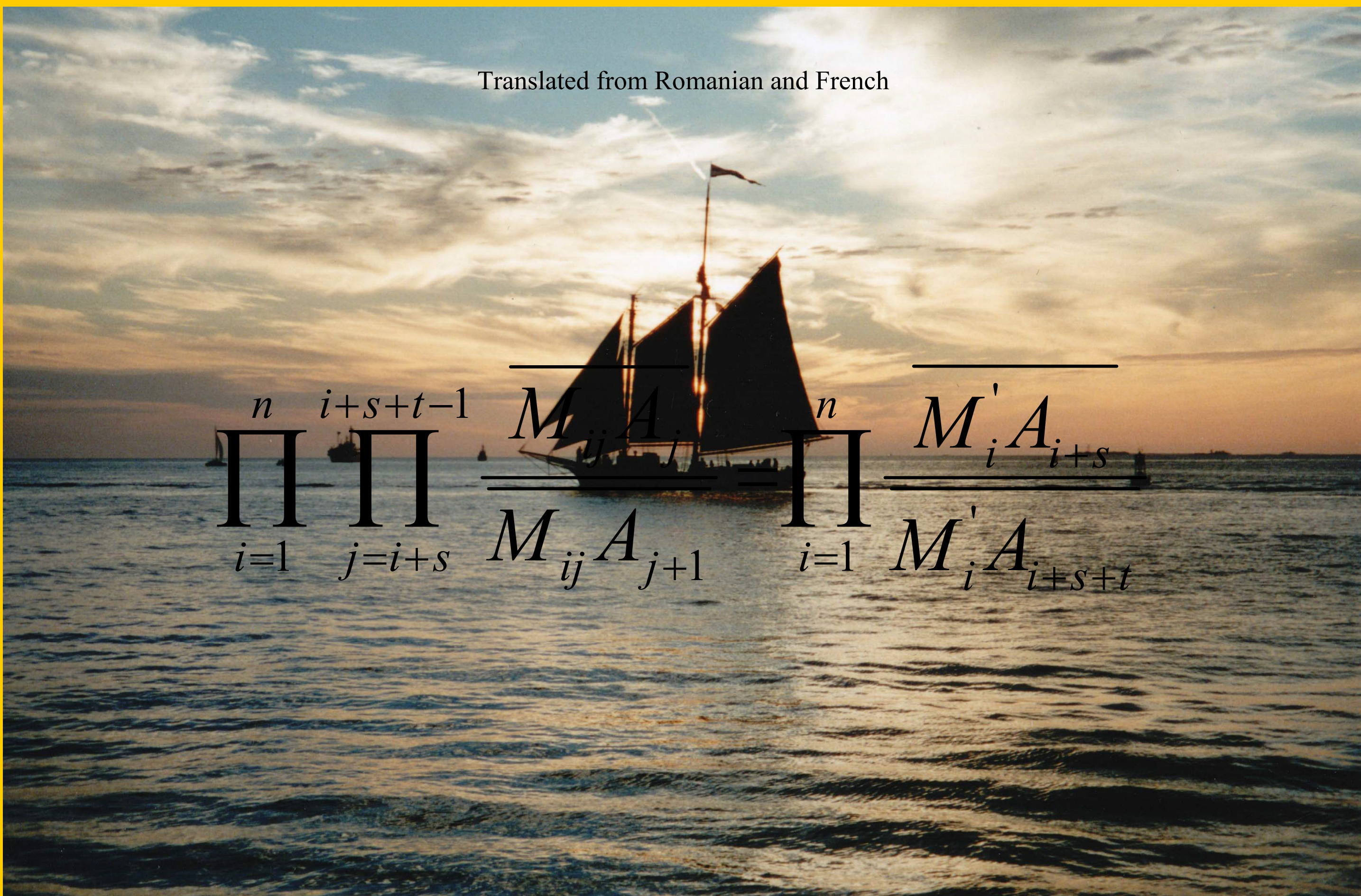
FLORENTIN SMARANDACHE

COLLECTED PAPERS, VOL. I

(SECOND EDITION)



ILQ

2007

Collected Papers, Vol. 1

(first edition 1996, second edition 2007)

Translated from Romanian and French into English

Florentin Smarandache, Ph D
Chair of Department of Mathematics & Sciences
University of New Mexico, Gallup, USA

ILQ

2007

This book can be ordered in a paper bound reprint from:

Books on Demand
ProQuest Information & Learning
(University of Microfilm International)
300 N. Zeeb Road
P.O. Box 1346, Ann Arbor
MI 48106-1346, USA
Tel.: 1-800-521-0600 (Customer Service)
http://wwwlib.umi.com/bod/basic

Many books can be downloaded from the following
Digital Library of Science:
http://www.gallup.unm.edu/~smarandache/eBooks-otherformats.htm

Peer Reviewers:

Prof. Mihaly Bencze, Department of Mathematics, Áprily Lajos College, Bra ov, Romania.

Dr. Sukanto Bhattacharya, Department of Business Administration, Alaska Pacific University, U.S.A.

Prof. Dr. Adel Helmy Phillips. Ain Shams University, 1 El-Sarayat st., Abbasia, 11517, Cairo, Egypt.

(ISBN-10): 1-59973-048-0
(ISBN-13): 978-1-59973-048-6
(EAN): 9781599730486
Printed in the United States of America

COLLECTED PAPERS[1]

(VOL. I, second edition)

(Articles, notes, generalizations, paradoxes, miscellaneous
in
Mathematics, Linguistics, and Education)

[1]Some papers not included in the volume were confiscated by the Secret Police in September 1988, when the author left Romania. He spent 19 months in a Turkish political refugee camp, and immigrated to the United States in March 1990. Despite the efforts of his friends, the papers were not recovered.

CONTENTS

A NUMERICAL FUNCTION IN CONGRUENCE THEORY

In this article we define a function L which will allow us to generalize (separately or simultaneously) some theorems from Numbers Theory obtained by Wilson, Fermat, Euler, Gauss, Lagrange, Leibnitz, Moser, Sierpinski.

§1. Let A be the set $\{m \in \mathbb{Z} | m = \pm p^\beta, \ \pm 2p^\beta$ with p an odd prime, $\beta \in N^*$, or $m = \pm 2^\alpha$ with $\alpha = 0,1,2$, or $m = 0\}$.

Let's consider $m = \varepsilon p_1^{\alpha_1} ... p_s^{\alpha_s}$, with $\varepsilon = \pm 1$, all $\alpha_i \in N^*$, and $p_1, ..., p_s$ distinct positive numbers.

We construct the FUNCTION $L : \mathbb{Z} \to \mathbb{Z}$,

$$L(x, m) = (x + c_1)...(x + c_{\varphi(m)})$$

where $c_1, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to m, and φ is the Euler's function.

If all distinct primes which divide x and m simultaneously are $p_{i_1} ... p_{i_r}$ then:

$$L(x, m) \equiv \pm 1 (\mathrm{mod}\, p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}),$$

when $m \in A$ respective by $m \notin A$, and

$$L(x, m) \equiv 0 (\mathrm{mod}\, m / (p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}})).$$

Noting $d = p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}$ and $m' = m / d$ we find:

$$L(x, m) \equiv \pm 1 + k_1^0 d \equiv k_2^0 m' (\mathrm{mod}\, m)$$

where k_1^0, k_2^0 constitute a particular integer solution of the Diophantine equation $k_2 m' - k_1 d = \pm 1$ (the signs are chosen in accordance with the affiliation of m to A).

This result generalizes the Gauss' theorem $(c_1, ..., c_{\varphi(m)} \equiv \pm 1 (\mathrm{mod}\, m))$ when $m \in A$ respectively $m \notin A$ (see [1]) which generalized in its turn the Wilson's theorem (if p is prime then $(p-1)! \equiv -1 (\mathrm{mod}\, m)$).

Proof.

The following two lemmas are trivial:

Lemma 1. If $c_1, ..., c_{\varphi(p^\alpha)}$ are all residues modulo p^α relatively prime to p^α, with p an integer and $\alpha \in N^*$, then for $k \in \mathbb{Z}$ and $\beta \in N^*$ we have also that $kp^\beta + c_1, ..., kp^\beta + c_{\varphi(p^\alpha)}$ constitute all residues modulo p^α relatively prime to it is sufficient to prove that for $1 \le i \le \varphi(p^\alpha)$ we have that $kp^\beta + c_i$ is relatively prime to p^α, but this is obvious.

Lemma 2. If $c_1, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to m, $p_i^{\alpha_i}$ divides m and $p_i^{\alpha_i + 1}$ does not divide m, then $c_1, ..., c_{\varphi(m)}$ constitute $\varphi(m / p_i^{\alpha_i})$ systems of all residues modulo $p_i^{\alpha_i}$ relatively prime to $p_i^{\alpha_i}$.

Lemma 3. If $c_1,...,c_{\varphi(m)}$ are all residues modulo q relatively prime to q and $(b,q)\sim 1$ then $b+c_1,...,b+c_{\varphi(q)}$ contain a representative of the class $\hat{0}$ modulo q.

Of course, because $(b,q-b)\sim 1$ there will be a $c_{i_0}=q-b$ whence $b+c_i=\mathcal{M}_q$.

From this we have the following:

Theorem 1. If $\left(x,m/\left(p_{i_1}^{\alpha_{i_1}}...p_{i_s}^{\alpha_{i_s}}\right)\right)\sim 1$,

then

$$(x+c_1)...(x+c_{\varphi(m)})\equiv 0\left(\operatorname{mod} m/\left(p_{i_1}^{\alpha_{i_1}}...p_{i_r}^{\alpha_{i_r}}\right)\right).$$

Lemma 4. Because $c_1,...,c_{\varphi(m)}\equiv \pm 1(\operatorname{mod} m)$ it results that $c_1,...,c_{\varphi(m)}\equiv \pm 1(\operatorname{mod} p_i^{\alpha_i})$, for all i, when $m\in A$ respectively $m\notin A$.

Lemma 5. If p_i divides x and m simultaneously then:

$$(x+c_1)...(x+c_{\varphi(m)})\equiv \pm 1(\operatorname{mod} p_i^{\alpha_i}),$$

when $m\in A$ respectively $m\notin A$. Of course, from the lemmas 1 and 2, respectively 4 we have:

$$(x+c_1)...(x+c_{\varphi(m)})\equiv c_1,...,c_{\varphi(m)}\equiv \pm 1(\operatorname{mod} p_i^{\alpha_i}).$$

From the lemma 5 we obtain the following:

Theorem 2. If $p_{i_1},...,p_{i_r}$ are all primes which divide x and m simultaneously then:

$$(x+c_1)...(x+c_{\varphi(m)})\equiv \pm 1(\operatorname{mod} p_{i_1}^{\alpha_{i_1}}...p_{i_r}^{\alpha_{i_r}}),$$

when $m\in A$ respectively $m\notin A$.

From the theorems 1 and 2 it results:

$$L(x,m)\equiv \pm 1+k_1 d=k_2 m',$$

where $k_1,k_2\in\mathbb{Z}$. Because $(d,m')\sim 1$ the Diophantine equation $k_2m'-k_1d=\pm 1$ admits integer solutions (the unknowns being k_1 and k_2). Hence $k_1=m't+k_1^0$ and $k_2=dt+k_2^0$, with $t\in\mathbb{Z}$, and k_1^0, k_2^0 constitute a particular integer solution of our equation. Thus:

$$L(x,m)\equiv \pm 1+m'dt+k_1^0 d=\pm 1+k_1^0(\operatorname{mod} m)$$

or

$$L(x,m)=k_2^0 m'(\operatorname{mod} m).$$

§2. APPLICATIONS

1) Lagrange extended Wilson's theorem in the following way: "If p is prime then

$$x^{p-1}-1\equiv (x+1)(x+2)...(x+p-1)(\operatorname{mod} p)".$$

We shall extend this result as follows: whichever are $m \neq 0, \pm 4$, we have for $x^2 + s^2 \neq 0$ that

$$x^{\varphi(m_s)+s} - x^s \equiv (x+1)(x+2)...(x+|m|-1)(\mathrm{mod}\, m)$$

where m_s and s are obtained from the algorithm:

$$(0)\qquad \begin{cases} x = x_0 d_0; \ \ (x_0, m_0) \sim 1 \\ m = m_0 d_0; \ d_0 \neq 1 \end{cases}$$

$$(1)\qquad \begin{cases} d_0 = d_0^1 d_1; \ \ (d_0^1, m_1) \sim 1 \\ m_0 = m_1 d_1; \ d_1 \neq 1 \end{cases}$$

……………………………………..

$$(s\text{-}1)\qquad \begin{cases} d_{s-2} = d_{s-2}^1 d_{s-1}; \ \ (d_{s-2}^1, m_{s-1}) \sim 1 \\ m_{s-2} = m_{s-1} d_{s-1}; \ d_{s-1} \neq 1 \end{cases}$$

$$(s)\qquad \begin{cases} d_{s-1} = d_{s-1}^1 d_s; \ \ (d_{s-1}^1, m_s) \sim 1 \\ m_{s-1} = m_s d_s; \ \ d_s \neq 1 \end{cases}$$

(see [3] or [4]). For m positive prime we have $m_s = m$, $s = 0$, and $\varphi(m) = m-1$, that is Lagrange.

2) L. Moser enunciated the following theorem: If p is prime then $(p-1)!a^p + a = \mathcal{M}\, p$", and Sierpinski (see [2], p. 57): if p is prime then $a^p + (p-1)!a = \mathcal{M}\, p$" which merge the Wilson's and Fermat's theorems in a single one.

The function L and the algorithm from §2 will help us to generalize that if "a" and m are integers $m \neq 0$ and $c_1, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to m then

$$c_1, ..., c_{\varphi(m)} a^{\varphi(m_s)+s} - L(0,m)a^s = \mathcal{M}\, m,$$

respectively

$$-L(0,m)a^{\varphi(m_s)+s} + c_1, ..., c_{\varphi(m)} a^s = \mathcal{M}\, m$$

or more:

$$(x+c_1)...(x+c_{\varphi(m)})a^{\varphi(m_s)+s} - L(x,m)a^s = \mathcal{M}\, m$$

respectively

$$-L(x,m)a^{\varphi(m_s)+s} + (x+c_1)...(x+c_{\varphi(m)})a^s = \mathcal{M}\, m$$

which reunite Fermat, Euler, Wilson, Lagrange and Moser (respectively Sierpinski).

3) A partial spreading of Moser's and Sierpinski's results, the author also obtained (see [6], problem 7.140, pp. 173-174), the following: if m is a positive integer, $m \neq 0$,4. and "a" is an integer, then $(a^m - a)(m-1)! = \mathcal{M}\, m$, reuniting Fermat and Wilson in another way.

4) Leibnitz enunciated that: ”If p is prime then $(p-2)! \equiv 1 (\bmod p)$" ”;

We consider ”$c_i < c_{i+1} (\bmod m)$” if $c_i^{'} < c_{i+1}^{'}$ where $0 \le c_i^{'} < |m|$, $0 \le c_{i+1}^{'} < |m|$, and $c_i \equiv c_i^{'} (\bmod m)$, $c_{i+1} \equiv c_{i+1}^{'} (\bmod m)$ it seems simply that $c_1, c_2, ..., c_{\varphi(m)}$ are all residues modulo m relatively prime to $m(c_i < c_{i+1} (\bmod m))$ for all $i, m \ne 0$, then $c_1, c_2, ..., c_{\varphi(m)-1} \equiv \pm (\bmod m)$ if $m \in A$ respectively $m \notin A$, because $c_{\varphi(m)} \equiv -1 (\bmod m)$.

REFERENCES:

[1] Lejeune-Dirichlet - Vorlesungen über Zahlentheorie” - 4[te] Auflage, Braunschweig, 1894, §38.

[2] Sierpinski, Waclaw, - Ce ştim şi ce nu ştim despre numerele prime - Ed. Stiinţifică, Bucharest, 1966.

[3] Smarandache, Florentin, - O generalizare a teoremei lui Euler referitoare la congruenţă - Bulet. Univ. Braşov, seria C, Vol. XXIII, pp. 7-12, 1981; see Mathematical Reviews: 84J:10006.

[4] Smarandache, Florentin - Généralisations et généralités - Ed. Nouvelle, Fés, Morocco, pp. 9-13, 1984.

[5] Smarandache, Florentin - A function in the number theory – An. Univ. Timişoara, seria şt. mat., Vol. XVIII, fasc. 1, pp. 79-88, 1980; see M. R.: 83c:10008.

[6] Smarandache, Florentin - Problèmes avec et sans…problèmes! - Somipress, Fés, Morocco, 1983; see M. R.: 84K:00003.

[Published in ”Libertas Mathematica», University of Texas, Arlington, Vol. XII, 1992, pp. 181-185]

A GENERAL THEOREM FOR THE CHARACTERIZATION OF N PRIME NUMBERS SIMULTANEOUSLY

§1. ABSTRACT. This article presents a necessary and sufficient theorem as N numbers, coprime two by two, to be prime simultaneously.

It generalizes V. Popa's theorem [3], as well as I. Cucurezeanu's theorem ([1], p.165), Clement's theorem, S. Patrizio's theorems [2], etc.

Particularly, this General Theorem offers different characterizations for twin primes, for quadruple primes, etc.

§2. INTRODUCTION. It is evident the following:

Lemma 1. Let A, B be nonzero integers. Then:

$$AB \equiv 0 (\mathrm{mod}\, pB) \Leftrightarrow A \equiv 0 (\mathrm{mod}\, p) \Leftrightarrow A / p \text{ is an integer.}$$

Lemma 2.Let $(p,q) \sim 1$, $(a,p) \sim 1$, $(b,q) \sim 1$.

Then:

$$A \equiv 0 (\mathrm{mod}\, p)$$

and

$$B \equiv 0 (\mathrm{mod}\, q) \Leftrightarrow aAq + bBp \equiv 0 (\mathrm{mod}\, pq) \Leftrightarrow aA + bBp / q \equiv 0 (\mathrm{mod}\, p)$$

$$aA / p + bB / q \text{ is an integer.}$$

Proof:

The first equivalence:

We have $A = K_1 p$ and $B = K_2 q$ with $K_1, K_2 \in \mathbb{Z}$ hence

$$aAq + bBp = (aK_1 + bK_2) pq .$$

Reciprocal: $aAq + bBp = Kpq$, with $K \in \mathbb{Z}$ it rezults that $aAq \equiv 0 (\mathrm{mod}\, p)$ and $bBp \equiv 0 (\mathrm{mod}\, q)$, but from our assumption we find $A \equiv 0 (\mathrm{mod}\, p)$ and $B \equiv 0 (\mathrm{mod}\, q)$.

The second and third equivalence results from lemma1.

By induction we extend this lemma to the following:

Lemma 3. Let $p_1, ..., p_n$ be coprime integers two by two, and let $a_1, ..., a_n$ be integer numbers such that $(a_i, p_i) \sim 1$ for all i. Then

$$A_1 \equiv 0 (\mathrm{mod}\, p_1), ..., A_n \equiv 0 (\mathrm{mod}\, p_n) \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=1}^{n} a_i A_i \prod_{j \neq i} p_j \equiv 0 (\mathrm{mod}\, p_1 ... p_n) \Leftrightarrow$$

$$\Leftrightarrow (P / D) \cdot \sum_{i=1}^{n} (a_i A_i / p_i) \equiv 0 (\mathrm{mod}\, P / D) ,$$

where $P = p_1 ... p_n$ and D is a divisor of p $\Leftrightarrow \sum_{i=1}^{n} a_i A_i / p_i$ is an integer.

§3. From this last lemma we can find immediately a GENERAL THEOREM:

Let $P_{ij}, 1 \le i \le n, 1 \le j \le m_i$, be coprime integers two by two, and let $r_1, ..., r_n, a_1, ..., a_n$ be integer numbers such that a_i be coprime with r_i for all i.

The following conditions are considered:

(i) $p_{i_1}, ..., p_{in_1}$, are simultaneously prime if and only if $c_i \equiv 0(\bmod r_i)$, for all i.

Then:

The numbers $p_{ij}, 1 \le i \le n, 1 \le j \le m_i$, are simultaneously prime if and only if

$$(*) \qquad (R/D)\sum_{i=1}^{n}(a_i c_i / r_i) \equiv 0(\bmod R/D),$$

where $P = \prod_{i=1}^{n} r_i$ and D is a divisor of R.

Remark:

Often in the conditions (i) the module r_i is equal to $\prod_{j=1}^{m_i} p_{ij}$, or to a divisor of it, and in this case the relation of the General Theorem becomes:

$$(P/D)\sum_{i=1}^{n}(a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \equiv 0(\bmod P/D)$$

where

$$P = \prod_{i,j=1}^{n,m_i} p_{ij} \text{ and } D \text{ is a divisor of } P.$$

Corollaries:

We easily obtain that our last relation is equivalent with:

$$\sum_{i=1}^{n}(a_i c_i (P / \prod_{j=1}^{m_i} p_{ij}) \equiv 0(\bmod P),$$

and

$$\sum_{i=1}^{n}(a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \text{ is an integer,}$$

etc.

The imposed restrictions for the numbers p_{ij} from the General Theorem are very wide, because if there would be two uncoprime distinct numbers, then at least one from these would not be prime, hence the $m_1 + ... + m_n$ numbers might not be prime.

The General Theorem has many variants in accordance with the assigned values for the parameters $a_1, ..., a_n$ and $r_1, ..., r_m$, the parameter D, as well as in accordance with the congruences $c_1, ..., c_n$ which characterize either a prime number or many other prime numbers simultaneously. We can start from the theorems (conditions c_i) which characterize a single prime number (see Wilson, Leibnitz, F. Smarandache [4], or Siminov (p is prime if and only if $(p-k)!(k-1)!-(-1)^k \equiv 0(\mathrm{mod}\, p)$, when $p \geq k \geq 1$; here, it is preferable to take $k=[(p+1)/2]$, where $[x]$ represents the gratest integer number $\leq x$, in order that the number $(p-k)!(k-1)!$ be the smallest possibly) for obtaining, by means of the General Theorem, conditions $c_j^{'}$, which characterize many prime numbers simultaneously. Afterwards, from the conditions $c_i, c_j^{'}$, using the General Theorem again, we find new conditions $c_h^{''}$ which characterize prime numbers simultaneously. And this method can be continued analogically.

Remarks

Let $m_i = 1$ and c_i represent the Simionov's theorem for all i

(a) If $D=1$ it results in V. Popa's theorem, which generalizes in the Cucurezeanu's theorem and the last one generalizes in its turn Clement's theorem!

(b) If $D = P / p_2$ and choosing convenintly the parameters a_i, k_i for $i = 1,2,3$, it results in S. Patrizio's theorem.

Several Examples:

1. Let $p_1, p_2, ..., p_n$ be positive integers >1, coprime integers two by two, and $1 \leq k_i \leq p_i$ for all i. Then $p_1, p_2, ..., p_n$ are simultaneously prime if and only if:

(T) $$\sum_{i=1}^{n}\left[(p_i-k_i)!(k_i-1)!-(-1)^{k_i}\right]\cdot\prod_{j\neq i} p_i \equiv 0(\mathrm{mod}\, p_1 p_2 ... p_n)$$

or

(U) $$\sum_{i=1}^{n}\left[(p_i-k_i)!(k_i-1)!-(-1)^{k_i}\right]\cdot\prod_{j\neq i} p_i / (p_{s+1}...p_n) \equiv 0(\mathrm{mod}\, p_1 ... p_s)$$

or

(V) $$\sum_{i=1}^{n}\left[(p_i-k_i)!(k_i-1)!-(-1)^{k_i}\right]\cdot p_j / p_i \equiv 0(\mathrm{mod}\, p_j)$$

or

(W) $$\sum_{i=1}^{n}\left[(p_i-k_i)!(k_i-1)!-(-1)^{k_i}\right]\cdot p_j / p_i$$ is an integer.

2. Another relation example (using the first theorem form [4]: p is a prime positive integer if and only if $(p-3)!-(p-1)/2 \equiv 0(\mathrm{mod}\, p)$

$$\sum_{i=1}^{n}\left[(p_i-3)!-(p_i-1)/2\right]\cdot p_1 / p_i \equiv 0(\mathrm{mod}\, p_1)$$

3. The odd numbers … and … are twin prime if and only if: $(p-1)!(3p+2)+2p+2 \equiv 0(\bmod p(p+2))$
   or
   $(p-1)!(p+2)-2 \equiv 0(\bmod p(p+2))$
   or
   $\left[(p-1)!+1\right]/p+\left[(p-1)!2+1\right]/(p+2)$ is an integer.
   These twin prime characterzations differ from Clement's theorem $((p-1)!4+p+4 \equiv 0(\bmod p(p+2)))$

4. Let $(p, p+k) \sim 1$ then: p and $p+k$ are prime simultaneously if and only if

$$(p-1)!(p+k)+(p+k-1)!p+2p+k \equiv 0(\bmod p(p+k)),$$

which differs from I. Cucurezeanu's theorem ([1], p. 165):

$$k \cdot k!\left[(p-1)!+1\right]+\left[K!-(-1)^k\right]p \equiv 0(\bmod p(p+k))$$

5. Look at a characterization of a quadruple of primes for

$p, p+2, p+6, p+8$:

$$\left[(p-1)!+1\right]/p+\left[(p-1)!2!+1\right]/(p+2)+\left[(p-1)!6!+1\right]/(p+6)+\left[(p-1)!8!+1\right]/(p+8)$$

be an integer.

6. For $p-2, p, p+4$ coprime integers tw by two, we find the relation:

$$(p-1)!+p\left[(p-3)!+1\right]/(p-2)+p\left[(p+3)!+1\right]/(p+4) \equiv -1(\bmod p),$$

which differ from S. Patrizio's theorem

$$\left(8\left[(p+3)!/(p+4)\right]+4\left[(p-3)!/(p-2)\right] \equiv -11(\bmod p)\right).$$

References

[1] Cucuruzeanu, I – Probleme de aritmetică şi teoria numerelor, Ed. Tehnică, Bucharest, 1966.

[2] Patrizio, Serafino – Generalizzazione del teorema di Wilson alle terne prime - Enseignement Math., Vol. 22(2), nr. 3-4, pp. 175-184, 1976.

[3] Popa, Valeriu – Asupra unor generalizări ale teoremei lui Clement - Studii şi Cercetări Matematice, Vol. 24, nr. 9, pp. 1435-1440, 1972.

[4] Smarandache, Florentin – Criterii ca un număr natural să fie prim - Gazeta Matematică, nr. 2, pp. 49-52; 1981; see Mathematical Reviews (USA): 83a:10007.

[Presented at the 15th American Romanian Academy Annual Convention, which was held in Montréal, Québec, Canada, from June 14-18, 1990, at École Polytechnique de Montréal. Published in ”Libertas Mathemaica”, University of Texas, Alington, Vol. XI, 1991, pp. 151-5]

A METHOD TO SOLVE THE DIOPHANTINE EQUATION

$ax^2 - by^2 + c = 0$

ABSTRACT

We consider the equation

(1) $ax^2 - by^2 + c = 0$, with $a, b \in \mathbb{N}^*$ and $c \in \mathbb{Z}^*$.

It is a generalization of the Pell's equation: $x^2 - Dy^2 = 1$. Here, we show that: if the equation has an integer solution and $a \cdot b$ is not a perfect square, then (1) has an infinitude of integer solutions; in this case we find a closed expression for (x_n, y_n), the general positive integer solution, by an original method. More, we generalize it for any Diophantine equation of second degree and with two unknowns.

INTRODUCTION

If $ab = k^2$ is a perfect square ($k \in \mathbb{N}$) the equation (1) has at most a finite number of integer solutions, because (1) become:

(2) $(ax - ky)(ax + ky) = -ac$

If (a, b) does not divide c, the Diophantine equation does not have solutions.

METHOD TO SOLVE. Suppose that (1) has many integer solutions. Let (x_0, y_0), (x_1, y_1) be the smallest positive integer solutions for (1), with $0 \le x_0 < x_1$. We construct the recurrent sequences:

$$(3) \qquad \begin{cases} x_{n+1} = \alpha x_n + \beta y_n \\ y_{n+1} = \gamma x_n + \delta y_n \end{cases}$$

making condition (3) verify (1). It results:

$$\begin{cases} a\alpha\beta = b\gamma\delta & (4) \\ a\alpha^2 - b\gamma^2 = a & (5) \\ a\beta^2 - b\delta^2 = -b & (6) \end{cases}$$

having the unknowns $\alpha, \beta, \gamma, \delta$.

We pull out $a\alpha^2$ and $a\beta^2$ from (5), respectively (6), and replace them in (4) at the square; we obtain

$$a\delta^2 - b\gamma^2 = a \qquad (7).$$

We subtract (7) from (5) and find:

$$\alpha = \pm\delta \qquad (8).$$

Replacing (8) in (4) we obtain:

$$\beta = \pm\frac{b}{a}\gamma \qquad (9).$$

Afterwards, replacing (8) in (5), and (9) in (6) we find the same equation:

$$a\alpha^2 - b\gamma^2 = a \quad (10).$$

Because we work with positive solutions only, we take

$$\begin{cases} x_{n+1} = a_0 x_n + \frac{b}{a}\gamma_0 y_n \\ y_{n+1} = \gamma_0 x_n + \alpha_0 y_n \end{cases}$$

where (a_0, γ_0) is the smallest, positive integer solution of (10) such that $a_0\gamma_0 \neq 0$.

Let $\begin{pmatrix} \alpha_0 & \frac{b}{a}\gamma_0 \\ \gamma_0 & \alpha_0 \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. It is evident that if (x', y') is an integer solution for (1) then $A\begin{pmatrix} x' \\ y' \end{pmatrix}$, $A^{-1}\begin{pmatrix} x' \\ y' \end{pmatrix}$ is another one – where A^{-1} is the inverse matrix of A, i.e. $A^{-1} \cdot A = A \cdot A^{-1} = I$ (unit matrix). Hence, if (1) has an integer solution it has an infinity. (Clearly $A^{-1} \in \mathcal{M}_2(\mathbb{Z})$).

The **general positive integer solution** of the equation (1) is:

$$(x_n', y_n') = \left(|x_n|, |y_n|\right)$$

$$(GS_1) \text{ with } \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}, \text{ for all } n \in \mathbb{Z},$$

where by convention $A^0 = I$ and $A^{-k} = A^{-1} ... A^{-1}$ of k times.

In problems it is better to write (GS) as:

$$\begin{pmatrix} x_n' \\ y_n' \end{pmatrix} = A^n \cdot \begin{pmatrix} x_0 \\ y_0 \end{pmatrix}, \quad n \in \mathbb{N}$$

$$(GS_2) \text{ and } \begin{pmatrix} x_n'' \\ y_n'' \end{pmatrix} = A^n \cdot \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \quad n \in \mathbb{N}^*$$

We prove, by reduction at absurdum that (GS_2) is a general positive integer solution for (1).

Let (u, v) be a positive integer particular solution for (1). If $\exists k_0 \in \mathbb{N} : (u, v) = A^{k_0}\begin{pmatrix} x_0 \\ y_0 \end{pmatrix}$, or $\exists k_1 \in \mathbb{N}^* : (u, v) = A^{k_1}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ then $(u, v) \in (GS_2)$. Contrary to this, we calculate $(u_{i+1}, v_{i+1}) = A^{-1}\begin{pmatrix} u_i \\ v_i \end{pmatrix}$, for $i = 0, 1, 2, ...$ where $u_0 = u$, $v_0 = v$. Clearly $u_{i+1} < u_i$ for all i. After a certain rank $x_0 < u_{i_0} < x_1$ it finds either $0 < u_{i_0} < x_0$, but that is absurd.

It is clear that we can put

$$(GS_3) \quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_0 \\ \varepsilon y_0 \end{pmatrix}, \quad n \in \mathbb{N}, \text{ where } \varepsilon = \pm 1.$$

Now we shall transform the general solution (GS_3) in a closed expression.

Let λ be a real number. $Det(A-\lambda\cdot I)=0$ involves the solutions $\lambda_{1,2}$ and the proper vectors $V_{1,2}$ (i.e., $Av_i=\lambda_i v_i$, $i\in\{1,2\}$). Note $P=\begin{pmatrix} v_1 \\ v_2 \end{pmatrix}^i \in \mathcal{M}_2(\mathbb{R})$

Then $P^{-1}AP=\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, whence $A^n=P\begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}P^{-1}$, and replacing it in (GS_3) and doing the computations we find a closed expression for (GS_3).

EXAMPLES

1. For the Diophantine equation $2x^2-3y^2=5$ we obtain

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix}=\begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix}^n\cdot\begin{pmatrix} 2 \\ \varepsilon \end{pmatrix},\ n\in\mathbb{N} \text{ and } \lambda_{1,2}=5\pm 2\sqrt{6},\ v_{1,2}=(\sqrt{6},\pm 2),$$

whence a closed expression for x_n and y_n:

$$\begin{cases} x_n=\dfrac{4+\varepsilon\sqrt{6}}{4}(5+2\sqrt{6})^n+\dfrac{4-\varepsilon\sqrt{6}}{4}(5-2\sqrt{6})^n \\ y_n=\dfrac{3\varepsilon+2\sqrt{6}}{6}(5+2\sqrt{6})^n+\dfrac{3\varepsilon-2\sqrt{6}}{6}(5-2\sqrt{6})^n \end{cases} \quad \text{for all } n\in\mathbb{N}$$

2. For equation $x^2-3y^2-4=0$ the general solution in positive integer is:

$$\begin{cases} x_n=(2+\sqrt{3})^n+(2-\sqrt{3})^n \\ y_n=\dfrac{1}{\sqrt{3}}(2+\sqrt{3})^n+(2-\sqrt{3})^n \end{cases} \quad \text{for all } n\in\mathbb{N},$$

that is (2,0), (4,2), (14,8), (52,30),…

EXERCICES FOR RADERS:

Solve the Diophantine equations:

3. $x^2-12y^2+3=0$

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix}=\begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n\cdot\begin{pmatrix} 3 \\ \varepsilon \end{pmatrix}=?,\ n\in\mathbb{N}$]

4. $x^2-6y^2-10=0$

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix}=\begin{pmatrix} 5 & 12 \\ 2 & 5 \end{pmatrix}^n\cdot\begin{pmatrix} 4 \\ \varepsilon \end{pmatrix}=?,\ n\in\mathbb{N}$]

5. $x^2-12y^2-9=0$

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix}=\begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n\cdot\begin{pmatrix} 3 \\ \varepsilon \end{pmatrix}=?,\ n\in\mathbb{N}$]

6. $14x^2-3y^2-18=0$

GENERALIZATIONS

If $f(x,y)=0$ is a Diophantine equation of second degree and with two unknowns, by linear transformation it becomes

(12) $ax^2+by^2+c=0$, with $a,b,c\in\mathbb{Z}$.

If $ab\geq 0$ the equation has at most a finite number of integer solutions which can be found by attempts.

It is easier to present an example:

7. The Diophantine equation

(13) $9x^2+6xy-13y^2-6x-16y+20=0$ becomes

(14) $2u^2-7v^2+45=0$, where

(15) $u=3x+y-1$ and $v=2y+1$

We solve (14). Thus:

$$(16)\ \begin{cases} u_{n+1}=15u_n+28v_n \\ v_{n+1}=8u_n+15v_n \end{cases},\quad n\in\mathbb{N} \text{ with } (u_0,v_0)=(3,3\varepsilon)$$

First solution:

By induction we prove that for all $n\in\mathbb{N}$ we have that v_n is odd, and u_n as well as v_n are multiple of 3. Clearly $v_0=3\varepsilon,\ u_0$. For $n+1$ we have: $v_{n+1}=8u_n+15v_n=even+odd=odd$, and of course u_{n+1},v_{n+1} are multiples of 3 because u_n,v_n are multiple of 3 too.

Hence, there exist x_n,y_n in positive integers for all $n\in\mathbb{N}$:

$$(17)\ \begin{cases} x_n=(2u_n-v_n+3)/6 \\ y_n=\qquad (v_n-1)/2 \end{cases}$$

(from (15)). Now we'll find the $\left(GS_3\right)$ for (14) as closed expression, and by means of (17) it results the general integer solution of the equation (13).

Second solution:

Another expression of the $\left(GS_3\right)$ for (13) will be obtained if we transform (15) as $u_n=3x_n+y_n-1$ and $v_n=2y_n+1$ for all $n\in\mathbb{N}$. Whence, using (16) and doing the computation, we find

$$(18)\ \begin{cases} x_{n+1}=11x_n+11x_n+\dfrac{52}{3}y_n+\dfrac{11}{3} \\ y_{n+1}=12x_n+19y_n+3 \end{cases}\quad n\in\mathbb{N}\ \text{, with } (x_0,y_0)=(1,1) \text{ or } (2,-2)$$

(two infinitude of integer solutions).

Let $A=\begin{pmatrix} 11 & \frac{52}{3} & \frac{11}{3} \\ 12 & 19 & 3 \\ 0 & 0 & 1 \end{pmatrix}$, then $\begin{pmatrix} x_n \\ y_n \\ 1 \end{pmatrix}=A^n\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ or

(19) $\begin{pmatrix} x_n \\ y_n \\ 1 \end{pmatrix} = A^n \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$, always $n \in \mathbb{N}$.

From (18) we have always $y_{n+1} \equiv y_n \equiv ... \equiv y_0 \equiv 1 (\bmod 3)$, hence always $x_n \in \mathbb{Z}$. Of course, (19) and (17) are equivalent as general integer solution for (13).

[The reader can calculate A^n (by the same method liable to the start on this note) and find a closed expression for (19).].

More generally:

This method can be generalized for the Diophantine equations:

(20) $\sum_{i=1}^{n} a_i X_i^2 = b$, with all $a_i, b \in \mathbb{Z}$.

If always $a_i a_j \geq 0,\ 1 \leq i < j \leq n$, the equation (20) has at most a finite number of integer solutions.

Now, we suppose $\exists i_0, j_0 \in \{1,...,n\}$ for which $a_{i_0} a_{j_0} < 0$ (the equation presents at least a variation of sign). Analogously, for $n \in \mathbb{N}$, we define the recurrent sequences:

(21) $x_h^{(n+1)} = \sum_{i=1}^{n} \alpha_{ih} x_i^{(n)}$, $1 \leq h \leq n$

considering $(x_1^0, ..., x_n^0)$ the smallest positive integer solution of (20). Replacing (21) in (20), it identifies the coefficients and it looks for n^2 unknowns α_{ih}, $1 \leq, i, h \leq n$. (This calculation is very intricate, but it can be done by means of a computer.) The method goes on similarly, but the calculations become more and more intricate – for example to calculate A^n, one must use a computer.

(The reader will be able to try this for the Diophantine equation $ax^2 + by^2 - cz^2 + d = 0$, with $a, b, c \in \mathbb{N}^*$ and $d \in \mathbb{Z}$)

REFERENCES

[1] M. Bencze - Applicații ale unor şiruri de recurență în teoria ecuațiilor Diophantine - Gamma (Braşov), XXI-XXII, Anul VII, Nr. 4-5, 1985, pp. 15-18.

[2] Z. I. Borevich, I.R. Shafarevich - Teoria numerelor - EDP, Bucharest, 1985.

[3] A. Kenstam - Contributions to the Theory of the Diophantine Equations $Ax^2 - By^2 = C$”.

[4] G. H. Hardy and E. M. Wright - Introduction to the theory of numbers - Fifth edition, Clarendon Press, Oxford, 1984.

[5] N. Ivăşchescu - Rezolvarea ecuațiilor în numere întregi - This is his work for obtaining the title of professor grade 2, (coordinator G. Vraciu), Univ. Craiova, 1985.

[6] E. Landau - Elementary Number Theory - Chelsea, 1955.

[7] Calvin T. Long - Elementary Introduction to Number Theory - D. C. Heath, Boston, 1965.
[8] L. J. Mordell - Diophantine equations - London, Academia Press, 1969.
[9] C. Stanley Ogibvy, John T. Anderson - Excursions in number theory - Oxford University Press, New York, 1966.
[10] W. Sierpinski - Oeuvres choisiers - Tome I, Warszawa, 1974-1976.
[11] F. Smarandache - Sur la resolution d'équation du second degré a dex inconnues dans Z in the book "Généralizations et généralités" – Ed. Nouvelle, Fes, Marocco; MR: 85, H: 00003.

[Published in "Gazeta Matematică", Serie 2, Vol. 1, Nr. 2, 1988, pp. 151-7; Translated in Spanish by Francisco Bellot Rasado, "Un metodo de resolucion de la ecuacion diofantica", Madrid.

SOME STATIONARY SEQUENCES

§1. Define a sequence $\{a_n\}$ by $a_1 = a$ and $a_{n+1} = P(a_n)$, where P is a polynomial with real coefficients. For which a values, and for which P polynomials will this sequence be constant after a certain rank?

In this note, the author answers this question using as reference F. Lazebnik & Y. Pilipenko's E 3036 problem from A. M. M., Vol. 91, No. 2/1984, p. 140.

An interesting property of functions admitting fixed points is obtained.

§2. Because $\{a_n\}$ is constant after a certain rank, it results that $\{a_n\}$ converges. Hence, $(\exists)e \in \mathbb{R}: \ e = P(e)$, that is the equation $P(x) - x = 0$ admits real solutions. Or P admits fixed points $((\exists)x \in \mathbb{R}: \ P(x) = x)$.

Let $e_1, ..., e_m$ be all real solutions of this equation. It constructs the recurrent set E as follows:

1) $e_1, ..., e_m \in E$;

2) if $b \in E$ then all real solutions of the equation $P(x) = b$ belong to E;

3) no other element belongs to E, then the obtained elements from the rule 1) or 2), applying for a finite number of times these rules.

We prove that this set E, and the set A of the "a" values for which $\{a_n\}$ becomes constant after a certain rank are indistinct, "$E \subseteq A$".

1) If $a = e_i, \ 1 \le i \le m$, then $(\forall)n \in \mathbb{N}^* \quad a_n = e_i = \text{constant}$.

2) If for $a = b$ the sequence $a_1 = b, \ a_2 = P(b)$ becomes constant after a certain rank, let x_0 be a real solution of the equation $P(x) - b = 0$, the new formed sequence: $a_1^{'} = x_0, \ a_2^{'} = P(x_0) = b, \ a_3^{'} = P(b)...$ is indistinct after a certain rank with the first one, hence it becomes constant too, having the same limit.

3) Beginning from a certain rank, all these sequences converge towards the same limit e (that is: they have the same e value from a certain rank) are indistinct, equal to e.

"$A \le E$"

Let "a" be a value such that: $\{a_n\}$ becomes constant (after a certain rank) equal to e. Of course $e \in \{e_1, ..., e_m\}$ because $e_1, ..., e_m$ are the single values towards these sequences can tend.

If $a \in \{e_1, ..., e_m\}$, then $a \in E$.

Let $a \notin \{e_1, ..., e_m\}$, then $(\exists)n_0 \in \mathbb{N}: \ a_{n_0+1} = P(a_{n_0}) = e$, hence we obtain a applying the rules 1) or 2) a finite number of times. Therefore, because $e \in \{e_1, ..., e_m\}$ and the equation $P(x) = e$ admits real solutions we find a_{n_0} among the real solutions of this equation: knowing a_{n_0} we find a_{n_0-1} because the equation $P(a_{n_0-1}) = a_{n_0}$ admits real solutions (because $a_{n_0} \in E$ and our method goes on until we find $a_1 = a$ hence $a \in E$.

Remark. For $P(x) = x^2 - 2$ we obtain the E 3036 Problem (A. M. M.).

Here, the set E becomes equal to

$$\{\pm 1, 0, \pm 2\} \cup \left\{ \underbrace{\pm\sqrt{2 \pm \sqrt{2 \pm \sqrt{\ldots \pm 2}}}}_{n_0 \ times}, \ \ n \in \mathbb{N}^* \right\} \cup \left\{ \underbrace{\pm\sqrt{2 \pm \sqrt{\ldots \sqrt{2 \pm \sqrt{3}}}}}_{n_0 \ times}, \ \ n \in \mathbb{N} \right\}.$$

Hence, for all $a \in E$ the sequence $a_1 = a,\ a_{n+1} = a_n^2 - 2$ becomes constant after a certain rank, and it converges (of course) towards –1 or 2:

$$(\exists) n_0 \in \mathbb{N}^* :\ (\forall) n \geq n_0 \qquad a_n = -1$$

or

$$(\exists) n_0 \in \mathbb{N}^* :\ (\forall) n \geq n_0 \qquad a_n = 2\,.$$

[Published in “Gamma”, Brasov, XXIII, Anul VIII, No. 1, October 1985, pp. 5-6.]

ON CARMICHAËL'S CONJECTURE

Carmichaël's conjecture is the following: "the equation $\varphi(x) = n$ cannot have a unique solution, $(\forall)n \in \mathbb{N}$, where φ is the Euler's function". R. K. Guy presented in [1] some results on this conjecture; Carmichaël himself proved that, if n_0 does not verify his conjecture, then $n_0 > 10^{37}$; V. L. Klee [2] improved to $n_0 > 10^{400}$, and P. Masai & A. Valette increased to $n_0 > 10^{10000}$. C. Pomerance [4] wrote on this subject too.

In this article we prove that the equation $\varphi(x) = n$ admits a finite number of solutions, we find the general form of these solutions, also we prove that, if x_0 is the unique solution of this equation (for a $n \in \mathbb{N}$), then x_0 is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$ (and $x_0 > 10^{10000}$ from [3]).

§1. Let x_0 be a solution of the equation $\varphi(x) = n$. We consider n fixed. We'll try to construct another solution $y_0 \neq x_0$.

The first method:

We decompose $x_0 = a \cdot b$ with a, b integers such that $(a, b) = 1$.

we look for an $a' \neq a$ such that $\varphi(a') = \varphi(a)$ and $(a', b) = 1$; it results that $y_0 = a' \cdot b$.

The second method:

Let's consider $x_0 = q_1^{\beta_1} ... q_r^{\beta_r}$, where all $\beta_i \in \mathbb{N}^*$, and $q_1, ..., q_r$ are distinct primes two by two; we look for an integer q such that $(q, x_0) = 1$ and $\varphi(q)$ divides $x_0 / (q_1, ..., q_r)$; then $y_0 = x_0 q / \varphi(q)$.

We immediately see that we can consider q as prime.

The author conjectures that for any integer $x_0 \geq 2$ it is possible to find, by means of one of these methods, a $y_0 \neq x_0$ such that $\varphi(y_0) = \varphi(x_0)$.

Lemma 1. The equation $\varphi(x) = n$ admits a finite number of solutions, $(\forall)n \in \mathbb{N}$.

Proof. The cases $n = 0, 1$ are trivial.

Let's consider n to be fixed, $n \geq 2$. Let $p_1 < p_2 < ... < p_s \leq n+1$ be the sequence of prime numbers. If x_0 is a solution of our equation (1) then x_0 has the form $x_0 = p_1^{\alpha_1} ... p_s^{\alpha_s}$, with all $\alpha_i \in \mathbb{N}$. Each α_i is limited, because:

$$(\forall)i \in \{1, 2, ..., s\},\ (\exists)a_i \in \mathbb{N} : p_i^{\alpha_i} \geq n.$$

Whence $0 \leq \alpha_i \leq a_i + 1$, for all i. Thus, we find a wide limitation for the number of solutions: $\prod_{i=1}^{s} (a_i + 2)$

Lemma 2. Any solution of this equation has the form (1) and (2):

$$x_0 = n \cdot \left(\frac{p_1}{p_1 - 1} \right)^{\varepsilon_1} \dots \left(\frac{p_s}{p_s - 1} \right)^{\varepsilon_s} \in \mathbb{Z} \;,$$

where, for $1 \le i \le s$, we have $\varepsilon_i = 0$ if $\alpha_i = 0$, or $\varepsilon_i = 1$ if $\alpha_i \ne 0$.

Of course, $n = \varphi(x_0) = x_0 \left(\frac{p_1}{p_1 - 1} \right)^{\varepsilon_1} \dots \left(\frac{p_s}{p_s - 1} \right)^{\varepsilon_s}$,

whence it results the second form of x_0.

From (2) we find another limitation for the number of the solutions: $2^s - 1$ because each ε_i has only two values, and at least one is not equal to zero.

§2. We suppose that x_0 is the unique solution of this equation.

Lemma 3. x_0 is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$.

Proof. We apply our second method.

Because $\varphi(0) = \varphi(3)$ and $\varphi(1) = \varphi(2)$ we take $x_0 \ge 4$.

If $2 \nmid x_0$ then there is $y_0 = 2x_0 \ne x_0$ such that $\varphi(y_0) = \varphi(x_0)$, hence $2 \mid x_0$; if $4 \nmid x_0$, then we can take $y_0 = x_0 / 2$.

If $3 \nmid x_0$ then $y_0 = 3x_0 / 2$, hence $3 \mid x_0$; if $9 \nmid x_0$ then $y_0 = 2x_0 / 3$, hence $9 \mid x_0$; whence $4 \cdot 9 \mid x_0$.

If $7 \nmid x_0$ then $y_0 = 7x_0 / 6$, hence $7 \mid x_0$; if $49 \nmid x_0$ then $y_0 = 6x_0 / 7$ hence $49 \mid x_0$; whence $4 \cdot 9 \cdot 49 \mid x_0$.

If $43 \nmid x_0$ then $y_0 = 43x_0 / 42$, hence $43 \mid x_0$; if $43^2 \nmid x_0$ then $y_0 = 42x_0 / 43$, hence $43^2 \mid x_0$; whence $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2 \mid x_0$.

Thus $x_0 = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 7^{\gamma_3} \cdot 43^{\gamma_4} \cdot t$, with all $\gamma_i \ge 2$ and $(t,\ 2 \cdot 3 \cdot 7 \cdot 43) = 1$ and $x_0 > 10^{10000}$ because $n_0 > 10^{10000}$.

§3. Let's consider $\gamma_l \ge 3$. If $5 \nmid x_0$ then $5x_0 / 4 = y_0$, hence $5 \mid x_0$; if $25 \nmid x_0$ then $y_0 = 4x_0 / 5$, whence $25 \mid x_0$.

We construct the recurrent set M of prime numbers:

a) the elements $2, 3, 5 \in M$;
b) if the distinct odd elements $e_1, \dots, e_n \in M$ and $b_m = 1 + 2^m \cdot e_1, \dots, e_n$ is prime, with $m = 1$ or $m = 2$, then $b_m \in M$;
c) any element belonging to M is obtained by the utilization (a finite number of times) of the rules a) or b) only.

The author conjectures that M is infinite, which solves this case, because it results that there is an infinite number of primes which divide x_0. This is absurd.

For example 2, 3, 5, 7, 11, 13, 23, 29, 31, 43, 47, 53, 61, … belong to M.

*

The method from §3 could be continued as a tree (for $\gamma_2 \geq 3$ afterwards $\gamma_3 \geq 3$, etc.) but its ramifications are very complicated…

REFERENCES

[1] R. K. Guy - Monthly unsolved problems - 1969-1983. Amer. Math. Monthly, Vol. 90, No. 10/1983, p. 684.

[2] V. L. Klee - Amer. Math. Monthly 76, (969), p. 288.

[3] P. Masai & A. Valette - A lower bound for a counter-example to Carmichaël's conjecture - Boll. Unione Mat. Ital, (6) A_1 (1982), pp. 313-316.

[4] C. Pomerance - Math. Reviews: 49:4917.

[Published in "Gamma", XXIV, Year VIII, No. 2, February 1986, pp. 13-14.]

A PROPERTY FOR A COUNTEREXAMPLE TO CARMICHAËL'S CONJECTURE

Carmichaël has conjectured that:
$(\forall)\ n \in \mathbb{N}$, $(\exists)\ m \in \mathbb{N}$, with $m \neq n$, for which $\varphi(n) = \varphi(m)$, where φ is Euler's totient function.

There are many papers on this subject, but the author cites the papers which have influenced him, especially Klee's papers.

Let n be a counterexample to Carmichaël's conjecture.

Grosswald has proved that n is a multiple of 32, Donnelly has pushed the result to a multiple of 2^{14}, and Klee to a multiple of $2^{42} \cdot 3^{47}$, Smarandache has shown that n is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$. Masai & Valette have bounded $n > 10^{10000}$.

In this note we will extend these results to: n is a multiple of a product of a very large number of primes.

We construct a recurrent set M such that:

a) the elements $2, 3 \in M$;

b) if the distinct elements $2, 3, q_1, ..., q_r \in M$ and $p = 1 + 2^a \cdot 3^b \cdot q_1 \cdots q_r$ is a prime, where $a \in \{0, 1, 2, ..., 41\}$ and $b \in \{0, 1, 2, ..., 46\}$, then $p \in M$; $r \geq 0$;

c) any element belonging to M is obtained only by the utilization (a finite number of times) of the rules a) or b).

Of course, all elements from M are primes.

Let n be a multiple of $2^{42} \cdot 3^{47}$;

if $5 \nmid n$ then there exists $m = 5n/4 \neq n$ such that $\varphi(n) = \varphi(m)$; hence $5 \mid n$; whence $5 \in M$;

if $5^2 \nmid n$ then there exists $m = 4n/5 \neq n$ with our property; hence $5^2 \mid n$;

analogously, if $7 \nmid n$ we can take $m = 7n/6 \neq n$, hence $7 \mid n$; if $7^2 \nmid n$ we can take $m = 6n/7 \neq n$; whence $7 \in M$ and $7^2 \mid n$; etc.

The method continues until it isn't possible to add any other prime to M, by its construction.

For example, from the 168 primes smaller than 1000, only 17 of them do not belong to M (namely: 101, 151, 197, 251, 401, 491, 503, 601, 607, 677, 701, 727, 751, 809, 883, 907, 983); all other 151 primes belong to M.

Note $M = \{2, 3, p_1, p_2, ..., p_s, ...\}$, then n is a multiple of $2^{42} \cdot 3^{47} \cdot p_1^2 \cdot p_2^2 \cdots p_s^2 \cdots$ From our example, it results that M contains at least 151 elements, hence $s \geq 149$.

If M is infinite then there is no counterexample n, whence Carmichaël's conjecture is solved.

(The author conjectures M is infinite.)

Using a computer it is possible to find a very large number of primes, which divide n, using the construction method of M, and trying to find a new prime p if $p - 1$ is a product of primes only from M.

REFERENCES

[1] R. D. Carmichaël - Note on Euler's ϕ function - Bull. Amer. Math. Soc. 28(1922), pp. 109-110.
[2] H. Donnelly - On a problem concerning Euler's phi-function - Amer. Math. Monthly, 80(1973), pp. 1029-1031.
[3] E. Grosswald - Contribution to the theory of Euler's function $\phi(x)$ - Bull. Amer. Math. Soc., 79(1973), pp. 337-341.
[4] R. K. Guy - Monthly Research Problems - 1969-1973, Amer. Math. Monthly 80(1973), pp. 1120-1128.
[5] R. K. Guy - Monthly Research Problems - 1969-1983, Amer. Math. Monthly 90(1983), pp. 683-690.
[6] R. K. Guy - Unsolved Problems in Number Theory - Springer-Verlag, 1981, problem B 39, 53.
[7] V. L. Klee - On a conjecture of Carmichaël - Bull. Amer. Math. Soc 53 (1947), pp. 1183-1186.
[8] V. L. Klee - Is there a n for which $\phi(x)$ has a unique solution? - Amer. Math. Monthly. 76(1969), pp. 288-289.
[9] P. Masai et A. Valette - A lower bound for a counterexample to Carmichaël's conjecture - Boll. Unione Mat. Ital. (6) A1(1982), pp. 313-316.
[10] F. Gh. Smarandache - On Carmichaël's conjecture - Gamma, Braşov, XXIV, Year VIII, 1986.

[Published in "Gamma", XXV, Year VIII, No. 3, June 1986, pp. 4-5.]

ON DIOPHANTINE EQUATION $X^2 = 2Y^4 - 1$

Abstract: In this note we present a method of solving this Diophantine equation, method which is different from Ljunggren's, Mordell's, and R.K.Guy's.

In his book of unsolved problems Guy shows that the equation $x^2 = 2y^4 - 1$ has, in the set of positive integers, the only solutions (1,1) and (239,13); (Ljunggren has proved it in a complicated way). But Mordell gave an easier proof.

We'll note $t = y^2$. The general integer solution for $x^2 - 2t^2 + 1 = 0$ is

$$\begin{cases} x_{n+1} = 3x_n + 4t_n \\ t_{n+1} = 2x_n + 3t_n \end{cases}$$

for all $n \in \mathbb{N}$, where $(x_0, y_0) = (1, \varepsilon)$, with $\varepsilon = \pm 1$ (see [6]) or

$$\begin{pmatrix} x_n \\ t_n \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ \varepsilon \end{pmatrix},$$ for all $n \in \mathbb{N}$, where a matrix to the power zero is equal to the unit matrix I.

Let's consider $A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$, and $\lambda \in \mathbb{R}$. Then $\det(A - \lambda \cdot I) = 0$ implies $\lambda_{1,2} = 3 \pm \sqrt{2}$, whence if v is a vector of dimension two, then: $Av = \lambda_{1,2} \cdot v$.

Let's consider $P = \begin{pmatrix} 2 & 2 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}$ and $D = \begin{pmatrix} 3+2\sqrt{2} & 0 \\ 0 & 3-2\sqrt{2} \end{pmatrix}$. We have $P^{-1} \cdot A \cdot P = D$, or

$$A^n = P \cdot D^n \cdot P^{-1} = \begin{pmatrix} \frac{1}{2}(a+b) & \frac{\sqrt{2}}{2}(a-b) \\ \frac{\sqrt{2}}{4}(a-b) & \frac{1}{2}(a+b) \end{pmatrix},$$

where $a = \left(3+2\sqrt{2}\right)^n$ and $b = \left(3-2\sqrt{2}\right)^n$.

Hence, we find:

$$\begin{pmatrix} x_n \\ t_n \end{pmatrix} = \begin{pmatrix} \frac{1+\varepsilon\sqrt{2}}{2}\left(3+2\sqrt{2}\right)^n + \frac{1-\varepsilon\sqrt{2}}{2}\left(3-2\sqrt{2}\right)^n \\ \frac{2\varepsilon+\sqrt{2}}{4}\left(3+2\sqrt{2}\right)^n + \frac{2\varepsilon-\sqrt{2}}{4}\left(3-2\sqrt{2}\right)^n \end{pmatrix}, \quad n \in \mathbb{N}.$$

Or $y_n^2 = \frac{2\varepsilon+\sqrt{2}}{4}\left(3+2\sqrt{2}\right)^n + \frac{2\varepsilon-\sqrt{2}}{4}\left(3-2\sqrt{2}\right)^n, \quad n \in \mathbb{N}$.

For $n = 0,\ \varepsilon = 1$ we obtain $y_0^2 = 1$ (whence $x_0^2 = 1$), and for $n = 3,\ \varepsilon = 1$ we obtain $y_3^2 = 169$ (whence $x_3 = 239$).

(1) $$y_n^2 = \varepsilon \sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{n}{2k} \cdot 3^{n-2k} 2^{3k} + \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2k+1} \cdot 3^{n-2k-1} 2^{3k+1}$$

We still must prove that y_n^2 is a perfect square if and only if $n = 0, 3$.

We can use a similar method for the Diophantine equation $x^2 = Dy^4 \pm 1$, or more generally: $C \cdot X^{2a} = DY^{2b} + E$, with $a, b \in \mathbb{N}^*$ and $C, D, E \in \mathbb{Z}^*$; denoting $X^a = U$, $Y^b = V$, and applying the results from F.S. [6], the relation (1) becomes very complicated.

REFERENCES

[1] J. H. E. Cohn - The Diophantine equation $y^2 = Dx^4 + 1$ - Math. Scand. 42 (1978), pp. 180-188, MR 80a: 10031.

[2] R. K. Guy - Unsolved Problems in Number Theory - Springer-Verlag, 1981, Problem D6, 84-85.

[3] W. Ljunggren - Zur Theorie der Gleichung $x^2 + 1 = Dy^4$ - Avh. Norske Vid. Akad., Oslo, I, 5(1942), #pp. 5-27; MR 8, 6.

[4] W. Ljunggren - Some remarks on the Diophantine equation $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$ - J. London Math. Soc. 41(1966), 542-544, MR 33 #5555.

[5] L. J. Mordell, The Diophantine equation $y^2 = Dx^4 + 1$, J. London Math. Soc. 39(1964, 161-164, MR 29#65.

[6] F. Smarandache - A Method to solve Diophantine Equations of two unknowns and second degree - "Gazeta Matematică", 2nd Series, Volume 1, No. 2, 1988, pp. 151-7; translated into Spanish by Francisco Bellot Rosado.
http://xxx.lanl.gov/pdf/math.GM/0609671.

[Published in "Gamma, Anul IX, November 1986, No.1, p. 12]

ON AN ERDÖS' OPEN PROBLEMS

In one of his books ("Analysis…") Mr. Paul Erdös proposed the following problem:

"The integer n is called a barrier for an arithmetic function f if $m + f(m) \leq n$ for all $m < n$.

Question: Are there infinitely many barriers for $\varepsilon v(n)$, for some $\varepsilon > 0$? Here $v(n)$ denotes the number of distinct prime factors of n."

We found some results regarding this question, which results make us to conjecture that there is a finite number of barriers, for all $\varepsilon > 0$.

Let $R(n)$ be the relation: $m + \varepsilon v(m) \leq n, \ \forall m < n$.

Lemma 1. If $\varepsilon > 1$ there are two barriers only: $n = 1$ and $n = 2$ (which we call trivial barriers).

Proof. It is clear for $n = 1$ and $, n = 2$ because $v(0) = v(1) = 0$.

Let's consider $n \geq 3$. Then, if $m = n - 1$ we have $m + \varepsilon v(m) \geq n - 1 + \varepsilon > n$, contradiction.

Lemma 2. There is an infinity of numbers which cannot be barriers for $\varepsilon v(n)$, $\forall \varepsilon > 0$.

Proof. Let's consider $s, k \in \mathbb{N}^*$ such that $s \cdot \varepsilon > k$. We write n in the form $n = p_{i_1}^{\alpha_{i_1}} \cdots p_{i_s}^{\alpha_{i_s}} + k$, where for all j, $\alpha_{i_j} \in \mathbb{N}^*$ and p_{i_j} are positive distinct primes.

Taking $m = n - k$ we have $m + \varepsilon v(m) = n - k + \varepsilon \cdot s > n$.

But there exists an infinity of n's because the parameters $\alpha_{i_1}, ..., \alpha_{i_s}$ are arbitrary in $\mathbb{N}^*$ and $p_{i_1}, ..., p_{i_s}$ are arbitrary positive distinct primes, also there is an infinity of couples (s, k) for an $\varepsilon > 0$, fixed , with the property $s \cdot \varepsilon > k$.

Lemma 3. For all $\varepsilon \in (0,1]$ there are nontrivial barriers for $\varepsilon v(n)$.

Proof. Let t be the greatest natural number such that $t\varepsilon \leq 1$ (always there is such t).

Let n be from $[3, ..., p_1 \cdots p_t p_{t+1})$, where $\{p_i\}$ is the sequence of the positive primes. Then $1 \leq v(n) \leq t$.

All $n \in [1, ..., p_1 \cdots p_t p_{t+1}]$ is a barrier, because: $\forall \ 1 \leq k \leq n - 1$, if $m = n - k$ we have $m + \varepsilon v(m) \leq n - k + \varepsilon \cdot t \leq n$.

Hence, there are at list $p_1 \cdots p_t p_{t+1}$ barriers.

Corollary. If $\varepsilon \to 0$ then n (the number of barriers) $\to \infty$.

Lemma 4. Let's consider $n \in [1,..., p_1 \cdots p_r p_{r+1}]$ and $\varepsilon \in (0,1]$. Then: n is a barrier if and only if $R(n)$ is verified for $m \in \{n-1, n-2,..., n-r+1\}$.

Proof. It is sufficient to prove that $R(n)$ is always verified for $m \le n-r$.

Let's consider $m = n - r - u$, $u \ge 0$. Then $m + \varepsilon v(m) \le n - r - u + \varepsilon \cdot r \le n$.

Conjecture.

We note $I_r \in [p_1 \cdots p_r, ..., \cdot p_1 \cdots p_r p_{r+1})$. Of course $\bigcup_{r \ge 1} I_r = \mathbb{N} \setminus \{0,1\}$, and $I_{r_1} \cap I_{r_2} = \Phi$ for $r_1 \ne r_2$.

Let $\mathcal{N}_r(1+t)$ be the number of all numbers n from I_r such that $1 \le v(n) \le t$.

We conjecture that there is a finite number of barriers for $\varepsilon v(n)$, $\forall \varepsilon > 0$; because

$$\lim_{r \to \infty} \frac{\mathcal{N}_r(1+t)}{p_1 \cdots p_{r+1} - p_1 \cdots p_r} = 0$$

and the probability (of finding of $r-1$ consecutive values for m, which verify the relation $R(n)$) approaches zero.

ON ANOTHER ERDÖS' OPEN PROBLEM

Paul Erdös has proposed the following problem:

(1) "Is it true that $\lim_{n\to\infty} \max_{m<n}(m+d(m))-n=\infty$?, where $d(m)$ represents the number of all positive divisors of m."

We clearly have :

Lemma 1. $(\forall)n\in\mathbb{N}\setminus\{0,1,2\}$, $(\exists)!s\in\mathbb{N}^*$, $(\exists)!\alpha_1,...,\alpha_s\in\mathbb{N}$, $\alpha_s\neq 0$, such that $n=p_1^{\alpha_1}\cdots p_s^{\alpha_s}+1$, where $p_1,p_2,...$ constitute the increasing sequence of all positive primes.

Lemma 2. Let $s\in\mathbb{N}^*$. We define the subsequence $n_s(i)=p_1^{\alpha_1}\cdots p_s^{\alpha_s}+1$, where $\alpha_1,...,\alpha_s$ are arbitrary elements of $\mathbb{N}$, such that $\alpha_s\neq 0$ and $\alpha_1+...+\alpha_s\to\infty$ and we order it such that $n_s(1)<n_s(2)<...$ (increasing sequence).

We find an infinite number of subsequences $\{n_s(i)\}$, when s traverses $\mathbb{N}^*$, with the properties:

a) $\lim_{i\to\infty} n_s(i)=\infty$ for all $s\in\mathbb{N}^*$.

b) $\{n_{s_1}(i),\ i\in\mathbb{N}^*\}\cap\{n_{s_2}(j),\ j\in\mathbb{N}^*\}=\Phi$, for $s_1\neq s_2$ (distinct subsequences).

c) $\mathbb{N}\setminus\{0,1,2\}=\bigcup_{s\in\mathbb{N}^*}\{n_s(i),\ i\in\mathbb{N}^*\}$

Then:

Lemma 3. If in (1) we calculate the limit for each subsequence $\{n_s(i)\}$ we obtain:

$$\lim_{n\to\infty}\left(\max_{m<p_1^{\alpha_1}\cdots p_s^{\alpha_s}}(m+d(m))-p_1^{\alpha_1}\cdots p_s^{\alpha_s}-1\right)\geq \lim_{n\to\infty}\left(p_1^{\alpha_1}\cdots p_s^{\alpha_s}+(\alpha_1+1)...(\alpha_s+1)-p_1^{\alpha_1}\cdots p_s^{\alpha_s}-1\right)=$$

$$=\lim_{n\to\infty}\left((\alpha_1+1)...(\alpha_s+1)-1\right)>\lim_{n\to\infty}\left(\alpha_1+...+\alpha_s\right)=\infty$$

From these lemmas it results the following:

Theorem: We have $\overline{\lim_{n\to\infty}}\max_{m<n}(m+d(m))-n=\infty$.

REFERENCES

[1] P. Erdös - Some Unconventional Problems in Number Theory - Mathematics Magazine, Vol. 57, No.2, March 1979.

[2] P. Erdös - Letter to the Author - 1986: 01: 12.

[Published in "Gamma", XXV, Year VIII, No. 3, June 1986, p. 5]

METHODS FOR SOLVING LETTER SERIES

Letter series problems occur in many American tests for measuring quantitative ability of supervisory personnel.

They are more difficult than number-series used for measuring mathematical ability because are unusual and complex.

According to the English alphabetic order:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

as well as to the a given sequence of letters, the equation consists of finding letters of the sequence which obey same rules.

For example, let $b\ d\ f\ h\ j\ \ldots$ be a given sequence; find the next two letters in this series.

Of course they are $l\ n$ because the letters are taken two by two from the alphabet: $b\ \cancel{c}\ d\ \cancel{e}\ f\ \cancel{g}\ h\ \cancel{i}\ j\ \cancel{k}\ \underline{l}\ \cancel{m}\ \underline{n}$.

In order to solve easier letter –series we transform them into number-series, and in this case it's simpler to use some well-known mathematical procedures.

Method I.

Associate to each letter from the alphabet a number in this way:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Sample: d c i h n m … becomes $\underline{4, 3}$; $\underline{\underline{9, 8}}$; $\underline{\underline{\underline{14, 13}}}\ldots$, whence the next two numbers will be 19, 18, i.e. $s\ r$

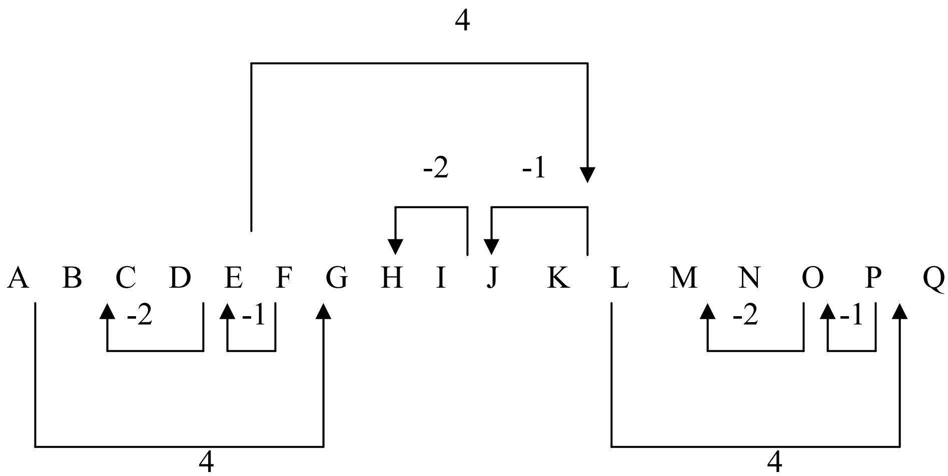
Method II.

Let $\mathcal{O}(\mathcal{L})$ be the order of the letter $\mathcal{L}$ in the above succession. For example $\mathcal{O}$(F)=6, $\mathcal{O}$(S)=19, etc.

According to the given sequence associate the number zero (0) to its first letter, for the second one the difference between second letter's order and first letter's order,

Sample: $b\ f\ e\ c\ g\ k\ j\ h\ \ldots$ becomes $\underline{0}$, $\underbrace{4,\ -1,\ -2}$; $\underbrace{4,\ -1,\ -2}$;..., whence the next numbers will be $4;\ 4, -1,\ -2$; equivalent to $l\ p\ o\ m$.

See the rule:



REFERENCE

Passbooks for career opportunities, computer Aptitude Test (CAT), ew York, 1983, National Learning Corporation.

GENERALIZATION OF AN ER'S MATRIX METHOD FOR COMPUTING

Er's matrix method for computing Fibonacci numbers and their sums can be extended to the s-additive sequence:

$$g_{-s+1} = g_{-s+2} = \ldots = g_{-1} = 0\,,\ \ g_0 = 1\,,$$

and

$$g_n = \sum_{i=1}^{s} g_{n-i} \ \text{ for } n > 0\,.$$

For example, if we note $S_n = \sum_{j=1}^{n-1} g_j$, we define two $(s+1)\times(s+1)$ matrixes such that:

$$B_n = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ S_n & g_n & g_{n-1} & \ldots & g_{n-s+2} & g_{n-s+1} \\ : & : & : & \ldots & : & : \\ S_{n-s+1} & g_{n-s+1} & g_{n-s} & \ldots & g_{n-2s+3} & g_{n-2s+2} \end{bmatrix},$$

$n \geq 1$, and

$$M = \begin{bmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & 1 & 1 & \ldots & 0 \\ : & : & : & \ldots & : \\ 1 & 1 & 0 & \ldots & 1 \\ 1 & 1 & 0 & \ldots & 0 \end{bmatrix},$$

thus, we have analogously:

$$B_{n+1} = M^{n+1},\ M^{r+c} = M^r \cdot M^c\,,$$

whence

$$S_{r+c} = S_r + g_r S_c + g_{r-1} S_{c-1} + \ldots + g_{r-s+1} S_{c-s+1}\,,$$
$$g_{r+c} = g_r g_c + g_{r-1} g_{c-1} + \ldots + g_{r-s+1} g_{c-s+1}\,,$$

and for $r = c = n$ it results:

$$S_{2n} = S_n + g_n S_n + g_{n-1} S_{n-1} + \ldots + g_{n-s+1} S_{n-s+1}\,,$$
$$g_{2n} = g_n^2 + g_{n-1}^2 + \ldots + g_{n-s+1}^2\,;$$

for $r = n$, $c = n-1$, we find:

$$g_{2n-1} = g_n g_{n-1} + g_{n-1} g_{n-2} + \ldots + g_{n-s+1} g_{n-s}\,, \text{ etc.}$$
$$S_{2n-1} = S_n + g_n S_{n-1} + g_{n-1} S_{n-2} + \ldots + g_{n-s+1} S_{n-s}$$

Whence we can construct a similar algorithm as M. C. Er for computing s-additive numbers and their sums.

REFERENCE:

M. C. Er, Fast Computation of Fibonacci Numbers and Their Sums, J. Inf. Optimization Sci. (Delhi), Vol. 6 (1985), No. 1. pp. 41-47.

[Published in "GAMMA", Braşov, Anul X, No.. 1-2, October 1987, p. 8]

ON A THEOREM OF WILSON

§1. In 1770 Wilson found the following result in the Number's Theory: "If p is prime, then $(p-1)! \equiv (-1 \bmod p)$".

Did you ever question yourself what happens if the module m is not anymore prime? It's simple, one answers, "if m is not prime and $m \neq 4$ then $(m-1)! \equiv 0(\bmod m)$"; for the proof see [4].

This is fine, I would continue, but if in the product from the left side of this congruence we consider only numbers that are prime with m?

For this reason we'll address this case, and provide a generalization of Wilson's theorem to any modulo, this will conduce to a nice result.

§2. Let m be a whole number. We note $A = \{x \in \mathbb{Z},\ x$ is of the form $\pm p^n,\ \pm 2p^n,\ \pm 2^r$, or 0, where p is odd prime, $n \in \mathbb{N}$, and $r = 0,1,2\ \}$.

Theorem*. Let $c_1, c_2, ..., c_{\varphi(m)}$ a reduced system of residues modulo m. Then $c_1 c_2 . \cdots c_{\varphi(m)} \equiv -1(\bmod m)$ if $m \in A$, respectively $+1$ if $m \notin A$; where φ is Euler's function.

To prove this we'll introduce some lemmas.

Lemma 1. $\varphi(m)$ is a multiple of 2.

Lemma 2. If $c^2 \equiv 1(\bmod m)$ then $(m-c)^2 \equiv 1(\bmod m)$ and $c(m-c) \equiv -1(\bmod m)$, and $m - c \not\equiv c(\bmod m)$.

Indeed, if $m - c \equiv c(\bmod m)$, we obtain $2c \equiv 0(\bmod m)$, that is $(c, m) \not\equiv 1$. This is absurd.

Therefore we proved that in any reduced system of residue modulo m it exists an even number of elements c with the property

$$P_1 :\ c^2 \equiv 1(\bmod m).$$

If c_{i_0} is part of the system, because $\left(c_{i_0}, m\right) \cong 1$, it results that also $c_1 c_{i_0}, c_2 c_{i_0}, ..., c_{\varphi(m)} c_{i_0}$ constitutes a reduced system of residues m. Because $(1, m) \cong 1$ results that for any c from $c_1, c_2, ..., c_{\varphi(m)}$ it exist and it is unique c' from $c_1, c_2, ..., c_{\varphi(m)}$ such that

$$(1) \qquad cc' \equiv 1(\bmod m)$$

and reciprocally: for any c' from $c_1, c_2, ..., c_{\varphi(m)}$ it exists an unique c such that

$$(2) \qquad c'c \equiv 1(\bmod m).$$

By multiplying these two congruence for all the elements from the system and selecting one of them in the case in which $c \neq c'$ it results that $c_1, c_2, ..., c_{\varphi(m)} \cdot b \equiv 1(\bmod m)$, where b represents the product of all elements c for which

$c = c'$, because in this case $c^2 \equiv 1(\bmod m)$. These elements which verify the property P_1 can be grouped in pairs as follows: c with $m-c$, and then $c(m-c) \equiv -1(\bmod m)$. Therefore

$$c_1, c_2, ..., c_{\varphi(m)} \equiv \pm 1(\bmod m),$$

depending of the number of distinct c in the system that have the property P_1 is or not a multiple of 4.

If $m \in A$ the equation $x^2 \equiv 1(\bmod m)$ has two solutions (see [1], pp. 38-88), therefore we conclude that $c_1, c_2, ..., c_{\varphi(m)} \equiv -1(\bmod m)$.

This first part of the theorem could have been proved also using the following reasoning:

If $m \in A$ then it exist primitive roots modulo m (see [1], pp. 65-68-72); let d be such a root; then we could represent the system reduced to residues modulo m, $\{c_1, c_2, ..., c_{\varphi(m)}\}$ as $\{d^1, d^2, ..., d^{\varphi(m)}\}$ after rearranging, from were

$$c_1, c_2, ..., c_{\varphi(m)} \equiv \left(d^{\frac{\varphi(m)}{2}}\right)^{1+\varphi(m} \equiv -1(\bmod m),$$

because from $d^{\varphi(m} \equiv 1(\bmod m)$ we have that

$$\left(d^{\frac{\varphi(m)}{2}} - 1\right)\left(d^{\frac{\varphi(m)}{2}} + 1\right) \equiv 0(\bmod m)$$

therefore

$$d^{\frac{\varphi(m)}{2}} \equiv -1(\bmod m);$$

contrary would have been implied that d is not a primitive root modulo m.

For the second part of the proof we shall present some other lemmas.

Lemma 3. Let's consider the integer numbers nonzero, non-unitary m_1 and m_2 with $(m_1, m_2) \cong 1$. Then

(3) $\quad x^2 \equiv 1(\bmod m_1)$ admits the solution x_1

and

(4) $\quad x^2 \equiv 1(\bmod m_2)$ admits the solution x_2

if and only if

(5) $\quad x^2 \equiv 1(\bmod m_1 m_2)$ admits the solution

(5') $\quad x_3 \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 (\bmod m_1 m_2)$,

where $m_1^{'}$ is the inverse of m_1 in rapport with modulo m_2.

Proof.

From (3) it results

$x = m_1 h + x_1$, $h \in \mathbb{Z}$,

and from (4) we find

$x = m_2 k + x_2$, $k \in \mathbb{Z}$.

Therefore

(6) $m_1 h - m_2 k = x_2 - x_1$

this Diophantine equation has integer solutions because

(7) $(m_1, m_2) \cong 1$

From (6) results $h \equiv (x_2 - x_1) m_1^{'} (\bmod m_2)$.

Therefore

$$h \equiv (x_2 - x_1) m_1^{'} + m_2 t, \quad t \in \mathbb{Z}$$

and

$$x \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 + m_1 m_2 t$$

or

$$x \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 \bmod (m_1 m_2).$$

(The rationale would have been analog if we would have determined k by finding

$$x \equiv (x_1 - x_2) m_2^{'} m_2 + x_2 \bmod (m_1 m_2),$$

but this solution is congruent modulo $m_1 m_2$ with the one found anterior; $m_2^{'}$ being the reciprocal of m_2 modulo m_1.)

Reciprocal. Immediately, results that

$$x_3 \equiv x_1 (\bmod m_1) \text{ and } x_3 \equiv x_2 (\bmod m_2).$$

Lemma 4. Let x_1, x_2, x_3 be the solutions for congruencies (3), (4) respective (5) such that

$$x_3 \equiv (x_2 - x_1) m_1^{'} m_1 + x_1 (\bmod m_1 m_2)$$

Analogue for $x_1^{'}, x_2^{'}, x_3^{'}$.

(O) Will consider from now on every time the classes of residue modulo m that have represents in the system $\{0, 1, 2, ..., |m| - 1\}$.

Then if $(x_1, x_2) \neq (x_1^{'}, x_2^{'})$ it results that $x_3 \not\equiv x_3^{'} (\bmod m)$.

Proof. By absurd.

Let $x_1 \neq x_1^{'}$ (analogue it can be shown for $x_2 \neq x_2^{'}$).

From $x_3 \equiv x_3^{'} (\bmod m_1 m_2)$ it would result that $x_3 \equiv x_3^{'} (\bmod m_1)$,

that is

$$(x_2 - x_1) m_1^{'} m_1 + x_1 \equiv (x_2^{'} - x_1^{'}) m_1^{'} m_1 + x_1^{'} (\bmod m_1),$$

Thus

$$x_1 \equiv x_1^{'} (\bmod m_1).$$

Since x_1 and $x_1^{'}$ are from $\{0, 1, 2, ..., |m| - 1\}$ it results that $x_1 = x_1^{'}$, which is absurd.

Lemma 5. The congruence $x^2 \equiv 1 (\bmod m)$ has an even number of distinct solutions.

This results from lemma 2.

Lemma 6. In the conditions of lemma 3 we have that the number of distinct solutions for congruence (5) is equal to the product between the number of congruencies' solutions (3) and (4). And, all solutions for congruence (5) are obtained from the solutions of congruencies (3) and (4) by applying formula (5').

Indeed, from lemmas 3, 4 we obtain the assertion.

Lemma 7. The congruence

(8) $x^2 \not\equiv 1\left(\bmod 2^m\right)$, has only four distinct solutions:

$\pm 1,\ \pm(2^{n-1}-1)$ modulo 2^n.

By direct verification it can be shown that these satisfy (8).

Using induction we will show that there don't exist others .

For $n = 3$ it verifies, by tries, analog for $n = 4$.

We consider the affirmation true for values $\leq n-1$. Let's prove it for n.

We retain observation (O) and the following remark:

(9) if x_0 is solution for congruence (8) it will be solution also for congruence $x^2 \equiv 1\left(\bmod 2^i\right),\ 3 \leq i \leq n-1$.

By absurdum let $a \not\equiv \pm 1,\ \pm(2^{n-1}-1)$ be a solution for (8). We will show that $(\exists) i \in \{3, 4, ..., n-1\}$ such that $a^2 \not\equiv 1(\bmod 2^i)$.

We can consider $2^{\frac{n}{2}} < a < 2^n - 1$; because a is solution for (8) if and only if $-a$ is solution for (8).

We consider the case $n = 2k,\ k \geq 2$, integer. (It will analogously be shown when n is odd). Let $a = 2^k + r$, $1 \leq r \leq 2^{2k} - 2^k - 2$

(10) $a^2 = 2^{2k} + r \cdot 2^{k+1} + r^2 \equiv 1(\bmod 2^n)$,

from here $r \neq 1$; it results that

$r^2 \equiv 1(\bmod 2^i),\ 3 \leq i \leq k+1$

From the induction's hypothesis, for $k+1$ we find $r \equiv 2^k - 1(\bmod 2^{k+1})$ and substituting in (10) we obtain:

$-2^{k+2} \equiv 0(\bmod 2^{2k})$,

or $k \leq 2$ thus $n = 4$, which is a contradiction.

Therefore, it results the lemma's validity.

Lemma 8. The congruence $x^2 \equiv 1\left(\bmod m\right)$ has

$$\begin{cases} 2^{s-1}, & \text{if } \alpha_1 = 0,1; \\ 2^s, & \text{if } \alpha_1 = 2; \\ 2^{s+1}, & \text{if } \alpha_1 \geq 3 \end{cases}$$

distinct solutions modulo $m = \varepsilon 2^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, where $\varepsilon = \pm 1$, $\alpha_j \in \mathbb{N}^*$, $j = 2, 3, ..., s$, and p_j are odd prime, different numbers two by two.

Indeed, the congruence $x^2 \equiv 1\left(\bmod 2^{\alpha_1}\right)$ has

$$\begin{cases} 1, & \text{if } \alpha_1 = 0,1; \\ 2, & \text{if } \alpha_1 = 2; \\ 4, & \text{if } \alpha_1 \geq 3 \end{cases}$$

distinct solutions, and congruence $x^2 \equiv 1\left(\bmod p_j^{\alpha_j}\right)$, $2 \leq j \leq s$ have each two distinct solutions (see [1], pp. 85-88). From lemma 6 and 7 it results this lemma too.

$*$

With these lemmas, it results that the congruence $c^2 \equiv 1(\bmod m)$ with $m \in A$ admits a number of distinct solutions which is a multiple of 4. From where $c_1 c_2 . \cdots c_{\varphi(m)} \equiv 1(\bmod m)$, that completely resolves the generalization of Wilson's theorem.

The reader could generalize lemmas 2, 3, 4, 5, 6, 8 and utilize lemma 7 for the case in which we have the congruence $x^2 \equiv a(\bmod m)$, with $(a, m) \cong 1$.

REFERENCES

[1] Francisco Bellot Rosada, Maria Victoria Deban Miguel, Felix Lopez Fernandez – Asenjo – "Olimpiada Matematica Española/Problemas propuestos en el distrito Universitario de Valladolid", Universidad de Valladolid, 1992.

[2] "Introducion a la teoria de numeros primos (Aspectos Algebraicos y Analiticos)", Felix Lopez Fernandez – Asenjo, Juan Tena Ayuso Universidad de Valladolid, 1990.

*[*After completing this paper the author read in the "History of the Theory of Numbers", by L. E. Dickson, Chelsea Publ. Hse., New York, 1992, that this theorem was also found by F. Gauss in 1801.]*

A METHOD OF RESOLVING IN INTEGER NUMBERS OF CERTAIN NONLINEAR EQUATIONS

Let's consider a polynomial with integer coefficients, of degree m

$$P(X_1,...,X_n)=\sum_{\substack{0\le i_1+...+i_n\le m\\ 0\le i_j\le m,\, j=\overline{1,n}}} a_{i_1...i_n}X_1^{i_1}...X_n^{i_n}$$

which can be decomposed in linear factors (which can eventually be established through the undetermined coefficients method):

$$P(X_1,...,X_n)=\left(A_1^{(1)}X_1+...+A_n^{(1)}X_n+A_{n+1}^{(1)}\right)\cdots\left(A_1^{(m)}X_1+...+A_n^{(m)}X_n+A_{n+1}^{(m)}\right)+B$$

with all $A_j^{(k)}$, B in $\mathbb{Q}$, but which by bringing to the same common denominator and by eliminating it from the equation $P(X_1,...,X_n)=0$ they can be considered integers.. Thus the equation transforms in the following system:

$$\begin{cases}A_1^{(1)}X_1+...+A_n^{(1)}X_n+A_{n+1}^{(1)}=D_1\\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ A_1^{(m)}X_1+...+A_n^{(m)}X_n+A_{n+1}^{(m)}=D_m\end{cases}$$

where $D_1,...,D_m$ are the divisors for B and $D_1\cdots D_m=B$.

We resolve separately each linear Diophantine equation and then we intersect the equations.

Example. Resolve in integer numbers the equation:

$$-2x^3+5x^2y+4xy^2-3y^3-3=0.$$

We'll write the equation in another format

$$(x+y)(2x-y)(-x+3y)=3.$$

Let $m,\ n$ and p be the divisors of $3, m\cdot n\cdot p=3$. Thus

$$\begin{cases}x+y&=m\\2x-y&=n\\-x+3y&=p\end{cases}$$

For this system to be compatible it is necessary that

$$\begin{vmatrix}1&1&m\\2&-1&n\\-1&3&p\end{vmatrix}=0,$$

or

$$5m-4n-3p=0 \qquad (1)$$

In this case

$$x=\frac{m+n}{3} \text{ and } y=\frac{2m-n}{3} \qquad (2)$$

Because $m,n,p\in\mathbb{Z}$, from (1) it results – by resolving in integer numbers – that:

$$\begin{cases} m = 3k_1 - k_2 \\ n = \quad\quad k_2 \\ p = 5k_1 - 3k_2 \end{cases} \quad k_1, k_2 \in \mathbb{Z}$$

which substituted in (2) will give us $x = k_1$ and $y = 2k_1 - k_2$. But $k_2 \in D(3) = \{\pm 1, \pm 3\}$; thus the only solution is obtained for $k_2 = 1$, $k_1 = 0$ from where $x = 0$ and $y = -1$.

Analogue it can be shown that, for example the equation:

$$-2x^3 + 5x^2y + 4xy^2 - 3y^3 = 6$$

does not have solutions in integer numbers.

REFERENCES

[1] Marius Giurgiu, Cornel Moroti, Florică Puican, Stefan Smărăndoiu – Teme şi teste de Matematică pentru clasele IV-VIII - Ed. Matex, Rm. Vîlcea, Nr. 3/1991

[2] Ion Nanu, Lucian Tuțescu – "Ecuații Nestandard", Ed. Apollo şi Ed. Oltenia, Craiova, 1994.

A GENERALIZATION REGARDING THE EXTREMES OF A TRIGONOMETRIQUE FUNCTION

After a passionate lecture of this book [1] (Mathematics plus literature!) I stopped at one of the problems explained here:

At page 121, the problem 2 asks to determine the maximum of expression:

$$E(x) = (9 + \cos^2 x)(6 + \sin^2 x).$$

Analogue, in G. M. 7/1981, page 280, problem 18820*.

Here, we'll present a generalization of these problems, and we'll give a simpler solving method, as follows:

Let $f : \mathbb{R} \to \mathbb{R},\ f(x) = (a_1 \sin^2 x + b_1)(a_2 \cos^2 x + b_2)$;
find the function's extreme values.

To solve it, we'll take into account that we have the following relation:

$$\cos^2 x = 1 - \sin^2 x,$$

and we'll note $\sin^2 x = y$. Thus $y \in [0,1]$.

The function becomes:

$$f(y) - (a_1 y + b_1)(-a_2 y + a_2 + b_2) = -a_1 a_2 y^2 + (a_1 a_2 + a_1 b_2 - a_2 b_1) y + b_1 a_2 + b_1 b_2,$$

where $y \in [0,1]$.

Therefore f is a parabola.

If $a_1 a_2 = 0$, the problem becomes banal.

If $a_1 a_2 > 0$, $f(y_{\max}) = \dfrac{-\Delta}{4a}$, $y_{\max} = \dfrac{-b}{2a}$ (*)

a) when $-\dfrac{b}{2a} \in [0,1]$, the values that we are looking for are those from (*), and

$$y_{\min} = \max\left\{-\frac{b}{2a} - 0, 1 + \frac{b}{2a}\right\}$$

b) when $-\dfrac{b}{2a} > 1$, we have $y_{\max} = 1$, $y_{\min} = 0$. (it is evident that $f_{\max} = f(y_{\max})$ and $f_{\min} = f(y_{\min})$)

c) when $-\dfrac{b}{2a} < 0$, we have $y_{\max} = 0$, $y_{\min} = 1$.

If $a_1 a_2 < 0$, the function admits a minimum for

$$y_{\min} = -\frac{b}{2a},\ f_{\min} \frac{-\Delta}{4a} \text{ (on the real axes)} \qquad (**)$$

a) when $-\dfrac{b}{2a} \in [0,1]$, the looked after solutions are those from (**). And

$$y_{\max} = \max\left\{-\frac{b}{2a}, 1 + \frac{b}{2a}\right\}$$

b) when $-\frac{b}{2a} > 1$, we have $y_{\max} = 0$, $y_{\min} = 1$

c) when $-\frac{b}{2a} < 0$, we have $y_{\max} = 1$, $y_{\min} = 0$.

Maybe the cases presented look complicated and unjustifiable, but if you plot the parabola (or the line), then the reasoning is evident.

REFERENCE

[1] Viorel Gh. Vod - Surprize în matematica elementar - Editura Albatros, Bucure ti, 1981.

ON SOLVING HOMOGENE SYSTEMS

In the High School Algebra manual for grade IX (1981), pp. 103-104, is presented a method for solving systems of two homogenous equations of second degree, with two unknowns. In this article we'll present another method of solving them.

Let's have the homogenous system

$$\begin{cases} a_1x^2 + b_1xy + c_1y^2 = d_1 \\ a_2x^2 + b_2xy + c_2y^2 = d_2 \end{cases}$$

with real coefficients.

We will note $x = ty$, (or $y = tx$), and by substitution, the system becomes:

$$\begin{cases} y^2(a_1t^2 + b_1t + c_1) = d_1 & (1) \\ y^2(a_2t^2 + b_2t + c_2) = d_2 & (2) \end{cases}$$

Dividing (1) by (2) and grouping the terms, it results an equation of second degree of variable t:

$$(a_1d_2 - a_2d_1)t^2 + (b_1d_2 - b_2d_1)t + (c_1d_2 - c_2d_1) = 0$$

If $\Delta_t < 0$, the system doesn't have solutions.

If $\Delta_t \geq 0$, the initial system becomes equivalent with the following systems:

$$(S_1)\begin{cases} x = t_1y \\ a_1x^2 + b_1xy + c_1y^2 = d_1 \end{cases}$$

and

$$(S_2)\begin{cases} x = t_2y \\ a_1x^2 + b_1xy + c_1y^2 = d_1 \end{cases}$$

which can simply be resolved by substituting the value of x from the first equation into the second.

Further we will provide an extension of this method.

Let have the homogeneous system:

$$\sum_{i=0}^{n} a_{i,j}x^{n-i}y^i, \quad j = \overline{1,m}$$

To resolve this, we note $x = ty$, it results:

$$y^n\sum_{i=0}^{n} a_{i,j}t^{n-i} = b_j, \quad j = \overline{1,m}$$

By dividing in order the first equation to the rest of them, we obtain:

$$\left(\sum_{i=0}^{n} a_{i,1}t^{n-i}\right) \Big/ \left(\sum_{i=0}^{n} a_{i,j}t^{n-i}\right) = b_1 \ / \ b_j, \ \ j = \overline{2,m}$$

or:

$$\sum_{i=0}^{n} (a_{i,1}b_j - a_{i,j}b_1)t^{n-i}, \ \ j = \overline{2,m}$$

We will find the real values $t_1,...,t_p$ from this system.
The initial system is equivalent with the following systems

$$(S_h) \quad \begin{cases} x = t_h y \\ \sum_{i=0}^{n} a_{i,1} x^{n-1} y^i = b_1 \end{cases} \text{ where } h = \overline{1, p}.$$

ABOUT SOME PROGRESSIONS

In this article one builds sets which have the following property: for any division in two subsets, at least one of these subsets contains at least three elements in arithmetic (or geometrical) progression.

Lemma 1. The set of natural numbers cannot be divided in two subsets not containing either one or the other 3 numbers in arithmetic progression.

Let us suppose the opposite, and have M_1 and M_2 two subsets. Let $k \in M_1$:

a) If $k+1 \in M_1$, then $k-1$ and $k+2$ belong to M_2, if not we can build an arithmetic progression in M_1. For the same reason, since $k-1$ and $k+2$ belong to M_2, then $k-4$ and $k+5$ are in M_1. Thus $k+1$ and $k+5$ are in M_1 thus $k+3$ is in M_2; $k-4$ and k are in M_1 thus $k+4$ is in M_1; we have obtained that M_2 contains $k+2$, $k+3$ and $k+4$, which is in contradiction with the hypothesis.

b) If $k+1 \in M_1$ then $k+1 \in M_2$. We analyze the element $k-1$. If $k-1 \in M_1$, we are in the case a) where two consecutive elements belong to the same set. If $k-1 \in M_2$, then, because $k-1$ and $k+1$ belong to M_2, it results that $k-3$ and $k+3 \in M_2$, then $\in M_1$. But we obtained the arithmetic progression $k-3$, k, $k+3$ in M_1, contradiction.

Lemma 2. If one puts aside a finite number of terms of the natural integer set, the set obtained still satisfies the property of the lemma 1.

In the lemma 1, the choice of k was arbitrary, and for each k one obtains at least in one of the sets M_1 or M_2 a triplet of elements in arithmetic progression: thus at least one of these two sets contains an infinity of such triplets.

If one takes a finite number of natural numbers, it takes also a finite number of triplets in arithmetic progression. But at least one of the sets M_1 or M_2 will contain an infinite number of triplets in arithmetic progression.

Lemma 3. If $i_1,\dots,i_s$ are natural numbers in arithmetic progression, and $a_1,a_2,\dots$ is an arithmetic progression (respectively geometric), then $a_{i_1},\dots,a_{i_s}$ is also an arithmetic progression (respectively geometric).

Proof:

For every j we have: $2i_j = i_{j-1} + i_{j+1}$

a) If $a_1,a_2,\dots$ is an arithmetic progression of ratio r:

$$2a_{i_j} = 2(a_1 + (i_j - 1)r) = (a_1 + (i_{j-1} - 1)r) + (a_1 + (i_{j+1} - 1)r) = a_{i_{j-1}} + a_{i_{j+1}}$$

b) If $a_1,a_2,\dots$ is a geometric progression of ratio r:

$$\left(a_{i_j}\right)^2 = \left(a \cdot r^{i_j - 1}\right)^2 = a^2 \cdot r^{2i_j - 2} = \left(a \cdot r^{i_{j-1}-1}\right)\cdot\left(a \cdot r^{i_{j+1}-1}\right) = a_{i_{j-1}} + a_{i_{j+1}}$$

Theorem 1.

It does not matter the way in which one partitions the set of the terms of an arithmetic progression (respectively geometric) in subsets: in at least one of these subsets there will be at least 3 terms in arithmetic progression (respectively geometric).

Proof:

According to lemma 3, it is enough to study the division of the set of the indices of the terms of the progression in 2 subsets, and to analyze the existence (or not) of at least 3 indices in arithmetic progression in one of these subsets.
But the set of the indices of the terms of the progression is the set of the natural numbers, and we proved in lemma 1 that it cannot be division in 2 subsets without having at least 3 numbers in arithmetic progression in one of these subsets: the theorem is proved.

Theorem 2.

A set M, which contains an arithmetic progression (respectively geometric) infinite, not constant, preserves the property of the theorem 1.

Indeed, this directly results from the fact that any partition of M implies the partition of the terms of the progression.

Application: Whatever the way in which one partitions the set $A = \left\{1^m, 2^m, 3^m, \ldots\right\}$, $(m \in \mathbb{R})$ in subsets, at least one of these subsets contains 3 terms in geometric progression.

(Generalization of the problem 0:255 from "Gazeta Matematică", Bucharest, no. 10/1981, p. 400).

The solution naturally results from theorem 2, if it is noticed that A contains the geometric progression $a_n = (2^m)^n$, $(n \in \mathbb{N}^*)$.

Moreover one can prove that in at least one of the subsets there is an infinity of triplets in geometric progression, because A contains an infinity of different geometric progressions: $a_n^{(p)} = (p^m)^n$ with p prime and $n \in \mathbb{N}^*$, to which one can apply the theorems 1 and 2.

ON SOLVING GENERAL LINEAR EQUATIONS IN THE SET OF NATURAL NUMBERS

The utility of this article is that it establishes if the number of the natural solutions of a general linear equation is limited or not. We will show also a method of solving, using integer numbers, the equation $ax - by = c$ (which represents a generalization of lemmas 1 and 2 of [4]), an example of solving a linear equation with 3 unknowns in N, and some considerations on solving, using natural numbers, equations with n unknowns.

Let's consider the equation:

(1) $\sum_{i=1}^{n} a_i x_i = b$ with all $a_i, b \in \mathbb{Z}$, $a_i \neq 0$, and the greatest common factor $(a_1, ..., a_n) = \mathrm{d}$.

Lemma 1: The equation (1) admits at least a solution in the set of integers, if d divides b.

This result is classic.

In (1), one does not diminish the generality by considering $(a_1, ..., a_n) = 1$, because in the case when $d \neq 1$, one divides the equation by this number; if the division is not an integer, then the equation does not admit natural solutions.

It is obvious that each homogeneous linear equation admits solutions in $\mathbb{N}$: at least the banal solution!

PROPERTIES ON THE NUMBER OF NATURAL SOLUTIONS OF A GENERAL LINEAR EQUATION

We will introduce the following definition:

Definition 1: The equation (1) has variations of sign if there are at least two coefficients a_i, a_j with $1 \leq i, j \leq n$, such that sign($a_i \cdot a_j$) = -1

Lemma 2: An equation (1) which has sign variations admits an infinity of natural solutions (generalization of lemma 1 of [4]).

Proof: From the hypothesis of the lemma it results that the equation has h no null positive terms, $1 \leq h \leq n$, and $k = n - h$ non null negative terms. We have $1 \leq k \leq n$; it is supposed that the first h terms are positive and the following k terms are negative (if not, we rearrange the terms).

We can then write:

$$\sum_{t=1}^{h} a_t x_t - \sum_{j=h+1}^{n} a_j^{'} x_j = b \text{ where } a_j^{'} = -a_j > 0 .$$

Let's consider $0 < M = \left[a_1, ..., a_n \right]$ the least common multiple, and $c_i = \left| M / a_i \right|$, $i \in \{1, 2, ..., n\}$.

Let's also consider $0 < P = [h,k]$ the least common multiple, and $h_1 = P/h$ and $k_1 = P/k$.

Taking $\begin{cases} x_t = h_1 c_t \cdot z + x_t^0, & 1 \le t \le h \\ x_j = k_1 c_j \cdot z + x_j^0, & h+1 \le j \le n \end{cases}$

where $z \in \mathbb{N}$, $z \ge \max\left\{\left[\frac{-x_t^0}{h_1 c_t}\right], \left[\frac{x_j^0}{k_1 c_j}\right]\right\} + 1$ with [γ] meaning integer part of γ, i.e. the greatest integer less than or equal to γ, and x_i^0, $i \in \{1,2,...,n\}$, a particular integer solution (which exists according to lemma 1), we obtain an infinity of solutions in the set of natural numbers for the equation (1).

Lemma 3:

a) An equation (1) which does not have variations of sign has at maximum a limited number of natural solutions.

b) In this case, for $b \ne 0$, constant, the equation has the maximum number of solutions if and only if all $a_i = 1$ for $i \in \{1,2,...,n\}$.

Proof: (see also [6]).

a) One considers all $a_i > 0$ (otherwise, multiply the equation by -1).

If $b < 0$, it is obvious that the equation does not have any solution (in $\mathbb{N}$).

If $b = 0$, the equation admits only the trivial solution.

If $b > 0$, then each unknown x_i takes positive integer values between 0 and $b / a_i = d_i$ (finite), and not necessarily all these values. Thus the maximum number of solutions is lower or equal to: $\prod_{i=1}^{n}(1+d_i)$, which is finite.

b) For $b \ne 0$, constant, $\prod_{i=1}^{n}(1+d_i)$ is maximum if and only if d_i are maximum, i.e. iff $a_i = 1$ for all i, where $i = \{1,2,...,n\}$.

Theorem 1. The equation (1) admits an infinity of natural solutions if and only if it has variations of sign.

This naturally follows from the previous results.

<u>Method of solving.</u>

Theorem 2. Let's consider the equation with integer coefficients $ax - by = c$, where a and $b > 0$ and $(a,b) = 1$. Then the general solution in natural numbers of this equation is:

$\begin{cases} x = bk + x_0 \\ y = ak + y_0 \end{cases}$ where (x_0, y_0) is a particular integer solution of the equation,

and $k \ge \max\{[-x_0 / b], [-y_0 / a]\}$ is an integer parameter (generalization of lemma 2 of [4]).

Proof: It results from [1] that the general integer solution of the equation is $\begin{cases} x = bk + x_0 \\ y = ak + y_0 \end{cases}$ where (x_0, y_0) is a particular integer solution of the equation and $k \in \mathbb{Z}$. Since x and y are natural integers, it is necessary for us to impose conditions for k such that x ≥ 0 and y ≥ 0, from which it results the theorem.

WE CONCLUDE!

To solve in the set of natural numbers a linear equation with n unknowns we will use the previous results in the following way:

a) If the equation does not have variations of sign, because it has a limited number of natural solutions, the solving is made by tests (see also [6])

b) If it has variations of sign and if b is divisible by d, then it admits an infinity of natural solutions. One finds its general integer solution (see [2], [5]);

$x_i = \sum_{j=1}^{n-1} \alpha_{ij} k_j + \beta_i$, $1 \le i \le n$ where all the $\alpha_{ij}, \beta_i \in \mathbb{Z}$ and the k_j are integer parameters.

By applying the restriction $x_i \ge 0$ for i from $\{1, 2, ..., n\}$, one finds the conditions which must be satisfied by the integer parameters k_j for all j of $\{1, 2, ..., n-1\}$. (c)

The case $n = 2$ and $n = 3$ can be done by this method, but when n is bigger, the condition (c) become more and more difficult to find.

Example: Solve in $\mathbb{N}$ the equation $3x - 7y + 2z = -18$.

Solution: In $\mathbb{Z}$ one obtains the general integer solution:

$$\begin{cases} x = k_1 \\ y = k_1 + 2k_2 \\ z = 2k_1 + 7k_2 - 9 \end{cases} \quad \text{with } k_1 \text{ and } k_2 \text{ in } \mathbb{Z}.$$

From the conditions (c) result the inequalities $x \ge 0,\ y \ge 0,\ z \ge 0$. It results that $k_1 \ge 0$ and also:

$k_2 \ge [-k_1/2] + 1$ if $-k_1/2 \notin Z$, or $k_2 \ge -k_1/2$ if $-k_1/2 \in Z$;

and $k_2 \ge [(9 - 2k_1)/7] + 1$ if $(9-2k_1)/7 \notin Z$, or $k_2 \ge (9-2k_1)/7$ if $(9-2k_1)/7 \in Z$;

that is $k_2 \ge [(2 - 2k_1)/7] + 2$ if $(2-2k_1)/7 \notin Z$, or $k_2 \ge (2-2k_1)/7 + 1$ if $(2-2k_1)/7 \in Z$.

With these conditions on k_1 and k_2 we have the general solution in natural numbers of the equation.

REFERENCES

[1] Creangă I, Cazacu C., Mihuț P., Opaiț Gh., Reisher, Corina – "Introducere în teoria numerelor" - Editura Didactică şi Pedagogică, Bucharest, 1965.

[2] Ion D. Ion, Niță C. – "Elemente de aritmetică cu aplicații în tehnici de calcul" - Editura Tehnică, Bucharest, 1978.

[3] Popovici C. P. – “Logica şi teoria numerelor” - Editura Didactică şi Pedagogică, Bucharest, 1970.

[4] Andrica Dorin, Andreescu Titu – “Existența unei soluții de bază pentru ecuația $ax^2 - by^2 = 1$” - Gazeta Matematică, Nr. 2/1981.

[5] Smarandache, Florentin Gh. – “Un algorithme de résolution dans l’ensemble des nombres entiers des équations linéaires”, 1981; a more general English version of this French article is: “Integer Algorithms to Solver Linear Equations and Systems” in arXiv at http://xxx.lanl.gov/pdf/math/0010134 ;

[6] Smarandache, Florentin Gh. – Problema E: 6919, Gazeta Matematică, Nr. 7/1980.

EXISTENCE AND NUMBER OF SOLUTIONS OF DIOPHANTINE QUADRATIC EQUATIONS WITH TWO UNKNOWNS IN $\mathbb{Z}$ AND $\mathbb{N}$

Abstract: In this short note we study the existence and number of solutions in the set of integers (Z) and in the set of natural numbers (N) of Diophantine equations of second degree with two unknowns of the general form $ax^2 - by^2 = c$.

Property 1: The equation $x^2 - y^2 = c$ admits integer solutions if and only if c belongs to $4\mathbb{Z}$ or is odd.

Proof: The equation $(x-y)(x+y) = c$ admits solutions in $\mathbb{Z}$ iff there exist c_1 and c_2 in $\mathbb{Z}$ such that $x - y = c_1$, $x + y = c_2$, and $c_1 c_2 = c$.
Therefore

$$x = \frac{c_1 + c_2}{2} \text{ and } y = \frac{c_2 - c_1}{2}.$$

But x and y are integers if and only if $c_1 + c_2 \in 2\mathbb{Z}$, i.e.:

1) or c_1 and c_2 are odd, then c is odd (and reciprocally).

2) or c_1 and c_2 are even, then $c \in 4\mathbb{Z}$.

Reciprocally, if $c \in 4\mathbb{Z}$, then we can decompose up c into two even factors c_1 and c_2, such that $c_1 c_2 = c$.

Remark 1:

Property 1 is true also for solving in $\mathbb{N}$, because we can suppose $c \geq 0$ {in the contrary case, we can multiply the equation by (-1)}, and we can suppose $c_2 \geq c_1 \geq 0$, from which $x \geq 0$ and $y \geq 0$.

Property 2: The equation $x^2 - dy^2 = c^2$ (where d is not a perfect square) admits an infinity of solutions in $\mathbb{N}$.

Proof: Let's consider $x = ck_1$, $k_1 \in \mathbb{N}$ and $y = ck_2$, $k_2 \in \mathbb{N}$, $c \in \mathbb{N}$. It results that $k_1^2 - dk_2^2 = 1$, which we can recognize as being the Pell-Fermat's equation, which admits an infinity of solutions in $\mathbb{N}$, (u_n, v_n).

Therefore

$$x_n = cu_n,\ y_n = cv_n$$

constitute an infinity of natural solutions for our equation.

Property 3: The equation $ax^2 - by^2 = c$, $c \neq 0$, where $ab = k^2$, ($k \in \mathbb{Z}$), admits a finite number of natural solutions.

Proof: We can consider a, b, c as positive numbers, otherwise, we can multiply the equation by (-1) and we can rename the variables.

Let us multiply the equation by a, then we will have:

$z^2 - t^2 = d$ with $z = ax \in \mathbb{N}$, $t = ky \in \mathbb{N}$ and $d = ac > 0$. (1)

We will solve it as in property 1, which gives z and t.

But in (1) there is a finite number of natural solutions, because there is a finite number of integer divisors for a number in $\mathbb{N}^*$. Because the pairs (z,t) are in a limited number, it results that the pairs $(z/a, t/k)$ also are in a limited number, and the same for the pairs (x, y).

Property 4: If $ax^2 - by^2 = c$, where $ab \neq k^2$ ($k \in \mathbb{Z}$) admits a particular nontrivial solution in $\mathbb{N}$, then it admits an infinity of solutions in $\mathbb{N}$.

Proof: Let's consider:

$$\begin{cases} x_n = x_0 u_n + b y_0 v_n \\ y_n = y_0 u_n + a x_0 v_n \end{cases} \quad (n \in \mathbb{N}) \qquad (2)$$

where (x_0, y_0) is the particular natural solution for the initial equation, and $(u_n, v_n)_{n\in\mathbb{N}}$ is the general natural solution for the equation $u^2 - abv^2 = 1$, called the solution Pell, which admits an infinity of solutions.

Then $ax_n^2 - by_n^2 = (ax_0^2 - by_0^2)(u_n^2 - abv_n^2) = c$.

Therefore (2) verifies the initial equation.

[1982]

CONVERGENCE OF A FAMILY OF SERIES

In this article we will construct a family of expressions $\mathcal{E}(n)$. For each element $E(n)$ from $\mathcal{E}(n)$, the convergence of the series $\sum_{n=n_E} E(n)$ could be determined in accordance to the theorems from this article.

This article gives also applications.

(1) Preliminary

To render easier the expression, we will use the recursive functions. We will introduce some notations and notions to simplify and reduce the size of this article.

(2) Definitions: lemmas.

We will construct recursively a family of expressions $\mathcal{E}(n)$.

For each expression $E(n) \in \mathcal{E}(n)$, the degree of the expression is defined recursive and is denoted $d^0 E(n)$, and its dominant coefficient is denoted $c(E(n))$.

1. If a is a real constant, then $a \in \mathcal{E}(n)$.

   $d^0 a = 0$ and $c(a) = a$.
2. The positive integer $n \in \mathcal{E}(n)$.

   $d^0 n = 1$ and $c(n) = 1$.
3. If $E_1(n)$ and $E_2(n)$ belong to $\mathcal{E}(n)$ with $d^0 E_1(n) = r_1$ and $d^0 E_2(n) = r_2$, $c(E_1(n)) = a_1$ and $c(E_2(n)) = a_2$, then:
   a) $E_1(n)E_2(n) \in \mathcal{E}(n)$; $d^0(E_1(n)E_2(n)) = r_1 + r_2$; $c(E_1(n)E_2(n))$ which is $a_1 a_2$.

   b) If $E_2(n) \neq 0 \ \ \forall n \in \mathbb{N}(n \geq n_{E_2})$, then $\frac{E_1(n)}{E_2(n)} \in \mathcal{E}(n)$ and

   $d^0\left(\frac{E_1(n)}{E_2(n)}\right) = r_1 - r_2$, $c\left(\frac{E_1(n)}{E_2(n)}\right) = \frac{a_1}{a_2}$.

   c) If α is a real constant and if the operation used has a sense $\left(E_1(n)\right)^{\alpha}$ (for all $n \in \mathbb{N},\ n \geq n_{E_1}$), then:

   $\left(E_1(n)\right)^{\alpha} \in \mathcal{E}(n)$, $d^0\left(\left(E_1(n)\right)^{\alpha}\right) = r_1\alpha$, $c\left(\left(E_1(n)\right)^{\alpha}\right) = a_1^{\alpha}$

   d) If $r_1 \neq r_2$, then $E_1(n) \pm E_2(n) \in \mathcal{E}(n)$, $d^0\left(E_1(n) \pm E_2(n)\right)$ is the max of r_1 and r_2, and $c\left(E_1(n) \pm E_2(n)\right) = a_1$, respectively a_2 resulting that the grade is r_1 and r_2.

   e) If $r_1 = r_2$ and $a_1 + a_2 \neq 0$, then $E_1(n) + E_2(n) \in \mathcal{E}(n)$, $d^0\left(E_1(n) + E_2(n)\right) = r_1$ and $c\left(E_1(n) + E_2(n)\right) = a_1 + a_2$.

f) If $r_1 = r_2$ and $a_1 - a_2 \neq 0$, then $E_1(n) - E_2(n) \in \mathcal{E}(n)$, $d^0\left(E_1(n) - E_2(n)\right) = r_1$ and $c\left(E_1(n) - E_2(n)\right) = a_1 - a_2$.

4. All expressions obtained by applying a finite number of step 3 belong to $\mathcal{E}(n)$.

Note 1. From the definition of $\mathcal{E}(n)$ it results that, if $E(n) \in \mathcal{E}(n)$ then $c\left(E(n)\right) \neq 0$, and that $c\left(E(n)\right) = 0$ if and only if $E(n) = 0$.

Lemma 1. If $E(n) \in \mathcal{E}(n)$ and $c\left(E(n)\right) > 0$, then there exists $n^{'} \in \mathbb{N}$, such that for all $n > n^{'}$, $E(n) > 0$.

Proof: Let's consider $c\left(E(n)\right) = a_1 > 0$ and $d^0\left(E(n)\right) = r$.

If $r > 0$, then $\lim\limits_{n\to\infty} E(n) = \lim\limits_{n\to\infty} n^r \dfrac{E(n)}{n^r} = \lim\limits_{n\to\infty} a_1 n^r = +\infty$, thus there exists $n^{'} \in \mathbb{N}$ such that, qqst $n > n^{'}$ we have $E(n) > 0$.

If $r < 0$, then $\lim\limits_{n\to\infty} \dfrac{1}{E(n)} = \lim\limits_{n\to\infty} \dfrac{n^{-r}}{\frac{E(n)}{n^r}} = \dfrac{1}{a_1} \lim\limits_{n\to\infty} n^{-r} = +\infty$ thus there exists $n^{'} \in \mathbb{N}$, such that for all $n > n^{'}$, $\dfrac{1}{E(n)} > 0$ we have $E(n) > 0$.

If $r = 0$, then $E(n)$ is a positive real constant, or $\dfrac{E_1(n)}{E_2(n)} = E(n)$, with $d^0 E_1(n) = d^0 E_2(n) = r_1 \neq 0$, according to what we have just seen, $c\left(\dfrac{E_1(n)}{E_2(n)}\right) = \dfrac{c\left(E_1(n)\right)}{c\left(E_2(n)\right)} = c\left(E(n)\right) > 0$.

Then: $c\left(E_1(n)\right) > 0$ and $c\left(E_2(n)\right) < 0$: it results

$$\left.\begin{array}{l}\text{there exists } n_{E_1} \in \mathbb{N},\ \forall n \in \mathbb{N} \text{ and } n \geq n_{E_1},\ E_1(n) > 0 \\ \text{there exists } n_{E_2} \in \mathbb{N},\ \forall n \in \mathbb{N} \text{ and } n \geq n_{E_2},\ E_2(n) > 0\end{array}\right\} \Rightarrow$$

there exists $n_E = \max(n_{E_1}, n_{E_2}) \in \mathbb{N},\ \forall n \in \mathbb{N},\ n \geq n_E,\ E(n) \dfrac{E_1(n)}{E_2(n)} > 0$

then $c\left(E_1(n)\right) < 0$ and $c\left(E_2(n)\right) < 0$ and it results:

$E(n) = \dfrac{E_1(n)}{E_2(n)} = \dfrac{-E_1(n)}{-E_2(n)}$ which brings us back to the precedent case.

Lemma 2: If $E(n) \in \mathcal{E}(n)$ and if $c\left(E(n)\right) < 0$, then it exists $n^{'} \in \mathbb{N}$, such that qqst $n > n^{'}$, $E(n) < 0$.

Proof:

The expression $-E(n)$ has the propriety that $c\left(-E(n)\right)>0$, according to the recursive definition. According to lemma 1: there exists $n^{'}\in\mathbb{N}$, $n\geq n^{'}$, $-E(n)>0$, i.e. $+E(n)<0$, q.e.d.

Note 2. To prove the following theorem, we suppose known the criterion of convergence of the series and certain of its properties

(3) Theorem of convergence and applications.

Theorem: Let's consider $E(n)\in\mathcal{E}(n)$ with $d^0\left(E(n)\right)=r$ having the series

$$\sum_{n\geq n_\varepsilon} E(n),\quad E(n)\not\equiv 0.$$

Then:

A) If $r<-1$ the series is absolutely convergent.
B) If $r\geq -1$ it is divergent where $E(n)$ has a sense $\forall n\geq n_E, n\in\mathbb{N}$.

Proof: According to lemmas 1 and 2, and because:

the series $\sum_{n\geq n_E} E(n)$ converge $\Leftrightarrow$ the series $-\sum_{n\geq n_E} E(n)$ converge,

we can consider the series $\sum_{n\geq n_E} E(n)$ like a series with positive terms.

We will prove that the series $\sum_{n\geq n_E} E(n)$ has the same nature as the series $\sum_{n\geq 1}\frac{1}{n^{-r}}$.

Let us apply the second criterion of comparison:

$$\lim_{n\to\infty}\frac{E(n)}{\frac{1}{n^{-r}}}=\lim_{n\to\infty}\frac{E(n)}{n^r}=c\left(E(n)\right)\neq\pm\infty.$$

According to the note 1 if $E(n)\not\equiv 0$ then $c\left(E(n)\right)\neq 0$ and then the series $\sum_{n\geq n_E} E(n)$ has the same nature as the series $\sum_{n\geq 1}\frac{1}{n^{-r}}$, i.e.:

A) If $r<-1$ then the series is convergent;
B) If $r>-1$ then the series is divergent;

For $r<-1$ the series is absolute convergent because it is a series with positive terms.

Applications:

We can find many applications of these. Here is an interesting one:

If $P_q(n)$, $R_s(n)$ are polynomials of n of degree q, s, and that $P_q(n)$ and $R_s(n)$ belong to $\mathcal{E}(n)$:

1) $\displaystyle\sum_{n \geq n_{PR}} \frac{\sqrt[k]{P_q(n)}}{\sqrt[h]{R_s(n)}}$ is $\begin{cases} \text{convergent, if } s/h - q/k > 1 \\ \text{divergent, } \quad \text{if } s/h - q/k \leq 1 \end{cases}$

2) $\displaystyle\sum_{n \geq n_R} \frac{1}{R_s(n)}$ is $\begin{cases} \text{convergent, if } s > 1 \\ \text{divergent, } \quad \text{if } s \leq 1 \end{cases}$

Example: The series $\displaystyle\sum_{n \geq 2} \frac{\sqrt[2]{n+1} \cdot \sqrt[3]{n-7} + 2}{\sqrt[5]{n^2} - 17}$ is divergent because $\displaystyle\frac{2}{5} - \left(\frac{1}{2} + \frac{1}{3}\right) < 1$ and if we call $E(n)$ each quotient of this series, $E(n)$ belongs to $\mathcal{E}(n)$ and it has a sense for $n \geq 2$.

ALGORITHMS FOR SOLVING LINEAR CONGRUENCES AND SYSTEMS OF LINEAR CONGRUENCES

In this article we determine several theorems and methods for solving linear congruences and systems of linear congruences and we find the number of distinct solutions. Many examples of solving congruences are given.

§1. Properties for solving linear congruences.

Theorem 1. The linear congruence $a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$ has solutions if and only if $(a_1,...,a_n,m) | b$.

Proof:

$a_1x_1 + ... + a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1x_1 + ... + a_nx_n - my = b$ is a linear equation which has solutions in the set of integer numbers $\Leftrightarrow$ $(a_1,...,a_n,\ -m) | b \Leftrightarrow (a_1,...,a_n,\ m) | b$.

If $m = 0$, $a_1x_1 + ... + a_nx_n \equiv b(\bmod 0)$ $\Leftrightarrow$ $a_1x_1 + ... + a_nx_n = b$ has solutions in the set of integer numbers $\Leftrightarrow$ $(a_1,...,a_n) | b$ $\Leftrightarrow$ $(a_1,...,a_n,0) | b$.

Theorem 2. The congruence $ax \equiv b(\bmod m)$, $m \neq 0$, with $(a,m) = d | b$, has d distinct solutions.

The proof is different of that from the number's theory courses: $ax \equiv b(\bmod m)$ $\Leftrightarrow$ $ax - my = b$ has solutions in the set of integer numbers; because $(a,m) = d | b$ it results: $a = a_1d$, $m = m_1d$, $b = b_1d$ and $(a_1,m_1) = 1$, $a_1dx - m_1dy = b_1d$ $\Leftrightarrow$ $a_1x - m_1y = b_1$. Because $(a_1,m_1) = 1$ it results that the general solution of this equation is $\begin{cases} x = m_1k_1 + x_0 \\ y = a_1k_1 + y_0 \end{cases}$, where k_1 is a parameter and $k_1 \in \mathbb{Z}$, and where (x_0,y_0) constitutes a particular solution in the set of integer numbers of this equation; $x = m_1k_1 + x_0$, $k_1 \in \mathbb{Z}$, $m_1,x_0 \in \mathbb{Z}$ $\Rightarrow$ $x \equiv m_1k_1 + x_0(\bmod m)$. We'll assign values to k_1 to find all the solutions of the congruence.

It is evident that $k_1 \in \{0,1,2,...,d-1,d,d+1,...,m-1\}$ which constitutes a complete system of residues modulo m.

(Because $ax \equiv b(\bmod m)$ $\Leftrightarrow$ $ax \equiv b(\bmod -m)$, we suppose $m > 0$.)

Let $D = \{0,1,2,...,d-1\}$; $D \subseteq M$, $\forall \alpha \in M$, $\exists \beta \in D$: $\alpha \equiv \beta(\bmod d) | m_1$ (because D constitutes a complete system of residues modulo d).

It results that $\alpha m_1 = \beta m_1(\bmod dm_1)$; because $x_0 = x_0(\bmod dm_1)$, it results:

$$m_1\alpha + x_0 \equiv m_1\beta + x_0(\bmod m).$$

Therefore $\forall \alpha \in M$, $\exists \beta \in D$: $m_1\alpha + x_0 \equiv m_1\beta + x_0(\bmod m)$; thus $k_1 \in D$.

$\forall \gamma,\delta \in D$, $\gamma \not\equiv \delta(\bmod d) | m_1$ $\Rightarrow$ $\gamma m_1 \not\equiv \delta m_1(\bmod dm_1)$; $m_1 \neq 0$. It results that $m_1\gamma + x_0 \equiv m_1\delta + x_0(\bmod m)$ is false, that is, we have exactly $cardD = d$ distinct solutions.

Remark 1. If $m = 0$, the congruence $ax \equiv b(\bmod 0)$ has one solution if $a | b$; otherwise it does not have solutions.

Proof:
$ax \equiv b(\bmod 0) \Leftrightarrow ax = b$ has a solution in the set of integer numbers $\Leftrightarrow a \mid b$.

Theorem 3. (A generalization of the previous theorem)
The congruence $a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$, $m_1 \neq 0$, with $(a_1, ..., a_n, m) = d \mid b$ has $d \cdot |m|^{n-1}$ distinct solutions.

Proof:
Because $a_1x_1 + ... + a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1x_1 + ... + a_nx_n \equiv b(\bmod -m)$, we can consider $m > 0$.

The proof is done by induction on $n =$ the number of variables.
For $n = 1$ the affirmation is true in conformity with theorem 2.
Suppose that it is true for $n-1$. Let's proof that it is true for n.
Let the congruence with n variables $a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$, $a_1x_1 + ... + a_{n-1}x_{n-1} \equiv b - a_nx_n(\bmod m)$. If we consider that x_n is fixed, the congruence $a_1x_1 + ... + a_{n-1}x_{n-1} \equiv b - a_nx_n(\bmod m)$ is a congruence with $n-1$ variables. To have solutions we must have $(a_1, ..., a_{n-1}, m) = \delta \mid b - a_nx_n \Leftrightarrow b - a_nx_n \equiv 0(\bmod \delta)$.

Because $\delta \mid m \Rightarrow \dfrac{m}{\delta} \in \mathbb{Z}$, therefore we can multiply the previous congruence with $\dfrac{m}{\delta}$. It results that

$$\frac{ma_n}{\delta} x_n \equiv \frac{mb}{\delta}(\bmod \delta \cdot \frac{m}{\delta}) \qquad (*)$$

which has $\left(\dfrac{ma_n}{\delta}, \delta\dfrac{m}{\delta}\right) = \dfrac{m}{\delta}(a_n, \delta) = \dfrac{m}{\delta}\big(a_n, (a_1, ..., a_{n-1}, m)\big) = \dfrac{m}{\delta}(a_1, ..., a_{n-1}, a_n, m)\dfrac{m}{\delta} \cdot d$ distinct solutions for x_n. Let x_n^0 be a particular solution of the congruence (*). It results that $a_1x_1 + ... + a_{n-1}x_{n-1} \equiv b - a_nx_n^0(\bmod m)$ has, conform to the induction's hypothesis, $\delta \cdot m^{n-2}$ distinct solutions for $x_1, ..., x_{n-1}$ where $\delta = (a_1, ..., a_{n-1}, m)$.

Therefore the congruence $a_1x_1 + ... + a_{n-1}x_{n-1} + a_nx_n \equiv b(\bmod m)$ has $\dfrac{m}{\delta} \cdot d \cdot \delta \cdot m^{n-2} = d \cdot m^{n-1}$ distinct solutions for $x_1, ..., x_{n-1}$ and x_n.

§2. A METHOD FOR SOLVING LINEAR CONGRUENCES

Let's consider the congruence $a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$, $m \neq 0$, $a_i \equiv a_i^{'}(\bmod m)$ and $b \equiv b^{'}(\bmod m)$ with $0 \leq a_i^{'}$, $b \leq m-1$ (we made the nonrestrictive hypothesis $m > 0$). We obtain:

$a_1x_1 + ... + a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1^{'}x_1 + ... + a_n^{'}x_n \equiv b^{'}(\bmod m)$, which is a linear equation; when it is resolved in $\mathbb{Z}$ it has the general solution:

$$\begin{cases} x_1 = \alpha_{11}k_1 + ... + \alpha_{1n}k_n + \gamma_1 \\ . \\ . \\ x_n = \alpha_{n1}k_1 + ... + \alpha_{nn}k_n + \gamma_n \\ y = \alpha_{n+1,1}k_1 + ... + \alpha_{n+1,n}k_n + \gamma_{n+1} \end{cases}$$

k_j being parameters $\in \mathbb{Z}$, $j = \overline{1,n}$, $\alpha_{ij}, \gamma_i \in \mathbb{Z}$, constants, $i = \overline{1, n+1}$, $j = \overline{1,n}$.

Let's consider $\alpha_{ij}^{'} \equiv \alpha_{ij} (\bmod m)$ and $\gamma_i^{'} \equiv \gamma_i (\bmod m)$ with $0 \le \alpha_{ij}^{'}$, $\gamma' \le m-1$; $i = \overline{1, n+1}$, $j = \overline{1,n}$.

Therefore

$$\begin{cases} x_1 = \alpha_{11}^{'}k_1 + ... + \alpha_{1n}^{'}k_n + \gamma_1^{'} (\bmod m) \\ . \\ . \\ x_n = \alpha_{n1}^{'}k_1 + ... + \alpha_{nn}^{'}k_n + \gamma_n^{'} (\bmod m) \end{cases} ; k_j = \text{ parameters } \in \mathbb{Z},\ j = \overline{1,n}; \quad (**)$$

Let's consider $(\alpha_{1j}^{'}, ..., \alpha_{nj}^{'}, m) = d_j$, $j \in \overline{1,n}$. We'll prove that for k_j it would be sufficient to only give the values 0, 1, $2, ..., \frac{m}{d_j} - 1$; for $k_j = \frac{m}{d_j} - 1 + \beta'$ with $\beta' \ge 1$ we obtain $k_j = \frac{m}{d_j} + \beta$ with $\beta \ge 0$; $\beta', \beta \in \mathbb{Z}$.

$\alpha_{ij}^{'} k_j = \alpha_{ij}^{''} d_j k_j = \alpha_{ij}^{''} m + \alpha_{ij}^{''} d_j \beta \equiv \alpha_{ij}^{''} d_j \beta (\bmod m)$; we denoted $\alpha_{ij}^{'} = \alpha_{ij}^{''} d_j$ because $d_j \mid \alpha_{ij}^{'}$.

We make the notation $m = d_j m_j$, $m_j = \frac{m}{d_j}$.

Let's consider $\eta \in \mathbb{Z}$, $0 \le \eta \le m-1$ such that $\eta = \alpha_{ij}^{''} d_j \beta (\bmod d_j m_j)$; it results $d_j \mid \eta$.

Therefore $\eta = d_j \gamma$ with $0 \le \gamma \le m_{j-1}$ because we have that $d_j \gamma \equiv \alpha_{ij}^{''} d_j (\bmod d_j m_j)$, which is equivalent to $\gamma \equiv \alpha_{ij}^{''} \beta (\bmod m_j)$.

Therefore $\forall k_j \in \mathbb{N}$, $\exists \gamma \in \{0, 1, 2, ..., m_{j-1}\}$: $\alpha_{ij}^{'} k_j \equiv d_j \gamma (\bmod m)$; analogously, if the parameter $k_j \in \mathbb{Z}$. Therefore k_j takes values from 0, 1, 2,... to at most $m_j - 1$; $j \in \overline{1,n}$.

Through this parameterization for each k_j in (**), we obtain the solutions of the linear congruence. We eliminate the repetitive solutions. We obtain exactly $d \cdot |m|^{n-1}$ distinct solutions.

Example 1. Let's resolve the following linear congruence:

$$2x + 7y - 6z \equiv -3 (\bmod 4)$$

Solution: $7 \equiv 3 (\bmod 4)$, $-6 \equiv 2 (\bmod 4)$, $-3 \equiv 1 (\bmod 4)$.

It results that $2x + 3y + 2z \equiv 1 (\bmod 4)$; $(2, 3, 2, 4) = 1 \mid 1$ therefore the congruence has solutions and it has $1 \cdot 4^{3-1} = 16$ distinct solutions.

The equation $2x+3y+2z-4t=1$ resolved in integer numbers, has the general solution:

$$\begin{cases} x = 3k_1 - k_2 - 2k_3 - 1 \equiv 3k_1 + 3k_2 + 2k_3 + 3 \pmod 4 \\ y = -2k_1 \qquad\qquad + 1 \equiv 2k_1 \qquad\qquad + 1 \pmod 4 \\ z = \qquad k_2 \qquad\qquad \equiv \qquad k_2 \qquad\qquad \pmod 4 \end{cases}$$

k_j are parameters $\in \mathbb{Z}$, $j = \overline{1,3}$.

(We did not write the expression for t, because it doesn't interest us).

We assign values to the parameters. k_j takes values from 0 to at most $m_j - 1$;

k_3 takes values from 0 to $m_3 - 1 = \dfrac{m}{d_3} - 1 = \dfrac{4}{(2,0,0)} - 1 = \dfrac{4}{2} - 1 = 1$;

$$k_3 = 0 \Rightarrow \begin{pmatrix} x \equiv 3k_1 + 3k_2 + 3 \pmod 4 \\ y \equiv 2k_1 \qquad + 1 \pmod 4 \\ z \equiv \qquad k_2 \quad \pmod 4 \end{pmatrix};$$

$$k_3 = 1 \Rightarrow \begin{pmatrix} 3k_1 + 3k_2 + 1 \\ 2k_1 \qquad + 1 \\ k_2 \end{pmatrix}$$

k_1 takes values from 0 to at most 3.

$$k_1 = 0 \Rightarrow \begin{pmatrix} 3k_2 + 3 \\ 1 \\ k_2 \end{pmatrix}, \begin{pmatrix} 3k_2 + 1 \\ 1 \\ k_2 \end{pmatrix}; \quad k_1 = 1 \Rightarrow \begin{pmatrix} 3k_2 + 2 \\ 3 \\ k_2 \end{pmatrix}, \begin{pmatrix} 3k_2 \\ 3 \\ k_2 \end{pmatrix};$$

for $k_1 = 2$ and 3 we obtain the same expressions as for $k_1 = 1$ and 0.

k_2 takes values from 0 to at most 3.

$$k_2 = 0 \Rightarrow \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}; \quad k_2 = 2 \Rightarrow \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix};$$

$$k_2 = 1 \Rightarrow \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix}; \quad k_2 = 3 \Rightarrow \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix};$$

which represent all distinct solutions of the congruence.

Remark 2. By simplification or amplification of the congruence (the division or multiplication with a number $\neq 0, 1, -1$), which affects also the module, we lose solutions, respectively foreign solutions are introduced.

Example 2.

1) The congruence $2x-2y \equiv 6 \pmod 4$ has the solutions

$$\begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}0\\3\end{pmatrix};$$

2) If we would simplify by 2, we would obtain the congruence $x-y \equiv 3 \pmod 2$, which has the solutions $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$; therefore we lose solutions.

3) If we would amplify with 2, we would obtain the congruence $4x-4y \equiv 12 \pmod 4$, which has the solutions:

$$\begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}5\\0\end{pmatrix}, \begin{pmatrix}7\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}4\\1\end{pmatrix}, \begin{pmatrix}6\\1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix},$$

$$\begin{pmatrix}5\\2\end{pmatrix}, \begin{pmatrix}7\\2\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}6\\3\end{pmatrix}, \begin{pmatrix}0\\3\end{pmatrix}, \begin{pmatrix}2\\3\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix},$$

$$\begin{pmatrix}7\\4\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix}, \begin{pmatrix}3\\4\end{pmatrix}, \begin{pmatrix}5\\4\end{pmatrix}, \begin{pmatrix}0\\5\end{pmatrix}, \begin{pmatrix}2\\5\end{pmatrix}, \begin{pmatrix}4\\5\end{pmatrix}, \begin{pmatrix}6\\5\end{pmatrix},$$

$$\begin{pmatrix}1\\6\end{pmatrix}, \begin{pmatrix}3\\6\end{pmatrix}, \begin{pmatrix}5\\6\end{pmatrix}, \begin{pmatrix}7\\6\end{pmatrix}, \begin{pmatrix}2\\7\end{pmatrix}, \begin{pmatrix}4\\7\end{pmatrix}, \begin{pmatrix}6\\7\end{pmatrix}, \begin{pmatrix}0\\7\end{pmatrix};$$

therefore we introduce foreign solutions.

Remark 3. By the division or multiplication of a congruence with a number which is prime with the module, without dividing or multiplying the module, we obtain a congruence which has the same solutions with the initial one.

Example 3. The congruence $2x+3y \equiv 2 \pmod 5$ has the same solutions as the congruence $6x+9y \equiv 6 \pmod 5$ as follows:

$$\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}2\\1\end{pmatrix}, \begin{pmatrix}3\\2\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix}, \begin{pmatrix}0\\4\end{pmatrix}.$$

§2. PROPERTIES FOR SOLVING SYSTEMS OF LINEAR CONGRUENCES.

In this paragraph we will obtain some interesting theorems regarding the systems of congruences and then a method of solving them.

Theorem 1. The system of linear congruences:

(1) $a_{i1}x_1 + ... + a_{in}x_n \equiv b \pmod{m_i}$, $i = \overline{1,r}$, has solutions if and only if the system of linear equations:

(2) $a_{i1}x_1 + ... + a_{in}x_n - m_i y_i = b$, y_i unknowns $\in \mathbb{Z}$, $i = \overline{1,r}$, has solutions in the set of integer numbers.

The proof is evident.

Remark 1. From the anterior theorem it results that to solve the system of congruences (1) is equivalent with solving in integer numbers the system of linear equations (2).

Theorem 2. (A generalization of the theorem from p. 20, from [1]).

The system of congruences $a_i x \equiv b_i (\bmod m_i)$, $m_i \neq 0$, $i = \overline{1,r}$ admits solutions if and only if: $(a_i, m_i) \mid b_i$, $i = \overline{1,r}$ and $(a_i m_j,\ a_j m_i)$ divides $a_i b_j - a_j b_i$, $i, j = \overline{1,r}$.

Poof:

$\forall i = \overline{1,r}$, $a_i x \equiv b_i (\bmod m_i) \Leftrightarrow \forall i = \overline{1,r}$, $a_i x = b_i + m_i y_i$, y_i being unknowns $\in \mathbb{Z}$; these Diophantine equations, taken separately, have solutions if and only if $(a_i, m_i) \mid b_i$, $i = \overline{1,r}$.

$\forall i, j = \overline{1,r}$, from: $a_i x = b_i + y_i m_i \mid a_j$ and $a_j \cdot x = b_j + y_j \cdot m_j \mid a_i$ we obtain: $a_i a_j \cdot x = a_j b_i + a_j \cdot m_i y_i = a_i b_j + a_i \cdot m_j y_j$, Diophantine equations which have solution if and only if $(a_i m_j,\ a_j m_i) \mid a_i b_j - a_j b_i$, $i, j = \overline{1,r}$.

Consequence. (We obtain a simpler form for the theorem from p. 20 of [1]). The system of congruences $x \equiv b_i (\bmod m_i)$, $m_i \neq 0$, $i = \overline{1,r}$ has solutions if and only if $(m_i, m_j) \mid b_i - b_j$, $i, j = \overline{1,r}$.

Proof:

From theorem 2, $a_i = 1$, $\forall i = \overline{1,r}$ and $(1, m_i) = 1 \mid b_i$, $i = \overline{1,r}$.

§4. METHOD FOR SOLVING SYSTEMS OF LINEAR CONGRUENCES

Let's consider the system of linear congruences:

(3) $a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in} \equiv b_i \ (\bmod\ m_i)$, $i = \overline{1,r}$, the system's matrix rank being $r < n$, a_{ij}, b_i, $m_i \in \mathbb{Z}$, $m_i \neq 0$, $i = \overline{1,r}$, $j = \overline{1,n}$.

According to §1 from this chapter, we can consider:

(*) $0 \leq a_{ij} \leq |m_i| - 1$, $0 \leq b_i \leq |m_i| - 1$, $\forall i = \overline{1,r}$, $j = \overline{1,n}$. From the theorem 1 and the remark 1 it results that, to solve this system of congruences is equivalent with solving in integer numbers the system of equations:

(4) $a_{i1}x_1 + \ldots + a_{in}x_n - m_i y_i = b_i$, $i = \overline{1,r}$, the system's matrix rank being $r < n$.

Using the algorithm from [2], we obtain the general solution of this system:

$$\begin{cases} x_1 = \alpha_{11}k_1 + \ldots + \alpha_{1n}k_n + \beta_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = \alpha_{n1}k_1 + \ldots + \alpha_{nn}k_n + \beta_n \\ y_1 = \alpha_{n+1,1}k_1 + \ldots + \alpha_{n+1,n}k_n + \beta_{n+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_r = \alpha_{n+r,1}k_1 + \ldots + \alpha_{n+r,n}k_n + \beta_{n+r} \end{cases}$$

$\alpha_{hj}, \beta_h \in \mathbb{Z}$ and k_j are parameters $\in \mathbb{Z}$.

Let's consider $m = [m_1, ..., m_r] > 0$; because the variables $y_1, ..., y_r$ don't interest us, we'll retain only the expressions of $x_1, ..., x_n$.
Therefore:

(5) $x_i = \alpha_{i1}k_1 + ... + \alpha_{in}k_n + \beta_i$, $i = \overline{1,n}$ and again we can suppose that

(**) $0 \le \alpha_{hj} \le m-1$, $0 \le \beta_h \le m-1$, $h = \overline{1,n}$, $j = \overline{1,n}$.

We have: $x_i \equiv \alpha_{i1}k_1 + ... + \alpha_{in}k_n + \beta_i (\bmod m)$, $i = \overline{1,n}$. Evidently k_j takes the values of at most the integer numbers from 0 to $m-1$. Conform to the same observations from §1 from this chapter, for k_j it is sufficient to give only the values $0,1,2,..., \frac{m}{d_j} - 1$ where

(***) $d_j = \left(\alpha_{1j}, ..., \alpha_{nj}, m\right)$, for any $j = \overline{1,n}$.

By the parameterization of $k_1, ..., k_n$ in (5) we obtain all the solutions of the system of linear congruence (1); k_j takes at most the values $0,1,2,..., \frac{m}{d_j} - 1$; we eliminate the repeating solutions.

Remark 2. The considerations (*), (**), and (***) have the roll of making the calculation easier, to reduce the computational volume. This algorithm of solving the linear congruence works also without these considerations, but it is more difficult.

Example. Let's solve the following system of linear congruences:

$$(6) \quad \begin{cases} 3x + 7y - z \equiv 2 (\bmod 2) \\ \quad 5y - 2z \equiv 1 (\bmod 3) \end{cases}$$

Solution: The system of linear congruences (6) is equivalent with:

$$(7) \quad \begin{cases} x + y + z \equiv 0 (\bmod 2) \\ \quad 2y + z \equiv 1 (\bmod 3) \end{cases}$$

which is equivalent with the system of linear equations:

$$(8) \quad \begin{cases} x + y + z - 2t_1 = 0 \\ \quad 2y + z - 3t_2 = 1 \end{cases}$$

x, y, z, t_1, t_2 unknowns $\in \mathbb{Z}$

This has the general solution (see [2]):

$$\begin{cases} x = -2k_1 + 2k_2 + 3k_3 + 1 \\ y = k_1 - 3k_3 - 1 \\ z = k_1 \\ t_1 = k_2 \\ t_2 = k_3 \end{cases}$$

where k_1, k_2, k_3 are parameters $\in \mathbb{Z}$.

The values of t_1 and t_2 don't interest us; $m = [2, 3] = 6$. Therefore:

$$\begin{cases} x \equiv 4k_1 + 2k_2 + 3k_3 + 1 \pmod 6 \\ y \equiv \;\; k_1 \qquad\quad + 3k_3 + 5 \pmod 6 \\ z \equiv \;\; k_1 \qquad\qquad\qquad\quad \pmod 6 \end{cases}$$

k_3 takes values from 0 to $\dfrac{6}{(3,3,0,6)} - 1 = 1$; k_2 from 0 to 2; k_1 from 0 to at most 5.

$$k_3 = 0 \;\Rightarrow\; \begin{pmatrix} x \equiv 4k_1 + 2k_2 + 1 \pmod 6 \\ y \equiv \;\; k_1 \qquad\quad + 5 \pmod 6 \\ z \equiv \;\; k_1 \qquad\qquad\quad \pmod 6 \end{pmatrix};$$

$$k_3 = 1 \;\Rightarrow\; \begin{pmatrix} 4k_1 + 2k_2 + 4 \\ k_1 \qquad + 2 \\ k_1 \end{pmatrix};$$

$$k_2 = 0,1,2 \;\Rightarrow\; \begin{pmatrix} 4k_1 + 1 \\ k_1 + 5 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 4 \\ k_1 + 2 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 3 \\ k_1 + 5 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 \\ k_1 + 2 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 5 \\ k_1 + 5 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 2 \\ k_1 + 2 \\ k_1 \end{pmatrix};$$

$k_1 = 0,1,2,3,4,5 \;\Rightarrow$

$$\begin{pmatrix}1\\5\\0\end{pmatrix}, \begin{pmatrix}4\\2\\0\end{pmatrix}, \begin{pmatrix}3\\5\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}5\\5\\0\end{pmatrix}, \begin{pmatrix}2\\2\\0\end{pmatrix}, \begin{pmatrix}5\\0\\1\end{pmatrix}, \begin{pmatrix}2\\3\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}4\\3\\1\end{pmatrix}, \begin{pmatrix}3\\0\\1\end{pmatrix}, \begin{pmatrix}0\\3\\1\end{pmatrix},$$

$$\begin{pmatrix}3\\1\\2\end{pmatrix}, \begin{pmatrix}0\\4\\2\end{pmatrix}, \begin{pmatrix}5\\1\\2\end{pmatrix}, \begin{pmatrix}2\\4\\2\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}, \begin{pmatrix}4\\4\\2\end{pmatrix}, \begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}4\\5\\3\end{pmatrix}, \begin{pmatrix}3\\2\\3\end{pmatrix}, \begin{pmatrix}0\\5\\3\end{pmatrix}, \begin{pmatrix}5\\2\\3\end{pmatrix}, \begin{pmatrix}2\\5\\3\end{pmatrix},$$

$$\begin{pmatrix}5\\3\\4\end{pmatrix}, \begin{pmatrix}2\\0\\4\end{pmatrix}, \begin{pmatrix}1\\3\\4\end{pmatrix}, \begin{pmatrix}4\\0\\4\end{pmatrix}, \begin{pmatrix}3\\3\\4\end{pmatrix}, \begin{pmatrix}0\\0\\4\end{pmatrix}, \begin{pmatrix}3\\4\\5\end{pmatrix}, \begin{pmatrix}0\\1\\5\end{pmatrix}, \begin{pmatrix}5\\4\\5\end{pmatrix}, \begin{pmatrix}2\\1\\5\end{pmatrix}, \begin{pmatrix}1\\4\\5\end{pmatrix}, \begin{pmatrix}4\\1\\5\end{pmatrix};$$

which constitute the 36 distinct solutions of the system of linear congruences (6).

REFERENCES

[1] Constantin P. Popovici – “Curs de teoria numerelor”, EDP, Bucureşti, 1973.

[2] Florentin Smarandache – “Integer algorithms to solve linear equations and systems”, Ed. Scientifique, Casablanca, 1984.

[Published in “Gamma”, Year X, Nos. 1-2, October 1987.]

BASES OF SOLUTIONS FOR LINEAR CONGRUENCES

In this article we establish some properties regarding the solutions of a linear congruence, bases of solutions of a linear congruence, and the finding of other solutions starting from these bases.

This article is a continuation of my article “On linear congruences”.

§1. Introductory Notions

Definition 1. (linear congruence)

We call linear congruence with n unknowns a congruence of the following form:

$a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$ (1)

where $a_1,...,a_n,\ m \in \mathbb{Z},\ n \geq 1,$ and $x_i,\ i = \overline{1,n}$, are the unknowns.

The following theorems are known:

Theorem 1. The linear congruence (1) has solutions if and only if $(a_1,...,a_n,m,b) \mid b$.

Theorem 2. If the linear congruence (1) has solutions, then: $|d| \cdot |m|^{n-1}$ is its number of distinct solutions. (See the article “On the linear congruences”.)

Definition 2. Two solutions $X = (x_1,...,x_n)$ and $Y = (y_1,...,y_n)$ of the linear congruence (1) are distinct (different) if $\exists i \in \overline{1,n}$ such that $x_i \not\equiv y_i (\bmod m)$.

§2. Definitions and proprieties of congruences

We’ll present some arithmetic properties, which will be used later.

Lemma 1. If $a_1,...,a_n \in \mathbb{Z}$, $m \in \mathbb{Z}$, then:

$$\frac{(a_1,...,a_n,m) \cdot m^{n-1}}{(a_1,m) \cdot ... \cdot (a_n,m)} \in \mathbb{Z}$$

The proof is done using complete induction for $n \in \mathbb{N}^*$.

When $n = 1$ it is evident.

Considering that it is true for values smaller or equal to n, let’s proof that it is true for $n+1$.

Let’s note $x = (a_1,...,a_n)$. Then:

$(a_1,...,a_n,a_{n+1},m) \cdot m^n = \left[(x,a_{n+1},m) \cdot m^{2-1}\right] \cdot m^{n-1}$, which, in accordance to the induction hypothesis, is divisible by:

$\left[(x,m) \cdot (a_{n+1},m)\right] \cdot m^{n-1} = \left[(a_1,...,a_n,m) \cdot (a_{n+1},m)\right] \cdot m^{n-1} = \left[(a_1,...,a_n,m) \cdot m^{n-1}\right] \cdot (a_{n+1},m)$,

which is divisible, also in accordance with the induction hypothesis, by $\left[(a_1,m) \cdot ... \cdot (a_n,m)\right] \cdot (a_{n+1},m) = (a_1,m) \cdot ... \cdot (a_n,m) \cdot (a_{n+1},m)$.

Theorem 3. If X^0 constitutes a (particular) solution of the linear congruence (1), and $p = \prod_{i=1}^{n}(a_i, m)$, then:

$$X_i \equiv x_i^0 + \frac{m}{(a_i,m)} t_i, \ \ 0 \le t_i < (a_i,m), \ \ t_i \in \mathbb{N} \quad (*)$$

(i taking values from 1 to n) constitute p distinct solutions of (1).

Proof:

Because the module of the congruence (m) is sub-understood, we omitted it, and we will continue to omit it.

$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i x_i^0 + \sum_{i=1}^{n} \frac{a_i m}{(a_i,m)} t_i \equiv b + 0$, therefore there are solutions. Let's show that they are also distinct.

$x_i^0 + \frac{m}{(a_i,m)}\alpha \not\equiv x_i^0 + \frac{m}{(a_i,m)}\beta$, for $\alpha, \beta \in \mathbb{N}, \ \alpha \ne \beta,$ and $0 \le \alpha, \beta < (a_i,m)$, because the set:

$\left\{ \frac{m}{(a_i,m)} t_i \mid \ 0 \le t_i < (a_i,m), \ t_i \in \mathbb{N} \right\} \subseteq \{0,1,...,n-1\}$, which constitutes a complete system of residues modulo m, and $\frac{m}{(a_i,m)}\alpha \ne \frac{m}{(a_i,m)}\beta$, for α and β previously defined .

Therefore the theorem is proved.

*

* *

One considers the Z-module A generated by the vectors V_i, where $V_i^* = \left(\underbrace{0,...,0}_{i-1 \ times}, \ \frac{m}{(a_i,m)}, \ \underbrace{0,...,0}_{n-i \ times} \right), \ i = \overline{1,n},$ from $\mathbb{Z}^n$. The module A has the rank $n, \ (n \ge 1)$. We could note it $A = \{v_1,...,v_n\}$.

We'll introduce a few new terms.

Definition 3. Two solutions (vectors solution) X and Y of congruence (1) are called independent if $X - Y \notin A$. Otherwise, they are called dependent solutions.

Remark 1. In other words, if X is a solution of the congruence (1), then the solution Y of the same congruence is independent of X, if it was not obtained from X by applying the formula (*) for certain values of the parameters $t_1,...,t_n$.

Definition 4. The solutions $X^1,...,X^n$ are called independent (all together) if they are independent two by two.

Otherwise, they are called dependent solutions (all together).

Definition 5. The solutions $X^1,...,X^n$ of the congruence (1) constitute a base for this congruence, if $X^1,...,X^n$ are independent amongst them, and with their help one obtains all (distinct) solutions of the congruence with the procedure (*) using the parameters $t_1,...,t_n$.

Some proprieties of the linear congruences solutions:

1) If the solution X^1 is independent with the solution X^2 then X^2 is independent with X^1 (the commutative property of the relation "independent").
2) X^1 is not independent with X^1.
3) If X^1 is independent with X^2, X^2 is independent with X^3, it does not imply that X^1 is independent with X^3 (the relation is not transitive).
4) If X is independent with Y, then X is independent with Y.

Indeed, if Y is dependent with Y, then $X-Y=\underbrace{(X-Y)}_{\notin A}+\underbrace{(Y-Y_1)}_{\in A}=Z$.

If $Z \in A$, it results that $(X-Y)=Z-(Y-Y_1)\in A$ because A is a Z- module. Absurdity.

*

* *

Theorem 4. Let's note $P_1=(a_1,...,a_n,m)\cdot|m|^{n-1}$ and $P_2=(a_1,m)\cdot...\cdot(a_n,m)$ then the linear congruence (1) has the base formed of: $\frac{P_1}{P_2}$ solutions.

Proof:

$P_1>0$ and $P_2>0$, from Lemma 1 we have $\frac{P_1}{P_2}\in\mathbb{N}^*$, therefore the theorem has sense (we consider LCD as a positive number).

P_1 represents the number of distinct solutions (in total) of congruence (1), in accordance to theorem 2.

P_2 represents the number of distinct solutions obtained for congruence (1) by applying the procedure (*) (allocating to parameters $t_1,...,t_n$ all possible values) to a single particular solution.

Therefore we must apply the procedure (*) $\frac{P_1}{P_2}$ times to obtain all solutions of the congruence, that is, it is necessary of exact $\frac{P_1}{P_2}$ independent particular solutions of the congruence. That is, the base has $\frac{P_1}{P_2}$ solutions.

Remark 2. Any base of solutions (for the same linear congruence) has the same number of vectors.

§3. Method of solving the linear congruences

In this paragraph we will utilize the results obtained in the precedent paragraphs.

Let's consider the linear congruence (1) with $(a_1,...,a_n,m)=d\,|\,b,\ m\neq 0$.

- we determine the number of distinct solutions of the congruence: $P_1=|d|\cdot|m|^{n-1}$;
- we determine the number of solutions from the base: $S=\dfrac{P_1}{\prod_{i=1}^{n}(a_i,m)}$;
- we construct the Z-module $A=\{V_1,...,V_n\}$, where

  $V_i^t=\left(\underbrace{0,...,0}_{i-1\ times},\ \dfrac{m}{(a_i,m)},\ \underbrace{0,...,0}_{n-i\ times}\right),\ \ i=\overline{1,n}$;
- we search to find s independent (particular) solutions of the congruence;
- we apply the procedure (*) as follows:

if X^j, $j=\overline{1,s}$, are the s independent solutions from the base, it results that

$$X^{j(t_1,...,t_n)}=\left(x_i^j+\frac{m}{(a_i,m)}t_i\right),\quad i=\overline{1,n}, \qquad (*)$$

are all P_1 solutions of the linear congruence (1),

$$j=\overline{1,s},\ \ t_1\times...\times t_n\in\{0,1,2,...,d_1-1\}\times...\times\{0,1,2,...,d_n-1\},$$

where $d_i=\left|(a_i,m)\right|,\ \ i=\overline{1,n}$.

Remark 3. The correctness of this method results from the anterior paragraphs.

Application. Let's consider the linear non-homogeneous congruence $2x-6y\equiv 2(\mathrm{mod}\,12)$. It has $(2,6,12)\cdot 12^{2-1}=24$ distinct solutions. Its base will have $24:\left[(2,12)\cdot(6,12)\right]=2$ solutions.

$V_1^t=(6,0),\ V_2^t=(0,2)$ and $A=\{V_1,V_2\}=\{(6t_1,2t_2)^t\ |\ t_1,t_2\in\mathbb{Z}\}$.

The solutions $x\equiv 7(\mathrm{mod}\,12)$ and $y\equiv 4(\mathrm{mod}\,12)$, $x\equiv 1$ and $y\equiv 0$ are dependent because:

$$\begin{pmatrix}7\\0\end{pmatrix}-\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}6\\4\end{pmatrix}=1\begin{pmatrix}6\\0\end{pmatrix}+2\begin{pmatrix}0\\2\end{pmatrix}\in A.$$

But $\begin{pmatrix}4\\1\end{pmatrix}$ is independent with $\begin{pmatrix}0\\1\end{pmatrix}$ because $\begin{pmatrix}4\\1\end{pmatrix}-\begin{pmatrix}0\\1\end{pmatrix}\notin A$.

Therefore, the 24 solutions of the congruence can be obtained from:

$$\begin{cases}x\equiv 1+6t_1, & 0\le t_1<2,\ \ t_1\in\mathbb{N}\\ y\equiv 0+2t_2, & 0\le t_2<6,\ \ t_2\in\mathbb{N}\end{cases}$$

and

$$\begin{cases}x\equiv 4+6t_1, & 0\le t_1<2,\ \ t_1\in\mathbb{N}\\ y\equiv 1+2t_2, & 0\le t_2<6,\ \ t_2\in\mathbb{N}\end{cases}$$

by the parameterization $(t_1,t_2)\in\{0,1\}\times\{0,1,2,3,4,5\}$.

$$\begin{cases} x \equiv 1 + 6t_1 \\ y \equiv 0 + 2t_2 \end{cases} \Rightarrow \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix}, \begin{pmatrix}1\\6\end{pmatrix}, \begin{pmatrix}1\\8\end{pmatrix}, \begin{pmatrix}1\\10\end{pmatrix}, \begin{pmatrix}7\\0\end{pmatrix}, \begin{pmatrix}7\\2\end{pmatrix}, \begin{pmatrix}7\\4\end{pmatrix}, \begin{pmatrix}7\\6\end{pmatrix}, \begin{pmatrix}7\\8\end{pmatrix}, \begin{pmatrix}7\\10\end{pmatrix}.$$

$$\begin{cases} x \equiv 4 + 6t_1 \\ y \equiv 1 + 2t_2 \end{cases} \Rightarrow \begin{pmatrix}4\\1\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix}, \begin{pmatrix}4\\5\end{pmatrix}, \begin{pmatrix}4\\7\end{pmatrix}, \begin{pmatrix}4\\9\end{pmatrix}, \begin{pmatrix}4\\11\end{pmatrix}, \begin{pmatrix}10\\1\end{pmatrix}, \begin{pmatrix}10\\3\end{pmatrix}, \begin{pmatrix}10\\5\end{pmatrix}, \begin{pmatrix}10\\7\end{pmatrix}, \begin{pmatrix}10\\9\end{pmatrix}, \begin{pmatrix}10\\11\end{pmatrix};$$

which constitute all 24 distinct solutions of the given congruence; $\begin{pmatrix}0\\1\end{pmatrix}$ means: $x \equiv 1 (\mathrm{mod}\, 12)$ and $y \equiv 0 (\mathrm{mod}\, 12)$; etc.

REFERENCES

[1] C. P. Popovici – “Teoria numerelor”, Editura didactică şi pedagogică, Bucureşti, 1973.

[2] F. Gh. Smarandache – “Rezolvarea ecuațiilor şi a sistemelor de ecuații liniare în numere întregi” - Lucrare de licență, Universitatea din Craiova, 1979.

[Published in “Bulet. Univ. Braşov”, series C, vol. XXII, pp. 25-31, 1980; and in “Bulet. Şt. şi Tehn. al Instit. Polit. “Traian Vuia”, Timişoara”, fascicolul 2, tomul 26 (40), pp. 13-6; MR: 83c: 10024]

CRITERIA OF PRIMALITY

Abstract: In this article we present four necessary and sufficient conditions for a natural number to be prime.

Theorem 1. Let p be a natural number, $p \geq 3$: p is prime if and only if $(p-3)! \equiv \frac{p-1}{2} (\bmod p)$.

Proof:

Necessity: p is prime $\Rightarrow (p-1)! \equiv -1 (\bmod p)$ conform to Wilson's theorem. It results that $(p-1)(p-2)(p-3)! \equiv -1 (\bmod p)$, or $2(p-3)! \equiv p-1 (\bmod p)$. But p being a prime number ≥ 3 it results that $(2, p) = 1$ and $\frac{p-1}{2} \in \mathbb{Z}$. It has sense the division of the congruence by 2, and therefore we obtain the conclusion.

Sufficiency: We multiply the congruence $(p-3)! \equiv \frac{p-1}{2} (\bmod p)$ with $(p-1)(p-2) \equiv 2 (\bmod p)$ (see [1], pp. 10-16) and it results that $(p-1)! \equiv -1 (\bmod p)$, from Wilson's theorem, which makes us conclude that p is prime.

Lemma 1. Let m be a natural number > 4. Then m is a composite number if and only if $(m-1)! \equiv 0 (\bmod m)$.

Proof:

The sufficiency is evident conform to Wilson's theorem.

Necessity: m can be written as $m = a_1^{\alpha_1} \ldots a_s^{\alpha_s}$, where a_i are positive prime numbers, two by two distinct and $\alpha_i \in \mathbb{N}^*$, for any i, $1 \leq i \leq s$.

If $s \neq 1$ then $a_i^{\alpha_i} < m$, for any i, $1 \leq i \leq s$.

Therefore $a_1^{\alpha_1} \ldots a_s^{\alpha_s}$ are distinct factors in the product $(m-1)!$ thus $(m-1)! \equiv 0 (\bmod m)$.

If $s = 1$ then $m = a^{\alpha}$ with $\alpha \geq 2$ (because m is non-prime). When $\alpha = 2$ we have $a < m$ and $2a < m$ because $m > 4$. It results that a and $2a$ are different factors in $(m-1)!$ and therefore $(m-1)! \equiv 0 (\bmod m)$. When $\alpha > 2$, we have $a < m$ and $a^{\alpha-1} < m$, and a and $a^{\alpha-1}$ are different factors in the product $(m-1)!$.

Therefore $(m-1)! \equiv 0 (\bmod m)$ and the lemma is proved for all cases.

Theorem 2. Let p be a natural number greater than 4. Then p is prime if and only if $(p-4)! \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p)$, where [x] is the integer part of x, i.e. the largest integer less than or equal to x.

Proof:

Necessity: $(p-4)!(p-3)(p-2)(p-1) \equiv -1 (\bmod p)$ from Wilson's theorem, or $6(p-4)! \equiv 1 (\bmod p)$; p being prime and greater than 4, it results that $(6, p) = 1$.

It results that $p = 6k \pm 1$, $k \in \mathbb{N}^*$.

A) If $p = 6k - 1$, then $6 \mid (p+1)$ and $(6, p) = 1$, and dividing the congruence $6(p-4)! \equiv p + 1 (\bmod p)$, which is equivalent with the initial one, by 6 we obtain:

$$(p-4)! \equiv \frac{p+1}{6} \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p).$$

B) If $p = 6k + 1$, then $6 \mid (1-p)$ and $(6, p) = 1$, and dividing the congruence $6(p-4)! \equiv 1 - p (\bmod p)$, which is equivalent to the initial one, by 6 it results:

$$(p-4)! \equiv \frac{1-p}{6} \equiv -k \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p).$$

Sufficiency: We must prove that p is prime. First of all we'll show that $p \neq \mathcal{M}6$.

Let's suppose by absurd that $p = 6k$, $k \in \mathbb{N}^*$. By substituting in the congruence from hypothesis, it results $(6k-4)! \equiv -k (\bmod 6k)$. From the inequality $6k - 5 \geq k$ for $k \in \mathbb{N}^*$, it results that $k \mid (6k-5)!$. From $2 \mid (6k-4)$, it results that $2k \mid (6k-5)!(6k-4)$. Therefore $2k \mid (6k-4)!$ and $2k \mid 6k$, it results (conform with the congruencies' property) (see [1], pp. 9-26) that $2k \mid (-k)$, which is not true; and therefore $p \neq \mathcal{M}6$.

From $(p-1)(p-2)(p-3) \equiv -6 (\bmod p)$ by multiplying it with the initial congruence it results that: $(p-1)! \equiv (-1)^{\left[\frac{p}{3}\right]} 6 \cdot \left[\frac{p+1}{6}\right] (\bmod p)$.

Let's consider lemma 1; for $p > 4$ we have:

$$(p-1)! \equiv \begin{cases} 0 (\bmod p), \text{ if } p \text{ is not prime;} \\ -1 (\bmod p), \text{ if } p \text{ is prime;} \end{cases}$$

a) If $p = 6k + 2 \Rightarrow (p-1)! \equiv 6k \not\equiv 0 (\bmod p)$.

b) If $p = 6k + 3 \Rightarrow (p-1)! \equiv -6k \not\equiv 0 (\bmod p)$.

c) If $p = 6k + 4 \Rightarrow (p-1)! \equiv -6k \not\equiv 0 (\bmod p)$.

Thus $p \neq \mathcal{M}6 + r$ with $r \in \{0, 2, 3, 4\}$.

It results that p is of the form: $p = 6k \pm 1$, $k \in \mathbb{N}^*$ and then we have: $(p-1)! \equiv -1 (\bmod p)$, which means that p is prime.

Theorem 3. If p is a natural number ≥ 5, then p is prime if and only if $(p-5)! \equiv rh + \frac{r^2 - 1}{24} (\bmod p)$, where $h = \left[\frac{p}{24}\right]$ and $r = p - 24h$.

Proof:

Necessity: if p is prime, it results that:

$(p-5)!(p-4)(p-3)(p-2)(p-1) \equiv -1 (\bmod p)$ or

$24(p-5)! \equiv -1 \pmod{p}$.

But p could be written as $p = 24h + r$, with $r \in \{1, 5, 7, 11, 13, 17, 19, 23\}$, because it is prime. It can be easily verified that $\frac{r^2-1}{24} \in \mathbb{Z}$.

$$24(p-5)! \equiv -1 + r(24h + r) \equiv 24rh + r^2 - 1 \pmod{p}.$$

Because $(24, p) = 1$ and $24 \mid (r^2 - 1)$ we can divide the congruence by 24, obtaining: $(p-5)! \equiv rh + \frac{r^2-1}{24} \pmod{p}$.

Sufficiency: p can be written $p = 24h + r$, $0 \le r < 24$, $h \in \mathbb{N}$.
Multiplying the congruence $(p-4)(p-3)(p-2)(p-1) \equiv 24 \pmod{p}$ with the initial one, we obtain: $(p-1)! \equiv r(24h + r) - 1 \equiv -1 \pmod{p}$.

Theorem 4. Let's consider $p = (k-1)!h + 1$, $k > 2$ a natural number.
Then: p is prime if and only if

$$(p-k)! \equiv (-1)^{h + \left[\frac{p}{h}\right] + 1} \cdot h \pmod{p}.$$

Proof: $(p-1)! \equiv -1 \pmod{p} \Leftrightarrow (p-k)!(-1)^{k-1}$ (k-1)!≡ -1(mod p) ⇔ (p-k)!(k-1)! ≡ (-1)^{k}(mod p) .

We have: $((k-1)!, p) = 1$ (1)

A) $p = (k-1)!h - 1$.

a) k is an even number $\Rightarrow (p-k)!(k-1)! \equiv 1 + p \pmod{p}$, and because of the relation (1) and $(k-1)! \mid (1+p)$, by dividing with $(k-1)!$ we have: $(p-k)! \equiv h \pmod{p}$.

b) k is an odd number $\Rightarrow (p-k)!(k-1)! \equiv -1 - p \pmod{p}$ and because of the relation (1) and $(k-1)! \mid (-1-p)$, by dividing with $(k-1)!$ we have: $(p-k)! \equiv -h \pmod{p}$

B) $p = (k-1)!h + 1$

a) k is an even number $\Rightarrow (p-k)!(k-1)! \equiv 1 - p \pmod{p}$, and because $(k-1)! \mid (1-p)$ and of the relation (1), by dividing with $(k-1)!$ we have: $(p-k)! \equiv -h \pmod{p}$.

b) k is an odd number $\Rightarrow (p-k)!(k-1)! \equiv -1 + p \pmod{p}$, and because $(k-1)! \mid (-1+p)$ and of the relation (1), by dividing with $(k-1)!$ we have $(p-k)! \equiv h \pmod{p}$.

Putting together all these cases, we obtain: if p is prime, $p = (k-1)!h \pm 1$, with $k > 2$ and $h \in \mathbb{N}^*$, then

$$(p-k)! \equiv (-1)^{h + \left[\frac{p}{h}\right] + 1} \cdot h \pmod{p}.$$

Sufficiency: Multiplying the initial congruence by $(k-1)!$ it results that:

$$(p-k)!(k-1)! \equiv (k-1)!h \cdot (-1)^{\left[\frac{p}{h}\right] + 1} \cdot (-1)^k \pmod{p}.$$

Analyzing separately each of these cases:

A) $p = (k-1)!h - 1$ and

B) $p = (k-1)!h + 1$, we obtain for both, the congruence:

$$(p-k)!(k-1)! \equiv (-1)^k (\mathrm{mod}\, p)$$

which is equivalent (as we showed it at the beginning of this proof) with $(p-1)! \equiv -1(\mathrm{mod}\, p)$ and it results that p is prime.

REFERENCE:

[1] Constantin P. Popovici, "Teoria numerelor", Editura Didactică şi Pedagogică, Bucharest, 1973.

[Published in "Gazeta Matematică", Bucharest, Year XXXVI, No. 2, pp. 49-52, February 1981]

INTEGER ALGORITHMS TO SOLVE DIOPHANTINE LINEAR EQUATIONS AND SYSTEMS

Abstract: Two algorithms for solving Diophantine linear equations and five algorithms for solving Diophantine linear systems, together with many examples, are presented in this paper.

Keywords: Diophantine equations, Diophantine systems, particular integer solutions, general integer solutions

Contents:

Introduction:

The present work includes some of the author's original researches on the integer solutions of equations and linear systems:

1. The notion of "general integer solution" of a linear equation with two unknowns is extended to linear equations with n unknowns and then, to linear systems.
2. The properties of the general integer solution are determined (both of a linear equation and of a linear system).
3. Seven original integer algorithms (two for linear equations and five for linear systems) are presented. The algorithms are carefully demonstrated and an example for each of them is presented. These algorithms can be easily introduced into computer.

INTEGER SOLUTIONS OF LINEAR EQUATIONS

Definitions and properties of the integer solutions of linear equations.

Consider the following linear equation:

(1) $$\sum_{i=1}^{n} a_i x_i = b,$$

with all $a_i \neq 0$ and b in $\mathbb{Z}$.

Again, let $h \in \mathbb{N}$, and $f_i : \mathbb{Z}^h \to \mathbb{Z}$, $i = \overline{1,n}$. ($\overline{1,n}$ means: all integers from 1 to n).

Definition 1.
$x_i = x_i^0$, $i = \overline{1,n}$, is a particular integer solution of equation (1), if all $x_i^0 \in \mathbb{Z}$ and $\sum_{i=1}^{n} a_i x_i^0 = b$.

Definition 2.
$x_i = f_i(k_1,...,k_h)$, $i = \overline{1,n}$, is the general integer solution of equation (1) if:

a) $\sum_{i=1}^{n} a_i f_i(k_1,...,k_h) = b; \quad \forall (k_1,...,k_h) \in \mathbb{Z}^h$,

b) For any particular integer solution of equation (1), $x_i = x_i^0$, $i = \overline{1,n}$, there exist $(k_1^0,...,k_h^0) \in \mathbb{Z}^h$ such that $x_i^0 = f_i(k_1^0,...,k_h^0)$ for all $i = \overline{1,n}$ {i. e. any particular integer solution can be extracted from the general integer solution by parameterization}.

We will further see that the general integer solution can be expressed by linear functions.

For $1 \le i \le n$ we consider the functions $f_i = \sum_{j=1}^{h} c_{ij} k_j + d_i$ with all $c_{ij},\ d_i \in \mathbb{Z}$.

Definition 3.
$A = (c_{ij})_{i,j}$ is the matrix associated with the general solution of equation (1).

Definition 4.
The integers $k_1,...,k_s$, $1 \le s \le h$ are independent if all the corresponding column vectors of matrix A are linearly independent.

Definition 5.
An integer solution is s-times undetermined if the maximal number of independent parameters is s.

Theorem 1. The general integer solution of equation (1) is $(n-1)$-times undetermined.

Proof:

We suppose that the particular integer solution is of the form:

(2) $x_i = \sum_{e=1}^{r} u_{ie} P_e + v_i,\ \ i = \overline{1,n}$, with all $u_{ie},\ v_i \in \mathbb{Z}$,

P_e are parameters of $\mathbb{Z}$, while $a \le r < n-1$.

Let $(x_1^0, ..., x_n^0)$ be a general integer solution of equation (1) (we are not interested in the case when the equation does not have an integer solution). The solution:

$$\begin{cases} x_j = a_n k_j + x_j^0, & j = \overline{1, n-1} \\ x_n = -\left(\sum_{j=1}^{n-1} a_j k_j - x_n^0 \right) \end{cases}$$

is undetermined $(n-1)$-times (it can be easily checked that the order of the associated matrix is $n-1$). Hence, there are $n-1$ undetermined solutions. Let's consider, in the general case, a solution be undetermined $(n-1)$-times:

$x_i = \sum_{j=1}^{n-1} c_{ij} k_j + d_i$, $i = \overline{1,n}$ with all $c_{ij},\ d_i \in \mathbb{Z}$.

Consider the case when $b = 0$.

Then

$$\sum_{i=1}^{n} a_i x_i = 0.$$

It follows:

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij} k_j + d_i \right) = \sum_{i=1}^{n} a_i \sum_{j=1}^{n-1} c_{ij} k_j + \sum_{i=1}^{n} a_i d_i = 0.$$

For $k_j = 0$, $j = \overline{1, n-1}$ it follows that $\sum_{i=1}^{n} a_i d_i = 0$.

For $k_{j_0} = 1$ and $k_j = 0,\ j \ne j_0$, it follows that $\sum_{i=1}^{n} a_i c_{ij_0} = 0$.

Let's consider the homogenous linear system of n equations with n unknowns:

$$\begin{cases} \sum_{i=1}^{n} x_i c_{ij} = 0, & j = \overline{1, n-1} \\ \sum_{i=1}^{n} x_i d_i = 0 \end{cases}$$

which, obviously, has the solution $x_i = a_i$, $i = \overline{1,n}$ different from the trivial one. Hence the determinant of the system is zero, i.e., the vectors $c_j = \left(c_{1j}, ..., c_{nj}\right)^t$, $j = \overline{1, n-1}$, $D = \left(d_1, ..., d_n\right)^t$ are linearly dependent.

But the solution being $(n-1)$-times undetermined it shows that $c_j,\ j=\overline{1,n-1}$ are linearly independent. Then $(c_1,...,c_{n-1})$ determines a free sub-module $\mathbb{Z}$ of order $n-1$ in $\mathbb{Z}_n$ of solutions for the given equation.

Let's see what can we obtain from (2). We have:
$$0=\sum_{i=1}^{n}a_i x_i=\sum_{i=1}^{n}a_i\left(\sum_{e=1}^{r}u_{ie}P_e+v_i\right).$$
As above, we obtain:
$$\sum_{i=1}^{n}a_i v_i=0 \text{ and } \sum_{e=1}^{r}a_i u_{ie_0}=0$$
similarly, the vectors $U_h=(u_{1h},...,u_{nh})$ are linearly independent, $h=\overline{1,r}$, U_h, $h=\overline{1,r}$ are $V=(v_1,...,v_n)$ particular integer solutions of the homogenous linear equation.

Sub-case (a1)

$U,h=\overline{1,r}$ are linearly dependent. This gives $\{U_1,...,U_r\}=$ the free sub-module of order r in $\mathbb{Z}^n$ of solutions of the equation. Hence, there are solutions from $\{V_1,...,V_{n-1}\}$ which are not from $\{U_1,...,U_r\}$; this contradicts the fact that (2) is the general integer solution.

Sub-case (a2)

$U_h,\ h=\overline{1,r},\ V$ are linearly independent. Then $\{U_1,...,U_r\}+V$ is a linear variety of the dimension $<n-1=\dim\{V_1,...,V_{n-1}\}$ and the conclusion can be similarly drawn.

Consider the case when $b\neq 0$. So, $\sum_{i=1}^{n}a_i x_i=b$.

Then:
$$\sum_{i=1}^{n}a_i\left(\sum_{j=1}^{n-1}c_{ij}k_j+d_i\right)=\sum_{j=1}^{n-1}\left(\sum_{i=1}^{n}a_i c_{ij}\right)k_j+\sum_{i=1}^{n}a_i d_i=b;\ \ \forall(k_1,...,k_{n-1})\in\mathbb{Z}^{n-1}.$$
As in the previous case, we obtain $\sum_{i=1}^{n}a_i d_i=b$ and $\sum_{i=1}^{n}a_i c_{ij}=0,\qquad \forall\ j=\overline{1,n-1}$.

The vectors $c_j=(c_{ij},...,c_{nj})^t$, $j=\overline{1,n-1}$, are linearly independent because the solution is undetermined $(n-1)$-times.

Conversely, if $c_1,...,c_{n-1},\ D$ (where $D=(d_1,...,d_n)^t$) were linearly dependent, it would mean that $D=\sum_{j=1}^{n-1}s_j c_j$ with all s_j scalar; it would also mean that
$$b=\sum_{i=1}^{n}a_i d_i=\sum_{i=1}^{n}a_i\left(\sum_{j=1}^{n-1}s_j c_{ij}\right)=\sum_{j=1}^{n-1}s_j\left(\sum_{i=1}^{n}a_i c_{ij}\right)=0.$$
This is impossible.

(3) Then $\{c_1,...,c_{n-1}\}+D$ is a linear variety.

Let us see what we can obtain from (2). We have:

$$b=\sum_{i=1}^{n}a_ix_i=\sum_{i=1}^{n}a_i\left(\sum_{e=1}^{r}u_{ie}P_e+v_i\right)=\sum_{e=1}^{r}\left(\sum_{i=1}^{n}a_iu_{ie}\right)P_e+\sum_{i=1}^{n}a_iv_i$$

and, similarly: $\sum_{i=1}^{n}a_iv_i=b$ and $\sum_{i=1}^{n}a_iu_{ie}=0,\quad \forall\ e=\overline{1,r}$, respectively. The vectors $U_e=\left(u_{1e},...,u_{ne}\right)^t$, $e=\overline{1,r}$ are linearly independent because the solution is undetermined r-times.

A procedure like that applied in (3) shows that $U_1,...,U_r,\ V$ are linearly independent, where $V=\left(v_1,...,v_n\right)^t$. Then $\left\{U_1,...,U_r\right\}+V$ = a linear variety = free sub-module of order $r<n-1$. That is, we can find vectors from $\left\{c_1,...,c_{n-1}\right\}+D$ which are not from $\left\{U_1,...,U_r\right\}+V$, contradicting the "general" characteristic of the integer number solution. Hence, the general integer solution is undetermined $(n-1)$-times.

Theorem 2. The general integer solution of the homogeneous linear equation $\sum_{i=1}^{n}a_ix_i=0$ (all $a_i\in\mathbb{Z}\setminus\{0\}$) can be written under the form:

(4) $$x_i=\sum_{j=1}^{n-1}c_{ij}k_j,\ \ i=\overline{1,n}$$

(with $d_1=...=d_n=0$).

Definition 6. This is called the standard form of the general integer solution of a homogeneous linear equation.

Proof:

We consider the general integer solution under the form:

$$x_i=\sum_{j=1}^{n-1}c_{ij}P_j+d_i,\ \ i=\overline{1,n}$$

with not all $d_i=0$. We'll show that it can be written under the form (4). The homogeneous equation has the trivial solution $x_i=0,\ i=\overline{1,n}$. There is $\left(p_1^0,...,p_{n-1}^0\right)\in\mathbb{Z}^{n-1}$ such that $\sum_{j=1}^{n-1}c_{ij}p_j^0+d_i=0,\ \ \forall i=\overline{1,n}$.

Substituting: $P_j=k_j+p_j,\ \ j=\overline{1,n-1}$ in the form shown at the beginning of the demonstration, we will obtain form (4). We have to mention that the substitution does not diminish the degree of generality as $P_j\in\mathbb{Z}\iff k_j\in\mathbb{Z}$ because $j=\overline{1,n-1}$.

Theorem 3. The general integer solution of a non-homogeneous linear equation is equal to the general integer solution of its associated homogeneous linear equation plus any particular integer solution of the non-homogeneous linear equation.

Proof:

Let's consider that $x_i = \sum_{j=1}^{n-1} c_{ij} k_j, \quad i = \overline{1,n}$, is the general integer solution of the associated homogeneous linear equation and, again, let $x_i = v_i,\ i = \overline{1,n}$, be a particular integer solution of the non-homogeneous linear equation. Then $x_i = \sum_{j=1}^{n-1} c_{ij} k_j + v_i, \quad i = \overline{1,n}$, is the general integer solution of the non-homogeneous linear equation.

Actually, $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij} k_j + v_i \right) = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij} k_j \right) + \sum_{i=1}^{n} a_i v_i = b$;

if $x_i = x_i^0,\ i = \overline{1,n}$, is a particular integer solution of the non-homogeneous linear equation, then $x_i = x_i - v_i,\ i = \overline{1,n}$, is a particular integer solution of the homogeneous linear equation: hence, there is $(k_1^0, ..., k_{n-1}^0) \in \mathbb{Z}^{n-1}$ such that

$$\sum_{j=1}^{n-1} c_{ij} k_j^0 = x_i^0 - v_i,\ \ \forall\ i = \overline{1,n},$$

i.e.:

$$\sum_{j=1}^{n-1} c_{ij} k_j^0 + v_i = x_i^0,\ \ \forall\ i = \overline{1,n},$$

which was to be proven.

Theorem 4. If $x_i = \sum_{j=1}^{n-1} c_{ij} k_j,\ i = \overline{1,n}$ is the general integer solution of a homogeneous linear equation $\left(c_{ij}, ..., c_{nj}\right) \sim 1\ \ \forall\ j = \overline{1, n-1}$.

The demonstration is done by reduction ad absurdum. If $\exists j_0,\ 1 \le j_0 \le n-1$ such that $\left(c_{ij_0}, ..., c_{nj_0}\right) \sim d_{j_0} \neq \pm 1$, then $c_{ij_0} = c'_{ij_0} d_{ij_0}$ with $\left(c'_{ij_0}, ..., c'_{nj_0}\right) \sim 1, \quad \forall\ i = \overline{1,n}$.

But $x_i = c'_{ij_0}, \quad i = \overline{1,n}$, represents a particular integer solution as

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i c'_{ij_0} = 1/d_{j_0} \cdot \sum_{i=1}^{n} a_i c_{ij_0} = 0$$

(because $x_i = c_{ij_0},\ i = \overline{1,n}$ is a particular integer solution from the general integer solution by introducing $k_{j_0} = 1$ and $k_j = 0,\ j \neq j_0$. But the particular integer solution $x_i = c'_{ij_0},\ i = \overline{1,n}$, cannot be obtained by introducing integer number parameters (as it should) from the general integer solution, as from the linear system of n equations and $n-1$ unknowns, which is compatible. We obtain:

$$x_i = \sum_{\substack{j=1 \\ j \neq j_0}}^{n} c_{ij} k_j + c'_{ij_0} d_{j_0} k_{j_0} = c'_{ij_0}, \quad i = \overline{1,n}.$$

Leaving aside the last equation – which is a linear combination of other $n-1$ equations – a Kramerian system is obtained, as follows:

$$k_{j_0}=\frac{\begin{vmatrix} c_{11}\ldots\ldots c'_{ij_0}\ldots\ldots c_{1,n-1} \\ \vdots \\ c_{n-1,1}\ldots c'_{n-1j_0}\ldots c_{n-1n-1} \end{vmatrix}}{\begin{vmatrix} c_{11}\ldots\ldots c'_{ij_0}d_{j_0}\ldots\ldots c_{1,n-1} \\ \vdots \\ c_{n-1,1}\ldots c'_{n-1j_0}d_{j_0}\ldots c_{n-1n-1} \end{vmatrix}}=\frac{1}{d_{j_0}}\notin\mathbb{Z}$$

Therefore the assumption is false (end of demonstration).

Theorem 5. Considering the equation (1) with $(a_1,...,a_n)\sim 1,\ \ b=0$ and the general integer solution $x_i=\sum_{j=1}^{n-1}c_{ij}k_j,\ \ i=\overline{1,n}$, then

$$(a_1,...,a_{i-1},a_{i+1},...,a_n)\sim(c_{i1},...,c_{in-1}),\ \ \forall i=\overline{1,n}.$$

Proof:

The demonstration is done by double divisibility.

Let's consider $i_0,\ 1\le i_0\le n$ arbitrary but fixed. $x_{i_0}=\sum_{j=1}^{n-1}c_{i_0j}k_j$. Consider the equation $\sum_{\mathrm{i}\ne\mathrm{i}_0}a_ix_i=-a_{i_0}x_{i_0}$. We have shown that $x_i=c_{ij},\ \ i=\overline{1,n}$ is a particular integer solution irrespective of $j,\ \ a\le j\le n-1$.

The equation $\sum_{\mathrm{i}\ne\mathrm{i}_0}a_ix_i=-a_{i_0}c_{i_0j}$ obviously, has the integer solution $x_i=c_{ij},\ \ i\ne i_0$. Then $(a_1,...,a_{i_0-1},a_{i_0+1},...,a_n)$ divides $-a_{i_0}c_{i_0j}$ as we have assumed, it follows that $(a_1,...,a_n)\sim 1$, and it follows that $(a_1,...,a_{i_0-1},a_{i_0+1},...,a_n)\,|\,c_{i_0j}$ irrespective of j. Hence $(a_1,...,a_{i_0-1},a_{i_0+1},...,a_n)\,|\,(c_{i_01},...,c_{i_0n-1}),\ \ \forall i=\overline{1,n}$, and the divisibility in one sense was proven.

Inverse divisibility:

Let us suppose the contrary and consider that $\exists i_1\in\overline{1,n}$ for which $(a_1,...,a_{i_1-1},a_{i_1+1},...,a_n)\sim d_{i_11}\ne d_{i_12}\sim(c_{i_11},...,c_{i_1n-1})$; we have considered d_{i_11} and d_{i_12} without restricting the generality. $d_{i_11}\,|\,d_{i_12}$ according to the first part of the demonstration. Hence, $\exists d\in\mathbb{Z}$ such that $d_{i_12}=d\cdot d_{i_11},\ \ |d|\ne 1$.

$$x_{i_1}=\sum_{j=1}^{n-1}c_{i_1j}k_j=d\cdot d_{i_11}\sum_{j=1}^{n-1}c'_{i_1j}k_j\ ;$$

$$\sum_{i=1}^{n}a_ix_i=0\Rightarrow\sum_{i\ne i_1}a_ix_i=-a_{i_1}x_{i_1}\sum_{i\ne i_1}a_ix_i=-a_{i_1}d\cdot d_{i_11}\sum_{j=1}^{n-1}c'_{i_1j}k_j\ ,$$

where $\left(c_{i_1 1},\dots,c_{i_1 n-1}\right)\sim 1$.

The non-homogeneous linear equation $\sum_{i\neq i_1} a_i x_i = -a_{i_1} d_{i_1 1}$ has the integer solution because $a_{i_1} d_{i_1 1}$ is divisible by $\left(a_1,\dots,a_{i_1-1},a_{i_1+1},\dots,a_n\right)$. Let's consider that $x_i = x_i^0,\ i\neq i_1$, is its particular integer solution. It follows that the equation $\sum_{i=1}^{n} a_i x_i = 0$ the particular solution $x_i = x_i^0,\ i\neq i_1,\ \ x_{i_1} = d_{i_1}$, which is written as (5). We'll show that (5) cannot be obtained from the general solution by integer number parameters:

$$(6)\qquad \begin{cases} \sum_{j=1}^{n-1} c_{ij} k_j = x_i^0, & i\neq i_1 \\ d\cdot d_{i_1 1}\sum_{j=1}^{n-1} c_{ij} k_j = d_{i_1 1} \end{cases}$$

But the equation (6) does not have an integer solution because $d\cdot d_{i_1 1} \mid d_{i_1 1}$ thus, contradicting, the "general" characteristic of the integer solution.

As a conclusion we can write:

Theorem 6. Let's consider the homogeneous linear equation $\sum_{i=1}^{n} a_i x_i = 0$, with all $a_i \in \mathbb{Z}\setminus\{0\}$ and $\left(a_1,\dots,a_n\right)\sim 1$.

Let $x_i = \sum_{j=1}^{h} c_{ij} k_j,\ i=\overline{1,n}$, with all $c_{ij}\in\mathbb{Z}$, all k_j integer parameters and let's consider $h\in\mathbb{N}$ be a general integer solution of the equation. Then,

1) the solution is undetermined $(n-1)$-times;
2) $\forall\ j=\overline{1,n-1}$ we have $\left(c_{1j},\dots,c_{nj}\right)\sim 1$;
3) $\forall\ i=\overline{1,n}$ we have $\left(c_{i1},\dots,c_{in-1}\right)\sim\left(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n\right)$.

The proof results from theorems 1,4 and 5.

Note 1. The only equation of the form (1) that is undetermined n-times is the trivial equation $0\cdot x_1+\dots+0\cdot x_n = 0$.

Note 2. The converse of theorem 6 is not true.

Counterexample:

$$(7)\qquad \begin{cases} x_1 = -k_1 + k_2 \\ x_2 = 5k_1 + 3k_2 \\ x_3 = 7k_1 - k_2; \quad k_1,k_2\in\mathbb{Z} \end{cases}$$

is not the general integer solution of the equation

$$(8)\qquad -13x_1 + 3x_2 - 4x_3 = 0$$

although the solution (7) verifies the points 1), 2) and 3) of theorem 6. (1, 7, 2) is the particular integer solution of (8) but cannot be obtained by introducing integer number parameters in (7) because from

$$\begin{cases} -k_1 + k_2 = 1 \\ 5k_1 + 3k_2 = 7 \\ 7k_1 - k_2 = 2 \end{cases}$$

it follows that $k = \frac{1}{2} \notin \mathbb{Z}$ and $k = \frac{3}{2} \notin \mathbb{Z}$ (unique roots).

REFERENCE

[1] Smarandache, Florentin – Whole number solution of linear equations and systems – diploma thesis work, 1979, University of Craiova (under the supervision of Assoc. Prof. Dr. Alexandru Dincă)

AN INTEGER NUMBER ALGORITHM TO SOLVE LINEAR EQUATIONS

An algorithm is given that ascertains whether a linear equation has integer number solutions or not; if it does, the general integer solution is determined.

Input

A linear equation $a_1x_1 + ... + a_nx_n = b$, with $a_i, b \in \mathbb{Z}$, x_i being integer number unknowns, $i = \overline{1,n}$, and not all $a_i = 0$.

Output

Decision on the integer solution of this equation; and if the equation has solutions in $\mathbb{Z}$, its general solution is obtained.

Method

Step 1. Calculate $d = (a_1, ..., a_n)$.

Step 2. If d / b then "the equation has integer solution"; go on to Step 3. If $d \nmid b$ then "the equation does not have integer solution"; stop.

Step 3. Consider $h := 1$. If $|d| \neq 1$, divide the equation by d; consider $a_i := a_i / d,\ i = \overline{1,n},\ b := b / d$.

Step 4. Calculate $a = \min\limits_{a_s \neq 0} |a_s|$ and determine an i such that $a_i = a$.

Step 5. If $a \neq 1$ then go to Step 7.

Step 6. If $a = 1$, then:

(A) $x_i = -(a_1x_1 + ... + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + ... + a_nx_n - b) \cdot a_i$

(B) Substitute the value of x_i in the values of the other determined unknowns.

(C) Substitute integer number parameters for all the variables of the unknown values in the right term: $k_1, k_2, ..., k_{n-2}$, and k_{n-1} respectively.

(D) Write, for your records, the general solution thus determined; stop.

Step7. Write down all $a_j,\ j \neq i$ and under the form:

$$a_j = a_i q_j + r_j$$

$$b = a_i q + r \text{ where } q_j = \left[\frac{a_j}{a_i}\right],\ q = \left[\frac{b}{a_i}\right].$$

Step 8. Write $x_i = -q_1x_1 - ... - q_{i-1}x_{i-1} - q_{i+1}x_{i+1} - ... - q_nx_n + q - t_h$. Substitute the value of x_i in the values of the other determined unknowns.

Step 9. Consider

$$\begin{cases} a_1 := r_1 \\ \vdots \\ a_{i-1} := r_{i-1} \\ a_{i+1} := r_{i+1} \\ \vdots \\ a_n := r_n \end{cases} \quad \text{and} \quad \begin{cases} a_i := -a_i \\ b := r \\ x_i := t_h \\ h := h+1 \end{cases}$$

and go back to Step 4.

Lemma 1. The previous algorithm is finite.

Proof:

Let's $a_1x_1 + ... + a_nx_n = b$ be the initial linear equation, with not all $a_i = 0$; check for $\min_{a_s \neq 0} |a_s| = a_1 \neq 1$ (if not, it is renumbered). Following the algorithm, once we pass from this initial equation to a new equation: $a_1^{'}x_1 + a_2^{'}x_2 + ... + a_n^{'}x_n = b'$, with $|a_1^{'}| < |a_i|$ for $i = \overline{2,n}$, $|b'| < |b|$ and $a_1^{'} = -a_1$.

It follows that $\min_{a_s^{'} \neq 0} |a_s^{'}| < \min_{a_s \neq 1} |a_s|$. We continue similarly and after a finite number of steps we obtain, at Step 4, $a := 1$ (the actual a is always smaller than the previous a, according to the previous note) and in this case the algorithm terminates.

Lemma 2. Let the linear equation be:

(25) $\quad a_1x_1 + a_2x_2 + ... + a_nx_n = b$, with $\min_{a_s \neq 0} |a_s| = a_1$ and the equation

(26) $\quad -a_1t_1 + r_2x_2 + ... + r_nx_n = r$, with $t_1 = -x_1 - q_2x_2 - ... - q_nx_n + q$, where $r_i = a_i - a_iq_i$, $i = \overline{2,n}$, $r = b - a_1q$ while $q_i = \left[\frac{a_i}{a}\right]$, $r = \left[\frac{b}{a_1}\right]$. Then $x_1 = x_1^0$, $x_2 = x_2^0, \dots, x_n = x_n^0$ is a particular solution of equation (25) if and only if $t_1 = t_1^0 = -x_1 - q_2x_2^0 - ... - q_nx_n^0 + q$, $x_2, ..., x_n = x_n^0$ is a particular solution of equation (26).

Proof:

$x_1 = x_1^0$, $x_2 = x_2^0, \dots, x_n = x_n^0$, is a particular solution of equation (25) $\Leftrightarrow$
$a_1x_1^0 + a_2x_2^0 + ... + a_nx_n^0 = b \Leftrightarrow a_1x_1^0 + (r_2 + a_1q_2)x_2^0 + ... + (r_n + a_1q_n)x_n^0 = a_1q + r \Leftrightarrow$
$r_2x_2^0 + ... + r_nx_n^0 - a_1(-x_1^0 - q_2x_2^0 - ... - q_nx_n^0 + q) = r \Leftrightarrow -a_1t_1^0 + r_2x_2^0 + ... + r_nx_n^0 = r \Leftrightarrow$
$\Leftrightarrow t_1 = t_1^0, x_2 = x_2^0, ..., x_n = x_n^0$ is a particular solution of equation (26).

Lemma 3. $x_i = c_{i1}k_1 + ... + c_{in-1}k_{n-1} + d_i$, $i = \overline{1,n}$, is the general solution of equation (25) if and only if

(28) $\quad t_1 = -(c_{11} + q_2c_{21} + ... + q_nc_{n1})k_1 - ... - (c_{1n-1} + q_2c_{2n-1} + ... + q_nc_{nn-1})k_n -$
$-(d_1 + q_2d_2 + ... + q_nd_n) + q$,
$x_j = c_{1j1}k_1 + ... + c_{jn-1}k_{n-1} + d_j$, $\quad j = \overline{2,n}$

is a general solution for equation (26).

Proof:

$t_1 = t_1^0 = -x_1^0 - q_2 x_2^0 - ... - q_n x_n^0 + q,\ x_2 = x_2^0, ..., x_n = x_n^0$ is a particular solution of the equation (25) $\Leftrightarrow$ $x_1 = x_1^0,\ x_2 = x_2^0, ..., x_n = x_n^0$ is a particular solution of equation (26) $\Leftrightarrow$ $\exists k_1 = k_1^0 \in \mathbb{Z}, ..., k_n = k_n^0 \in \mathbb{Z}$ such that

$$x_i = c_{i1} k_1^0 + ... + c_{in-1} k_{n-1}^0 + d_i = x_i^0,\ i = \overline{1,n} \Leftrightarrow \exists k_1 = k_1^0 \in \mathbb{Z}, ..., k_n = k_n^0 \in \mathbb{Z},$$

such that

$$x_i = c_{i1} k_1^0 + ... + c_{in-1} k_{n-1}^0 + d_i = x_i^0,\ \ i = \overline{2,n},$$

and

$$t_1 = -(c_{11} + q_2 c_{21} + ... + q_n c_{n1}) k_1^0 - ... - (c_{1n-1} + q_2 c_{2n-1} + ... + q_n c_{nn-1}) k_{n-1}^0 -$$
$$(d_1 + q_2 d_2 + ... + q_n d_n) + q = -x_1^0 - q_2 x_2^0 - ... - q_n x_n^0 + q = t_1^0$$

Lemma 4. The linear equation

(29) $\quad a_1 x_1 + a_2 x_2 + ... + a_n x_n = b$ with $|a_1| = 1$ has the general solution:

$$(30)\quad \begin{cases} x_1 = -(a_2 k_2 + ... + a_n k_n - b) a_1 \\ x_i = k_i \in \mathbb{Z} \\ i = \overline{2,n} \end{cases}$$

Proof:

Let's consider $x_1 = x_1^0,\ x_2 = x_2^0, \ldots, x_n = x_n^0$, a particular solution of equation (29). $\exists k_2 = x_2^0,\ k_n = x_n^0$, such that $x_1 = \left(-a_2 x_2^0 + ... + a_n x_n^0 - b\right) a_1 = x_1^0,\ \ x_2 = x_2^0, ..., x_n = x_n^0$.

Lemma 5. Let's consider the linear equation $a_1 x_1 + a_2 x_2 + ... + a_n x_n = b$, with $\min\limits_{a_s \neq 0} |a_s| = a_1$ and $a_i = a_1 q_i,\ \ i = \overline{2,n}$.

Then, the general solution of the equation is:

$$\begin{cases} x_1 = -(q_2 k_2 + ... + q_n k_n - q) \\ x_i = k_i \in \mathbb{Z} \\ i = \overline{2,n} \end{cases}$$

Proof:

Dividing the equation by a_1 the conditions of Lemma 4 are met.

Theorem of Correctness. The preceding algorithm calculates correctly the general solution of the linear equation $a_1 x_1 + ... + a_n x_n = b$, with not all $a_i = 0$.

Proof:

The algorithm is finite according to Lemma 1. The correctness of steps 1, 2, and 3 is obvious. At step 4 there is always $\min\limits_{a_s \neq 0} |a_s|$ as not all $a_i = 0$. The correctness of sub-step 6 A) results from Lemmas 4 and 5, respectively. This algorithm represents a method of obtaining the general solution of the initial equation by means of the general solutions of the linear equation obtained after the algorithm was followed several times (according to Lemmas 2 and 3); from Lemma 3, it follows that to obtain the general solution of the initial linear equation is equivalent to calculate the general solution of an equation at step 6 A), equation whose general solution is given in algorithm (according to Lemmas 4 and 5). The Theorem of correctness has been fully proven.

Note. At step 4 of the algorithm we consider $a := \min_{a_s \neq 0} |a_s|$ such that the number of iterations is as small as possible. The algorithm works if we consider $a := |a_i| \neq \max_{s=\overline{1,n}} |a_s|$ but it takes longer. The algorithm can be introduced into a computer program.

Application

Calculate the integer solution of the equation:

$$6x_1 - 12x_2 - 8x_3 + 22x_4 = 14\ .$$

Solution

The previous algorithm is applied.

1. $(6,-12,-8,22) = 2$
2. $2\,|\,14$ therefore the solution of the equation is in $\mathbb{Z}$.
3. $h := 1$; $|2| \neq 1$; dividing the equation by 2 we obtain:

$3x_1 = 6x_2 - 4x_3 + 11x_4 = 7$.

4. $a := \min\{|3|,\ |-6|,\ |-4|,\ |11|\} = 3,\ i = 1$
5. $a \neq 1$
7. $-6 = 3 \cdot (-2) + 0$

$-4 = 3 \cdot (-2) + 2$

$11 = 3 \cdot 3 + 2$

$7 = 3 \cdot 2 + 1$

8. $x_1 = 2x_2 + 2x_3 - 3x_4 + 2 - t_1$
9.

$a_2 := 0 \qquad a_1 := -3$

$a_3 := 2 \qquad b := 1$

$a_4 := 2 \qquad x_1 := t_1$

$h := 2$

4. We have a new equation:

$-3t_1 - 0 \cdot x_2 + 2x_3 + 2x_4 = 1$

$a := \min\{|-3|,|2|,|2|\}$ and

$i = 3$

5. $a \neq 1$
7. $-3 = 2 \cdot (-2) + 1$

$0 = 2 \cdot 0 + 0$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 0$

8. $x_3 = 2t_1 + 0 \cdot x_2 - x_4 + 0 - t_2$. Substituting the value of x_3 in the value determined for x_1 we obtain: $x_1 = 2x_2 - 5x_4 + 3t_1 - 2t_2 + 2$

9. $a_1 := 1$ $\quad a_3 := -2$
$a_2 := 0$ $\quad b := 1$
$a_4 := 0$ $\quad x_3 := t_2$
$h := 3$

4. We have obtained the equation:
$1 \cdot t_2 + 0 \cdot x_2 - 2 \cdot t_2 + 0 \cdot x_4 = 1$, $a = 1$, and $i = 1$

6. (A) $t_1 = -(0 \cdot x_2 - 2t_2 + 0 \cdot x_4 - 1) \cdot 1 = 2t_2 + 1$

(B) Substituting the value of t_1 in the values of x_1 and x_3 previously determined, we obtain:

$x_1 = 2x_2 - 5x_4 + 4t_2 + 5$ and
$x_3 = -x_4 + 3t_2 + 2$

(C) $x_2 := k_1$, $x_4 := k_2$, $t_2 := k_3$, $k_1, k_2, k_3 \in \mathbb{Z}$

(D) The general solution of the initial equation is:

$x_1 = 2k_1 - 5k_2 + 4k_3 + 5$
$x_2 = k_1$
$x_3 = -k_2 + 3k_3 + 2$
$x_4 = k_2$
k_1, k_2, k_3 are parameters $\in \mathbb{Z}$

REFERENCE

[1] Smarandache, Florentin – Whole number solution of equations and systems of equations – part of the diploma thesis, University of Craiova, 1979.

ANOTHER INTEGER ALGORITHM TO SOLVE LINEAR EQUATIONS (USING CONGRUENCES)

In this section is presented a new integer number algorithm for linear equation. This algorithm is more "rapid" than W. Sierpinski's presented in [1] in the sense that it reaches the general solution after a smaller number of iterations. Its correctness will be thoroughly demonstrated.

Another Integer Algorithm.

Let's us consider the equation (1); (the case $a_i, b \in \mathbb{Q}$, $i = \overline{1,n}$ is reduced to the case (1) by reducing to the same denominator and eliminating the denominators). Let $d = (a_1, ..., a_n)$. If $d \mid b$ then the equation does not have integer solutions, while if $d \nmid b$ the equation has integer solutions (according to a well-known theorem from the number theory).

If the equation has solutions and $d \neq$ we divide the equation by d. Then $d = 1$ (we do not make any restriction if we consider the maximal co-divisor positive).

Also,

(a) If all a_i the equation is trivial; it has the general integer solution $x_i = k_i \in \mathbb{Z}$, $i = \overline{1,n}$, when $b = 0$ (the only case when the general solution is n-times undetermined) and does not have solution when $b \neq 0$.

(b) If $\exists i,\ 1 \leq i \leq n$ such that $a_i = \pm 1$ then the general integer solution is: $x_i = -a_i \left(\sum_{\substack{j=1 \\ j \neq i}}^{n} a_j k_j - b \right)$ and $x_s = k_s \in \mathbb{Z},\ s \in \{1, ..., n\} \setminus \{i\}$

The proof of this assertion was given in [4]. All these cases are trivial, therefore we will leave them aside. The following algorithm can be written:

Input

A linear equation:

(2) $$\sum_{i=1}^{n} a_i x_i = b,\ a_i, b \in \mathbb{Z},\ \ a_i \neq \pm 1,\ i = \overline{1,n},$$

with not all $a_i = 0$ and $(a_1, ..., a_n) = 1$.

Output

The integer general solution of the equation.

Method

1. $h := 1,\ p := 1$

2. Calculate $\min_{1 \leq i, j \leq n} \{ |r|,\ r \equiv a_i (\bmod a_j),\ |r| < |a_j| \}$ and determine r and the pair (i, j) for which this minimum can be obtained (when there are more possibilities we have to choose one of them).

3. If $|r| \neq$ go to step 4.
If $|r| = 1$, then

$$\begin{cases} x_i := r\left(-a_j t_h - \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s + b\right) \\ x_j := r\left(a_i t_h + \dfrac{a_i - r}{a_j} \cdot \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s + \dfrac{r - a_i}{a_j} b\right) \end{cases}$$

(A) Substitute the values thus determined of these unknowns in all the statements $(p),\ p = 1, 2, \ldots$ (if possible).
(B) From the last relation (p) obtained in the algorithm substitute in all relations: $(\overline{p} - 1), (\overline{p} - 2), \ldots, (1)$
(C) Every statement, starting in order from $(\overline{p} - 1)$ should be applied the same procedure as in (B): then $(\overline{p} - 2), \ldots, (3)$ respectively.
(D) Write the values of the unknowns $x_i,\ i = \overline{1, n}$, from the initial equation (writing the corresponding integer number parameters from the right term of these unknowns with $k_1, \ldots, k_{n-1}$), STOP.

4. Write the statement (p): $x_j = t_h - \dfrac{a_i - r}{a_j} x_i$

5. Assign $\quad x_j := t_h \quad h := h + 1$
$\quad a_i := r \quad p := p + 1$

The other coefficients and variables remain unchanged go back to step 2.

The Correctness of the Algorithm

Let us consider linear equation (2). Under these conditions, the following properties exist:

Lemma 1. The set $M = \left\{ |r|,\ r \equiv a_i (\operatorname{mod} a_j),\ 0 < |r| < |a_j| \right\}$ has a minimum.

Proof:

Obviously $M \subset \mathbb{N}^*$ and M is finite because the equation has a finite number of coefficients: n, and considering all the possible combinations of these, by twos, there is the maximum AR_n^2 (arranged with repetition) = n^2 elements.

Let us show, by *reductio ad absurdum*, that $M \neq \emptyset$.

$M \neq \emptyset \Leftrightarrow a_i \equiv 0 (\operatorname{mod} a_j)\ \forall i, j = \overline{1, n}$. Hence $a_j \equiv 0 (\operatorname{mod} a_i)\ \forall i, j = \overline{1, n}$. Or this is possible only when $|a_i| = |a_j|,\ \forall i, j = \overline{1, n}$, which is equivalent to

$(a_1,..,a_n)=a_i,\ \forall i\in\overline{1,n}$. But $(a_1,..,a_n)=1$ are a restriction from the assumption. It follows that $|a_i|=\overline{1,n},\ \forall i\in\overline{1,n}$ a fact which contradicts the other restrictions of the assumption.

$M\neq 0$ and finite, it follows that M has a minimum.

Lemma 2. If $|r|=\min\limits_{1\le i,j\le n} M$, then $|r|<|a_i|,\ \forall i\in\overline{1,n}$.

Proof:

We assume conversely, that $\exists i_0,\ 1\le i_0\le n$ such that $|r|\ge\left|a_{i_0}\right|$.

Then $|r|\ge\min\limits_{1\le j\le n}\left\{\ |a_j|\right\}=\left|a_{j_0}\right|\neq 1$, $1\le j_0\le n$. Let a_{p_0}, $1\le p_0\le n$, such that $\left|a_{p_0}\right|>\left|a_{j_0}\right|$ and a_{p_0} is not divided by a_j^0.

There is a coefficient in the equation, $\left|a_{j_0}\right|$ which is the minimum and the coefficients are not equal among themselves (conversely, it would mean that $(a_1,..,a_n)=a_1=\pm 1$ which is against the hypothesis and, again, of the coefficients whose absolute value is greater that $\left|a_{ij_0}\right|$ not all can be divided by a_{j_0} (conversely, it would similarly result in $(a_1,..,a_n)=a_{j_0}\neq\pm 1$.

We write $\left[a_{p_0}/a_{j_0}\right]=q_0\in\mathbb{Z}$ (integer portion), and $r=a_{p_0}-q_0a_{j_0}\in\mathbb{Z}$. We have $a_{p_0}\equiv r_0(\mathrm{mod}\,a_{j_0})$ and $0<|r_0|<\left|a_{j_0}\right|<\left|a_{i_0}\right|\le|r|$. Thus, we have found an r_0 which $|r_0|<|r|$ contradicts the definition of minimum given to $|r|$.

Thus $|r|<|a_i|,\ \forall i\in\overline{1,n}$.

Lemma 3. If $|r|=\min M=1$ for the pair of indices (i,j), then:

$$\begin{cases} x_i=r\left(-a_jt_h-\sum\limits_{\substack{s=1\\ s\notin\{i,j\}}}^{n}a_sk_s+b\right)\\ x_j=r\left(a_it_h+\dfrac{a_i-r}{a_j}\cdot\sum\limits_{\substack{s=1\\ s\notin\{i,j\}}}^{n}a_sk_s+\dfrac{r-a_i}{a_j}b\right)\\ x_s=k_s\in\mathbb{Z},\ s\in\{1,...,n\}\setminus\{i,j\} \end{cases}$$

is the general integer solution of equation (2).

Proof:

Let $x_e = x_e^0,\ e = \overline{1,n}$, be a particular integer solution of equation (2). Then $\exists k_s = x_s^0 \in \mathbb{Z},\ s \in \{1,...,n\} \setminus \{i,j\}$ and $t_h = x_j^0 + \frac{a_i - r}{a_j} x_i^0 \in \mathbb{Z}$ (because $a_i - r = Ma_j$) such that:

$$x_i = r - a_j\left(x_j^0 + \frac{a_i - r}{a_j} x_i\right) - \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^0 + b = x_i^0$$

$$x_j = r - a_j\left(x_j^0 + \frac{a_i - r}{a_j} x_i^0\right) + \frac{a_i - r}{a_j} - \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^0 + \frac{r - a_i}{a_j} b = x_i^0$$

and $x_s = k_s = x_s^0,\ s \in \{1,...,n\} \setminus \{i,j\}$.

Lemma 4. Let $|r| \neq$ and (i,j) be the pair of indices for which this minimum can be obtained. Again, let's consider the system of linear equations:

$$(3) \qquad \begin{cases} a_j t_h + r x_i + \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s = b \\ t_h = x_j + \dfrac{a_i - r}{a_j} x_i \end{cases}$$

Then $x_e = x_e^0,\ e = \overline{1,n}$ is a particular integer solution for (2) if and only if $x_e = x_e^0$, $e \in \{1,...,n\} \setminus \{j\}$ and $t_h = t_h^0 = x_j^0 + \frac{a_i - r}{a_j} x_i$ is the particular integer solution of (3).

Proof:

$x_e = x_e^0,\ e = \overline{1,n}$ is a particular solution for (2) if and only if

$$\sum_{e=1}^{n} a_e x_e^0 = b \Leftrightarrow \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^0 + a_j\left(x_j^0 + \frac{a_i - r}{a_j} x_i^0\right) + r x_i^0 = b \Leftrightarrow$$

$$\Leftrightarrow a_j t_h^0 + r x_i^0 + \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^0 = b \qquad \text{and} \qquad t_h^0 = x_j^0 + \frac{a_i - r}{a_j} x_i^0 \in \mathbb{Z} \qquad \Leftrightarrow x_e = x_e^0,$$

$e \in \{1,...,n\} \setminus \{j\}$ and $t_h = t_h^0$ is a particular integer solution for (3).

Lemma 5. The previous algorithm is finite.

Proof:

When $|r| = 1$ the algorithm stops at step 3. We will discuss the case when $|r| \neq 1$. According to the definition of r, $|r| \in \mathbb{N}^*$. We will show that the row of $r - s$ successively obtained by following the algorithm several times is decreasing with cycle, and each cycle is not equal to the previous, by 1. Let r_1 be the first obtained by following the algorithm one time. $|r_1| \neq 1$ then go to step 4, and then step 5. According to lemma 2, $|r_1| < |a_i|$, $\forall i = \overline{1,n}$.

Now we shall follow the algorithm a second time, but this time for an equation in which r_1 (according to step 5) is substituted by a_i. Again, according to lemma 2, the new $|r|$ written $|r_2|$ will have the propriety: $|r_2| < |r_1|$. We will get to $|r| = 1$ because $|r| \geq 1$ and $|r| < \infty$, and if $|r| \neq 1$, following the algorithm once again we get $|r| < |r_1|$ and so on. Hence, the algorithm has a finite number of repetitions.

Theorem of Correctness. The previous algorithm calculates the general solution of the linear equation correctly (2).

Proof:

According to lemma 5 the algorithm is finite. From lemma 1 it follows that the set M has a minimum, hence step 2 of the algorithm has meaning. When $|r| = 1$ it was shown in lemma 3 that step 3 of the algorithm calculates the general integer solution of the respective equation correctly the equation that appears at step 3). In lemma 4 it is shown that if $|r| \neq 1$the substitutions steps 4 and 5 introduced in the initial equation, the general integer solution remains unchanged. That is, we pass from the initial equation to a linear system having the same general solution as the initial equation. The variable h is a counter of the newly introduced variables, which are used to successively decompose the system in systems of two linear equations. The variable p is a counter of the substitutions of variables (the relations, at a given moment between certain variables).

When the initial equation was decomposed to $|r| = 1$, we had to proceed in the reverse way, i.e. to compose its general integer solution. This reverse way is directed by the sub-steps 3(A), 3(B) and 3(C). The sub-step 3(D) has only an aesthetic role, i.e., to have the general solution under the form: $x_i = f_i(k_1, ..., k_{n-1})$, $i = \overline{1,n}$, f_i being linear functions with integer number of coefficients. This "if possible" shows that substitutions are not always possible. But when they are we must make all possible substitutions.

Note 1. The previous algorithm can be easily introduced into a computer program.

Note 2. The previous algorithm is more "rapid" than that of W. Sierpinski's [1], i.e., the general integer solution is reached after a smaller number of iterations (or, at least, the same) for any linear equation (2).

In the first place, both methods aim at obtaining the coefficient ± 1 for at least one unknown variable. While Sierpinski started only by chance, decomposing the greatest coefficient in the module (writing it under the form of a sum between a multiple of the following smaller coefficient (in the module) and the rest), in our algorithm this decomposition is not accidental but always seeks the smallest $|r|$

and also choose the coefficients a_i and a_j for which this minimum is achieved. That is, we test from the beginning the shortest way to the general integer solution. Sierpinski does not attempt to find the shortest way; he knows that his method will take him to the general integer solution of the equation and is not interested in how long it will take. However, when an algorithm is introduced into a computer program it is preferable that the process time should be as short as possible.

Example 1.

Let us solve in $\mathbb{Z}^3$ the equation $17x - 7y + 10z = -12$.

We apply the former algorithm.

1. $h = 1, p = 1$
2. $r = 3,\ i = 3,\ j = 2$
3. $|3| \neq 1$ go on to step 4.
4. (1) $y = t_1 - \dfrac{10-3}{-7} \cdot z = t_1 + z$
5. Assign

$$y := t_1 \qquad h := 2$$
$$a_3 := 3 \qquad p := 2$$

with the other coefficients and variables remaining unchanged, go back to step 2.

2. $r = -1,\ i = 1,\ j = 3$
3. $|-1| = 1$

$$x = -1(-3t_2 - (-7t_1) - 12) = 3t_2 - 7t_1 - 12$$

$$z = -1\left(17t_2 + (-7t_1) \cdot \frac{17-(-1)}{3} + \frac{-1-17}{3}(-12)\right) = 17t_2 + 42t_1 - 72$$

(A) We substitute the values of x and z thus determined into the only statement (p) we have:

(1) $\quad y = t_1 + z = --17t_2 + 43t_1 - 72$

(B) The substitution is not possible.

(C) The substitution is not possible.

(D) The general integer solution of the equation is:

$$\begin{cases} x = 3k_1 - 7k_2 + 12 \\ y = -17k_1 + 43k_2 - 72 \\ z = -17k_1 + 42k_2 - 72; \qquad k_1, k_2 \in \mathbb{Z} \end{cases}$$

REFERENCES:

[1] Sierpinski, W, - Ce ştim şi ce nu ştim despre numerele prime? - Editura Stiințifică, Bucharest, 1966.
[2] Creangă, I., Cazacu, C., Mihuț, P., Opaiț, Gh., Corina Reisher – Introducere în teoria numerelor, Ed. Did. şi Ped., Bucharest, 1965.
[3] Popovici, C. P. – Aritmetica şi teoria numerelor, Ed. Did. şi Ped., Bucharest, 1963.
[4] Smarandache, Florentin – Un algoritm de rezolvare în numere întregi a ecuațiilor liniare.

INTEGER NUMBER SOLUTIONS OF LINEAR SYSTEMS

Definitions and Properties of the Integer Solution of a Linear System

Let's consider

$$(1) \qquad \sum_{j=1}^{n} a_{ij} x_j = b_i, \quad i = \overline{1,m}$$

a linear system with all coefficients being integer numbers (the case with rational coefficients is reduced to the same).

Definition 1. $x_j = x_j^0$, $j = \overline{1,n}$, is a particular integer solution of (1) if $x_j^0 \in \mathbb{Z}$, $j = \overline{1,n}$ and $\sum_{j=1}^{n} a_{ij} x_j^0 = b_i$, $i = \overline{1,m}$.

Let's consider the functions $f_j : \mathbb{Z}^h \to \mathbb{Z}$, $j = \overline{1,n}$, where $h \in \mathbb{N}^*$.

Definition 2. $x_j = f_j(k_1, ..., k_h)$, $j = \overline{1,n}$, is the general integer solution for (1) if:

(a) $\sum_{j=1}^{n} a_{ij} f_j(k_1, ..., k_h) = b_i$, $i = \overline{1,m}$, irrespective of $(k_1, ..., k_h) \in \mathbb{Z}$;

(b) Irrespective of $x_j = x_j^0$, $j = \overline{1,n}$ a particular integer solution of (1) there is $(k_1^0, ..., k_h^0) \in \mathbb{Z}$ such that $f_j(k_1^0, ..., k_h^0) = x_j$, $j = \overline{1,n}$. (In other words the general solution that comprises all the other solutions.)

Property 1.
A general solution of a linear system of m equations with n unknowns, $r(A) = m < n$, is undetermined $(n-m)$-times.

Proof:
We assume by reduction ad absurdum that it is of order r, $1 \le r \le n-m$ (the case $r = 0$, i.e., when the solution is particular, is trivial). It follows that the general solution is of the form:

$$(S_1) \qquad \begin{cases} x_1 = u_{11} p_1 + ... + u_{1r} p_r + v_1 \\ \vdots \\ x_n = u_{n1} p_1 + ... + u_{nr} p_r + v_n, \quad u_{ih}, \forall i \in \mathbb{Z} \\ p_h = \text{parameters} \in \mathbb{Z} \end{cases}$$

We prove that the solution is undetermined $(n-m)$-times.

The homogeneous linear system (1), resolved in r has the solution:

$$\begin{cases} x_1 = \frac{D^1_{m+1}}{D} x_{m+1} + \ldots + \frac{D^1_n}{D} x_n \\ \vdots \\ x_m = \frac{D^m_{m+1}}{D} x_{m+1} + \ldots + \frac{D^m_n}{D} x_n \end{cases}$$

Let $x_i = x_i^0,\ i = \overline{1,n}$, be a particular solution of the linear system (1).

Considering

$$\begin{cases} x_{m+1} = D \cdot k_{m+1} \\ \vdots \\ x_n = D \cdot k_n \end{cases}$$

we obtain the solution

$$\begin{cases} x_1 = D^1_{m+1} \cdot k_{m+1} + \ldots + D^1_n \cdot k_n + x_1^0 \\ \vdots \\ x_m = D^m_{m+1} \cdot k_{m+1} + \ldots + D^m_n \cdot k_n + x_m^0 \\ x_{m+1} = D \cdot k_{m+1} + x^0_{m+1} \\ \vdots \\ x_n = D \cdot k_n + x_n^0, \qquad\qquad k_j = \text{parameters} \in \mathbb{Z} \end{cases}$$

which depends on the $n-m$ independent parameters, for the system (1). Let the solution be undetermined $(n-m)$-times:

$$(S_2) \qquad \begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + u_{nn-m}k_{n-m} + d_n \\ c_{ij},\ d_i \in \mathbb{Z},\ k_j = \text{parameters} \in \mathbb{Z} \end{cases}$$

(There are such solutions, we have proved it before.) Let the system be:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}$$

x_i = unknowns $\in \mathbb{Z}$, $a_{ij},\ b_i \in \mathbb{Z}$.

I. The case $b_i = 0,\ i = \overline{1,m}$ results in a homogenous linear system:

$a_{i1}x_i + \ldots + a_{in}x_n = 0;\ i = \overline{1,m}$.

(S2) $\Rightarrow a_{i1}\left(c_{i1}k_1 + \ldots + c_{1n-m}k_{n-m} + d_1\right) + \ldots + a_{in}\left(c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} + d_n\right) = 0$

$0 = \left(a_{i1}c_{11} + \ldots + a_{in}c_{n1}\right)k_1 + \ldots + \left(a_{i1}c_{1n-m} + \ldots + a_{in}c_{nn-m}\right)k_{n-m} + \left(a_{i1}d_1 + \ldots + a_{in}d_n\right)$

$\forall k_j \in \mathbb{Z}$

For $k_1 = \ldots = k_{n-m} = 0 \Rightarrow a_{i1}d_1 + \ldots + a_{in}d_n = 0$.

For $k_1 = \ldots = k_{h-1} = k_{h+1} = \ldots = k_{n-m} = 0$ and $k_h = 1 \Rightarrow$

$$\Rightarrow (a_{i1}c_{ih} + ... + a_{in}c_{nh}) + (a_{i1}d_1 + ... + a_{in}d_d^{(n)}) = 0 \Rightarrow$$

$$a_{i1}c_{ih} + ... + a_{in}c_{nh} = 0,\ \forall\ i = \overline{1,m},\ \forall\ h = \overline{1,n-m}.$$

The vectors

$$V_h = \begin{pmatrix} c_{1h} \\ : \\ : \\ c_{nh} \end{pmatrix},\ h = \overline{1,n-m}$$

are the particular solutions of the system.

$V_h,\ h = \overline{1,n-m}$ also linearly independent because the solution is undetermined $(n-m)$-times $\{V_1,...,V_{n-m}\} + d$ is a linear variety that includes the solutions of the system obtained from (S_2).

Similarly for (S_1) we deduce that

$$U_s = \begin{pmatrix} U_{1s} \\ : \\ : \\ U_{ns} \end{pmatrix},\ s = \overline{1,r}$$

are particular solutions of the given system and are linearly independent, because (S_1) is undetermined $(n-m)$-times, and $V = \begin{pmatrix} V_1 \\ : \\ : \\ V_n \end{pmatrix}$ is a solution of the given system.

Case (a) $U_1,...,U_r,\ V =$ linearly dependent, it follows that $\{U_1,...,U_r\}$ is a free sub-module of order $r < n - m$ of solutions of the given system, then, it follows that there are solutions that belong to $\{V_1,...,V_{n-m}\} + d$ and which do not belong to $\{U_1,...,U_r\}$, a fact which contradicts the assumption that (S_1) is the general solution.

Case (b) $U_1,...,U_r,\ V =$ linearly independent.

$\{U_1,...,U_r\}$+V is a linear variety that comprises the solutions of the given system, which were obtained from (S_1). It follows that the solution belongs to $\{V_1,...,V_{n-m}\} + d$ and does not belong to $\{U_1,...,U_r\}$+V, a fact which is a contradiction to the assumption that (S_1) is the general solution.

II. When there is an $i \in \overline{1,m}$ with $b_i \neq 0$ then non-homogeneous linear system

$$a_{i1}x_i + ... + a_{in}x_n = b_1,\ i = \overline{1,m}$$

(S_2) $\Rightarrow a_{i1}(c_{11}k_1 + ... + c_{1n-m}k_{n-m} + d_1) + ... + a_{in}(c_{n1}k_1 + ... + c_{nn-m}k_{n-m} + d_n) = b_i$

it follows that

$$\Rightarrow (a_{i1}c_{11} + ... + a_{in}c_{n1})k_1 + ... + (a_{i1}c_{1n-m} + ... + a_{in}c_{nn-m})k_{n-m} + (a_{i1}d_1 + ... + a_{in}d_n) = b_i$$

For $k_1 = ... = k_{n-m} = 0 \Rightarrow a_{i1}d_1 + ... + a_{in}d_n = b_1$;

For $k_1 = ... = k_{j-1} = k_{j+1} = ... = k_{n-m} = 0$ and $k_j = 1 \Rightarrow$

$\Rightarrow \left(a_{i1}c_{1j} + ... + a_{in}c_{nj}\right) + \left(a_{in}d_1 + ... + a_{in}d_n\right) = b_i$ it follows that

$$\begin{cases} a_{i1}c_{1j} + ... + a_{in}c_{nj} = 0 \\ a_{i1}d_1 + ... + a_{in}d_n = b_i \end{cases}; \quad \forall i = \overline{1,m}, \ \forall j = \overline{1,n-m}.$$

$V_j = \begin{pmatrix} c_{1j} \\ : \\ c_{nj} \end{pmatrix}$, $j = \overline{1,n-m}$, are linearly independent because the solution (S_2) is undetermined $(n-m)$-times.

(?!) V_j, $j = \overline{1,n-m}$, and $d = \begin{pmatrix} d_1 \\ : \\ d_n \end{pmatrix}$

are linearly independent.

We assume that they are not linearly independent. It follows that

$$d = s_1V_1 + ... + s_{n-m}V_{n-m} = \begin{pmatrix} s_1c_{11} + ... + s_{n-m}c_{1n-m} \\ : \\ s_1c_{n1} + ... + s_{n-m}c_{nn-m} \end{pmatrix}.$$

Irrespective of $i = \overline{1,m}$:

$$b_1 = a_{i1}d_1 + ... + a_{in}d_n = a_{i1}\left(s_1c_{11} + ... + s_{n-m}c_{1n-m}\right) + ... + a_{in}\left(s_1c_{n1} + ... + s_{n-m}c_{nn-m}\right) =$$
$$= \left(a_{i1}c_{11} + ... + a_{in}c_{n1}\right)s_1 + ... + \left(a_{i1}c_{1n-m} + ... + a_{in}c_{nn-m}\right)s_{n-m} = 0.$$

Then, $b_i = 0$, irrespective of $i = \overline{1,m}$, contradicts the hypothesis (that there is an $i \in \overline{1,m}$, $b_i \neq 0$). It follows that $V_1,...,V_{n-m}, d$ are linearly independent.

$\{V_1,...,V_{n-m}\} + d$ is a linear variety that contains the solutions of the non-homogeneous system, solutions obtained from (S_2). Similarly it follows that $\{G_1,...,G_r\} + V$ is a linear variety containing the solutions of the non-homogeneous system, obtained from (S_1).

$n - m > r$ it follows that there are solutions of the system that belong to

“?!” means “to prove that”

$\{V_1,...,V_{n-m}\} + d$ and which do not belong to $\{G_1,...,G_r\} + V$, this contradicts the fact that (S_1) is the general solution. Then, it shows that the general solution depends on the $n - m$ independent parameters.

Theorem 1. The general solution of a non-homogeneous linear system is equal to the general solution of an associated linear system plus a particular solution of the non-homogeneous system.

Proof:

Let’s consider the homogeneous linear solution:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases}, \quad (AX = 0)$$

with the general solution:

$$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} + d_n \end{cases}$$

and

$$\begin{cases} x_1 = x_1^0 \\ \vdots \\ x_n = x_n^0 \end{cases}$$

with the general solution a particular solution of the non-homogeneous linear system $AX = b$;

$$(?!) \qquad \begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} + d + x_1^0 \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} + d_n + x_n^0 \end{cases}$$

is a solution of the non-homogeneous linear system.

We note:

$$A = \begin{pmatrix} a_{11} \ldots a_{1n} \\ \vdots \\ a_{m1} \ldots a_{mn} \end{pmatrix}, \ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \ b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \ 0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

(vector of dimension m),

$$K = \begin{pmatrix} k_1 \\ \vdots \\ k_{n-m} \end{pmatrix}, \ C = \begin{pmatrix} c_{11} \ldots c_{1n-m} \\ \vdots \\ c_{n1} \ldots c_{nn-m} \end{pmatrix}, \ d = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}, \ x^0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix};$$

$$AX = A\left(Ck + d + x^0\right) = A(Ck + d) + AX^0 = b + 0 = b$$

We will prove that irrespective of

$$\begin{aligned} x_1 &= y_1^0 \\ &\vdots \\ x_n &= y_n^0 \end{aligned}$$

there is a particular solution of the non-homogeneous system

$$\begin{cases} k_1 = k_1^0 \in \mathbb{Z} \\ \vdots \\ k_{n-m} = k_{n-m}^0 \in \mathbb{Z} \end{cases},$$

with the property:

$$\begin{cases} x_1 = c_{11}k_1^0 + \ldots + c_{1n}k_{n-m}^0 + d_1 + x_1^0 = y_1^0 \\ \vdots \\ x_n = c_{n1}k_1^0 + \ldots + c_{nn-m}k_{n-m}^0 + d_1 + x_n^0 = y_n^0 \end{cases}$$

We note $Y^0 = \begin{pmatrix} y_1^0 \\ \vdots \\ y_n^0 \end{pmatrix}$.

We'll prove that those $k_j^0 \in \mathbb{Z},\ j = \overline{1, n-m}$ are those for which $A\left(CX^0 + d\right) = 0$ (there are such $X_j^0 \in \mathbb{Z}$ because

$$\begin{cases} x_1 = 0 \\ \vdots \\ x_n = 0 \end{cases}$$

is a particular solution of the homogeneous linear system and $X = CK + d$ is a general solution of the non-homogeneous linear system)

$$A\left(CK^0 + d + X^0 - Y^0\right) = A\left(CK^0 + d\right) + AX^0 - AY^0 = 0 + b - b = 0 \quad .$$

Property 2 The general solution of the homogeneous linear system can be written under the form:

(SG)

$$(2) \qquad \begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} \end{cases}$$

k_j is a parameter that belongs to $\mathbb{Z}$ (with $d_1 = d_2 = \ldots = d_n = 0$).

Poof:

(SG) = general solution. It results that (SG) is undetermined $(n-m)$-times.

Let's consider that (SG) is of the form

$$(3) \qquad \begin{cases} x_1 = c_{11}p_1 + \ldots + c_{1n-m}p_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1}p_1 + \ldots + c_{nn-m}p_{n-m} + d_n \end{cases}$$

with not all $d_i = 0$; we'll prove that it can be written under the form (2); the system has the trivial solution

$$\begin{cases} x_1 = 0 \in \mathbb{Z} \\ \vdots \\ x_n = 0 \in \mathbb{Z} \end{cases};$$

it results that there are $p_j \in \mathbb{Z},\ j = \overline{1, n-m}$,

(4) $$\begin{cases} x_1 = c_{11}p_1^0 + \ldots + c_{1n-m}p_{n-m}^0 + d_1 = 0 \\ \vdots \\ x_n = c_{n1}p_1^0 + \ldots + c_{nn-m}p_{n-m}^0 + d_n = 0 \end{cases}$$

Substituting $p_j = k_j + p_j^0$, $j = \overline{1, n-m}$ in (3)

$$\left.\begin{array}{l} k_j \in \mathbb{Z} \\ p_j^0 \in \mathbb{Z} \end{array}\right\} \Rightarrow p_j \in \mathbb{Z},$$

$$\left.\begin{array}{l} p_j \in \mathbb{Z} \\ p_j^0 \in \mathbb{Z} \end{array}\right\} \Rightarrow k_j = p_j - p_j^0 \in \mathbb{Z}$$

which means that that they do not make any restrictions.

It results that

$$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} + \left(c_{11}p_1^0 + \ldots + c_{1n-m}p_{n-m}^0 + d_1\right) \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} + \left(c_{n1}p_1^0 + \ldots + c_{nn-m}p_{n-m}^0 + d_n\right) \end{cases}$$

But

$$c_{h1}p_1^0 + \ldots + c_{hn-m}p_{n-m}^0 + d_h = 0,\ h = \overline{1, n}\ \text{(from (4))}.$$

Then the general solution is of the form:

$$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} \end{cases}$$

k_j = parameters $\in \mathbb{Z}$, $j = \overline{1, n-m}$; it results that $d_1 = d_2 = \ldots = d_n = 0$.

Theorem 2. Let's consider the homogeneous linear system:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{cases},$$

$r(A) = m$, $\left(a_{h1}, \ldots, a_{hn}\right) = 1$, $h = \overline{1, m}$ and the general solution

$$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} \end{cases}$$

then

$$\left(a_{h1}, \ldots, a_{hi-1}, a_{hi+1}, \ldots, a_{hn}\right) \mid \left(c_{i1}, \ldots, c_{in-m}\right)$$

irrespective of $h = \overline{1, m}$ and $i = \overline{1, n}$.

Proof:

Let's consider some arbitrary $h \in \overline{1, m}$ and some arbitrary $i \in \overline{1, n}$;

$$a_{h1}x_1 + \ldots + a_{hi-1}x_{i-1} + a_{hi+1}x_{i+1} + \ldots + a_{hn}x_n = a_{hi}x_i.$$

Because

$$\left(a_{h1},...,a_{hi-1},a_{hi+1},...,a_{hn}\right)\big| a_{hi}$$

it results that

$$d=\left(a_{h1},...,a_{hi-1},a_{hi+1},...,a_{hn}\right)\big| x_i$$

irrespective of the value of x_i in the vector of particular solutions.

For $k_2 = k_3 = ... = k_{n-m} = 0$ and $k_1 = 1$ we obtain the particular solution:

$$\begin{cases} x_1 = c_{11} \\ \vdots \\ x_i = c_{i1} \;\Rightarrow d \mid c_{i1} \\ \vdots \\ x_n = c_{n1} \end{cases}$$

For $k_1 = k_2 = ... = k_{n-m-1} = 0$ and $k_{n-m} = 1$ it results the following particular solution:

$$\begin{cases} x_1 = c_{1n-m} \\ \vdots \\ x_i = c_{in-m} \;\Rightarrow d \mid c_{in-m}\,; \\ \vdots \\ x_n = c_{nn-m} \end{cases}$$

hence

$$d \mid c_{ij},\; j=\overline{1,n-m} \Rightarrow d\big|\left(c_{i1},...,c_{in-m}\right).$$

Theorem 3.

If

$$\begin{cases} x_1 = c_{11}k_1 + ... + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + ... + c_{nn-m}k_{n-m} \end{cases}$$

k_j = parameters $\in \mathbb{Z}$, $c_{ij} \in \mathbb{Z}$ being given, is the general solution of the homogeneous linear system

$$\begin{cases} a_{11}x_1 + ... + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + ... + a_{mn}x_n = 0 \end{cases}, \quad r(A) = m < n$$

then $\left(c_{1j},...,c_{nj}\right)=1$, $\forall j=\overline{1,n-m}$.

Proof:

We assume, by reduction ad absurdum, that there is $j_0 \in \overline{1,n-m} : \left(c_{1j_0},...,c_{nj_0}\right) = d$ we consider the maximal co-divisor >0; we reduce to the case when the maximal co-divisor is $-d$ to the case when it is equal to d (non restrictive hypothesis); then the general solution can be written under the form:

$$(5)\qquad \begin{cases} x_1 = c_{11}k_1 + ... + c'_{1j_0}dk_{j_0} + ... + c_{1n-m}k_{n-m} \\ : \\ x_n = c_{n1}k_1 + ... + c'_{nj_0}dk_{j_0} + ... + c_{nn-m}k_{n-m} \end{cases}$$

where $d = \left(c_{ij_0},..,c_{nj_0}\right)$, $c_{ij_0} = d \cdot c'_{ij_0}$ and $\left(c'_{ij_0},...,c'_{nj_0}\right) = 1$.

We prove that

$$\begin{cases} x_1 = c'_{1j_0} \\ : \\ x_n = c'_{nj_0} \end{cases}$$

is a particular solution of the homogeneous linear system.

We'll note:

$$C = \begin{pmatrix} c_{11} & ... & c'_{ij_0} & d & ... & c_{1n-m} \\ : & & : & & & : \\ c_{n1} & ... & c'_{nj_0} & d & ... & c_{nn-m} \end{pmatrix},\ k = \begin{pmatrix} k_1 \\ : \\ k_{j_0} \\ : \\ k_{n-m} \end{pmatrix}$$

$x = C \cdot k$ the general solution.

We know that $AX = 0 \Rightarrow A(CK) = 0$, $A = \begin{pmatrix} a_{11} ... \ a_{1n} \\ : \\ a_{n1} ... \ a_{mn} \end{pmatrix}$.

We assume that the principal variables are $x_1,...,x_m$ (if not, we have to renumber). It follows that $x_{m+1},...,x_n$ are the secondary variables.

For $k_1 = ... = k_{j_0-1} = k_{j_0+1} = ... = k_{n-m} = 0$ and $k_{j_0} = 1$ we obtain a particular solution of the system

$$\begin{cases} x_1 = c'_{1j_0}d \\ : \\ x_n = c'_{nj_0}d \end{cases} \Rightarrow 0 = A\begin{pmatrix} c'_{1j_0}d \\ : \\ c'_{nj_0}d \end{pmatrix} = d \cdot A\begin{pmatrix} c'_{1j_0} \\ : \\ c'_{nj_0} \end{pmatrix} \Rightarrow A\begin{pmatrix} c'_{1j_0} \\ : \\ c'_{nj_0} \end{pmatrix} = 0 \Rightarrow \begin{cases} x_1 = c'_{1j_0} \\ : \\ x_n = c'_{nj_0} \end{cases}$$

is the particular solution of the system.

We'll prove that this particular solution cannot be obtained by

$$(6)\qquad \begin{cases} x_1 = c_{11}k_1 + ... + c'_{1j_0}dk_{j_0} + ... + c_{1n-m}k_{n-m} = c'_{1j_0} \\ : \\ x_n = c_{n1}k_1 + ... + c'_{nj_0}dk_{j_0} + ... + c_{nn-m}k_{n-m} = c'_{nj_0} \end{cases}$$

(7) $$\begin{cases} x_{m+1} = c_{m+1}k_1 + \ldots + c'_{m+1}dk_{j_0} + \ldots + c_{m+1,n-m}k_{n-m} = c'_{m+1j_0} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c'_{nj_0}dk_{j_0} + \ldots + c_{nn-m}k_{n-m} = c'_{nj_0} \end{cases}$$

$$\Rightarrow\ k_{j_0} = \frac{\begin{vmatrix} c_{m+1,1} & \ldots & c_{m+1j} & \ldots & c_{m+1,n-m} \\ \vdots & & \vdots & 0. & \vdots \\ c_{h,1} & \ldots & c_{nj} & \ldots & c_{n,n-m} \end{vmatrix}}{\begin{vmatrix} c_{m+1,1} & \ldots & c'_{m+1j_0}d & \ldots & c_{m+1,n-m} \\ \vdots & & \vdots & 0. & \vdots \\ c_{h,1} & \ldots & c'_{nj}d & \ldots & c_{n,n-m} \end{vmatrix}} = \frac{1}{d} \notin \mathbb{Z}$$

(because $d \neq 1$).

It is important to point out the fact that those $k_j = k_j^0$, $j = \overline{1, n-m}$, that satisfy the system (7) also satisfy the system (6), because, otherwise (6) would not satisfy the definition of the solution of a linear system of equations (i.e., considering the system (7) the hypothesis was not restrictive). From $X_{j_0} \in \mathbb{Z}$ follows that (6) is not the general solution of the homogeneous linear system contrary to the hypothesis); then $\left(c_{1j}, \ldots, c_{nj}\right) = 1$, irrespective of $j = \overline{1, n-m}$.

Property 3. Let's consider the linear system

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}$$

$a_{ij}, b_i \in \mathbb{Z}$, $r(A) = m < n$, $x_j =$ unknowns $\in \mathbb{Z}$

Resolved in $\mathbb{R}$, we obtain

$$\begin{cases} x_1 = f_1\left(x_{m+1}, \ldots, x_n\right) \\ \vdots \\ x_m = f_m\left(x_{m+1}, \ldots, x_n\right) \end{cases},\ x_1, \ldots, x_m \text{ are the main variables,}$$

where f_i are linear functions of the form:

$$f_i = \frac{c^i_{m+1}x_{m+1} + \ldots + c^i_n x_n + e_i}{d_i},$$

where $c^i_{m+j},\ d_i,\ e_i \in \mathbb{Z}$; $i = \overline{1, m},\ j = \overline{1, n-m}$.

If $\dfrac{e_i}{d_i} \in \mathbb{Z}$ irrespective of $i = \overline{1, m}$ then the linear system has integer solution.

Proof:

For $1 \leq i \leq m,\ x_i \in \mathbb{Z}$, then $f_j \in \mathbb{Z}$. Let's consider

$$\begin{cases} x_{m+1} = u_{m+1}k_{m+1} \\ \vdots \\ x_n = u_n k_n \\ \vdots \\ x_1 = v_{m+1}^1 k_{m+1} + \ldots + v_n^1 k_n + \dfrac{e_1}{d_1} \\ \vdots \\ x_m = v_{m+1}^m k_{m+1} + \ldots + v_n^m k_n + \dfrac{e_m}{d_m} \end{cases}$$

a solution, where u_{m+1} is the maximal co-divisor of the denominators of the fractions $\dfrac{c_{m+j}^i}{d_i}$, $i = \overline{1,m}$, $j = \overline{1,n-m}$ calculated after their complete simplification.

$v_{m+j}^i = \dfrac{c_{m+j}^i u_{m+j}}{d_i} \in \mathbb{Z}$ is a $(n-m)$-times undetermined solution which depends on $n-m$ independent parameters $(k_{m+1},\ldots,k_n)$ but is not a general solution.

Property 4. Under the conditions of property 3, if there is an $i_0 \in \overline{1,m}$: $f_{i_0} = u_{m+1}^{i_0} x_{m+1} + \ldots + u_n^{i_0} x_n + \dfrac{e_{i_0}}{d_{i_0}}$ with $u_{m+j}^{i_0} \in \mathbb{Z}$, $j = \overline{1,n-m}$, and $\dfrac{e_{i_0}}{d_{i_0}} \notin \mathbb{Z}$ then the system does not have integer solution.

Proof:

$\forall x_{m+1},\ldots,x_n$ in $\mathbb{Z}$, it results that $x_{i_0} \notin \mathbb{Z}$.

Theorem 4. Let's consider the linear system

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}$$

$a_{ij}, b_i \in \mathbb{Z}$, x_j = unknowns $\in \mathbb{Z}$, $r(A) = m < n$. If there are indices $1 \le i_1 < \ldots < i_m \le n$, $i_h \in \{1,2,..,n\}$, $h = \overline{1,m}$, with the property:

$$\Delta = \begin{vmatrix} a_{1i_1} & \ldots & a_{1i_m} \\ \vdots & & \vdots \\ a_{mi_1} & \ldots & a_{mi_m} \end{vmatrix} \neq 0 \text{ and}$$

$$\Delta_{x_{i_1}} = \begin{vmatrix} b_1 & a_{1i_2} & \dots & a_{1i_m} \\ : & : & & : \\ b_m & a_{mi_2} & \dots & a_{mi_m} \end{vmatrix} \text{ is divided by } \Delta$$

.
.
.

$$\Delta_{x_{i_m}} = \begin{vmatrix} a_{1i_1} & \dots & a_{1i_{m-1}} & b_1 \\ : & & : & : \\ a_{mi_1} & \dots & a_{mi_{m-1}} & b_m \end{vmatrix} \text{ is divided by } \Delta$$

then the system has integer number solutions.

Proof:

We use property 3

$$d_i = \Delta,\ i = \overline{1, m};\ e_{i_h} = \Delta_{x_{i_h}},\ h = \overline{1, m}$$

Note 1. It is not true in the reverse case.

Consequence 1. Any homogeneous linear system has integer number solutions (besides the trivial one); $r(A) = m < n$.

Proof:

$$\Delta_{x_{i_h}} = 0 : \Delta, \text{ irrespective of } h = \overline{1, m}.$$

Consequence 2. If $\Delta = \pm 1$, it follows that the linear system has integer number solutions.

Proof:

$\Delta_{x_{i_h}} : (\pm 1)$, irrespective of $h = \overline{1, m}$;

$\Delta_{x_{i_h}} \in \mathbb{Z}$.

FIVE INTEGER NUMBER ALGORITHMS TO SOLVE LINEAR SYSTEMS

This section further extends the results obtained in chapters 4 and 5 (from linear equation to linear systems). Each algorithm is thoroughly proved and then an example is given.

Five integer number algorithms to solve linear systems are further given.

Algorithm 1. (Method of Substitution)

(Although simple, this algorithm requires complex computations but is, nevertheless, easy to implement into a computer program).

Some integer number equation are initially solved (which is usually simpler) by means of one of the algorithms 4 or 5. (If there is an equation of the system which does not have integer systems, then the integer system does not have integer systems, then Stop.) The general integer solution of the equation will depend on $n-1$ integer number parameters (see [5]):

$$(p_1) \qquad x_{i_1} = f_{i_1}^{(1)}\left(k_1^{(1)},...,k_{n-1}^{(1)}\right),\ i=\overline{1,n},$$

where all functions $f_{i_1}^{(1)}$ are linear and have integer number coefficients.

This general integer number system (p_1) is introduced into the other $m-1$ equations of the system. We obtain a new system of $m-1$ equations with $n-1$ unknown variables:

$$k_{i_1}^{(1)},\ i_1=\overline{1,n-1},$$

which is also to be solved with integer numbers. The procedure is similar. Solving a new equation, we obtain its general integer solution:

$$(p_2) \qquad k_{i_2}^{(1)} = f_{i_2}^{(2)}\left(k_1^{(2)},...,k_{n-2}^{(2)}\right),\ i_2=\overline{1,n-1},$$

where all functions $f_{i_2}^{(2)}$ are linear, with integer number coefficients. (If, along this algorithm we come across an equation, which does not have integer solutions, then the initial system does not have integer solution. Stop.)

In the case that all solved equations had integer system at step (j), $1\le j\le r$ (r being of the same rank as the matrix associated to the system) then:

$$(p_j) \qquad k_{i_j}^{(j-1)} = f_{i_j}^{(j)}\left(k_1^{(j)},...,k_{n-j}^{(j)}\right),\ i_j=\overline{1,n-j+1},$$

$f_{i_j}^{(j)}$ are linear functions and have integer number coefficients.

Finally, after r steps, and if all solved equations had integer solutions, we obtain the integer solution of one equation with $n-r+1$ unknown variables.

The system will have integer solutions if and only if in this last equation has integer solutions.

If it does, let its general integer solution be:

$$(p_r) \qquad k_{i_r}^{(r-1)} = f_{i_r}^{(r)}\left(k_1^{(r)},...,k_{n-1}^{(r)}\right),\ i_r=\overline{1,n-r+1},$$

where all $f_{i_r}^{(r)}$ are linear functions with integer number coefficients.

We'll present now the reverse procedure as follows.

We introduce the values of $k_{i_r}^{(r-1)}$, $i_r=\overline{1,n-r+1}$, at step p_r in the values of

$$k_{i_{r-1}}^{(r-2)},\ i_{r-1}=\overline{1,n-r+2}$$

from step (p_{r-1}).

It follows:

$$k_{i_{r-1}}^{(r-2)}=f_{i_{r-1}}^{(r-1)}\left(f_1^{(r)}\left(k_1^{(r)},...,k_{n-r}^{(r)}\right),...,f_{n-r+1}^{(r)}\left(k_1^{(r)},...,k_{n-r}^{(r)}\right)\right)=g_{i_{r-1}}^{(r-1)}\left(k_1^{(r)},...,k_{n-r}^{(r)}\right),$$

$i_{r-1}=\overline{1,n-r-1}$, from which it follows that $g_{i_r}^{(r-1)}$ are linear functions with integer number coefficients.

Then follows those (p_{r-2}) in (p_{r-e}) and so on, until we introduce the values obtained at step (p_2) in those from the step (p_1).

It will follow:

$$x_{i_j}=g_i^1\left(k_1^{(r)},...,k_{n-r}^{(r)}\right)$$

notation $g_{i_1}\left(k_1,...,k_{n-r}\right)$, $i=\overline{1,n}$, with all g_{i_1} most obviously, linear functions with integer number coefficients (the notation was made for simplicity and aesthetical aspects). This is, thus, the general integer solution, of the initial system.

The correctness of Algorithm 1.

The algorithm is finite because it has r steps on the forward way and $r-1$ steps on the reverse, $(r<+\infty)$. Obviously, if one equation of one system does not have (integer number) solutions then the system does not have solutions either.

Writing S for the initial system and S_j the system resulted from step (p_j), $1\le j\le r-2$, it follows that passing from (p_j) to (p_{j+1}) we pass from a system S_j to a system S_{j+1} equivalent from the point of view of the integer number solution, i.e.

$$k_{i_j}^{(j-1)}=t_{i_j}^0,\ \ i_j=\overline{1,n-j+1},$$

which is a particular integer solution of the system S_j if and only if

$$k_{i_{j+1}}^{(j)}=h_{i_{j+1}}^0,\ i_{j+1}=\overline{1,n-j},$$

is a particular integer solution of the system S_{j+1} where

$$k_{i_{j+1}}^0=f_{i_{j+1}}^{(j+1)}\left(t_1^0,...,t_{n-j+1}^0\right),\ i_{j+1}=\overline{1,n-j}.$$

Hence, their general integer solutions are also equivalent (considering these substitutions). Such that, in the end, resolving the initial system S is equivalent with solving the equation (of the system consisting of one equation) S_{r-1} with integer number coefficients. It follows that the system S has integer number solution if and only if the systems S_j have integer number solution, $1\le j\le r-1$.

Example 1. By means of algorithm 1, let us calculate the integer number solution of the following system:

$$(S)\qquad \begin{cases} 5x-7y-2z+6w=6 \\ -4x+6y-3z+11w=0 \end{cases}$$

Solution: We solve the first integer number equation. We obtain the general solution (see [4] or [5]):

(p_1)
$$\begin{cases} x = t_1 + 2t_2 \\ y = t_1 \\ z = -t_1 + 5t_2 + 3t_3 - 3 \\ w = t_3 \end{cases}$$
where $t_1,\ t_2,\ t_3 \in \mathbb{Z}$.

Substituting in the second, we obtain the system:

(S_1) $$5t_1 - 23t_2 + 2t_3 + 9 = 0.$$

Solving this integer equation we obtain its general integer solution:

(p_2)
$$\begin{cases} t_1 = k_1 \\ t_2 = k_1 + 2k_2 + 1 \\ t_3 = 9k_1 + 23k_2 + 7 \end{cases}$$
where $k_1,\ k_2 \in \mathbb{Z}$.

The reverse way. Substituting (p_2) in (p_1) we obtain:
$$\begin{cases} x = 3k_1 + 4k_2 + 2 \\ y = k_1 \\ z = 31k_1 + 79k_2 + 23 \\ w = 9k_1 + 23k_2 + 7 \end{cases}$$
where $k_1,\ k_2 \in \mathbb{Z}$, which is the general integer solution of the initial system (S). Stop.

Algorithm 2.

Input

A linear system (1) without all $a_{ij} = 0$.

Output

We decide on the possibility of an integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. $t = 1,\ h = 1,\ p = 1$

2. (A) Divide each equation by the largest co-divisor of the coefficients of the unknown variables. If you do not obtain an integer quotient for at least one equation, then the system does not have integer solutions. Stop.

(B) If there is an inequality in the system, then the system does not have integer solutions. Stop.

(C) If repetition of more equations occurs, keep one and if an equation is an identity, remove it from the system.

3. If there is (i_0, j_0) such that $\left|a_{i_0 j_0}\right| = 1$ then obtain the value of the variable x_{j_0} from equation i_0; statement (T_t).

Substitute this statement (where possible) in the other equations of the system and in the statement (T_{t-1}), (H_h) and (P_p) for all i, h, and p. Consider $t := t + 1$, remove equation (i_0) from the system. If there is no such pair, go to step 5.

4. Does the system (left) have at least one unknown variable? If it does, consider the new data and go on to step 2. If it does not, write the general integer solution of the system substituting $k_1, k_2, ...$ for all variables from the right term of each expression which gives the value of the unknowns of the initial system. Stop.

5. Calculate

$$a = \min_{i, j_1, j_2} \left\{ |r| \, a_{ij_1} \equiv r \left(\operatorname{mod} a_{ij_2} \right), \ 0 < |r| < \left| a_{ij_2} \right| \right\}$$

and determine the indices i, j_1, j_2 as well as the r for which this minimum can be calculated. (If there are more variables, choose one arbitrarily.)

6. Write: $x_{j_2} = t_h \dfrac{a_{ij_1} - r}{a_{ij_2}} x_{ij_2}$, statement (H_h). Substitute this statement (where possible in all the equations of the system and in the statements $(T_t), (H_h)$ and (P_p) for all t, h, and p.

7. (A) If $a \neq 1$, consider $x_{j_2} := t_h, \ h := h + 1$, and go on to step 2.

(B) If $a = 1$, then obtain the value of x_{j_1} from the equation (i); statement (P_p). Substitute this statement (where possible in the other equations of the system and in the relations $(T_t), (H_h)$ and (P_{p-1}) for all t, h, and p.

Remove the equation (i) from the system.

Consider $h := h + 1, \ p := p + 1$, and go back to step 4.

The correctness of algorithm 2. Let consider system (1).

Lemma 1. We consider the algorithm at step 5. Also, let

$$M = \left\{ |r|, \ a_{ij_1} \equiv r \left(\operatorname{mod} a_{ij_2} \right), \ 0 < |r| < \left| a_{ij_2} \right|, \ i, j_1, j_2 = 1, 2, 3, ... \right\}.$$

Then $M \neq \emptyset$.

*Proof***:**

Obviously, M is finite and $M \subset \mathbb{N}^*$. Then, M has a minimum if and only if $M \neq \emptyset$. We suppose, conversely, that $M = \emptyset$. Then

$$a_{ij_2} \equiv 0 (\operatorname{mod} a_{ij_2}), \ \forall \ i, j_1, j_2.$$

It follows as well that

$$a_{ij_2} \equiv 0 (\operatorname{mod} a_{ij_1}), \ \forall \ i, j_1, j_2.$$

That is

$$\left| a_{ij_1} \right| = \left| a_{ij_2} \right|, \ \forall \ i, j_1, j_2.$$

We consider an i_0 arbitrary but fixed. It is clear that

$$(a_{i_0 1}, ..., a_{i_0 n}) : \ a_{i_0 j} \neq 0, \ \forall j$$

(because the algorithm has passed through the sub-steps 2(B) and 2(C). But, because it has also passed through step 3, it follows that

$$\left| a_{i_0 j} \right| \neq 1, \ \forall j,$$

but as it previously passed through step 2(A), it would result that

$$\left|a_{i_0 j}\right| = 1,\ \forall j .$$

This contradiction shows that the assumption is false.

Lemma 2. Let's consider $a_{i_0 j_1} \equiv r(\bmod a_{ij_2})$. Substitute

$$x_{j_2} = t_h - \frac{a_{i_0 j} - r}{a_{i_0 j_2}} x_{j_1}$$

in system (A) obtaining system (B). Then

$$x_j = x_j^0,\ j = \overline{1,n}$$

is the particular integer solution of (A) if and only if

$$x_j = x_j^0,\ j \neq j_2 \text{ and } t_h = x_{j_2}^0 - \frac{a_{i_0 j_1} - r}{a_{i_0 j_2}}$$

is the particular integer solution of (B).

Lemma 3. Let $a_1 \neq$ and a_2 obtained at step 5.

Then $0 < a_2 < a_1$

Proof:

It is sufficient to show that $a_1 < \left|a_{ij}\right|,\ \forall\ i,\ j$ because in order to get a_2, step 6 is obligatory, when the coefficients if the new system are calculated, a_1 being equal to a coefficient form the new system (equality of modules), the coefficient on $(i_0\, j_1)$.

Let $a_{i_0 j_0}$ with the property $\left|a_{i_0 j_0}\right| \leq a_1$.

Hence, $a_1 \geq \left|a_{i_0 j}\right| = \min\left\{\left|a_{i_0 j}\right|\right\}$. Let $a_{i_0 j_s}$ with $\left|a_{i_0 j_s}\right| > \left|a_{ij_m}\right|$; there is such an element because $\left|a_{i_0 j_m}\right|$ is the minimum of the coefficients in the module and not all $\left|a_{i_0 j}\right|,\ j = \overline{1,n}$ are equal (conversely, it would result that $(a_{i_0 j}, \ldots., a_{i_0 n}) \sim a_{i_0 j},\ \forall j \in \overline{1,r}$, the algorithm passed through sub-step 2(A) has simplified each equation by the maximal co-divisor of its coefficients; hence, it would follow that $\left|a_{i_0 j}\right| = 1,\ \forall j = \overline{1,n}$, which, again, cannot be real because the algorithm also passed through step 3). Out of the coefficients $a_{i_0 j_m}$ we choose one with the property $a_{i_0 j_{s_0}} \neq M a_{i_0 j_m}$ there is such an element (contrary, it would result $(a_{i_0 j}, \ldots, a_{i_0 n}) \sim \left|a_{i_0 j_m}\right|$ but the algorithm has also passed through step 2(A) and it would mean that $\left|a_{i_0 j_m}\right| = 1$ which contradicts step 3 through which the algorithm has also passed).

Considering $q_0 = \left[a_{i_0 j_{s_0}} / a_{i_0 j_m}\right] \in \mathbb{Z}$ and $r = a_{i_0 j_{s_0}} - q_0 a_{i_0 j_m} \in \mathbb{Z}$, we have $a_{i_0 j_{s_0}} \equiv r_0(\bmod a_{i_0 j_m})$ and $0 < \left|r_0\right| < \left|a_{i_0 j_m}\right| < \left|a_{i_0 j_0}\right| \leq a_1$. We have, thus, obtained an r_0 with $\left|r_0\right| < a_1$, which is in contradiction with the very definition of a_1. Thus $a_1 < \left|a_{ij}\right|,\ \forall i, j$.

Lemma 4. Algorithm 2 is finite.

Proof:

The functioning of the algorithm is meant to transform a linear system of m equations and n unknowns into one of $m_1 \times n_1$ with $m_1 < m$, $n_1 < n$, thus, successively into a final linear equation with $n - r + 1$ unknowns (where r is the rank of the associated matrix). This equation is solved by means of the same algorithm (which works as [5]). The general integer solution of the system will depend on the $n-1$ integer number independent parameters (see [6] – similar properties can be established also the general integer solution of the linear system). The reduction of equations occurs at steps 2, 3 and sub-step 7(B). Step 2 and 3 are obvious and, hence, trivial; they can reduce the equation of the system (or even put an end to it) but only under particular conditions. The most important case finds its solution at step 7(B), which always reduces one equation of the system. As the number of equations is finite we come to solve a single integer number equation. We also have to show that the transfer from one system $m_i \times n_i$ to another $m_{i+1} \times n_{i+1}$ is made in a finite interval of time: by steps 5 and 6 permanent substitution of variables are made until we to $a = 1$(we to $a = 1$ because, according to lemma 3, all $a - s$ are positive integer numbers and form a strictly decreasing row).

Theorem of correctness.

Algorithm 2 correctly calculates the general integer solution of the linear system.

Proof:

Algorithm 2 is finite according to lemma 4. Steps 2 and 3 are obvious (see also [4], [5]). Their part is to simplify the calculations as much as possible. Step 4 tests the finality of the algorithm; the substitution with the parameters $k_1, k_2, \ldots$ has systematization and aesthetic reasons. The variables $t,\ h, p$ are counter variables (started at step 1) and they are meant to count the statement of the type T, H, P (numbering required by the substitutions at steps 3, 6 and sub-step 7(B); h also counts the new (auxiliary) variables introduced in the moment of decomposition of the system. The substitution from step 6 does not affect the general integer solution of the system (it follows from lemma 2). Lemma 1 shows that at step 5 there is always a, because $\emptyset \neq M \subset \mathbb{N}^*$.

The algorithm performs the transformation of a system $m_i \times n_i$ into another $m_{i+1} \times n_{i+1}$, equivalent to it, preserving the general solution (taking into account, however, the substitutions) (see also lemma 2).

Example 2. Calculate the integer solution of:

$$\begin{cases} 12x - 7y + 9z = 12 \\ -5y + 8z + 10w = 0 \\ 0z + 0w = 0 \\ 15x + 21z + 69w = 3 \end{cases}$$

Solution:

We apply algorithm 2 (we purposely selected an example to be passed through all the steps of this algorithm):

1. $t = 1,\ h = 1,\ p = 1$
2. (A) The fourth equation becomes $5x + 7z + 23w = 1$

(B) –
(C) Equation 3 is removed.
3. No; go on to step5.
5. $a = 2$ and $i = 1,\ j_1 = 2,\ j_2 = 3$, and $r = 2$.
6. $z = t_1 + y$, the statement (H_1). Substituting it in the

$$\begin{cases} 12x - 2y + 9t_1 \qquad\quad = 12 \\ \qquad 3y + 9t_1 + 10w \ = 0 \\ 5x \ + 7y + 7t_1 + 23w \ = 1 \end{cases}$$

7. $a \neq 1$ consider $z = t_1, h := 2$, and go back to step 2.
2. –
3. No. Step 5.
5. $a = 1$ and $i = 2,\ j_1 = 4,\ j_2 = 2$, and $r = 1$.
6. $y = t_2 - 3w$, the statement (H_2). Substituting in the system:

$$\begin{cases} -12x + 2t_2 + 9t_1 - 6w = 12 \\ \qquad\quad 3t_2 + 8t_1 + \ \ w = 0 \\ \ \ 5x \ + 7t_2 + 7t_1 + 2w = 1 \end{cases}$$

Substituting it in statement (H_1), we obtain:

$z = t_1 + t_2 - 3w$, statement $(H_1)'$.

7. $w = -3t_2 - 8t_1$ statement (P_1).
Substituting it in the system, we obtain:

$$\begin{cases} -12x - 20t_2 + 57t_1 = 12 \\ \ \ 5x \quad\ + t_2 - \ \ 9t_1 = 1 \end{cases}$$

Substituting it in the other statements, we obtain:

$z = 10t_2 + 25t_1,\ \ (H_1)''$

$y = 10t_2 + 24t_1,\ \ (H_2)''$

$h := 3,\ p := 2$, and go back to step 4.

4. Yes.
2. –
3. $t_2 = 1 - 5x + 9t_1$, statement (T_1).
Substituting it (where possible) we obtain:

$\{-112x + 237t_1 = -8$ (the new system);

$z = \ 10 - 50x + 115t_1,\ \ (H_1)'''$

$y = \ 10 - 50x + 114t_1,\ \ (H_2)''$

$w = -3 + 15x + \ \ 35t_1,\ \ (P_1)'$

Consider $t := 2$ go on to step 4.
4. Yes. Go back to step 2. (From now on algorithm 2 works similarly with that from [5], with the only difference that the substitution must also be made in the statements obtained up to this point).
2. –
3. No. Go on to step 5.

5. $a = 13$ (one three) and $i = 1,\ j_1 = 2,\ j_2 = 1$, and $r = 13$.

6. $x = t_3 + 2t_1$, statement (H_3).

After substituting we obtain:

$$\{-112t_3 + 13t_1 = -8 \text{ (the system)}$$

$$z = 10 - 50t_3 + 15t_1,\quad (H_1)^{IV};$$

$$y = 10 - 50t_3 + 14t_1,\ (H_2)''';$$

$$w = -3 + 15t_3\ - 5t_1,\quad (P_1)'';$$

$$t_2 = \ 1 - \ 5t_3\ -\ t_{1,}\quad (T_1)';$$

7. $x := t_3,\ h := 4$ and go on to step 2.

2. –

3. No, go on to step 5.

5. $a = 5$ and $i = 1,\ j_1 = 1,\ j_2 = 2$ and $r = 5$

6. $t_1 = t_4 + 9t_3$, statement (H_4).

Substituting it, we obtain :

$$5t_3 + 13t_4 = -8 \text{ (the system).}$$

$$z = \ 10 + 85t_3 + 15t_4,\quad (H_1)^{V};$$

$$y = \ 10 + 76t_3 + 14t_4,\ (H_2)^{IV};$$

$$x = \qquad 19t_3 + \ 2t_4,\quad (H_3)';$$

$$w = -3 - 30t_3 - \ 5t_4,\quad (P_1)''';$$

$$t_2 = \ 1 - 14t_3 - \quad t_{4,}\quad (T_1)'';$$

7. $t_1 := t_4; h := 5$ and go back to step 2.

2. –

3. No. Step 5.

5. $a = 2$ and $i = 1,\ j_1 = 2,\ j_2 = 1$ and $r = -2$.

6. $t_3 = t_5 - 3t_4$ statement (H_5). After substituting, we obtain:

$$5t_5 - 2t_4 = -8 \text{ (the system).}$$

$$z = 10 + 85t_5 - 240t_4,\quad (H_1)^{VI};$$

$$y = 10 + 76t_5 - 214t_4,\quad (H_2)^{V};$$

$$x = \qquad 19t_5 - 55t_4,\quad (H_3)^{IV};$$

$$w = -3 - 30t_5 + 85t_4,\quad (P_1)^{IV};$$

$$t_2 = -1 - 14t_5 + 41t_4\ ,\quad (T_1)''';$$

$$t_1 = \qquad\quad 9t_5 + 26t_4,\quad (H_4)';$$

7. $t_3 := t_6, h := 6$ and go back to step 2.

2. –

3. No. Step 5.

5. $a = 1$ and $i = 1,\ j_1 = 2,\ j_2, r = 1$.

6. $t_4 = t_6 + 2t_5$ statement (H_6). After substituting, we obtain:

$$t_5 - 2t_6 = -8 \text{ (the system)}$$

$$z = 10 - 395t_5 - 240t_6, \quad (H_1)^{VII};$$
$$y = 10 - 392t_5 - 214t_6, \quad (H_2)^{IV};$$
$$x = \quad -91t_5 - 55t_6, \quad (H_3)^{'''};$$
$$w = -3 + 140t_5 + 85t_6, \quad (P_1)^{V};$$
$$t_2 = \quad 1 + 68t_5 + 41t_6, \quad (T_1)^{IV};$$
$$t_1 = \quad -43t_5 - 26t_6, \quad (H_4)'';$$
$$t_3 = \quad -5t_5 - 3t_6, \quad (H_5);$$

7. $t_5 = 2t_6 - 8$ statement (P_2). Substituting it in the system we obtain: 0=0. Substituting it in the other statements, it follows:

$$z = -1030t_6 + 3170$$
$$y = -918t_6 + 2826$$
$$x = -237t_6 + 728$$
$$w = 365t_6 - 1123$$
$$\left.\begin{array}{l} t_2 = 177t_6 - 543 \\ t_1 = 112t_6 + 344 \\ t_3 = 13t_6 + 40 \\ t_4 = 5t_6 - 16 \end{array}\right\} \text{statements of no importance.}$$

Consider $h := 7, p := 3$, and go back to step 4. $t_6 \in \mathbb{Z}$

4. No. The general integer solution of the system is:

$$\begin{cases} x = -237k_1 + 728 \\ y = -918k_1 + 2826 \\ z = 1030k_1 + 3170 \\ w = 365k_1 - 1123 \end{cases}$$

where k_1 is an integer number parameter.

Stop.

Algorithm 3.

Input

A linear system (1)

Output

We decide on the possibility of an integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. Solve the system in $\mathbb{R}^n$. If it does not have solutions in $\mathbb{R}^n$, it does not have solutions in $\mathbb{Z}^n$ either. Stop.
2. $f = 1, \ t = 1, \ h = 1, \ g = 1$

3. Write the value of each main variable x_i under the form:

$$\left(E_{f,\,i}\right)_i : x_i = \sum_j q_{ij} x_j^{'} + q_i + \left(\sum_j r_{ij} x_j^{'} + r_i\right) / \Delta_i$$

with all $q_{ij},\ q_i,\ r_{ij},\ r_i,\ \Delta_i$ in $\mathbb{Z}$ such that all $\left|r_{ij}\right| < \left|\Delta_i\right|,\ \Delta_i \neq 0,\ \left|r_i\right| < \left|\Delta_i\right|$ (where all $x_j^{'}$ of the right term are integer number variables: either of the secondary variables of the system or other new variables introduced with the algorithm). For all i, we write

$r_{ij_f} \equiv \Delta_i$.

4. $\left(E_{f,\,i}\right)_i : \sum_j r_{ij} x_j^{'} - r_{ij_f} Y_{f,\,i} + r_i = 0$ where $\left(Y_{f,\,i}\right)_i$ are auxiliary integer number variables. We remove all the equations $\left(F_{f,\,i}\right)$ which are identities.

5. Does at least one equation $\left(F_{f,\,i}\right)$ exist? If it does not, write the general integer solution of the system substituting $k_1, k_2, \ldots$ for all the variables from the right term of each expression representing the value of the initial unknowns of the system. Stop.

6. (A) Divide each equation $\left(F_{f,\,i}\right)$ by the maximal co-divisor of the coefficients of their unknowns. If the quotient is not an integer number for at least one i_0 the system does not have integer solutions. Stop.

   (B) Simplify –as in m - all the fractions from the statements $\left(E_{f,\,i}\right)_i$.

7. Does $r_{i_0 j_0}$ exist having the absolute value 1? If it does not, go on to step 8. If it does, find the value of $x_j^{'}$ from the equation $\left(F_{f,\,i_0}\right)$; write $\left(T_t\right)$ for this statement, and substitute it (where it is possible) in the statements $\left(E_{f,\,i}\right)$, $\left(T^{t-1}\right)$, $\left(H_h\right)$, $\left(G_g\right)$ for all $i,\ t,\ h$ and g. Remove the equation $\left(F_{f,\,i_0}\right)$. Consider $f := f+1,\ t := t+1$, and go back to step3.

8. Calculate

$$a = \min_{i, j_1, j_2} \left\{ \left|r\right|,\ r_{ij_1} \equiv r (\operatorname{mod} r_{ij_2}),\ 0 < \left|r\right| < \left|r_{ij_2}\right| \right\}$$

and determine the indices $i_m,\ j_1,\ j_2$ as well as the r for which this minimum can be obtained. (When there are more variables, choose only one).

9. (A) Write $x_{j_2}^{'} = z_h - \dfrac{a_{i_m j_1} - r}{a_{j_m j_2}} x_{j_1}^{'}$, where z_h is a new integer variable; statement $\left(H_h\right)$.

   (B) Substitute the letter (where possible) in the statements $\left(E_{f,\,i}\right)$, $\left(F_{f,\,i}\right)$, $\left(T_t\right)$, $\left(H_{h-1}\right)$, $\left(G_g\right)$ for all $i,\ t,\ h$ and g.

   (C) Consider $h := h+1$.

10. (A) If $a \neq 1$ go back to step 4.

   (B) If $a = 1$ calculate the value of the variable $x_j^{'}$ from the equation $\left(F_{f,\,i}\right)$;

relation $\left(G_g^1\right)$. Substitute it (where possible) in the statements $\left(E_{f,\,i}\right)$, $\left(T_t\right)$, $\left(H_h\right)$, $\left(G_{g-1}\right)$ for all $i,\ t,\ h$, and g. Remove the equation $\left(F_{f,\,i}\right)$. Consider $g := g+1,\ f := f+1$ and go back to step 3.

The correctness of algorithm 3

Lemma 5. Let i be fixed. Then $\left(\sum_{j=n_1}^{n_2} r_{ij}x_j^{'} + r\right)|\Delta_i$ (with all $r_{ij},\ r_i,\ \Delta_i,\ n_1,\ n_2$ being integers, $n_1 \le n_2$, $\Delta_i \ne 0$ and all $x_j^{'}$ being integer variables) can have integer values if and only if $\left(r_{in_1},...,r_{in_2},\Delta_i\right)|\,r_i$.

Proof:

The fraction from the lemma can have integer values if and only if there is a $z \in \mathbb{Z}$ such that

$$\left(\sum_{j=n_1}^{n_2} r_{ij}x_j^{'} + r_i\right)|\,\Delta_i = z \Leftrightarrow \sum_{j=n_1}^{n_2} r_{ij}x_j^{'} - \Delta_i z + r_i = 0\,,$$

which is a linear equation. This equation has integer solution $\Leftrightarrow \left(r_{in_1},...,r_{in_2},\Delta_i\right)|\,r_i$.

Lemma 6. The algorithm is finite. It is true. The algorithm can stop at steps 1,5 or sub-steps 6(A). (It rarely stops at step 1).

One equation after another are gradually eliminated at step 4 and especially 7 and 10(B) $\left(F_{f,\,i}\right)$ - the number of equation is finite.

If at steps 4 and 7 the elimination of equations may occur only in special cases elimination of equations at sub step 10 (B) is always true because, through steps 8 and 9 we get to $a=1$ (see [5]) or even lemma 4 (from the correctness of algorithm 2). Hence, the algorithm is finite.

Theorem of Correctness.

The algorithm 3 correctly calculates the general integer solution of the system (1).

Proof:

The algorithm if finite according to lemma 6. It is obvious that the system does not have solution in $\mathbb{R}^n$ it does not have in $\mathbb{Z}^n$ either, because $\mathbb{Z}^n \subset \mathbb{R}^n$ (step 1).

The variables $f,\ t,\ h,\ g$ are counter variables and are meant to number the statements of the type $E,\ F,\ T,\ H$ and G, respectively. They are used to distinguish between the statements and make the necessary substitutions (step 2).

Step 3 is obvious. All coefficients of the unknowns being integers, each main variable x_i will be written:

$$x_i = \left(\sum_j c_{ij}x_j^{'} + c_i\right)|\,\Delta_i$$

which can assume the form and conditions required in this step.

Step 4 is obtained from 3 by writing each fraction equal to an integer variable $Y_{f,\,i}$ (this being $x_i \in \mathbb{Z}$).

Step 5 is very close to the end. If there is no fraction among all $(E_{f,\,i})$ it means that all main variables x_i already have values in $\mathbb{Z}$, while the secondary variables of the system can be arbitrary in $\mathbb{Z}$, or can be obtained from the statements T, H or G (but these have only integer expressions because of their definition and because only integer substitutions are made). The second assertion of this step is meant to systematize the parameters and renumber; it could be left out but aesthetic reasons dictate its presence. According to lemma 5 the step 6(A) is correct. (If a fraction depending on certain parameters (integer variables) cannot have values in $\mathbb{Z}$, then the main variable which has in the value of its expression such a fraction cannot have values in $\mathbb{Z}$ either; hence, the system does not have integer system). This 6(A) also has a simplifying role. The correctness of step 7, trivial as it is, also results from [4] and the steps 8-10 from [5] or even from algorithm 2 (lemma 4).

Ther initial system is equivalent to the "system" from step 3 (in fact, $(E_{f,\,i})$ as well, can be considered a system) Therefore, the general integer solution is preserved (the changes of variables do not prejudice it (see [4], [5], and also lemma 2 from the correctness of algorithm 2)). From a system $m_i \times n_i$ we form an equivalent system $m_{i+1} \times n_{i+1}$ with $m_{i+1} < m_i$ and $n_{i+1} < n_i$. This algorithm works similarly to algorithm 2.

Example 3. Employing algorithm 3, find an integer solution of the following system:

$$\begin{cases} 3x_1 + 4x_2 \quad + 22x_4 - 8x_5 = 25 \\ 6x_1 \qquad\quad + 46x_4 - 12x_5 = 2 \\ \qquad 4x_2 + 3x_3 - x_4 + 9x_5 = 26 \end{cases}$$

Solution

1. Common resolving in $\mathbb{R}^3$ it follows:

$$\begin{cases} x_1 = \dfrac{23x_4 - 6x_5 - 1}{-3} \\ x_2 = \dfrac{x_4 + 2x_5 + 24}{4} \\ x_3 = \dfrac{11x_5 + 2}{3} \end{cases}$$

2. $f = 1,\ t = 1,\ h = 1,\ g = 1$

3. $$\begin{cases} x_1 = -7x_4 + 2x_5 + \dfrac{2x_4 - 1}{-3} & (E_{1,\,1}) \\ x_2 = \qquad\quad 6 + \dfrac{x_4 + 3x_5}{4} & (E_{1,\,2}) \\ x_3 = \qquad -4x_5 + \dfrac{x_5 + 2}{3} & (E_{1,\,3}) \end{cases}$$

4. $$\begin{cases} 2x_4 \quad\quad +3y_{11}-1=0 & (F_{1,\,1}) \\ x_4+2x_5-4y_{12} \quad\quad =0 & (F_{1,\,2}) \\ \quad\quad x_5-3y_{13}+2=0 & (F_{1,\,3}) \end{cases}$$

5. Yes.
6. –
7. Yes: $|r_{35}|=1$. Then $x_5=3y_{13}-2$ the statement (T_1). Substituting it in the others, we obtain:

$$\begin{cases} x_1=-7x_4+6y_{13}-4+\dfrac{2x_4-1}{-3} & (E_{1,\,1}) \\ x_2= \quad\quad 6+\dfrac{x_4+6y_{13}-4}{4} & (E_{1,\,2}) \\ x_3= \quad -12y_{13}+8+\dfrac{3y_{13}-2+2}{3} & (E_{1,\,3}) \end{cases}$$

Remove the equation $(F_{1,\,3})$.
Consider $f:=2,\ t:=2$; go back to step 3.

3 $$\begin{cases} x_1=-7x_4+6y_{13}-4+\dfrac{2x_4-1}{-3} & (E_{2,\,1}) \\ x_2= \quad\quad y_{13}+5+\dfrac{x_4+2y_{13}}{4} & (E_{2,\,2}) \\ x_3= \quad -11y_{13}+8 & (E_{2,\,3}) \end{cases}$$

4. $$\begin{cases} 2x_4 \quad\quad +3y_{21}-1=0 & (F_{2,\,1}) \\ x_4+2y_{13}-4y_{22} \quad\quad =0 & (F_{2,\,2}) \end{cases}$$

5. Yes.
6. –
7. Yes $|r_{24}|=1$. We obtain $x_4=-2y_{13}+4y_{22}$ statement (T_2). Substituting it in the others we obtain:

$$\begin{cases} x_1=-28y_{22}+20y_{13}+\dfrac{-4y_{13}+8y_{22}-1}{-3} & (E_{2,\,1})' \\ x_2= \quad y_{22}+\ y_{13}+5 & (E_{2,\,2})' \\ x_3= \quad -11y_{13}+8 & (E_{2,\,3})' \end{cases}$$

Remove the equation $(F_{2,\,2})$
Consider $f:=3,\ t:=3$ and go back to step 3.
3.

$$\begin{cases} x_1 = -22y_{13} + 30y_{22} + \dfrac{2y_{13} + 2y_{22} - 1}{-3} & (E_{3,\,1}) \\ x_2 = \quad y_{13} + y_{22} + 5 & (E_{2,\,2}) \\ x_3 = \quad -11y_{13} + 8 & (E_{3,\,3}) \end{cases}$$

4. $2y_{13} + 2y_{22} + 3y_{31} - 1 = 0 \quad (F_{3,\,1})$
5. Yes.
6. –
7. No.
8. $a = 1$ and $i_m = 1,\ j_1 = 31,\ j_2 = 22$, and $r = 1$.
9. (A) $y_{22} = z_1 - y_{31}$ (statement (H_1)).

   (B) Substituting it in the others we obtain:

$$\begin{cases} x_1 = -22y_{13} - 30z_1 + 30y_{31} - 4 + \dfrac{2y_{13} + 2z_1 - 2y_{31} - 1}{-3} & (E_{3,\,1})' \\ x_2 = \quad y_{13} + z_1 - y_{31} + 5 & (E_{3,\,2})' \\ x_3 = -11y_{13} + 8 & (E_{3,\,3})' \end{cases}$$

$$2y_{13} + 2z_1 + y_{31} - 1 = 0 \quad (F_{3,\,1})'$$

$$x_4 = -2y_{13} + 4z_1 - 4y_{13} \quad (T_2)'$$

   (C) Consider $h := 2$

10. (B) $y_{13} = 1 - 2y_{13} - 2z_1$, statement (G_1).

    Substituting it in the others we obtain:

$$x_1 = -40y_{13} - 92z_1 + 27 \quad (E_{3,1})''$$

$$x_2 = 3y_{13} + 3z_1 + 4 \quad (E_{3,2})''$$

$$x_3 = -11y_{13} + 8 \quad (E_{3,3})''$$

$$x_4 = 6y_{13} + 12z_1 - 4 \quad (T_2)''$$

$$y_{22} = 2y_{13} + 3z_1 - 1 \quad (H_1)'$$

Remove equation $(F_{3,\,1})$.

Consider $g := 2,\ f := 4$ and go back to step 3.

3.

$$\begin{cases} x_1 = -40y_{13} - 92z_1 + 27 & (E_{4,1}) \\ x_2 = \quad 3y_{13} + 3z_1 + 4 & (E_{4,2}) \\ x_3 = -11y_{13} + 8 & (E_{4,3}) \end{cases}$$

4. -
5. No. The general solution of the initial system is:

$$
\begin{cases}
x_1 = -40k_1 - 92k_2 + 27, & \text{from } \left(E_{4,1}\right) \\
x_2 = \quad 3k_1 + \ 3k_2 \ \ + 4, & \text{from } \left(E_{4,2}\right) \\
x_3 = -11k_1 \qquad\quad + 8, & \text{from } \left(E_{4,3}\right) \\
x_4 = \quad 6k_1 + 12k_2 \ \ - 4, & \text{from } \left(T_2\right)" \\
x_5 = \quad 3k_1 \qquad\quad - 2, & \text{from } \left(T_1\right)
\end{cases}
$$

where $k_1, k_2 \in \mathbb{Z}$.

Algorithm 4
Input
A linear system (1) with not all $a_{ij} = 0$.

Output

We decide on the possibility of integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. $h = 1,\ v = 1$.
2. (A) Divide every equation i by the largest co-divisor of the coefficients of the unknowns. If the quotient is not an integer for at least one i_0 then the system does not have integer solutions. Stop.

   (B) If there is an inequality in the system, then it does not have integer solutions

   (C) In case of repetition, retain only one equation of that kind.

   (D) Remove all the equations which are identities.
3. Calculate $a = \min\limits_{i,j}\left\{\left|a_{ij}\right|,\ a_{ij} \neq 0\right\}$ and determine the indices i_0, j_0 for which this minimum can be obtained. (If there are more variables, choose one, at random.)
4. If $a \neq 1$ go on to step 6.
   If $a = 1$, then:
   (A) Calculate the value of the variable x_{j_0} from the equation i_0 note this statement $\left(V_v\right)$.

   (B) Substitute this statement (where possible) in all the equations of the system as well as in the statements $\left(V_{v-1}\right)$, $\left(H_h\right)$, for all v and h.

   (C) Remove the equation i_0 from the system.

   (D) Consider $v := v + 1$.

5. Does at least one equation exist in the system?
   (A) If it does not, write the general integer solution of the system substituting $k_1, k_2, \ldots$ for all the variables from the right term of each expression representing the value of the initial unknowns of the system.
   (B) If it does, considering the new data, go back to step 2.
6. Write all $a_{i_0 j}$, $j \neq j_0$ and b_{i_0} under the form :

$$a_{i_0 j} = a_{i_0 j_0} q_{i_0 j} + r_{i_0 j}, \text{ with } \left|r_{i_0 j}\right| < \left|a_{i_0 j}\right|.$$

$$b_{i_0 j} = a_{i_0 j_0} q_{i_0} + r_{i_0}, \text{ with } \left|r_{i_0}\right| < \left|a_{i_0 j_0}\right|.$$

7. Write $x_{j_0} = -\sum_{j \neq j_0} q_{i_0 j} x_j + q_{i_0} + t_h$, statement (H_h).
   Substitute (where possible) this statement in all the equations of the system as well as in the statement (V_v), (H_h), for all v and h.
8. Consider

$$x_{j_0} := t_h,\ h := h+1,$$
$$a_{i_0 j} := r_{i_0 j},\ j \neq j_0,$$
$$a_{i_0 j_0} := \pm a_{i_0 j_0},\ b_{i_0} := +r_{i_0},$$

   and go back to step 2

The correctness of Algorithm 4

This algorithm extends the algorithm from [4] (integer solutions of equations to integer solutions of linear systems). The algorithm was thoroughly proved in our previous article; the present one introduces a new cycle – having as cycling variable the number of equations of system – the rest remaining unchanged, hence, the correctness of algorithm 4 is obvious.

Discussion

1. The counter variables h and v count the statements H and V, respectively, differentiating them (to enable the substitutions);
2. Step 2 ((A)+(B) + (C)) is trivial and is meant to simplify the calculations (as algorithm 2);
3. Sub-step 5 (A) has aesthetic function (as all the algorithms described). Everything else has been proved in the previous chapters (see [4], [5], and algorithm 2).

Example 4. Let us use algorithm 4 to calculate the integer solution of the following linear system:

$$\begin{cases} 3x_1 \qquad\quad - 7x_3 + 6x_4 \qquad\quad = -2 \\ 4x_1 + 3x_2 \qquad + 6x_4 - 5x_5 = 19 \end{cases}$$

Solution

1. $h = 1,\ v = 1$
2. –

3. $a = 3$ and $i = 1, j = 1$
4. $3 \neq 1$. Go on to step 6.

6. Then,

$$-7 = 3 \cdot (-3) + 2$$
$$6 = 3 \cdot 2 + 0$$
$$-2 = 3 \cdot 0 - 2$$

7. $x_1 = 3x_3 - 2x_4 + t_1$ statement (H_1). Substituting it in the second equation we obtain:

$$4t_1 + 3x_2 + 12x_3 - x_4 - 5x_5 = 19$$

8. $x_1 := t_1,\ h := 2,\ a_{12} := 0,\ a_{13} := +2,\ \ a_{14} := 0,\ \ a_{11} := +3,\ b := -2$.

Go back to step 2.

2. The equivalent system was written:

$$\begin{cases} 3t_1 \quad\quad + 3x_3 \quad\quad\quad = -2 \\ 4t_1 + 3x_2 + 12x_3 - x_4 - 5x_5 = 19 \end{cases}$$

3. $a = 1,\ i = 2,\ j = 4$
4. 1=1
   (A) Then: $x_4 = 4t_1 + 3x_2 + 12x_3 - 5x_5 - 19$ statement (V_1).
   (B) Substituting it in (H_1), we obtain:
   $x_1 = -7t_1 - 6\,x_2 - 21x_3 + 10x_5 + 38,\quad (H_1)$
   (C) Remove the second equation of the system.
   (D) Consider: $v := 2$.
5. Yes. Go back to step 2.

2. The equation $+3t_1\ + 2x_3 = -2$ is left.
3. $a = 2$ and $i = 1,\ j = 3$
4. $2 \neq 2$, go to step 6.

6.

$$+3 = +2 \cdot 2 - 1$$
$$-2 = +2(-1) + 0$$

7. $x_3 = -2t_1 + t_2 - 1$ statement (H_2).
   Substituting it in $(H_1)'$, (V_1), we obtain:

$$x_1 = 35t_1 - 6\,x_2 - 21t_2 + 10x_5 + 59 \quad (H_1)''$$
$$x_4 = -20t_1 + 3x_2 + 12t_2 - 5x_5 - 31 \quad (V_1)'$$

8. $x_3 := t_2,\ h := 3,\ a_{11} := -1,\ \ a_{13} := +2,\ b_1 := 0$, (the others being all = 0). Go back to step 2.

2. The equation $-5t_1 + 2t_2 = 0$ was obtained.
3. $a = 1$, and $i = 1,\ j = 1$
4. 1=1
   (A) Then $t_1 = 2t_2$ statement (V_2).
   (B) After substitution, we obtain:

$$x_1 = 49t_2 - 6x_2 + 10x_5 + 59 \qquad (H_1)''';$$
$$x_4 = -28t_2 + 3x_2 - 5x_5 - 31 \qquad (V_1)'';$$
$$x_3 = -3t_2 \qquad (H_2)';$$

(C) Remove the first equation from the system.

(D) $v := 3$

5. No. The general integer solution of the initial system is:

$$\begin{cases} x_1 = 49k_1 - 6k_2 + 10k_3 + 59 \\ x_2 = k_2 \\ x_3 = -3k_1 - 1 \\ x_4 = -28k_1 + 3k_2 - 5k_3 - 31 \\ x_5 = k_3 \end{cases}$$

where $(k_1,\ k_2, k_3) \in \mathbb{Z}^3$.

Stop.

Algorithm 5

Input

A linear system (1)

Output

We decide on the possibility of an integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. We solve the common system in $\mathbb{R}^n$, then it does not have solutions in $\mathbb{R}^n$, then it does not have solutions in $\mathbb{Z}^n$ either. Stop.
2. $f = 1,\ v = 1,\ h = 1$
3. Write the value of each main variable x_i under the form:

$$\left(E_{f,\,i}\right)_i : x_i = \sum_j q_{ij} x_j^{'} - q_i + \left(\sum_j r_{ij} x_j^{'} + r_i\right) / \Delta_i ,$$

with all $q_{ij},\ q_i,\ r_{ij},\ r_i,\ \Delta_i$ from $\mathbb{Z}$ such that all $|r_{ij}| < |\Delta_i|,\ \ |r_i| < |\Delta_i|,\ \ \Delta_i \neq$ (where all $x_j^{'} - S$ of the right term are integer variables: either from the secondary variables of the system or the new variables introduced with the algorithm). For all i, we write $r_{ij_f} \equiv \Delta_i$

4. $\left(E_{f,\,i}\right)_i : \sum_j r_{ij} x_j - r_{i,j_f} y_{f,i} + r_i = 0$ where $\left(y_{f,i}\right)$ are auxiliary integer variables.

   Remove all the equations $\left(F_{f,\,i}\right)$ which are identities.
5. Does at least one equation $\left(F_{f,\,i}\right)$ exist? If it does not, write the general integer solution of the system substituting $k_1,\ k_2,...$ for all the variables of the right number of each expression representing the value of the initial unknowns of the system. Stop.

6. (A) Divide each equation $(F_{f,\,i})$ by the largest co-divisor of the coefficients of their unknowns. If the quotient is an integer for at least one i_0 then the system does not have integer solutions. Stop.
   (B) Simplify – as previously ((A)) all the functions in the relations $(E_{f,\,i})_i$.
7. Calculate $a = \min_{i,j}\left\{|r_{ij}|,\ r_{ij} \neq 0\right\}$, and determine the indices i_0, j_0 for which this minimum is obtained.
8. If $a \neq 1$, go on to step 9.
   If $a = 1$, then:
   (A) Calculate the value of the variable x'_{j_0} from the equation $(F_{f,\,i})$ write (V_v) for this statement.
   (B) Substitute this statement (where possible) in the statement $(E_{f,\,i})$, (V_{v+1}), (H_h), for all i, v, and h.
   (C) Remove the equation $(E_{f,\,i})$.
   (D) Consider $v := v+1$, $f := f+1$ and go back to step 3.
9. Write all $r_{i_0 j}$, $j \neq j_0$ and r_{i_0} under the form:

$$r_{i_0 j} = \Delta_{i_0} \cdot q_{i_0 j} + r'_{i_0 j}, \text{ with } |r'_{i_0 j}| < |\Delta_i|;$$

$$r_{i_0 j} = \Delta_{i_0} \cdot q_{i_0} + r'_{i_0}, \text{ with } |r'_{i_0}| < |\Delta_i|.$$

10. (A) Write $x'_{j_0} = -\sum_{j \neq j_0} q_{i_0 j} x'_j + q_{i_0} + t_h$ statement (H_h).
    (B) Substitute this statement (where possible) in all the statements $(E_{f,\,i})$, $(F_{f,\,i})$, (V_v), (H_{h-1}).
    (C) Consider $h := h+1$ and go back to step 4.

The correctness of the algorithm is obvious. It consists of the first part of algorithm 3 and the end part of algorithm 4. Then, steps 1-6 and their correctness were discussed in the case of algorithm 3. The situation is similar with steps 7-10. (After calculating the real solution in order to calculate the integer solution, we resorted to the procedure from 5 and algorithm 5 was obtained). This means that all these insertions were proven previously.

Example 5

Using algorithm 5, let us obtain the general integer solution of the system:

$$\begin{cases} 3x_1 \qquad + 6x_3 + 2x_4 \qquad = 0 \\ \qquad 4x_2 - 2x_3 \qquad - 7x_5 = -1 \end{cases}$$

Solution

1. Solving in $\mathbb{R}^5$ we obtain:

$$\begin{cases} x_1 = \dfrac{-6x_3 - 2x_4}{3} \\ x_2 = \dfrac{-2x_3 + 7x_5 - 1}{4} \end{cases}$$

2. $f = 1,\ v = 1,\ h = 1$

3. $(E_{1,1}): x_1 = 2x_3 + \dfrac{-2x_4}{3}$

$(E_{1,2}): x_2 = \quad x_5 + \dfrac{2x_3 + 3x_5 - 1}{4}$

4. $(F_{1,1}): -2x_4 - 3y_{11} = 0$

$(F_{1,2}): 2x_3 + 3x_5 - 4y_{12} - 1 = 0$

5. Yes

6. –

7. $i = 2$ and $i_0 = 2,\ j_0 = 3$

8. $2 \neq 1$

9. $3 = 2 \cdot 1 + 1$

$-4 = 2 \cdot (-2)$

$-1 = 2 \cdot 0 - 1$

10. $x_3 = -x_5 + 2y_{12} + t_1$ statement (H_1). After substitution:

$$(E_{1,1})': x_1 = 2x_5 - 4y_{12} - 2t_1 + \frac{-2x_4}{3}$$

$$(E_{1,2})': x_2 = x_5 \qquad + \frac{x_5 + 4y_{12} + 2t_1 - 1}{4}$$

$$(F_{1,2})': x_5 + 2t_1 - 1 = 0$$

Consider $h := 2$ and go back to step 4.

4. $(F_{1,1})': -2x_4 - 3y_{11} = 0$

$(F_{1,2})': 2t_1 + x_5 - 1 = 0$

5. Yes.

6. –

7. $a = 1$ and $i_0 = 2$, $j_0 = 5$

(A) $x_5 = -2t_1 + 1$ statement (V_1)

(B) Substituting it, we obtain:

$$(E_{1,1})'': \ x_1 = -6t_1 + 2 - 4y_{12} + \frac{-2x_4}{3}$$

$$(E_{1,2})'': \ x_2 = -2t_1 + 1 + \ y_{12}$$

$$(H_1)': \ x_3 = 3t_1 + 1 - 1 + 2y_{12}$$

(C) Remove the equation $(F_{1,2})$.

(D) Consider $v = 2,\ f = 2$ and go back to step 3.

3. $\left(E_{2,1}\right)$: $x_1 = -6t_1 - 4y_{12} + 2 + \dfrac{-2x_4}{3}$

$\left(E_{2,2}\right)$: $x_2 = -2t_1 + y_{12} + 1$

4. $\left(F_{2,1}\right)$: $-2x_4 - 3y_{12} = 0$

   5. Yes.
   6. –
   7. $a = 2$ and $i_0 = 1,\ j_0 = 4$
   8. $2 \neq 1$
   9. $-3 = -2 \cdot (1) - 1$
   10. (A) $x_4 = -y_{21} + t_2$ statement $\left(H_2\right)$

       (B) After substitution, we obtain:

       $\left(E_{2,1}\right)'$: $x_1 = -6t_1 - 4y_{12} + 2 + \dfrac{-2y_{21} - 2t_2}{3}$

       $\left(F_{2,1}\right)'$: $-y_{21} - 2t_2 = 0$

       Consider $h := 3,$ and go back to step 4.

4. $\left(F_{2,1}\right)'$: $-y_{21} - 2t_2 = 0$

   5. Yes
   6. –
   7. $a = 1$ and $i_0 = 1,\ j_0 = 21$ (two, one).

      (A) $y_{21} = -2t_2$ statement $\left(V_2\right)$.

      (B) After substitution, we obtain:

      (C) Remove the equation $\left(F_{2,1}\right)$.

      (D) Consider $v = 3,\ f = 3$ and go back to step 3.

3. $\left(E_{3,1}\right)$: $x_1 = -6t_1 - 4y_{12} - 2t_2 + 2$

$\left(E_{3,2}\right)$: $x_2 = -2t_1 + y_{12} \qquad + 1$

   4. –
   5. No. The general integer solution of the system is:

$$\begin{cases} x_1 = -6k_1 - 4k_2 - 2k_3 + 2\ , & \text{from } \left(E_{3,1}\right); \\ x_2 = -2k_1 + k_2 \qquad\qquad + 1, & \text{from } \left(E_{3,2}\right); \\ x_3 = 3k_1 + 2k_2 \qquad\qquad - 1, & \text{from } \left(H_1\right)'; \\ x_4 = \qquad\qquad 3k_3 \qquad\ \ , & \text{from } \left(H_2\right)'; \\ x_5 = -2k_1 \qquad\qquad\qquad + 1, & \text{from } \left(V_1\right); \end{cases}$$

where $\left(k_1,\ k_2, k_3\right) \in \mathbb{Z}$.

Stop.

Note 1. Algorithm 3, 4, and 5 can be applied in the calculation of the integer solution of a linear equation.

Note 2. The algorithms, because of their form, are easily adapted to a computer program.

Note 3. It is up to the reader to decide on which algorithm to use. Good luck!

REFERENCES

[1] Smarandache, Florentin – Rezolvarea ecuațiilor şi a sistemelor de ecuații liniare în numere întregi - diploma paper, University of Craiova, 1979.

[2] Smarandache, Florentin – Généralisations et généralités - Edition Nouvelle, Fès (Maroc), 1984.

[3] Smarandache, Florentin – Problems avec et sans .. problèmes! Somipress, Fès (Maroc), 1983.

[4] Smarandache, Florentin – General solution proprieties in whole numbers for linear equations – Bul. Univ. Braşov, Series C, Mathematics, vol. XXIV, pp. 37-39, 1982.

[5] Smarandache, Florentin – Baze de soluții pentru congruențe lineare – Bul. Univ. Braşov, Series C, Mathematics, vol. XXII, pp. 25-31, 1980, re-published in Buletinul Ştiinţific şi Tehnic al Institutului Politehnic "Traian Vuia", Timişoara, Series Mathematics-Physics, tome 26 (40) fascicle 2, pp. 13-16, 1981, reviewed in Mathematical Rev. (USA): 83e:10006.

[6] Smarandache, Florentin – O generalizare a teoremei lui Euler referitoare la congruențe – Bul. Univ. Braşov, series C, mathematics, vol. XXII, pp. 07-12, reviewed in Mathematical Reviews (USA): 84j:10006.

[7] Creangă, I., Cazacu, C., Mihuţ, P., Opaiţ, Gh., Corina Reischer – Introcucere în teoria numerelor - Editura Didactică şi Pedagogică, Bucharest, 1965.

[8] Cucurezeanu, Ion – Probleme de aritmetică şi teoria numerelor, Editura Tehnică, Buharest, 1976.

[9] Ghelfond, A. O. – Rezolvarea ecuațiilor în numere întregi - translation from Russian, Editura Tehnică, Bucharest, 1954.

[10] Golstein, E., Youndin, D. – Problemes particuliers de la programmation lineaire - Edition Mir, Moscou, Traduit de russe, 1973.

[11] Ion, D. Ion, Niță, C. – Elemente de aritmetică cu aplicații în tehnici de calcul, Editura Tehnică, Bucharest, 1978.

[12] Ion, D. Ion, Radu, K. – Algebra - Editura Didactică şi Pedagogică, Bucharest 1970.

[13] Mordell, L. – Two papers on number theory - Veb Deutscher Verlag der Wissenschafen, Berlin, 1972.

[14] Popovici, C. P. – Aritmetica şi teoria numerelor - Editura Didactică şi Pedagogică, Bucharest, 1963.

[15] Popovici, C. P. – Logica şi teoria numerelor - Editura Didactică şi Pedagogică, Bucharest, 1970.
[16] Popovici, C. P. – Teoria numerelor – lecture course, Editura Didactică şi Pedagogică, Bucharest, 1973.
[17] Rusu, E – Aritmetica si teoria numerelor - Editura Didactică şi Pedagogică, Bucharest, 1963.
[18] Rusu, E. – Bazele teoriei numerelor - Editura Tehincă, Bucharest, 1953.
[19] Sierpinski, W. – Ce ştim şi ce nu ştim despre numerele prime – Editura. Ştiințifică, Bucharest, 1966.
[20] Sierpinski, W. – 250 problemes de theorie elementaires des nombres - Classiques Hachette, Paris, 1972.

[Partialy published in "Bulet. Univ. Braşov", series C, Vol. XXIV, pp. 37-9, 1982, under the title: "General integer solution properties for linear equations".]

A METHOD TO GENERALIZE BY RECURRENCE OF SOME KNOWN RESULTS

A great number of articles widen known results, and this is due to a simple procedure, of which it is good to say a few words:

Let say that one generalizes a known mathematical proposition $P(a)$, where a is a constant, to the proposition $P(n)$, where n is a variable which belongs to subset of N. To prove that P is true for n by recurrence means the following: the first step is banal, since it is about the known result $P(a)$ (and thus it was already verified before by other mathematicians!). To pass from $P(n)$ to $P(n+1)$, one uses too $P(a)$: therefore one widens a proposition by using the proposition itself, in other words the found generalization will be paradoxically proved with the help of the particular case from which one started! (e. g. the generalizations of Hölder, Minkovski, Tchebychev, Euler).

A GENERALIZATION OF THE INEQUALITY OF HÖLDER

One generalizes the inequality of Hödler thanks to a reasoning by recurrence. As particular cases, one obtains a generalization of the inequality of Cauchy-Buniakovski-Scwartz, and some interesting applications.

Theorem: If $a_i^{(k)} \in \mathrm{R}_+$ and $p_k \in]1,+\infty[$, $i \in \{1,2,...,n\}$, $k \in \{1,2,...,m\}$, such that:, $\frac{1}{p_1}+\frac{1}{p_2}+...+\frac{1}{p_m}=1$, then:

$$\sum_{i=1}^{n}\prod_{k=1}^{m} a_i^{(k)} \le \prod_{k=1}^{m}\left(\sum_{i=1}^{n}\left(a_i^{(k)}\right)^{p_k}\right)^{\frac{1}{p_k}} \text{ with } m \ge 2.$$

Proof:

For $m=2$ one obtains exactly the inequality of Hödler, which is true. One supposes that the inequality is true for the values which are strictly smaller than a certain m .

Then:,

$$\sum_{i=1}^{n}\prod_{k=1}^{m} a_i^{(k)} = \sum_{i=1}^{n}\left(\left(\prod_{k=1}^{m-2} a_i^{k}\right)\cdot\left(a_i^{(m-1)}\cdot a_i^{(m)}\right)\right) \le \left(\prod_{k=1}^{m-2}\left(\sum_{i=1}^{n}\left(a_i^{(k)}\right)^{p_k}\right)^{\frac{1}{p_k}}\right)\cdot\left(\sum_{i=1}^{n}\left(a_i^{(m-1)}\cdot a_i^{(m)}\right)^{p}\right)^{\frac{1}{p}}$$

where $\frac{1}{p_1}+\frac{1}{p_2}+...+\frac{1}{p_{m-2}}+\frac{1}{p}=1$ and $p_h>1,\ 1\le h\le m-2$, $p>1$;

but

$$\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^{p}\cdot\left(a_i^{(m)}\right)^{p} \le \left(\sum_{i=1}^{n}\left(\left(a_i^{(m-1)}\right)^{p}\right)^{t_1}\right)^{\frac{1}{t_1}}\cdot\left(\sum_{i=1}^{n}\left(\left(a_i^{(m)}\right)^{p}\right)^{t_2}\right)^{\frac{1}{t_2}}$$

where $\frac{1}{t_1}+\frac{1}{t_2}=1$ and $t_1>1,\ \ t_2>2$.

From it results that:

$$\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^{p}\cdot\left(a_i^{(m)}\right)^{p} \le \left(\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^{pt_1}\right)^{\frac{1}{pt_1}}\cdot\left(\sum_{i=1}^{n}\left(a_i^{(m)}\right)^{pt_2}\right)^{\frac{1}{pt_2}}$$

with $\frac{1}{pt_1}+\frac{1}{pt_2}=\frac{1}{p}$.

Let us note $pt_1 = p_{m-1}$ and $pt_2 = p_m$. Then $\frac{1}{p_1} + \frac{1}{p_2} + ... + \frac{1}{p_m} = 1$ is true and one has $p_j > 1$ for $1 \le j \le m$ and it results the inequality from the theorem.

Note: If one poses $p_j = m$ for $1 \le j \le m$ and if one raises to the power m this inequality, one obtains a generalization of the inequality of Cauchy-Buniakovski-Scwartz:

$$\left(\sum_{i=1}^{n} \prod_{k=1}^{m} a_i^{(k)} \right)^m \le \prod_{k=1}^{m} \sum_{i=1}^{n} \left(a_i^{(k)} \right)^m .$$

Application:

Let $a_1, a_2, b_1, b_2, c_1, c_2$ be positive real numbers.

Show that:

$$(a_1 b_1 c_1 + a_2 b_2 c_2)^6 \le 8(a_1^6 + a_2^6)(b_1^6 + b_2^6)(c_1^6 + c_2^6)$$

Solution:

We will use the previous theorem. Let us choose $p_1 = 2$, $p_2 = 3$, $p_3 = 6$; we will obtain the following:

$$a_1 b_1 c_1 + a_2 b_2 c_2 \le (a_1^2 + a_2^2)^{\frac{1}{2}} (b_1^3 + b_2^3)^{\frac{1}{3}} (c_1^6 + c_2^6)^{\frac{1}{6}},$$

or more:

$$(a_1 b_1 c_1 + a_2 b_2 c_2)^6 \le (a_1^2 + a_2^2)^3 (b_1^3 + b_2^3)^2 (c_1^6 + c_2^6),$$

and knowing that

$$(b_1^3 + b_2^3)^2 \le 2(b_1^6 + b_2^6)$$

and that

$$(a_1^2 + a_2^2)^3 = a_1^6 + a_2^6 + 3(a_1^4 a_2^2 + a_1^2 a_2^4) \le 4(a_1^6 + a_2^6)$$

since

$$a_1^4 a_2^2 + a_1^2 a_2^4 \le a_1^6 + a_2^6 \quad \text{(because: } -\left(a_2^2 - a_1^2\right)^2 \left(a_1^2 + a_2^2\right) \le 0 \text{)}$$

it results the exercise which was proposed.

A GENERALIZATION OF THE INEQUALITY OF MINKOWSKI

Theorem : If p is a real number ≥ 1 and $a_i^{(k)} \in \mathbf{R}^+$ with $i \in \{1, 2, ..., n\}$ and $k \in \{1, 2, ..., m\}$, then:

$$\left(\sum_{i=1}^{n} \left(\sum_{k=1}^{m} a_i^{(k)} \right)^p \right)^{1/p} \leq \left(\sum_{k=1}^{m} \left(\sum_{i=1}^{n} a_i^{(k)} \right)^p \right)^{1/p}$$

Demonstration by recurrence on $m \in \mathbf{N}^*$.

First of all one shows that:

$\left(\sum_{i=1}^{n} \left(a_i^{(1)}\right)^p \right)^{1/p} \leq \left(\sum_{i=1}^{n} \left(a_i^{(1)}\right)^p \right)^{1/p}$, which is obvious, and proves that the inequality is true for $m = 1$.

(The case $m = 2$ precisely constitutes the inequality of Minkowski, which is naturally true!).

Let us suppose that the inequality is true for all the values less or equal to m

$$\left(\sum_{i=1}^{n} \left(\sum_{k=1}^{m+1} a_i^{(k)} \right)^p \right)^{1/p} \leq \left(\sum_{i=1}^{n} a_i^{(1)^p} \right)^{1/p} + \left(\sum_{i=1}^{n} \left(\sum_{k=2}^{m+1} a_i^{(k)} \right)^p \right)^{1/p} \leq$$

$$\leq \left(\sum_{i=1}^{n} \left(a_i^{(1)}\right)^p \right)^{1/p} + \left(\sum_{k=2}^{m+1} \left(\sum_{i=1}^{n} a_i^{(k)} \right)^p \right)^{1/p}$$

and this last sum is $\left(\sum_{k=1}^{m+1} \left(\sum_{i=1}^{n} a_i^{(k)} \right)^p \right)^{1/p}$ therefore the inequality is true for the level $m+1$.

A GENERALIZATION OF AN INEQUALITY OF TCHEBYCHEV

Statement: If $a_i^{(k)} \geq a_{i+1}^{(k)}$, $i \in \{1, 2, ..., n-1\}$, $k \in \{1, 2, ..., m\}$, then:

$$\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m}a_i^{(k)} \geq \frac{1}{n^m}\prod_{k=1}^{m}\sum_{i=1}^{n}a_i^{(k)} .$$

Demonstration by recurrence on m .

Case $m = 1$ is obvious: $\frac{1}{n}\sum_{i=1}^{n}a_i^{(1)} \geq \frac{1}{n}\sum_{i=1}^{n}a_i^{(1)}$.

In the case $m = 2$, this is the inequality of Tchebychev itself:

If $a_1^{(1)} \geq a_2^{(1)} \geq ... \geq a_n^{(1)}$ and $a_1^{(2)} \geq a_2^{(2)} \geq ... \geq a_n^{(2)}$, then:

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

One supposes that the inequality is true for all the values smaller or equal to m . It is necessary to prove for the rang $m+1$:

$$\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m+1}a_i^{(k)} = \frac{1}{n}\sum_{i=1}^{n}\left(\prod_{k=1}^{m}a_i^{(k)}\right)\cdot a_i^{(m+1)} .$$

This is $\geq \left(\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m}a_i^{(k)}\right)\cdot\left(\frac{1}{n}\sum_{i=1}^{n}a_i^{(m+1)}\right) \geq \left(\frac{1}{n^m}\prod_{k=1}^{m}\sum_{i=1}^{n}a_i^{(k)}\right)\cdot\left(\frac{1}{n}\sum_{i=1}^{n}a_i^{(m+1)}\right)$

and this is exactly $\frac{1}{n^{m+1}}\prod_{k=1}^{m+1}\sum_{i=1}^{n}a_i^{(k)}$ (Quod Erat Demonstrandum).

A GENERALIZATION OF EULER'S THEOREM

In the paragraphs which follow we will prove a result which replaces the theorem of Euler:

"If $(a,m)=1$, then $a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$",

for the case when a and m are not relative prime.

Introductory concepts.

One supposes that $m>0$. This assumption will not affect the generalization, because Euler's indicator satisfies the equality:

$\varphi(m)=\varphi(-m)$ (see [1]), and that the congruencies verify the following property:

$a \equiv b(\mathrm{mod}\, m) \Leftrightarrow a \equiv b\left(\mathrm{mod}\left(-m\right)\right)$ (see [1] pp 12-13).

In the case of congruence modulo 0, there is the relation of equality. One denotes (a,b) the greater common factor of the two integers a and b, and one chooses $(a,b)>0$.

B - Lemmas, theorem.

Lemma 1: Let be a an integer and m a natural number >0. There exist d_0, m_0 from **N** such that $a=a_0 d_0$, $m=m_0 d_0$ and $(a_0, m_0)=1$.

Proof:

It is sufficient to choose $d_0=(a,m)$. In accordance with the definition of the greatest common factor (GCF), the quotients of a_0 and m_0 and of a and m by their TGFC are relative prime (of [3] pp 25-26).

Lemma 2: With the notations of lemma 1, if $d_0 \neq 1$ and if:
$d_0 = d_0^1 d_1$, $m_0 = m_1 d_1$, $(d_0^1, m_1)=1$ and $d_1 \neq 1$, then $d_0 > d_1$ and $m_0 > m_1$, and if $d_0 = d_1$, then after a limited number of steps i one has $d_0 > d_{i+1} = (d_i, m_i)$.

Proof:

$$(0)\begin{cases} a = a_0 d_0 \quad ; \quad (a_0, m_0)=1 \\ m = m_0 d_0 \quad ; \quad d_0 \neq 1 \end{cases}$$

$$(1)\begin{cases} d_0 = d_0^1 d_1 \quad ; \quad (d_0^1, m_1)=1 \\ m_0 = m_1 d_1 \quad ; \quad d_1 \neq 1 \end{cases}$$

From (0) and from (1) it results that $a = a_0 d_0 = a_0 d_0^1 d_1$ therefore $d_0 = d_0^1 d_1$ thus $d_0 > d_1$ if $d_0^1 \neq 1$.

From $m_0 = m_1 d_1$ we deduct that $m_0 > m_1$.

If $d_0 = d_1$ then $m_0 = m_1 d_0 = k \cdot d_0^z$ ($z \in \mathbf{N}^*$ and $d_0 \nmid k$).

Therefore $m_1 = k \cdot d_0^{z-1}$; $d_2 = (d_1, m_1) = (d_0, k \cdot d_0^{z-1})$. After the $i = z$ step, it results $d_{i+1} = (d_0, k) < d_0$.

Lemma 3: For each integer a and for each natural number $m > 0$ one can build the following sequence of relations:

$$(0)\begin{cases} a = a_0 d_0 & ; \quad (a_0, m_0) = 1 \\ m = m_0 d_0 & ; \quad d_0 \neq 1 \end{cases}$$

$$(1)\begin{cases} d_0 = d_0^1 d_1 & ; \quad (d_0^1, m_1) = 1 \\ m_0 = m_1 d_1 & ; \quad d_1 \neq 1 \end{cases}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(s-1)\begin{cases} d_{s-2} = d_{s-2}^1 d_{s-1} & ; \quad (d_{s-2}^1, m_{s-1}) = 1 \\ m_{s-2} = m_{s-1} d_{s-1} & ; \quad d_{s-1} \neq 1 \end{cases}$$

$$(s)\begin{cases} d_{s-1} = d_{s-1}^1 d_s & ; \quad (d_{s-1}^1, m_s) = 1 \\ m_{s-1} = m_s d_s & ; \quad d_s \neq 1 \end{cases}$$

Proof:

One can build this sequence by applying lemma 1. The sequence is limited, according to lemma 2, because after r_1 steps, one has $d_0 > d_{r_1}$ and $m_0 > m_{r_1}$, and after r_2 steps, one has $d_{r_1} > d_{r_1 + r_2}$ and $m_{r_1} > m_{r_1 + r_2}$, etc., and the m_i are natural numbers. One arrives at $d_s = 1$ because if $d_s \neq 1$ one will construct again a limited number of relations $(s+1), \ldots, (s+r)$ with $d_{s+r} < d_s$.

Theorem: Let us have $a, m \in \mathbf{Z}$ and $m \neq 0$. Then $a^{\varphi(m_s)+s} \equiv a^s \pmod{m}$ where s and m_s are the same ones as in the lemmas above.

Proof:

Similar with the method followed previously, one can suppose $m > 0$ without reducing the generality. From the sequence of relations from lemma 3, it results that:

(0) (1) (2) (3) (s)

$$a = a_0 d_0 = a_0 d_0^1 d_1 = a_0 d_0^1 d_1^1 d_2 = \ldots = a_0 d_0^1 d_1^1 \ldots d_{s-1}^1 d_s$$

and

(0) (1) (2) (3) (s)

$$m = m_0 d_0 = m_1 d_1 d_0 = m_2 d_2 d_1 d_0 = \ldots = m_s d_s d_{s-1} \ldots d_1 d_0$$

and

$$m_s d_s d_{s-1} \ldots d_1 d_0 = d_0 d_1 \ldots d_{s-1} d_s m_s.$$

From (0) it results that $d_0 = (a, m)$, and of (i) that $d_i = (d_{i-1}, m_{i-1})$, for all i from $\{1, 2, ..., s\}$.

$d_0 = d_0^1 d_1^1 d_2^1 ....d_{s-1}^1 d_s$

$d_1 = d_1^1 d_2^1 ....d_{s-1}^1 d_s$

……………………

$d_{s-1} = \qquad d_{s-1}^1 d_s$

$d_s = \qquad d_s$

Therefore $d_0 d_1 d_2 ....d_{s-1} d_s = (d_0^1)^1 (d_1^1)^2 (d_2^1)^3 ...(d_{s-1}^1)^s (d_s^1)^{s+1} = (d_0^1)^1 (d_1^1)^2 (d_2^1)^3 ...(d_{s-1}^1)^s$ because $d_s = 1$.

Thus $m = (d_0^1)^1 (d_1^1)^2 (d_2^1)^3 ...(d_{s-1}^1)^s \cdot m_s$;

therefore $m_s \mid m$;

(s) (s)

$(d_s, m_s) = (1, m_s)$ and $(d_{s-1}^1, m_s) = 1$

(s-1)

$1 = (d_{s-2}^1, m_{s-1}) = (d_{s-2}^1, m_s d_s)$ therefore $(d_{s-2}^1, m_s) = 1$

(s-2)

$1 = (d_{s-3}^1, m_{s-2}) = (d_{s-3}^1, m_{s-1} d_{s-1}) = (d_{s-3}^1, m_s d_s d_{s-1})$ therefore $(d_{s-3}^1, m_s) = 1$

………..

(i+1)

$$1 = (d_i^1, m_{i+1}) = (d_i^1, m_{i+1} d_{i+2}) = (d_i^1, m_{i+3} d_{i+3} d_{i+2}) = ... =$$

$= (d_i^1, m_s d_s d_{s-1} ... d_{i+2})$ thus $(d_i^1, m_s) = 1$, and this is for all i from $\{0, 1, ..., s-2\}$.

………..

(0)

$1 = (a_0, m_0) = (a_0, d_1 ... d_{s-1} d_s m_s)$ thus $(a_0, m_s) = 1$.

From the Euler's theorem results that:

$(d_i^1)^{\varphi(m_s)} \equiv 1 (\mathrm{mod}\, m_s)$ for all i from $\{0, 1, ..., s\}$,

$a_0^{\varphi(m_s)} \equiv 1 (\mathrm{mod}\, m_s)$

but $a_0^{\varphi(m_s)} = a_0^{\varphi(m_s)} (d_0^1)^{\varphi(m_s)} (d_1^1)^{\varphi(m_s)} ...(d_{s-1}^1)^{\varphi(m_s)}$

therefore $a^{\varphi(m_s)} \equiv \underbrace{1........1}_{s+1 \ times} (\mathrm{mod}\, m_s)$

$a^{\varphi(m_s)} \equiv 1 (\mathrm{mod}\, m_s)$.

$a_0^s (d_0^1)^{s-1} (d_1^1)^{s-2} (d_2^1)^{s-3} ...(d_{s-2}^1)^1 \cdot a^{\varphi(m_s)} \equiv a_0^s (d_0^1)^{s-1} (d_1^1)^{s-2} ...(d_{s-2}^1)^1 \cdot 1 (\mathrm{mod}\, m_s)$.

Multiplying by:

$(d_0^1)^1 (d_1^1)^2 (d_2^1)^3 ...(d_{s-2}^1)^{s-1} (d_{s-1}^1)^s$ we obtain:

$a_0^s (d_0^1)^s (d_1^1)^s ...(d_{s-2}^1)^s (d_{s-1}^1)^s a^{\varphi(m_s)} \equiv$

$\equiv a_0^s (d_0^1)^s (d_1^1)^s ...(d_{s-2}^1)^s (d_{s-1}^1)^s (\mathrm{mod} (d_0^1)^1 ...(d_{s-1}^1)^s m_s)$

but $a_0^s(d_0^1)^s(d_1^1)^s...(d_{s-1}^1)^s \cdot a^{\varphi(m_s)} = a^{\varphi(m_s)+s}$ and $a_0^s(d_0^1)^s(d_1^1)^s...(d_{s-1}^1)^s = a^s$ therefore $a^{\varphi(m_s)+s} \equiv a^s (\mathrm{mod}\, m)$, for all a, m from $\mathbf{Z}\,(\mathrm{m} \neq 0)$.

Observations:

If $(a,m)=1$ then $d=1$. Thus $s=0$, and according to the theorem one has $a^{\varphi(m_0)+0} \equiv a^0 (\mathrm{mod}\, m)$ therefore $a^{\varphi(m_0)+0} \equiv 1(\mathrm{mod}\, m)$.
But $m = m_0 d_0 = m_0 \cdot 1 = m_0$. Thus:
$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$, and one obtains Euler's theorem.
Let us have a and m two integers, $m \neq 0$ and $(a,m) = d_0 \neq 1$, and $m = m_0 d_0$. If $(d_0, m_0) = 1$, then $a^{\varphi(m_0)+1} \equiv a(\mathrm{mod}\, m)$.
Which, in fact, it results from the theorem with $s=1$ and $m_1 = m_0$.
This relation has a similar form to Fermat's theorem:
$a^{\varphi(p)+1} \equiv a(\mathrm{mod}\, p)$.

C – AN ALGORITHM TO SOLVE CONGRUENCIES

One will construct an algorithm and will show the logic diagram allowing to calculate s and m_s of the theorem.

Given as input: two integers a and m, $m \neq 0$.

It results as output: s and m_s such that

$a^{\varphi(m_s)+s} \equiv a^s (\mathrm{mod}\, m)$.

Method:

(1) $A := a$
$M := m$
$i := 0$
(2) Calculate $d = (A, M)$ and $M' = M / d$.
(3) If $d=1$ take $S=i$ and $m_s = M'$ stop.
If $d \neq 1$ take $A := d$, $M = M'$
$i := i+1$, and go to (2).

Remark: the accuracy of the algorithm results from lemma 3 end from the theorem.
See the flow chart on the following page.
In this flow chart, the SUBROUTINE LCD calculates $D = (A, M)$ and chooses $D > 0$.

Application: In the resolution of the exercises one uses the theorem and the algorithm to calculate s and m_s.

Example: $6^{25604} \equiv ?(\mathrm{mod}\, 105765)$

One cannot apply Fermat or Euler because (6,105765)=3$\neq 1$. One thus applies the algorithm to calculate s and m_s and then the previous theorem:
$d_0 = (6,105765) = 3$ $\quad m_0 = 105765 / 3 = 35255$

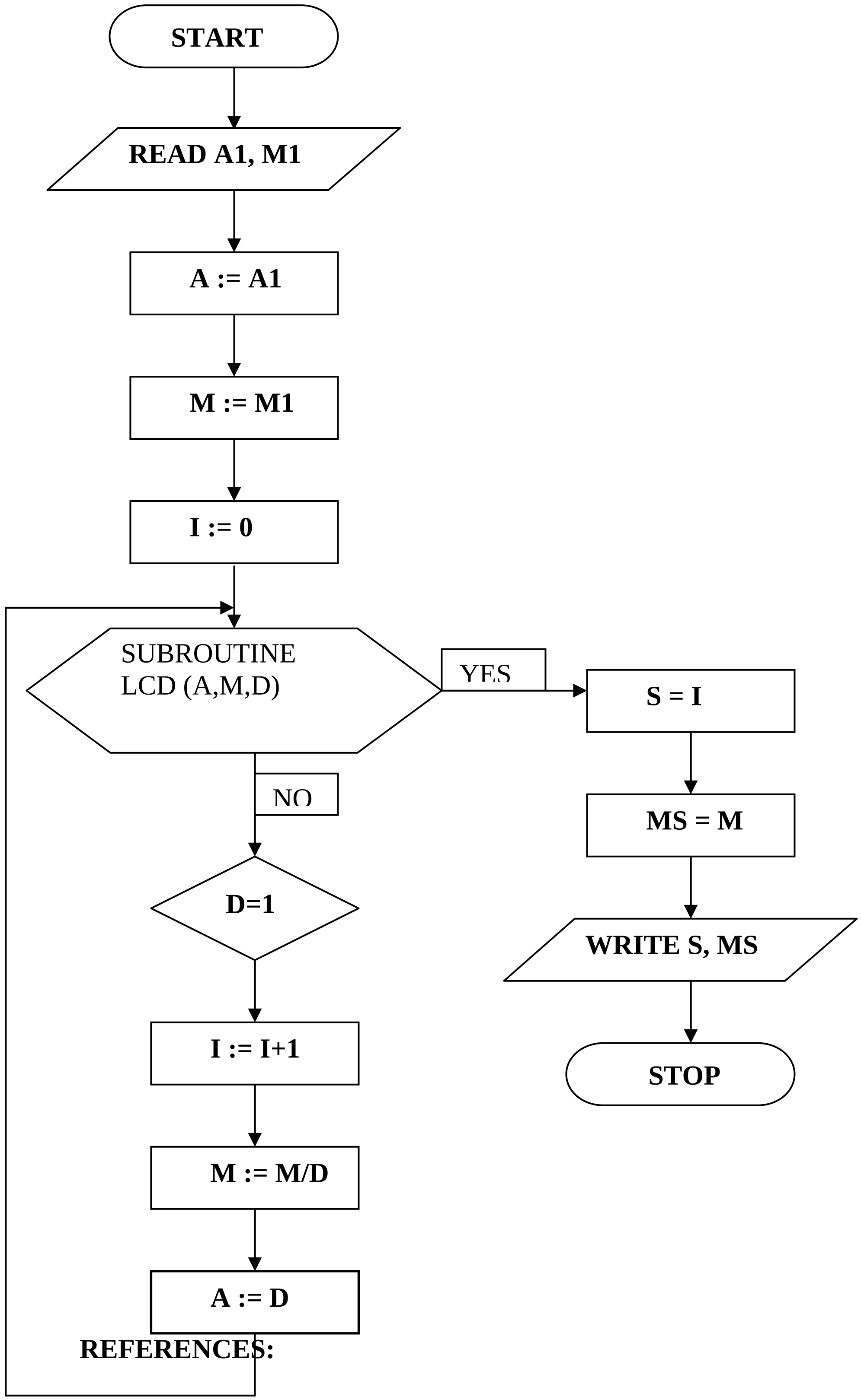
$i = 0; 3 \neq 1$ thus $i = 0 + 1 = 1$, $d_1 = (3, 35255) = 1$, $m_1 = 35255 / 1 = 35255$.
Therefore $6^{\varphi(35255)+1} \equiv 6^1 (\text{mod} 105765)$ thus $6^{25604} \equiv 6^4 (\text{mod} 105765)$.

*

*   *

*

Flow chart:



REFERENCES:

[1] Popovici, Constantin P. – “Teoria numerelor”, Curs, Bucharest, Editura didactic i pedagogic , 1973.
[2] Popovici, Constantin P – “Logica i teaoria numerelor”, Editura didactic i pedagogic , Bucharest, 1970.
[3] Creang I, Cazacu C, Mihu P, Opai Gh, Reischer Corina – “Introducere în teoria numerelor”, Editura didactic i pedagogic , Bucharest, 1965.
[4] Rusu E, - “Aritmetica i teoria numerelor”, Editura didactic i pedagogic , Editia a 2-a, Bucharest, 1963.

[Published in “Bulet. Univ. Bra ov”, seria C, Vol. XXIII, 1981, pp. 7-12; MR: 84j:10006.]

A GENERALIZATION OF THE INEQUALITY CAUCHY-BOUNIAKOVSKI-SCHWARZ

Statement: Let us consider the real numbers $a_i^{(k)}$, $i \in \{1, 2, ..., n\}$, $k \in \{1, 2, ..., m\}$, with $m \geq 2$. Then:

$$\left(\sum_{i=1}^{n} \prod_{k=1}^{m} a_i^{(k)}\right)^2 \leq \prod_{k=1}^{m} \sum_{i=1}^{n} \left(a_i^{(k)}\right)^2 .$$

Proof:

One notes A the left member of the inequality and B the right member. One has:

$$A = \sum_{i=1}^{n} \left(a_i^{(1)} ... a_i^{(m)}\right)^2 + 2\sum_{i=1}^{n-1} \sum_{k=i+1}^{n} \left(a_i^{(1)} ... a_i^{(m)}\right)\left(a_k^{(1)} ... a_k^{(m)}\right)$$

and

$$B = \sum_{(i_1, ..., i_m) \in E} \left(a_{i_1}^{(1)} ... a_{i_m}^{(m)}\right)^2 ,$$

where

$$E = \{(i_1, ..., i_m) / i_k \in \{1, 2, ..., n\}, 1 \leq k \leq m\}.$$

From where:

$$B = \sum_{i=1}^{n} \left(a_i^{(1)} ... a_i^{(m)}\right)^2 + \sum_{i=1}^{n-1} \sum_{k=i+1}^{n} \left[\left(a_i^{(1)} ... a_i^{(m-1)} a_k^{(m)}\right)^2 + \left(a_k^{(1)} ... a_k^{(m-1)} a_i^{(m)}\right)^2\right] +$$

$$+ \sum_{(i_1, ..., i_m) \in E - (\Delta_E \cup L^m)} \left(a_{i_1}^{(1)} ... a_{i_m}^{(m)}\right)^2$$

with

$$\Delta_E = \left\{ (\underbrace{\gamma, ..., \gamma}_{\text{m times}}) / \gamma \in \{1, 2, ..., n\} \right\}$$

and

$$L = \left\{ (\underbrace{\alpha, ..., \alpha}_{\text{m-1 times}}, \beta), (\underbrace{\beta, ..., \beta}_{\text{m-1 times}}, \alpha) / (\alpha, \beta) \in \{1, 2, ..., n\}^2 \text{ and } \alpha < \beta \right\}$$

Then

$$A - B = \sum_{i=1}^{n-1} \sum_{k=i+1}^{n} \left[-\left(a_i^{(1)} ... a_i^{(m-1)} a_k^{(m)}\right)^2 - \left(a_k^{(1)} ... a_k^{(m-1)} a_i^{(m)}\right)^2\right] -$$

$$- \sum_{(i_1, ..., i_m) \in E - (\Delta_E \cup L)} \left(a_{i_1}^{(1)} ... a_{i_m}^{(m)}\right)^2 \leq 0$$

Note: for $m = 2$ one obtains the inequality of Cauchy-Bouniakovski-Schwarz.

GENERALIZATIONS OF THE THEOREM OF CEVA

In these paragraphs one presents three generalizations of the famous theorem of Céva, which states:

"If in a triangle ABC one plots the convergent straight lines

AA_1, BB_1, CC_1 then $\dfrac{\overline{A_1B}}{\overline{A_1C}} \cdot \dfrac{\overline{B_1C}}{\overline{B_1A}} \cdot \dfrac{\overline{C_1A}}{\overline{C_1B}} = -1$".

Theorem: Let us have the polygon $A_1A_2...A_n$, a point M in its plane, and a circular permutation

$p = \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ 2 & 3 & ... & n & 1 \end{pmatrix}$. One notes M_{ij} the intersections of the line A_iM with the lines $A_{i+s}A_{i+s+1}, ..., A_{i+s+t-1}A_{i+s+t}$ (for all i and j, $j \in \{i+s, ..., i+s+t-1\}$).

If $M_{ij} \neq A_n$ for all the respective indices, and if $2s + t = n$, one has:

$\prod_{i,j=1,i+s}^{n,i+s+t-1} \dfrac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_p(j)}} = (-1)^n$ (s and t are natural non zero numbers).

Analytical demonstration: Let M be a point in the plain of the triangle ABC, such that it satisfies the conditions of the theorem. One chooses a Cartesian system of axes, such that the two parallels with the axes which pass through M do not pass by any point A_i (this is possible).

One considers $M(a,b)$, where a and b are real variables, and $A_i(X_i, Y_i)$ where X_i and Y_i are known, $i \in \{1, 2, ..., n\}$.

The former choices ensure us the following relations:

$X_i - a \neq 0$ and $Y_i - b \neq 0$ for all $i \in \{1, 2, ..., n\}$.

The equation of the line A_iM $(1 \leq i \leq n)$ is:

$\dfrac{x-a}{X_i - a} - \dfrac{y-b}{Y_i - b}$. One notes that $d(x, y; X_i, Y_i) = 0$.

One has

$$\frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p(j)}}} = \frac{\delta(A_j, A_iM)}{\delta(A_{p(j)}, A_iM)} = \frac{d(X_j, Y_j; X_i, Y_i)}{d(X_{p(j)}, Y_{p(j)}; X_i, Y_i)} = \frac{D(j,i)}{D(p(j), i)}$$

where $\delta(A, ST)$ is the distance from A to the line ST, and where one notes with $D(a,b)$ for $d(X_a, Y_a; X_b, Y_b)$.

Let us calculate the product, where we will use the following convention: $a + b$ will mean $\underbrace{p(p(...p}_{\text{b times}}(a)...))$, and $a - b$ will mean $\underbrace{p^{-1}(p^{-1}(...p^{-1}}_{\text{b times}}(a)...))$

$$\prod_{j=i+s}^{i+s+t-1} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{j+1}}} = \prod_{j=i+s}^{i+s+t-1} \frac{D(j,i)}{D(j+1,i)} =$$

$$=\frac{D(i+s,i)}{D(i+s+1,i)}\cdot\frac{D(i+s+1,i)}{D(i+s+2,i)}\cdots\frac{D(i+s+t-1,i)}{D(i+s+t,i)}=$$

$$=\frac{D(i+s,i)}{D(i+s+t,i)}=\frac{D(i+s,i)}{D(i-s,i)}$$

The initial product is equal to:

$$\prod_{i=1}^{n}\frac{D(i+s,i)}{D(i-s,i)}=\frac{D(1+s,1)}{D(1-s,1)}\cdot\frac{D(2+s,2)}{D(2-s,2)}\cdots\frac{D(2s,s)}{D(n,s)}\cdot$$

$$\cdot\frac{D(2s+2,s+2)}{D(2,s+2)}\cdots\frac{D(2s+t,s+t)}{D(t,s+t)}\cdot\frac{D(2s+t+1,s+t+1)}{D(t+1,s+t+1)}\cdot$$

$$\cdot\frac{D(2s+t+2,s+t+2)}{D(t+2,s+t+2)}\cdots\frac{D(2s+t+s,s+t+s)}{D(t+s,s+t+s)}=$$

$$=\frac{D(1+s,1)}{D(1,1+s)}\cdot\frac{D(2+s,2)}{D(2,2+s)}\cdots\frac{D(2s+t,s+t)}{D(s+t,2s+t)}\cdots\frac{D(s,n)}{D(n,s)}=$$

$$=\prod_{i=1}^{n}\frac{D(i+s,i)}{D(i,i+s)}=\prod_{i=1}^{n}\left(-\frac{P(i+s)}{P(i)}\right)=(-1)^{n}$$

because:

$$\frac{D(r,p)}{D(p,r)}=\frac{\dfrac{X_r-a}{X_p-a}-\dfrac{Y_r-b}{Y_p-b}}{\dfrac{X_p-a}{X_r-a}-\dfrac{Y_p-b}{Y_r-b}}=-\frac{(X_r-a)(Y_r-b)}{(X_p-a)(Y_p-b)}=-\frac{P(r)}{P(p)},$$

The last equality resulting from what one notes: $(X_t-a)(Y_t-b)=P(t)$. From (1) it results that $P(t)\neq 0$ for all t from $\{1,2,...,n\}$. The proof is completed.

Comments regarding the theorem:

t represents the number of lines of a polygon which are intersected by a line $A_{i_0}M$; if one notes the sides A_iA_{i+1} of the polygon, by a_i, then $s+1$ represents the order of the first line intersected by the line A_1M (that is a_{s+1} the first line intersected by A_1M).

Example: If $s=5$ and $t=3$, the theorem says that :

- the line A_1M intersects the sides A_6A_7, A_7A_8, A_8A_9.
- the line A_2M intersects the sides $A_7A_8, A_8A_9, A_9A_{10}$.
- the line A_3M intersects the sides $A_8A_9, A_9A_{10}, A_{10}A_{11}$, etc.

Observation: The restrictive condition of the theorem is necessary for the existence of the ratios $\dfrac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p(j)}}}$.

Consequence 1: Let us have a polygon $A_1A_2...A_{2k+1}$ and a point M in its plan. For all i from $\{1,2,...,2k+1\}$, one notes M_i the intersection of the line $A_iA_{p(i)}$ with the line which passes through M and by the vertex which is opposed to this line. If $M_i \notin \{A_i, A_{p(i)}\}$ then one has: $\prod_{i=1}^{n} \dfrac{\overline{M_iA_i}}{\overline{M_iA_{p(i)}}} = -1$.

The demonstration results immediately from the theorem, since one has $s = k$ and $t = 1$, that is $n = 2k+1$.

The reciprocal of this consequence is not true.

From where it results immediately that the reciprocal of the theorem is not true either.

Counterexample:

Let us consider a polygon of 5 sides. One plottes the lines A_1M_3, A_2M_4 and A_3M_5 which intersect in M.

Let us have $K = \dfrac{\overline{M_3A_3}}{\overline{M_3A_4}} \cdot \dfrac{\overline{M_4A_4}}{\overline{M_4A_5}} \cdot \dfrac{\overline{M_5A_5}}{\overline{M_5A_1}}$

Then one plots the line A_4M_1 such that it does not pass through M and such that it forms the ratio:

(2) $\dfrac{\overline{M_1A_1}}{\overline{M_1A_2}} = 1/K$ or $2/K$. (One chooses one of these values, for which A_4M_1 does not pass through M).

At the end one traces A_5M_2 which forms the ratio $\dfrac{\overline{M_2A_2}}{\overline{M_2A_3}} = -1$ or $-\dfrac{1}{2}$ in function of (2). Therefore the product:

$$\prod_{i=1}^{5} \frac{\overline{M_iA_i}}{\overline{M_iA_{p(i)}}}$$ without which the respective lines are concurrent.

Consequence 2: Under the conditions of the theorem, if for all i and $j, j \notin \{i, p^{-1}(i)\}$, one notes $M_{ij} = A_iM \cap A_jA_{p(j)}$ and $M_{ij} \notin \{A_j, A_{p(j)}\}$ then one has:

$$\prod_{\substack{i,j=1 \\ j \notin \{i, p^{-1}(i)\}}}^{n} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p(j)}}} = (-1)^n .$$

In effect one has $s = 1$, $t = n-2$, and therefore $2s + t = n$.

Consequence 3: For $n = 3$, it comes $s = 1$ and $t = 1$, therefore one obtains (as a particular case) the theorem of Céva.

AN APPLICATION OF THE GENERALIZATION OF CEVA'S THEOREM

Theorem: Let us consider a polygon $A_1A_2...A_n$ inserted in a circle. Let s and t be two non zero natural numbers such that $2s+t=n$. By each vertex A_i passes a line d_i which intersects the lines $A_{i+s}A_{i+s+1},....,A_{i+s+t-1}A_{i+s+t}$ at the points $M_{i,i+s},...,M_{i+s+t-1}$ respectively and the circle at the point $M_i^{'}$. Then one has:

$$\prod_{i=1}^{n}\prod_{j=i+s}^{i+s+t-1}\frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{j+1}}}=\prod_{i=1}^{n}\frac{\overline{M_i^{'}A_{i+s}}}{\overline{M_i^{'}A_{i+s+t}}}.$$

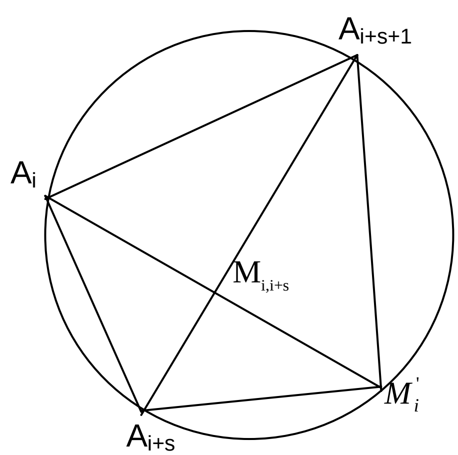
Proof:

Let i be fixed.

1) The case where the point $M_{i,i+s}$ is inside the circle.

There are the triangles $A_iM_{i,i+s}A_{i+s}$ and $M_i^{'}M_{i,i+s}A_{i+s+1}$ similar, since the angles $M_{i,i+s}A_iA_{i+s}$ and $M_{i,i+s}A_{i+s+1}M_i^{'}$ on one side, and $A_iM_{i,i+s}A_{i+s}$ and $A_{i+s+1}M_{i,i+s}M_i^{'}$ are equal. It results from it that:

(1) $$\frac{\overline{M_{i,i+s}A_i}}{\overline{M_{i,i+s}A_{i+s+1}}}=\frac{\overline{A_iA_{i+s}}}{\overline{M_i^{'}A_{i+s+1}}}$$

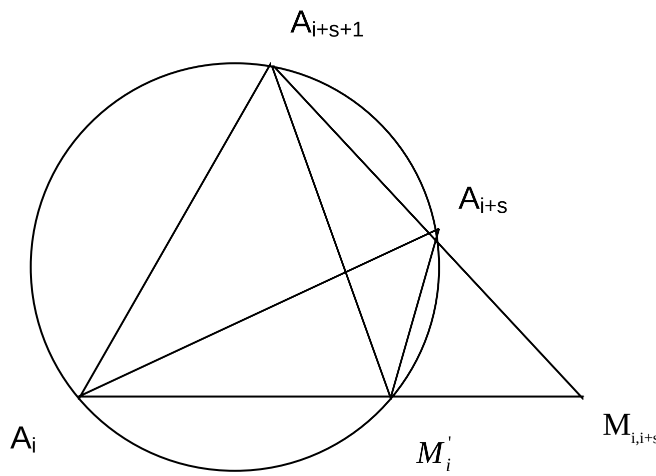


In a similar manner, one shows that the triangles $M_{i,i+s}A_iA_{i+s+1}$ and $M_{i,i+s}A_{i+s}M_i^{'}$ are similar, from which:

(2) $$\frac{\overline{M_{i,i+s}A_i}}{\overline{M_{i,i+s}A_{i+s}}}=\frac{\overline{A_iA_{i+s+1}}}{\overline{M_i^{'}A_{i+s}}}.$$ Dividing (1) by (2) we obtain:

(3) $$\frac{\overline{M_{i,i+s}A_{i+s}}}{\overline{M_{i,i+s}A_{i+s+1}}} = \frac{\overline{M'_iA_{i+s}}}{\overline{M'_iA_{i+s+1}}} \cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+1}}}.$$

2) The case where $M_{i,i+s}$ is exterior to the circle is similar to the first, because the triangles (notations as in 1) are similar also in this new case. There are the same interpretations and the same ratios; therefore one has also the relation (3).



Let us calculate the product:

$$\prod_{j=i+s}^{i+s+t-1} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{j+1}}} = \prod_{j=i+s}^{i+s+t-1} \left(\frac{\overline{M'_iA_j}}{\overline{M'_iA_{j+1}}} \cdot \frac{\overline{A_iA_j}}{\overline{A_iA_{j+1}}} \right) =$$

$$= \frac{\overline{M'_iA_{i+s}}}{\overline{M'_iA_{i+s+1}}} \cdot \frac{\overline{M'_iA_{i+s+1}}}{\overline{M'_iA_{i+s+2}}} \cdots \frac{\overline{M'_iA_{i+s+t-1}}}{\overline{M'_iA_{i+s+t}}} \cdot$$

$$\cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+1}}} \cdot \frac{\overline{A_iA_{i+s+1}}}{\overline{A_iA_{i+s+2}}} \cdots \frac{\overline{A_iA_{i+s+t-1}}}{\overline{A_iA_{i+s+t}}} = \frac{\overline{M'_iA_{i+s}}}{\overline{M'_iA_{i+s+t}}} \cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}}$$

Therefore the initial product is equal to:

$$\prod_{i=1}^{n} \left(\frac{\overline{M'_iA_{i+s}}}{\overline{M'_iA_{i+s+t}}} \cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}} \right) = \prod_{i=1}^{n} \frac{\overline{M'_iA_{i+s}}}{\overline{M'_iA_{i+s+t}}}$$

since:

$$\prod_{i=1}^{n} \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}} = \frac{\overline{A_1A_{1+s}}}{\overline{A_1A_{1+s+t}}} \cdot \frac{\overline{A_2A_{2+s}}}{\overline{A_2A_{2+s+t}}} \cdots \frac{\overline{A_sA_{2s}}}{\overline{A_{s+1}A_1}}.$$

$$\cdot\frac{\overline{A_{s+2}A_{2s+2}}}{\overline{A_{s+2}A_2}}\cdots\frac{\overline{A_{s+t}A_n}}{\overline{A_{s+t}A_t}}\cdot\frac{\overline{A_{s+t+1}A_1}}{\overline{A_{s+t+1}A_{t+1}}}\cdot\frac{\overline{A_{s+t+2}A_2}}{\overline{A_{s+t+2}A_{t+2}}}\cdots\frac{\overline{A_nA_s}}{\overline{A_nA_{s+t}}}=1$$

(by taking into account the fact that $2s+t=n$).

Consequence 1: If there is a polygon $A_1A_2,....,A_{2s-1}$ inscribed in a circle, and from each vertex A_i one traces a line d_i which intersects the opposite side $A_{i+s-1}A_{i+s}$ in M_i and the circle in $M_i^{'}$ then:

$$\prod_{i=1}^{n}\frac{\overline{M_iA_{i+s-1}}}{\overline{M_iA_{i+s}}}=\prod_{i=1}^{n}\frac{\overline{M_i^{'}A_{i+s-1}}}{\overline{M_i^{'}A_{i+s}}}$$

In fact for $t=1$, one has n odd and $s=\frac{n+1}{2}$.

If one makes $s=1$ in this consequence, one finds the mathematical note from [1], pages 35-37.

Application: If in the theorem, the lines d_i are concurrent, one obtains:

$\prod_{i=1}^{n}\frac{\overline{M_i^{'}A_{i+s}}}{\overline{M_i^{'}A_{i+s+t}}}=(-1)^n$ (For this, see [2]).

Bibliography:

[1] Dan Barbilian (Ion Barbu) – "Pagini inedite", Editura Albatros, Bucharest, 1981 (Ediție îngrijită de Gerda Barbilian, V. Protopopescu, Viorel Gh. Vodă).

[2] Florentin Smarandache – "Généralisation du théorème de Céva".

A GENERALIZATION OF A THEOREM OF CARNOT

Theorem of Carnot: Let M be a point on the diagonal AC of an arbitrary quadrilateral $ABCD$. Through M one draws a line which intersects AB in α and BC in β. Let us draw another line, which intersects CD in γ and AD in δ. Then one has:

$$\frac{A\alpha}{B\alpha}\cdot\frac{B\beta}{C\beta}\cdot\frac{C\gamma}{D\gamma}\cdot\frac{D\delta}{A\delta}=1.$$

Generalization: Let $A_1 \ldots A_n$ be a polygon. On a diagonal A_1A_k of this polygon one takes a point M through which one draws a line d_1 which intersects the lines $A_1A_2, A_2A_3, \ldots, A_{k-1}A_k$ respectively in the points $P_1, P_2, \ldots, P_{k-1}$ and another line d_2 intersects the other lines $A_kA_{k+1}, , \ldots, A_{n-1}A_n, A_nA_1$ respectively in the points $P_k, \ldots, P_{n-1}, P_n$. Then one has:

$$\prod_{i=1}^{n}\frac{A_iP_i}{A_{\varphi(i)}P_i}=1,$$

where φ is the circular permutation

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}.$$

Proof:

Let us have $1 \le j \le k-1$. One easily shows that:

$$\frac{A_jP_j}{A_{j+1}P_j}=\frac{D(A_j,d_1)}{D(A_{j+1},d_1)}$$

where $D(A,d)$ represents the distance from the point A to the line d, since the triangles $P_jA_jA_j^{'}$ and $P_jA_{j+1}A_{j+1}^{'}$ are similar. (One notes with $A_j^{'}$ and $A_{j+1}^{'}$ the projections of the points A_j and A_{j+1} on the line d_1).

It results from it that:

$$\frac{A_1P_1}{A_2P_1}\cdot\frac{A_2P_2}{A_3P_2}\cdots\frac{A_{k-1}P_{k-1}}{A_kP_{k-1}}=\frac{D(A_1,d_1)}{D(A_2,d_1)}\cdot\frac{D(A_2,d_1)}{D(A_3,d_1)}\cdots\frac{D(A_{k-1},d_1)}{D(A_k,d_1)}=\frac{D(A_1,d_1)}{D(A_k,d_1)}$$

In a similar way, for $k \le h \le n$ one has:

$$\frac{A_hP_h}{A_{\varphi(h)}P_h}=\frac{D(A_h,d_2)}{D(A_{\varphi(h)},d_2)}$$

and

$$\prod_{h=k}^{n}\frac{A_hP_h}{A_{\varphi(h)}P_h}=\frac{D(A_k,d_2)}{D(A_1,d_2)}$$

The product of the theorem is equal to:

$$\frac{D(A_1,d_1)}{D(A_k,d_1)}\cdot\frac{D(A_k,d_2)}{D(A_1,d_2)},$$

but

$$\frac{D(A_1,d_1)}{D(A_k,d_1)}=\frac{A_1M}{A_kM}$$

since the triangles $MA_1A_1^{'}$ and $MA_kA_k^{'}$ are similar. In the same way, because the triangles $MA_1A_1^{''}$ and $MA_kA_k^{''}$ are similar (one notes with $A_1^{''}$ and $A_k^{''}$ the respective projections of A_1 and A_k on the line d_2), one has:

$$\frac{D(A_k,d_2)}{D(A_1,d_2)}=\frac{A_kM}{A_1M}.$$

The product from the statement is therefore equal to 1.

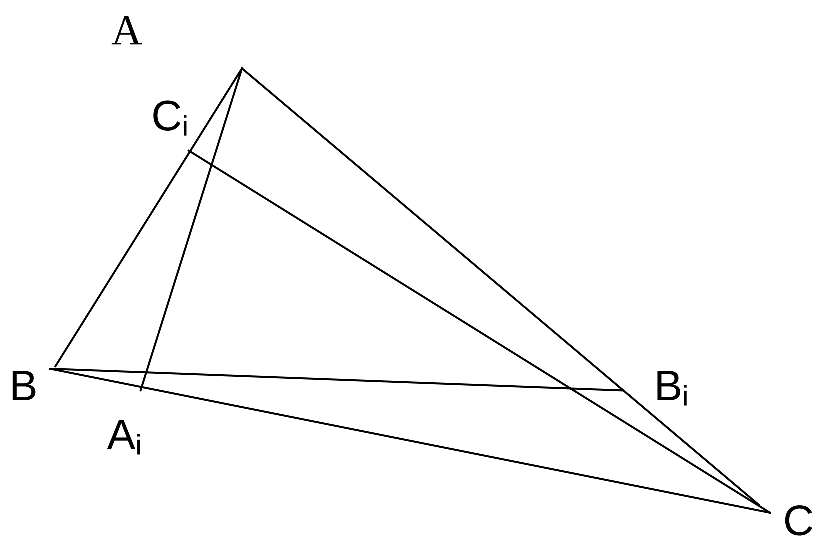
Remark: If one replaces n by 4 in this theorem, one finds the theorem of Carnot.

SOME PROPERTIES OF NEDIANES

This article generalizes certain results on the nedianes (see [1] pp. 97-99). One calls *nedianes* the segments of a line that passes through a vertex of a triangle and partitions the opposite side in n equal parts. A nediane is called to be of order i if it partitions the opposite side in the rapport i/n.

For $1 \le i \le n-1$ the nedianes of order i (that is AA_i, BB_i and CC_i) have the following properties:

1) With these 3 segments one can construct a triangle.



2) $|AA_i|^2 + |BB_i|^2 + |CC_i|^2 = \dfrac{i^2 - i\cdot n + n^2}{n^2}(a^2 + b^2 + c^2)$.

Proofs:

$$\overrightarrow{AA_i} = \overrightarrow{AB} + \overrightarrow{BA_i} = \overrightarrow{AB} + \frac{i}{n}\overrightarrow{BC} \qquad (1)$$

$$\overrightarrow{BB_i} = \overrightarrow{BC} + \overrightarrow{CB_i} = \overrightarrow{BC} + \frac{i}{n}\overrightarrow{CA} \qquad (2)$$

$$\overrightarrow{CC_i} = \overrightarrow{CA} + \overrightarrow{AC_i} = \overrightarrow{CA} + \frac{i}{n}\overrightarrow{AB} \qquad (3)$$

By adding these 3 relations, we obtain:

$$\overrightarrow{AA_i} + \overrightarrow{BB_i} + \overrightarrow{CC_i} = \frac{i+n}{n}(\overrightarrow{AB} + \overrightarrow{BC} + \overrightarrow{CA}) = 0$$

therefore the 3 nedianes can be the sides of a triangle.

(2) By raising to the square the relations and then adding them we obtain:

$$|AA_i|^2 + |BB_i|^2 + |CC_i|^2 = a^2 + b^2 + c^2 + \frac{i^2}{n^2}(a^2 + b^2 + c^2) +$$

$$+ \frac{i}{n}(2\overrightarrow{AB}\cdot\overrightarrow{BC} + 2\overrightarrow{BC}\cdot\overrightarrow{CA} + 2\overrightarrow{CA}\cdot\overrightarrow{AB}) \qquad (4)$$

Because $2\overrightarrow{AB} \cdot \overrightarrow{BC} = -2ca \cdot \cos B = b^2 - c^2 - a^2$ (the theorem of cosines), by substituting this in the relation (4), we obtain the requested relation.

REFERENCE:

[1] Vodă, Dr. Viorel Gh. – "Surprize în matematica elementară", Editura Albatros, Bucharest, 1981.

GENERALIZATIONS OF DEGARGUES THEOREM*

Let's consider the points $A_1,...,A_n$ situated on the same plane, and $B_1,...,B_n$ situated on another plane, such that the lines A_iB_i are concurrent. Let's prove that if the lines A_iA_j and B_iB_j are concurrent, then their intersecting points are collinear.

Solution. Let α be the plane that contains the points $A_1,...,A_n$ (in the case in which the points are non-collinear α is unique), and analogously, let $\beta = P(B_1,...,B_n)$, and consider $\alpha \cap \beta = d$.

Because the lines A_iA_j and B_iB_j are concurrent, $A_iA_j \subset \alpha$, and $B_iB_j \subset \beta$, therefore their intersection belongs to line d.

Remark 1.

For $n = 3$ and A_1, A_2, A_3 non-collinear, B_1, B_2, B_3 non-collinear, and $A_i \neq B_j$ we obtain Desargues theorem.

Remark 2.

An extension of this generalization is: If we consider $A_1,...,A_n$ situated in a plane, and $B_1,...,B_m$ situated on another plane, prove that if A_iA_j and B_kB_r are concurrent, then their intersection points are concurrent.

Remark 3.

For $n = m$, and A_iB_i concurrent lines, we obtain the first generalization.

Remark 4.

If in addition we also have $n = m = 3$ along with the previous conditions, we obtain the Desargues theorem.

* Gamma, Anul X, nr. 1-2, Oct. 1987.

K-NOMIAL COEFFICIENTS

In this article we will widen the concepts of" binomial coefficients" and" trinomial coefficients" to the concept of "k-nomial coefficients", and one obtains some general properties of these. As an application, we will generalize the" triangle of Pascal".

Let's consider a natural number $k \geq 2$; let $P(x) = 1 + x + x^2 + ... + x^{k-1}$ be the polynomial formed of k monomials of this type; we'll call it "k-nomial".

We will call *k-nomial coefficients* the coefficients of the power of x of $(1 + x + x^2 + ... + x^{k-1})^n$, for n positive integer. We will note them Ck_n^h with $h \in \{0,1,2,...,2pn\}$.

In continuation one will build by recurrence a triangle of numbers which will be called " *triangle of the numbers of order k*".

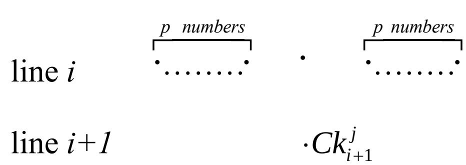
CASE 1: $k = 2p + 1$.

On the first line of the triangle one writes 1 and one calls it "line 0".

(1) It is agreed that all the cases which are to the left and to the right of the first (respectively of the last) number of each line will be consider like being 0. The lines which follow are called "line 1", "line 2", etc… Each line will contain $2p$ numbers to the left of the first number, p numbers on the right of the last number of the preceding line. Numbers of the line $i + 1$ are obtained by using those of the line i in the following way:

Ck_{i+1}^j is equal to the addition of p numbers which are to its left on the line i and of p numbers which are to the right on the line i, to the number which is above it (see. Fig. 1). One will take into account the convention 1.

Fig. 1



Example for $k = 5$:

								1								
						1	1	1	1	1						
				1	2	3	4	5	4	3	2	1				
		1	3	6	10	15	18	19	18	15	10	6	3	1		
1	4	10	20	35	52	68	80	85	80	68	52	35	20	10	4	1

……………………………………………………………………………………

The number

$$C5_1^0 = 0+0+0+0+1 = 1;$$
$$C5_1^3 = 0+1+0+0+0 = 1;$$
$$C5_2^3 = 0+1+1+1+1 = 4;$$
$$C5_3^7 = 4+5+4+3+2 = 18;$$

etc.

Properties of the triangle of numbers of order k:

1) The line i has $2pi+1$ elements.
2) $Ck_n^h = \sum_{i=0}^{2p} Ck_{n-1}^{h-i}$ where by convention $Ck_n^t = 0$ for $\begin{cases} t<0 \\ t>2pr \end{cases}$ and

   This is obvious taking into account the construction of the triangle.
3) Each line is symmetrical relative to the central element.
4) First elements of the line i are 1 and i.
5) The line i of the triangle of numbers of order k represent the k-nomial coefficients of $(1+x+x^2+\ldots+x^{k-1})^i$.

   The demonstration is done by recurrence on i of $\mathbb{N}^*$:

   a) For $i=1$ it is obvious; (in fact the property would be still true for $i=0$).

   b) Let's suppose the property true for n. Then

$$(1+x+x^2+\ldots+x^{k-1})^{n+1} = (1+x+x^2+\ldots+x^{k-1})(1+x+x^2+\ldots+x^{k-1})^n =$$

$$= (1+x+x^2+\ldots+x^{2p}) \cdot \sum_{j=0}^{2pn} Ck_n^j \cdot x^j =$$

$$= \sum_{t=0}^{2p(n+1)} \sum_{\substack{i+j=t \\ 0\le j\le 2p \\ 0\le i\le 2pn}} Ck_n^i \cdot x^i \cdot x^j =$$

$$= \sum_{t=0}^{2p(n+1)} \left(\sum_{j=0}^{2p} Ck_n^{t-j} \right) x^t = \sum_{t=0}^{2p(n+1)} Ck_{n+1}^t \cdot x^t .$$

6) The sum of the elements locate on line n is equal to k^n.

The first method of demonstration uses the reasoning by recurrence. For $n=1$ the assertion is obvious. One supposes the property truth for n, i.e. the sum of the elements located on the line n is equal to k^n. The line $n+1$ is calculated using the elements of the line n. Each element of the line n uses the sum which calculates each of p elements locate to its left on the line $n+1$, each of p elements locate to its right on the line $n+1$ and that which is located below: thus it is used to calculate k numbers of the line $n+1$.

Thus the sum of the elements of the line $n+1$ is k times larger than the sum of those of the line n, therefore it is equal to k^{n+1}.

7) The difference between the sum of the k-nomial coefficients of an even rank and the sum of the k-nomial coefficients of an odd rank located on the same line $\left(Ck_n^0 - Ck_n^1 + Ck_n^2 - Ck_n^3 + ...\right)$ is equal to 1.

One obtains it if in $(1+x+x^2+...+x^{k-1})^n$ one takes $x=-1$.

8) $Ck_n^0 \cdot Ck_m^h + Ck_n^1 \cdot Ck_m^{h-1} + ... + Ck_n^h \cdot Ck_m^0 = Ck_{n+m}^h$

This results from the fact that, in the identity

$$(1+x+x^2+...+x^{k-1})^n \cdot (1+x+x^2+...+x^{k-1})^m = (1+x+x^2+...+x^{k-1})^{n+m}$$

the coefficient of x^h in the member from the left is $\sum_{i=0}^{h} Ck_n^i \cdot Ck_m^{h-i}$ and that of x^h on the right is Ck_{n+m}^h.

9) The sum of the squares of the k-nomial coefficients locate on the line n is equal to the k-nomial coefficient located in the middle of the line $2n$.

For the proof one takes $n=m=h$ in the property 8. One can find many properties and applications of these k-nomial coefficients because they widen the binomial coefficients whose applications are known.

CASE 2: $k=2p$.

The construction of the triangle of numbers of order k is similar:

On the first line one writes 1; it is called line 0

The lines which follow are called line 1, line 2, etc. Each line will have $2p-1$ elements more than the preceding one; because $2p-1$ is an odd number, the elements of each line will be placed between the elements of the preceding line (which is different from the case 1 where they are placed below).

The elements locate on the line $i+1$ are obtained by using those of the line i in the following way:

Ck_{i+1}^j is equal to the sum of p elements located to its left on the line i with p elements located to its right on the line i.

Fig. 2

line i $\quad \overbrace{\cdot\ldots\ldots\cdot}^{p\ numbers} \quad \cdot \quad \overbrace{\cdot\ldots\ldots\cdot}^{p\ numbers}$

line $i+1$ $\quad \cdot Ck_{i+1}^{j}$

Example for $k = 4$:

$$
\begin{array}{c}
1 \\
1 \quad 1 \quad 1 \quad 1 \\
1 \quad 2 \quad 3 \quad 4 \quad 3 \quad 2 \quad 1 \\
1 \quad 3 \quad 6 \quad 10 \quad 12 \quad 12 \quad 10 \quad 6 \quad 3 \quad 1 \\
1 \quad 4 \quad 10 \quad 20 \quad 31 \quad 40 \quad 44 \quad 40 \quad 31 \quad 20 \quad 10 \quad 4 \quad 1 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{array}
$$

From the property 1': $Ck_n^h = \sum_{i=0}^{2p-1} Ck_{n-1}^{h-i}$

By joining together properties 1 and 1': $Ck_n^h = \sum_{i=0}^{k-1} Ck_{n-1}^{h-i}$

The other properties of Case 1 are preserved in Case 2, with similar profs. However in the property 7, one sees that the difference between the sum of the k-nomial coefficients of even rank and that of the k-nomial coefficients of odd rank locate on the same line is equal to 0.

A CLASS OF RECURSIVE SETS

In this article one builds a class of recursive sets, one establishes properties of these sets and one proposes applications. This article widens some results of [1].

1) Definitions, properties.

One calls recursive sets the sets of elements which are built in a recursive manner: let T be a set of elements and f_i for i between 1 and s, of operations n_i, such that $f_i : T^{n_i} \to T$. Let's build by recurrence the set M included in T and such that:

(Def. 1) 1^o) certain elements $a_1, ..., a_n$ of T, belong to M.

2^o) if $(\alpha_{i_1}, ..., \alpha_{i_{n_i}})$ belong to M, then $f_i(\alpha_{i_1}, ..., \alpha_{i_{n_i}})$ belong to M for all $i \in \{1, 2, ..., s\}$.

3^o) each element of M is obtained by applying a number finite of times the rules 1^o or 2^o.

We will prove several proprieties of these sets M, which will result from the manner in which they were defined. The set M is the representative of a class of recursive sets because in the rules 1^o and 2^o, by particularizing the elements $a_1, ..., a_n$ respectively $f_1, ..., f_s$ one obtains different sets.

Remark 1 : To obtain an element of M, it is necessary to apply initially the rule 1.

(Def. 2) The elements of M are called elements M-recursive.

(Def. 3) One calls order of an element a of M the smallest natural $p \geq 1$ which has the propriety that a is obtained by applying p times the rule 1^o or 2^o.

One notes M_p the set which contains all the elements of order p of M. It is obvious that $M_1 = \{a_1, ..., a_n\}$.

$$M_2 = \bigcup_{i=1}^{s} \left\{ \bigcup_{(\alpha_{i_1}, ..., \alpha_{i_{n_i}}) \in M_1^{n_i}} f_i(\alpha_{i_1}, ..., \alpha_{i_{n_i}}) \right\} \setminus M_1 .$$

One withdraws M_1 because it is possible that $f_j(a_{j_1}, ..., a_{j_{n_j}}) = a_i$ which belongs to M_1, and thus does not belong to M_2.

One proves that for $k \geq 1$ one has:

$$M_{k+1} = \bigcup_{i=1}^{s} \left\{ \bigcup_{(\alpha_{i_1}, ..., \alpha_{i_{n_i}}) \in \prod_k^{(i)}} f_i(\alpha_{i_1}, ..., \alpha_{i_{n_i}}) \right\} \setminus \bigcup_{h=1}^{k} M_h$$

where each

$\prod_k^{(i)} = \{(\alpha_{i_1}, ..., \alpha_{i_{n_i}}) / \alpha_{i_j} \in M_{q_j} \quad j \in \{1, 2, ..., n_i\};\ 1 \leq q_j \leq k$ and at least an element $a_{i_{j_o}} \in M_k, 1 \leq j_o \leq n_i \}$.

The sets M_p, $p \in \mathbb{N}^*$, form a partition of the set M.

Theorem 1:

$$M = \bigcup_{p \in \mathbb{N}^*} M_p \text{, where } \mathbb{N}^* = \{1, 2, 3, ...\}.$$

Proof:

From the rule 1^o it results that $M_1 \subseteq M$.

One supposes that this propriety is true for values which are less than p. It results that $M_p \subseteq M$, because M_p is obtained by applying the rule 2^o to the elements of $\bigcup_{i=1}^{p-1} M_i$.

Thus $\bigcup_{p \in \mathbb{N}^*} M_p \subseteq M$. Reciprocally, one has the inclusion in the contrary sense in accordance with the rule 3^o.

Theorem 2: The set M is the smallest set, which has the properties 1^o and 2^o.

Proof:

Let R be the smallest set having properties 1^o and 2^o. One will prove that this set is unique.

Let's suppose that there exists another set R' having properties 1^o and 2^o, which is the smallest. Because R is the smallest set having these proprieties, and because R' has these properties also, it results that $R \subseteq R'$; of an analogue manner, we have $R' \subseteq R$: therefore $R = R'$.

It is evident that $M' \subseteq R$. One supposes that $M_i \subseteq R$ for $1 \le i < p$. Then (rule 3^o), and taking in consideration the fact that each element of M_p is obtained by applying rule 2^o to certain elements of M_i, $1 \le i < p$, it results that $M_p \subseteq R$. Therefore $\bigcup_p M_p \subseteq R$ $(p \in \mathbb{N}^*)$, thus $M \subseteq R$. And because R is unique, $M = R$.

Remark 2. The theorem 2 replaces the rule 3^o of the recursive definition of the set M by: " M is the smallest set that satisfies proprieties 1^o and 2^o".

Theorem 3: M is the intersection of all the sets of T which satisfy conditions 1^o and 2^o.

Proof:

Let T_{12} be the family of all sets of T satisfying the conditions 1^o and 2^o. We note $I = \bigcap_{A \in T_{12}} A$.

I has the properties 1^o and 2^o because:

1) For all $i \in \{1, 2, ..., n\}$, $a_i \in I$, because $a_i \in A$ for all A of T_{12}.

2) If $\alpha_{i_1}, ..., \alpha_{i_{n_i}} \in I$, it results that $\alpha_{i_1}, ..., \alpha_{i_{n_i}}$ belong to A that is A of T_{12}. Therefore,

$\forall i \in \{1,2,...,s\}$, $f_i(\alpha_{i_1},...,\alpha_{i_{n_i}}) \in A$ which is A of T_{12}, therefore $f_i(\alpha_{i_1},...,\alpha_{i_{n_i}}) \in I$ for all i from $\{1,2,...,s\}$.

From theorem 2 it results that $M \subseteq I$.

Because M satisfies the conditions 1^o and 2^o, it results that $M \in T_{12}$, from which $I \subseteq M$. Therefore $M = I$

(Def. 4) A set $A \subseteq I$ is called closed for the operation f_{i_0} if and only if for all $\alpha_{i_0 1},...,\alpha_{i_0 n_{i_0}}$ of A, one has $f_{i_0}(\alpha_{i_0 1},...,\alpha_{i_0 n_{i_0}})$ belong to A.

(Def. 5) A set $A \subseteq T$ is called M-recursively closed if and only if:

1) $\{a_1,...,a_n\} \subseteq A$.

2) A is closed in respect to operations $f_1,..., f_s$.

With these definitions, the precedent theorems become:

Theorem 2': The set M is the smallest M - recursively closed set.

Theorem 3': M is the intersection of all M - recursively closed sets.

(Def. 6) The system of elements $\langle \alpha_1,...,\alpha_m \rangle$, $m \geq 1$ and $\alpha_i \in T$ for $i \in \{1,2,...,m\}$, constitute a M-recursive description for the element α, if $\alpha_m = \alpha$ and that each α_i ($i \in \{1,2,...,m\}$) satisfies at least one of the proprieties:

1) $\alpha_i \in \{a_1,...,a_n\}$.

2) α_i is obtained starting with the elements which precede it in the system by applying the functions f_j, $1 \leq j \leq s$ defined by property 2^o of (Def. 1).

(Def. 7) The number m of this system is called the length of the M-recursive description for the element α.

Remark 3: If the element α admits a M-recursive description, then it admits an infinity of such descriptions.

Indeed, if $\langle \alpha_1,...,\alpha_m \rangle$ is a M-recursive description of α then $\left\langle \underbrace{a_1,...,a_1}_{h \ times}, \alpha_1,...,\alpha_m \right\rangle$ is also a M-recursive description for α, h being able to take all values from $\mathbb{N}$.

Theorem 4: The set M is identical with the set of all elements of T which admit a M-recursive description.

Proof: Let D be the set of all elements, which admit a M-recursive description. We will prove by recurrence that $M_p \subseteq D$ for all p of $\mathbb{N}^*$.

For $p = 1$ we have: $M_1 = \{a_1,...,a_n\}$, and the a_j, $1 \leq j \leq n$, having as M-recursive description: $< a_j >$. Thus $M_1 \subseteq D$. Let's suppose that the property is true for the values smaller than p. M_p is obtained by applying the rule 2^o to the elements of

$\bigcup_{i=1}^{p-1} M_i$; $\alpha \in M_p$ implies that $\alpha \in f_j(\alpha_{i_1},...,\alpha_{i_{n_i}})$ and $\alpha_{i_j} \in M_{h_j}$ for $h_j < p$ and $1 \le j \le n_i$.
But a_{i_j}, $1 \le j \le n_i$, admits M-recursive descriptions according to the hypothesis of recurrence, let's have $\left\langle \beta_{j1},...,\beta_{js_j} \right\rangle$. Then $\left\langle \beta_{11},...,\beta_{1s_1},\beta_{21},...,\beta_{2s_2},...,\beta_{n_i1},...,\beta_{n_is_{n_i}},\alpha \right\rangle$ constitute a M-recursive description for the element α. Therefore if α belongs to D, then $M_p \subseteq D$ which is $M = \bigcup_{p \in \mathbb{N}^*} M_p \subseteq D$.

Reciprocally, let x belong to D. It admits a M-recursive description $\langle b_1,...,b_t \rangle$ with $b_t = x$. It results by recurrence by the length of the M-recursive description of the element x, that $x \in M$. For $t = 1$ we have $\langle b_1 \rangle$, $b_1 = x$ and $b_1 \in \{a_1,...,a_n\} \subseteq M$. One supposes that all elements y of D which admit a M-recursive description of a length inferior to t belong to M. Let $x \in D$ be described by a system of length t: $\langle b_1,...,b_t \rangle$, $b_t = x$. Then $x \in \{a_1,...,a_n\} \subseteq M$, where x is obtained by applying the rule 2° to the elements which precede it in the system: $b_1,...,b_{t-1}$. But these elements admit the M-recursive descriptions of length which is smaller that t: $\langle b_1 \rangle, \langle b_1, b_2 \rangle, ..., \langle b_1,...,b_{t-1} \rangle$. According to the hypothesis of the recurrence, $b_1,...,b_{t-1}$ belong to M. Therefore b_t belongs also to M. It results that $M \equiv D$.

Theorem 5: Let $b_1,...,b_q$ be elements of T, which are obtained from the elements $a_1,...,a_n$ by applying a finite number of times the operations [illegible]. Then M can be defined recursively in the following mode:

1) Certain elements $a_1,...,a_n,b_1,...,b_q$ of T belong to M.
2) M is closed for the applications f_i, with $i \in \{1,2,...,s\}$.
3) Each element of M is obtained by applying a finite number of times the rules (1) or (2) which precede.

Proof: evident. Because $b_1,...,b_q$ belong to T, and are obtained starting with the elements $a_1,...,a_n$ of M by applying a finite number of times the operations f_i, it results that $b_1,...,b_q$ belong to M.

Theorem 6: Let's have g_j, $1 \le j \le r$, of the operations n_j, where $g_j : T^{n_j} \to T$ such that M to be closed in rapport to these operations. Then M can be recursively defined in the following manner:

1) Certain elements $a_1,...,a_n$ de T belong to M.
2) M is closed for the operations f_i, $i \in \{1,2,...,s\}$ and g_j, $j \in \{1,2,...,r\}$.
3) Each element of M is obtained by applying a finite number of times the precedent rules.

Proof is simple: Because M is closed for the operations g_j (with $j \in \{1,2,...,r\}$), one has, that for any $\alpha_{j1},...,\alpha_{jn_j}$ from M, $g_j(\alpha_{j1},...,\alpha_{jn_j}) \in M$ for all $j \in \{1,2,...,r\}$.

From the theorems 5 and 6 it results:

Theorem 7: The set M can be recursively defined in the following manner:
1) Certain elements $a_1,...,a_n,b_1,...,b_q$ of T belong to M.
2) M is closed for the operations f_i ($i \in \{1,2,...,s\}$) and for the operations g_j ($j \in \{1,2,...,r\}$) previously defined.
3) Each element of M is defined by applying a finite number of times the previous 2 rules.
(Def. 8) The operation f_i conserves the property P iff for any elements $\alpha_{i1},...,\alpha_{in_i}$ having the property P, $f_i(\alpha_{i1},...,\alpha_{in_i})$ has the property P.

Theorem 8: If $a_1,...,a_n$ have the property P, and if the functions $f_1,...,f_s$ preserve this property, then all elements of M have the property P.

Poof:

$M = \bigcup_{p \in \mathbb{N}^*} M_p$. The elements of M_1 have the property P.

Let's suppose that the elements of M_i for $i < p$ have the property P. Then the elements of M_p also have this property because M_p is obtained by applying the operations $f_1, f_2,..., f_s$ to the elements of: $\bigcup_{i=1} M_i$, elements which have the property P. Therefore, for any p of $\mathbb{N}$, the elements of M_p have the property P.

Thus all elements of M have it.

Corollary 1: Let's have the property P: "x can be represented in the form $F(x)$".

If $a_1,...,a_n$ can be represented in the form $F(a_1),...,$ respectively $F(a_n)$, and if $f_1,...,f_s$ maintains the property P, then all elements α of M can be represented in the form $F(\alpha)$.

Remark. One can find more other equivalent def. of M.

2) APPLICATIONS, EXAMPLES.

In applications, certain general notions like: M - recursive element, M-recursive description, M - recursive closed set will be replaced by the attributes which characterize the set M. For example in the theory of recursive functions, one finds notions like: recursive primitive functions, primitive recursive description, primitively recursive closed sets. In this case " M " has been replaced by the attribute "primitive" which characterizes this class of functions, but it can be replaced by the attributes "general", "partial".

By particularizing the rules 1^o and 2^o of the def. 1, one obtains several interesting sets:

Example 1: (see [2], pp. 120-122, problem 7.97).

Example 2: The set of terms of a sequence defined by a recurring relation constitutes a recursive set.

Let's consider the sequence: $a_{n+k} = f(a_n, a_{n+1}, ..., a_{n+k-1})$ for all n of $\mathbb{N}^*$, with $a_i = a_i^0$, $1 \le i \le k$. One will recursively construct the set $A = \{a_m\}_{m \in \mathbb{N}^*}$ and one will define in the same time the position of an element in the set A:

1°) $a_1^0, ..., a_k^0$ belong to A, and each a_i^0 ($1 \le i \le k$) occupies the position i in the set A;

2°) if $a_n, a_{n+1}, ..., a_{n+k-1}$ belong to A, and each a_j for $n \le j \le n+k-1$ occupies the position j in the set A, then $f(a_n, a_{n+1}, ..., a_{n+k-1})$ belongs to A and occupies the position $n+k$ in the set A.

3°) each element of B is obtained by applying a finite number of times the rules 1° or 2°.

Example 3: Let $G = \{e, a^1, a^2, ..., a^p\}$ be a cyclic group generated by the element a. Then $(G, \bullet)$ can be recursively defined in the following manner:

1°) a belongs to G.

2°) if b and c belong to G then $b \bullet c$ belongs to G.

3°) each element of G is obtained by applying a finite number of times the rules 1 or 2.

Example 4: Each finite set $ML = \{x_1, x_2, ..., x_n\}$ can be recursively defined (with $ML \subseteq T$):

1°) The elements $x_1, x_2, ..., x_n$ of T belong to ML.

2°) If a belongs to ML, then $f(a)$ belongs to ML, where $f: T \to T$ such that $f(x) = x$;

3°) Each element of ML is obtained by applying a finite number of times the rules 1° or 2°.

Example 5: Let L be a vectorial space on the commutative corps K and $\{x_1, ..., x_m\}$ be a base of L. Then L, can be recursively defined in the following manner:

1°) $x_1, ..., x_m$ belong to L;

2°) if x, y belong to L and if a belongs to K, then $x \perp y$ y belong to L and $a * x$ belongs to L;

3°) each element of L is recursively obtained by applying a finite number of times the rules 1° or 2°.

(The operators $\perp$ and $*$ are respectively the internal and external operators of the vectorial space L).

Example 6: Let X be an A-module, and $M \subset X$ $(M \ne \varnothing)$, with $M = \{x_i\}_{i \in I}$. The sub-module generated by M is:

$$\langle M \rangle = \{x \in X / x = a_1 x_1 + ... + a_n x_n,\ \ a_i \in A,\ \ x_i \in M,\ \ i \in \{1, ..., n\}\}$$

can be recursively defined in the following way:

1°) for all i of $\{1, 2, ..., n\}$, $\{1, 2, ..., n\} \bullet x_i \in \langle M \rangle$;

2°) if x and y belong to $\langle M \rangle$ and a belongs to A, then $x + y$ belongs to $\langle M \rangle$, and ax also;

3°) each element of $\langle M \rangle$ is obtained by applying a finite number of times the rules 1° or 2°.

In accordance to the paragraph 1 of this article, $\langle M \rangle$ is the smallest sub-set of X that verifies the conditions 1° and 2°, that is $\langle M \rangle$ is the smallest sub-module of X that includes M. $\langle M \rangle$ is also the intersection of all the subsets of X that verify the conditions 1° and 2°, that is $\langle M \rangle$ is the intersection of all sub-modules of X that contain M. One also directly refines some classic results from algebra.

One can also talk about sub-groups or ideal generated by a set: one also obtains some important applications in algebra.

Example 7: One also obtains like an application the theory of formal languages, because, like it was mentioned, each regular language (linear at right) is a regular set and reciprocally. But a regular set on an alphabet $\Sigma = \{a_1, ..., a_n\}$ can be recursively defined in the following way:

1°) $\emptyset, \{\varepsilon\}, \{a_1\}, ..., \{a_n\}$ belong to R.

2°) if P and Q belong to R, then $P \cup Q$, PQ, and P^* belong to R, with $P \cup Q = \{x / x \in P \text{ or } x \in Q\}$; $PQ = \{xy / x \in P \text{ and } y \in Q\}$, and $P^* = \bigcup_{n=0}^{\infty} P^n$ with $P^n = \underbrace{P \cdot P \cdots P}_{n \text{ times}}$ and, by convention, $P^0 = \{\varepsilon\}$.

3°) Nothing else belongs to R other that those which are obtained by using 1° or 2°.

From which many properties of this class of languages with applications to the programming languages will result.

REFERENCES:

[1] C. P. Popovici, L. Livovschi, H. Georgescu. N. Ţăndăreanu, "Curs de bazele informaticii (funcții booleene şi circuite combinaționale)", Tipografia Universității din Bucureşti, 1976

[2] F. Smarandache, "Problèmes avec et sans…problèmes!", Somipress, Fès (Morocco), 1983.

A GENERALIZATION IN SPACE OF JUNG'S THEOREM

In this short note we will prove a generalization of Joung's theorem in space.

Theorem. Let us have n points in space such that the maximum distance between any two points is a. Prove that there exists a sphere of radius $r \le a\frac{\sqrt{6}}{4}$ that contains in its interior or on its surface all these points.

Proof:

Let $P_1, ..., P_n$. be the points. Let $S_1(O_1, r_1)$ be a sphere of center O_1 and radius r_1, which contains all these points. We note $r_2 = \max_{1 \le i \le n} P_i O_1 = P_1 O_1$ and construct the sphere $S_2(O_1, r_2)$, $r_2 \le r_1$, with $P_1 \in Fr(S_2)$, where $Fr(S_2) =$ frontier (surface) of S_2.

We apply a homothety H in space, of center P_1, such that the new sphere $H(S_2) = S_3(O_3, r_3)$ has the property: $Fr(S_3)$ contains another point, for example P_2, and of course S_3 contains all points P_i.

1) If P_1, P_2 are diametrically opposite in S_3 then $r_{\min} = \frac{a}{2}$.

If no, we do a rotation R so that $R(S_3) = S_4(O_4, r_4)$ for which $\{P_3, P_2, P_1\} \subset Fr(S_4)$ and S_4 contains all points P_i.

2) If $\{P_1, P_2, P_3\}$ belong to a great circle of S_4 and they are not included in an open semicircle, then $r_{\min} \le \frac{a}{\sqrt{3}}$ (Jung's theorem).

If no, we consider the fascicule of spheres S for which $\{P_1, P_2, P_3\} \subset Fr(S)$ and S contains all points P_i. We choose a sphere S_5 such that $\{P_1, P_2, P_3, P_4\} \subset Fr(S_5)$.

3) If $\{P_1, P_2, P_3, P_4\}$ are not included in an open semisphere of S_5, then the tetrahedron $\{P_1, P_2, P_3, P_4\}$ can be included in a regulated tetrahedron of side a, whence we find that the radius of S_5 is $\le a\frac{\sqrt{6}}{4}$.

If no, let's note. $\max_{1 \le i \le j \le 4} P_i P_j = P_1 P_4$. Does the sphere S_6 of diameter $P_1 P_4$ contain all points P_i?

If yes, stop (we are in the case 1).

If no, we consider the fascicule of spheres S' such that $\{P_1, P_4\} \subset Fr(S')$ and S' contains all the points P_i. We choose another sphere S_7, for which $P_5 \notin \{P_1, P_2, P_3, P_4\}$ and $P_5 \in Fr(S_7)$.

With these new notations (the points P_1, P_4, P_5 and the sphere S_7) we return to the case 2.

This algorithm is finite; therefore it constructs the required sphere.

[Published in “GAZETA MATEMATICA”, Nr. 9-10-11-12, 1992, Bucharest, Romania, p. 352.]

MATHEMATICAL RESEARCH AND NATIONAL EDUCATION

In our days we focus strongly on the interrelation between research and production. Between these two fields there is actually a very tight relation (osmosis), a dialectical union, while each is maintaining its own identity.

Education has been developed in accordance to its needs and demands resulting from the technical and scientific revolution: the introduction of faculties in the fields of production, research and design areas, and vice versa, the necessity of introducing the process of production and research work in the school units.

Therefore, it should be emphasized, that the students' dissertation projects be immediately applied in the production process. In this case, it is the school's responsibility to train and shape the future specialists in all fields of activity.

In the light of the present reality, we are witnessing an informational burst in all domains, and we notice the sustained effort which is being made by the educational system to adapt itself to the over increasing exigencies of the society, to keep the pace with the techniques and science conquests. Within these science conquests, mathematics occupies a central place – "the queen of sciences", as Gauss has said.

The Mathematics, for those who are studying it, confess to them, by the precision of the formulae and expressions on epoch, that there have been developed much, such a way that it was transformed from a science of numbers and of quantities (as it was called in ancient times), in a science of essential structures. New branches of mathematics have appeared, many of them due to its interpenetration with other sciences, and even branches such as: Mathematical Linguistics, Mathematical Poetics (in the latter a remarkable contribution is due to Prof. Solomon Marcus from Bucharest University). (The Mathematical Linguistics having as a starting point the topic models of the natural language and developing on algebraic grammar, by which are being studied the phenomenon of the natural languages).

"(…) mathematics have no limits, and the space that it finds is, so far, too reduced for its aspirations. The possibilities in Mathematics are as unlimited as the ones of the worlds which ceaselessly grow and multiply under the scrutinizing gaze of the astronomers; the mathematics could not be reduced by limited, precise keys or to be reduced to valid definitions eternally, but as the conscience life, which seem dormant in every world, each stone, each leaf, each bloom of flower, and in each which it is permanently ready to burst in new forms of animal life and vegetal existence" (James – Joseoh Sylvester, English Mathematician).

Mathematics in other sciences.

We say that is about their mathematization. All these sciences could not progress if they were not mathematized. Therefore, a whole group of discoveries wouldn't have taken place had it not been for the knowledge of certain scientific procedures, if mathematics had not possessed a certain quantity of knowledge (i.e., Einstein would not have discovered the theory of relativity and if before him the Tensorial Calculus would not have been discovered). Although other discoveries have been made before using math's calculations, which afterwards experimentally have been proved (The physician Maxwell – has generalized the concept of the field of electromagnetic forces, emphasizing the fact that even reforming to an electric or magnetic field this is propagated in existence by waves with the speed of light.).

Mathematics also offers its possibilities to the technical field, solving problems arising in the production process.

The very high abstractness in Mathematics does not hinder under its immediate applicability in practical manner, therefore would be worthwhile mentioning a few examples:

- The Romanian Geometer Gh. Țițeica made discoveries in the field of differential geometry- which led twenty years later to the conclusion that these could be applied in the theory of generalized relativity;

- Cayley has discovered the notion of matrix, discovery which found its applicability eighty seven years later when Heisenberg used it in the quantum mechanics;

- The English Mathematician George Boole, by the middle of XIX century, discovered the algebra which carries his name and which occupies the worthy place in the software – electronic computers.

An interesting correlation exists between mathematics and arts: music, painting, sculpture, architecture, and poetry.

Art is the pure expression of the "sentiment" while Mathematics is the crystalline expression of the pure "reasoning". Art, gushing from a sentiment, is warmer and more human, while mathematics, springing out from reasoning, is colder, but glitters more. An interesting correlation between Arts (and Literature especially), has been made by Solomon Marcus, Professor in the Department of Mathematics and of Languages also, showing the superiority of the pure artistic language vis-à-vis of the scientific language.

While the scientific language has a unique sense, the literary one has infinites. Therefore, in science the ambiguous language is eliminated. Recalling "this luminous point where geometry meets the poetry" as the mathematician and poet Dan Barbilian was saying, and we are reminded also the following idea:

"The poem of the future, by excellence, the sublime poem, will be borrowed from science" (Piere-Jules-Cesar Jensen).

Generally speaking about research, the risks that the scientist might run should be mentioned:

- he may find results already known (this shouldn't represent a disillusion, but even satisfaction);

- there could be a lead to suggestive results (one should have patience, and persevere);

- one could have errors in his demonstrations (deductions) – (almost all mathematicians have committed errors).

JUBILEE OF "GAMMA" JOURNAL

This autumn will be a few years since the school journal "Gamma" was founded at Lyceum "Steagul Roşu" in Braşov, Romania, under the guidance of the good hearted professor MIHAIL BENCZE, who has not spared any effort for it.

In the 28 numbers issued up to present, the "Gamma" journal has encouraged over two thousands students in solving problems of mathematics, helping them prepare for scientific competitions, exams for grades and degrees for universities. Each year, the Editorial Office grants prizes and honorable mentions to the most hardworking pupils who solve problems.

The journal's structure is classic. The wider space is dedicated to the original proposed problems of mathematics for grades 8-12 and college levels of computer science, up to present exceeding 7000, out of which we are sure that any time a bunch of very interesting problems, highly difficult, can be selected. We remember that some of those have already appeared in prestigious foreign journals – i.e. "American Mathematical Monthly", "Mathematics Magazine", etc. We also remember the over 80 open problems. Among which some may constitute topics of research for the mathematicians of tomorrow. Some elegant and ingenious problems are solved/resolved in the pages of this journal. The journal also contains problems translated from foreign magazines ("Kvant", A. M. M.) or foreign collections, problems given at Olympiads of mathematics from other countries (Spain, Belgium, Tunisia, Morocco, etc.) as well as from our country (GMB, RMT, Matematikai Lapok) some with solutions or even with generalizations of problems from the magazines mentioned above. Also, over one hundred "Where is the fault? (in demonstrations)" notes of mathematics.

There have been over 130 papers for popularization of mathematics or matters concerning inter disciplinary, mathematics and other domains (physics, philosophy, psychology, etc.) or even of creation.

The column "Mini Mathematical History", sustained with regularity by Prof. M. Bencze, schematically presented approximately 150 Romanian and foreign biographies of mathematicians.

Among the journal's collaborators included (other than the students, who are the most numerous, because, in fact, it is their journal) are professors, engineers, computer science specialists, and university faculty. Many are recognized in their field of specialty. The foreign collaborators Dr. E. Grosswald, Dr. Leroy F. Meyers (U. S. A.), Prof. Francisco Bellot (Spain), are famous in the world of Mathematics.

Additionally, the Editorial Office sporadically published Mathematical Paradoxes, cross words, "Mathematical Poems", and columns (such as "…did you know that…"), graphic themes and mottos (let us better call them, words of wisdom) of famous people.

It remains Long Live Mathematics.

September 1987

[Published in "Gamma", XXIX-XXX, Anul X, 1-2, October 1987, pp. 7-8.]

HAPPY NEW MATHEMATICAL YEARS!

Due to professor Gane Policarp's kindness, I have several issues of "Caietul de informare matematică" ("The Notebook of Mathematical Information"), which has been put together with attention to detail and skill, and which attracted and persuaded me, from the very beginning, to collaborate with small materials.

The redactor's preoccupation to present the problems given at competitions and scholar Olympiads, at exams and baccalaureates, determined me to give it a special place in my modest bookcase, and to work with my students proposed problems, some of the students having their names included on the list of those who correctly solved the problems.

Now, I found out, with a pleasant surprise, that the Câmpina mathematicians' journal celebrates its 10th anniversary of continuous publishing.

Long road and continuous success!

(January 1988)

DEDUCIBILITY THEOREMS IN BOOLEAN LOGIC

ABSTRACT

In this paper we give two theorems from the Propositional Calculus of the Boolean Logic with their consequences and applications and we prove them axiomatically.

§1. THEOREMS, CONSEQUENCES

In the beginning I shall put forward the axioms of the Propositional Calculus.

I. a) $\vdash A \supset (B \supset A)$,

b) $\vdash (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

II. a) $\vdash A \wedge B \supset A$,

b) $\vdash A \wedge B \supset B$,

c) $\vdash (A \supset B) \supset ((A \supset C) \supset (A \supset B \wedge C))$.

III. a) $\vdash A \supset A \vee B$,

b) $\vdash B \supset A \vee B$,

c) $\vdash (A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$.

IV. a) $\vdash (A \supset B) \supset (\overline{B} \supset \overline{A})$,

b) $\vdash A \supset \overline{\overline{A}}$,

c) $\vdash \overline{\overline{A}} \supset A$.

.

THEOREMS. If: $\vdash A_i \supset B_i, i = \overline{1,n}$**,** then

1) $\vdash A_1 \wedge A_2 \wedge ... \wedge A_n \supset B_1 \wedge B_2 \wedge ... \wedge B_n$,

2) $\vdash A_1 \vee A_2 \vee ... \vee A_n \supset B_1 \vee B_2 \vee ... \vee B_n$.

Proof:

It is made by complete induction. For $n = 1$: $\vdash A_1 \supset B_1$, which is true from the given hypothesis. For $n = 2$: hypotheses $\vdash A_1 \supset B_1$, $\vdash A_2 \supset B_2$; let's show that $\vdash A_1 \wedge A_2 \supset B_1 \wedge B_2$. We use the axiom II, c) replacing $A \to A_1 \wedge A_2$, $B \to B_1$, $C \to B_2$, it results:

(1) $\vdash (A_1 \wedge A_2 \supset B_1) \supset ((A_1 \wedge A_2 \supset B_2) \supset (A_1 \wedge A_2 \supset B_1 \wedge B_2))$.

We use the axiom II, a) replacing $A \to A_1$, $B \to A_2$; we have $\vdash A_1 \wedge A_2 \supset A_1$. But $\vdash A_1 \supset B_1$ (hypothesis) applying the syllogism rule, it results $\vdash A_1 \wedge A_2 \supset B_1$. Analogously, using the axiom II, b), we have $\vdash A_1 \wedge A_2 \supset B_2$. We know that $\vdash A_1 \wedge A_2 \supset B_i$, $i = 1, 2$, are deducible, then applying in (I) inference rule twice, we have $\vdash A_1 \wedge A_2 \supset B_1 \wedge B_2$.

We suppose it's true for n; let's prove that for $n+1$ it is true. In $\vdash A_1 \wedge A_2 \supset B_1 \wedge B_2$ replacing $A_1 \to A_1 \wedge ... \wedge A_n$, $A_2 \to A_{n+1}$, $B_1 \to B_1 \wedge ... \wedge B_n$, $B_2 \to B_{n+1}$ and using induction hypothesis it results $\vdash A_1 \wedge ... \wedge A_n \wedge A_{n+1} \supset B_1 \wedge ... \wedge B_n \wedge B_{n+1}$ and item 1) from the Theorem is proved.

2) It is made by induction. For $n=1$; if $\vdash A_1 \supset B_1$, then of course $\vdash A_1 \supset B_1$. For $n=2$: if $\vdash A_1 \supset B_1$ and $\vdash A_2 \supset B_2$, then $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$.

We use axiom III, c) replacing $A \to A_1$, $B \to A_2$, $C \to B_1 \vee B_2$ we get

(2) $\vdash (A_1 \supset B_1 \vee B_2) \supset ((A_2 \supset B_1 \vee B_2) \supset (A_1 \vee A_2 \supset B_1 \vee B_2))$.

Let's show that $\vdash A_1 \supset B_1 \vee B_2$. We use the axiom III, a) replacing $A \to B_1$, $B \to B_2$ we get $\vdash B_1 \supset B_1 \vee B_2$ and we know from the hypothesis $A_1 \quad B_1$. Applying the syllogism we get $\vdash A_1 \supset B_1 \vee B_2$.

In the axiom III, b) replacing $A \to B_1$, $B \to B_2$, we get $\vdash B_2 \supset B_1 \vee B_2$. But $\vdash A_2 \supset B_2$ (from the hypothesis), applying the syllogism we get $\vdash A_2 \supset B_1 \vee B_2$. Applying the inference rule twice in (2) we get $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$.

Suppose it's true for n and let's show that for $n+1$ it is true. Replace in $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$ (true formula if $\vdash A_1 \supset B_1$ and $\vdash A_2 \supset B_2$) $A_1 \to A_1 \vee ... \vee A_n$, $A_2 \to A_{n+1}$, $B_1 \to B_1 \vee ... \vee B_n$, $B_2 \to B_{n+1}$. From induction hypothesis it results $\vdash A_1 \vee ... \vee A_n \vee A_{n+1} \supset B_1 \vee ... \vee B_n \vee B_{n+1}$ and the theorem is proved.

CONSEQUENCES.

1°) If $\vdash A_i \supset B$, $i = \overline{1,n}$ then $\vdash A_1 \wedge ... \wedge A_n \supset B$.

2°) If $\vdash A_i \supset B$, $i = \overline{1,n}$, then $\vdash A_1 \vee ... \vee A_n \supset B$.

Proof: 1°) Using 1) from the theorem, we get

(3) $\vdash A_1 \wedge ... \wedge A_n \supset B \wedge ... \wedge B$ (n times).

In axiom II, a) we replace $A \to B$, $B \to B \wedge ... \wedge B$ ($n-1$ times), and we get

(4) $\vdash B \wedge ... \wedge B \supset B$ (n times).

From (3) and (4) by means of the syllogism rule we get $\vdash A_1 \wedge ... \wedge A_n \supset B$.

2°) Using 2) from theorem, we get $\vdash A_1 \vee ... \vee A_n \supset B \vee ... \vee B$ (n times).

LEMMA. $\vdash B \vee ... \vee B \supset B$ (n times), $n \geq 1$.

Proof:

It is made by induction. For $n=1$, obvious. For $n=2$: in axiom III, c) we replace $A \to B$, $C \to B$ and we get $\vdash (B \supset B) \supset ((B \supset B) \supset (B \vee B \supset B))$. Applying the inference rule twice we get $\vdash B \vee B \supset B$.

Suppose for n that the formula is deducible, let's prove that is for $n+1$.

We proved that $\vdash B \supset B$. In axiom III, c) we replace $A \to B \vee ... \vee B$ (n times), $C \to B$, and we get $\vdash (B \vee ... \vee B \supset B) \supset ((B \supset B) \supset (B \vee ... \vee B \supset B))$ (n times). Applying two times the interference rule, we get $\vdash B \vee ... \vee B \supset B$ ($n+1$ times) so lemma is proved.

From $\vdash A_1 \vee ... \vee A_n \supset B \vee ... \vee B$ (n times) and applying the syllogism rule, from lemma we get $\vdash A_1 \vee ... \vee A_n \supset B$.

3°) $\vdash A \wedge ... \wedge A \supset A$ (n times)

4°) $\vdash A \vee ... \vee A \supset A$ (n times).

Previously we proved, replacing in Consequence 1°) and 2°), $B \to A$. Analogously, the consequences are proven:

5°) If $\vdash A \supset B_i, i = \overline{1,n}$, then $\vdash A \supset B_1 \wedge ... \wedge B_n$.

6°) If $\vdash A \supset B_i, i = \overline{1,n}$, then $\vdash A \supset B_1 \vee ... \vee B_n$.

Analogously,

7°) $\vdash A \supset A \wedge ... \wedge A$ (n times)

8°) $\vdash A \supset A \vee ... \vee A$ (n times)

9°) $\vdash A_1 \wedge ... \wedge A_n \supset A_1 \vee ... \vee A_n$.

Proof:

Method I. It is initially proved by induction: $\vdash A_1 \wedge ... \wedge A_n \supset A_i$, $i = \overline{1,n}$ and 2) is applied from the Theorem.

Method II. It is proven by induction that: $\vdash A_i \supset A_1 \wedge ... \wedge A_n$, $i = \overline{1,n}$ and then 1) is applied from the Theorem.

10°) If $\vdash A_i \supset B_i$, $i = \overline{1,n}$, then $\vdash A_1 \wedge ... \wedge A_n \supset B_1 \vee ... \vee B_n$.

Proof:

Method I. Using 1) from the Theorem, it results:

(5) $\vdash A_1 \wedge ... \wedge A_n \supset B_1 \wedge ... \wedge B_n$

We apply the Consequence 9°) where we replace $A_i \to B_i$, $i = \overline{1,n}$ and results:

(6) $\vdash B_1 \wedge ... \wedge B_n \supset B_1 \vee ... \vee B_n$.

From (5) and (6), applying the syllogism rule we get 10°).

Method II. We firstly use the Consequence 9°) and then 2) from the Theorem and so we obtain the Consequence 10°).

§2. APPLICATIONS AND REMARKS ON THEOREMS

The theorems are used in order to prove the formulae of the shape:

$\vdash A_1 \wedge ... \wedge A_p \supset B_1 \wedge ... \wedge B_r$

$\vdash A_1 \vee ... \vee A_p \supset B_1 \vee ... \vee B_r$, where $p, r \in \mathbb{N}^*$

It is proven that $\vdash A_i \supset B_j$, i.e.

$$\forall i \in \overline{1,p},\ \exists j_0 \in \overline{1,r},\ j_0 = j_0(i),\ \vdash A_i \supset B_{j_0}$$

and

$$\forall j \in \overline{1,r},\ \exists i_0 \in \overline{1,p},\ i_0 = i_0(j),\ \vdash A_{i_0} \supset B_j.$$

EXAMPLES: The following formulas are deducible:

(i) $\vdash A \supset (A \vee B) \wedge (B \supset A)$,

(ii) $\vdash (A \wedge B) \vee C \supset A \vee B \vee C$,

(iii) $\vdash A \wedge C \supset A \vee C$.

Solution:

(i) We have $\vdash A \supset A \vee B$ and $\vdash A \supset (B \supset A)$ (axiom III, a) and I, a)) and according to 1) from Theorem it results (i).

(ii) From $\vdash A \supset (B \supset A)$, $\vdash A \wedge B \supset B$, $\vdash C \supset C$ and Theorem 1), we have (ii).

(iii) Method I. From $\vdash A \wedge C \supset A$, $\vdash A \wedge C \supset C$ and Theorem 2).
Method II. From $\vdash A \supset A \vee C$, $\vdash C \supset A \vee C$ and using Theorem 1).

REMARKS. 1) The reciprocals of Theorem 1) and 2) are not always true.

a) Counter-example for Theorem 1). The formula $\vdash A \wedge B \supset A \wedge A$ is deducible from axiom II, a), $\vdash A \wedge A \supset A$ (Consequence 7°) and the syllogism rule. But $\vdash A \supset A$ for all A, that the formula $B \supset A$ is not deducible, so the reciprocal of the Theorem 1) is false.

Counter-example for Theorem 2). The formula $\vdash A \vee A \supset A \vee B$ is deducible from Lemma, axiom III, a) and applying the syllogism rule. But $\vdash A \supset A$ for all A, that the formula $A \supset B$ is not deducible, so the reciprocal of Theorem 2) is false.

2) The reciprocals of Theorem 1) and 2) are not always true.

Counter-examples:

a) for Theorem 1): $\vdash A \supset A$ and $B \not\supset A$ results that $\vdash A \wedge B \supset A \wedge A$ so the reciprocal of Theorem 1) is false.
b) for Theorem 2): $\vdash A \supset A$ and $A \not\supset B$ results that $\vdash A \vee A \supset A \vee B$ so the reciprocal of Theorem 2) is false.

REFERENCES:

[1] P. S. NOVOKOV. Elemente de logică matematică, Editura Ştiinţifică, Bucureşti, 1966.
[2] H. FREUDENTHAL, Limbajul logicii matematice, Editura Tehnică, Bucureşti, 1973.

UNIVERSITATEA DIN CRAIOVA
Facultatea de tiinte Exacte
24.10.1979

[Published in "An. Univ. Timişoara", Seria Şt. Matematice, Vol. XVII, Fasc. 2, 1979, pp. 164-8.]

LINGUISTIC-MATHEMATICAL STATISTICS IN RECENT ROMANIAN POETRY

"Mathematics is logical enough to be able to detect the internal logics of poetry and crazy enough not to lag behind the poetic ineffable" (Solomon Marcus).

The author of this article aims a statistical investigation of a recently published volume of poetry [3], which will make possible some more general conclusions on the evolution of poetry in the XXth century (either the literary current hermetism, surrealism or any other). Certain modifications in the structure of poetry, occurred in its evolution from classicism to modernism, are also presented. Men of letters have never agreed with mathematics and, especially, with its interference in art. Let us quote one of them: "Remarque que, a mon avis, tout literature est grotesque…(…) La seule excuse de l'écrivain c'est de se rendre compte qu'il joue, que la littérature est un jeu" (Eugène Ionesco). Well, if literature is a game why could not be subjected to mathematical investigation?

The book chosen for this study (see [3]) contains 44 poems (from which the first and the last are sort of poems essays on Romanian poetry). It comprises over 250 sentences, over 700 verses, over 2,500 words and over 11,700 letters (not sounds).

MORPHOLOGICAL ASPECTS

1. The frequency of words depending on the grammatical category they belong to.

1. Nouns 2. Verbs (predicate moods) 3. Adjectives 4. Adverbs	35.592% 13.079% 6.183% 4.829%	"Empty" words 40.271%
"Full" words	59.729%	

1. The "full" words category includes – according to the author – nouns, verbs (predicative moods only), adjectives and adverbs. The "empty" words category includes verbs (i,e, infinitives, gerunds, poet participles, supines), numerals, articles, pronouns, conjunctions, prepositions and interjections. The same terminology was also used by Solomon Marcus in his "Poetica matematica" published by Ed. Academiei, Bucharest, 1970 (it was translated in German and published by Athenäum, Frankfurt-am-Mein, 1973).

2. The average distribution of “full” words[1] per verses (lines), sentences, poems

a) 1.255	nouns/line
b) 0.461	verbs (p.m)/line
c) 0.218	adjectives/line
d) 0.172	adverbs/line
e) 3.464	nouns/sentence
f) 1.273	verbs (p.m)/sentence
g) 0.602	adjectives/sentence
h) 0.475	adverbs/sentence
i) 20.393	nouns/poem
j) 7.492	verbs (p.m)/poem
k) 3.543	adjectives/poem
l) 2.792	adverbs/poem

We may conclude:

CONJECTURE 1. In the recent Romanian poetry the percentage of adjectives is, on average, under that of the total of words.

CONJECTURE 2. The percentage of verbs (predicative moods) is., on average, under 15% of the total of the total words.

In support of conjectures 1 and 2 we also mention:

- only one in six nouns is modified by an adjective, i.e. the role of the adjective diminishes and there are poems with no adjectives (see [3], pp. 9, 12, 20);

- on average, there is one verb in a predicative mood in more than two lines, i.e. the role of the verbal predicate decreases and there are poems with no verbal predicates (see [3], p. 20);

(From classicism to modernism both adjectives and verbal predicates gradually but constantly regressed).

- the poetry of the young poets is characterized by economy of words and, implicitly, by the avoidance of the overused words; the adjectives were favored by the romantics and the young poets feel the necessity to “renew” poetry;

- this renewal and effort to avoid the trivial may be also helped by elimination of adjectives. The strict use of adjectives or verbal predicates is also accounted for by the characteristics of the two main literary currents of our century.

a) hermetism – appeared after World War I – consists, mainly in the hyper intellectualization of language and its codification; an adjective (i.e. an explanation concerning an object) or the predicative mood of a verb (strict definition of the grammatical tense) may diminish the degree of ambiguity, generalization or abstraction intended by the poet.

b) Surrealism – literary of vanguard – aimed at detecting the irrational, the unconscious, the dream; because of its precise definite character, the adjective makes the reader “plunge” into the so carefully avoided real world.

CONJECTURE 3. In the recent Romanian poetry percentage of “full” words is over 55% of the total words.

Unlike in the spoken language in which the percentage of “full” and “empty” words is equal (see [1]) in poetry the percentage of “full” words is greater. This is due to the fact that poetry is essence, it is dense, concentrated. The percentage of “full” words and the “density” of a literary work are directly proportional.

As a conclusion to the three conjectures we may say that:

- in its evolution from classicism to modernism the percentage of nouns increased, while that of verbs decreased, less adverbs are used, on the other hand, because of the smaller number of verbs. In all, however, the percentage of “full” words increased.

3. The frequency of the nouns with and without an article.

1. Percentage of nouns with an article	- 47.884%
2. Percentage of nouns without an article	- 52.116%

CONJECTURE 4. In the recent Romanian poetry the number of nouns with an article is, on an average, smaller than the number of those without an article. With an article the noun is more definite, specified which are characteristics undesirable from the same viewpoint as that mentioned above. That is why the indefinite article is favored in modern poetry. The consequence of this preferred indefinite character of the noun enlarges the abstraction, generalization, ambiguity and, hence, the “density “ of the poem. (See also the second part of assertions 1 and 2 and the statistical conjecture 3). In its evolution from classicism to modernism the number of nouns without an article used in poetry also increased.

4. The frequency of nouns depending on the grammatical case they belong to.

Nominative	Genitive	Dative	Accusative	Vocative
29.497%	19.888%	0.335%	50.056%	0.224%
2	3	4	1	5

↑C L A S S I F I C A T I O N↑

CONJECTURE 5. In the poems under study, over 75% of the nouns are accusative or nominative.

5. Sentences, lines, words, syllables, letters – average relationships

a) 2.402	letters/syllable
b) 1.933	syllables/word
c) 4.643	letters/word
d) 3.528	words/line

e) 6.820	syllables/line
f) 16.380	letters/line
g) 2.760	lines/sentence
h) 9.737	words/sentence
i) 18.823	syllables/sentence
j) 45.208	letters/sentence
k) 5.887	sentences/poem
l) 16.250	lines/poem
m) 57.330	words/poem
n) 110.825	syllables/poem
o) 266.175	letters/poem

Conclusion: the poems are of medium length; the lines are short while the sentences are, again, of medium length.

6. The frequency of words according to their length (in syllables)

Syllables	Percentages	Order
1	41.509%	1
2	32.069%	2
3	19.363%	3
4	5.688%	4
5	1.371%	5
6	0.000%	6

The total number of syllables in the volume is … 4,800. The frequency of words and their length (in syllables are in inverse ratio. Long words seem "less poetical".

CONJECTURE 6. In the recent Romanian poetry the percentage of words of one and two syllables is … 75%. Again, it seems that short and very short words (of one and two syllables) appear more adequate to satisfy the internal rhythm of the poem. Longer words already have their own rhythm dictated by the juxtaposition of the syllables; it is very probable that this rhythm comes into … with the rhythm imposed by the poem. Shorter words are more easily uttered; longer words seem to render the text more difficult.

7. The frequency of words according to their length (in letters)

1 letter	2	3	4	5	6	7	8	9	10	11	12	13	14
3.604%	25.426%	8.475%	11.089%	13.347%	13.149%	13.703%	5.861%	3.129%	1.149%	0.752%	0.237%	0.079%	0.000%

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

In the whole volume there are only two words of 13 letters and 6 of twelve. A 90% of the words consist of no more than 7 letters.

CONJECTURE 7. In the recent Romanian poetry the percentage of the two letter words is, on average, about 25% of the words. In fact, the same percentage, or even higher, is found in the ordinary language. Because of esthetic reasons in poetry there is a slight tendency of reducing the frequency of the two letter words – which are especially, prepositions and conjunctions.

8. The frequency of the letters

The order of the letter	Letter	The average % of the frequency of the letter	The average % of vowels	The average % of cons
1	E	11.994%		
2	I	10.166%		
3	A	8.406%		
4	R	7.680%		
5	N	6.407%		
6	U	6.347%		
7	T	5.792%		
8	L	5.237%		
9	C	5.143%	46.865%	
10	S	4.220%		
11	O	3.699%		
12	P	3.451%		
13	Ă	3.417%		53.135%
14	M	3.178%		
15	D	2.981%		
16	Î	2.828%		
17	V	1.435%		
18	G	1.48%		
19	B	1.358%		
20	Ș	1.281%		
21	F	1.179%		
22	Z	0.846%		
23	Ț	0.803%		
24	H	0.496%		
25	J	0.196%		
26	X	0.034%		
27	Ă	0.008%		
28-31	K	0.000%		
28-31	Q	0.000%		
28-31	Y	0.000%		

28-31	W	0.000%		

CONJECTURE 8. In the recent Romanian poetry the percentage of vowels is, on average, over 45% of the total of letters.

Explanation: in the ordinary language the percentage of vowels is 42.7% (see [1]). In poetry it is greater because:

- vowels are more "musical" than consonants; therefore the words with more vowels "seem" more poetical; words with many vowels confer a special sonority to the text;
- modern poets and poetry are more preoccupied by form than by content, so that more attention is given to expression; the form may prejudice the content, because, very often, the reader is "caught" by sonority and less by essence;
- the internal rhythm of poetry, usually absent in the ordinary language, is also conditioned, partially, by a greater number of vowels;
- rhyme, when used, also favors a greater percentage of vowels. The percentage of vowels was greater in the period of classicism of poetry when the rhythm and rhyme were more frequently used. The special requirements of poetry impose a thorough filtration of the ordinary language.

Given the frequency of the letters in the Romanian language [1] in general:

1. E	5. N	9. L	13. D	17. S	21. F	25. J
2. I	6. T	10. S	14. P	18. B	22. T	26. X
3. A	7.T	11. O	15. M	19. V	23. Z	27. K
4. R	8. C	12. A	16. I	20. G	24. H	

we may calculate the deviation of this volume of verses from the ordinary language:

$$\alpha(v) = \frac{1}{27}\sum_{i=1}^{27}|\alpha(A_i)| \approx 0.741$$

where $\alpha(A_i)$ is the deviation of the letter A_i, $1 \le i \le 27$.

The informational energy, according to O. Onicescu, is

$$\varepsilon(v) = \sum_{i=1}^{27} p_i^2 \approx 0.064 ,$$

where p_i, $1 \le i \le 27$, is the probability that the letter p_i may appear in the volume (see [1]).

The first order entropy of the volume (according to Shannon) is:

$$H_1(v) = -\frac{1}{\log_{10}2}\cdot\sum_{i=1}^{27} p_i \log_{10} p_i \approx 4.222 .$$

9. The themes of the volume are studied by determining the recurrent elements, those that seem to obsess the poet. We will call these elements "key-words" and they are, in order: nouns, verbs, adjectives. Their frequency in the volume is studied. The more frequent words are all included in common notional spheres that will "decode" the themes dealt with by the poet in the volume under study, i.e.:

Elements of the Nature

trees leaves water

birds
street
wind
soft-hearted
to ripe
tender

Cosmological Elements

sky
Moon
Sun
stars light
night evening
hours
time

Existence Elements

life
death
to live
spirit tears
to put out
to love
to lower
to deplore
not to be

Poet's condition

poem

to read
to dream

to write
verses
words

These 33 key-words (together with their synonyms) confer certain pastoral note (this was noticed by Constantin Matei, the newspaper ”Înainte”, Craiova), cosmological (Constantin M. Popa), existentialist nuances (Aureliu Goci, “Luceafarul”, Bucharest); the preoccupation of the poet for the condition of the poet and society (Ion Pachia Tatomirescu, Craiova) is also revealed by the frequent use of certain suggestive words.

Of all the words, 33 key-words together with their synonyms have the greatest frequency in the volume.

10. The frequency of words and phrases strongly deviated from the “normal”, i.e. the rules of the literary language are about 1.980 of the total of words. (We mean expressions like: “state of self”, “very near myself”, “it is raining at plus infinite” or words like “nontime”, etc. (see [3], pp. 9, 29, 40, 31).

CONJECTURE 9. In the recent Romanian poetry the percentage of words and phrases that strongly deviated from the “normal” of the ordinary language, as well as the rules of the literary language, is slightly over 1. This fact may be accounted for by:

- content seems less important; poets are more concerned with form;
- poets invent words and expressions to be able to better reveal their feelings and emotions;
- the association of antonyms may give birth to constructions that, somehow “violate” the normal;
- poetry is, in fact, destined to break the rules and rebel against the ordinary fact (if, this right is denied, any newspaper article could be called poetry).

“In art” said Voltaire, “rules are only meant to be broken”.

In its evaluation from classicism to modernism the percentage of such abnormal words and constructions increased, starting, in fact from zero. Modern literary currents favor the appearance of them.

REFERENCES

[1] Marcus, Solomon – “Poetica matematică” – Ed. Academiei, Bucharest, 1970 (translated into German, Athenäum, Frankfurt-am-Mein, 1973).

[2] Marcus, Solomon, Edmond Nicolau, Sorin Stati – “Introducere în lingvistica matematică”, Bucharest, 1966 (translated in Italian, Patron, Bologna, 1971 and in Spanish, Teide, Barcelona, 1978).

[3] Florentin, Ovidiu – “Formule pentru spirit”, Ed. Litera, Bucharest, 1981 (Translated in French, les Editions Express, Fès, Morocco, 1983); modern poems.

[4] Smarandache, Florentin – “A mathematical linguistic approach to Rebus” – article published in “Revue roumain de linguistique”, tome XXVIII, 1983, collection “Cahiers de linguistique théorique et appliquée”, tome XX, 1983, No. 1, pp. 67-76.

[Editions Scientifiques, Casablanca, Morocco, 1984]

A MATHEMATICAL LINGUISTIC APPROACH TO REBUS

INTRODUCTION

The aim of this paper is the investigation of some combinatorial aspects of written language, within the framework determined by the well-known game of crossword puzzles. Various types of probabilistic regularities appearing in such puzzles reveal some hidden, not well-known restrictions operating in the field of natural languages. Most of the restrictions of this type are similar in each natural language. Our direct concern will be the Romanian language.

Our research may have some relevance for the phono-statistics of Romanian. The distribution of phonemes and letters is established for a corpus of a deviant morphological structure with respect to the standard language. Another aspect of our research may be related to the so-called tabular reading in poetry. The correlation horizontal-vertical considered in the first part of the paper offers some suggestions concerning a bi-dimensional investigation of the poetic sing.

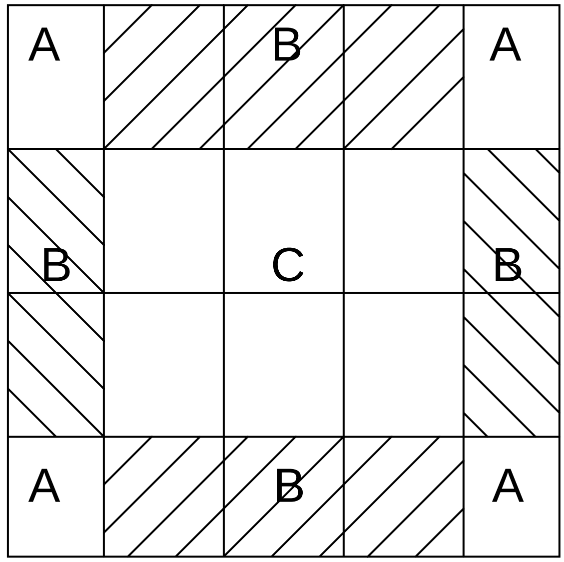
Our investigation is concerned with the Romanian crossword puzzles published in [4]. Various concepts concerning crossword puzzles are borrowed from N. Andrei [3]. Mathematical linguistic concepts are borrowed from S. Marcus [1], and S. Marcus, E. Nicolau, S. Stati [2].

SECTION 1. THE GRID

§1. MATHEMATICAL RESEARCHES ON GRIDS

It is known that a word in a grid is limited on the left and right side either by a black point or by a grid final border.

We will take into account the words consisting of one letter (though they are not clued in the Rebus), and those of two (even they have no sense (e.g. NT, RU,…)), three or more letters – even they represent that category of rare words (foreign localities, rivers, etc., abbreviations, etc., which are not found in the Romanian Language Dictionary (see [3], pp. 82-307 ("Rebus glossary")).



The grids have both across and down words.

We divide the grid into 3 zones:

a) the four peaks of the grid (zone A)
b) grid border (without de four peaks) (zone B)
c) grid middle zone (zone C)

We assume that the grid has n lines, m columns, and p black points.

Then:

Proposition 1. The words overall number (across and down) of the grid is equal to $n + m + pNB + 2 \cdot pNC$, where

pNB = black points number in zone B,

pNC = black points number in zone C.

Proof: We consider initially the grid without any black points. Then it has $n + m$ words.

- If we put a black point in zone A, the words number is the same. (So it does not matter how many black points are found in zone A).

- If we put a black point in zone B, e.g. on line 1 and column j, $i < j < m$, words number increases with one unit (because on line 1, two words were formed (before there was only one), and on column j one word rests, too). The case is analog if we put a black point on column 1 and line i, $1 < i < n$ (the grid may be reversed: the horizontal line becomes the vertical line and vice versa). Then, for each point in zone B a word is added to the grid words overall number.

- If we put a black point in zone C, let us say i, $1 < i < n$, and column j, $1 < j < m$, then the words number increases by two: both on line i and column j two words appear now, different from the previous case, when only one word was there on each line. Thus, for each black point in zone C, two words are added at the grid words overall number. From this proof results:

Corollary 1. Minimum number of words of grid $n \times m$ is $n + m$. Actually, this statement is achieved when we do not have any black points in zones B and C.

Corollary 2. Maximum number of words of a grid $n \times m$ having p black points is $n + m + 2p$ and it is achieved when all p black points are found in zone C.

Corollary 3. A grid $n \times m$ having p black points will have a minimum number of words when we fix first the black points in zone A, then in zone B (alternatively – because it is not allowed to have two or more black points juxtaposed), and the rest in zone C.

Proposition 2. The difference between the number of words on the horizontal and on the vertical of a grid $n \times m$ is $n - m + pNBO - pNBV$, where

$pNBO$ = black points number in zone ,

$pNBV$ = black points number in zone BV.

We divide zone B into two parts:

- zone BO = B zone horizontal part (line 1 and n)
- zone BV = B zone vertical part (line 1 and m).

The proof of this proposition follows the previous one and uses its results.

If we do not have any black points in the grid, the difference between the words on the horizontal and those on the vertical line is $n - m$.

- If we have a black point in zone A, the difference does not change. The same for zone C.

If we have a black point in zone BO, then the difference will be $n - m - 1$. From this proposition 2 results:

Proposition 3. A grid $n \times m$ has $n + pNBO + pNC$ words on the horizontal and $m + pNBV + pNC$ words on the vertical.

The first solving method uses the results of propositions 1 and 2.

The second method straightly calculates from propositions 1 and 2 the across and down words number (their sum (proposition 1) and difference (proposition 2) are known).

Proposition 4. Words mean length (=letters number) of a grid $n \times m$ with p black points is $\geq \dfrac{2(nm - p)}{n + m + 2p}$.

Actually, the maximum words number is $n + m + 2p$, the letter number is $nm - p$, and each letter is included in two words: one across and another down. One grid is the more crossed, the smaller the number of the words consisting of one or two letters and of black points (assuming that it meets the other known restrictions). Because in the Romanian grids the black points percentage is max.

15% out of the total (rounding off the value at the closer integer – e.g. 15% with a grid 13x13 equals 25.35 $\approx$ 25; with a grid 12x12 is 21.6 $\approx$ 22), so for the previous properties, for grids $n \times m$ with p black points we replace p by $\left[\dfrac{3}{20}\right] nm$, where

$[x] = \max\left\{\alpha \in \mathrm{N},\ |\alpha - x| \leq 0.5\right\}$.

§2. STATISTIC RESEARCHES ON GRIDS

In [1] we find the notion "écart of a sound x", denoted by $\alpha(x)$, which equals the difference between the rank of x in Romanian and the rank of x in the analyzed text.

We will extend this notion to the notion of *a text écart* which will be denoted by: $\alpha(t)$, and

$$\alpha(t) = \frac{1}{n}\sum_{i=1}^{n}|\alpha(A_i)|$$

where $\alpha(A_i)$ is A_i sound écart (in [1]) and n represents distinct sounds number in text t. (If there are letters in the alphabet, which are not found in the analyzed text, these will be written in the frequency table giving them the biggest order.)

Proposition 1. We have a double inequality:

$0 \le \alpha(t) \le \frac{n-1}{2} + \frac{1}{n}\left[\frac{n}{2}\right]$ where $[y]$ represents the whole part of real number y.

Actually, the first inequality is evident.

Let $\Phi = \begin{pmatrix} 1 & 2 & \ldots & n \\ & & & \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$. Then $\sum_{i=1}^{n}|\alpha(A_i)| = \sum_{i=1}^{n}|i - j_i|$

This permutation constitutes a mathematical pattern of the two frequency tables of sounds; in Romanian (the first line), in text t (the second line).

For permutation $\psi = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ n & n-1 & \ldots & 2 & 1 \end{pmatrix}$ we have

$$\sum_{i=1}^{n}|i - j_i| = 2[(n-1) + (n-3) + (n-5) + \ldots] = 2\sum_{k=1}^{\left[\frac{n}{2}\right]}(n - 2k + 1) =$$

$$= 2\left[\frac{n}{2}\right]\left(n - \left[\frac{n}{2}\right]\right) = \frac{n(n-1)}{2} + \left[\frac{n}{2}\right],$$

where $\alpha(t) = \frac{n-1}{2} + \frac{1}{n}\cdot\left[\frac{n}{2}\right]$.

By induction with respect to $n \ge 2$, we prove now the sum $S = \sum_{i=1}^{n}|i - j_i|$ has max. value for permutation ψ.

For $n = 2$ and 3 it is easily checked directly. Let us suppose the assertion true for values $< n+2$. Let us show for $n+2$:

$$\psi = \begin{pmatrix} 1 & 2 & \ldots & n+1 & n+2 \\ n+2 & n+1 & \ldots & 2 & 1 \end{pmatrix}$$

Removing the first and last column, we obtain:

$$\psi' = \begin{pmatrix} 2 & \ldots & n+1 \\ n+1 & \ldots & 2 \end{pmatrix},$$

which is a permutation of n elements and for which S will have the same value as for permutation

$$\psi'' = \begin{pmatrix} 1 & \dots & n \\ n & \dots & 1 \end{pmatrix},$$

i.e. max. value (ψ'' was obtained from ψ' by diminishing each element by one).

The permutation of 2 elements $\eta = \begin{pmatrix} 1 & n+2 \\ n+2 & 1 \end{pmatrix}$ gives maximum value for S.

But ψ is obtained from ψ' and η;

$$\psi(i) = \begin{cases} \psi'(i), & \text{if } i \notin \{1, n+2\} \\ \eta(i), & \text{otherwise} \end{cases}$$

Remark : The bigger one text écart, the bigger the "angle of deviation" from the usual language.

It would be interesting to calculate, for example, the écart of a poem.

Then the notion of écart could be extended even more:

a) *the écart of a word* being equal to the difference between word order in language and word order in the text;
b) *the écart of a text (ref. words):*

$$\alpha_c(t) = \frac{1}{n} \sum_{i=1}^{n} |\alpha_c(a_i)|,$$

where $\alpha_c(a_i)$ is word a_i écart, and n - distinct words number in the text t.

*

We give below some rebus statistic data. By examining 150 grids [4] we obtain the following results:

Occurrence frequency of words in the grid, depending on their length (in letters)

<table>
<tr><th>Letter order</th><th>Letter</th><th>Letter occurrence mean percentage</th><th>Vowels mean percentage</th><th>Consonants mean percentage</th></tr>
<tr><td>1</td><td>A</td><td>15.741%</td><td rowspan="23">47.462%</td><td rowspan="23">52.538%</td></tr>
<tr><td>2</td><td>I</td><td>12.849%</td></tr>
<tr><td>3</td><td>T</td><td>9.731%</td></tr>
<tr><td>4</td><td>R</td><td>9.411%</td></tr>
<tr><td>5</td><td>E</td><td>8.981%</td></tr>
<tr><td>6</td><td>O</td><td>5.537%</td></tr>
<tr><td>7</td><td>N</td><td>5.053%</td></tr>
<tr><td>8</td><td>U</td><td>4.354%</td></tr>
<tr><td>9</td><td>S</td><td>4.352%</td></tr>
<tr><td>10</td><td>C</td><td>4.249%</td></tr>
<tr><td>11</td><td>L</td><td>4.248%</td></tr>
<tr><td>12</td><td>M</td><td>4.010%</td></tr>
<tr><td>13</td><td>P</td><td>3.689%</td></tr>
<tr><td>14</td><td>D</td><td>1.723%</td></tr>
<tr><td>15</td><td>B</td><td>1.344%</td></tr>
<tr><td>16</td><td>G</td><td>1.290%</td></tr>
<tr><td>17</td><td>F</td><td>0.860%</td></tr>
<tr><td>18</td><td>V</td><td>0.806%</td></tr>
<tr><td>19</td><td>Z</td><td>0.752%</td></tr>
<tr><td>20</td><td>H</td><td>0.537%</td></tr>
<tr><td>21</td><td>X</td><td>0.430%</td></tr>
<tr><td>22</td><td>J</td><td>0.053%</td></tr>
<tr><td>23</td><td>K</td><td>0.000%</td></tr>
</table>

It is easy to see that a percentage of 49,035% consists of the words formed only of 1, 2 or 3 letters; - of course, there are lots of incomplete words.

*

The study of 50 grids resulted in:

Occurrence frequency of words in a grid (see next page).

It is noticed that vowels percentage in the grid (47.462%) exceeds the vowels percentage in language (42.7%).

So, we can generalize the following:

Statistical proposition (1): In a grid, the vowels number tends to be almost equal to 47.5% of the total number of the letters.

Here is some evidence: one word with *n* syllables has at least *n* vowels (in Romanian there is no syllable without vowel (see [2]).

The vowels percentage in Romanian is 42.7%; because a grid is assumed to form words across and down, the vowels number will increase. Also, the last two lines and columns are endings of other words in the grid; thus they will usually have more vowels. When black points number decreases, vowels number will increase (in order to have an easier crossing, you need either more black points or more vowels) (A vowel has a bigger probability to enter in the contents of a word than a consonant.)

Especially in "record grids" (see [3], pp. 33-48) the vowels and consonants alternation is noticed. Another criterion for estimating the grid value is the bigger deviation from this "statistical law" (the exception confirms the rule!): i.e. the smaller the vowel percentage in a grid, the bigger its value.

Statistical proposition (2): Generally, the horizontal words number 73 equals the vertical one.

Here is the following evidence: 100 classical grids were experimentally analyzed, in [4], getting the percentage of 49.932% horizontal words. Usually, the classical grids are square clues, the difference between the horizontal and vertical words being (see Proposition 2):

$$n - m + pNBO - pNBV = pNBO - pNBV\ .$$

The difference between the black points number in zone BO and zone BV can not be too big (± 1, ± 2 and rarely ± 3). (Usually, there are not many black points in zone B, because it is not economical in crossing (see proof of Proposition 1)).

Taking from [1] the following letters frequency in language:

1. E	5.N	9. L	13. P	17. G	21. J
2. I	6.T	10. S	14. M	18. F	22. X
3.A	7.U	11. O	15. B	19. Z	23. K
4.R	8.C	12. D	16. V	20. H	

(because in the grid Ă, Â, Î, Ş, Ţ: are replaced by A: I: S: T, respectively, in the above order they were cancelled) the écart of the 150 grids becomes

$$\alpha(g) = \frac{1}{23}\sum_{i=1}^{23}\left|\alpha(A_i)\right| \approx 1.391\,;$$

the entropy is:

$$H_1 = -\frac{1}{log_{10} 2}\sum_{i=1}^{23} p_i\ log_{10} p_i \approx 3.865$$

and the informational energy (after O. Onicescu) is:

$$E(g) = \sum_{i=1}^{23} p_i^2 \approx 0.084$$

Examining 50 grids we obtain:

Words frequency in a grid with respect to the syllables number

Mean percentage of occurrence of a word in a grid								**Mean length of a word in syllables**
1 syllable	**2**	**3**	**4**	**5**	**6**	**7**	**8**	
35.588%	**26.920%**	**21.765%**	**9.551%**	**5.294%**	**0.882%**	**0.000%**	**0.000%**	**2.246**

(in the category of the one syllable-words, the word of one, two or, three letters, without any sense – rare words – were also considered.) One can see that the percentage of words consisting of one and two syllables is 65.508% (high enough).

Another statistics (of 50 grids), concerning the predominant parts of speech in a grid has established the following first three places:

1. nouns 45.441%
2. verbs 6.029%
3. adjectives 2.352%

Notice the large number of nouns.

*****

SECTION II. REBUS CLUES

§1. STATISTICAL RESEARCHES ON REBUS CLUES

Studying the clues of 100 "clues grids", the following statistical data resulted:

Rebus clues frequency according to their length (words number)

(see the next page)

It is noticed that the predominant clues are formed of 2, 3, or 4 words. For results obtained by investigating 100 "clues grids", see the next page.

It is worth mentioning that vowels percentage (46.467%) from rebus clues exceeds vowels percentage in the language (42.7%).

By calculating the clues écart (in accordance with the previous formula) it results:

$$\alpha(dr) = \frac{1}{27}\sum_{i=1}^{27}\left|\alpha(A_i)\right| \approx 1.185$$

(sound frequency used by Solomon Marcus in [1] was used here), the entropy (Shannon) is:

$$H_1 = -\frac{1}{log_{10} 2} \sum_{i=1}^{27} p_i \ log_{10} p_i \approx 4.226$$

and informational energy (O. Onicescu) is:

$$E(dr) = \sum_{i=1}^{27} p_i^2 \approx 0.062 .$$

(The calculations were done by means of a pocket calculator).

Letters occurrence frequency in the rebus clues

Letter order	Letter	Mean percentage of letter occurrence in clues	Vowels percentage	Conso-nants mean percentage	Letters no. (mean) necessary to clue a grid	Mean length of a word (in letters) used in clues
1	E	10.996%	46.679%	53.321%	657.342	4.374
2	I	9.778%				
3	A	9.266%				
4	R	7.818%				
5	U	6.267%				
6	N	6.067%				
7	T	5.611%				
8	C	5.374%				
9	L	4.920%				
10	O	4.579%				
11	P	4.027%				
12	Ă	3.992%				
13	S	3.831%				
14	Î	3.309%				
15	D	3.079%				
16	Â	1.801%				
17	V	1.527%				
18	F	1.449%				
19	Ş	1.360%				
20	Ţ	1.338%				
21	G	1.330%				
22	B	1.238%				
23	H	0.532%				
24	J	0.358%				
25	Z	0.092%				
26	X	0.037%				
27	K	0.024%				

REFERENCES

[1] Marcus, Solomon – "Poetica matematica" – Ed. Academiei, Bucureşti, 1970 (German translation, Athenäum, Frankfurt am Mein, 1973).
[2] Marcus, Solomon, Edmond Nicolau, S. Stati – Introducere în lingvistica matematică, Bucureşti, 1966 (Italian translation, Patron, Bologna, 1971; Spanish translation, Teide, Barcelona, 1978).
[3] Andrei, Dr. N. – Îndreptar rebusist, Ed. Sport-Turism, Bucureşti, 1981.
[4] "Rebus" magazine collection, Bucureşti, 1979-1982.

The Craiova University
Natural Sciences Department

[Published in "Review Roumaine de linguistique", Tome XXVIII, 1983, "Cahiers de linguistique théorique et appliquée", Bucharest, Tome XX, 1983, No. 1, pp. 67-76.]

HYPOTHESIS ON THE DETERMINATION OF A RULE FOR THE CROSS WORDS PUZZLES

The problems of cross words are composed, as we know, of grids and definitions. In the Romanian language one imposes the condition that the percentage of black boxes compared to the total number of boxes of the grid not to go over 15%.

Why 15%, and not more or less? This is the question to which this article tries to answer. (This question is due to Professor Solomon MARCUS - National Symposium of Mathematiques "Traian Lalesco", Craiova University, June 10, 1982).

First of all we present here a table which shows in a synthetic manner, a statistics on the grids containing a very small percentage of black boxes (of [2], pp. 27-29):

THE GRIDS-RECORDS

Grid dimension	Minimum number of registered black boxes	Percentage of black boxes	Number of grids-records constructed until June 1, 1982
8x8	0	0.000%	24
9x9	0	0.000%	3
10x10	3	3.000%	2
11x11	4	3.305%	1
12x12	8	5.555%	1
13x13	12	7.100%	1
14x14	14	7.142%	1
15x15	17	7.555%	1
16x16	20	7.812%	2

In this table, one can see that the larger the dimension of the grid, the larger is the percentage of black boxes, because the number of long words is reduced.

The current dimensions for grids go from 10x10 to 15x15.

One can notice that the number of the grids having a percentage of black boxes smaller than 8 is very reduced: the totals in the last column represent all the grids created in Romania since 1925 (the appearance of the first problems of cross words in Romania), until today. It is thus seen that the number of the grid-records is negligible when one compares it with the thousands of grids created. For this reason, the rule that imposed the percentage of the black boxes, should have established to be greater than 8%. But the cross words being puzzles, they must address to a large audience, thus one did not have to make these problems too difficult.

From which a percentage of black boxes at least equal to 10%.

They must be not too easy either, that is not to necessitate any effort from those who would compose them, from where a percentage of black boxes smaller than 20%. (If not, in effect, it becomes possible to compose grids wholly formed of words boxes of 2 or 3 letters).

To support the second assertion, one assumes that the average length of the words of a $n \times m$ grid with p black boxes is sensible equal to $\frac{2(n \cdot m - p)}{n + m + 2p}$ (from [3]. § 1, Prop. 4). For us, p is 20% of $n \cdot m$, therefore it results that

$$\frac{2(n \cdot m - \frac{20}{100} n \cdot m)}{n + m + 2\frac{20}{100} n \cdot m} \leq 3 \Leftrightarrow \frac{1}{n} + \frac{1}{m} \geq \frac{2}{15}.$$

Thus, for current grids having 20% of black boxes, the average lengths of the words would be smaller than 3.

Similarly at the beginnings of the puzzle of cross words the percentage of black boxes were not too large: thus in a grid from 1925 of 11x11, one counts 33 black boxes, therefore a percentage of 27.272% (from [2], p. 27).

While being developed, for these puzzles were imposed "stronger" conditions – that is a reduction in the black boxes.

For selecting a percentage between 10 and 20%, it is supposed that the peoples' predilection for round numbers was essential (the cross words are puzzles, no need for mathematic precision of sciences). That's why the rule of 15%.

A statistic (from [3], § 2), shows that the percentage of black boxes in the current grids is approximately 13.591%. The rule is thus relatively easy to follow and it can only attract new crossword enthusiasts.

To completely answer the proposed question, one would need to consider also some philosophical, psychological, and especially sociological aspects, especially those connected to the history of this puzzle, its ulterior development, and with its traditions.

REFERENCES

[1] Marcus Solomon, Edmond Nicolau, S. Stati – "Introducere in lingvistica matematică", Bucharest, 1966 (translated in Italian, Patron, Bologna, 1971; in Spanish, Teide, Barcelona, 1978).

[2] Andrei, Dr. N. – "Îndreptar rebusist", Editura Sport-Turism, Bucharest, 1981.

[3] Smarandache, Florentin – "A mathematical linguistic approach to Rebus", published in "Review roumaine de linguistique", Tome XXVIII, 1983, collection "Cahiers de linguistique théorique et appliquée", Tome XX, 1983, no. 1, pp. 67-76, Bucharest.

[Published in "Caruselul enigmistic", Bacău, Nr. 5, 1986, 2-6 May, pp. 29 and 31]

THE LANGUAGE OF SPIRITUAL REBUS DEFINITIONS

"The rebus' language" is somewhere at the border of the scientific language and, that, perhaps, having many common things with usual language too, and even with the musical one (the puzzles, because they have a certain acoustic resonance).

While the semantic deficiencies, having direct definitions (close to those from dictionary [3], pp. 50-56) of a language close to the scientific one (even to the usual one through the simple mode of expression) of "the grid's definitions". The language is close to the poetic one. There are even literary definitions (see [3], p. 57, [4]), which utilize literary stylistic procedures: like the metaphor, the comparison, the allegory, practice, etc. Later we will present a parallelism between the SCIENTIFIC LANGUAGE, POETIC LANGUAGE, REBUS' LANGUAGE ("THE GRIDS' DEFINITIONS") closely following the rules from [1] (chap. "Oppositions between the scientific language and the poetic one"), results which we will limit to the rebus' language.

SCIENTIFIC LANGUAGE	POETIC LANGUAGE	REBUS' LANGUAGE
- rational hypothesis	- emotional hypothesis	- rational + emotional hypothesis (reading the definition, you think for an instant, sometimes you go on a wrong road; when you err the answer (the corresponding word from the grid, you get enlightened and enthusiast).
- logical density	- density of suggestion	- logical density + suggestion (the definition must use very few words to explain a lot – logical density); to be unpublished, enlightening, emotional (density of suggestion).
- infinite synonymy	- absent synonymy	- reduced synonymy (not truly infinite, but not absurd); (two identical words from the grid cannot have more than one rebus definition; but a definition will be almost uniquely expressed, therefore the synonymy is quasi absent).
- absent anonymity	- infinite anonymity	- large anonymity (neither absent, nor infinite) (in the case of the definition, the meaning is up to the author:

		even if the reader understands something else, it will intervene the rational part, the word must fulfill the proper place in the grid, even the literary definitions, in the grids, don't have anymore an infinite anonymity, because here intervene also the rational part: the finding by all means of an answer: in the case of the theme grids with direct definitions, the anonymity is almost absent).
- artificial	- natural	- natural and artificial (in general the definitions have a natural character; but the definitions based on letter's puzzles (example, the definition "Night's beginning" has the answer "NI" have an artificial character).
- general	- singular	- singular and general (only the definitions based on the puzzles of letters may have a general character).
- translatable	- untranslatable	- translatable (in the sense that the definition has a logical meaning).
- the presence of style problems	- the absence of style problems	- the absence of style problems (the same definition cannot be used without changing the nuance – while a word in the grid can be defined in multiple ways).
- finitude in space, constant in time	- variability in space and time	- the variability in space and time, smaller variability than that from the poetic language.
- numerable	- innumerable	- innumerable
- transparent	- opaque	- semi-opaque (or semitransparent - at the

		beginning the definition seems opaque, until one finds the answer).
- transitive	- reflexive	- reflexive (except, again, the definitions based on games of letters, which have also a transitional character).
- independency on expression	- dependency on expression	- dependency on expression.
- independency on musical structure	- dependency on musical structure	- dependency on musical structure.
- paradigmatic	- syntagmatic	- syntagmatic
- concordance between the paradigmatic and syntagmatic distance	- non concordance between the paradigmatic and syntagmatic distance	- the paradigmatic and syntagmatic distance (are pairs of different words, word games, methods used ass in poetry).
- short contexts	- long contexts	- short contexts (1) (here it is closer to the scientific language, because it is taken into account the Latin proverb "*Non multa sed multum*"; from the anterior statistic investigations it resulted that the medium length of a (spiritual) rebus definition is 4.192 words: the definitions with letter puzzles usually have very few words.
- contextual dependency	- it tends towards expression independency	- contextual dependency (in the case of the theme grids it is also a small dependency; there exist also rare cases when a definition is dependent of an anterior definition (usually the definitions with letters or word games)).
- logic	- illogic	- logic
- denotation	- annotation	- connotation (if a definition would reveal the direct meaning of an word, we would have direct definitions (like in a

		dictionary)) and then we would totally loose “the surprise”, “the spirituality”, “the ingenious”, “the spontaneity” of thematic grids, the definitions with denotative character.
- routine	- creation	- creation and … experience (not to call it routine!)
-general stereotypes	- personal stereotypes	- personal stereotypes (it exists even the so called grids of “personal manner” – (see [3], pp. 56-58)
- explicable	- ineffable	- ineffable … which explains it! (Taken separately, the definition, not-seen as a question, is ineffable taken along, with the answer becomes explicable: in general, the definition presents also an ambiguity degree (more tracks for guidance) – otherwise it would be banal – a degree of indetermination: it is used many times the proper sense instead of the figurative one, or reciprocally defined it has also its own logic, which becomes tangible once one finds the answer).
- lucidity	- magic	- magic – lucidity (in accordance with those that are immediately anterior) (at the beginning the rebus language dominates the person, until he finds the “key” when he’ll become at his turn the dominant – the poetic language.
- predictable	- unpredictable	- at the beginning is unpredictable, and becomes predictable after solving it: (unpredictable converted in predictable) .

CONSIDERATIONS REGARDING THE SCIENTIFIC LANGUAGE AND "LITERARY LANGUAGE"

As in nature nothing is absolute, evidently there will not exist a precise border between the scientific language and "the literary" one (the language used in literature): thus there will be zones where these two languages intersect.

In [1], chapter "Instances between the scientific and poetic languages", Solomon Marcus presents the differences between these two, differences that make them closer.

We will skate a little on the edge of this material, presenting common parts of the scientific language and the literary language:

- both are geared to find the unpublished, the novelty
- both suppose a creative process (finding the solution of a problem means creation: writing of a phrase the same).
- both literature and science have an art of being taught, studied and learned (the methodology of teaching arithmetic, or Romanian language, etc.) .
- in science too there is an esthetic (for example: "the mathematical esthetic"), the same in literature there exists a logic (even the absurd of Eugene Ionesco, the myths of Mircea Eliade have their own specific logic: analogously, we can extend the idea to Tristan Tzara's Dadaism, which has a specific logic (of construction; one cuts words from newspapers, mix them, and then form verses).
- the scientific development implies a literary development in a special sense: it appeared, thus, the science-fiction literature in literary writings which use informations obtained by science: contemporaneous literature treats also scientific problems (for example Augustin Buzura wrote the roman "The absents" describing the life of a medical researcher: the engineer poet George Stanca introduces technical terms in his poems; one verse from his volume "Maximum tenderness" sounds: "$\sin^2 x + \cos^2 x = 1$"!); analogously the engineer poet Gabriel Chifu (the volume "An interpretation of the Purgatory") and mathematics professor Ovidiu Florentin, author of a volume even entitled "Formulas for the spirit" – each poem being considered as a momentous "formula" (depending of time, place, space, individual) for the spirit.
- even the writing of some contemporary novels inspired from the worker's and peasant's life requires a scientific documentation from the writers' part.

The literature has an esthetic influence for science; there exist mathematical metaphors (see [1], [2]) and, in general, we can say "scientific metaphors", one cannot know what ideas and relations will be discovered in science. The understanding degree (exegesis) of a poetry and of a literary text in general, depends also of the culture's degree of each individual, of his initiation (the seniority in that domain), of his scientific knowledge.

- there are many scientists who, besides their scientific works, write also literary works or related domains (for example, the memories book of the academician (mathematician) Octav Onicescu "On the life's roads", the renown Romanian physician Gheorghe Marinescu writes poems (using Dacic words), under the penname George Dinizvor, the great Ion Barbu – Dan Barbilian excelled as a poet and as a mathematician. The great poet Vasile Voiculescu was a good physician; and the mathematics professor Aurel M. Buricea writes poetry, analogously the mathematician Ovidiu Florentin –

Florentin Smarandache writes poems and mathematics articles; in the world literature we find the poet-mathematician Omar Khayyam and Lewis Caroll – Charles L. Dodgson), but writers that would do fundamental scientific or technical research don't quite exist!

REFERENCES

[1] Marcus, Solomon – "Poetica matematică", Ed. Academiei, Bucharest, 1970.

[2] Marcus, Solomon – "Introducere în lingvistica matematică", Bucharest, 1966.

[3] Andrei, Dr. N. – "Îndreptar rebusist", Ed. Sport-Turism, Bucharest, 1981.

[4] Magazine collection "Rebus", 1979-1982.

[5] Marcus, Solomon – "Limbajul poetic - limbajul matematic", in the "Orizont" magazine (Timişoara), 26 March 1982.

THE LETTERS' FREQUENCY (BY EQUAL GROUPS) IN THE ROMANIAN JURIDICAL TEXTS

Analyzing the deterioration's degree of the keys of a typing machine which functioned for more than 40 years at the clerk's office of a court of a Rumanian district (Vâlcea), one partitions them in the following groups:

1) Letters completely deteriorated (one cannot read anything anymore on the typewriter).
2) Letters from which one sees only one point, hardly perceptible.

……………………..

10) Letters from which is missing only one point.
11) Letters, which are seen perfectly, without anything missing.
12) Letters which, almost have not been touched, being covered with dust.

The following resultants were obtained:

1) E, A	7) O, C, U, D, Z
2) I	8) N
3) R	9) L
4) T	10) V, M
5) S	11) F, G, B, H, X, J, K
6) P	12) W, Q, Y

This classification is a little different of that of [1], because the letters A, Ă**,** Â are here counted as one letter: A, The same I and Î in I, S and Ş in S, T and Ţ in T.

By studying the chart of this text (from [2]), we obtain:

$$\alpha(j) = \frac{1}{23}\sum_{i=1}^{23}\left|\alpha(A_i)\right| \approx 2.348$$

thus the chart of the juridical language of current frequencies is much more larger than that of the cross words language: $\alpha(g) \approx 1.391$ and $\alpha(d_r) \approx 1.185$.

The letters P, Z and N realized the most spectacular jump:

$$\alpha(P) = 6\ ,\ \alpha(Z) = 7\ ,\alpha(N) = 8\,.$$

Perhaps this article surprises by its banality. But, whereas other authors spent month of calculations using computers, choosing certain books and counting the letters (!) by the computer, I have deducted this frequency of the letters in a few minutes (!), by a simple observation.

REFERENCES

[1] Marcus, Solomon – “Poetica matematică”, Editura Academiei, Bucharest, 1970 (translated in German, Athenäum, Frankfurt, 1973).

[2] Smarandache, Florentin – “A mathematical linguistic approach to Rebus”, Tome XXVIII, 1983, collection “Cahiers de linguistique théorique et appliquée”, Tome XX, 1983, No. 1, pp. 67-76, Bucharest.

MATHEMATICAL FANCIES AND PARADOXES

MISCELLANEA

1. Archimedes' "fixed point theorem": Give me a fixed point in space, and I shall lift the Earth".

2. MATHEMATICAL LINGUISTICS[1]

Poem by Ovidiu Florentin[2]

Definition

A word's sequence converges if it is found in a neighborhood of our heart.

*

The hermetic verses are linear equations.

*

Theorem

For any X there is no Y such that Y knows everything which X knows. And the reciprocal.

The proof is very intricate and long, and we will present it. We leave it to the readers to solve it!

**

Smarandache's law: Give me a point in space and I shall write the proposition behind it.

Final Motto

- O, MATHEMATICS, YOU, EXPRESSION OF THE ESSENTIAL IN NATURE!

1 Volume which includes this mathematical poem (pp. 39-41).

2 (Translated from Romanian by the author.) It is the mathematician's pen name. He wrote many poetical volumes (in Romanian and French), as "Legi de compoziție internă. Poeme cu…probleme!" (Laws of internal composition. Poems with…problems!), Ed. El Kitab, Fès, Morocco, 1982.

AMUSING PROBLEMS

1. Calculate the volume of a square.

(Solution: Volume = Area of the Base x Height = Side^2 x 0 = 0! We look at the square as an extreme case of parallelepiped with the height null.)

2. ? x 7 = 2?

(Solution: of course $\frac{2}{7} \times 7 = 2$!)

3. Ten birds are on a fence. A hunter shoots three of them. How many birds remain?

(Answer: **none**, because the three dead birds fell down from the fence and the other seven flew away!)

4. Ten birds are in a meadow. A hunter shoots three of them. How many birds remain?

(Answer: **three birds**, the dead birds, because the others flew away!)

5. Ten birds are in a cage. A hunter shoots three of them. How many birds remain?

(Answer: **ten birds**, dead and alive, because none could get out!)

6. Ten birds are up in the sky. A hunter shoots three of them. How many birds remain?

(Answer: **seven birds**, at last, those who are still flying and those that fell down!)

7. Prove that the equation $X = X + 2$ has two distinct solutions.

(Answer: $X = \pm\infty$!)

8. (Solving Fermat's last theorem) Prove that for any non-null integer n, the equation $X^n + Y^n = Z^n$, $XYZ \neq$, has at least one integer solution!

(Answer: (a) $n \geq 1$. Let $X_k = Y_k = Z_k = 2^k$, $k = 1, 2, 3, \ldots$ All $X_k \in N$, $K \geq 1$. $L = \lim_{k \to \infty} X_{k \in N}$. But $L = \infty \in N$, that is the integer infinite, and $\infty^n + \infty^n = \infty^n$! If n is even, the equation has eight distinct integer solutions: $X = Y = Z = \pm\infty$! Similarly, we take the negative infinite integer: - $\infty \in Z$]

(b) $n \leq -1$. Clearly there are at last eight distinct integer solutions: $X = Y = Z = \pm\infty$!)

WHERE IS THE ERROR IN THE BELOW DIOPHANTINE EQUATIONS ?

Statement:

(1) To solve in $\mathbb{Z}$ the equation: $14x + 26y = -20$.

"Resolution": The integer general solution is:

$$\begin{cases} x = -26k + 6 \\ y = 14k - 4 \end{cases} \quad (k \in \mathbb{Z})$$

(2) To solve in $\mathbb{Z}$ the equation: $15x - 37y + 12z = 0$.

"Resolution" The integer general solution is:

$$\begin{cases} x = k + 4 \\ y = 15k \qquad (k \in \mathbb{Z}) \\ z = 45k - 5 \end{cases}$$

(3) To solve in $\mathbb{Z}$ the equation: $3x - 6y + 5z - 10w = 0$.

"Resolution" the equation is written: $3(x - 2y) + 5z - 10w = 0$.

Since x, y, z, w are integer variables, it results that 3 divides z and that 3 divides w. I. e: $z = 3t_1$ $(t_1 \in \mathbb{Z})$ and $w = 3t_2$ $(t_2 \in \mathbb{Z})$.

Thus $3(x - 2y) + 3(5t_1 - 10t_2) = 0$ where $x - 2y + 5t_1 - 10t_2 = 0$.

Then: $\begin{cases} x = 2k_1 + 5k_2 - 10k_3 \\ y = k_1 \\ z = 3k_2 \\ w = 3k_3 \end{cases}$ with $(k_1, k_2, k_3 \in \mathbb{Z}^3)$,

constitute the integer general solution of the equation.

Find the error of each "resolution".

SOLUTIONS.

(1) $x = -26k + 6$ and $y = 14k - 4$ ($k \in \mathbb{Z}$) is an integer solution for the equation (because it verifies it), but it is not the general solution, because $x = -7$ and $y = 3$ verify the equation, they are a particular integer solution, but:

$\begin{cases} -26k + 6 = -7 \\ 14k - 4 = 3 \end{cases}$ implies that $k = \frac{1}{2}$ (does not belong to $\mathbb{Z}$).

Thus one cannot obtain this particular from the previous general solution.

The true general solution is: $\begin{cases} x = -13k + 6 \\ y = 7k - 4 \end{cases}$ $(k \in \mathbb{Z})$. (from [1])

(2) In the same way, $x = 5$, $y = 3$, $z = 3$ is a particular solution of the equation, but which cannot be obtained from the "general solution" because:

$$\begin{cases} k + 4 = 5 \quad \Rightarrow k = -1 \\ 15k = 3 \quad \Rightarrow k = \frac{1}{5} \\ 45k - 5 = 3 \Rightarrow k = \frac{8}{45} \end{cases},$$

contradictions.

The integer general solution is: $\begin{cases} x = k_1 \\ y = 3k_1 + 12k_2 \\ z = 8k_1 + 37k_2 \end{cases}$ (with $(k_1, k_2) \in \mathbb{Z}^2$, cf. [1]).

(3) The error is that: "3 divides ($5z - 10w$)" does not imply that "3 divides z and 3 divides w". If one believes that one loses solutions, then this is true because

$(x, y, z, w) = (-5, 0, 5, 1)$ constitutes a particular integer solution, which cannot be obtained from the "solution" of the statement.

The correct resolution is: $3(x-2y)+5(z-2w)=0$, that is $3p_1+5p_2=0$, with $p_1 = x-2y$ in $\mathbb{Z}$, and $p_2 = z-2w$ in $\mathbb{Z}$.

It results that: $\begin{cases} p_1 = -5k = x-2y \\ p_2 = 3k = z-2w \end{cases}$ in $\mathbb{Z}$.

From which one obtains the integer general solution:

$$\begin{cases} x = 2k_1 - 5k_2 \\ y = \quad k_1 \\ z = \qquad 3k_2 + 2k_3 \\ w = \qquad\qquad k_3 \end{cases} \quad \text{with } (k_1, k_2, k_3) \in \mathbb{Z}^3$$

[1] One can find these solutions using: Florentin SMARANDACHE - "Un algorithme de résolution dans l'ensemble des numbers entiers pour les équations linéaires".

WHERE IS THE ERROR ON THE BELOW INTEGRALS ?

Let the function $f:\mathbb{R}\to\mathbb{R}$ be defined by $f(x) = 2\sin x\ \cos x$.

Let us calculate its primitive:

(1) First method.

$$\int 2\sin x\ \cos x\ dx = 2\int u\ du = 2\frac{u^2}{2} = u^2 = \sin^2 x, \text{ with } u = \sin x.$$

One thus has $F_1(x) = \sin^2 x$.

(2) Second method:

$$\int 2\sin x\ \cos x\ dx = -2\int \cos x(-\sin x)dx = -2\int v\ dv = -v^2,$$

thus $F_2(x) = -\cos^2 x$

(3) Third method:

$$\int 2\sin x\ \cos x\ dx = \int \sin 2x\ dx = \frac{1}{2}\int (\sin 2x)\ 2dx = \frac{1}{2}\int \sin t\ dt = -\frac{1}{2}\cos t$$

thus $F_3(x) = -\frac{1}{2}\cos 2x$.

One thus obtained 3 different primitives of the same function.

How is this possible?

Answer: There is no error! It is known that a function admits an infinity of primitives (if it admits one), which differ only by one constant.

In our example we have:

$F_2(x) = F_1(x) - 1$ for any real x, and $F_3(x) = F_1(x) - \frac{1}{2}$ for any real x.

WHERE IS THE ERROR IN THE BELOW REASONING BY RECURRENCE ?

At an admission contest at an University, was given the following problem:

"Find the polynomials $P(x)$ with real coefficients such that $xP(x-1)=(x-3)P(x)$, for all x real."

Some candidates believed that they would be able to show by recurrence that the polynomials of the statement are those which verify the following property: $P(x)=0$ for all natural values.

In fact, they said, if one puts $x=0$ in this relation, it results that $0\cdot P(-1)=-3\cdot P(0)$, therefore $P(0)=0$.

Likewise, with $x=1$, one has: $1\cdot P(0)=-2\cdot P(1)$, therefore $P(1)=0$, etc.

Let's suppose that the property is true for ($n-1$), therefore $P(n-1)=0$, and we are looking to prove it for n:

One has: $n\cdot P(n-1)=(n-3)\cdot P(n)$, and since $P(n-1)=0$, it results that $P(n)=0$.

Where the proof failed?

Answer: If the candidates would have checked for the rank $n=3$, they would have found that: $3\cdot P(2)=0\cdot P(3)$ thus $0=0\cdot P(3)$, which does not imply that $P(3)$, is null: in fact this equality is true for any real $P(3)$.

The error, therefore, is created by the fact that the implication: "$(n-3)\cdot P(n)=n\cdot P(n-1)=0\Rightarrow P(n)=0$" is not true.

One can find easily that $P(x)=x(x-1)(x-2)k$, $k\in\mathbb{R}$.

WHERE IS THE ERROR?

Given the functions $f,g:\mathbb{R}\to\mathbb{R}$, defined as follows:

$$f(x)=\begin{cases} e^x, & x\le 3 \\ e^{-x}, & x>3 \end{cases} \quad \text{and } g(x)=\begin{cases} x^2, & x\le 0 \\ -2x+7, & x>3 \end{cases}$$

Compute $f\circ g$.

"*Solution*": We can write:

$$f(x)=\begin{cases} e^x, & x\le 0 \\ e^x, & 0<x\le 3 \\ e^{-x}, & x>0 \end{cases} \qquad \text{and} \qquad g(x)=\begin{cases} x^2, & x\le 0 \\ -2x+7, & 0<x\le 3 \\ -2x+7, & x>3 \end{cases}$$

from where

$$(f\circ g)(x)=f(g(x))=\begin{cases} e^{x^2}, & x\le 0 \\ e^{-2x+7}, & 0<x\le 3 \\ e^{2x-7}, & x>3 \end{cases}$$

and $f \circ g : \mathbb{R} \to \mathbb{R}$.

Correct solution:

$$f \circ g = f(g(x)) = \begin{cases} e^{g(x)}, & \text{if } g(x) \le 3 \\ e^{-g(x)}, & \text{if } g(x) > 3 \end{cases} \qquad f \circ g : \mathbb{R} \to \mathbb{R}$$

$$g(x) \le 3 \Rightarrow \begin{cases} x^2 \le 3 \quad \Rightarrow x \in [-\sqrt{3}, 0] \\ or \\ -2x + 7 \le 3 \Rightarrow x \in [2, +\infty) \end{cases}$$

$$g(x) > 3 \Rightarrow \begin{cases} x^2 > 3 \quad \Rightarrow x \in (-\infty, -\sqrt{3}) \\ or \\ -2x + 7 > 3 \Rightarrow x \in (0, 2) \end{cases}$$

Therefore

$$f \circ g)(x) = \begin{cases} e^{-x^2}, & x \in (-\infty, -\sqrt{3}) \\ e^{x^2}, & x \in [-\sqrt{3}, 0) \\ e^{2x-7}, & x \in (0, 2) \\ e^{2x-7}, & x \in [2, +\infty) \end{cases}$$

[Published in “Gazeta matematică”, nr.7/1981, Anul LXXXVI, pp. 282-283.]

WHERE IS THE ERROR IN THE BELOW SYSTEM OF INEQUALITIES ?

Solve the following inequalities system:

$$\begin{cases} x \ge 0 & (1) \\ y \ge 0 & (2) \\ x - 2y + 3z \ge 0 & (3) \\ -3x - y + 4z \ge 4 & (4) \end{cases}$$

“Solution”: Multiply the third inequality by 3 and add it to the fourth inequality. The sense will be conserved. It results:

$-7y + 13z \ge 4$, or $z \ge \frac{1}{13}(7y + 4)$.

Therefore, $x \ge 0$ and $y \ge 0$ (from the inequalities (1) and (2))

and $z \ge \frac{1}{13}(7y + 4)$ (*).

But $x = 13 \geq 0$, $y = 0 \geq 0$, and $z = 2 \geq \frac{4}{13} = \frac{1}{13}(7 \cdot 0 + 4)$ verifies (*). But we observe that it does not verify the inequalities system, because substituting in the fourth inequality we obtain: $-3 \cdot 13 - 0 + 4 \cdot 2 \geq 4$ which is not true.

Where is the contradiction?

Solution.

The previous solution is incomplete. We didn't intersect all four inequalities. Giving a geometrical interpretation in $\mathbb{R}^3$, and writing the inequalities as equations, we have, in fact, four planes, each dividing the space in semi spaces. Therefore, the system's solution will be formed by the points which belong to the intersection of those four semi spaces, (each inequality determines a semi space). The inequality obtained by adding the third inequality with the fourth represents, is, in fact, another semi space that includes the system's solution, and it does not simplify the system (in the sense that we cannot eliminate any of the system's inequalities).

Therefore $x = 0$, $y = 3$, $z = \frac{5}{13}$ verifies (*) but it does not verify, this time, the third inequality (although the fourth one is verified).

THE ILLOGICAL MATHEMATICS!

Find a "logic" for the following statements:

(1) $4 - 5 \approx 5!$

(2) 8 divided by two is equal to zero!

(3) 10 minus 1 equals 0.

(4) $\int f(x)\ dx = f(x)!$

(5) 8+8=8!

Solutions:

These mathematical fantasies are entertainments, amusing problems; they disregard current logic, but having their own "logic", fantasist logic: thus

(1) can be explained if one does not consider "4 - 5" as the writing of "4 minus 5" but that of "from 4 to 5"; from which a reading of the statement "$4 - 5 \approx 5$" should be: "between 4 and 5, but closer to 5".

(2) 8 can be divided by two … in the following way:…, i. e. it will be cut into two equal parts, which are equal to "0" above and below the cutting line!

(3) "10 minus 1" can be treated as: the two typographical characters 1, 0 minus the 1, which justifies that there remains the character 0.

(4) The sign will be considered as the opposite function of the integral.

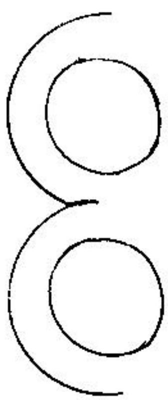
(5) The operation "$\infty + \infty = \infty$" is true: writing it vertically:

∞
$+$
∞
$=$
∞

which, transposed horizontally (by a mechanic rotation of the graphic signs) will give us the statement: “$8+8=8$”.

OPTICAL ILLUSION
(Mathematical Psychology)

What digit is it, 8 or 3?



[Answer: Both of them!]

1. EPMEK = Reverse of Kempe.

2. DEDE/KIND = DedeKind’s cut.

3.
B
R
O = Angle of Brocard.
C
A
R
D

4. •
BRIANCHON = Point of Brianchon.

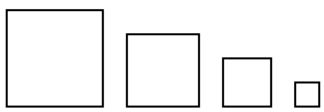
5. $\begin{vmatrix} \mathrm{SYL} \\ \mathrm{VES} \\ \mathrm{TER} \end{vmatrix}$ = Determinant of Sylvester.

6. E A O T E E
r t sh n s = The Sieve of Eratosthenes.

7. $\begin{array}{ccccc} & & A & & \\ & R & & C & \\ & & T & & S \\ D & & E & & S \end{array}$ = Foliate curve of Descartes.

8. $\begin{pmatrix} M & R & X \\ R & A & I \\ X & I & T \end{pmatrix}$ = Symmetrical matrix.

9. $\overline{\mathrm{SHEFFER}}$ = Bar of Sheffer.

10.  = Method of the smallest squares.

11. $\begin{pmatrix} J&1&0&0&0&0 \\ 0&\varnothing&1&0&0&0 \\ 0&0&R&1&0&0 \\ 0&0&0&D&1&0 \\ 0&0&0&0&A&1 \\ 0&0&0&0&0&N \end{pmatrix}$ = Matrix of Jordan.

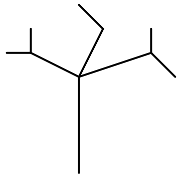
12. NOITCNUF = Inverse function.

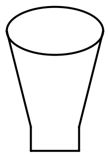
13. SERUGIF = Inverse figures.

14. $\begin{array}{cccccccc} & R & & V & & R & & V \\ M & & K & & M & & K & \\ & A & & O & & A & & O \end{array}$ = Markov Chains.

15. $\dfrac{\text{USA}}{\text{WEST EUROPE}}$ = Harmonious rapport.

16. $\frac{\text{USA}}{\text{USSR}}$ = Unharmonious rapport.

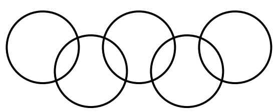
17.  = Tree.

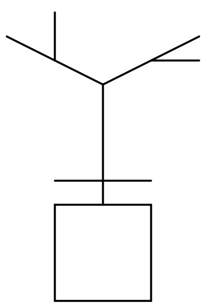
18.  = Convergent filter.

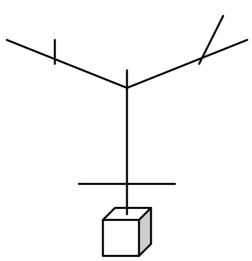
19.
A
P S

O U = Apollonius' circle.

L I
O N

20.  = Fascicles of circles.

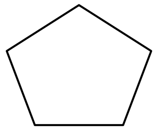
21.  = Square root.

22.  = Cubic root

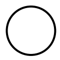
23. $X^{\infty} + Y^{\infty} = Z^{\infty}$ = Fermat's last theorem

24. I-W-A-S-A-W-A = Iwasawa's decomposition

25. R E
O M = Latin square!

26.  = The Pentagon!

27. Ø = *Reductio ad absurdum.*

28.  = Ring.

29. F N
U O = Convex function.
N I
C T

30. P N S = Non-collinear points.
I T
O

31. G
R P = Group of rotations.
O U

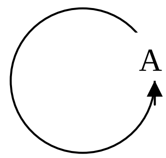
32. ELEMENTS = Non-disjoint elements.

33. M
X A = Circular matrix.
I T
R

O L
34. P I = 7-gon.
N
O G

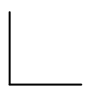
35. SPA
CE = Compact space.

36. A
L
G
E = Higher algebra
B
R
A

37. 

= Vicious circle

38. A
R
I
T
H
M
E
T
I
C
= The higher arithmetic.

39. 
= Square angle.

40. SYMBOL OF (LEOPOLD) KRONECKER = L.K.

41. KOLMOGOROV'S SPACE = USSR.

42. LANGUAGE OF CHOMSKY = American.

43. GRAMMAR OF KLEENE = English.

44. CATASTROPHIC POINT = Atom bomb.

45. MACHINE OF TURING = Motor car.

46. NUMBER OF GOLD = 79 (Chemically).

47. FLY OF LA HIRE = Insect.

48. MOMENT OF INERTIA = Apathy.

49. AXIOM OF SEPARATION = Divorce.

50. CLOSED SET = Prisoners.

51. RUSSIAN MULTIPLICATION = Conquest.

52. SLIPS OF MÖBUS = Bathing trunks.

53. SINGULAR CARDINAL	=	Mazarin (1602-1661, France).
54. CLAN OF LEBESGUE	=	His family.
55. SPHERE OF RIEMANN	=	Head.
56. MATHEMATICAL HOPE	=	Fields prize.
57. CRITICAL WAY	=	Slope.
58. BOTTLE OF KLEIN	=	Beer bottle.
59. CONSTANT OF EULER	=	Mathematics.
60. CONTRACTING FUNCTION	=	Frost.
61. BILINEAR COMBINATION	=	Concubine.
62. HARDY SPACE	=	England.
63. INTRODUCTION TO ALGEBRA!	=	AL.
64. INTRODUCTORY ECONOMETRICS	=	ECO.
65. BOREL BODY	=	Corpse.
66. CHOICE FUNCTION	=	Marriage.
67. GEOMETRICAL PLACES	=	ATHENA, ERLANGEN, etc.

[Published in GAMMA, Year IX, Nr. 1, November 1986.]

MATHEMATICAL LOGIC

How many propositions are true and which ones from the following:
1. There exists one false proposition amongst those n propositions.
2. There exist two false propositions amongst those n propositions.

…………………………………………………………………….

… There exist i false propositions amongst those n propositions.

…………………………………………………………………….

n. There exist n false propositions amongst those n propositions.

(This is a generalization of a problem proposed by professor FRANCISCO BELLOT ROSADO, in the journal NUMEROS, No. 9/1984, p. 69, Canary Island, Spain.)

Comments:

Let P_i be the proposition i, $1 \le i \le n$. If n is even, then the propositions $1, 2, ..., \frac{n}{2}$ are true and the rest are false. (We start our reasoning from the end; P_n cannot be true, therefore P_1 is true; then P_{n-1} cannot be true, then P_2 is true, etc.)

Remark: If n is odd we have a **paradox**, because if we follow the same solving method we find that P_n is false, which implies that P_1 is true; P_{n-1} false, implies that P_2 is true,…, $P_{\frac{n+1}{2}}$ false implies $P_{n+1-\frac{n+1}{2}}$ true, that is $P_{\frac{n+1}{2}}$ false implies $P_{\frac{n+1}{2}}$ true, which is absurd.

If $n = 1$, we obtain a variant of liar's paradox ("I lie" is true or false?)

1. There is a false proposition in this rectangle.

Which is obviously a paradox.

PARADOX OF RADICAL AXES

Property: The radical axes of n circles in the same plan, taken two by two, whose centers are not aligned, are convergent.

"Proof" by recurrence on $n \ge 3$.

For the case $n = 3$ it is known that 3 radical axes are concurrent in a point which is called the radical center. One supposes that the property is true for the values smaller or equal to a certain n.

To the n circles one adds the $(n+1)$-th circle.

One has (1): the radical axes of first n circles are concurrent in M.

Let us take 4 arbitrary circles, among which is the $(n+1)$-th.

Those have the radical axes convergent, in conformity with the recurrence hypothesis, in the point M (since the first 3 circles, which belong to n circles of the recurrence hypothesis, have their radical axes concurrent in M).

Thus the radical axes of $(n+1)$ circles are convergent, which shows that the property is true for all circles $n \ge 3$ of N.

AND YET, one can build the following counterexample:

Consider the parallelogram $ABCD$ which does not have any right angle.

Then one builds 4 circles of centers A, B, C and D respectively, and of the same radius. Then the radical axes of the circles $e(A)$ and $e(B)$, respectively $e(C)$ and $e(D)$, are two lines, which are medians of the segments AB and CD respectively.

Because (AB) and (CD) are parallel, and that the parallelogram does not have any right angle, it results that the two radical axes are parallel, i.e. they never intersect.

Can we explain this (apparent!) contradiction with the previous property?

Response: The "property "is true only for $n = 3$. However in the demonstration suggested one utilizes the premise (distorted) according to which for $m + 4$ the property would be true. To complete the proof by recurrence it would have been necessary to be able to prove that $P(3) \Rightarrow P(4)$, which is not possible since $P(3)$ is true but the counterexample proves that $P(4)$ is false.

A CLASS OF PARADOXES

Let A be an attribute and non-A its negation.

P1. ALL IS "A", THE "NON-A" TOO.

Examples:

E_{11}: All is possible, the impossible too.

E_{12}: All are present, the absentee too.

E_{13}: All is finite, the infinite too.

P2. ALL IS "NON-A", THE "A" TOO.

Examples:

E_{21}: All is impossible, the possible too.

E_{22}: All are absent, the present too.

E_{23}: All is infinite, the finite too.

P3. NOTHING IS "A" NOT EVEN THE "A".

Examples:

E_{31}: Nothing is perfect, not even the perfect.

E_{32}: Nothing is absolute, not even the absolute.

E_{33}: Nothing is finite, not even the finite.

Remark: $P1 \Leftrightarrow P2 \Leftrightarrow P3$.

More generally: ALL (verb) "A", the "NON-A" too.

Of course, from these appear unsuccessful paradoxes, but the proposed method obtains beautiful ones.

Look at a pun, which reminds you of Einstein:

All is relative, the (theory of) relativity too! So:

The shortest way between two pints is the meandering way!

The unexplainable is, however, explained by this word: "unexplainable"!

[Presented at "The Eugene Strens Memorial on Intuitive and Recreational Mathematics and its History", University of Calgary, Alberta, Canada; July 27 – August 2, 1986.

Partially published in “Beta”, Craiova, 1987; “Gamma”, Braşov, 1987; and “Abracadabra”, Salinas (California), USA, 1993-4.]

Articles,
notes,
generalizations,
paradoxes,
miscellaneous
in
Mathematics,
Linguistics,
and
Education.

ISBN 1-59973-048-0
53995>
9 781599 730486