt{3}-\sqrt{2}$ is a rational number, which is not the case.

## ERRATUM

Unfortunately, the proposed problems in the 3-4/2011 issue of GMA were wrongly counted from 323 to 336, same as the problems from the previous issue. In fact they should have been counted from 337 to 350. Therefore a problem indexed as $n$ in the 3-4/2011 issue should be regarded as problem $n + 14$.