ACTA ACADEMIAE PAEDAGOGICAE AGRIENSIS

NOVA SERIES TOM. XXXI.

SECTIO MATHEMATICAE

REDIGUNT
MIKLÓS HOFFMANN,
KÁLMÁN LIPTAI,
FERENC MÁTYÁS

ESZTERHÁZY KÁROLY FŐISKOLA
EGER • 1774

EGER, 2004

AZ ESZTERHÁZY KÁROLY FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI
ÚJ SOROZAT XXXI. KÖTET

TANULMÁNYOK A MATEMATIKAI TUDOMÁNYOK KÖRÉBŐL

SZERKESZTI
HOFFMANN MIKLÓS, LIPTAI KÁLMÁN, MÁTYÁS FERENC

EGER, 2004

ACTA ACADEMIAE PAEDAGOGICAE AGRIENSIS

NOVA SERIES TOM. XXXI.

SECTIO MATHEMATICAE

REDIGUNT
FERENC MÁTYÁS, MIKLÓS HOFFMANN, KÁLMÁN LIPTAI

EGER, 2004

ISSN 1216–6014

EMTEX—JATEX

A kiadásért felelős:
az Eszterházy Károly Főiskola rektora
Megjelent az EKF Líceum Kiadó gondozásában
A szedés az EMTEX–JATEX szo"vegformázó programmal to"rtént
Igazgató: Hekeli Sándor
Felelős szerkesztő: Rimán János
Műszaki szerkesztő: Béres Zsuzsanna
Megjelent: 2005. január Példányszám: 80

Készült: B. V. B. Nyomda és Kiadó Kft., Eger
Ügyvezető: Budavári Sándor

EKF
LÍCEUM KIADÓ

PRIME NUMBERS AND CYCLOTOMY

Panayiotis G. Tsangaris (Athens, Greece)

Abstract. First, an explicite expression for $(1-\zeta^k)^{-1}$, where $\zeta=\exp(2\pi i/n)$, is given, in the form of a polynomial in ζ, with rational coefficients. Then a new primality criterion is obtained, which involves the greatest integer function. Further, using a result due to Yu.I. Vološin [10], we transform this criterion into a series of criteria involving rational expressions of ζ [one of these criteria involves the numbers $(1-\zeta^k)^{-1}$, $1\leq k\leq n-1$]. Finally, these criteria are refined to a trigonometric primality criterion, that involves only sums of cosines.

AMS Classification Number: 11A51, 11R18

Introduction

Denote by $F_n(x)$ the n-th cyclotomic polynomial, while ϕ will denote Euler's function and $\zeta = \exp(2\pi i/n)$. Given two polynomials $f(v)$, $g(v)$ in variable v, denote by $R_v(f(v), g(v))$ their resultant.

In Section 1 we express $(1-\zeta^k)^{-1}$, explicitly, in the form of a polynomial in ζ, by employing a series of new properties of the cyclotomic polynomial (Theorems 1.1 and 1.2).

In Section 2 a new primality criterion is obtained. Our primality criterion (Theorem 2.1) extends a previous result of author [7] which improves upon classical result of Hacks [5].

In Section 3 the result of (Section 2) is given in "cyclotomic" form by using roots of unity and trigonometric functions. The key result for such a "cyclotomic" modification is a Theorem of Yu. I. Vološin [10] expressing $[a/n]$ by means of a primitive root of 1 of order n. Specifically, our Theorem 3.1 is a first primality criterion for n formulated in terms of ζ and involving $(1-\zeta^k)^{-1}$, $1 \leq k \leq n-1$. To calculate the inverse of $(1-\zeta^k)$ (Corollary 1.4), we thus obtain a second "cyclotomic" primality criterion (Theorem 3.2). The "trigonometric elaboration" of this result leads to our final Theorem 3.4, which is a "trigonometric" primality criterion.

1. Expressing $(1-\zeta^k)^{-1}$ as a polynomial in ζ

Theorem 1.1. *Let n, s be natural numbers and let $d = (n, s)$. Then*

$$R_v(v^s - x^s, F_n(v)) = \begin{cases} F_{n/d}(x^s)^{\phi(n)/\phi(n/d)} \text{ for } n > 1 \text{ except for } d = n = 2, \\ -F_1(x^s) = 1 - x^s \text{ for } d = n = 2, \\ (-1)^{s+1}F_1(x^s) = (-1)^{s+1}(x^s - 1) \text{ for } n = 1. \end{cases}$$

Proof. Let $R(x) = R_v(v^s - x^s, F_n(v))$, $G(x) = F_{n/d}(x^s)^{\phi(n)/\phi(n/d)}$ and $\rho_1, \rho_2, \ldots, \rho_s$ be the s-th roots of unity. Then $\rho_1 x, \rho_2 x, \ldots, \rho_s x$ are the roots of $v^s - x^s$ (for x fixed). Hence

$$R(x) = F_n(\rho_1 x) \cdots F_n(\rho_s x).$$

Let ξ be a root of $R(x)$. Hence, $F_n(\rho_k \xi) = 0$ for some k, with $1 \leq k \leq s$, i.e. $\rho_k \xi$ is a root of $F_n(v)$. Thus, $\rho_k \xi$ is a primitive n-th root of unity. Set $\rho_k \xi = \zeta$, then $\xi^s = \zeta^s$. But the order of ζ^s is n/d. Hence ξ^s is a primitive n/d-th root of unity, i.e.

$$F_{n/d}(\xi^s) = 0.$$

Hence,

$$F_{n/d}(\xi^s)^{\phi(n)/\phi(n/d)} = 0,$$

i.e. ξ is a root of $G(x)$. Hence, every root of $R(x)$ is a root of $G(x)$, i.e.

$$R(x) \mid G(x). \tag{1}$$

Also

$$\deg G(x) = \deg R(x) = s\phi(n). \tag{2}$$

From (1) and (2) we have:

$$G(x) = cR(x), \quad \text{where} \quad c \text{ is a (rational) constant.} \tag{3}$$

Hence $G(0) = cR(0)$, that is

$$F_{n/d}(0)^{\phi(n)/\phi(n/d)} = cF_n(0)^s. \tag{4}$$

To derive the sought formula it suffices now to evaluate the constant c. We have to examine two cases:

(a) If $n > 1$. In case $d \neq n$, then $n/d > 1$. Also $F_n(0) = 1$ and $F_1(0) = -1$. Then, in view of (4) we have $c = 1$. In case $d = n > 1$, we have in view of (4) that

$$c = (-1)^{\phi(n)} = \begin{cases} -1, & \text{if} \quad n = 2, \\ 1, & \text{if} \quad n > 2. \end{cases}$$

(b) If $n = 1$, then (4) implies that

$$c = \begin{cases} 1, & \text{if } s \text{ is odd,} \\ -1, & \text{if } s \text{ is even.} \end{cases}$$

Remark. Theorem 1.2 should be considered as closely related to a corresponding Theorem of T. Apostol [1] on the resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$.

Theorem 1.2. *Let n, s be natural numbers. Denote by $\rho_1 = 1, \rho_2, \ldots, \rho_s$ all the s-th roots of unity, and let*

$$K_n^s(x) \equiv F_n(\rho_1 x) \cdots F_n(\rho_s x) - F_n(\rho_1) \cdots F_n(\rho_s).$$

Then:
(i) $(x^s - 1) | K_n^s(x)$.
(ii) If $n \not| s$, then

$$(1 - \zeta^s)^{-1} = L_n^s(\zeta)/R(v^s - 1, F_n(v)),$$

where

$$L_n^s(x) = K_n^s(x)/(x^s - 1).$$

Proof. The numbers $\rho_1, \rho_2, \ldots, \rho_s$ form a cyclic group. Hence

$$K_n^s(\rho_k) = F_n(\rho_1 \rho_k) \cdots F_n(\rho_s \rho_k) - F_n(\rho_1) \cdots F_n(\rho_s) = 0 \quad \text{for} \quad k = 1, 2, \ldots, s.$$

Also $\rho_1 x, \ldots, \rho_s x$ are the roots of $v^s - x^s = 0$ (for x fixed). Thus

$$K_n^s(x) = R_v(v^s - x^s, F_n(v)) - R(v^s - 1, F_n(v))$$

is a polynomial of x with integer coefficients. Since every ρ_k is a root of $K_n^s(x)$, part (i) follows immediately. Then

$$L_n^s(\zeta) = K_n^s(\zeta)/(\zeta^s - 1)$$

and so

$$K_n^s(\zeta) = -F_n(\rho_1) \cdots F_n(\rho_s) = -R(v^s - 1, F_n(v)).$$

In conclusion

$$(1 - \zeta^s)^{-1} = L_n^s(\zeta)/R(v^s - 1), F_n(v)).$$

Theorem 1.3. *Let n, k be natural numbers such that $n > 1$, $n \not| k$ and let $d = (n, k)$. Define*

$$K_n^k(x) = F_{n/d}(x^k)^{\phi(n)/\phi(n/d)} - F_{n/d}(1)^{\phi(n)/\phi(n/d)}.$$

Then $x^k - 1$ is a divisor of $K_n^k(x)$, and

$$(1-\zeta^k)^{-1} = L_n^k(\zeta)/F_{n/d}(1)^{\phi(n)/\phi(n/d)},$$

where

$$L_n^k(x) = K_n^k(x)/(x^k - 1).$$

Proof. Immediate by using Theorems 1.1 and 1.2.

Corollary 1.4. *If n is a prime and $k < n$, then we have*

$$(1-\zeta^k)^{-1} = \frac{1}{n} \sum_{1 \le w \le n-1} w\zeta^{k(n-w-1)}.$$

Proof. Here $(n,k) = 1$ and $F_n(1) = n$, so by Theorem 1.3 we have

$$L_n^k(x) = (F_n(x^k) - F_n(1))/(x^k - 1) = \sum_{1 \le w \le n-1} wx^{k(n-w-1)},$$

which proves the corollary.

2. A Primality Criterion

The known formula of Hacks [5, p. 205] for the g.c.d. of two natural numbers

$$(n,j) = 2 \sum_{1 \le i \le n-1} [ji/n] - jn + j + n$$

together with the fact that n is prime if and only if $\sum_{1 \le j \le m} (n,j) = m$ where $m = [\sqrt{n}\,]$ implies the following:

Theorem 2.1. *Let n be a natural number with $n > 1$, $m = [\sqrt{n}\,]$ and*

$$g(n) = 4 \sum_{\substack{1 \le j \le m \\ 1 \le i \le n-1}} [ji/n] - (m-1)m(n-1).$$

Then the following hold true:
(i) n is prime if and only if $g(n) = 0$.
(ii) n is composite if and only if $g(n) > 0$.

3. Prime numbers, roots of unity, cyclotomy and trigonometry

By Vološin's Theorem [10] we have:

$$\left[\frac{a}{n}\right] = \frac{a}{n} - \frac{n-1}{2n} - \frac{1}{n} \sum_{1 \le s \le n-1} \frac{\zeta^{s(a+1)}}{1-\zeta^{s}} \tag{5}$$

for any pair of (positive) integers a, n. Hence by (5) and Theorem 2.1 we have the following:

Theorem 3.1. *Let n be a natural number with $n > 1$ and $m = [\sqrt{n}\,]$. Then, n is prime if and only if*

$$2 \sum_{\substack{1 \le j \le m \\ 1 \le t,k \le n-1}} \frac{\zeta^{k(tj+1)}}{1-\zeta^{k}} = m(n-1).$$

Theorem 3.2. *Let n be a natural number with $n > 1$ and $m = [\sqrt{n}\,]$. Then n is prime if and only if*

$$2 \sum_{\substack{1 \le j \le m \\ 1 \le t,k \le n-1}} \frac{\zeta^{tjk}(1-\zeta^{k})}{\zeta^{k(n-1)} + \zeta^{k} - 2} = m(n-1). \tag{6}$$

Proof. If n is a prime, by Theorem 3.1 and Corollary 1.4 we obtain:

$$\frac{2}{n} \sum_{\substack{1 \le j \le m \\ 1 \le t,k \le n-1}} \zeta^{(tj+1)k} \sum_{1 \le w \le n-1} w\zeta^{k(n-w-1)} = m(n-1). \tag{7}$$

Let $\zeta^{k} = 1/z$. Clearly $\zeta^{k} \neq 1$, i.e. $z \neq 1$. Therefore

$$\sum_{1 \le w \le n-1} w\zeta^{k(n-w-1)} = \frac{1}{z^{n-2}} \sum_{1 \le w \le n-1} wz^{w-1} = \frac{n(\zeta^{k(n-1)} - 1)}{\zeta^{k(n-1)} + \zeta^{k} - 2}. \tag{8}$$

By (7) and (8) follows (6).

Assume now that (6) holds true. We have $\zeta^{k(n-1)} + \zeta^{k} - 2 \neq 0$ and $\zeta^{k(n-1)} \neq 1$ because $\zeta^{k} \neq 1$. Also, the following hold true:

$$\frac{1-\zeta^{k}}{\zeta^{k(n-1)} + \zeta^{k} - 2} = \frac{1}{\zeta^{k(n-1)} - 1}.$$

Hence

$$\frac{\zeta^{tjk}(1-\zeta^{k})}{\zeta^{k(n-1)} + \zeta^{k} - 2} = \frac{\zeta^{k(tj+1)}}{1-\zeta^{k}}.$$

Hence by our assumption we have:

$$m(n-1) = 2 \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\zeta^{tjk}(1-\zeta^k)}{\zeta^{k(n-1)}+\zeta^k-2} = 2 \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\zeta^{k(tj+1)}}{1-\zeta^k}.$$

Finally, by Theorem 3.1, n is prime Q.E.D.

Our next Lemma 3.3 aims at transforming the above Theorem 3.2 into a "trigonometric" primality criterion.

Lemma 3.3. *Let m, n be natural numbers with $n > 1$ and $m = [\sqrt{n}\,]$. Then*

$$2 \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\zeta^{tjk}(1-\zeta^k)}{\zeta^{k(n-1)}+\zeta^k-2} = - \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n}.$$

Proof. The following hold true

$$\zeta^{tjk}(1-\zeta^k) = 2\sin\frac{\pi k(2tj+1)}{n}\sin\frac{\pi k}{n} - 2i\sin\frac{\pi k}{n}\cos\frac{\pi k(2tj+1)}{n}. \qquad (9)$$

Also

$$\zeta^{k(n-1)}+\zeta^k-2 = -4\sin^2\frac{\pi k}{n}. \qquad (10)$$

From (9) and (10) we obtain:

$$2 \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\zeta^{tjk}(1-\zeta^k)}{\zeta^{k(n-1)}+\zeta^k-2} = - \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\sin\frac{\pi k(2tj+1)}{n}}{\sin\frac{\pi k}{n}} + i \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\cos\frac{\pi k(2tj+1)}{n}}{\sin\frac{\pi k}{n}}. \qquad (11)$$

Moreover

$$- \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\sin\frac{\pi k(2tj+1)}{n}}{\sin\frac{\pi k}{n}} = - \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \sin\frac{2\pi tjk}{n}\cot\frac{\pi k}{n} - \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n}. \qquad (12)$$

On the other hand

$$\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\cos\frac{\pi k(2tj+1)}{n}}{\sin\frac{\pi k}{n}} = \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n}\cot\frac{\pi k}{n} - \sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \sin\frac{2\pi tjk}{n}. \quad (13)$$

The following hold true

$$\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \sin\frac{2\pi tjk}{n}\cot\frac{\pi k}{n} = 0, \quad (14)$$

$$\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n}\cot\frac{\pi k}{n} = 0 \quad (15)$$

and

$$\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \sin\frac{2\pi tjk}{n} = 0. \quad (16)$$

Finally, by (11) together with (12), (13), (14), (15) and (16) we obtain:

$$2\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \frac{\zeta^{tjk}(1-\zeta^k)}{\zeta^{k(n-1)}+\zeta^k-2} = -\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n}.$$

It is now clear that Theorem 3.2 and Lemma 3.3 imply the following

Theorem 3.4. *Let n be a natural number with $n>1$ and $m=[\sqrt{n}\,]$. Then n is prime if and only if*

$$\sum_{\substack{1\le j\le m\\ 1\le t,k\le n-1}} \cos\frac{2\pi tjk}{n} = -m(n-1).$$

References

[1] Apostol, T. M., The Resultant of the Cyclotomic Polynomials $F_m(ax)$ and $F_n(bx)$, *Math. Comp.* **29** (1975), 1-6.

[2] Dickson, L. E., *History of the Theory of Numbers*, vol. 1 (reprint), Chelsea, New York, 1952.

[3] Dixon, J. D., Factorization and Primality Tests, *Amer. Math. Monthly* **91** (1984), 333-352.

[4] Dudley, U., History of a Formula for Primes, *Amer. Math. Monthly* **76** (1969), 23-28.

[5] HACKS, J., Über Einige für Primzahlen Charakteristische Beziehungen, *Acta Math.* **17** (1893), 205–208.

[6] KNOPFMACHER, J., Recursive Formulae for Prime Numbers, *Arch. Math.* **33** (1979), 144–149.

[7] TSANGARIS, P. G., New (recursive) Formula for the nth Prime, *J. Elefteria* **4B** (1986), 231–233.

[8] TSANGARIS, P. G., JONES, J. P., An Old Theorem on the G.C.D. and its Application to Primes, *The Fibonacci Quart.* **30** (1992), 194–198.

[9] TSANGARIS, P. G., Prime Numbers and Cyclotomy-Primes of the form $x^2 + (x+1)^2$, PhD Thesis, Athens University, Athens, 1984 (in Greek).

[10] VOLOŠIN, YU. I. On the Integral part of a Rational Number, *Latvijas Valsts Univ. Zinath. Raksti* **28** (1959), 95–98.

Panayiotis G. Tsangaris
Department of Mathematics
Athens University
Panepistimiopolis, 15784 Athens
Greece
E-mail: ptsagari@cc.uoa.gr

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 11–18*

ON SEPARATELY CONTINUOUS FUNCTIONS $f: \ell^2 \to \mathbf{R}$

J. Činčura, T. Šalát, T. Visnyai (Bratislava, Slovakia)

Abstract. In this paper the notions of separately continuous and strongly separately continuous functions $f:l^2 \to \mathbf{R}$ are introduced and properties of such functions are investigated. The obtained results are compared with the corresponding known results for functions defined on $\mathbf{R}^m$ $(m \geq 2)$. It is shown that there are several interesting and essential differences between properties of (strongly) separately continuous functions defined on ℓ^2 and properties of (strongly) separately continuous functions defined on $\mathbf{R}^m$.

Introduction

Separately continuous functions $f: \mathbf{R}^m \to \mathbf{R}$ were investigated in several papers (see e.g. [2], [4], [8], [11]). Recall that a function $f: \mathbf{R}^m \to \mathbf{R}$ is said to be *separately continuous at a point* $x_0 = (x_1^0, \dots, x_m^0) \in \mathbf{R}^m$ provided that for each $k = 1, 2, \dots, m$ the function $\varphi_k: \mathbf{R} \to \mathbf{R}$ defined by $\varphi_k(t) = f(x_1^0, \dots, x_{k-1}^0, t, x_{k+1}^0, \dots, x_m^0)$ is continuous at x_k^0. It is well known that a function can be separately continuous at x^0 without being continuous at x^0. The standard example illustrating this phenomenon is the function $f: \mathbf{R}^2 \to \mathbf{R}$ given by $f(x_1, x_2) = 0$ if $x_1 \cdot x_2 \neq 0$, while $f(x_1, x_2) = 1$ if $x_1 \cdot x_2 = 0$. This function is separately continuous at $(0,0)$ without being continuous at $(0,0)$. On the other hand, if a function $f: \mathbf{R}^m \to \mathbf{R}$ is continuous at x^0 then it is separately continuous at x^0 as well.

In the paper [4] the author introduced the notion of strongly separately continuous function $f: \mathbf{R}^m \to \mathbf{R}$ at x^0 and obtained the following result: A function $f: \mathbf{R}^m \to \mathbf{R}$ is continuous at a point x^0 if and only if it is strongly separately continuous at x^0 (see [4; Theorem 2.1])

In this paper we extend the notions of separately continuous function and strongly separately continuous function to the functions defined defined on the space ℓ^2 and prove several basic results about functions. We show that there are essential differences between some properties of (strongly) separately continuous functions $f: \mathbf{R}^m \to \mathbf{R}$ and the corresponding properties of functions $f: \ell^2 \to \mathbf{R}$.

The paper consists of three sections. In the first section we introduce the notions of separately and strongly separately continuous function for the functions $f: \ell^2 \to \mathbf{R}$ and prove some basic results. In the second section we will investigate some properties of limit functions with respect to pointwise and weakly locally uniform convergence of sequences of (strongly) separately continuous functions $f: \ell^2 \to \mathbf{R}$ and also with respect to pointwise convergence of transfinite sequences of (strongly) separately continuous functions $f\colon \ell^2 \to \mathbf{R}$. In the third section we will study determining sets for the class of (strongly) separately continuous functions on ℓ^2.

In this paper we, as usually, denote by ℓ^2 the metric space consisting of all sequences $x = (x_j)_{j=1}^{\infty}$ of real numbers such that $\sum\limits_{k=1}^{\infty} x_k^2 < +\infty$ endowed with the metric ϱ defined by

$$\varrho(x,y) = \sqrt{\sum_{k=1}^{\infty}(x_k - y_k)^2}$$

for all $x, y \in \ell^2$.

If $x^0 \in \ell^2$ and $\delta > 0$, then $B(x^0, \delta)$ denotes the set $\{x \in \ell^2 : \varrho(x^0, x) < \delta\}$.

1. Separately and strongly separately continuous functions

The definitions of separate and strong separate continuity of functions $f\colon \mathbf{R}^m \to \mathbf{R}$ can be in a natural way extended to the case of functions $f\colon \ell^2 \to \mathbf{R}$.

Definition 1.1.

(a) A function $f\colon \ell^2 \to \mathbf{R}$ is said to be *separately continuous at a point* $x^0 = (x_j^0)_{j=1}^{\infty} \in \ell^2$ *with respect to a variable* x_k provided that the function $\varphi_k\colon \mathbf{R} \to \mathbf{R}$ defined by $\varphi_k(t) = f(x_1^0, \dots, x_{k-1}^0, t, x_{k+1}^0, \dots)$ is continuous at x_k^0. If f is separately continuous at x^0 with respect to x_k for all $k \in \mathbf{N}$, then f is said to be *separately continuous at* x^0. If f is separately continuous at every point $x^0 \in \ell^2$, then f is said to be *separately continuous on* ℓ^2.

(b) A function $f\colon \ell^2 \to \mathbf{R}$ is said to be *strongly separately continuous at a point* $x^0 = (x_j^0)_{j=1}^{\infty} \in \ell^2$ *with respect to a variable* x_k provided that for each $\varepsilon > 0$ there exists $\delta > 0$ such that $|f(x) - f(x')| < \varepsilon$ holds for each $x = (x_j)_{j=1}^{\infty} \in B(x^0, \delta)$, and $x' = (x_1, \dots, x_{k-1}, x_k^0, x_{k+1}, \dots)$. If f is strongly separately continuous at x^0 with respect to x_k for all $k \in \mathbf{N}$, then f is said to be *strongly separately continuous at* x^0. The function $f\colon \ell^2 \to \mathbf{R}$ is said to be *strongly separately continuous on* ℓ^2 provided that it is strongly separately continuous at every $x^0 \in \ell^2$.

Remark. Observe that in Definition 1.1 (b) $\varrho(x^0, x') \le \varrho(x^0, x)$. Hence, if $x \in B(x^0, \delta)$, then $x' \in B(x^0, \delta)$ as well. It is also obvious that a function $f\colon \ell^2 \to \mathbf{R}$ is strongly separately continuous at $x^0 = (x_j^0)_{j=1}^{\infty}$ with respect to x_k if only if for any sequence $(x^{(n)})_{n=1}^{\infty}$ in ℓ^2 which converges to x^0 we obtain that $\lim\limits_{n\to\infty} (f(x^{(n)}) - f(x^{(n)\prime})) = 0$, where $x^{(n)} = (x_j^{(n)})_{j=1}^{\infty}$ and $x^{(n)\prime} = (x_1^{(n)}, \dots, x_{k-1}^{(n)}, x_k^0, x_{k+1}^{(n)}, \dots)$ for all $n \in \mathbf{N}$.

From the above definition it follows the following:

Proposition 1.2.

(a) If a function $f: \ell^2 \to \mathbf{R}$ is continuous at x^0, then f is strongly separately continuous at x^0.

(b) If a function $f: \ell^2 \to \mathbf{R}$ is strongly separately continuous at x^0, then f is separately continuous at x^0.

Proof. (a) Let $(x^{(n)})_{n=1}^{\infty}$ be a sequence in ℓ^2 which converges to x^0, $x^{(n)} = (x_j^{(n)})_{j=1}^{\infty}$. Then, obviously, $\lim\limits_{n\to\infty} f(x^{(n)}) = f(x^0)$. Let $k \in \mathbf{N}$. For every $n \in \mathbf{N}$ put $x^{(n)'} = (x_1^{(n)}, \ldots, x_{k-1}^{(n)}, x_k^0, x_{k+1}^{(n)}, \ldots)$. Since $\varrho(x^{(n)'}, x^0) \leq \varrho(x^0, x^{(n)})$ for all $n \in \mathbf{N}$ we obtain that $\lim\limits_{n\to\infty} x^{(n)'} = x^0$ and it follows that $\lim\limits_{n\to\infty} f(x^{(n)'}) = f(x^0)$. Hence, $\lim\limits_{n\to\infty} (f(x^{(n)}) - f(x^{(n)'})) = 0$ and this yields that f is strongly separately continuous at x^0 with respect to x_k for arbitrary $k \in \mathbf{N}$.
(b) Similarly to (a).

In the paper [4] the following result was proved.

Theorem A. *A function $f: \mathbf{R}^m \to \mathbf{R}$ is continuous at x^0 if and only if f is strongly separately continuous at x^0.*

In the case of functions $f: \ell^2 \to \mathbf{R}$ only the implication presented in Proposition 1.2 (a) is valid and we show that there exist strongly separately continuous functions $f: \ell^2 \to \mathbf{R}$ (on ℓ^2) which are discontinuous at every point of the space ℓ^2. For defining such functions the following notion seems to be useful. A subset $\mathcal{S}$ is said to be a set of type (P$_1$) provided the following holds: If $x = (x_j)_{j=1}^{\infty} \in \mathcal{S}$, $y = (y_j)_{j=1}^{\infty} \in \ell^2$ and the set $\{j \in \mathbf{N}; x_j \neq y_j\}$ contains at most one element, then $y \in \mathcal{S}$. Next we present some examples of subsets $\mathcal{S} \subseteq \ell^2$ such that $\mathcal{S}$ is a set of type(P$_1$) and $\mathcal{S}$ as well as $\ell^2 \setminus \mathcal{S}$ are dense in ℓ^2.

Example 1.3.

(a) $\mathcal{S} = \{x = (x_j)_{j=1}^{\infty} \in \ell^2: j \in \mathbf{N};\quad x_j$ is a rational (irrational, algebraic, transcendent) number$\}$ is a finite set (see [14]).

(b) $$\mathcal{S}' = \left\{ x = (x_j)_{j=1}^{\infty} \in \ell^2 : \sum_{j=1}^{\infty} x_j < +\infty \right\}$$

Theorem 1.4. *There exists a function $g: \ell^2 \to \mathbf{R}$ such that g is strongly separately continuous on ℓ^2 and g is discontinuous at every point of ℓ^2.*

Proof. Let $\mathcal{S} \subseteq \ell^2$ be a set of type (P$_1$) such that $\mathcal{S}$ and $\ell^2 \setminus \mathcal{S}$ are dense in ℓ^2 (we can take some of the sets from Examples 1.3). Let $c \in \mathbf{R}$, $c \neq 0$. Define a function $g: \ell^2 \to \mathbf{R}$ by $g(x) = c$ for all $x \in \mathcal{S}$ and $g(x) = 0$ otherwise. If $x^0 \in \ell^2$, then for every neighbourhood U of x^0 we have $U \cap \mathcal{S} \neq \emptyset$, $U \cap (\ell^2 \setminus \mathcal{S}) \neq \emptyset$, and this yields that g is discontinuous at x^0. On the other hand, let $k \in \mathbf{N}$ and $x^0 = (x_j^0)_{j=1}^\infty$, $x = (x_j)_{j=1}^\infty$, $x' = (x_j')_{j=1}^\infty$ be arbitrary points of ℓ^2 such that for all $j \neq k, x_j = x_j'$ and $x_k^0 = x_k'$. It is obvious that if $x \in \mathcal{S}$, then also $x' \in \mathcal{S}$ and if $x \notin \mathcal{S}$, then also $x' \notin \mathcal{S}$. Hence we always obtain $|g(x) - g(x')| = 0$ so that for each $x^0 \in \ell^2$ and each $k \in \mathbf{N}$ the function g is strongly separately continuous at x^0 with respect to x_k.

Remark. While all separately continuous functions $f\colon \mathbf{R}^m \to \mathbf{R}$ belong to the first Baire class $\mathcal{B}_1$, Theorem 1.4 shows that neither strongly separately continuous nor separately continuous functions $f\colon \ell^2 \to \mathbf{R}$ have this property. The function $g\colon \ell^2 \to \mathbf{R}$ defined in the proof of Theorem 1.4 does not belong to $\mathcal{B}_1$ because the set of all discontinuity points of g is a set of the second Baire category.

We close this section with two examples. The function $f\colon \ell^2 \to \mathbf{R}$ define by $f(x_1, x_2, \ldots) = 1$ if $\sum\limits_{k=1}^{\infty} x_k^2 \in \mathbf{Q}$, $\mathbf{Q}$ being the set of all rationals, and $f(x_1, x_2, \ldots) = 0$ otherwise is an example of a function which is nowhere separately continuous. The function $g\colon \ell^2 \to \mathbf{R}$ given by $g(x_1, x_2, \ldots) = 0$ if $x_1 \cdot x_2 \neq 0$ while $g(x_1, x_2, \ldots) = 1$ in the opposite case is separately continuous at $(0, 0, \ldots)$ without being strongly separately continuous at this point.

2. Limit functions of sequences of separately continuous functions $f\colon \ell^2 \to \mathbf{R}$

If a sequence $(f_n\colon \ell^2 \to \mathbf{R})_{n=1}^\infty$ converges pointwise to a function $f\colon \ell^2 \to \mathbf{R}$ and all f_n are (strongly) separately continuous, then the function f need not be separately continuous.

Theorem 2.1. *There exists a sequence $(f_n\colon \ell^2 \to \mathbf{R})_{n=1}^\infty$ of functions each of which is continuous on ℓ^2 such that it converges pointwise to a function $f\colon \ell^2 \to \mathbf{R}$ which is not separately continuous on ℓ^2.*

Proof. For each $n \in \mathbf{N}$ define a function $g_n\colon \mathbf{R} \to \mathbf{R}$ by $g_n(x) = \sin \frac{1}{x}$ for all $x \in \langle \frac{1}{(n+1)\pi}, \frac{1}{\pi} \rangle$ and $g_n(x) = 0$ otherwise. It is clear that all g_n are continuous functions on $\mathbf{R}$ and the sequence $(g_n)_{n=1}^\infty$ converges pointwise to the function $g\colon \mathbf{R} \to \mathbf{R}$ given by $g(x) = \sin \frac{1}{x}$ for all $x \in (0, \frac{1}{\pi} \rangle$ and $g(x) = 0$ otherwise. Obviously, g is discontinuous at 0. For each $n \in \mathbf{N}$ define a function $f_n\colon \ell^2 \to \mathbf{R}$ by $f_n(x_1, x_2, \ldots) = g_n(x_1)$ and let $f\colon \ell^2 \to \mathbf{R}$ be the function given by $f(x_1, x_2, \ldots) = g(x_1)$. It is evident that for all $n \in \mathbf{N}$, f_n is a continuous function on ℓ^2 ($f_n = g_n \circ p_1$, where $p_1\colon \ell^2 \to \mathbf{R}$ is the first projection) and f is not separately continuous at the point $(0, 0, \ldots)$ with respect to x_1. Clearly, the sequence $(f_n)_{n=1}^\infty$ converges pointwise to f.

It is natural to ask whether some of various types of convergence of functions which are stronger than the pointwise convergence can guarantee that the limit function of a sequence of (strongly) separately continuous functions on ℓ^2 with respect to this type of convergence is also a (strongly) separately continuous function on ℓ^2. Next we show that there is a weaker type of locally uniform convergence (see [14], [5; p. 149]) which fulfills this requirement in the case of strongly separately continuous functions on ℓ^2.

Definition 2.2. Let X be a topological space, $(f_n\colon X \to \mathbf{R})_{n=1}^{\infty}$ be a sequence of functions and $x^0 \in X$. A sequence $(f_n)_{n=1}^{\infty}$ is said *to converge weakly locally uniformly to a function $f\colon X \to \mathbf{R}$ at x^0* if for every $\varepsilon > 0$ there exist $\delta > 0$ and $p \in \mathbf{N}$ such that $|f_n(x) - f(x)| < \varepsilon$ holds for each $n \in \mathbf{N}$ with $n \geq p$ and each $x \in B(x^0, \delta)$.

If a sequence $(f_n)_{n=1}^{\infty}$ converges weakly locally uniformly to a function f at every point $x^0 \in X$, then it is said *to converge weakly locally uniformly to f on X*.

Theorem 2.3. *If a sequence $(f_n\colon \ell^2 \to \mathbf{R})_{n=1}^{\infty}$ converges weakly locally uniformly to $f\colon \ell^2 \to \mathbf{R}$ at $x^0 \in \ell^2$ and for each $n \in \mathbf{N}$ the function f_n is strongly separately continuous at x^0, then the function f is also strongly separately continuous at x^0.*

Proof. Let $k \in \mathbf{N}$. We will prove that f is strongly separately continuous at x^0 with respect to x_k. Let $\varepsilon > 0$. Since $(f_n)_{n=1}^{\infty}$ converges weakly locally uniformly to f at x^0 there exist an open ball $B(x^0, \delta_1)$ and $p \in \mathbf{N}$ such that $|f_n(x) - f(x)| < \frac{\varepsilon}{3}$ holds for all $n \geq p$ and $x \in B(x^0, \delta_1)$. The function f_p is strongly separately continuous at x^0 with respect to x_k and it follows that there exists $\delta_2 > 0$ such that $|f_p(x) - f_p(x')| < \frac{\varepsilon}{3}$ holds for each $x = (x_j)_{j=1}^{\infty} \in B(x^0, \delta_2)$ and $x' = (x_1, \dots, x_{k-1}, x_k^0, x_{k+1}, \dots)$. Put $\delta = \min\{\delta_1, \delta_2\}$. Then for each $x \in B(x^0, \delta)$ we obtain that $|f_p(x) - f_p(x')| < \frac{\varepsilon}{3}$, $|f_p(x) - f(x)| < \frac{\varepsilon}{3}$ and because $\varrho(x', x^0) \leq \varrho(x^0, x) < \delta$ we have also $|f_p(x') - f(x')| < \frac{\varepsilon}{3}$. Hence, for all $x \in B(x^0, \delta)$ we obtain $|f(x) - f(x')| \leq |f(x) - f_p(x)| + |f_p(x) - f_p(x')| + |f_p(x') - f(x')| < \varepsilon$ and this yields that f is strongly separately continuous at x^0 with respect to x_k.

In the rest of this section we will investigate some properties of limit functions of convergent transfinite sequences of (strongly) separately continuous functions. Recall that a transfinite sequence $(x_\xi)_{\xi<\Omega}$ (Ω is the first uncountable ordinal) in a metric space (X, σ) converges to a point $x \in X$ (we write $x_\xi \to x$) if for every $\varepsilon > 0$ there exists $\xi_0 < \Omega$ such that $\sigma(x_\xi, x) < \varepsilon$ holds for each ξ, $\xi_0 \leq \xi < \Omega$. It is well known (see e.g. [9]) that if $x_\xi \to x$ in a metric space (X, σ), then there exists $\xi_0 < \Omega$ such that $x_\xi = x$ holds for each $\xi \geq \xi_0$. A transfinite sequence $(f_\xi\colon M \to \mathbf{R})_{\xi<\Omega}$ of functions, M is a set, converges pointwise to a function $f\colon M \to \mathbf{R}$ (we write $f_\xi \to f$) on M, if for each $x \in M$ we have $f_\xi(x) \to f(x)$ in $\mathbf{R}$. In the next theorem we show that the pointwise convergence of transfinite sequences of functions preserves (strong) separate continuity.

Theorem 2.4. *Let $(f_\xi\colon \ell^2 \to \mathbf{R})_{\xi<\Omega}$ be a transfinite sequence of functions which converges pointwise to a function $f\colon \ell^2 \to \mathbf{R}$ on ℓ^2. If for all $\xi < \Omega$ the function f_ξ is (strongly) separately continuous at x^0, then the function f is also (strongly) separately continuous at x^0.*

Proof. Let for each $\xi < \Omega$ the function f_ξ be strongly separately continuous at x^0 with respect to x_k. We show that f is strongly separately continuous at x^0 with respect to x_k. Let $(x^{(n)})_{n=1}^\infty$ be a sequence in ℓ^2 which converges to x^0, $x^{(n)} = (x_j^{(n)})_{j=1}^\infty$. For each $n \in \mathbf{N}$ put $x^{(n)'} = (x_1^{(n)}, \ldots, x_{k-1}^{(n)}, x_k^0, x_{k+1}^{(n)}, \ldots)$. It suffices to check that $\lim\limits_{n\to\infty}(f(x^{(n)}) - f(x^{(n)'})) = 0$. Let $n \in \mathbf{N}$. For every $\xi < \Omega$ we have $\lim\limits_{n\to\infty}(f_\xi(x^{(n)}) - f_\xi(x^{(n)'})) = 0$. Since $f_\xi \to f$ on ℓ^2 we obtain $f_\xi(x^{(n)}) \to f(x^{(n)})$ and $f_\xi(x^{(n)'}) \to f(x^{(n)'})$. Then there exists $\xi_n < \Omega$ such that $f_\xi(x^{(n)}) = f(x^{(n)})$ and $f_\xi(x^{(n)'}) = f(x^{(n)'})$ holds for all $\xi \geq \xi_n$. We can choose $\xi_0 < \Omega$ such that for all $n \in \mathbf{N}$ we have $\xi_n \leq \xi_0$. Then for all $n \in \mathbf{N}$ $f_{\xi_0}(x^{(n)}) = f(x^{(n)})$ and $f_{\xi_0}(x^{(n)'}) = f(x^{(n)'})$. Clearly, $\lim\limits_{n\to\infty}(f(x^{(n)}) - f(x^{(n)'})) = \lim\limits_{n\to\infty}(f_{\xi_0}(x^{(n)}) - f_{\xi_0}(x^{(n)'})) = 0$. Hence, the function f is strongly separately continuous at x^0 with respect to x_k. The case of separate continuity immediately follows from the known fact that a limit of a transfinite sequence$(f_\xi\colon \mathbf{R} \to \mathbf{R})_{\xi<\Omega}$ of continuous functions is a continuous function (see e. g. [10], [9]).

3. Determining sets for separately continuous functions $f\colon \ell^2 \to \mathbf{R}$

If $\mathcal{F}$ is a class of (real) functions defined on a set X and $M \subseteq X$, then the set M is said to be a determining set for $\mathcal{F}$ provided that any functions $f, g \in \mathcal{F}$ satisfying $f|_M = g|_M$ are coincidental on X. For the class $\mathcal{G}$ of all separately continuous function of two variables the following result was proved (see [13], [11], [8]).

Theorem B. *Let $\mathcal{G}$ be the class of all separately continuous functions defined on $\mathbf{R}^2$. Then a set $M \subseteq \mathbf{R}^2$ is a determining set for the class $\mathcal{G}$ if and only if M is dense in $\mathbf{R}^2$.*

Obviously, this result can be extended to the class of all separately continuous functions defined on $\mathbf{R}^m$,$m \geq 2$. On the other hand, from Theorem 1.4 it follows that there exist dense subsets of the space ℓ^2, e. g. $\mathcal{S}, \ell^2 \setminus \mathcal{S}, \mathcal{S}', \ell^2 \setminus \mathcal{S}'$ where $\mathcal{S}, \mathcal{S}'$ are presented in Example 1.3, that are not determining sets for the class of all (strongly) separately continuous functions on ℓ^2. Another example is given in the next theorem.

Theorem 3.1. *There exists a strongly separately continuous function $h: \ell^2 \to \mathbf{R}$ and a residual (and, consequently, dense) set E in ℓ^2 such that $h(x) = 0$ for all $x \in E$ and $h(y) \neq 0$ for some $y \in \ell^2 \setminus E$.*

Proof. Denote by H the set of all $x = (x_j)_{j=1}^{\infty} \in \ell^2$ for which $\sum_{j=1}^{\infty} x_j$ converges. Put

E $= \ell^2 \setminus$ H and define $h: \ell^2 \to \mathbf{R}$ by $h(x) = \sum_{j=1}^{\infty} x_j$ for all $x \in$ H and $h(x) = 0$ otherwise. According to [7; Theorem 3.1.] (it suffices to put $\alpha_n = 1$ for all $n = 1, 2, \ldots$ and $p = q = 2$) the set E is residual in ℓ^2. To complete the proof it suffices to show that h is strongly separately continuous on ℓ^2. Let $x^0 = (x_j^0)_{j=1}^{\infty} \in \ell^2$ and $k \in \mathbf{N}$. We show that h is strongly separately continuous at x^0 with respect to x_k. Let $\varepsilon > 0$. If $x = (x_j)_{j=1}^{\infty} \in B(x^0, \varepsilon)$, then also $x' = (x_1, \ldots, x_{k-1}, x_k^0, x_{k+1}, \ldots) \in B(x^0, \varepsilon)$. If $x \in$ H and $h(x) = \sum_{j=1}^{\infty} x_j$, then $|h(x) - h(x')| = |x_k - x_k^0| \leq \varrho(x, x^0) < \varepsilon$. If $x \notin$ H, then $h(x) = h(x') = 0$ and we have $|h(x) - h(x')| = 0 < \varepsilon$. This yields that h is strongly separately continuous at x^0 with respect to x_k.

In connection with determining sets for strongly separately continuous functions on ℓ^2 the following observation seems to be useful. Let M be a subset of ℓ^2 and $\widetilde{M}$ is the set of all $y = (y_j)_{j=1}^{\infty} \in \ell^2$ such that there exists $x = (x_j)_{j=1}^{\infty} \in M$ for which the set $\{j \in \mathbf{N} : x_j \neq y_j\}$ is finite. It is obvious, that $M \subseteq \widetilde{M}, \widetilde{\widetilde{M}} = \widetilde{M}$ and $\widetilde{M}$ is a set of type (P_1). Similarly to the proof of Theorem 1.4 it can be checked that for any subset $M \subseteq \ell^2$ the function $g: \ell^2 \to \mathbf{R}$ given by $g(x) = 0$ for all $x \in \widetilde{M}$ and $g(x) = 1$ otherwise is strongly separately continuous. Hence, we obtain:

Proposition 3.2. *If M is a subset of ℓ^2 such that $\widetilde{M} \neq \ell^2$, then M is not a determining set for the class of all (strongly) separately continuous functions on ℓ^2.*

It is easy to see that if $M \subseteq \ell^2$ and card $M < \mathbf{c}$, $\mathbf{c}$ being the cardinality of continuum, then $\widetilde{M} \neq \ell^2$ (evidently, there exists $y = (y_j)_{j=1}^{\infty} \in \ell^2$ such that for each $x = (x_j)_{j=1}^{\infty} \in M$, $\{j \in \mathbf{N} : x_j = y_j\} = \emptyset$). Hence, as a consequence of Proposition 3.2 we obtain.

Proposition 3.3. *If $M \subseteq \ell^2$ is a determining set for the class of all (strongly) separately continuous functions on ℓ^2, then card $M = \mathbf{c}$.*

References

[1] Bruckner, A. M., *Differentiation of Real Functions*, Spinger-Verlag, Berlin-Heidelberg-New York, 1978.

[2] Carrol, F. M., Separately continuous functions, *Amer. Math. Monthly* **78** (1971), 175.

[3] DRAHOVSKÝ, Š., ŠALÁT, T., TOMA, V., Points of uniform convergence and oscillation of sequences of functions, *Real Anal. Exchange* **20** (1994–95), 753–767.

[4] DZAGNIDZE, O. P., Separately continuous functions in a new sense are continuous, *Real Anal. Exchange* **24** (1998–99), 695–702.

[5] GOFFMAN, C., *Reelle Funktionen*, Bibiographisches Institut, Mannheim–Wien–Zürich, 1976.

[6] KURATOWSKI, K., *Topologie I*, PWN, Warsaw, 1958.

[7] Legéň, A., Šalát, T., On some applications of the category method in the theory of sequence spaces , *Mat.-fyz. čas. SAV* **14** (1964), 217–233 (Russian).

[8] MAREUS, S., On functions continuous in each variable, *Doklady AN SSSR* **112** (1957), 812–814 (Russian).

[9] ŠALÁT, T., On transfinite sequences of B-measurable functions, *Fund. Math.* **LXXVIII** (1973), 157–162.

[10] SIERPIŃSKI, W., Sur les suites transfinies convergentes de fonctions de Baire, *Fund. Math.* **I** (1920), 132–141.

[11] SIERPIŃSKI, W., Sur une propriété de fonctions de deux variables réelles, continues par rapport à chacune de variables, *Publ. Math. Univ. Belgrade* **1** (1932), 125–128.

[12] SIKORSKI, R., *Real Functions I*, PWN, Warsaw, 1958 (Polish).

[13] TOLSTOV, G. P., On partial derivatives, *Izv. Akad. Nauk SSSR* **13** (1949), 425–446 (Russian).

[14] VRŤO, V., Some questions connected with the quasicontinuity in metric space (Dissertation), *PriF UK, Bratislava*, 1980 (Slovak).

J. Činčura, T. Visnyai
Faculty of Mathematics,
Physics and Informatics,
Comenius University,
Mlynská dolina, 842 48 Bratislava,
Slovakia
E-mail: [cincura,visnyai]@fmph.uniba.sk

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 19–24*

PRIMITIVE DIVISORS OF LUCAS SEQUENCES AND PRIME FACTORS OF x^2+1 AND x^4+1

Florian Luca (Michoacán, México)

Abstract. In this paper, we show that $24208144^2+1=29^3\cdot37^2\cdot53\cdot61^2\cdot89$ is the largest instance in which n^2+1 does not have any prime factor >100.

1. Introduction

For any integer n let $P(n)$ be the largest prime factor of n with the convention that $P(0)=P(\pm1)=1$. In [8], it is shown that if x is an integer, then $P(x^2+1)\geq 17$ once $|x|\geq 240$. The method presented in [8] is elementary, and the computations were done using congruences with respect to small moduli.

The purpose of this note is two fold. First of all, we improve the lower bound from [8] by showing that $P(x^2+1)\geq 101$ once $|x|\geq 24208145$. Secondly, our method is entirely different from the one presented in [8] in the sense that it uses the existence of primitive prime divisors for the Lucas sequences associated to certain Pell equations. This method has been used previously by Lehmer in [6] to compute all the positive integer solutions x of the inequality $P(x(x+1))\leq 41$. The method is completely general and, in practice, armed with a good computer, one can employ it to find all the integer solutions x of the inequality $P(x^2+1)<K$, where K is any given reasonable constant. We also use the same method to show that $P(x^4+1)\geq 233$ for $x\geq 11$, which extends the range of computations described in [7] and [9] where it was shown that $P(x^4+1)\geq 73$ if $x\geq 3$. We recall that explicit lower bounds for $P(x^3+1)$ appear in [1].

This note is organized as follows. In the second section, we present our algorithm and computational findings. In the third section, we make an analysis of the running time of our algorithm for computing all positive integer solutions x of the inequality $P(x^2+1)<K$ in terms of K.

2. Computational Results

Theorem 2.1.

(i) The largest positive integer solution x of the inequality

$$P(x^2+1)<101 \tag{1}$$

is $x = 24208144$.

(ii) The largest positive integer solution x of the inequality

$$P(x^4+1) < 233 \tag{2}$$

is $x = 10$.

Proof. We start with the first question. Assume that x is a positive integer such that $P(x^2+1) < 101$. The only prime numbers p that can divide a number of the form x^2+1 are either $p = 2$, or $p \equiv 1 \pmod 4$. There are only 12 such primes p less than 101 and they are

$$p \in \mathcal{P} = \{2,\ 5,\ 13,\ 17,\ 29,\ 37,\ 41,\ 53,\ 61,\ 73,\ 89,\ 97\}.$$

In particular, the number x has the property that

$$x^2+1 = dy^2, \tag{3}$$

where $d > 1$ and $y \geq 1$ are integers whose factors belong to $\mathcal{P}$, and d is squarefree. If we rewrite equation (3) as

$$x^2 - dy^2 = -1, \tag{4}$$

it follows that the pair $(x,\ y)$ is a positive integer solution of a Pell equation of the form (4) for some squarefree $d > 1$ whose prime factors are in the set $\mathcal{P}$. Let $\mathcal{A}$ be the set of all the squarefree positive integers $d > 1$ whose prime factors are in the set $\mathcal{P}$. Clearly, $\mathcal{A}$ contains precisely $2^{|\mathcal{P}|} - 1 = 2^{12} - 1 = 4095$ elements. For each $d \in \mathcal{A}$ let $(X_1(d), Y_1(d))$ be the first positive integer solution of the Pell equation

$$X^2 - dY^2 = \pm 1. \tag{5}$$

It is wellknown that if we denote by m_d the length of the continued fraction of $\sqrt{d}$, then $(X_1(d),\ Y_1(d)) = (P_{m_d-1},\ Q_{m_d-1})$, where for a nonnegative integer k we have denoted by P_k/Q_k the kth convergent to $\sqrt{d}$. Moreover, if m_d is even, then equation (5) has no integer solution $(X,\ Y)$ with the sign -1 appearing on the right hand side. Of the totality of 4095 elements d of $\mathcal{A}$, only 2672 of them have the property that the period m_d is odd. Let us denote by $\mathcal{B}$ the subset of $\mathcal{A}$ consisting of only these elements. We used Mathematica to compute $(X_1(d),\ Y_1(d))$ for all $d \in \mathcal{B}$. These computations took about 7 hours.

Assume now that $(x,\ y)$ is a solution of equation (4) for some $d \in \mathcal{B}$. It then follows that $(x,\ y) = (X_n(d),\ Y_n(d))$ for some odd value of $n \geq 1$, where $X_n(d)$ and $Y_n(d)$ can be computed using the formulae

$$X_n(d) = \frac{(\alpha(d))^n + (\beta(d))^n}{2} \qquad \text{and} \qquad Y_n(d) = \frac{(\alpha(d))^n - (\beta(d))^n}{2\sqrt{d}}$$

for all $n \geq 1$, where

$$\alpha(d) = X_1(d) + \sqrt{d}Y_1(d), \qquad \beta(d) = X_1(d) - \sqrt{d}Y_1(d).$$

It is wellknown that $Y_1(d) \mid Y_n(d)$ for all $n \geq 1$. Thus, since in equation (4) the number y has $P(y) < 101$, it follows that $P(Y_1(d)) < 101$ must hold. Of the totality of 2672 pairs $(X_1(d),\ Y_1(d))$ with $d \in B$, only 143 of them satisfy this condition. Testing this took a few minutes with Mathematica. Of course, we did not factor the numbers $Y_1(d)$ because some of them are quite large. Instead, we computed, for each given d, the largest divisor M_d of $Y_1(d)$ having $P(M_d) < 101$, and we tested if $Y_1(d)$ is equal to M_d.

Let now C be the set consisting of these 143 elements $d \in B$ for which $P(Y_1(d)) < 101$, and assume that $y = Y_n(d)$ for some odd $n \geq 1$ and some $d \in C$. Since

$$Y_n(d)Y_1(d) = \frac{\alpha(d)^n - \beta(d)^n}{\alpha(d) - \beta(d)}, \qquad \text{for all } n \geq 1,$$

it follows that the sequence $\left\{\frac{Y_n(d)}{Y_1(d)}\right\}_{n\geq 1}$ is a *Lucas sequence* of the first kind with roots $\alpha(d)$ and $\beta(d)$. Since $\alpha(d)$ and $\beta(d)$ are real, it follows, by a result of Carmichael (see [2]), that the nth term of this sequence has a *primitive divisor* for all $n > 12$. We recall that a primitive divisor of the nth term of a Lucas sequence is a prime divisor p of it which, among other properties, it also fulfills the condition that $p \equiv \pm 1 \pmod{n}$. In particular, if $n > 12$ is odd, then there exists a prime number $p \mid Y_n(d)$ such that $p \geq 2n - 1$. Since we are searching for values of n and d such that $P(Y_n(d)) \leq 97$, it follows that n is an odd number such that $2n - 1 \leq 97$, hence, $n \leq 49$. Thus, we used Mathematica to compute, for every one of the 143 values of $d \in C$, the numbers $Y_n(d)$ for all odd values of $n \leq 49$, resulting in a totality of $143 \cdot 25 = 3575$ such numbers. For each one of these numbers, we applied the procedure described above to eliminate the ones for which $P(Y_n(d)) > 97$. The computation took a few minutes, and a totality of 156 numbers $Y_n(d)$ survived (that is, only 13 new numbers $Y_n(d)$ for $n > 1$ odd and $d \in C$ were found). For each of these numbers we computed $x = X_n(d)$. The conclusion of these computations is that there are precisely 156 positive integer values of x for which $P(x^2 + 1) < 101$. Of these 156 positive integers, 140 of them are less than 10^5, 10 more of them are between 10^5 and 10^6, and the largest 6 of them are 1984933, 2343692, 3449051, 6225244, 22709274, and 24208144. Thus, the largest positive integer solution x of the inequality $P(x^2 + 1) < 101$ is

$$24208144^2 + 1 = 29^3 \cdot 37^2 \cdot 53 \cdot 61^2 \cdot 89.$$

We now turn our attention to $P(x^4 + 1)$. Suppose that x is a positive integer such that $P(x^4 + 1) < 233$. If p is a prime number dividing $x^4 + 1$, then either $p = 2$, or

p is congruent to 1 modulo 8. There are only 9 such primes which are smaller than 233, namely

$$\mathcal{P}_1 = \{2,\ 17,\ 41,\ 73,\ 89,\ 97,\ 113,\ 137,\ 193\}.$$

So, with $z = x^2$, we need to find all the solutions of the equation

$$z^2 - dy^2 = -1, \tag{6}$$

where $d > 1$ and $y \geq 1$ are integers whose factors belong to $\mathcal{P}_1$, and d is squarefree. There are precisely $2^{|\mathcal{P}_1|} - 1 = 2^9 - 1 = 511$ possible values for d. We used Mathematica to find, for every such d, the smallest solution $(X_1(d),\ Y_1(d))$ of the Pell equation (5). Only 255 values of d have the property that equation (5) has a solution with the sign -1 in the right hand side. Out of these values of d, only 13 have the property that all prime factors of $Y_1(d)$ are in $\mathcal{P}_1$. Now suppose that $(z,\ y) = (X_n(d),\ Y_n(d))$ is a solution of equation (6) for some odd value of n and one of these 13 values of d. Since $P(Y_n(d)) \leq 197$, it follows, by the primitive divisor theorem, that $2n - 1 \leq 197$, i.e. $n \leq 99$. Thus, we have computed all the $50 \cdot 13 = 650$ values of $Y_n(d)$ (i.e., for each one of the 13 values of d, and for each odd n with $n \leq 99$), and we tested each one of these numbers to see if their prime factors are in $\mathcal{P}_1$. No new number was found, so $n = 1$. Thus, $z = X_1(d)$ for one of the 13 values of d. Since $z = x^2$, we tested if $X_1(d)$ is a perfect square. Five values of x were found, namely $x = 1,\ 2,\ 3,\ 9,\ 10$. So, the largest solution of the inequality $P(x^4 + 1) < 233$ is

$$10^4 + 1 = 73 \cdot 137,$$

and $P(x^4 + 1) \geq 233$ holds for all integers $x \geq 11$.

We conclude this section by remarking that we could have done the final testing for $P(x^4 + 1) < 233$ by combining the primitive divisor technique with a result of J. H. E. Cohn from [3]. Namely, in [3], the following result is proved: Assume that $d > 1$ is a squarefree number. Then the equation $X^4 - dY^2 = -1$ can have at most one solution in positive integers $(X,\ Y)$. Moreover, let $(X_1(d),\ Y_1(d))$ denote the smallest positive solution of $X^2 - dY^2 = -1$, and write $X_1(d) = AB^2$, where A is squarefree. Then the only possible value of the odd integer k for which $X_k(d)$ can be a square is $k = A$.

3. The running time of the algorithm

Given $K > 1$, an algorithm to compute all positive integer solutions x of the inequality $P(x^2+1) \leq K$ was presented in section 1, together with its findings when $K = 100$. Let $f(X) \in \mathbf{Z}[X]$ be a polynomial having at least two distinct roots. In his PhD thesis, Haristoy (see [4]) improved upon earlier estimates of Shorey and Tijdeman (see chapter 7 of [10]) and showed that the inequality $P(f(x)) \gg \log_2 x \log_3 x / \log_4 x$ holds if x is a sufficiently large positive integer. Here and in what follows, for a positive real number y we use $\log y$ for the maximum between the natural logarithm of y and 1, and for a positive integer k we use $\log_k y$ for the kth fold iterate of the function $\log y$. From this result, if follows that if $P(x^2+1) < K$, then $x < \exp(\exp(O(K \log_2 K / \log K)))$, so if one wants to find all the positive integer solutions x of the inequality $P(x^2+1) < K$ by simply factoring x^2+1 for all positive integers x up to the above upper bound, then the running time of such a naïve algorithm will be almost doubly exponential in K. In this section, we present the following result.

Theorem 3.1. *The algorithm presented in section 2 finds all positive integer solutions x of the inequality $P(x^2+1) \le K$ after at most $\exp(O(K))$ elementary bit operations.*

Proof. Here, we keep the notations from section 2. First, to generate $\mathcal{A}$, one first generates the $2^{\pi(K;4,1)+1} = \exp(O(K))$ squarefree numbers d all whose prime factors are 2 or congruent to $1 \pmod 4$ and having $P(d) \le K$. Secondly, to find $\mathcal{B}$, for each one of the numbers $d \in \mathcal{A}$ one computes the minimal solution $(X_1(d), Y_1(d))$ of the Pell equation $X^2 - dY^2 = \pm 1$. Then $\mathcal{B}$ is the subset of those $d \in \mathcal{A}$ such that $(X_1(d), Y_1(d))$ is a solution of the equation $X^2 - dY^2 = -1$. The continued fraction algorithm for quadratic irrationalities shows that this is computable in $O(d^{1/2}) = \exp(O(K))$ steps and since $d < 4^K$, it follows that at each step only numbers of the form $\exp(O(K))$ are being handled. Now with each one of these numbers $Y_1(d)$, we test if $P(d) < K$. This step requires $\exp(O(K))$ elementary operations. Indeed, let $p \le K$ be a fixed prime and assume that $p^\alpha || Y_1(d)$. Then $\alpha ll \log Y_1(d) = \exp(O(K))$. Moreover, since $a \pmod b$ requires $O(\log^2(a+b))$ elementary bit operations (using naïve arithmetic, and even less using Fast Fourier Transform), it follows that this part of the computation requires $\exp(O(K))$ elementary bit operations. Thus, the subset $\mathcal{C}$ of $\mathcal{B}$ consisting of those $d \in \mathcal{B}$ such that $P(d) \le K$ can be generated after at most $\exp(O(K))$ elementary bit operations. Finally, one now generates $Y_k(d)$ for $k \le K$ and tests again if $P(Y_k(d)) \le K$. As previously, this requires again at most $\exp(O(K))$ elementary bit operations after which the set consisting of all the positive integers x such that $x^2 + 1 = dY_k(d)^2$ has the largest prime factor $\le K$ is obtained.

Acknowledgments. The computations were carried out on the machines at the Tata Institute for Fundamental Research in Mumbai, India, on June 25 and June 26, 2001. I would like to thank the Tata Institute for its hospitality, Professors Yann Bugeaud, Maurice Mignotte, Igor Shparlinski and Tarlok Shorey for useful advice, and the Third World Academy of Sciences for financial support.

References

[1] Buchmann, J., Győry, K., Mignotte, M., Tzanakis, N., Lower bounds for $P(x \supset 3 + k)$, an elementary approach, *Publ. Math. Debrecen* **38** (1991), no. 1–2, 145–163.

[2] Carmichael, R. D., On the numerical factors of arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30–70.

[3] Cohn, J. H. E., The Diophantine equation $x^4 + 1 = Dy^2$, *Math. Comp.* **66** no. 219 (1997), 1347–1351.

[4] Haristoy, J., Equations diophantiennes exponentielles, *Prépublications de IRMA* **029**, 2003.

[5] Hua, L.-K., On the least solution to Pell equation, *Bull. Amer. Math. Soc.* **48** (1942), 731–735; *Selected papers*, Springer, New York, 1983, 119–123.

[6] Lehmer, D. H., On a problem of Störmer, *Illinois J. Math.* **8** (1964), 57–79.

[7] Mabkhout, M., Minoration de $P(x^4+1)$, *Rend. Sem. Fac. Sci. Univ. Cagliari* **63** no. 2 (1993), 135–148.

[8] Mignotte, M., $P(x^2+1) \geq 17$ si $x \geq 240$, *C.R. Acad. Sci. Paris Sér. I Math.* **301** no. 13 (1985), 661–664.

[9] Mureddu, M., A lower bound for $P(x^4+1)$, *Ann. Fac. Sci. Toulouse Math.* (5) **8** no. 2 (1986/1987), 109–119.

[10] Shorey, T. N., Tijdeman, R., *Exponential diophantine equations*, Cambridge Tracts in Mathematics **87**, Cambridge University Press, Cambridge, 1986.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58180, Morelia, Michoacán,
México
E-mail: fluca@matmor.unam.mx

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 25–31*

GENERALIZATIONS OF BOTTEMA'S THEOREM ON PEDAL POINTS

Éva Sashalmi and Miklós Hoffmann (Eger, Hungary)

Abstract. Given a polygon and one of its inner points P, the orthogonal projections of P onto the sides of the polygon are called pedal points of P. Here we prove different results concerning configurations by attaching different types of polygons to the segments of the sides defined by the pedals. These theorems can be considered as the generalizations of Bottema's classical theorem.

1. Introduction

Consider a triangle ABC and one of its inner points P. Let the orthogonal projection of P onto the sides AB, BC, CA be P_1, P_2 and P_3, respectively. These are the pedal points of P. If we build squares on the segments of the sides defined by the pedals (outside of the triangle), we obtain six different squares. In [1] Bottema proved the following theorem about the areas of these squares:

Theorem 1. *The sum of the areas of the squares erected on the segments AP_1, BP_2 and CP_3 equals the sum of the squares erected on the segments P_1B, P_2C and P_3A.*

More recently van Lamoen and other studied similar configurations ([2], [3]) and showed the following in [3]:

Theorem 2. *Let $A_1B_1C_1$ be the triangle bounded by the lines containing the sides of the squares opposite to AP_1, BP_2 and CP_3. Similarly let $A_2B_2C_2$ be the triangle bounded by the lines containing the sides of the squares opposite to P_1B, P_2C and P_3A. These two triangles are each homothetic to ABC and the ratio of homothety is*

$$\lambda = 1 + \frac{a^2 + b^2 + c^2}{4t},$$

where a, b, c are the sides and t is the area of ABC.

To simplify the equation we use the following notations:

Definition. The *Brocard point* Ω and the *Brocard angle* ω of ABC is the point and angle for which

$$\angle AB\Omega = \angle BC\Omega = \angle CA\Omega = \omega.$$

Since for the Brocard angle

$$\cot\omega = \frac{a^2+b^2+c^2}{4t} \tag{1}$$

holds (c.f. [4]), the ratio of the homothety in Theorem 2 can simply be written as

$$\lambda = 1 + \cot\omega.$$

Throughout the paper we use the phrases "left" and "right" to distinguish the two families of squares or other builded polygons.

2. New results on triangles

At first we prove that Bottema's statement holds not only for squares but for any rectangles similar for each other and also for regular triangles. Then we examine the ratio of homothety of Theorem 2 in the case when the squares are erected onto the inner side of the triangle and show that it equals $\cot\omega - 1$.

Theorem 3. *Consider the triangle ABC and one of its inner points P. Let the pedals of P on the sides AB, BC, CA be P_1, P_2 and P_3, respectively. If we build similar rectangles on the segments of the sides defined by the pedals, then the sum of the areas of the rectangles erected on the segments AP_1, BP_2 and CP_3 (i.e. the "left" rectangles) equals the sum of the rectangles erected on the segments P_1B, P_2C and P_3A (i.e. the "right" rectangles).*

Proof. Here we use the basic idea of [3]. Let us denote the sides of the triangle by a, b, c and the segments defined by the pedals by the following: $c_l = AP_1$; $c_r = P_1B$; $a_l = BP_2$; $a_r = P_2C$; $b_l = CP_3$; $b_r = P_3A$. From Theorem 1 it is follows, that

$$a_l^2 + b_l^2 + c_l^2 = a_r^2 + b_r^2 + c_r^2. \tag{2}$$

Let us denote the other side of the rectangle erected onto a_l by s and let $\rho = \frac{s}{a_l}$. Thus the area of this rectangle can be written as $a_l s = a_l \rho a_l = a_l^2 \rho$. Since the rectangles are similar to each other, ρ is the ratio of their sides for all rectangles. Thus the sum of the areas of the "left" rectangles is

$$a_l^2\rho + b_l^2\rho + c_l^2\rho = \rho(a_l^2 + b_l^2 + c_l^2).$$

Similarly for the "right" rectangles

$$a_r^2\rho + b_r^2\rho + c_r^2\rho = \rho(a_r^2 + b_r^2 + c_r^2)$$

holds, which, together with (2) proves the statement.

Corollary. *Let $A_1B_1C_1$ be the triangle bounded by the lines containing the sides of the rectangles opposite to AP_1, BP_2 and CP_3. Similarly let $A_2B_2C_2$ be the triangle bounded by the lines containing the sides of the rectangles opposite to P_1B, P_2C and P_3A. These two triangles are each homothetic to ABC and the ratio of homothety is $\lambda = 1 + \rho \cot \omega$.*

Back to the original situation, building the squares to the inner side of the segments of the side of the triangle, Theorem 1 naturally remains valid (see Fig. 1). The ratio of the homotethy, however will be changed as follows.

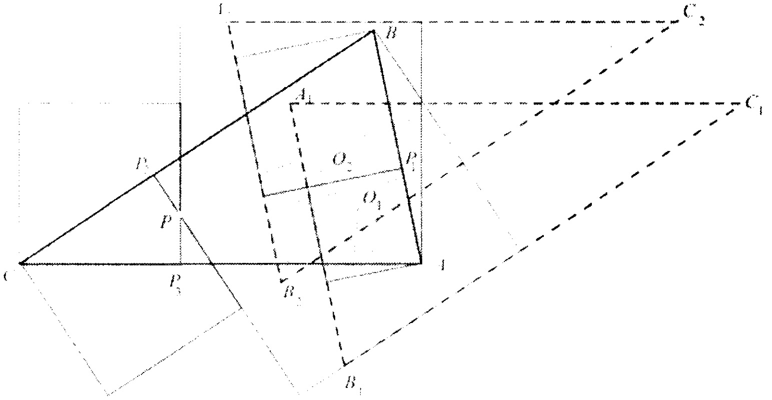


Figure 1.

Theorem 4. *Consider the triangle ABC and one of its inner points P. Let the pedals of P on the sides AB, BC, CA be P_1, P_2 and P_3, respectively. If we build squares onto the inner side of the segments of the sides defined by the pedals, as in Fig.1., then the ratio of the homothety between the triangle ABC and $A_1B_1C_1$ as well as between ABC and $A_2B_2C_2$ is $\lambda = \cot \omega - 1$.*

Proof. Denote the center of homothety between ABC and $A_1B_1C_1$ by O_1 and the segments BP_2, CP_3, AP_1 by a_l, b_l and c_l. Let the distances of the sides BC, CA, AB from O_1 be f, g, h, respectively. Obviously the distances of the sides B_1C_1, C_1A_1, A_1B_1 from O_1 are $(a_l - f), (b_l - g)$ and $(c_l - h)$. Due to the homothety $f : g : h = (a_l - f) : (b_l - g) : (c_l - h)$ holds. From equation (2)

$$a_l^2 + b_l^2 + c_l^2 = (a - a_l)^2 + (b - b_l)^2 + (c - c_l)^2.$$

Applying equation (1) this can be written as

$$aa_l + bb_l + cc_l = \frac{a^2 + b^2 + c^2}{2} = 2t \cot \omega,$$

where t is the area of the triangle ABC. Summarizing the area of the subtriangles O_1BC, O_1AC and O_1AB we find

$$af + bg + ch = 2t,$$

which, together with the previous equation yields

$$\frac{a_l}{f}=\frac{b_l}{g}=\frac{c_l}{h}=\cot\omega.$$

Thus the ratio of homothety is

$$\lambda=\frac{a_l-f}{f}=\frac{b_l-g}{g}=\frac{c_l-h}{h}=\cot\omega-1,$$

which completes the proof.

By applying this method one can prove several similar theorems and compute the ratios of homothety. Here we mention only one more example (see Fig. 2).

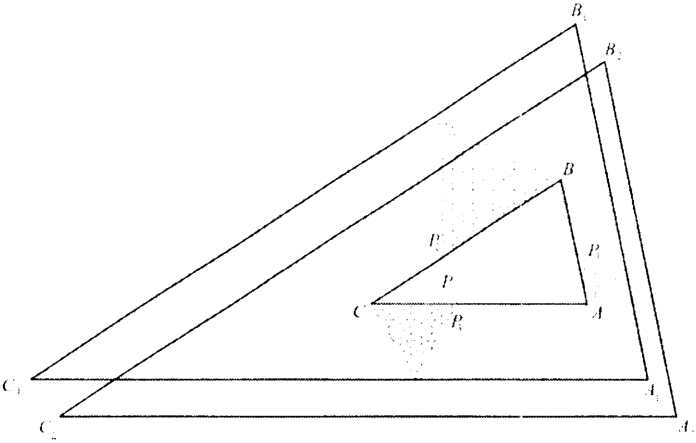


Figure 2.

Theorem 5. *Consider the triangle ABC and one of its inner points P. Let the pedals of P on the sides AB, BC, CA be P_1, P_2 and P_3, respectively. If we build regular triangles on the segments of the sides defined by the pedals, then the sum of the areas of the triangles erected on the segments AP_1, BP_2 and CP_3 equals the sum of the triangles erected on the segments P_1B, P_2C and P_3A. Moreover, if we consider those vertices of the "left" triangles which are not on the sides of ABC and draw parallel lines to the sides of the original triangle through of them, then the triangle bounded by these lines is homothetic to ABC and the ratio of homothety is*

$$\lambda=1+\frac{\sqrt{3}}{2}\cot\omega.$$

Similar homothety holds for the triangle constructed from the "right" builded triangles.

3. New results on polygons

In this section we generalize Theorem 1 for convex polygons and prove some further results about quadrilaterals.

Theorem 6. *Consider the convex polygon $A_1A_2\dots A_n$ and one of its inner points P. Let the pedals of P on the sides $A_1A_2, A_2A_3, \dots, A_{n-1}A_n, A_nA_1$ be $P_1, P_2, \dots, P_{n-1}, P_n$, respectively. If we build "left" squares onto the segments A_iP_i, $(i = 1, \dots, n)$ and "right" squares onto the segments P_iA_{i+1}, $(i = 1, \dots, n-1)$ and P_nA_1, then the sum of the areas of "left" squares equals the sum of the area of "right" squares.*

Proof. Applying the phytagorean theorem for the triangles PA_iP_i one can write

$$A_iP_i^2 = PA_i^2 - PP_i^2, \ i = 1, \dots, n.$$

Similarly

$$\begin{aligned} P_iA_{i+1}^2 &= PA_{i+1}^2 - PP_i^2, \ i = 1, \dots, n-1 \\ P_nA_1^2 &= PA_1^2 - PP_n^2. \end{aligned}$$

This yields

$$\begin{aligned} \sum_{i=1}^{n} A_iP_i^2 &= \sum_{i=1}^{n} (PA_i^2 - PP_i^2) \\ &= \sum_{i=1}^{n-1} (PA_{i+1}^2 - PP_i^2) + PA_1^2 - PP_n^2 \\ &= \sum_{i=1}^{n-1} P_iA_{i+1}^2 + P_nA_1^2, \end{aligned}$$

which completes the proof.

The statement remains valid if the builded quadrilaterals are not squares but rectangles similar to each other as it was in the triangle case (c.f. the proof of Theorem 3).

The statement of Theorem 6 can be seen for pentagons in Fig. 3. We have to remark, that if we consider the pentagons bounded by the lines containing the sides of the squares parallel to the sides of the original pentagon, the two pentagons are not homothetic to each other. Generally speaking this property is valid only for triangles. For special cases, however, homothety still holds for quadrilaterals, as we will see in the next theorems.

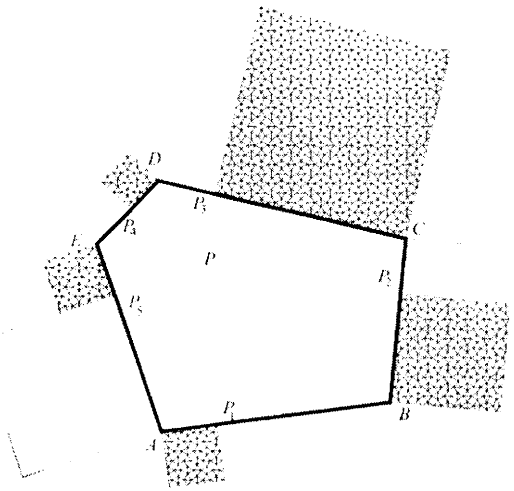


Figure 3.

Theorem 7. *Consider the rectangle $ABCD$ and one of its inner points P. Let the pedals of P on the sides AB, BC, CD and DA be P_1, P_2, P_3 and P_4, respectively. If we build similar rectangles on the segments of the sides defined by the pedals in a way, that the larger sides of the rectangles are all parallel to the larger side of the original one, then the sum of the areas of the rectangles erected on the segments AP_1, BP_2, CP_3 and DP_4 equals the sum of the rectangles erected on the segments P_1B, P_2C, P_3D and P_4A. Moreover, the rectangle bounded by the lines containing the outer sides of the "left" rectangles is homothetic to the original one and the ratio of homothety is $\lambda = 2$. Similar statement holds for the rights rectangles.*

Proof. The first part of the statement can be proved analogously to Theorem 3 and 6. For the ratio of homothety let us denote the ratio of the two sides of the rectangle by $\rho = \frac{AB}{BC}$. Consider the "left" rectangles. The sides of these rectangles parallel to AB are AP_1, ρBP_2, CP_3 and ρDP_4 (c.f. Fig. 4).

The side $A'B'$ of the large rectangle parallel to AB is the sum of these sides:

$$A'B' = AP_1 + \rho BP_2 + CP_3 + \rho DP_4,$$

but $AP_1 + CP_3 = AB$, while $\rho BP_2 + \rho DP_4 = \rho BC = AB$, thus $A'B' = 2AB$. Similarly $B'C' = 2BC$ and this was to be proved.

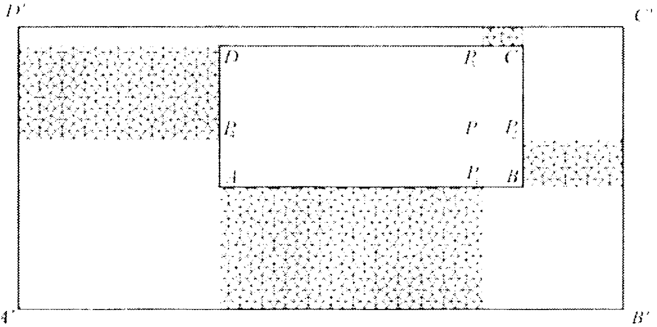


Figure 4.

Finally we remark, that the orientation of the builded rectangles in Theorem 7 is important only in terms of homothety. If the rectangles are builded in a way that always their longer sides coincide to the segments defined by the pedals, then the sum of the areas of the "left" rectangles remains equal to the "right" one, but the large rectangle is no longer similar to the original one: the ratio of its sides is

$$\frac{A'B'}{B'C'} = \frac{a^2+b^2}{2ab},$$

where a and b are the sides of the original rectangle.

References

[1] Bottema, O., *De Elementaire Meetkunde van het Platte Vlak*, Nordhoff, 1938.

[2] Dergiades, N., van Lamoen, F., Rectangles attached to sides of a triangle, *Forum Geom.* **3** (2003), 145–159.

[2] Ehrmann, J. P., van Lamoen, F., Some similarities associated with pedals, *Forum Geom.* **2** (2002), 163–166.

[3] Kimberling, C., Triangle centers and central triangles, *Congressus Numerantinum* **129** (1998), 1–285.

Éva Sashalmi and Miklós Hoffmann
Department of Mathematics
Károly Eszterházy College
Leányka str. 4.
H-3300 Eger, Hungary
E-mail: saske@ektf.hu; hofi@ektf.hu

ELEMENTARY PROBLEMS WHICH ARE EQUIVALENT TO THE GOLDBACH'S CONJECTURE

Bui Minh Phong and Li Dongdong (Budapest, Hungary)

Abstract. We denote by $\{p_1=2,\ p_2=3,\ p_3=5,\dots,\ p_k,\dots\}$ the sequence of increasing primes, and for each positive integer $k \geq 1$ let

$$S(k):=\min\{2n>p_k:\ 2n-p_1,\ 2n-p_2,\dots,\ 2n-p_k \text{ all are composite numbers}\}.$$

We prove that the following conjectures are equivalent to the Goldbach's conjecture.

Conjecture B. For every positive integer k, we have

$$S(k) \geq p_{k+1} + 3.$$

Conjecture C. For every positive integer k, the number $S(k)$ is the sum of two odd primes.

1. Introduction

Goldbach wrote a letter to Euler in 1742 suggesting that every integer $n > 5$ is the sum of three primes. Euler replied that this is equivalent to the following statement:

Conjecture A. *Every even integer* $2n > 4$ *is the sum of two odd primes.*

This is now known as Goldbach's conjecture. A. Schinzel showed that Goldbach's conjecture is equivalent to every integer $n > 17$ is the sum of three distinct primes. It has been proven that every even integer is the sum of at most six primes [2] (Goldbach suggests two) and in 1966 Chen proved every sufficiently large even integers is the sum of a prime plus a number with no more than two prime factors. In 1993 Sinisalo [5] verified Goldbach's conjecture for all integers less than $4\cdot 10^{11}$. More recently Jean-Marc Deshouillers, Yannick Saouter and Herman te Riele [1] have verified this up to 10^{14} with the help of a Cray C90 and various workstations. In July 1998, Joerg Richstein [4] completed a verification to $4\cdot 10^{14}$ and placed a list of champions online. See the monograf of P. Ribenboim [3] for more information.

In the following, we shall denote by $\mathcal{P}$ the set of all increasing primes, that is

$$\mathcal{P} := \{p_1 = 2,\ p_2 = 3,\ p_3 = 5, \dots,\ p_k,\ \dots\}.$$

For each positive integer $k \geq 1$, let

$$\mathcal{A}_k := \{2n > p_k\colon\ 2n - p_1, 2n - p_2, \ldots, 2n - p_k \text{ all are composite numbers}\}.$$

Since $p_1 \cdots p_k \in \mathcal{A}_k \subseteq \mathbf{N}$, therefore $\mathcal{A}_k$ has a minimum element. Let

$$S(k) := \min \mathcal{A}_k.$$

We shall prove that the following conjectures are equivalent to Conjecture A.

Conjecture B. *For every positive integer k, we have*

$$S(k) \geq p_{k+1} + 3.$$

Conjecture C. *For every positive integer k, the number $S(k)$ is the sum of two odd primes.*

The purpose of this note is to prove the following

Theorem. *We have*

(a) *Every even integer $2n > 4$ is the sum of two odd primes if and only if*

$$S(k) \geq p_{k+1} + 3. \tag{1}$$

holds for every positive integer k.

(b) *Every even integer $2n > 4$ is the sum of two odd primes if and only if the number $S(k)$ is the sum of two odd primes for all positive integers k.*

In the other words, Conjectures A, B and C are equivalent.

2. Lemmas

In the following we denote by G the set of all even positive integers which are the sums of two odd primes. Goldbach's conjecture states that G contains all even integers $2n \geq 6$.

Lemma 1. *We have*

$$\{\,2n\colon\ 6 \leq 2n \leq p_k + 3\,\} \subset G \quad \textit{if and only if} \quad \{2n\colon\ 6 \leq 2n < S(k)\} \subset G.$$

Proof. It follows from the definition of $S(k)$ that $S(k) \geq p_k + 9$, consequently

$$\{2n\colon\ 6 \leq 2n \leq p_k + 3\} \subset G \quad \text{if} \quad \{2n\colon\ 6 \leq 2n < S(k)\} \subset G.$$

Now assume that $\{2n\colon\ 6\ \le 2n\ \le p_k+3\} \subset G$. Let $2N$ be an even integer with $6\ \le\ 2N\ <\ S(k)$. If $2N\ \le\ p_k+3$, then we have $2N\ \in\ G$ by our assumption. Let $p_k+3\ <\ 2N\ <\ S(k)$. Hence

$$2N - p_1\ >\ 2N - p_2\ >\ \cdots\ >\ 2N - p_k\ >\ 3.$$

On the other hand, the conditions $2N\ <\ S(k)$ and $S(k) = \min\ \mathcal{A}_k$ yield

$$2N \notin \mathcal{A}_k.$$

Since

$$\mathcal{A}_k =\ \{2n > p_k\colon\ 2n - p_1,\ 2n - p_2,\ \ldots,\ 2n - p_k\ \text{ all are composite numbers}\},$$

the last relations imply that

$$2N - p_i \quad \text{is a prime for some} \quad p_i \in \{p_1,\ p_2,\ p_3, \ldots,\ p_k\}.$$

Consequently, $2N\ \in\ G$, and so Lemma 1 is proved.

Lemma 2. *Let k be a positive integer. Then*

$$\{2n\colon\ S(k) \le 2n < S(k+1)\}\ \subset\ G \quad \textit{if and only if} \quad S(k) \ge p_{k+1}+3.$$

Proof. Assume that $S(k) \ne S(k+1)$ and $\{2n\colon\ S(k) \le 2n < S(k+1)\} \subset G$. Then we have $S(k) = p+q$ for for some primes p and q. Since the numbers $S(k)-p$ and $S(k)-q$ are primes, we infer from the definition of $S(k)$ that $p > p_k$ and $q > p_k$. Consequently, $S(k) = p+q \ge 2p_k+4 \ge p_{k+1}+3$.

Now assume that $S(k) \ne S(k+1)$ and $S(k) > p_{k+1}+3$. Let $2N$ be an even integer for which $S(k) \le 2N < S(k+1)$ is satisfied. As we have seen in the proof of Lemma 1, in this case we also have $2N \notin \mathcal{A}_{k+1}$ and

$$2N - p_1\ >\ 2N - p_2\ >\ \ldots\ >\ 2N - p_k\ > 2N - p_{k+1} \ge S(k) - p_{k+1} >\ 3.$$

Consequently,

$$2N - p_i \quad \text{is a prime for some} \quad p_i \in \{p_1,\ p_2,\ p_3, \cdots,\ p_k,\ p_{k+1}\},$$

which shows that $2N \in G$.

Finally, in the case $S(k) = S(k+1)$ we also have that $S(k) = S(k+1) \ge p_{k+1}+9 > p_{k+1}+1$ by the definition of $S(k+1)$.

The proof of Lemma 2 is finished.

3. Proof of the theorem

Proof of (a). Assume that every even integer $2n > 4$ is the sum of two odd primes. In this case we infer from Lemma 2 that $S(k) \geq p_{k+1}+3$. Thus, Conjecture A implies Conjecture B.

Now we assume that Conjecture B is true, that is (1) holds for every positive integer k. Hence, Lemma 2 shows that

$$\{2n\colon 6 \leq 2n < S(k+1)\} \subset G \tag{2}$$

holds for all positive integers k.

Finally, let $2n > 4$ be any even integer. It is clear to see from the definition of $S(k)$ that $S(k) > p_k$. Hence

$$S(k) \to \infty \quad \text{as} \quad k \to \infty.$$

Consequently, $S(\ell) > 2n$ is true for some positive integer ℓ, and so we get from (2) that $2n \in G$. The proof of the the part (a) of the theorem is completed.

Proof of (b). It is obvious that Conjecture C is a consequence of Conjecture A.

Assume now that the conjecture C is true, that is, for each positive integer k, we have $S(k) = p + q$ for for some primes p and q. Since the numbers $S_k - p$ and $S(k) - q$ are primes, we also have $p > p_k$ and $q > p_k$. Consequently,

$$S(k) = p + q > 2p_k \geq p_{k+1} + 1,$$

and so Conjecture B is true. This with (a) completes the proof of (b). The assertion (b) is proved.

The proof of the theorem is finished.

References

[1] Deshoulliers, J. M., te Riele, H. J. J., Saouter, Y., New experimental results concerning the Goldbach conjecture, *Proc. 3rd Int. Symp. on Algorithmic Number Theory,* LNCS 1423 (1998), 204–215.

[2] Ramar, U, O., On Schnirelman's constant, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **22:4** (1995) 645–706.

[3] Ribenboim, P., *The New Book of Prime Number Records,* Springer-Verlag, New York, 1995.

[4] Richstein, J., Verifying the Goldbach Conjecture up to $4 \cdot 10^{14}$, to appear in *Mathematics of Computation.*

[5] SINISALO, M. K., Checking the Goldbach Conjecture up to $4 \cdot 10^{11}$, *Math. Comp.* **61** (1993), 931–934.

Bui Minh Phong and Li Dongdong
Eötvös Loránd University
Department of Computer Algebra
Pázmány Péter sétány I/D.
H-1117 Budapest, Hungary
E-mail: bui@compalg.inf.elte.hu

GENERALIZED FIBONACCI-TYPE NUMBERS AS MATRIX DETERMINANTS

Ferenc Mátyás (Eger, Hungary)

Abstract. In this note we construct such matrix determinants of complex entries which are equal to the numbers defined by Fibonacci-type linear recursions of order $k \geq 2$.

AMS Classification Number: 11B39, 11C20

1. Introduction

Let $k \geq 2$ be an integer. The recursive sequence $\{G_n\}_{n=2-k}^{\infty}$ of order k is defined for every $n \geq 2$ by the recursion

$$G_n = p_1 G_{n-1} + p_2 G_{n-2} + \cdots + p_k G_{n-k}, \tag{1}$$

where p_i $(1 \leq i \leq k)$ and G_j $(2-k \leq j \leq 1)$ are given complex numbers and $p_1 p_k G_1$ is not equal to zero. For brevity, we will use the formula

$$G_n = G_n(p_1, p_2, \ldots, p_k, G_{2-k}, G_{3-k}, \ldots, G_1),$$

as well. In the case $k = 2$ we get the wellknown family of second order linear recurrences of complex numbers. The two most important sequences from this family are the Fibonacci $\{F_n\}$ and the Lucas $\{L_n\}$ sequences, where

$$F_n = G_n(1,1,0,1) \text{ and } L_n = G_n(1,1,2,1),$$

respectively.

The close connections between the Fibinacci (and Lucas) numbers and suitable matrix determinants have been known for ages. For example, it is known that for $k \geq 1$ F_k is equal to the following tridiagonal matrix determinant of $k \times k$:

$$F_k = \det \begin{pmatrix} 1 & i & & & & \\ i & 1 & i & & & \\ & i & 1 & i & & \\ & & i & 1 & \ddots & \\ & & & \ddots & \ddots & i \\ & & & & i & 1 \end{pmatrix}.$$

Recently, some papers have been publicated in this field. (For more information about the list of these papers see [1].) One of the latest such papers was written by Nathan D. Cahill and Darren A. Narayan [1]. They have constructed such family of tridiagonal matrix determinants of $k \times k$ which generate any arbitrary linear subsequence

$$F_{\alpha k+\beta} \text{ or } L_{\alpha k+\beta} \ (k = 1, 2, \dots)$$

of the Fibonacci or Lucas numbers. For example,

$$F_{4k-2} = \det \begin{pmatrix} 1 & 0 & & & & \\ 0 & 8 & 1 & & & \\ & 1 & 7 & 1 & & \\ & & 1 & 7 & \ddots & \\ & & & \ddots & \ddots & 1 \\ & & & & 1 & 7 \end{pmatrix}.$$

The aim of this note is to investigate suitable matrix determinants of $n \times n$ which form the terms G_n of the Fibonacci-type sequences defined by (1). In this paper we suppose that in (1) $p_1 \neq 0, p_j = 0$ $(2 \leq j \leq k-1$ for $3 \leq k), p_k = \pm 1$, and $G_1 \neq 0$, that is we deal with the family of sequences

$$G_n = G_n(p_1, 0, \dots, 0, \pm 1, G_{2-k}, G_{3-k}, \dots, G_1). \tag{2}$$

(Naturally, the sign ± in (2) is fixed in a given sequence.)

For our aim we construct the matrix $\mathbf{A}_{n \times n} = (a_{t,j})$ of complex numbers by the following forms: $a_{1,1} = G_1$, $a_{1,j} = -e^{j+1}G_{j-k}$ $(2 \leq j \leq k)$, $a_{j+1,j} = -e^3$ $(1 \leq j \leq n-1)$, $a_{j,k+j-1} = -e^{k+1}$ $(2 \leq j \leq n+1-k), a_{j,j} = p_1$ $(2 \leq j \leq n)$ and the other entries are equal to 0. That is,

$$\mathbf{A}_{n \times n} \tag{3}$$

$$= \begin{pmatrix} G_1 & -e^3G_{2-k} & -e^4G_{3-k} & \cdots & -e^{k+1}G_0 & 0 & 0 & \cdots & 0 & 0 \\ -e^3 & p_1 & 0 & \cdots & 0 & -e^{k+1} & 0 & \cdots & 0 & 0 \\ 0 & -e^3 & p_1 & \cdots & 0 & 0 & -e^{k+1} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & -e^3 & p_1 \end{pmatrix}$$

where $e = -1$ if $p_k = -1$ and $e = -i$ if $p_k = 1$.

2. Result

We shall prove the following theorem.

Theorem. *Let the sqeuence $\{G_n\}_{n=2-k}^{\infty}$ be defined by (2), where $p_1G_1 \neq 0$, $p_k = \pm 1$ and $k \geq 2$. Let the matrix $\mathbf{A}_{n\times n}$ be defined by (3). Then for every $n \geq 1$*

$$G_n = \det(\mathbf{A}_{n\times n}).$$

Remark. In the case $k = 2$ our matrices $\mathbf{A}_{n\times n}$ are of tridiagonal ones.

Proof. First we consider the case $1 \leq n \leq k$. Then, for $n = 1$

$$\det(\mathbf{A}_{1\times 1}) = G_1.$$

If $n = 2$ or 3, then

$$\det\begin{pmatrix} G_1 & -e^3G_{2-k} \\ -e^3 & p_1 \end{pmatrix} = p_1G_1 - e^6G_{2-k}$$

$$= p_1G_1 + p_kG_{2-k} = G_2$$

and

$$\det\begin{pmatrix} G_1 & -e^3G_{2-k} & -e^4G_{3-k} \\ -e^3 & p_1 & 0 \\ 0 & -e^3 & p_1 \end{pmatrix}$$

$$= p_1G_2 - e^4G_{3-k}e^6 = p_1G_2 - e^2G_{3-k} = p_1G_2 + p_kG_{3-k} = G_3.$$

Suppose that $G_{n-j} = \det(\mathbf{A}_{n-j\times n-j})$ $(j = 1, 2, 3)$ holds for an integer n, where $4 \leq n < k$. Then, developing the determinant

$$\det\left(\mathbf{A}_{n\times n}\right) = \det\begin{pmatrix} G_1 & -e^3G_{2-k} & -e^4G_{3-k} & \cdots & -e^nG_{n-1-k} & -e^{n+1}G_{n-k} \\ -e^3 & p_1 & 0 & \cdots & 0 & 0 \\ 0 & -e^3 & p_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -e^3 & p_1 \end{pmatrix}$$

with respect to the last column, we have

$$\det\left(\mathbf{A}_{n\times n}\right) = p_1G_{n-1} - (-1)^{n+1}e^{n+1}G_{n-k}\left(-e^3\right)^{n-1}$$

$$= p_1G_{n-1} + (-1)^{2n+1}e^{4n-2}G_{n-k} = p_1G_{n-1} + p_kG_{n-k} = G_n.$$

That is, our theorem holds for every n, if $1 \leq n \leq k$.

Now, we shall deal with the case $n > k$. If $n = k+1$ then

$$\det\left(\mathbf{A}_{k+1\times k+1}\right) = \det\begin{pmatrix} G_1 & -e^3G_{2-k} & -e^4G_{3-k} & \cdots & -e^{k+1}G_0 & 0 \\ -e^3 & p_1 & 0 & \cdots & 0 & -e^{k+1} \\ 0 & -e^3 & p_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -e^3 & p_1 \end{pmatrix}$$

$$= p_1G_k + e^3\det\begin{pmatrix} G_1 & -e^3G_{2-k} & -e^4G_{3-k} & \cdots & -e^kG_{-1} & 0 \\ -e^3 & p_1 & 0 & \cdots & 0 & -e^{k+1} \\ 0 & -e^3 & p_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -e^3 & 0 \end{pmatrix}.$$

Developing successively the resulting determinants with respect to their last rows, we have

$$\det\left(\mathbf{A}_{n\times n}\right) = p_1G_k + \left(e^3\right)^{k-1}\det\begin{pmatrix} G_1 & 0 \\ -e^3 & -e^{k+1} \end{pmatrix}$$

$$= p_1G_k - e^{3k-3}e^{k+1}G_1 = p_1G_k + p_kG_1 = G_{k+1}.$$

Let us suppose that $\det\left(\mathbf{A}_{n-j\times n-j}\right) = G_{n-j}$ $(1 \le j \le k)$ holds for an integer $n \geq k+2$. In this case

$$\det\left(\mathbf{A}_{n\times n}\right)$$

$$= \det\begin{pmatrix} G_1 & -e^3G_{2-k} & \cdots & -e^{k+1}G_0 & 0 & 0 & \cdots & 0 & 0 \\ -e^3 & p_1 & \cdots & 0 & -e^{k+1} & 0 & \cdots & 0 & 0 \\ 0 & -e^3 & \cdots & 0 & 0 & -e^{k+1} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & -e^3 & p_1 \end{pmatrix}$$

$$= p_1G_{n-1} + e^3\det\begin{pmatrix} G_1 & -e^3G_{2-k} & \cdots & -e^{k+1}G_0 & 0 & \cdots & 0 & 0 \\ -e^3 & p_1 & \cdots & 0 & -e^{k+1} & \cdots & 0 & 0 \\ 0 & -e^3 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & -e^3 & 0 \end{pmatrix}.$$

Now, develop successively the resulting determinants with respect to their last rows. Then one can get the following equalities:

$$\det\left(\mathbf{A}_{n\times n}\right) = p_1G_{n-1} + \left(e^3\right)^{k-1}\left(-e^{k+1}\right)G_{n-k}$$

$$= p_1G_{n-1} - e^2G_{n-k} = p_1G_{n-1} + p_kG_{n-k} = G_n.$$

This completes the proof of the Theorem.

Reference

[1] Cahill, N. D., Narayan, D. A., Fibonacci and Lucas Numbers as Tridiagonal Matrix Determinant, *The Fibonacci Quarterly* **42** (2004), 216–221.

Ferenc Mátyás
Department of Mathematics
Eszterházy Károly College
H-3301 Eger, P.O. Box 43.
Hungary
E-mail: matyas@ektf.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 45–51*

ON TRANSFORMATION MATRICES CONNECTED TO NORMAL BASES IN RINGS

J. Kostra (Žilina, Slovakia), M. Vavroš (Ostrava, Czech Republic)

Abstract. In the paper [6, Problem 7] there is presented an open problem to characterize all circulant matrices which transform any normal basis of any order of cyclic algebraic number field K to a normal basis of its suborder in K. A conjecture is that if a circulant matrix $\mathbf{A}=\mathrm{circ}_n(a_1,a_2,\dots,a_n)$, $\sum\limits_{i=1}^{n} a_i=\pm 1$, transforms some normal basis of ring to normal basis of its subring then it transforms any normal basis of ring to normal basis of its subring. In this paper it is shown that if $\sum\limits_{i=1}^{n} a_i\neq\pm 1$, then the related conjecture is false.

AMS Classification Number: 11R16, 11C20

1. Introduction

Let K be a tamely ramified cyclic algebraic number field of degree n over the rational numbers $\mathbb{Q}$. It seems that $K\subset\mathbb{Q}(\zeta_m)$, where ζ_m is a m-th primitive root of unity and m is square free. Such a field has a normal basis over the rationals $\mathbb{Q}$, i.e. a basis consisting of all conjugations of one element. Transformation matrices between two normal bases of K over $\mathbb{Q}$ are exactly regular rational circulant matrices of degree n.

In the paper [6, Problem 7] there is presented an open problem to characterize all circulant matrices which transform any normal basis of any order of cyclic algebraic number field K to a normal basis of its suborder in K. A conjecture is that if a circulant matrix $\mathbf{A}=\mathrm{circ}_n(a_1,a_2,\dots,a_n)$, $\sum\limits_{i=1}^{n} a_i=\pm 1$, transforms some normal basis of ring to a normal basis of its subring, then it transforms any normal basis of ring to a normal basis of its subring. In the paper it is shown that if $\sum\limits_{i=1}^{n} a_i\neq\pm 1$, then the related conjecture is false.

In the paper [5], the special class of circulant matrices with integral rational elements is characterized by the following proposition.

This research was supported by VEGA 2/4138/24

Proposition 1. *Let K be a cyclic algebraic number field of degree n over rational numbers. Let*

$$\mathbf{A} = \mathrm{circ}_n(a_1, a_2, \ldots, a_n)$$

be a circulant matrix and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. By A_i, $i = 1, 2, \ldots n$ we denote the algebraic complement of element a_i in the matrix $\mathbf{A}$. Let

$$a_1 + a_2 + \cdots + a_n = \pm 1$$

and

$$a_i \equiv a_j \pmod{h}$$

for $i, j \in \{1, 2, \ldots, n\}$, where

$$h = \frac{\det \mathbf{A}}{\gcd(A_1, A_2, \ldots, A_n)}.$$

Then the matrix $\mathbf{A}$ transforms a normal basis of an order B of the field K to a normal basis of an order C of the field K, where $C \subseteq B$.

In the papers [3, 4] previous matrices are characterized by Theorem 3 [4].

Proposition 2. *Let G be a multiplicative semigroup of circulant matrices of degree n, satisfying the assumptions of Proposition 1. Let U be multiplicative group of integral unimodular circulant matrices of degree n. Let H be the semigroup of circulant matrices of type $\mathrm{circ}_n(a, b, \ldots, b)$, such that*

$$a + (n-1)b = \pm 1.$$

Then $G = H \cdot U$.

2. Results

First we recall the definition of order of algebraic number field.

Definition 1. Let K be an algebraic number field and let the degree of the extension $K/\mathbb{Q}$ be equal to n. A $\mathbb{Z}$-module $B \subset K$ is called an order of the field K if it satisfies the following conditions:

1. $1 \in B$,
2. B has a basis over $\mathbb{Z}$ consisting of n elements,
3. B is a ring.

Remark 1. Matrices from Proposition 1 transform also normal bases rings which have a basis over $\mathbb{Z}$ consisting of n elements to normal bases of their subrings. Such rings we will call semiorders.

Definition 2. Let K be an algebraic number field and let the degree of the extension $K/\mathbb{Q}$ be equal to n. A $\mathbb{Z}$-module $B \subset K$ is called a semiorder of the field K if it satisfies the following conditions:

1. B has a basis over $\mathbb{Z}$ consisting of n elements,
2. B is a ring.

In the following it will be shown that the condition

$$a + (n-1)b = \pm 1.$$

from Proposition 1 for matrix $\mathrm{circ}_n(a, b, \dots, b)$ is necessary.

Example 1. Let ζ_7 be a 7-th primitive root of unity and let $\langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle$ be a normal integral basis of the field $K = \mathbb{Q}^+(\zeta_7)$ over $\mathbb{Q}$, where

$$\varepsilon_1 = \zeta_7 + \zeta_7^6,\ \varepsilon_2 = \zeta_7^2 + \zeta_7^5,\ \varepsilon_3 = \zeta_7^3 + \zeta_7^4.$$

Let $\mathbf{A} = \mathrm{circ}_3(0, 5, 5)$ and $\langle \alpha_1, \alpha_2, \alpha_3 \rangle = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3 \rangle \cdot \mathbf{A}$, so

$$\begin{aligned} \alpha_1 &= 5\varepsilon_2 + 5\varepsilon_3\,, \\ \alpha_2 &= 5\varepsilon_1 + 5\varepsilon_3\,, \\ \alpha_3 &= 5\varepsilon_1 + 5\varepsilon_2\,. \end{aligned}$$

Then

$$\alpha_1 \cdot \alpha_2 = \frac{-5}{2}\alpha_1 + \frac{5}{2}\alpha_2 + \frac{5}{2}\alpha_3$$

and the module $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is not a ring, so $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is not a semiorder.

Example 2. Let $\varepsilon_1, \varepsilon_3, \varepsilon_3$ and $\mathbf{A}$ be the same as in above example.

Let

$$\begin{aligned} \alpha_1 &= 2\varepsilon_1\,, \\ \alpha_2 &= 2\varepsilon_2\,, \\ \alpha_3 &= 2\varepsilon_3\,. \end{aligned}$$

and $\langle \beta_1, \beta_2, \beta_3 \rangle = \langle \alpha_1, \alpha_2, \alpha_3 \rangle \cdot \mathbf{A}$, so

$$\begin{aligned} \beta_1 &= 5\alpha_2 + 5\alpha_3\,, \\ \beta_2 &= 5\alpha_1 + 5\alpha_3\,, \\ \beta_3 &= 5\alpha_1 + 5\alpha_2\,. \end{aligned}$$

Then

$$\begin{aligned} \beta_1^2 &= -50\alpha_1 - 100\alpha_2 - 150\alpha_3\,, \\ \beta_2^2 &= -150\alpha_1 - 50\alpha_2 - 100\alpha_3\,, \\ \beta_3^2 &= -100\alpha_1 - 150\alpha_2 - 50\alpha_3\,. \end{aligned}$$

and

$$\begin{aligned}\beta_1 \cdot \beta_2 &= 50\alpha_1\,,\\ \beta_2 \cdot \beta_3 &= 50\alpha_2\,,\\ \beta_3 \cdot \beta_1 &= 50\alpha_3\,.\end{aligned}$$

We have

$$\begin{aligned}\beta_1^2 &= -20\beta_1 - 10\beta_2\,,\\ \beta_2^2 &= -20\beta_2 - 10\beta_3\,,\\ \beta_3^2 &= -10\beta_1 - 20\beta_3\,.\end{aligned}$$

and

$$\begin{aligned}\beta_1 \cdot \beta_2 &= -5\beta_1 + 5\beta_2 + 5\beta_3\,,\\ \beta_2 \cdot \beta_3 &= 5\beta_1 - 5\beta_2 + 5\beta_3\,,\\ \beta_3 \cdot \beta_1 &= 5\beta_1 + 5\beta_2 - 5\beta_3\,.\end{aligned}$$

And so $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3]$ is a semiorder.

By the previous examples we have that in the case $\mathbf{A} = \mathrm{circ}_n(a_1, a_2, \ldots, a_n)$, $\sum\limits_{i=1}^{n} a_i \neq \pm 1$, the conjecture from [6], that if a circulant matrix transforms some normal basis of a semiorder to normal basis of its subsemiorder then it transforms any normal basis of any semiorder to normal basis of its subsemiorder, does not hold.

Theorem 1. *Let $\mathbf{A}' = \mathrm{circ}_n(a, b, \ldots, b)$, $a + (n-1)b = 1$. Let $\mathbf{A} = \mathrm{circ}_n(0, b-a, \ldots, b-a)$. Let $b \equiv 1 \pmod{n-1}$, then matrix $\mathbf{A} \cdot \mathbf{U}$, where $\mathbf{U}$ is a unimodular circulant matrix of degree n, transforms any normal basis of any semiorder R to a normal basis of its subsemiorder S.*

Proof. Let $\mathbf{A}' = \mathrm{circ}_n(a, b, \ldots, b)$, $a + (n-1)b = 1$, $\mathbf{A} = \mathrm{circ}_n(0, b-a, \ldots, b-a)$ and $b \equiv 1 \pmod{n-1}$. From

$$a + (n-1)b = 1$$

we obtain

$$b - a = nb - 1.$$

So

$$\det \mathbf{A} = (-1)^{n-1} \cdot (n-1) \cdot (nb-1)^n.$$

Then

$$\mathbf{A}^{-1} = \mathrm{circ}_n\left(-\frac{n-2}{(n-1)\cdot(nb-1)}, \frac{1}{(n-1)\cdot(nb-1)}, \ldots, \frac{1}{(n-1)\cdot(nb-1)}\right).$$

Let $\langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle$ be a normal basis of semiorder R. Let

$$\langle \beta_1, \beta_2, \ldots, \beta_n \rangle = \langle \alpha_1, \alpha_2, \ldots, \alpha_n \rangle \cdot \mathbf{A}$$

be a normal basis of submodule $S \subset R$. Then

$$\begin{aligned}
\beta_1 &= (nb-1)\alpha_2 + (nb-1)\alpha_3 + \cdots + (nb-1)\alpha_n\,, \\
\beta_2 &= (nb-1)\alpha_1 + (nb-1)\alpha_3 + \cdots + (nb-1)\alpha_n\,, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\beta_n &= (nb-1)\alpha_1 + (nb-1)\alpha_2 + \cdots + (nb-1)\alpha_{n-1}\,.
\end{aligned}$$

From the above it follows that for all i, j

$$\beta_i \beta_j = (nb-1)^2 \cdot (b_1\alpha_1 + b_2\alpha_2 + \cdots + b_n\alpha_n),$$

where $b_i \in \mathbb{Z}$ for all i. By the expression of $\mathbf{A}^{-1}$ we have for any i, j

$$\begin{aligned}
\beta_i \beta_j &= c_1\beta_1 + \cdots + c_n\beta_n \\
&= \frac{(nb-1)}{(n-1)} \cdot (d_1\beta_1 + \cdots + d_n\beta_n).
\end{aligned}$$

If $b \equiv 1 \pmod{n-1}$, then coefficients $c_i \in \mathbb{Z}$, and S is a subsemiorder of the semiorder R. Clearly the same holds for $\mathbf{A} \cdot \mathbf{U}$, where $\mathbf{U}$ is a unimodular circulant matrix of degree n.

Remark 2. Matrix $\mathbf{A} = \mathrm{circ}_3(0, 5, 5)$ from Examples 1, 2 was obtained from matrix $\mathbf{A}' = \mathrm{circ}_3(-3, 2, 2)$ and $2 \not\equiv 1 \pmod 2$.

Remark 3. If in the above Theorem 1 $a + (n-1)b = -1$, then if $b \equiv -1 \pmod{n-1}$ matrix $\mathbf{A}$ transforms a normal basis of any semiorder R to a normal basis of subsemiorder $S \subset R$.

The previous Theorem 1 gives the way to find a circulant matrix $\mathbf{A}$ of arbitrary degree for which there exist semiorders R_1, R_2 such that $\mathbf{A}$ transforms a normal basis of R_i to a normal basis of submodule $S_i \subset R_i$ and S_1 is a semiorder and S_2 is not a ring and so S_2 is not a semiorder.

Example 3. Let ζ_{11} be an 11-th primitive root of units and let $\langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle$, where

$$\varepsilon_1 = \zeta_{11} + \zeta_{11}^{10},\ \varepsilon_2 = \zeta_{11}^{2} + \zeta_{11}^{9},\ \varepsilon_3 = \zeta_{11}^{3} + \zeta_{11}^{8},\ \varepsilon_4 = \zeta_{11}^{4} + \zeta_{11}^{7},\ \varepsilon_5 = \zeta_{11}^{5} + \zeta_{11}^{6},$$

be a normal integral basis of the field $K = \mathbb{Q}^+(\zeta_{11})$ over $\mathbb{Q}$. The field $K = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ is the maximal real subfield of $\mathbb{Q}(\zeta_{11})$.

Let $\mathbf{A}' = \mathrm{circ}_5(a, b, b, b, b) = \mathrm{circ}_5(-7, 2, 2, 2, 2)$, $a + 4b = 1$, $b \not\equiv 1 \pmod 4$. Let

$$\mathbf{A} = \mathrm{circ}_5(0,\ 5b-1,\ 5b-1,\ 5b-1,\ 5b-1) = \mathrm{circ}_5(0, 9, 9, 9, 9),$$

$$A^{-1} = circ_5\left(-\frac{1}{12}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}\right)$$

and $R_2 = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle$, $S_2 = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle$, where

$$\langle \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5 \rangle = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle \cdot \mathbf{A},$$

so

$$\alpha_1 = 9\varepsilon_2 + 9\varepsilon_3 + 9\varepsilon_4 + 9\varepsilon_5\,,$$
$$\alpha_2 = 9\varepsilon_1 + 9\varepsilon_3 + 9\varepsilon_4 + 9\varepsilon_5\,.$$

Then

$$\alpha_1 \cdot \alpha_2 = 81\varepsilon_1 - 81\varepsilon_4 - 81\varepsilon_5.$$

After transformation by matrix $\mathbf{A}^{-1}$ we have

$$\alpha_1 \cdot \alpha_2 = -\frac{45}{4}\alpha_1 - \frac{9}{4}\alpha_2 - \frac{9}{4}\alpha_3 - \frac{81}{4}\alpha_4 - \frac{81}{4}\alpha_5.$$

From this it follows that S_2 is not a ring.

And now let $R_1 = \langle \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5 \rangle$ and $S_1 = \langle \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \rangle$, where

$$\beta_1 = 6\varepsilon_1\,,$$
$$\beta_2 = 6\varepsilon_2\,,$$
$$\beta_3 = 6\varepsilon_3\,,$$
$$\beta_4 = 6\varepsilon_4\,,$$
$$\beta_5 = 6\varepsilon_5\,.$$

$$\langle \gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5 \rangle = \langle \beta_1, \beta_2, \beta_3, \beta_4, \beta_5 \rangle \cdot \mathbf{A}$$

We have $\gamma_i\gamma_j = 36 \cdot (b_1\beta_1 + b_2\beta_2 + \cdots + b_5\beta_5)$. From the expression of $\mathbf{A}^{-1}$ it follows that $\gamma_i\gamma_j = c_1\gamma_1 + c_2\gamma_2 + \cdots + c_5\gamma_5$ with integral rational coefficients c_i. So S_1 is a semiorder.

References

[1] Borevich, Z. I., Shafarevich, I. R., *Number theory*, Nauka, Moscow, 1985. 3rd ed. (in Russian).

[2] Davis, P. J., *Circulant matrices*, A. Wiley-Interscience Publisher, John Wiley and Sons, New York–Chichester–Brisbane–Toronto, 1979.

[3] DIVIŠOVÁ, Z., KOSTRA, J., POMP, M., On transformation matrices connected to normal bases in cubic fields, *Acta Acad. Paed. Agriensis, Sectio Mathematicae* **29** (2002), 61–66.

[4] DIVIŠOVÁ, Z., KOSTRA, J., POMP, M., On transformation matrix connected to normal bases in orders, *JP Jour. Algebra, Number Theory and Appl.* **3/1** (2003), 43–52.

[5] KOSTRA, J., Orders with a normal basis, *Czechoslovak Math. Journal* **35** (1985), 391–404.

[6] KOSTRA, J., Open problems on the relation between additive and multiplicative structure, *Annales Mathematicae Silesianae* **16** (2003), 21–25.

J. Kostra
Department of Algebra, Geometry and Didactics
University of Žilina
Hurbanova 15
Žilina, Slovak Republic
E-mail: juraj.kostra@fpv.utc.sk

M. Vavroš
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: michal.vavros@osu.cz

LINEAR DIOPHANTINE EQUATION WITH THREE CONSECUTIVE BINOMIAL COEFFICIENTS

Florian Luca[*] **(UNAM, Mexico)**
László Szalay (Sopron, Hungary)

Abstract. In this note, we study the diophantine equation $A\binom{n}{k}+B\binom{n}{k+1}+C\binom{n}{k+2}=0$ in positive integers (n,k), where A, B and C are fixed integers.

AMS Classification Number: 11D04, 11D09

1. Introduction

D. Singmaster (see [3]) found infinitely many positive integer solutions (n,k) to the diophantine equation

$$(1)\qquad \binom{n}{k}=\binom{n-1}{k+1}.$$

All such solutions arise in a natural way from the sequence of Fibonacci numbers $(F_m)_{m\geq 0}$ given by $F_0=0$, $F_1=1$ and $F_{m+2}=F_{m+1}+F_m$ for $m\geq 0$. Goetgheluck (see [1]) extended the above result and found infinitely many positive integer solutions (n,k) for the diophantine equation

$$2\binom{n}{k}=\binom{n-1}{k+1}.$$

These solutions arise in a natural way from the positive integer solutions of the Pell equation $x^2-3y^2=-2$. Several other diophantine equations involving binomial coefficients have been considered in [2], [4] and [5].

In this note, we fix three integers A, B, C, not all zero, and look at the positive integer solutions (n,k) of the equation $A\binom{n}{k}+B\binom{n}{k+1}+C\binom{n}{k+2}=0$. To avoid degenerate cases, we shall assume that $1\leq k<k+2\leq n-1$. We shall also assume that $AC\neq 0$. Indeed, say if $A=0$, then the above equation simplifies to

[*] This research was partially sponsored by grants SEP-CONACYT 37259-E and 37260-E.

$$B\binom{n}{k+1}+C\binom{n}{k+2}=0. \tag{2}$$

Obviously, equation (2) has no solution if $BC>0$. Suppose that $BC<0$ (say, up to changing signs, that $B<0$ and $C>0$) and that $\gcd(B,C)=1$. Then equation (2) implies $B(k+2)+C(n-k-1)=0$, which can be rewritten as $n=((C-B)k+C-2B)/C=k+1-B(k+2)/C$. Thus, n is an integer if and only if $k\equiv -2 \pmod{C}$. Moreover, the conditions $1\le k<k+2\le n-1$ are always fulfilled if $k>1$ and $k\ge -2(1+C/B)$, and therefore (2) has infinitely many solutions.

The case when $C=0$ can be reduced to the case when $A=0$ by using the symmetry of the binomial coefficients and the substitution $(A,C,k)\longmapsto(C,A,n-k-2)$.

Acknowledgements. This paper was written during a very enjoyable visit by the first author to University of West Hungary in Sopron; he wishes to express his thanks to that institution for the hospitality and support.

2. Main Result

It is clear that we may assume that $\gcd(A,B,C)=1$ and that $A>0$. Our main result is the following.

Theorem. *Let A, B and C be integers with $A>0$, $C\neq 0$ and $\gcd(A,B,C)=1$. If the diophantine equation*

$$A\binom{n}{k}+B\binom{n}{k+1}+C\binom{n}{k+2}=0. \tag{3}$$

admits infinitely many integer solutions $1\le k<k+2\le n-1$, then one of the following holds:

(i) $B=A+C$ and $C<0$, case in which all the solutions (n,k) are on the line

$$A(k+2)+C(n-k)=0,$$

(ii) $A=A_0^2$, $B=-2A_0C_0$, $C=C_0^2$ hold with some positive coprime integers A_0 and C_0, case in which all solutions (n,k) with $1\le k<k+2\le n-1$ of (3) are of the form

$$k+2=\frac{t(t+C_0)}{A_0(A_0+C_0)} \qquad \text{and} \qquad n-k=\frac{t(t-A_0)}{C_0(A_0+C_0)} \tag{4}$$

for some positive integer t.
(iii) $B \neq A + C$, $D = B^2 - 4AC > 0$ is not a perfect square, and

$$X^2 - DY^2 = E \tag{5}$$

holds, where $X = (B^2 - 4AC)(n-k) - A(B-2C)$, $Y = 2A(k+2) + B(n-k) - A$, $E = 4A^2C(A-B+C)$, case in which all positive integer solutions (n,k) of equation (3) can be found by solving the Pell like equation (5).

Proof. After simplifications, equation (3) becomes

$$A(k+1)(k+2) + B(k+2)(n-k) + C(n-k)(n-k-1) = 0.$$

Writing $k+2 = x$, $n-k = y$ we get

$$Ax(x-1) + Bxy + Cy(y-1) = 0,$$

or, equivalently,

$$Ax^2 + Bxy + Cy^2 - Ax - Cy = 0. \tag{6}$$

We shall assume that $D := B^2 - 4AC \neq 0$, and we shall return to the case when $D = 0$ later.

With the substitution $x = u + \alpha$, $y = v + \beta$, we get that the above relation becomes

$$(Au^2 + Buv + Cv^2) + (2A\alpha + B\beta - A)u + (B\alpha + 2C\beta - C)v \tag{7}$$
$$= -(A\alpha^2 + B\alpha\beta + C\beta^2) + A\alpha + C\beta.$$

We choose α and β such that the coefficients of the linear terms in u and v in equation (7) vanish. These lead to the system of equations

$$2A\alpha + B\beta = A,$$
$$B\alpha + 2C\beta = C,$$

whose rational solution is

$$\alpha = \frac{C(B-2A)}{B^2 - 4AC},$$
$$\beta = \frac{A(B-2C)}{B^2 - 4AC}.$$

Note that we may divide by $D = B^2 - 4AC$, because $D \neq 0$. With the above formulas for α and β, we get that

$$-(A\alpha^2 + B\alpha\beta + C\beta^2) + A\alpha + C\beta = \frac{-AC(A-B+C)}{B^2-4AC},$$

and so equation (7) becomes

$$Au^2 + Buv + Cv^2 = \frac{-AC(A-B+C)}{B^2-4AC}.$$

This last equation implies that

$$(2Au + Bv)^2 - (B^2 - 4AC)v^2 = \frac{-4A^2C(A-B+C)}{B^2-4AC},$$

and since

$$2Au + Bv = (2Ax + By) - (2A\alpha + B\beta)$$
$$= (2Ax + By) - \frac{2AC(B-2A) + AB(B-2C)}{B^2-4AC} = 2Ax + By - A,$$

while

$$v = y - \beta = \frac{(B^2-4AC)y - A(B-2C)}{B^2-4AC},$$

it follows that if we write

$$X := (B^2 - 4AC)y - A(B-2C),$$
$$Y := 2Ax + By - A,$$
$$E := 4A^2C(A-B+C),$$

we get that $X, Y \in \mathbb{Z}$ and

$$(8) \qquad X^2 - DY^2 = E.$$

We thus see that if $D < 0$, then the diophantine equation (3) has at most finitely integer solutions $1 \leq k < k+2 \leq n-1$. We now assume that $D > 0$. If $E = 0$, then since $AC \neq 0$, it follows that $B = A+C$. In this case, $D = B^2 - 4AC = (A-C)^2$, and so pairs of integers X, Y satisfying equation (8) satisfy either

$$X = (C-A)Y \qquad \text{or} \qquad X = (A-C)Y.$$

In terms of the variables x and y, the above lines become

$$x + y = 1 \qquad \text{or} \qquad Ax + Cy = 0.$$

It is clear that the first one admits no integer solutions $x = k + 2$ and $y = n - k$ for $1 \le k < k + 2 \le n - 1$, while the second one admits infinitely many such solutions if and only if $C < 0$ (whereas if $C > 0$, then the second one does not admit any such solutions either). Finally, if $E \neq 0$, then equation (8) admits only finitely many solutions (or none) if D is a perfect square, while if D is not a perfect square, the above equation (8) is a Pell like equation, which either has no solutions, or it has infinitely many, and in this later case all integer solutions (X, Y) of such equation belong to finitely many binary recurrent sequences whose roots are the fundamental unit ζ of norm 1 in the quadratic order $\mathbb{K} = \mathbb{Q}[\sqrt{D}]$ and its conjugate ζ_1, respectively.

Finally, we deal with the case $D = 0$. In this case, $B^2 = 4AC$, so $B = 2B_0$, and $B_0^2 = AC$. Since $\gcd(A, B, C) = 1$, and $A > 0$, it follows that $\gcd(A, C) = 1$, and then that $A = A_0^2$ and $C = C_0^2$ hold with some positive integers A_0 and C_0. Hence, $B_0 = \pm A_0C_0$. When $B_0 = A_0C_0$, it is clear that the left hand side of equation (3) is positive whenever $1 \le k < k + 2 \le n - 1$. Thus, $B_0 = -A_0C_0$, and therefore $B = -2A_0C_0$. Equation (6) becomes

$$A_0^2x^2 - 2A_0C_0xy + C_0^2y^2 = A_0^2x + C_0^2y,$$

which can be rewritten as

$$(A_0x - C_0y)^2 = A_0^2x + C_0^2y = A_0(A_0x - C_0y) + C_0(A_0 + C_0)y.$$

Setting $t := A_0x - C_0y$, we get that

$$C_0(A_0 + C_0)y = t^2 - A_0t,$$

leading to

$$y = \frac{t(t - A_0)}{C_0(A_0 + C_0)},$$

and since $A_0x = C_0y + t$, we get that

$$x = \frac{t(t + C_0)}{A_0(A_0 + C_0)},$$

which lead to formulae (4) via the fact that $x = k + 2$, and $y = n - k$. Note that since x, t, and y are integers, it follows that t is in certain arithmetical progressions modulo $A_0C_0(A_0 + C_0)$, and from the fact that $x \ge 3$ and $y \ge 3$, it follows that either $t > G_1 := G_1(A_0, C_0)$, or $t < G_2 := G_1(A_0, C_0)$, where G_1 and G_2 are two constants which depend on A_0 and C_0 and which can be easily computed by solving the coresponding quadratic inequalities.

This completes the proof of the Theorem.

3. Examples

Example 1. The equation

$$\binom{n}{k} - \binom{n}{k+1} - 2\binom{n}{k+2} = 0 \tag{9}$$

is a particular case of equation (3) for $A = 1$, $B = -1$ and $C = -2$. Since $B = A + C$, all solutions of equation (9) satisfy

$$(k+2) - 2(n-k) = 0,$$

which is equivalent to $2n - 3k = 2$. The integer solutions of the above equation are given by $n = 1 + 3t$ and $k = 2t$ with some integer t, and since n and k must be positive, we must have $t > 1$. Conversely, one verifies easily that

$$\binom{3t+1}{2t} - \binom{3t+1}{2t+1} - 2\binom{3t+1}{2t+2} = 0$$

holds for all positive integers t.

Example 2. The equation

$$\binom{n}{k+2} - 2\binom{n}{k+1} + \binom{n}{k} = 0 \tag{10}$$

has $A = C = 1$ and $B = 2$, therefore $D = 0$. Moreover, $A_0 = C_0 = 1$, so all solutions (n, k) of the above diophantine equation (10) have

$$k + 2 = \frac{t(t+1)}{2} \quad \text{and} \quad n - k = \frac{t(t-1)}{2},$$

which gives

$$k = \frac{t^2 + t - 4}{2} \quad \text{and} \quad n = t^2 - 2.$$

Since $n > k > 0$, it follows that either $t \geq 3$, or $t \leq -3$. Conversely, one may check that if t is any integer which is ≤ -3, or ≥ 3, then

$$\binom{t^2-2}{\frac{t^2+t-4}{2}} - 2\binom{t^2-2}{\frac{t^2+t-2}{2}} + \binom{t^2-2}{\frac{t^2+t}{2}} = 0.$$

Example 3. The equation

$$\binom{n}{k+2}=\binom{n}{k+1}+\binom{n}{k} \tag{11}$$

reduces to equation (3) for $A = 1$, $B = 1$, and $C = -1$. In this case, $D = B^2-4AC = 5$, $E = 4A^2C(A-B+C) = 4$, $X = (B^2-4AC)(n-k)-A(B-2C) = 5(n-k)-3$, and $Y = 2A(k+2)+B(n-k)-A = 2(k+2)+(n-k)-1$. Since $X^2-5Y^2 = 4$, it follows that $X = L_m$ and $Y = F_m$ hold with some even positive integer m, where $(L_\ell)_{\ell\geq 0}$ is the Lucas sequence given by $L_0 = 2$, $L_1 = 1$, and $L_{\ell+2} = L_{\ell+1}+L_\ell$ for all $\ell \geq 0$, and $(F_\ell)_{\ell\geq 0}$ is the Fibonacci sequence. We now get that $n-k = (X+3)/5 = (L_m+3)/5$, and that $k+2 = (Y-(n-k)+1)/2 = (5F_m-L_m+2)/10$. Hence, $k = (5F_m-L_m-18)/10$, and $n = (5F_m+L_m-12)/10$. Since n and k are integers, we need that $5|L_m+3$, and that $10|5F_m-L_m+2$. Thus, $5|L_m+3$ and $2|F_m+L_m$. The second relation is always fulfilled, while the first one is fulfilled precisely if $m \equiv 0 \pmod 4$. Thus, $n = (5F_{4t}+L_{4t}-12)/10$, and $k = (5F_{4t}-L_{4t}-18)/10$. Since $k > 0$, we also need that $5F_{4t} > L_{4t}+18$, which forces $t \geq 2$. One can now easily verify that

$$\binom{\frac{5F_{4t}+L_{4t}-12}{10}}{\frac{5F_{4t}-L_{4t}+2}{10}}=\binom{\frac{5F_{4t}+L_{4t}-12}{10}}{\frac{5F_{4t}-L_{4t}-8}{10}}+\binom{\frac{5F_{4t}+L_{4t}-12}{10}}{\frac{5F_{4t}-L_{4t}-18}{10}}$$

holds for all integers $t \geq 2$. Note also that since

$$\binom{n}{k+1}+\binom{n}{k}=\binom{n+1}{k+1},$$

it follows that the diophantine equation (11) reduces to the diophantine equation (11), which in turn is a consequence of our Theorem.

Remark. We remark that at instance (iii) of our Theorem, it could be possible that the Pell equation (5) has integer solutions (X, Y), and yet none such that the additional congruence $X \equiv -A(B-2C) \pmod{B^2-4AC}$ (necessary in order for $n-k$ to be an integer) is satisfied.

References

[1] Goetgheluck, P., Infinite families of solutions of the equation $\binom{n}{k} = 2\binom{a}{b}$, *Math. Comp.* **67** (1998), 1727–1733.

[2] Luca, F. Consecutive binomial coefficients in Pythagorian triples, *The Fibonacci Quart.* **40** No. 2 (2002), 76–78.

[3] Singmaster, D., Repeated binomial coefficients and Fibonacci numbers, *The Fibonaci Quart.* **13** (1975), 295–298.

[4] Stroeker, R., and de Weger, B. M. M., Elliptic binomial diophantine equations, *Math. Comp.* **68** (1999), 1257–1281.

[5] Szalay, L., A note on binomial coefficients and equations of Pythagorean type, *Acta Acad. Paed. Agriensis, Sect. Math.* **30** (2003), 173–177.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58180, Morelia, Michoacán, México
E-mail: fluca@matmor.unam.mx

László Szalay
Institute of Mathematics and Statistics
University of West Hungary
H-9400, Sopron, Bajcsy-Zs. út 4, Hungary
E-mail: laszalay@ktk.nyme.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 61–68*

SHAPE MODIFICATION OF CUBIC B-SPLINE CURVES BY MEANS OF KNOT PAIRS

Róbert Tornai (Debrecen, Hungary)

Abstract. The effect of the modification of not consecutive knot values on the shape of B-spline curves is examined in this paper. It is known that an envelope of the one-parameter family of B-spline curves of order k, obtained by the modification of a knot, is also a B-spline curve of the same control polygon and of order $k-m$, where m is the multiplicity of the modified knot. An extension of shape modification methods are provided for cubic B-spline curves, that utilize this envelope. This paper extends the possibilities for choosing the new position of a point of the curve by allowing to modify knots that are not consecutive.

AMS Classification Number: 68U05

1. Introduction

Computer aided design widely use B-spline curves and their rational generalizations (NURBS curves) that play central role today. Besides, they are used in computer graphics and animations. These curves are excellent tools in design systems to create new objects, but the modification and shape control of the existing objects are also essential.

The data structure of a B-spline curve of order k is fairly simple. It only consists of control points and knot values. Hence shape control methods can modify such curves only by altering these data. One of the most comprehensive books of this field is [9] where shape modifications, based on control point repositioning are also described. Some publications discuss shape modifications, e.g., [10] which present constraint-based curve manipulations of curves of arbitrary degree and basis functions. [11] proposes direct modification of free-form curves by displacement functions, which method comprises knot refinement and removal, control point repositioning and degree elevation.

Some aspects of knot modification is also been studied, like in [12] where the effect of knot variation is examined from numerical point of view. Several papers and articles investigate the choice of knot values in curve approximation and interpolation, cf. the recently published [13] and the references therein.

It is an obvious fact, that the modification of the knot vector affects the shape of the curve. Some results concerning the geometric aspects of knot modifications have already been presented by Juhász and Hoffmann for B-spline curves in [2],

[3] and [6], where the main result was the following: the one-parameter family of B-spline curves of order k, resulted by the modification of a knot, possesses an envelope which is also a B-spline curve of the same control polygon and of order $k - m$, where m is the multiplicity of the modified knot. This envelope can be used for geometric constraint-based shape modification of cubic B-spline curves. This property forms the basis of constrained modification of the curve which first outlined in [1] and discussed in a detailed form in [4] and [7]. Further special shape control techniques discussed in [8]. In terms of surfaces the theoretical generalization of these theorems can be found in [5].

In this paper I extend the possibilities of a shape control method described in [4] and [7] by letting not necessarily neighboring knots to change.

2. Modifying a knot

Definition 1. The curve $\mathbf{s}(u)$ defined by

$$\mathbf{s}(u) = \sum_{l=0}^{n} N_l^k(u)\,\mathbf{d}_l \,, u \in [u_{k-1}, u_{n+1}]$$

is called B-spline curve of order k (degree $k - 1$), $(1 < k \leq n + 1)$, where $N_l^k(u)$ is the lth normalized B-spline basis function of order k, for the evaluation of which the knots $u_0, u_1, \ldots, u_{n+k}$ are necessary. Points $\mathbf{d}_l$ are called control points or de Boor points, while the polygon formed by these points is called control polygon.

The jth arc of the B-spline curve of Definition 1 is of the form

$$\mathbf{s}_j(u) = \sum_{l=j-k+1}^{j} \mathbf{d}_l N_l^k(u)\,,\ u \in [u_j, u_{j+1})\,,\ (j = k-1, \ldots, n)$$

The modification of the knot value u_i alters the shape of the arcs $\mathbf{s}_\mathrm{j}(\mathbf{u})$, $j = i-k+1, i-k+2, \ldots, i+k-2$. The point of such an arc that corresponds to an arbitrarily chosen parameter value $\tilde{u} \in [u_j, u_{j+1})$ describes the curve

$$\mathbf{s}_j(\tilde{u}, u_i) = \sum_{l=j-k+1}^{j} \mathbf{d}_l N_l^k(\tilde{u}, u_i)\,,\ u_i \in [u_{i-1}, u_{i+1}]\,.$$

In [2] Juhász and Hoffmann proved the following property.

Theorem 1. *Altering a knot value $u_i \in [u_{i-1}, u_{i+1})$ of a B-spline curve $\mathbf{s}(u)$ of order k $(k > 2)$, the one-parameter family of B-spline curves*

$$\mathbf{s}(u, u_i) = \sum_{l=0}^{n} \mathbf{d}_l N_l^k(u, u_i)\,,\ u \in [u_{k-1}, u_{n+1}]$$

has an envelope which is a B-spline curve of order $(k-1)$ and can be written in the form

$$\mathbf{h}(v) = \sum_{l=i-k+1}^{i-1} \mathbf{d}_l N_l^{k-1}(v),\ v \in [v_{i-1}, v_i]$$

where the knot values

$$v_j = \begin{cases} u_j, & if\, j < i \\ u_{j+1}, & otherwise \end{cases}$$

i.e., from the knot values $\{u_j\}$ we have to leave out the ith one, where the multiplicity of u_i is one. Their points of contact are $\mathbf{h}(u_i) = \mathbf{s}(u_i, u_i)$.

For $k = 4$ by the modification of the knot value u_{i+1}, we obtain a one-parameter family of cubic B-spline curves of the form

$$\mathbf{s}(u, u_{j+1}) = \sum_{l=0}^{n} \mathbf{d}_l N_l^4(u, u_{j+1}),\ u \in [u_3, u_{n+1}],\ u_{j+1} \in [u_j, u_{j+2})$$

with knots $u_0, u_1, \ldots u_{n+4}$, and the envelope is the parabolic arc

$$\mathbf{h}_j(v) = \sum_{l=j-2}^{j} N_l^3(v)\,\mathbf{d}_l,\ v \in [v_j, v_{j+1}) \tag{1}$$

with knots $v_{j-2} = u_{j-2}, v_{j-1} = u_{j-1}, v_j = u_j, v_{j+1} = u_{j+2}, v_{j+2} = u_{j+3}, v_{j+3} = u_{j+4}$.

3. Move a point of the curve to a specified location

A generally accepted shape modification method is, when the user picks a point of the curve, then species a new location where the picked point has to be moved. Furthermore, let's assume that for the parameter of the picked point $\mathbf{s}(\tilde{u}), \tilde{u} \in [u_j, u_{j+2})$ holds. The new location will be denoted by $\mathbf{p}$, and its coordinates in the coordinate system $\{\mathbf{d}_{j-1}; \mathbf{d}_{j-2} - \mathbf{d}_{j-1}; \mathbf{d}_j - \mathbf{d}_{j-1}\}$ by x and y. It is known (c.f. [1], [4], [7]) that the $\mathbf{s}(\tilde{u}) \to \mathbf{p}$ shape modification can be performed by the alteration of three consecutive knots of the curve $\mathbf{s}(u)$.

For the determination of the permissible positions of $\mathbf{p}$ the following has to be taken into account: in the Bézier representation of the envelope the value $\tilde{t}$ which corresponds to $\tilde{v} = \tilde{u}$ varies with the variation of the knots v_j and v_{j+1}, since $\tilde{t} = (\tilde{v} - v_j)/(v_{j+1} - v_j)$. Therefore, the B-spline representation of the envelope can be used.

Utilizing that $N_{j-2}^3(v) + N_{j-1}^3(v) + N_j^3(v) = 1, \forall v \in [v_j, v_{j+1})$ Eq. (1) can be written in the form

$$\mathbf{h}_j(v) = \mathbf{d}_{j-1} + N_{j-2}^3(v)(\mathbf{d}_{j-2} - \mathbf{d}_{j-1}) + N_j^3(v)(\mathbf{d}_j - \mathbf{d}_{j-1})$$

where

$$N^3_{j-2}(v) = \frac{(v_{j+1}-v)^2}{(v_{j+1}-v_{j-1})(v_{j+1}-v_j)}$$
$$N^3_j(v) = \frac{(v-v_j)^2}{(v_{j+2}-v_j)(v_{j+1}-v_j)}.$$

3.1. Examined areas so far

In [1], [4] and [7] three pairs of knots are allowed to change. These are (v_{j-1}, v_j), (v_j, v_{j+1}) and (v_{j+1}, v_{j+2}). The corresponding permissible regions of $\mathbf{p}$ will be denoted by Ω_1, Ω_2 and Ω_3 respectively. (In this case the aim is to minimize the number of altering arcs of $\mathbf{s}(u)$, so only the change of consecutive knots are allowed.) The boundary of sub regions Ω_1, Ω_2 and Ω_3 are formed by paths that belong to different extreme positions of the point $\mathbf{h}(\tilde{v})$.

Ω_1 is bounded by three paths. The first path is determined by letting $v_{j-2} = v_{j-1}$ and varying v_j; the second by letting $v_j = \tilde{v}_j$ and varying v_{j-1} and the third path is determined by letting $v_{j-1} = v_j$ and varying them simultaneously.

Ω_2 is bounded by four paths. The first path is determined by letting $v_{j+1} = v_{j+2}$ and varying v_j; the second by letting $v_{j+1} = \tilde{v}_j$ and varying v_j the third by letting $v_j = v_{j-1}$ and varying v_{j+1} and the fourth path is determined by letting $v_j = \tilde{v}_j$ and varying v_{j+1}.

Ω_3 is bounded by three paths. The first path is determined by letting $v_{j+2} = v_{j+3}$ and varying v_{j+1}; the second by letting $v_{j+1} = \tilde{v}_j$ and varying v_{j+2} and the third path is determined by letting $v_{j+1} = v_{j+2}$ and varying them simultaneously.

These three overlapping regions are shown in Fig. 1. a), d), e).

Thus, if the point $\mathbf{p}$ is in the union of these three regions above, then the solution to the shape modification problem $\mathbf{s}(\tilde{u}) \to \mathbf{p}$ is guaranteed. In such a case, the number of solutions can be 1, 2 or 3 depending on the position of $\mathbf{p}$ with respect to the regions Ω_1, Ω_2 and Ω_3. In order to obtain the solutions, we have to solve the system of equations

$$\begin{aligned} x &= \frac{(v_{j+1}-\tilde{v})^2}{(v_{j+1}-v_{j-1})(v_{j+1}-v_j)} \\ y &= \frac{(\tilde{v}-v_j)^2}{(v_{j+2}-v_j)(v_{j+1}-v_j)} \end{aligned} \tag{2}$$

either for the pair of unknowns (v_{j-1}, v_j) or for (v_j, v_{j+1}) or for (v_{j+1}, v_{j+2}). Only those solutions of Eq. (2) provide solutions to the shape modification problem which fulfills the monotonicity condition

$$v_{j-1} \leq v_j \leq \tilde{v} \leq v_{j+1} \leq v_{j+2}$$

as well. Such a solution always exists, when $\mathbf{p}$ is in the region that corresponds to the pair of unknowns, for which the system is solved.

3.2. New areas, that extend the possibilites

What is more interesting, we can choose not consecutive knots of the curve. This way we can reach points of three other regions. In this case three pairs of knots are allowed to change also. These are (v_{j-1}, v_{j+1}), (v_{j-1}, v_{j+2}) and (v_j, v_{j+2}). The corresponding permissible regions of $\mathbf{p}$ will be denoted by Ω_4, Ω_5 and Ω_6 respectively. The boundary of sub regions are formed by paths that belong to different extreme positions of the point $\mathbf{h}(\tilde{v})$. These new three regions will overlap each other and unfortunately they mean only a little region compared to the union of Ω_1, Ω_2 and Ω_3. Another disadvantage is that the union of Ω_1, Ω_2 and Ω_3 overlaps mainly the union of Ω_4, Ω_5 and Ω_6. In spite of all of these facts, these new solutions can be useful. They let greater freedom for the designer to modify the shape of a curve. Here we shall discuss these three regions. The detailed discussion of the permissible positions of the point, the parameter values and the unknowns can be found in [7].

3.2.1. Ω_4: the unknowns are v_{j-1} and v_{j+1}

The boundaries of the permissible positions of the point $\mathbf{p}$ in this case are the paths connecting the following four extreme positions of a point of the quadratic B-spline curve arc $\mathbf{b}_j(v)$, ($v_{j-1} \in [v_{j-2}, v_j]$ and $v_{j+1} \in [\tilde{u}, v_{j+2}]$):

(1) $v_{j-2} = v_{j-1} < v_j < \tilde{u} = v_{j+1} < v_{j+2}$

(2) $v_{j-2} = v_{j-1} < v_j < \tilde{u} < v_{j+1} = v_{j+2}$

(3) $v_{j-2} < v_{j-1} = v_j < \tilde{u} = v_{j+1} < v_{j+2}$

(4) $v_{j-2} < v_{j-1} = v_j < \tilde{u} < v_{j+1} = v_{j+2}$.

The paths can be described similarly to the preceding case, but only three of them are actual boundaries, the other three paths run inside the region. The boundaries can be seen in Fig. 1. b).

3.2.2. Ω_5: the unknowns are v_{j-1} and v_{j+2}

The boundaries in this case are straight line segments. The paths connect the following extreme positions:

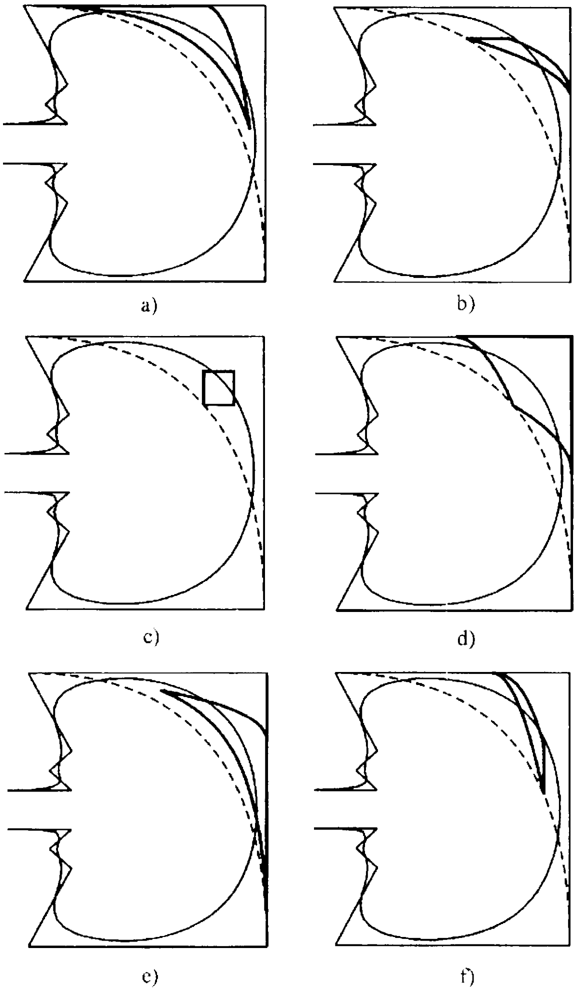
(1) $v_{j-2} = v_{j-1} < v_j < \tilde{u} < v_{j+1} = v_{j+2} < v_{j+3}$

(2) $v_{j-2} = v_{j-1} < v_j < \tilde{u} < v_{j+1} < v_{j+2} = v_{j+3}$

(3) $v_{j-2} < v_{j-1} = v_j < \tilde{u} < v_{j+1} = v_{j+2} < v_{j+3}$

(4) $v_{j-2} < v_{j-1} = v_j < \widetilde{u} < v_{j+1} < v_{j+2} = v_{j+3}$

In this case only four of the six paths form the boundary of the area that can be seen in Fig. 1. c).



a) b) c) d) e) f)

Figure 1.

3.2.3. Ω_6: the unknowns are v_j and v_{j+2}

Due to the symmetry this final case is similar to the one with the unknowns v_{j-1}, v_{j+1}. The four extreme cases can be described as follows ($v_j \in [v_{j-1}, \tilde{u}], v_{j+2} \in [v_{j+1}, v_{j+3}]$):

(1) $v_{j-1} = v_j < \tilde{u} < v_{j+1} = v_{j+2} < v_{j+3}$
(2) $v_{j-1} < v_j = \tilde{u} < v_{j+1} = v_{j+2} < v_{j+3}$
(3) $v_{j-1} = v_j < \tilde{u} < v_{j+1} < v_{j+2} = v_{j+3}$
(4) $v_{j-1} < v_j = \tilde{u} < v_{j+1} < v_{j+2} = v_{j+3}$

The resulted region can be seen in Fig. 1. f).

4. Results

By fixing one parameter and choosing two parameters for unknown, we got a system of two equations having two unknown parameters. (So it has a solution.) These three parameters shall not be necessarily neighbours. The resulted new areas will overlap partly. However points can be chosen from these areas, where from up to now could not.

References

[1] Hoffmann M., Juhász I., Shape control of cubic B-spline and NURBS curves by knot modifications, in: Banissi, E. et al (eds.): *Proc. of the 5th International Conference on Information Visualisation*, London, IEEE CS-Press, 63–68, 2001.

[2] Juhász I., Hoffmann M., The effect of knot modifications on the shape of B-spline curves, *Journal for Geometry and Graphics* **5** (2001), 111–119.

[3] Hoffmann M., On the derivatives of a special family of B-spline curves, *Acta Acad. Paed. Agriensis* **28** (2001), 61–68.

[4] Juhász I., Hoffmann M., Knot modification of B-spline curves, in: Szirmay-Kalos, L, Renner, G. (eds.): *I. Magyar Számítógépes Grafika és Geometria Konferencia*, Budapest, (2002), 38–44.

[5] Hoffmann M., Juhász I., Geometric aspects of knot modification of B-spline surfaces, *Journal for Geometry and Graphics* **6** (2002), 141–149.

[6] Juhász I., Hoffmann M., Modifying a knot of B-spline curves, *Computer Aided Geometric Design* **20** (2003), 243–245.

[7] Juhász I., Hoffmann M., Constrained shape modification of cubic B-spline curves by means of knots, *Computer-Aided Design* **36** (2004), 437–445.

[8] Juhász I., A shape modifiaction of B-spline curves by symmetric translation of two knots, *Acta Acad. Paed. Agriensis* **28** (2001), 69–77.

[9] Piegl, L., Tiller, W., *The NURBS book*, Springer-Verlag, 1995.

[10] Fowler, B., Bartels, R., Constrained-based curve manipulation, *IEEE Computer Graphics and Applications* **13** (1993), 43–49.

[11] Zheng, J.M., Chan, K. W., Gibson, I., A new approach for direct manipulation of free-form curve, *Computer Graphics Forum* **17** (1998), 327–334.

[12] Lyche, T., Morken, K., The sensitivity of a spline function to perturbations of the knots, *BIT* **39** (1999), 305–322.

[13] Piegl, L., Tiller, W., Surface approximation to scanned data, *The visual computer* **16** (2000), 386–395.

Róbert Tornai
Institute of Informatics
University of Debrecen
Egyetem tér 1.
H-4010 Debrecen, Hungary

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 69–77*

EXAMINATION OF THE MSSQL SERVER FROM THE USER'S POINT OF VIEW CONSIDERING DATA INSERTION

Tibor Radványi (Eger, Hungary)

Abstract. In this paper we summarize the experiences of the partial effectiveness examination made on the MSSQL server. We examined the effectiveness of the insert sample databases on the server. The client program was written in C++ language, in the Visual.NET system. We have done the examination of the data insert both from single--and multiclient environment. The examination contains insert options of the ADO.NET subsystem given by the .NET system - and insert options of stored procedures that were stored on the MSSQL server. These comparisons were extended with the analysis of the different network speed environments. Tests were made on high speed intranet and on Internet, ADSL (512 kbs), connection. We think that the profound and various examination of the database servers is very important. Here we relate test results that can be usable either in research in connection with database servers or in practical usage of the same systems.

AMS Classification Number: 68P30, 68P10

1. Introduction

The testing of the database systems and the measuring of their effectiveness has an important part in todays research fields [1]. When talking about systems with great data traffic, the insert of data is an especially resource-required operation. In the case of the benchmark test both the servers and the clients software options must be kept in view [2], [3]. Our test expressly closes and examines the functioning of the database from the clients side. Comparison means the collation of the different opportunities given by the programming environment during the creation of the client software. The first task is the recording of environment that influences the test results such as the size of the DataSet, the complexity of the SQL commands, hardware/software environment, the expandantion and capability of the network [1]. The goal of our test is to compare two data uploading methods given by the new .NET technology. We can only do this with an appropriately built program on the clients side and with the measuring of the results on the clients side. The client program was made in the Visual.NET system, in C++ language. To reach the database, the ADO.NET technology is a new and effective tool. In order to get best performance we used the Microsofts recommendations and research results [2], [5].

2. Hardware and software systems that were used during the test

A server computer that was indispensable for the test was installed on the Computing Department of the Károly Eszterházy College. This machine gave us the opportunity that show acceptable performance on the servers side and dont go off from the opportunities given by ensured by real user environments. As the formation of the current environment greatly influences the test results, the most important information for us are not the exact time information, but the differences shown between usage of the different programming tools, so we have to examine the proportion of the measured time values. The parameters of the server and the client machines can be found in the appendix. The program development was done on the C++ language that is part of the Microsoft Visual Studio .NET 2003. The database can be found on the Microsoft SQL Server 2000 Enterprise Edition.

3. The database

During the test the following database has been used:

Subtables: these simple tables contain basic data that are used for the random filling of the table with the subscriptors data: (sHelysegnev, sVezeteknev, sKeresztnev, sUtcanev). These have no role in the test, they help to create the appropriate environment. As this system is a simplified model of a real system, the starting data information about the subscriptors are generated by a procedure that uses the subtables as a help. These subtables do not contribute to the database on the classical way, they do not take part in the test, they have no influence on its results so their connection to the database through keys and references is superfluous and harmful. What still indicates their usage is the nearly 10 million generated record, that can be used later to test requests and to get readable results and lists that are true to life. The test is influenced by the data of the following tables, these are the ones that give results.

Elofiz: stores the data of the telephon companys subscriptors. These data will be generated by the help of the subtables.

Fields:

ID	Int (Identity)	The subscriptors unique identifier. A serial number given by the system.
Vnev	Varchar(25)	The subscribers family name (from the SVezeteknev table)
Knev	Varchar(20)	The subscribers christian name (from the Skeresztnev table)
Lakhely	Varchar(25)	The city where he lives (from the SHelysegnev table)
Utca	Varchar(25)	Street (from the SUtcanev table)
SzulDatum	Datetime	Date of birth
SzemIg	Char(8)	ID Cards number (a randonly created series of characters)

Telszam: phone numbers that belong to the costumers
Fields:

Tszam	Char(12)	Unique phone number
IDElofiz	Int	The ID of the subscriber, foreign key, have connection with the Elofiz table. The connection between the two tables is one-more, as one subscriber may have more phone numbers, but one number can only belong to 1 subscriber.

Hmod: Type of call (line, cell, inland)
Fields:

ID	Int (Identity)	Unique identifier, primary key, a serial number given by the system.
Típus	Varchar(20)	To differentiate the many district numbers in the case of cell phones and to differentiate the line phone. Hungarian specific.
Cel	Varchar(1)	The destination of the inland or foreign call.

Forg: The traffic table that serves as the base of test, storing information about the calls. Approximately 10 million items were inserted into this table during the test. ItIl will have a basic role during the experimentation of the requests.

Fields:

ID	Bigint (Identity)	Primary key, a serial number given by the system.
IDTszam	Char(12)	The costumers phone number.
IDHMod	Int	The type of the call, foreign key to the HMod table, holds the connection between the tables.
Hszam	Char(12)	The called phone number
Hkezd	Datetime	The time of the calls begining
Hbef	Datetime	The time of the calls end
Hido	Int	The time period of the call, its value is counted by a trigger.

LogTab: We store the results of the tests in this table. The system automatically generates a record for every test in this table.

Fields:

ID	int (Identity)	Primary key, a serial number given by the system.
Midopont	Datetime	The costumers phone number.
Mkezd	Datetime	The tests beginning date and time
Mbef	Datetime	End of test
Mido	Float	Time period of the test
MtipSQL	Char(10)	The type of SQL command that we test. In our case, the type is INSERT
Rekordszam	Bigint	The number of inserted records during the test.
TriggerAll	Bit	Counter to show that if every trigger was active or not. It is a factor in the systems load
Mtip	Char(10)	Type of test
Gepszam	Smallint	Number of machines in the test
Cel	Char(10)	Destination datatable, Forg in our case
Modszer	Char(10)	StoredProc/ADO comparison

Triggers: two triggers belong to the forgalom table:

`forg_hmod`: Sets the time and type of the call after the record was inserted. It worth using the automatic data-definition as it can reduce the networks data-traffic.

`forg_hbef`: Counts the calls the time period after the Hívás befejezése field was filled, than it puts it to the records appropriate column.

4. The program

The client programs technology uses the latest Microsoft development, the Visual.Net system. The software was written on C++ language, that gives a flexible tool to do the appropriate tests.

As our test included the Microsoft MSSQL servers data-insert partition, we chose the DataSet solution from the options of the DataReader on-line read-only connection and the DataSet off-line solution. The DataSet class communication with the SQL server is well represented by the picture below. The program in its current state from the tests view point uses two different datahandling method. One amplifies the Rows Collection of the SqlDataSets DataTable class given by the ADO.NET frame with new records and at the end of the amplification, it uses the SqlDataAdapter class Update method to actualise the content of the database. The other does the same by using stored procedures. Practically, holding the connection with the database lays on ADO.NET bases in both cases, but in the last case the procedures stored on the server are responsible for the uploading that we call with parameters by the SqlCommad class help. When using a stored procedure for uploading we only need the SQLCommand class with right parameters and the running of the command. So the goal of the test is to compare the two data uploading methods given by the new .NET technology. We can only do this with an appropriately built program on the clients side and with the measuring of the results on the clients side. The test includes the examination of the whole system, as itll seem from the results shown later, the results are unambiguously and consistently influenced by the speed of the network and the servers software and hardware preparation. As our goal is the test on the clients side, the results are valid to this given system. Inasmuch as we would only test the performance of the SQL server, we could only make test with programs run on the server to exclude the clients and the network. This is possible, but the goal of the article is not that. The test of the two methods was our goal, and well show the results of these now.

5. Tests and results

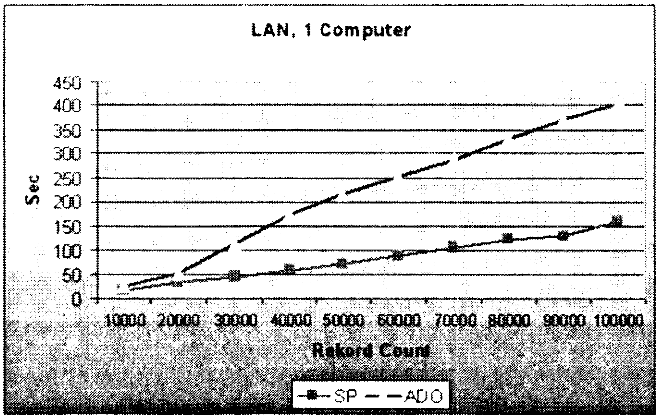
With the tests, we kept in view that many factors may influence the results due to the complexity of the system. A test result row starts with the selection of given method (Stored Procedures (SP) or DataSet (ADO)) and with the definition records number that will inserted. We repeat such a test for fifty times to exclude errors. We did approximately 800 tests with the different record numbers. The test results went through an examination before they were averaged and the once or twice occurred extreme results didnt get in to the average. These deviations always had cause that was independent from the test (hardware error, non-planned load on the server). We stopped all other resource requiring processes on the server for the tests duration. No other SQL servers (Oracle, MySQL) were running. This was the way we tried to ensure the most undisturbed conditions.

Signs, abbreviations:

Rcount:	number of inserted records;
SP:	usage of Stored Procedures;
ADO:	usage of DataNet.

(a) Local Area Network, one client machine (results in seconds)

Rcount	SP	ADO
10000	14.26565	24.2969
20000	30.9583	52.224
30000	44.401	113.5
40000	59.4896	174.3
50000	71.32825	216.016
60000	89.25	289.2373
70000	106.37	330.556914
80000	121.474	371.876529
90000	129.271	406.723
100000	159.161	289.2373



The curve that took shape can be approximated by a linear equation, where, from the

$$y = mx + b$$

equation, we examine the value of the m parameter compared to each other. We did the definition of the equation with the method of the smallest squares, thats how we fit the line on the measured value pairs. The results from this count:

$$mSP = 0.00150933 \qquad mADO = 0.00411515$$

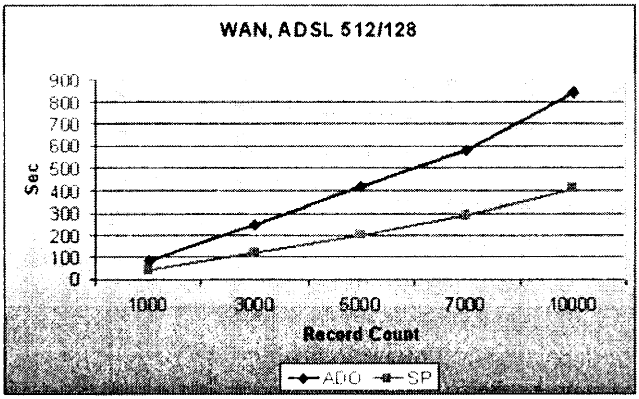
As the graph shows the usage of the stored procedure is more even amd have a better rate of effectiveness:

$$M = mADO/mSP = 2.7265$$

This shows that the usage of the stored procedure, in this case, gives a three times faster speed than the DataSet class ensured by the ADO.NET as a tool. An important note: If we would use the Update method not after the creation of the full record group in the memory, but after each and every record, this number could grow to a 100 times bigger. So if we are inserting thousands of records and the momental actualisation is not a must, than we should do it after the inserting of the records, but at least after greater groups.

(b) WAN network, through ADSL connection

Rcount	ADO	SP
1000	82.8625	39.9775
3000	248.073	120.266
5000	415.618	200.004
7000	583.255	286.318
10000	847.462	407.74



The curve that took shape can again be described with a linear equation. After the counting, the following factors remain:

$$mSP = 0.040665 \quad mADO = 0.084036$$

As the graph shows, the usage of the stored procedure is more even and have a better rate of effectiveness:

$$M = mADO/mSP = 2.06652$$

The redundancy of the rate of effectiveness can be influenced by the different speed of the network and by its stability.

6. Conclusions, further directions

The programming of databases, its access from application sofwares is a wide spread and major problem in many places that occurs in many fields of live. The first step of handling data their storage a method that occurs in every system, uses great resources from the given frame at some places. Our goal with this test was to examine the reducing possibilities in the case of a wide spread system. The test results unambiguously supports that the systems inserting effectiveness can be greatly improved if we use the options given by the SQL servers, the use of the stored procedures, even in the case of such tasks that seem to be easily solved by other methods. We will expand the examination of the insert method to the Oracle, the IBM DB2 and to the Interbase SQL servers. We will not only do this by comparing the different methods, but will also compare the test results to find the most effective data insert method on the above mentioned servers. For a more flexible and easier handling, we also need to upgrade the client program written in C++ language. Itll be a task to create different classes for the different database-handling devices, for the different methods. All classes must have the same procedures for in the main program, we only need to use an object of the appropriate class instead of the conditional, that are getting more and more complex. The timing system should be altered to a form, where the timing should not be set again and again on each and every machine, be we only need to put them into timing mode. The actual timings would appear centrally in the database, and the timed programs would continuously check if there is a task for them. This would greatly improve and mke the testing easier, even in the case of a small number of computers, and it is obligatory for a large number of clients.

Appendix

Server(dragon.ektf.hu)
Processor type: 2 db Intel Pentium III Xeon
Memory: 1024 MB
HDD: 2 db SCSI controlled, 30 Gb size, no Raidbe
Operating system: Microsoft Windows 2003 server
Database server: Microsoft SQL Server Enterprise Edition
Version Number: 8.00.760 (SP3)

Workstation
Processor: Intel Pentium 4 (1600 MHz)
Memory: 256 MB
HDD: 1 db 40 Gb size, IDE controlled 7200 turn/min
Operating system: Microsoft Windows XP professional SP1

Network
Internal network: 100 Mbps, DHCP, DNS options
External network: 512 Kbps ADSL, DHCP and DNS options

References

[1] Ailamaki, A., Shao, M., DBMbench: Microbenchmarking Database Systems in a Small, Yet Real World in Confidential, (*submitted to ICDE 2004*).

[2] Microsoft Co.: Improving .NET Application Performance and Scalability, (2004), 639-682.

[3] Ruthruff, M. (Microsoft Co.), Microsoft SQL server 2000 Index Defragmentation Best Practices, 2003.

[4] Gray, J., *The Benchmark Handbook for Database and Transaction Processing Systems*, Morgan Kaufman Publishers, Inc. 2nd edition, 1993.

[5] Gray. J., `http://research.microsoft.com/gray`.

Tibor Radványi
Department of Computing
Károly Eszterházy College
Leányka str. 6.
H-3300 Eger, Hungary
E-mail: dream@aries.ektf.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 79–95*

ANALYTIC GEOMETRY OF THE PLANE AND MATHEMATICA

Maja Bator, Zvonko Čerin, Milena Ćulav (Zagreb, Croatia)

Abstract. We describe the use of the program Mathematica in the analytic geometry of the plane in the rectangular coordinates. As an illustration of possible applications of this method we present the solutions of fifteen problems from the problem book for the first class of gymnasiums in Croatia.

AMS Classification Number: 00A35

1. Introduction

In this article we describe the computer approach to the analytic geometry of the plane. In order to do this we shall use the symbolic computation program **Mathematica.** Of course, the same could be done in the rival program **Maple V.** These are the most widely known and the most popular extensive systems or CAS that "know mathematics". Each of them has its own programming language. Our task is reduced to describing basic functions that are needed for solving geometry problems with the analytic method.

This is the translation to English of the article [2] that is in Croatian. In the references [1], [3] and [4] that are also in Croatian the same task was done in the program Maple V. The whole project is the result of the second author's course "Geometry and computers" at the Mathematics Department of the University of Zagreb (in Croatia) in which the first and the third authors (the undergraduate mathematics teachers students) have been enrolled in the academic year 2002/2003.

This elective course is offered to all fourth year mathematics major students. The number of students is growing so that for the academic year 2004/2005 there will be ten participants. The aim of the course is to teach how to use computers in mathematics working on projects under the guidance of the professor. We meet four hours each week in the computer laboratory. The first few weeks the professor is presenting the basics of text processing (LaTeX) in the program WinEdt and the commands in Mathematica and Maple. For figures in geometry we use the Geometer's Sketchpad. None of these programs is really explained in all details because we believe that they could be helpful even if we have rather limited knowledge of them just as we drive cars without being mechanics. The students pick up on their own more advanced features of these programs later on while working on the project.

What the project can be will become clear in the rest of this article because this is an example of the final outcome. In short, here the project was to program functions in Mathematica which cover analytic geometry in the plane and use them to solve with computers several problems from the secondary school level as we wanted to publish this in the Croatian mathematics and physics journal for high schools "Matematičko–fizički list". Some other projects were geometric inequalities, properties of regular polygons, and identities for Fibonacci and Lucas numbers.

All this effort is in the direction to help teachers in Croatia to accept computers as an important tool in teaching mathematics. The Croatian Mathematical Society has started an experimental program for two groups of the first and the third year pupils of gymnasiums in Zagreb that could be described as mathematics with computers. Both high school and university professors are involved in this effort but a lot of work still remains to effectively introduce computers into all levels of schools. Ours is only a small contribution on this way.

2. Basic function of analytic geometry

The key idea of the analytic geometry is to associate algebraic entities with geometric objects and then investigate them using algebraic methods.

The input of points on the plane in Maple V is quite simple because they are just ordered pairs of real numbers (their rectangular coordinates). For example, the input

```
tA:={2, 3}; tB:={5, 7}; tC:={-2, 0}; tT:={x, y};
```

defines four points on the plane $A(2,3)$, $B(5,7)$, $C(-2,0)$, $T(x,y)$.

The function `FS` is a shortcut for the simultaneous use of commands `Factor` and `FullSimplify` while `distance` measures the distance.

```
FS[m_]:=Factor[FullSimplify[m]]
distance[{a_,u_}, {b_,v_}]:=Sqrt[FS[(b-a)^2+(v-u)^2]]
```

The name of this function is *distance.* It asks for two ordered pairs of real numbers. The first pair has the components a and u while the components of the second pair are b and v. The machine first computes $(b-a)^2+(v-u)^2$ and then tries as much as possible to simplify and factor this sum of squares (the command `FS`). In the end it finds the square root of everything (the command `Sqrt`).

Many times it is important to determine the *midpoint* of the segment whose endpoints are given or the point which divides this segment either in *ratio* k (real number different from -1) or in the ratio $\frac{m}{n}$ (of real numbers whose sum is not zero).

```
midpoint[{a_,u_}, {b_,v_}] :=FS[{(a+b)/2,(u+v)/2}]
```

```
ratio[{a_,u_},{b_,v_},k_]:= FS[{(a+k*b)/(1+k),(u+k*v)/(1+k)}]
ratiomn[{a_,u_},{b_,v_},m_,n_] :=FS[{(a*n+b*m)/(m+n),(u*n+v*m)/(m+n)}]
```

The lines in the program Mathematica are represented as ordered triples $[a, b, c]$ of coefficients of their linear equations. For example, the input

```
pX:={1,0,0}; pY:={0,1,0}; pD:={1,-1,0}; pG:={-1,2,2}
```

defines four lines in the plane. They are the y-axis, the x-axis, the bisector of the first and the third quadrant and the line $-x+2y+2=0$.

The line is given either by one of its points and the tangent k of the angle which it makes with the positive direction of the x-axis (better known as its *slope*) or by two different points.

```
line1[k_, {b1_,b2_}]:=FS[{k,-1,b2-b1*k}]
line2[{x1_,y1_},{x2_,y2_}]:=FS[{y2-y1,x1-x2,x1*y2-x2*y1}]
```

Sometimes it is useful to have the following functions which test if a point lies on a line and if three points are collinear. The letter Q in their names suggests the word“question”. A point is on a line or points are collinear if and only if the function evaluates to zero.

```
onlineQ[{a_,b_},{x_,y_,z_}] :=FS[a*x+y*b+z]
collinearQ[{x1_,y1_},{x2_,y2_},{x3_,y3_}]:=
                       FS[y2*x3-y1*x3+x1*y3-x2*y3+x1*y2-x2*y1]
```

The intersection of lines or the information that they are parallel (when we get the error message of division with zero) gives our next function.

```
inter[{a_,b_,c_},{i_,j_,k_}]:=
                       FS[(-j*c+k*b)/(-i*b+a*j), (i*c-a*k)/(-i*b+a*j)]
```

Functions for the parallel and the perpendicular through a point to a line and tests if lines are parallel or perpendicular are next.

```
parallel[{a_,b_},{x_,y_,z_}] :=FS[{x,y,-x*a-b*y}]
perpen[{a_,b_},{x_,y_,z_}] :=FS[{y,-x,x*b-y*a}]
parallelQ[{a_,b_,c_},{x_,y_,z_}] :=FS[a*y-x*b]
perpenQ[{a_,b_,c_},{x_,y_,z_}] :=FS[a*x+y*b]
```

When the functions `parallelQ` or `perpenQ`, for a given pair of lines, return the value zero, then these two lines are parallel or perpendicular, respectively.

In Mathematica the test for concurrency of three lines (i.e., whether they are parallel or intersect in a point) is the following.

```
concurQ[{a_,b_,c_},{i_,j_,k_},{p_,q_,r_}]:=
                       FS[a*j*r-a*k*q-i*b*r+i*c*q+p*b*k-p*c*j]
```

Hence, three lines either intersect in a point or are parallel provided the value of the function `concurQ` in them is zero.

In solving problems using the analytic geometry it is often necessary to determine the projection of a point onto a line. Since the projection is the intersection of the line and the perpendicular to the line through the point, if we input into Mathematica

```
P:={p, q}; m:={a, b, c}; Q:=inter[m, perpen[P, m]];
```

the output will be the coordinates of the projection Q of the point P onto the line m. Hence, the corresponding function looks as follows:

```
project[{p_, q_},{a_, b_, c_}]:=
    FS[{-(c*a+b*q*a-p*b^2)/(b^2+a^2),(-b*c+q*a^2-a*p*b)/(b^2+a^2)}]
```

This concludes the listing of the most basic functions for the analytic geometry of the plane. In the rest of this paper we shall present fifteen geometry problems from the problem collection [6] and give detailed solutions of them in Mathematica. The collection is for the first year high school level (age 15–16) but some solutions require knowledge from the second and the third year.

3. Fifteen problems

Our first example is the problem 395 from the book [6] that reads as follows:

Problem 1. Prove that the area P of a triangle ABC with vertices in the points $A(x_1, y_1)$, $B(x_2, y_2)$ and $C(x_3, y_3)$ is given by the formula:

$$P = \frac{|x_1(y_2 - y_3) + x_2(y_3 - y_1) + x_3(y_1 - y_2)|}{2}$$

or

$$P = \frac{|y_1(x_2 - x_3) + y_2(x_3 - x_1) + y_3(x_1 - x_2)|}{2}.$$

Solution. Recall that the area of a triangle is a half of the product of lengths of any of its sides with the corresponding altitude. Hence, with the help of Mathematica functions introduced earlier, the area is easily computed as follows:

```
tA:={Subscript[x,1],Subscript[y,1]};
tB:={Subscript[x,2],Subscript[y,2]};
tC:={Subscript[x,3],Subscript[y,3]};
tD:=project[tC,line2[tA,tB]];
vP:=FS[distance[tA,tB]*distance[tC,tD]/2];
```

The output in Mathematica will be a rather complicated expression

$$\frac{1}{2}\sqrt{\frac{(-y_3x_1+x_3y_1+y_3x_2-x_2y_1-x_3y_2+x_1y_2)^2}{x_2{}^2-2\,x_2x_1+x_1{}^2+y_1{}^2-2\,y_1y_2+y_2{}^2}}\;\sqrt{x_2{}^2-2\,x_2x_1+x_1{}^2+y_1{}^2-2\,y_1y_2+y_2{}^2}.$$

As the computer is just a machine and we have not explained the nature of symbols representing the coordinates of the vertices, it will not cancel out the denominator in the first square root with the second square root even though they are clearly identical. It also does not notice that the square root of the square in the numerator of the first square root is equal to the absolute value

$$|-y_3x_1 + x_3y_1 + y_3x_2 - x_2y_1 - x_3y_2 + x_1y_2|.$$

When we make these simplifications we shall obviously get the required formula.

It is interesting to note that without the absolute value the above formula computes the oriented area of the triangle ABC. If this triangle is positively oriented, i.e., if the movement $ABCA$ is in the counterclockwise direction, then this real number will be positive and otherwise is negative. It will be zero if and only if the points A, B and C are collinear.

The function that gives this oriented area in Mathematica is realized in the following input:

```
area[{a_, x_},{b_, y_},{c_, z_}]:=FS[(x*c-b*x-a*z+a*y+b*z-c*y)/2]
```

The second example is the problem 425 from the same book [6].

Problem 2. Let ABC be a triangle and let U, V, W be midpoints of sides $\overline{BC}$, $\overline{CA}$ and $\overline{AB}$. The segments $\overline{AU}$, $\overline{BV}$ and $\overline{CW}$ are called the **medians** of the triangle ABC. Prove analytically that the three medians intersect in a point that we call the **centroid** of the triangle and that the centroid divides each median in the ratio $2:1$ counting from the vertex.

Solution. The proof on the computer, in Mathematica, begins by typing the following input:

```
tA := {Subscript[x,1],Subscript[y,1]};
tB := {Subscript[x,2], Subscript[y,2]};
tC := {Subscript[x,3],Subscript[y,3]};
tU:=midpoint[tB,tC]; tV:=midpoint[tC,tA];tW:=midpoint[tA,tB];
concurQ[line2[tA,tU],line2[tB,tV],line2[tC,tW]];
```

In amazingly short time the computer will output the value zero which proves that the medians intersect in a point. The coordinates of this point are revealed with the commands:

```
tG := inter[line2[tA,tU], line2[tB,tV]];
```

The point G has the coordinates $(\frac{x_1+x_2+x_3}{3}, \frac{y_1+y_2+y_3}{3})$ so that we can immediately write down the Mathematica function which associates the centroid to a triangle:

```
centroid[{a_,x_},{b_,y_},{c_,z_}]:=FS[(a+b+c)/3,(x+y+z)/3]
```

In order to prove the second claim of the problem we shall find the point that divides the median of the vertex A (i.e., the segment $\overline{AU}$) in the ratio $2:1$ counting from the vertex A and show that it coincides with the point G (the centroid of the triangle ABC). The same argument could be repeated for the medians of the vertices B and C.

```
tT:=ratiomn[tA, tU, 2, 1]; distance[tG, tT]
```

Since the returned value is zero, the points G and T coincide so that the proof of the problem is completed successfully.

The third example is the problem 989 also from the collection [6].

Problem 3. Prove that the midpoints of sides and the feet of the altitudes of a triangle lie on the same circle.

Solution. Without loss of generality we can assume that the points A, B and C are selected in the plane so that their coordinates are $(0, 0)$, $(c, 0)$ and (u, v), where c, u and v are real numbers with c and v different from zero.

```
eA:={0, 0}; eB:={c, 0}; eC:={u, v};
```

Then we get the midpoints of the sides applying the function `midpoint`:

```
eAp:=midpoint[eB,eC]; eBp:=midpoint[eC,eA]; eCp:=midpoint[eA,eB];
```

The feet of the altitudes are the projections of the vertices onto the opposite sidelines:

```
eApp:=project[eA,line2[eB,eC]]; eBpp:=project[eB,line2[eC,eA]];
eCpp:=project[eC,line2[eA,eB]];
```

The center of the circle circumscribed to a triangle is the intersection of perpendicular bisectors of its sides. Hence, in our situation, the center S of the circle circumscribed to the triangle $A'B'C'$ with vertices in the midpoints of sides is defined as follows:

```
eS:=inter[perpen[midpoint[eBp,eCp],line2[eBp,eCp]],
          perpen[midpoint[eCp,eAp],line2[eCp,eAp]]]
```

Applying the same method to the triangle $A''B''C''$ with vertices at the feet of the altitudes we can find the center T of its circumscribed circle.

```
eT:=inter[perpen[midpoint[eBpp,eCpp],line2[eBpp,eCpp]],
          perpen[midpoint[eCpp,eApp],line2[eCpp,eApp]]]
```

After we type in the above commands the computer will output the coordinates of the points S and T. We see that they are equal, so that the points S and T coincide.

In order to complete the proof it remains still to prove that the radii of the circumcircles of the triangles $A'B'C'$ and $A''B''C''$ are equal. This is checked in Mathematica with the following input:

```
FS[distance[eS,eCp]-distance[eT,eCpp]]
```

Since the returned value is zero the proof is successfully accomplished.

With almost no effort we can now prove that the radius of the above circle (also known as the nine-point circle because it also goes through the midpoints of the segments joining vertices with the orthocenter) is equal to the half of the radius of the circle circumscribed to the triangle ABC. In order to check this using the same method as above we first find the coordinates of the center O of the circumcircle of ABC

```
eO:=inter[perpen[midpoint[eB,eC],line2[eB,eC]],
            perpen[midpoint[eC,eA],line2[eC,eA]]]
```

and request from Mathematica to compute the following:

```
FS[distance[eO,eC]/distance[eS,eCp]]
```

Of course, the result is the number two.

The fourth example are the problems 719 and 720 from the book [6].

Problem 4. Prove that if a triangle has two equal altitudes or two equal medians, then it is isosceles.

Solution. With the assumptions and the notation from the proof of the Problem 3, typing in

```
FS[distance[eA,eApp]^2-distance[eB,eBpp]^2]
```

we obtain $\frac{c^3v^2(2u-c)}{(v^2+u^2-2uc+c^2)(v^2+u^2)}$. Hence, if the altitudes AA'' and BB'' have the same lengths then $u=\frac{c}{2}$ so that ABC is an isosceles triangle because the vertex C lies on the perpendicular bisector of the side AB.

Similarly we see that after typing into the program Mathematica

```
FS[distance[eA,eAp]^2-distance[eB,eBp]^2]
```

the output is $\frac{3c(2u-c)}{4}$ that leads to the same conclusion for medians.

More complicated to prove is the Problem 721 from [6]. Our method of its proof assumes the knowledge of the trigonometric functions (the cotangent in particular).

Problem 5. Prove that a triangle is isosceles if and only if it has two equal angle bisectors.

Solution. In order to have simple expressions we shall assume that the vertices A and B and the incenter I (i.e., the center I of the circle inscribed to the triangle ABC) have the coordinates $(0,\ 0)$, $(f+g,\ 0)$, and $(f,\ 1)$, where f and g are positive real numbers. In fact, these are the cotangents of the halves of the angles A and B. In addition, we assumed that the inradius is equal to 1.

```
tA:={0, 0}; tB:={f+g, 0}; tI:={f, 1}; tJc:={f, 0};
```

If the points J_a, J_b, J_c are the projections of the incenter I onto the sides of ABC, then J_c has the coordinates $(f,\ 0)$ while we get the coordinates of J_a as solutions of the following system of equations:

```
sys:=Solve[{distance[tB,{p, q}]==distance[tB,tJc],
            distance[tI,{p, q}]==1},{p, q}];
```

where p and q are the coordinates of the point J_a that we are trying to determine. This system has only two solutions. The first are the coordinates of the point J_c while the second are the required coordinates $\frac{f(g^2+1)+2g}{g^2+1}$ and $\frac{2g^2}{g^2+1}$ of the point J_a.

```
tJa:={p,q} /. Extract[sys, 2]
```

In a similar way we can find also the coordinates $\frac{f(f^2-1)}{f^2+1}$ i $\frac{2f^2}{f^2+1}$ of the point J_b.

```
tJb:={p,q} /. Extract[Solve[{distance[tA,{p, q}]==
        distance[tA,tJc], distance[tI,{p, q}]==1},{p, q}], 2]
```

Now we can find the points A_i and B_i of intersection of bisectors of angles A and B with the opposite sides as intersections $AI \cap BJ_a$ and $BI \cap AJ_b$.

```
tAi:=inter[line2[tA,tI],line2[tB,tJa]];
tBi:=inter[line2[tB,tI],line2[tA,tJb]];
```

Let us now ask the program Mathematica to calculate the difference of the squares of lengths of angle bisectors with the following input:

```
Q:=FS[distance[tA,tAi]^2-distance[tB,tBi]^2];
```

The output will be the quotient

$$\frac{4\,(f+g)^3\,(f-g)\,(f^4g^2+4\,g^3f^3-5\,f^2g^2+g^4f^2+4\,fg-1)}{(g^2+2\,fg-1)^2\,(f^2+2\,fg-1)^2}.$$

Since its numerator contains $f-g$ as a factor and $f+g$ is obviously never zero, we conclude that the proof will be completed provided we show that the long parenthesis

$$Z = f^4g^2+4\,g^3f^3-5\,f^2g^2+g^4f^2+4\,fg-1$$

in the numerator is always positive.

First note that the sum $\frac{A}{2}+\frac{B}{2}$ of halves of the angles is at most $\frac{\pi}{2}$ so that

$$\cot\left(\frac{A}{2}+\frac{B}{2}\right) = \frac{\cot(\frac{A}{2})\cot(\frac{B}{2})-1}{\cot(\frac{A}{2})+\cot(\frac{B}{2})} = \frac{f\,g-1}{f+g} > 0.$$

We conclude that $f\,g > 1$.

The first and the fourth term of Z together give

$$f^4g^2+f^2g^4 = (f^2+g^2)(f\,g)^2 \geq 2(f\,g)(f\,g)^2 = 2(f\,g)^3$$

because $f^2+g^2 \geq 2fg$. If we introduce the notation $\vartheta = fg$ then

$$Z \geq 6\vartheta^3 - 5\vartheta^2 + 4\vartheta - 1.$$

Since $\vartheta > 1$ we can replace ϑ in the above cubic polynomial with $1+\eta$ with $\eta > 0$ and get $(3\,\eta+2)\,(2\,\eta^2+3\,\eta+2)$. This expression is always positive because the new variable η is positive. This completes the proof.

Notice that the same could be obtained with the substitution $f = \frac{1+k}{g}$ for the positive real number k in the polynomial Z. Following the input

```
Collect[Extract[Q,4] /. f->(1+k)/g, g];
```

the program Mathematica outputs

$$(1+k)^2 g^2 + \frac{(1+k)^4}{g^2} + 2 + 6\,k + 7\,k^2 + 4\,k^3$$

which is obviously always positive.

We continue with the problem 833 from [6] which is in the section about similarity of triangles.

Problem 6. Let r be the radius of the circle inscribed to a triangle ABC and let R be the radius of its circumscribed circle. Prove that $R \geq 2r$.

Solution. The following proof has great similarity with the solution of the previous problem. Without loss of generality we can assume that the angles A and B of the triangle ABC are acute (i.e. less than $\frac{\pi}{2}$ radians) and that the vertices A, B and the center I of the incircle have the coordinates $(0, 0)$, $(r(f+g), 0)$ and (fr, r) for some real numbers $f > 1$, $g > 1$ and $r > 0$.

Our idea of the proof is first to determine the coordinates of the vertex C and the center O of the circumcircle. This will make it possible to compute the radius R of the circumcircle. Finally, we show that the difference $R - 2\,r$ is always positive except in the case of the equilateral triangle when it is zero.

Let J_a, J_b, J_c be projections of the center I of the incircle onto the sides of the triangle ABC. The point J_c has the coordinates $(f\,r, 0)$ while we get the coordinates of the J_a from the following system of the equations

```
sys:=Solve[{distance[tB,{p, q}]==
            distance[tB,tJc], distance[tI,{p, q}]==r},{p, q}];
```

where p and q are the wanted coordinates of the point J_a. This system has two solutions: the coordinates of the point J_c and the coordinates $\frac{(g^2 f+2\,g+f)r}{1+g^2}$ and $\frac{2rg^2}{1+g^2}$ of J_a. In a similar way we get the coordinates $\frac{f(f^2-1)r}{f^2+1}$ and $\frac{2\,f^2\,r}{f^2+1}$ of the point J_b.

```
tJa:={p,q} /. Extract[sys, 2]
tJb:={p,q} /. Extract[Solve[{distance[tA,{p, q}]==
            distance[tA,tJc], distance[tI,{p, q}]==r},{p, q}], 2]
```

The vertex C is the intersection $AJ_b \cap BJ_a$.

```
tC:=inter[line2[tA,tJb],line2[tB,tJa]];
```

The center O of the circumcircle and its radius R are given as the solutions of the following system of equations:

```
tO:={p,q}; Solve[{distance[tA,tO]==R, distance[tB,tO]==R,
            distance[tC,tO]==R},{p,q,R}];
```

From the two solutions of the system only the one where

$$R=\frac{r\,(1+g^2)\,(1+f^2)}{4(fg-1)}$$

is correct. In the second solution the radius R is negative which is not acceptable.

```
R:=r*(1+f^2)*(1+g^2)/4/(f*g-1);
M:=Collect[Extract[FS[R-2*r],2],f]; \[CapitalDelta]:=
   FS[Coefficient[M,f,1]^2- 4*Coefficient[M,f,2]*Coefficient[M,f,0]]
```

The difference $R-2\,r$ is equal to $\frac{M\,r}{4(fg-1)}$, where M is the quadratic trinomial

$$(g^2+1)f^2-8\,g\,f+g^2+9$$

in f. Its discriminant is $-4\,\left(-3+g^2\right)^2$ which is always negative (so that $M>0$ because the leading coefficient g^2+1 is positive) except when $g=\cot\frac{B}{2}=\sqrt{3}$ and $f=\sqrt{3}$ (i.e. the triangle ABC is equilateral) when $M=0$.

Next is the problem 312 from [6] which is in the second chapter on the perimeter and the area of circles.

Problem 7. Let T be a point inside the triangle ABC and let A_1, B_1, C_1 be interior points of the sides $\overline{BC}$, $\overline{CA}$, $\overline{AB}$. Let R_i for $i=1, 2, 3, 4, 5, 6$ be radii of the circumcircles of the triangles AC_1T, C_1BT, BA_1T, A_1CT, CB_1T, B_1AT. Prove that $R_1\,R_3\,R_5=R_2\,R_4\,R_6$.

Solution. Let us first define in Mathematica the function which associates to a given triple of points the radius of the circumcircle of the triangle whose vertices are these points.

```
bisector[a_, b_]:=perpen[midpoint[a,b],line2[a,b]];
CC[a_, b_, c_]:=inter[bisector[a,b],bisector[a,c]];
RC[a_, b_, c_]:=distance[a,CC[a, b, c]];
```

Let us now input the points A, B, C and T.

```
tA:={0,0}; tB:={c,0}; tC:={s,t}; tT:={p,q};
```

If $s\neq c$ then the position of a point A_1 on the line BC can be described by a real number u and the coordinates of this point are $\left(u,\,\frac{t(c-u)}{c-s}\right)$. We get this by requiring that the point with the coordinates $(u,\,z)$ lies on the line BC and then solve the condition with respect to z.

```
tA1:={u,z} /. Solve[onlineQ[{u,z}, line2[tB,tC]]==0, z];
```

Similarly, if $s\neq 0$, then any point B_1 on the line CA has the coordinates $(v,\,\frac{t\,v}{s})$ and any point C_1 on the line AB has the coordinates $(w,\,0)$ for some real numbers v and w.

```
tA1:={u,t*(c-u)/(c-s)}; tB1:={v,t*v/s}; tC1:={w,0};
```

If $s = c$ then any point A_2 on the line BC has the coordinates $(c,\ u)$ for some real number u. If $s = 0$ then any point B_2 on the line CA has the coordinates $(0,\ v)$ for some real number v.

```
tA2:={c,u}; tB2:={0, v};
```

Let us now define a function which computes the difference of the squares of the products of radii of the circumcircles for seven points in the plane.

```
FR[a_, b_, c_, d_, e_, f_,g_]:= FS[(RC[a,f,g]*RC[b,d,g]*RC[c,e,g])^2-
                (RC[f,b,g]*RC[d,c,g]*RC[e,a,g])^2];
```

It is now easy to check that the following values are zero:

```
FR[tA, tB, tC, tA1, tB1, tC1, tT]
s:=c; FR[tA, tB, tC, tA2, tB1, tC1, tT]
s:=0, FR[tA, tB, tC, tA1, tB2, tC1, tT]
```

This completes the solution of the Problem 312 from [6] in the program Mathematica.

Remark. It is clear from the above proof that we have never used the assumption that the point T is inside of the triangle ABC nor the assumption that the points A_1, B_1, C_1 are interior points of the sides $\overline{BC}$, $\overline{CA}$, $\overline{AB}$. In this way, using the computer, we succeeded to prove a more general statement.

The following example is the Problem 644 from the collection [6] which is in the section on the volume of the cylinder, cone, and ball.

Problem 8. On the bottom of the cylindrical container whose base has the diameter 15 cm there is a ball with the diameter 12 cm. The water is poured into the container up to the highest point of the ball. For how many cm will drop the level of the water when the ball is taken out?

Solution. Recall the formulas $V_B = \frac{4}{3}\left(\frac{D}{2}\right)^3 \pi$ for the volume of the ball with the diameter D and $V_C = \left(\frac{d}{2}\right)^2 h\,\pi$ for the volume of the cylinder of the height h whose base is a circle with the diameter d.

In the program Mathematica these volume functions are defined as follows:

```
VB[d_]:=d^3*Pi/6; VC[d_, h_]:=d^2*h*Pi/4;
```

The volume of the water in the container is the difference of the volume of the cylinder (with the height equal to the diameter of the ball) and the volume of the ball:

```
Vwater:=VC[15, 12]-VB[12];
```

After the removal of the ball the water will fill in the cylindrical container whose base is the circle with the diameter of 15 cm and its height will be $12-p$ cm where p is the required drop in the level of the water in the container. This drop p is found in the program Mathematica as follows:

```
Solve[Vwater==VC[15, 12-p], p]
```

The solution is $p = 5.12$ cm.

Another nice example is the Problem 963 from [6]. We assume again the knowledge of trigonometric functions.

Problem 9. A trapezium is circumscribed about the circle with the radius R. The chord that joins the touching points of the lateral sides has the length b and is parallel to the bases. Prove that the area of the trapezium is $\frac{8R^3}{b}$.

Solution. Select the rectangular coordinate system so that the circle k with the radius R inscribed to the trapezium $ACEG$ has the center in the origin and its parallel sides (bases) AC and EG touch k in the points $B(0,\,-R)$ and $F(0,\,R)$. Let the lateral sides CE and AG touch k in the points $D(R\cos\theta,\,R\sin\theta)$ and $H(R\cos\sigma,\,R\sin\sigma)$ for some angles θ and σ.

Let us first input into the program Mathematica the points O, B, F, D, H and the lines AC, EG.

```
tO:={0, 0}; tB:={0, -R}; tF:={0, R};
tD:={R Cos[\[Theta]], R Sin[\[Theta]]};
tH:={R Cos[\[Sigma]], R Sin[\[Sigma]]};
pAC:={0, 1, R}; pEG:={0, 1, -R};
```

Then we ask when will the chord DH joining the touching points D and H of the lateral sides be parallel with the bases.

```
parallelQ[line2[tD, tH], pAC]
```

The condition is $R(\sin\theta - \sin\sigma) = 0$ so that we must have $\sigma = \pi - \theta$. Hence, the trapezium $ACEG$ is equilateral and symmetrical with respect to the line BF. It suffices therefore to find the area only of the right half $BCEF$.

The line CE is the perpendicular in the point D to the line OD (the property of the tangent to the circle) and the points C and E are the intersections of the line CE with the lines AC and EG.

```
pCE:=perpen[tD, line2[tO, tD]];
tC:=inter[pAC, pCE]; tE:=inter[pEG, pCE];
```

The area of the right half $BCEF$ is the sum of the areas of the triangles BCE and BEF.

```
FS[area[tB, tC, tE]+area[tB, tE, tF]]
```

The program Mathematica will compute that this sum has the value $\frac{2R^2}{\cos\theta}$. Since $b = 2\,R\cos\theta$, we conclude that the wanted area of the trapezium $ACEG$ is indeed $\frac{8\,R^3}{b}$.

Remark. In the book [6] there is the incorrect claim that the area of the trapezium is $\frac{4R^3}{b}$. Using the approach from the solution of the Problem 13 (i.e., the Problem 1112 from [6]) it is possible to completely avoid the trigonometric functions. This solution we leave to the readers as an exercise.

We continue with the solution of the Problem 1026 from [6].

Problem 10. Prove that in every regular heptagon $A_1A_2A_3A_4A_5A_6A_7$ the following equality holds:

$$\frac{1}{|A_1A_2|}=\frac{1}{|A_1A_3|}+\frac{1}{|A_1A_4|}.$$

Solution. Choose the coordinate system so that the circle k with the center at the origin and with the radius R is circumscribed to the heptagon $A_1A_2A_3A_4A_5A_6A_7$. We can assume that the vertex A_1 has the coordinates $(R,\,0)$. The other relevant vertices have the coordinates $A_2\left(R\cos\frac{2\pi}{7},\,R\sin\frac{2\pi}{7}\right)$, $A_3\left(R\cos\frac{4\pi}{7},\,R\sin\frac{4\pi}{7}\right)$, $A_4\left(R\cos\frac{6\pi}{7},\,R\sin\frac{6\pi}{7}\right)$.

Let us input these points into the program Mathematica:

```
tA1:={R, 0}; tA2:={RCos[2 Pi/7], RSin[2 Pi/7]};
tA3:={RCos[4 Pi/7], RSin[4 Pi/7]};
tA4:={RCos[6 Pi/7], RSin[6 Pi/7]};
```

In order to check the above relation among the reciprocal values we must type into the program Mathematica the following:

```
FullSimplify[Numerator[Together[1/distance[tA1,tA2]-
    1/distance[tA1,tA3]-1/distance[tA1,tA4]]],R>0]
```

For few seconds the computer will output the value zero which proves that the statement in the problem holds.

Remark. Several other interesting properties of the regular heptagon proved in the program Maple V are described in the article [5].

Next is the Problem 1084 from the section eight of the collection [6].

Problem 11. The projections of the legs of the right triangle onto the hypothenuse have lengths $\frac{18}{5}$, $\frac{32}{5}$. Find the radius of the circle inscribed into this triangle?

Solution. Select the rectangular coordinate system so that its origin is the vertex C of the right triangle and its legs are on the coordinate axes. We can assume that the remaining vertices A and B have the coordinates $(0,\,b)$ and $(a,\,0)$, for some positive real numbers a and b.

In the program Mathematica these points are input as follows:

```
tC:={0, 0}; tA:={0, b}; tB:={a, 0};
```

Then we find the projection D of the vertex C onto the hypotenuse AB.

```
tD:=project[tC, line2[tA, tB]];
```

The values for the variables a and b can be determined from the information that $|AD|=\frac{18}{5}$ and $|BD|=\frac{32}{5}$.

```
Solve[{distance[tA,tD]==18/5, distance[tB,tD]==32/5},{a, b}];
```

There are eight solutions (four real and four complex) but only one when $a=8$ and $b=6$ is acceptable. Hence, this right triangle has sides 8, 6, 10 (that are twice as long as the sides of the standard (Egyptian) right triangle with sided 4, 3, 5) so that its inscribed circle has the radius $r = 2$.

This could also be seen by asking that the center I of the inscribed circle with the coordinates (r, r) is at the distance r from the line AB.

```
a:=8; b:=6; tI:={r, r};
Solve[distance[tI, project[tI, line2[tA,tB]]==r, r];
```

¿From the two solutions $r = 2$ and $r = 12$ only the first satisfies the conditions of the problem. The second solution gives the radius of the corresponding excircle.

Now we consider the Problem 1103 again from the collection [6].

Problem 12. Two sides of the triangle have the length 6 cm and 8 cm. The medians of these sides are perpendicular. Find the third side of this triangle.

Solution. Let the triangle ABC be embedded into the rectangular coordinate system so that $A(0, 0)$, $B(c, 0)$, and $C(u, v)$ for positive real numbers c and v and for a real number u.

In the program Mathematica these points and the centroid T are input as follows:

```
tA:={0,0}; tB:={c,0}; tC:={u,v}; tT:=centroid[tA,tB,tC];
```

Since the medians of the vertices A and B are perpendicular, ABT is the right triangle and $c^2 = |AB|^2 = |AT|^2 + |BT|^2$ by the Pythagorean theorem. On the other hand $|BC| = 6$ and $|AC| = 8$. If we ask the program Mathematica to solve this system of three equations in the variables c, u, and v with the input

```
Solve[{distance[tB,tC]==6, distance[tA,tC]==8,
             c^2==distance[tA,tT]^2+distance[tB,tT]^2},{c,u,v}]
```

it will respond with two solutions. Only the one where $c = 2\sqrt{5}$ cm is correct.

Our next example is the Problem 1112 from [6].

Problem 13. A circle is inscribed into a trapezium. Prove that the ratio of the areas of the circle and the trapezium is equal to the ratio of their perimeters.

Solution. Choose the rectangular coordinate system so that the circle k with the radius R which is inscribed to the trapezium $ACEG$ has the center in the origin while its parallel sides (bases) AC and EG touch k in the points $B(0, -R)$ and $F(0, R)$. Let the vertices A and C have the coordinates $(-u, -R)$ and $(v, -R)$ for positive real numbers u and v. Let the lateral sides CE and AG touch k in the points D and H. Our first goal is to find the coordinates of these points and then the coordinates of the vertices E and G.

Let us first input into the program Mathematica the points O, B, F, A, C and the lines AC, EG.

```
tO:={0, 0}; tB:={0, -R}; tF:={0, R}; tA:={-u, -R};
tC:={v, -R}; pAC:={0, 1, R}; pEG:={0, 1, -R};
```

Assume that the point H has the coordinates (p, q). They must satisfy two conditions. The first is $p^2 + q^2 = R^2$ i.e. that the point H lies on the circle k. The second condition is that the distance from A to H is equal to u because the lines AB and AH are tangents through the point A onto the circle k.

```
H:=Solve[{p^2+q^2==R^2, distance[{p,q},tA]==u}, {p,q}]
tH:={p,q} /.H
```

In a similar way we can determine the coordinates of the point D.

```
K:=Solve[{p^2+q^2==R^2, distance[{p,q},tC]==v}, {p,q}]
tD:={p,q} /.K
```

The vertices E and G are the intersections of the line EG with the lines CD and AH, respectively.

```
pAH:=line2[tA,tH]; pCD:=line2[tC,tD];
tE:=inter[pEG,pCD]; tG:=inter[pEG,pAH];
```

The first coordinates of the points E and G are $\frac{R^2}{v}$ and $-\frac{R^2}{u}$. Hence, the perimeter O_{ACEG} of the trapezium $ACEG$ is $2(u+v+\frac{R^2}{u}+\frac{R^2}{v})$. Its area P_{ACEG} is

```
FS[area[tA, tC, tE]+area[tA, tE, tG]]
```

equal to $\frac{R(u+v)(u\,v+R^2)}{u\,v}$. Now it is easy to check that

$$\frac{2\,R\,\pi}{O_{ACEG}} = \frac{R^2\,\pi}{P_{ACEG}}.$$

Remark. In [6] there are no solutions for the Problem 1112.

The next example is the Problem 1139 from [6].

Problem 14. Prove that if the angle bisector of a triangle is also the bisector of the angle determined by the altitude and the median, then this triangle is right.

Solution. Let us choose the rectangular coordinate system so that the points $A(0, 0)$, $B((f+g)r, 0)$, $C\left(\frac{rg(f^2-1)}{fg-1}, \frac{2fgr}{fg-1}\right)$ are the vertices of the triangle and the center of its inscribed circle is the point $I(fr, r)$, where f and g are cotangents of $\frac{A}{2}$ and $\frac{B}{2}$ and r is the radius of the incircle.

We shall first input into the program Mathematica the points A, B, the midpoint C_g of the segment AB, the points C, I and the feet C_h of the altitude of the vertex C on the line AB.

```
tA:={0, 0}; tB:={r*(f+g), 0}; tCg:=midpoint[tA,tB];
tC:={r*g*(f^2-1)/(f*g-1), 2*f*g*r/(f*g-1)}; tI:={f*r,r};
tCh:=project[tC,line2[tA,tB]];
```

In order that the bisector of the angle C (i.e. the line CI) is the bisector of the angle between the altitude (i.e. the line CC_h) and the median (i.e. the line CC_g)

it is necessary and sufficient that the segments II_h and II_g have the same length, where I_h and I_g are the projections of the point I onto the lines CC_h and CC_g.

```
tIh:=project[tI,line2[tC,tCh]]; tIg:=project[tI,line2[tC,tCg]];
IZ:=FS[distance[tI,tIg]^2-distance[tI,tIh]^2]
```

The program Mathematica reports that the expression IZ is equal

$$\frac{r^2\,(f-g)^2\,(fg+g+f-1)\,(fg-g-f-1)\,(fg+1)^2}{(12\,f^2g^2+g^2f^4-2\,f^3g^3+g^4f^2+2\,f^3g+2\,fg^3+f^2-2\,fg+g^2)\,(fg-1)^2}.$$

Hence, it will be zero if and only if $f = g$ (i.e. $|BC| = |CA|$ so that the triangle ABC is isosceles) or

$$(fg+g+f-1)(fg-g-f-1)=0$$

which is the condition for the lines BC and CA to be perpendicular (i.e. that the angle C has 90 degrees and the triangle ABC is right).

```
perpenQ[line2[tB, tC], line2[tC, tA]]
```

Remark. In the collection [6] the possibility that the triangle ABC is isosceles is absent.

Our final example is the Problem 1152 from [6].

Problem 15. Let different points A and B be given and let the point T be outside the line AB. Through the point T construct the line m so that the ratio of the distances of the points A and B to the line m is $2:3$.

Solution. Choose the rectangular coordinate system so that the given points are $A(0,\,0)$, $B(c,\,0)$, and $T(p,\,q)$ for real numbers c, p, q. Let the line m has the equation $u\,x+v\,y+w=0$ for some real numbers u, v, w. In order that it goes through the point T the free term w must be equal to $-u\,p-v\,q$.

Let us input into the program Mathematica the points A, B, T and the line m.

```
tA:={0, 0}; tB:={c, 0}; tT:={p, q}; pm:={u, v, -u*p-v*q};
```

Let A_m and B_m be the projections of the points A and B onto the line m.

```
tAm:=project[tA, pm]; tBm:=project[tB, pm];
```

By the requirement of the problem the quotient $\frac{|AA_m|}{|BB_m|}$ is equal to $\frac{2}{3}$. Notice that the expression

```
IZ:=FS[distance[tA,tAm]^2/distance[tB,tBm]^2-4/9]
```

has as the numerator the product $(5\,up+5\,vq-2\,uc)\,(up+vq+2\,uc)$. Hence, there are two possibilities $q=\frac{-u(2c+p)}{q}$ and $q=\frac{u(2c-5p)}{q}$. They give lines $q\,x-(2c+p)y+2qc=0$ and $5q\,x+(2c-5p)y-2qc=0$ as solutions of the problem. Even though we know the solutions the question remains how to construct them. But, it is simple to see that they intersect the line AB in the points $C(-2c, 0)$ and $D(\frac{2}{5}c, 0)$ and these are easily constructed.

Remark. In the collection [6] there are no solutions for the problem 1152.

Remark. A longer version of this paper with figures is available on the Internet at the home page of the second author: `http://www.math.hr/~cerin`

References

[1] Bator, M., Čerin, Z., Ćulav, M., Analitička geometrija ravnine računalom, *Matematičko-fizički list* 54 (2003/2004), 26–36.

[2] Bator, M., Čerin, Z., Ćulav, M., Analitička geometrija ravnine i Mathematica, *Prim. Math.* (to appear).

[3] Čerin, Z., Šest zadataka riješenih programom Maple V, *Matematičko-fizički list* 54 (2003/2004), 105–112.

[4] Čerin, Z., Još šest zadataka riješenih programom Maple V, *Matematičko-fizički list* 54 (2003/2004), 194–200.

[5] Čerin, Z., Geometrija pravilnog sedmerokuta, *Poučak* 14 (2003), 5–14.

[6] Pavković, B., Veljan, D., *Matematika 1*, Školska knjiga, Zagreb, 1999.

Maja Bator
Odranska 8
10000 Zagreb
Croatia
E-mail: batormaja@yahoo.com

Zvonko Čerin
Kopernikova 7
10000 Zagreb
Croatia
E-mail: cerin@math.hr

Milena Ćulav
Lhotkina 3
10000 Zagreb
Croatia
E-mail: mickey@student.math.hr

METHODOLOGICAL PAPERS

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 99–105*

COMMON TERMS IN CERTAIN BINARY RECURRENCES

Erzsébet Orosz (Eger, Hungary)

Abstract. The purpose of this paper is to prove that the common terms of linear recurrences $M(2a,-1,0,b)$ and $N(2c,-1,0,d)$ have at most 2 common terms if $p{=}2$, and have at most three common terms if $p{>}2$ where D and p are fixed positive integers and p is a prime, such that neither D nor $D{+}p$ is perfect square, further a,b,c,d are nonzero integers satisfying the equations $a^2-Db^2{=}1$ and $c^2-(D{+}p)d^2{=}1$.

AMS Classification Number: 95U50

1. Introduction

Let $G = G(A, B, G_0, G_1) = \{G_n\}_{n=0}^{\infty}$ be a second order linear recursive sequence of rational integers defined by the recursion

$$G_n = AG_{n-1} + BG_{n-2} \quad (n > 1),$$

where A, B and the initial terms G_0, G_1 are fixed integers, $AB \neq 0$ and $G_0^2{+}G_1^2 \neq 0$.

Let α and β be the roots of the characteristic polynomial $x^2 - Ax - B$ of the sequence G. Throughout this paper we assume that $|\alpha| \geq |\beta|$ and the sequence G is nondegenerate, that is, $\frac{\alpha}{\beta}$ is not a root of unity.

It is well-known that the terms of G can be written in the form

$$G_n = \frac{q\alpha^n - \epsilon\beta^n}{\alpha - \beta}, \tag{1}$$

where $q = G_1 - G_0\beta$ and $\epsilon = G_1 - G_0\alpha$.

It can be proved that in the case $A^2 + 4B > 0$

$$|G_n| > c|\alpha|^n,$$

while in the case $A^2 + 4B < 0$

$$(2) \qquad |G_n| > \frac{c_1|\alpha|^n}{n^{-c_0}}$$

holds by the results of C. L. Stewart [13], where c, c_1, c_0, n_0 are positive real constants depending on the parameters of G and $n > n_0$.

Thus $|G_n| > x$ for all fixed real x, if n is large enough, that is all elements can be equal to finitely many other elements of the sequence G.

A similar problem is to determine the common terms of distinct sequences.

G. Revuz [11] proved a general theorem for the common terms of different second order linear recurrences G and H defined by the same A, B constants: The equation $G_x = H_y$ has finitely many solutions (x, y); if $x > n_0$ then $G_x \neq H_y$.

A variety of classical algebraic and elementary estimations to the common terms of recursive sequences and similar problems can be found in the papers of M. D. Hirsch [3], P. Kiss [4], [5], M. Mignotte [9], F. Mátyás [8], H. P. Schlickewei, W. M. Schmidt [12] and others.

Using Shure's theorem K. Liptai [7] proved that certain recursive sequences have finitely many common elements.

J. Binz [2] proved that the sequences $G\,(6, -1, 0, 6)$ and $H\,(10, -1, 0, 10)$ have only one common term.

There is a connection between the number of solutions of a special type of Pell's equations and the number of common terms in certain recurrences, that is why we use the following result:

Michael A. Bennett [1] proved that if a and b are distinct nonzero integers then the simultaneous Pell's equations

$$x^2 - az^2 = 1, y^2 - bz^2 = 1$$

possess at most three solutions in positive integers (x, y, z).

1. Results and proofs

Some special cases are the most interesting because the number of the common terms can be determined.

The aim of the next part is to give the common terms in certain binary recurrences and generalize the result of J. Binz. Our main result is the following.

Theorem 1. *Let D and p be fixed positive integers, where p is a prime, such that neither D nor $D + p$ is perfect square. Further let a, b, c, d be non-zero integers satisfying the equations $a^2 - Db^2 = 1$ and $c^2 - (D + p)\,d^2 = 1$. Then the sequences $M\,(2a, -1, 0, b)$ and $N\,(2c, -1, 0, d)$, apart from the zero initial terms, have at most two common terms if $p = 2$.*

Proof. First we prove that $(x, y) = (x, M_n)$ is a solution of the equation

$$x^2 - Dy^2 = 1 \tag{3}$$

for all M_n. The number pairs (x_n, y_n) are also solutions, where

$$x_n + y_n\sqrt{D} = \left(a + b\sqrt{D}\right)^n \ (n = 0, 1, 2, ...). \tag{4}$$

This follows from the condition $(x, y) = (a, b)$ and

$$\begin{aligned} x_n^2 - Dy_n^2 &= \left(x_n + y_n\sqrt{D}\right)\left(x_n - y_n\sqrt{D}\right) \\ &= \left(a + b\sqrt{D}\right)^n \left(a - b\sqrt{D}\right)^n = \left(a^2 - Db^2\right)^n = 1. \end{aligned}$$

From (4) we have

$$y_n = \frac{1}{2\sqrt{D}}\left[\left(a + b\sqrt{D}\right)^n - \left(a - b\sqrt{D}\right)^n\right].$$

The roots of the characteristic polynomial $x^2 - 2ax + 1$ of the sequence M are:

$$\alpha = a + \sqrt{a^2 - 1} = a + b\sqrt{D},$$

$$\beta = a - b\sqrt{D},$$

so with $M_0 = 0, M_1 = b$, $\alpha - \beta = 2b\sqrt{D}$ and by (1) the equality $y_n = M_n$ holds. It is similarly true for all terms N_k that $(z, y) = (z, N_k)$ is a solution of the equation

$$z^2 - (D + p)\, y^2 = 1.$$

If the sequences M and N have some common terms, then the number of integer solutions (x, y, z) of the equation system

$$\begin{aligned} x^2 - Dy^2 &= 1, \\ z^2 - (D + p)\, y^2 &= 1 \end{aligned} \tag{5}$$

is the number of the different common terms. It is enough to prove that the equation system has at most two solutions if $y \neq 0$. Assume that (x, y, z) is the solution of (5). In this case

$$x^2 - Dy^2 = z^2 - (D + p)\, y^2$$

so

$$x^2 + py^2 = z^2 \tag{6}$$

and $\gcd(x,y) = 1$, $\gcd(z,y) = 1$. The solution (x,y,z) is a positive solution of equation (6). If $\gcd(x,z) > 1$ then $p \mid x^2 + y^2$ and $p \mid y$ contradict to what is mentioned before. Now $p = 2$. Then (6) can be written in form

$$x^2 + 2y^2 = z^2. \tag{7}$$

The primitive solutions of (7) are: $x = |u^2 - 2v^2|, y = 2uv, z = u^2 + v^2$,$\gcd(u,v) = 1$, where u is an odd integer. Substitute these into the first part of (5)

$$\left(u^2 - 2v^2\right)^2 - 4Du^2v^2 = 1.$$

It can be written in the form

$$[u^2 - (2 + 2D)\,v^2]^2 - \left(8D + 4D^2\right) v^4 = 1. \tag{8}$$

The diophantine equation $x^2 - Dy^4 = 1$ has at most two solutions (Mordell [11]), $8D + 4D^2 = (2D+2)^2 - 4$ is not perfect square. Thus (8) holds for at most two pairs (u,v). If $p = 2$ than the equation system (5) has at most two solutions.

Theorem 2. *Let D and p be a fixed positive integer and a prime, respectively, such that neither D nor $D+p$ is perfect square. Further let a,b,c,d be non-zero integers satisfying the equations $a^2 - Db^2 = 1$ and $c^2 - (D+p)\,d^2 = 1$. Then the sequences $M\,(2a,-1,0,b)$ and $N\,(2c,-1,0,d)$, apart from the zero initial terms have at most three common terms if $p > 2$.*

Proof. If the sequences M and N have some common terms then the equation system

$$x^2 - Dy^2 = 1,$$
$$z^2 - (D+p)\,y^2 = 1$$

has at most three solutions. It follows from the first Proof. It is enough to prove that this equation system have at most three solutions if $y \neq 0$. It follows from the result of M. A. Bennett which was published in [1]. Our simultaneous Pell' s equation system has at most three solutions in positive integers (x,y,z). If $p > 2$ then the sequences $M(2a,-1,0,b)$ and $N(2c,-1,0,d)$ apart from the zero initial terms have at most three common terms.

Remark: If we use the result of Mordell [10] then it can be proved that the number of common terms at most four.

If $p > 2$ then the primitive solutions of (6)

$$x = |pm^2 - n^2|, y = 2mn, z = pm^2 + n^2 \tag{9}$$

or

$$x = \left|\frac{pu^2 - v^2}{2}\right|, y = uv, z = \frac{pu^2 + v^2}{2} \tag{10}$$

where m and n are different and $\gcd(m,n) = 1$, $\gcd(u,v) = 1$. Substitute these into the first equation of (5) and we get from (9)

$$\left(pm^2 - n^2\right)^2 - 4Dm^2n^2 = 1,$$

whereas from (10)

$$\left(\frac{pu^2 - v^2}{2}\right)^2 - Du^2v^2 = 1.$$

These can be formed as

$$(11) \qquad \left(n^2 - (p+2D)m^2\right)^2 - (4D^2 + 4pD)m^4 = 1,$$

$$(12) \qquad \left(\frac{v^2 - (p+2D)u^2}{2}\right)^2 - (D^2 + pD)u^4 = 1.$$

It can be shown that neither $4D^2 + 4pD$ nor $D^2 + pD$ are perfect squares. Equations (11) and (12) have at most 2 solutions. So the equation system of (5) has at most 4 integer solutions.

Theorem 3. *Let L be a fixed positive integer such that neither L nor $L + 8$ is perfect square and $8 \mid L$. Further let r, s, k, t be non-zero integers satisfying the equations*

$$r^2 - Ls^2 = 1$$

and

$$k^2 - (L + 16)t^2 = 1.$$

Then the sequences $H = H(2r, -1, 0, s)$ and $K = K(2k, -1, 0, t)$ apart from the zero initial terms, have at most 2 common terms.

Proof. The proof is based on the proof of the Theorem 1.

Remarks

1. Let D be a positive integer which is not a perfect square. Pell's equation

$$x^2 - Dy^2 = 1$$

has infinitely many integer solutions pairs of (x, y). It can be seen that there are infinitely many a, b, c, d or r, s, k, t integers for which our conditions hold.

2. If $L = 8$, then J. Binz's theorem follows from the Theorem 3. In this case we can determine the common terms of the sequences $G(6, -1, 0, 6)$ and $H(10, -1, 0, 10)$.
3. In particular, it would be interesting to prove a similar result for any sequence of $G(A, B, G_0, G_1)$ and $H(C, D, H_0, H_1)$ for which there are finitely many common terms. But the upper bound of the common terms would be too large.

References

[1] Bennett, M. A., On the number of solutions of simultaneous Pell equations, *J. Reine Angew. Math.* **498** (1998), 173–199.

[2] Binz, J., *Elemente der Math.* **35** (1980), 155.

[3] Hirch, M. D., Additive sequences, *Math. Mag.* **50** (1977), 262.

[4] Kiss, P., On Common terms of linear recurrences, *Acta Math. Acad. Sci. Hungar.* **40** (1–2), (1982), 119–123.

[5] Kiss, P., Közös elemek másodrendű rekurzív sorozatokban. *Az egri Ho Si Minh Tanárképző Főiskola füzetei* XVI. (1982), 539–546.

[6] Kiss, P., Differences of the terms of linear recurrences, *Studia Scientiarum Mathematicarum Hungarica* **20** (1985), 285–293.

[7] Liptai, K., Közös elemek másodrendű rekurzív sorozatokban, *Acta. Acad. Pead. Agriensis, Sect. Math.* **21** (1994), 47–54.

[8] Mátyás, F., On common terms of second order linear recurrences, *Mat. Sem. Not. (Kobe Univ. Japan)* **9** (1981), 89–97.

[9] Mignotte, M., Intersection des images de certains suites recurrentes lineaires, *Theoretical Comput. Sci.* **7** (1978), 117–122.

[10] Mordell, L. J., *Diophantine equations*, Acad. Press, London, (1969), 270.

[11] Revuz, G., Equations deiphanties exponentielles, *Bull. Soc. Math. France, Mém.* **37** (1974), 139–156.

[12] Schlickewei, H. P., Schmidt, W. M., Linear equations in members of recurrence sequences, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **20** (1993), 219–246.

[13] STEWART, C. L., On divisors of terms of linear recurrence sequences, *J. Reine Angew, Math.* **333** (1982), 12–31.

Erzsébet Orosz
Department of Mathematics
Károly Eszterházy College
Leányka str. 4.
H-3300 Eger, Hungary
E-mail: ogyne@ektf.hu

REMARKS ON THE CONCEPT OF SIMILARITY IN TEACHING GEOMETRY IN TEACHERS' TRAINING COLLEGE

István Krisztin Német (Szeged, Hungary)

Abstract. In [12] and [13] (textbooks for teachers' training colleges written by B. Pelle) isometry and similarity are defined not in the classical way, but as a product of reflections, and as a product of central dilatation and isometry. We make some remarks on this way of definition, and we study some important theorems on similarity (e.g. fixed point, classification) by using this way of definition.

AMS Classification Number: 00A35 (ZDM: G55, G59)

1. Introduction

In the classical treatment of geometrical transformations isometry is defined as a transformation which preserves distance, and by similarity one means a transformation in which the ratio of each corresponding line segments is constant (e.g. [5], [17], [18]). In [12] and [13] (textbooks for teachers' training colleges) these concepts are defined in a different way. The basis of the structure is the group of the axioms of Reflection refering to the primitive concept of "reflection in plane"; then follows the concept of reflection in line. Space (plane) isometry is defined as a product of reflections in plane (in line). After the axioms of Metric and Parallelism, the theorems of parallel secants and the concept and properties of central dilatation, similarity is defined as a product of central dilatation and isometry. If we want to describe the difference between the two ways of definition, we can say that the classical one is based on a property, and the other one is a "constructive" way; it provides technique to give the transformation.

In this paper we examine the connection between the classical and "constructive" ways. We shall apply the latter way consistently throughout the study of similarity; we aspire to the complete analogy with the concepts and theorems involved in studying of isometry. Related to these purposes we suggest some complements, changes to the structure involved in [12] and [13]. There are some topics which are not detailed in [12] and [13], namely the theorems on the fixpoint and the classification of similarities, the concept of dilatation; we shall examine these topics also in the "constructive" way. We make these suggestions with the aim of forming a unified system of concepts and theorems for the students in this very important domain of geometry.

We note here that the axioms of Reflection involved in [12] and [13] are used instead of the classical axioms of Congruence only. So the concept of reflection has not such a central role as in [1] or in [14] (chapters 5., 6.).

2. Isometry

The axioms of Reflection which we use are a little bit different from the axioms involved in [12] and [13] ([12] pp. 21–22; [13] pp. 17–18), therefore we list them (R1–R5). In [8] we wrote some remarks on these axioms and the concept of orthogonality and reflection in line. We note that in this paper by space (plane) transformation we mean a bijective mapping from the space (plane) onto itself; two transformations are said to be equal, if they transform any point into the same point; by line-preserving mapping we mean a mapping, which transforms collinear points into collinear points; by fixed point of a mapping we mean a point which coincides with its image under the mapping; by fixed plane (line) of a mapping we mean a plane (line) whose points are fixed by the mapping; by plane-flag we mean the union of a halfplane and a ray on its boundary, and by space-flag we mean the union of a halfspace and a plane flag on its boundary.

R1: Any reflection in plane is a line-preserving involutory space-transformation, which has a fixed plane; and this plane separates every P–P' pair, if P is not on it.

R2: For any plane there is a unique reflection in plane, whose fixed plane is the given one.

R3: For any two points there is a unique reflection in plane, in which they are corresponding points.

R4: For any two rays, starting from the same point, there is a unique reflection in plane, which transforms the given rays into each other.

R5: If two products of reflections in plane transform a space-flag into the same one, then the products are equal.

Definition 2.1. By space (plane) isometry we mean a product of reflections in plane (in line). ([12] pp. 58, 198; [13] pp. 57, 190)

We make some remarks on this definition. Students in secondary school learn the classical definition (e.g. [4]), so the different definitons may cause confusion. To avoid this, we think that it is important to show them the equivalence of the definitions. It is easy to see that isometry, defined in 2.1, preserves distance; since we defined the distance of two points as the length of their line segment ([12] p. 41; [13] p. 34) and in the axiom of Metric we postulate that the lengths of congruent segments are equal ([12] p. 40; [13] p. 34). For the equivalence we need the following theorem.

Theorem 2.2. *If a space (plane) transformation preserves distance, then it can be got as an isometry.*

Proof of Theorem 2.2. First we shall prove the case on the plane. Since the given transformation preserves distance, then due to the triangle-inequality the images of three points are collinear iff the points are collinear. So it is a line-preserving transformation. Let us consider three noncollinear points and their images. The corresponding sides of the triangles are equal due to the distance-preserving property, so due to the "three sides" congruency theorem of triangles ([12] p. 55; [13] p. 54) there is an isometry, under which the images of the three points are the same as under the given transformation. Finally it is easy to see, that due to the line- and distance-preserving properties our previous statement is true for every point, so the isometry and the given transformation are equal. In the proof of the case on the space the only difference is that we have to take four noncoplanar points instead of three noncollinear points, and we have to refer to the congruence of tetrahedra instead of that of triangles.

Classically the previous proof is related to the theorem, which states that on the plane any two triangles whose corresponding sides are equal, are related by a unique isometry (e.g. [3], [15]). In the structure based on axioms of Reflection the analogue of this "fundamental" theorem is the following one ([13] p. 43, only the case on the plane).

Theorem 2.3. *Any two space (plane) flags are related by a unique isometry.*

This theorem can be proved easily by axioms of Reflection and their equivalents refering to the case on the plane. At the same time we also proved the following Theorem 2.4. We use axiom R5 instead of axiom XII. of [12] and [13] because of its great importance in these fundamental theorems. (In [8] we examined the connection between the two axioms.)

Theorem 2.4. *Any space (plane) isometry can be obtained as the product of at most four reflections in plane (at most three reflections in line).*

([12] p. 58, [13] p. 43., only the case on the plane.)

We start the classification of isometries with this theorem. Naturaly, we finish it only after the axiom of Parallelism. After the classification it is worth remarking that any isometry can be obtained as the product of at most two of the following transformations: reflection in plane, reflection in line, reflection in point. (This statement is a simple corollary of classification.)

3. Central dilatation

In [12] and [13] the concept of central dilatation is defined after the Euclidean axiom of Parallelism and the theorems of parallel secants ([12] p. 110, [13] p. 105). Our definition is a little bit different from that, because we use negative ratio, too (as e.g. in [3], [4], [15]). We make this change for the sake of unity and brevity in

Paragraphs 5. and 6. Due to this change, there is a difference between the properties of central dilatation on the plane and on the space: it preserves orientation on space iff its ratio is positive, while it preserves orientation on plane with any ratio. For the sake of brevity in the definition we use oriented segments; we defined the operations related to them in the usual way.

Definition 3.1. By central dilatation we mean the following mapping. Suppose that there is a point O and a $\lambda(\neq 0)$ constant. The image of the point P is those P', for which $OP' = \lambda OP$.

We shall use the notation $\mathrm{N}_{O,\lambda}$ for this mapping. We make some other definitions. By invariant plane (line) of a mapping we mean a plane (straight line) which coincides with its image under the mapping. By the center of a mapping we mean a point, through which every straight line passing is invariant. To emphasize the analogies with the axioms of Reflection we list some properties of central dilatation.

I. Any central dilatation is a line-preserving space (plane) transformation, which has a center; this point separates every other P-P' pair, iff $\lambda < 0$.

II. For any point O and any constant $\lambda(\neq 0)$, there is a unique $\mathrm{N}_{O,\lambda}$.

III. For any three collinear points O, P and P', so that P and P' differ from O, there is a unique central dilatation with center O, under which the image of P is P'.

IV. For any point O and any two parallel lines a, a' which are off O, but coplanar with it, there is a unique central dilatation with center O, under which the image of a is a'. (Two coplanar lines are called parallel, if they coincide or do not meet.)

(We need the Euclidean axiom of Parallelism only for the proof of line-preserving property and statement IV.)

These properties are just the analogues of the first four axioms of Reflection. The analogue of the fifth one will occur at the concept of similarity, in Theorem 4.2. As in the case of axioms of Reflection, statements II., III. and IV. provide techniques to give a central dilatation; and the first one contains the most important (non metric) properties of central dilatation. We declare these the most important ones because of the following theorem.

Theorem 3.2. *If a mapping on the Euclidean space (plane) is a line-preserving transformation with a center, then it can be got as a central dilatation.*

Proof of Theorem 3.2. Since mapping is a line-preserving transformation, any line is coplanar with its image, and the images of parallel lines are also parallel. Planes passing through the center are invariant, and the images of parallel planes are also parallel. Let O denote the center. O is fixed, since it is the point of intersection of invariant lines. Let us first assume that there is another fixed point, say C. Let α be a plane that contains C, and let β be the plane that contains O, which is parallel to α. Since β is invariant and the mapping preserves parallelism,

α is also invariant. If every plane passing through C is invariant, then C is a center. Since there are two centers, we can fit two invariant lines on every point, so every point is fixed. In this case the mapping is the identity, which is a central dilatation. Let us now assume that O is the only fixed point. First we shall show that any line, which is off O, is not invariant, but it is parallel to its image. If it were invariant, its points would be fixed. If it intersected its image, their point of intersection would be fixed. Finally, the theorem of the parallel secants concludes that $\frac{OP'}{OP}$ is constant for any $P(\neq O)$. So the mapping is $\mathrm{N}_{O,\lambda}$, the proof is completed.

We think that it is also very important to emphasize the connection between the line-preserving property of the central dilatation and the Euclidean axiom of Parallelism in the lectures. In general, after the axiom of Parallelism, textbooks list some statements equivalent to the axiom, but generally the line-preserving property of the central dilatation is missing. In this treatment which is based on the axioms of Reflection and products, it would be important to mention this, too. The first reason for that is that the concept of similarity is (partially) based on the central dilatation. The other reason is, that the concept of isometry is based on the primitive concept of reflection in plane, whose line-preserving property is declared in an axiom (R1). We can prove easily the line-preserving property of the central dilatation by axiom of Parallelism ([12] p. 110, [13] p. 106). For the equivalence we need the following theorem.

Theorem 3.3. *If the statement of Euclidean axiom of Parallelism is false, then central dilatation is not line-preserving mapping.*

The proof of this theorem can be found e.g. in [7], where the basis of proof is a modell, while the following one does not use modell.

Proof of Theorem 3.3. Let P be a point, e a line, and $P \notin e$. We shall work on the plane of P and e. Let m be the line, for which $P \in m$, and $m \perp e$, let $C = m \cap e$, and f the line, for which $P \in f$, and $m \perp f$ (Fig. 1).

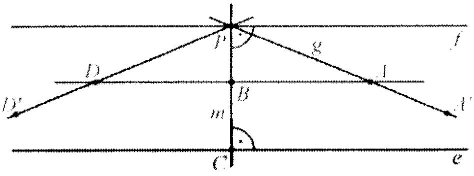


Figure 1.

It is known that f does not meet e. Let g be another line through P, which does not meet e. It is obvious that the reflected image of g under the reflection in line m, does not meet e either. Let A be a point on g between e and f, let D denote the image of A under the reflection in line m, and let $B = m \cap (AD)$, which is obviously an inner point of the segment PC. Let us consider the central dilatation with center P, which transforms B to C. The images of A and D under this central dilatation remain between e and f, and they are separated by m. So, according to axioms of Order, they are not collinear with C.

In [12] and [13] the product of central dilatations is worked out immediatelly after the investigation of the properties of central dilatation, before the definition of similarity ([12] p. 113, [13] p. 109). For the sake of unity, we choose the way which was used in [12], [13] and by us to observe isometries. Namely, we first deal with the general concept of similarity and the fundamental theorems related to it, and we shall observe special products only after these theorems.

4. Similarity

In [12] and [13] plane similarity is defined as a product of a central dilatation and an isometry ([12] p. 114, [13] p. 111). The definition for the case on the space is a little bit different: the factors of the product are in plural ([12] p. 200, [13] p. 192). We choose the latter way for both cases.

Definition 4.1. By space (plane) similarity we mean a product of central dilatations and space (plane) isometries.

We choose this way for two reasons. The first is that the analogy with the definition of isometry in 2.1 comes with the use of plural. The second is that this form gives immedatelly the closure of the set of similarities for composition. In [12] and [13] this statement ([12] p. 115, [13] p. 111) is derived from the following facts: a product of isometries is also an isometry ([12] p. 58, [13] p. 57), a product of central dilatations is either a central dilatation or a translation ([12] p. 113, [13] p. 110). In [12] and [13] the concept of the ratio of similarity is defined in the classical way, namely, it is the constant ratio of corresponding segments. In our opinion, another way of definition fits better the Definiton 4.1. Namely, the modulus of the product of the ratios of the central dilatations involved in the product in Definition 4.1 is taken as the ratio of similarity.

The equivalence of Definition 4.1 and the classical one comes from the following facts. From the properties of isometry and central dilatation we get the statement: for the similarity defined by 4.1 the ratio of each corresponding segments is constant. On the other hand, the following theorem is valid.

Theorem 4.2. *If the ratio of each corresponding segments related by a transformation is constant, then it can be got as a similarity.*

It is true, because it is easy to show that the given transformation is a product of an isometry and a central dilatation (e.g. [4], [10], [17]).

We note that in secondary school similarity is defined as in [12] and [13] for the case on the plane, namely, as a product of a central dilatation and an isometry (e.g. [4]). So this transformation is a similarity in the sense of Definition 4.1, too. On the other hand, from Theorem 4.2 we get that every similarity in the sense of Definition 4.1 is a product of a central dilatation and an isometry. This means that the two definitions are equivalent. The second statement which gives the equivalence will occur later in Theorem 4.4, which will be important for this treatment from another point of wiew, too.

After the examination of the different ways of definition, there follow the fundamental theorems on similarity. The simple properties of similarity (e.g. line-, ratio- and angle-preserving property) come directly from Definition 4.1, as the common properties of the factors of the product. The further observations are based on the following theorem, which is the analogue of Theorem 2.3 and axiom R5.

Theorem 4.3. *Suppose that Z and V are space (plane) flags, P and Q are points on their ray. Then there exists a unique similarity, which transforms Z to V and P to Q.*

In [12] and [13] there is not a theorem like this. In the classical treatment the equivalent statement of Theorem 4.3 is the one which says that any two triangles (tetrahedra) whose corresponding sides (edges) have a constant ratio, are related by a unique similarity (e.g. [3], [15]); or this one: on the plane any two segments are related by just two similarities, a direct one and an opposite one (e.g. [3], [9]). We use the above Theorem 4.3 instead of these theorems, because it fits better this structure than the classical theorems mentioned.

Proof of Theorem 4.3. First let us consider the isometry, **M**, which transforms Z to V (Theorem 2.3). Then we consider the central dilatation, whose center is the starting point of the ray of V, and which transforms $\mathbf{M}(P)$ to Q. The product of these transformations has the desired properties. If there is another similarity, then it is equal to the first product, due to the ratio- and angle-preserving properties.So for the sake of unity and consistency, in the sequel we shall use Theorem 4.3 for the investigation of similarities.

From the construction involved in the previous proof, we get the following two important consequences. The first is the analogue of Theorem 2.4.

Theorem 4.4. *Any similarity can be obtained as a product of an isometry and a central dilatation, whose ratio is the ratio of the given similarity (so it is positive).*

Theorem 4.5. *A similarity can be got as an isometry iff its ratio is 1.*

These theorems have already been mentioned above when we discussed equivalence, but if we observe this structure on its own this is the right place for them.

5. Classification of similarities

We start with the classification theorem for plane similarities.

Theorem 5.1. *Any plane similarity, which is not isometry, can be got either as a dilative rotation or as a dilative reflection.*

(We regard the central dilatation as a dilative rotation with rotation angle 0°.)

This theorem is not in [12] and [13], but the two special transformations are mentioned in [13] ([13] p. 111). This theorem is usually proved after the theorem on the fixed point of similarity. We observe these two questions together.

There are many ways to prove the existence of the fixed point. The classical one—using parallelograms—is e.g. in [3], [6], [10], [15], [17]. There is another way to construct the fixed point—using circles—e.g. in [2], [9], [11], [16]. A proof based on continuity can be found e.g. in [2]. Also in [2] there is special construction for the case on the plane.

Here we give a proof of Theorem 5.1, which is in close connection with the structure that has been built above. It is based on the product-definition of similarity and isometry, and on Theorems 4.3 and 4.4. Some details in case II. are similar to the constuction in [2]. Our proof is more lengthy than the previously mentioned ones, but our aim is to make a consistent structure. We note that in the proof we use orientated segments and angles, we defined the operations related to them in the usual way; we denote the reflection in line a by $\mathbf{T}_a$; we use the term "axis" for the fixed line of reflection in line; we make the products of transformations from right to left.

Proof of Theorem 5.1. Let $\mathbf{H}$ be a similarity which is not isometry. From Theorem 4.4 we get that $\mathbf{H} = \mathbf{N}_{O,\lambda}\mathbf{M}$, where $\mathbf{M}$ is an isometry, $\lambda > 0$, $\lambda \neq 1$. We shall consider six cases depending on the type of $\mathbf{M}$.

I. If $\mathbf{M}$ is either the identity, a rotation about O, or a reflection in line passing through O, then proof is complete.

II. If $\mathbf{M}$ is a reflection in line, $\mathbf{M} = \mathbf{T}_b$, $O \notin b$, then let m be the line, for which $O \in m$, $m \perp b$, and $B = b \cap m$ (Fig. 2.). Let C be the point, for which $BC = \dfrac{\lambda - 1}{\lambda + 1}OB$. C is fixed point of $\mathbf{H}$. Let a be the line, for which $C \in a$, $a \parallel b$. It is obvious that a is invariant line of $\mathbf{H}$, and $\mathbf{H}$ interchanges the halfplanes bounded by a. Let P be a point on a ($P \neq C$), and $P' = \mathbf{H}(P)$. Since C is fixed, $CP' = \lambda CP$. The similarity $\mathbf{N}_{C,\lambda}\mathbf{T}_a$ also has these properties. Then let us consider the plane flag which contains the ray $[CP)$ and one of the halfplanes bounded by a. From the results above we get that the images of this flag and P under $\mathbf{H}$ and $\mathbf{N}_{C,\lambda}\mathbf{T}_a$ are the same. So according to Theorem 4.3 $\mathbf{H} = \mathbf{N}_{C,\lambda}\mathbf{T}_a$.

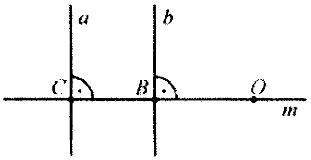


Figure 2.

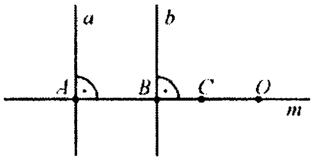


Figure 3.

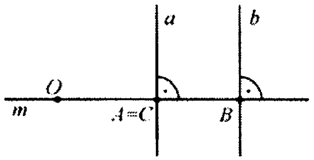


Figure 4.

We reduce the further cases to case II. in the following way. Translation—and rotation, too—is the product of two reflections in line, where one of the axes is partially arbitrary. We observe how to take it, so that the fixed point of the product of the reflection in this line and $\mathbf{N}_{O,\lambda}$ should be incident to the other axis. If it is satisfied, then $\mathbf{H}$ also fixes this point. In the case of glide reflection, we shall base our proof on the fact that it is the product of a translation and a reflection in line.

III. If $\mathbf{M}$ is a translation, $\mathbf{M} = \mathbf{T}_b\mathbf{T}_a$, $a \parallel b$, then let m and B be as in II., $A = m \cap a$, and let C be the fixed point of $\mathbf{N}_{O,\lambda}\mathbf{T}_b$ (Fig. 3.). C is on a iff $BC = BA$ (Fig. 4.), so iff $OB = \frac{1+\lambda}{1-\lambda}AB$. (Because, according to II., $BC = \frac{\lambda-1}{\lambda+1}OB$ and $\lambda \neq 1$.) Instead of the original axes we take new ones for which the previous equation stands for OB. (We can construct the new B, b by using O, λ and the original AB segment.) So by the new axes we get that $\mathbf{H}$ fixes the new C. According to II. $\mathbf{N}_{O,\lambda}\mathbf{T}_b$=$\mathbf{N}_{C,\lambda}\mathbf{T}_a$, so it also comes that $\mathbf{H} = \mathbf{N}_{C,\lambda}$.

Among rotations first we examine the half-turn, and then the other ones.

IV. If $\mathbf{M}$ is a half-turn, $\mathbf{M} = \mathbf{T}_b\mathbf{T}_a$, $a \perp b$, $a \cap b = K$, $K \neq O$, then let the new axes be (OK) and the line perpendicular to it through K (Fig. 5.) According to II., the fixed point of $\mathbf{N}_{O,\lambda}\mathbf{T}_b$, C, lies on a, so $\mathbf{H}$ also fixes it. Moreover $\mathbf{N}_{O,\lambda}\mathbf{T}_b = \mathbf{N}_{C,\lambda}\mathbf{T}_e$, where e is the line for which $C \in e$ and $e \parallel b$, so $\mathbf{H} = \mathbf{N}_{C,-\lambda}$.

V. If $\mathbf{M}$ is a rotation, $\mathbf{M} = \mathbf{T}_b\mathbf{T}_a$, $(a,b)\angle = \phi$, $\phi \neq 90°$, $a \cap b = K$, $K \neq O$, then let m, B and C be as in III., and let $\omega = ((KO),b)\angle$ (Fig. 6.).

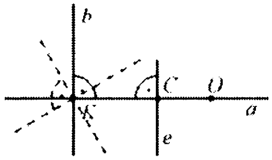


Figure 5.

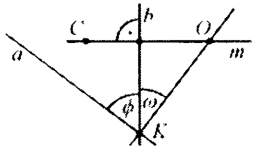


Figure 6.

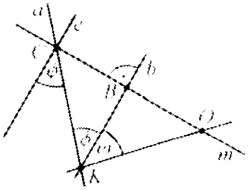


Figure 7.

C is on a iff $\frac{\tan\omega}{\tan\phi} = \frac{OB}{CB}$ (Fig. 7.), so iff $\tan\omega = \frac{1+\lambda}{1-\lambda}\tan\phi$. (Because, according to II., $BC = \frac{\lambda-1}{\lambda+1}OB$.) Instead of the original axes we take new ones for which the previous equation holds for $\tan\omega$. (We can construct the new ω, b by using O, λ and the original ϕ angle.) So by the new axes we get that $\mathbf{H}$ fixes the new C. According to II. $\mathbf{N}_{O,\lambda}\mathbf{T}_b = \mathbf{N}_{C,\lambda}\mathbf{T}_e$, where e is the same as in IV. (Fig. 7.), so $\mathbf{H} = \mathbf{N}_{C,\lambda}\mathbf{T}_e\mathbf{T}_a$, $C = e \cap a$ and the angle of rotation is 2ϕ.

VI. If $\mathbf{M}$ is a glide reflection, $\mathbf{M} = \mathbf{T}_b\mathbf{T}_a\mathbf{T}_c$, $a \perp c \perp b$, then according to III. there exists a point K for which $\mathbf{N}_{O,\lambda}\mathbf{T}_b\mathbf{T}_a = \mathbf{N}_{K,\lambda}$ (Fig. 8.). ($(OK) \parallel c$). According to II. there exists a point C and a line e for which $\mathbf{N}_{K,\lambda}\mathbf{T}_c = \mathbf{N}_{C,\lambda}\mathbf{T}_e$ and $C \in e$. So $\mathbf{H} = \mathbf{N}_{C,\lambda}\mathbf{T}_e$. (According to IV. $C \in (OB)$.)

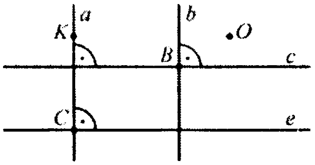


Figure 8.

Since there is not a further case for **M**, the proof is complete. It is obvious that the center of the central dilatation is the only fixed point of the product. In each case the proof also provides a way to construct this point.

There follows the classification theorem for space similarities. In [13] this theorem is included, but its proof is missing ([13] p. 192). Recall that dilative rotation on the space is the product of a rotation about a line and a central dilatation whose center lies on the axis of the rotation.

Theorem 5.2. *Any space similarity, which is not isometry, can be got as a dilative rotation.*

(We regard the central dilatation as a dilative rotation with rotation angle 0°.)

Proof of Theorem 5.2. The principle of the proof is the same as in the previous one so we do it breefly. First we put the given similarity into the form of $\mathbf{N}_{O,\lambda}\mathbf{M}$, and make classification according to the type of the **M** isometry. If **M** is either the identity, a reflection in plane, a translation, a rotation about a line, or a glide reflection, then we get—in the same way as in the corresponding case of the proof of Theorem 5.1—that the given similarity is a dilative rotation. (For reflection in plane and glide reflection the axis is the line passing through the fixed point and perpendicular to the fixed plane of the original reflection, the angle is 180°, and the ratio is $-\lambda$. For rotation about line the new axis is the line passing through the fixed point and parallel to the original one, the angle and the ratio do not change. For translation and identity we get central dilatation also with the original ratio.) For those isometries which do not have corresponding case in the proof of Theorem 5.1—namely, if **M** is either a rotatory reflection or a screw displacement—we get the desired result by using completed cases: either rotation about line and reflection in plane, or translation and rotation about line. We use the method which we used in case VI. in the proof of Theorem 5.1, where the question were reduced to cases II. and III. (For both cases the new axis is the line passing through the fixed point and parallel to the original one. For screw displacement the angle and the ratio do not change, for rotatory reflection the angle increases by 180° and the ratio is $-\lambda$.)

6. Dilatation

Finally, we deal with the concept of dilatation. We examine here the question mentioned at the end of Paragraph 3.: product of central dilatations.

In the classical treatment dilatation (or parallel similarity) is defined as a transformation, which transforms each line into a parallel line (e.g. [3], [5], [10], [18]). Here we give another definition which fits the structure using products (see Definitions 2.1 and 4.1).

Definition 6.1. By dilatation we mean a product of central dilatations and translations.

This definition is equivalent to the classical one, naturally. It is obvious that the dilatation 6.1 is a transformation and it transforms each line into a parallel line. On the other hand, it is involved e.g. in [3], [10], that if a transformation transforms each line into a parallel line, then it is either a central dilatation or a translation. (Those proofs refer to the case on the plane, but it is easy to extend them to the space.) Besides the equivalence of the definitions these facts proove the following theorem, too:

Theorem 6.2. *Any dilatation can be got either as a central dilatation or as a translation.*

It is worth emphasizing this theorem for another reason, too. This is the analogue of Theorems 2.4 and 4.4. We can get this theorem in our structure in a different way, too:

Proof of Theorem 6.2. According to Definition 4.1 the dilatations defined in 6.1 are similarities, so we can apply our results on classification of isometries and similarities. Since the product transforms each line into a parallel line, if it is an isometry, then it is either the identity, a translation or a reflection in point, and if it is not an isometry, then according to Theorems 5.1 and 5.2 it is a dilative rotation with rotation angle 0°. Thus the theorem is proved, because every transformation mentioned except the translation is a central dilatation.If we examine the question in details, first we find that it is enough to examine products with two factors. If we observe the products of isometries, we find that the set containing the identity, translations and reflections in point, contains the product of any two. So we have to examine only products with central dilatation whose ratio is not 1 or -1. The product of such central dilatation and translation is not isometry, so according to the previous proof it is a central dilatation. We get the center as the point of intersection of two lines passing through corresponding points. The other case, in which the product is not isometry, is the product of two central dilatations with product of ratios neither 1 nor -1. We get the center similarly to the previous case. If the product of ratios is 1, then the line passing through the centers and the halfplanes bounded by that line are invariant. So the product is either the identity or a translation depending on the centers whether they coincide or not. If the product of the ratios is -1, then the mentioned halfpanes interchange with their coplanar pair, so the product is a reflection in point. We get the center also in the way described above.

References

[1] BACHMANN, F., *Aufbau der Geometrie aus dem Spiegelungsbegrieff* (zweite Auflage) Springer-Verlag, Berlin–Heidelberg–New York, 1973.

[2] COXETER, H. S. M., *Introduction to geometry*, J. Wiley & Sons Inc., New York London, 1961.

[3] COXETER, H. S. M., *A geometriák alapjai*, Műszaki Kiadó, Budapest, 1973.

[4] HAJNAL, I., NÉMETHY, K., *Matematika II.* (gimn.) (2. kiadás), Tankönyvkiadó, Budapest, 1990.

[5] HAJÓS, GY., *Bevezetés a geometriába* (8. kiadás), Tankönyvkiadó, Budapest, 1987.

[6] HOLLAI, M., HORVÁTH, J., TEMESVÁRI, Á., A sík és a tér egybevágósági és hasonlósági transzformációi, *ELTE Szakmódszertani közleményei*, ELTE, Budapest, 1978.

[7] HORVÁTH, J., *Sztereografikus projekció és alkalmazásai* (Elemi geometria a Poincaré-féle félgömbmodellen), ELTE, Budapest, 1980.

[8] KRISZTIN NÉMET, I., Megjegyzések az egybevágóság és a merőlegesség fogalmának megalapozásához a főiskolai geometriaoktatásban, *Berzsenyi Dániel Főiskola Tudományos Közleményei XIII. Természettudományok 8.*, Szombathely, 2002. 17–37.

[9] KUTUZOV, B. V., *Geometria*, Tankönyvkiadó, Budapest, 1954.

[10] MARTIN, G.E., *Transformation Geometry* (An Introduction to Symmetry), Springer-Verlag, New York, 1982.

[11] MOLNÁR, E. (SZERK.), *Elemi matematika II. (Geometriai transzformációk)*, ELTE jegyzet (14. kiadás), Tankönyvkiadó, Budapest, 1989.

[12] PELLE, B., *Geometria*, Tankönyvkiadó, Budapest, 1979.

[13] PELLE, B., *Geometria* (átdolgozott kiadás), EKTF Líceum Kiadó, Eger, 1997.

[14] RADÓ, F., ORBÁN, B., *A geometria mai szemmel*, Dacia Kiadó, Kolozsvár (Cluj Napoca), 1981.

[15] REIMAN, I., *A geometria és határterületei*, Gondolat, Budapest, 1986.

[16] RÉDLING, E., *Hasonlósági transzformációk*, Tankönyvkiadó, Budapest, 1982.

[17] SZABÓ, Z., *Bevezető fejezetek a geometriába* 1. kötet, JATE Bolyai Intézet, Szeged, 1982.

[18] SZÁSZ, G., *Geometria*, Tankönyvkiadó, Budapest, 1964.

István Krisztin Német
Mathematical Department
University of Szeged, Juhász Gyula Teachers' Training College
Boldogasszony sgt. 6.
H-6725 Szeged, Hungary
E-mail: krisztin@jgytf.u-szeged.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **31** *(2004) 121–123*

A COMMENT ON THE DARBOUX TRANSFORMATION

J. H. Caltenco, J. López Bonilla, M. A. Acevedo (Mexico)

Abstract. It is known that the Darboux transformation (DT) allows us to construct isospectral potentials in the frame of the Schrödinger equation. Here we give a simple mathematical deduction for the DT.

Introduction

In the one-dimensional stationary case the Schrödinger equation is given by [1, 2]

$$-\frac{d^2}{dx^2}\psi + u(x)\psi = \lambda\psi \tag{1}$$

which is written in natural units taking $\frac{\hbar}{2m} = 1$. The values of λ represent the energy spectrum allowed for determinated boundary conditions and corresponding to the standard potential $u(x)$. With the very useful Darboux transformation (DT) [3–6] we can generalize any specific standard potential and thus generate new interaction models with the same energy levels. The DT is related to the Sturm–Liouville theory [7–10], and it is easy to see the implicit presence of DT in supersymmetric quantum mechanics [1, 2, 5, 11–15]. We suppose that (1) accepts the particular solution ψ_1 for the eigenvalue λ_1

$$-\psi_1{}'' + u(x)\psi_1 = \lambda_1\psi_1 \tag{2}$$

then we employ ψ_1 as a"seed function" to construct the DT [3–5, 16]:

$$\phi(x) = \psi' - \sigma_1(x)\psi \qquad \sigma_1 = \frac{d}{dx}ln\psi_1 \tag{3}$$

therefore (1) adopts the structure:

$$-\frac{d^2}{dx^2}\phi + U(x)\phi = \lambda\phi \tag{4}$$

with the generalized isospectral potential:

$$U(x) = u(x) - 2\frac{d}{dx}\sigma_1 \tag{5}$$

That is, the Schrödinger equation is covariant with respect to DT. Selecting other"seed functions" we can generate many DT-s and thus a great family of generalized potentials with the same energy spectrum.

In the next section we show a simple procedure to motivate (3), (4) and (5), that is, we exhibit how the basic expressions of the DT are born.

Darboux transformation

If in (1) we introduce the new dependent variable $y(x) = \psi/\theta(x)$, where θ is an arbitrary function for the time being, then this equation takes the form:

$$y'' + 2\frac{\theta'}{\theta}y' + \left(\lambda - \lambda_1 + \frac{\theta''}{\theta} - \frac{\psi''}{\psi_1}\right) y = 0 \tag{6}$$

because from (2) we have that $u = \lambda_1 + \psi_1{}''/\psi_1$. Therefore it is natural the election $\theta = \psi_1$, that yields:

$$y = \frac{\psi}{\psi_1} \tag{7}$$

and reduces this equation to the form:

$$y'' + 2\frac{\psi_1{}'}{\psi_1}y' + (\lambda - \lambda_1)y = 0 \tag{8}$$

if the definition of y written above is applied in deducing each of the equations of (7) and (8). Now we apply $\frac{d}{dx}$ to (8) and introduce the notation:

$$\eta(x) = \frac{d}{dx}y(x), \qquad \sigma_1 = \frac{\psi_1{}'}{\psi_1} \tag{9}$$

for thus to obtain the equation:

$$\eta'' + 2\sigma_1\eta' + (\lambda - \lambda_1 + 2\sigma_1{}')\eta = 0 \tag{10}$$

Finally, in (10) we make a transformation similar to (7):

$$\eta = \frac{\phi}{\psi_1} \tag{11}$$

Then this equation adopts the structure of (4) with the generalized isospectral potential $U(x) = \sigma_1^2 - \sigma_1{}' + \lambda_1 = u - 2\sigma_1{}'$, in according with (5). Besides, from (7), (9) and (11) we have that $\phi = \psi_1\eta = \psi_1 y' = \psi_1\frac{d}{dx}(\psi/\psi_1)$, which reproduces (3) q.e.d.

In the literature on DT there is not an explicit motivation for these important transformations of mathematical physics. Thus, the present Note was dedicated to a simple demonstration of the basic expressions of DT.

References

[1] de Lange O. L., Raab, R. E., *Operators methods in quantum mechanics*, Clarendon Press, Oxford (1991)

[2] Schwabl, F., *Quantum mechanics*, Springer-Verlag, Berlin (1992)

[3] Darboux, G., Compt. Rend. Acad. Sc. (Paris) 94 (1882) 1456.

[4] Khare, A., Sukhatme, U. J. Phys. A: Math. Gen 22 (1989) 2847.

[5] V. B. Matveev and M-A. Salle, *Darboux transformations and solitons*, Springer-Verlag, Berlin (1991)

[6] J. Morales, J. J. Peña and J. López Bonilla J. Math. Phys. 42 (2001) 966.

[7] C. Lanczos, *Linear differential operators*, D. van Nostrand, London (1961)

[8] H. Hochstadt, *The functions of mathematical physics*, Dover NY (1986)

[9] J. B. Seaborn, *Hypergeometric functions and their applications*, Springer-Verlag, Berlin (1991)

[10] Z. Ahsan, *Differential equations and their applications*, Prentice Hall, India (2000)

[11] A. A. Andrianov, N. V. Borisov and M. J. Ioffe, Theor. Math. Fiz. 61 (1) (1984) 17 and 61 (2) (1984) 183.

[12] A. A. Andrianov, N. V. Borisov and M. J. Ioffe, Phys. Lett. B181 (1986) 141.

[13] R. W. Haymaker and A. R. P. Rau Am. J. Phys. 54 (1986) 928.

[14] F. Cooper, A. Khare and U. Sukhatme Phys. Rep. 251 (1995) 267.

[15] H. R. Hauslin Helv. Phys. Acta 61 (1988) 901.

[16] M. Crum Quat. J. Math. 6 (1955) 121.

J. H. Caltenco, J. López Bonilla, M. A. Acevedo
Sección de Estudios de Posgrado e Investigación
Escuela Superior de Ingenieria Mecánica y Eléctrica
Instituto Politécnico Nacional
Edificio Z, acceso 3, 3er Piso. Col. Lindavista C.P. 07738 México D.F.
E-mail: lopezbjl@hotmail.com; jcaltenco@ipn.mx

ON ODD-SUMMING NUMBERS

Erzsébet Orosz (Eger, Hungary)

Abstract. In this paper we investigate two theorems dealing with those natural numbers which can be written as the sum of two or more consecutive odd numbers.

AMS Classification Number: 95U50

1. Introduction

Olson [3] proved that a natural number n is the sum of two or more consecutive natural numbers if and only if n is not a power of 2.

C. Ray and S. Harris [3] proved the following:

The natural number n can be written as the sum of consecutive odd natural numbers $2r+1, 2r+3, \dots, 2s-1$ if and only if

$$n = s^2 - r^2 = (s-r)(s+r).$$

The natural number n is odd-summing if and only if either n is the product of two odd numbers, each greather than 1, or n is the product of two even numbers.

Suppose that $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$, where $p_1, p_2, \dots, p_t$ are distinct primes, $p_1 < p_2 < \dots < p_t$, and each $k_i > 0$. In [3] the following statements have been proved:

(i) If n is odd and is not a square then

$$\frac{(k_1+1)(k_2+1)\cdots(k_t+1)-2}{2}$$

representation of n exist.

(ii) If n is odd square then

$$\frac{(k_1+1)(k_2+1)\cdots(k_t+1)-1}{2}$$

representation of n exists.

(iii) If $p_1 = 2$ and n is not a square then

$$\frac{(k_1-1)(k_2+1)\cdots(k_t+1)}{2}$$

representation of n exists.

(iv) If $p_1 = 2$ and n is a square then

$$\frac{(k_1-1)(k_2+1)\cdots(k_t+1)+1}{2}$$

representation of n exists.

The natural number n has a unique representation as the sum of consecutive odd numbers if and only if n is the square of a prime number, if n is the cube of a prime number, if n is four times a prime number, or if n is the product of two different odd prime numbers.

The author proved in [2] that no set of four consecutive natural numbers exists that are all odd-summing or that are all not odd-summing.

The purpose of this paper is to form some new results of the properties of the odd-sumning numbers. First we define by [2] and [3] the concept of these special numbers, then we give our theorems and proofs.

2. Results and proofs

Definition. All natural numbers that are the sum of two or more consecutive odd numbers are called odd-summing numbers.

Remark. It is clear that all square numbers are odd-summing numbers but keep in mind that not all odd-summing numbers are square numbers, take 8 as a counterexample: $8 = 3 + 5$. In this paper we denote the set of the odd-summing numbers by N_o.

Theorem 1. *If $n \geq 2$ and $k \geq 2$ are integers then n^kcan be written as the sum of n consecutive odd-numbers, ($n^k \in N_o$, or n^k is an odd-summing number).*

Proof. Write n^k as the sum of equal terms.

$$n^k = nn^{k-1} = n^{k-1} + n^{k-1} + \cdots + n^{k-1}. \tag{1}$$

Next we show, that the sum (1) can be written as the sum of consecutive odd numbers. Form pairs of the first and last terms, the second and the one but last terms, and so on. We separate the proof into two parts according to the parity of n.

1.1. If n is an even number then the terms are also even numbers, because $k-1 \geq 1$.

Subtract 1 from the first term of the middle pair and add 1 to the second term of the middle pair. Thus we get $n^{k-1}-1$ and $n^{k-1}+1$; are consecutive odd numbers.

Similarly dencrease the $(\frac{n}{2}-1)$st and increase the $(\frac{n+2}{2}+1)$st terms by the next odd number, 3 or $2\cdot 1+1$; the $(\frac{n}{2}-2)$th and $\frac{n+2}{2}+2$th by 5, or $2\cdot 2+1$, and so on, at the end the $\frac{n}{2}-(\frac{n}{2}-1)=$ 1st and the $\frac{n+2}{2}+(\frac{n}{2}-1)=n$th terms by $2(\frac{n}{2}-1)+1=n-1$.

We get from (1)

$$\begin{aligned}(2)\qquad & n^k=(n^{k-1}-n+1)+(n^{k-1}-n+3)+\ldots+(n^{k-1}-3)+(n^{k-1}-1)+\\ & (n^{k-1}+1)+(n^{k-1}+3)+\cdots+(n^{k-1}+n-3)+(n^{k-1}+n-1).\end{aligned}$$

The terms of (2) are odd, the difference of two consecutive terms is 2, the number of terms is

$$(3)\qquad 1+\frac{(n^k+n-1)-(n^k-n+1)}{2}=n.$$

1.2. If n is an odd number then the middle term of (1) is alone, the number of pairs is $\frac{n-1}{2}$.

The middle term is the $\frac{n-1}{2}+1=\frac{n+1}{2}$th one, the adjacent elements are $\frac{n-1}{2}$ and $\frac{n+3}{2}$.

In this case the terms are odd numbers. So starting from the middle term we change the terms of pairs by $2,4,\ldots,2\frac{n-1}{2}=n-1$ so from (1) we get

$$\begin{aligned}(4)\qquad & n^k=(n^{k-1}-n+1)+(n^{k-1}-n+3)+\cdots+(n^{k-1}-4)+(n^{k-1}-2)+\\ & n^{k-1}+(n^{k-1}+2)+(n^{k-1}+4)+\cdots+(n^{k-1}+n-3)+(n^{k-1}+n-1).\end{aligned}$$

The number of terms is n, all terms are odd numbers, and the difference of adjacent terms is 2. Theorem 1 is proved.

Note. Theorem 1 can be proved by a simpler method as well. Adding the n numbers $-n+1,-n+3,\ldots,n-1$ to the numbers of the sum we get:

$$(n^{k-1}-n+1)+(n^{k-1}-n+3)+\cdots+(n^{k-1}+n-3)+(n^{k-1}+n-1).$$

The difference of the consecutive numbers in the sum is 2 and each of the numbers added are odd since $k\geq 2$.

Theorem 2. *If $n \geq 1$ then the $n(n+1)(n+2)(n+3)+1$ is an odd-summing number.*

Proof. The proof follows immediately from the fact that $n(n+1)(n+2)(n+3)+1 = k^2$ for all natural numbers $k \geq 1$.

If we add 1 to the product of four consecutive natural number then

$$\begin{aligned} n(n+1)(n+2)(n+3)+1 =&(n^2+n)(n^2+5n+6)+1 \\ =&n^4+n^3+5n^3+5n^2+6n^2+6n+1 \\ =&n^4+6n^3+11n^2+6n+1 \end{aligned}$$

holds. This can be written in the form

$$\begin{aligned} [(n^2+3n)+1]^2 =&(n^2+3n)^2+2(n^2+3n)+1 \\ =&n^4+6n^3+9n^2+2n^2+6n+1 = n^4+6n^3+11n^2+6n+1 \\ =&n(n+1)(n+2)+(n+3)+1 = k^2. \end{aligned}$$

It is well known that a perfect square is an odd-summing number. Thus Theorem 2 is proved.

The converse of Theorem 2 does not hold.

Remarks

1. The proof of Theorem 1 furnishes an algorithm to find all terms of consecutive odd numbers that adds to n^k.
2. Theorem 1 and Theorem 2 can be proved by the results of C. Ray and S. Harris in [3].
3. If n is a natural number then $n(n+1)(n+2)(n+3)$ and $n(n+1)(n+2)(n+3)+1$ are consecutive odd-summing numbers. Theorem 2 amplifies and clarifies this fact.

   Examples:

   If $n = 1$ then $1 \cdot 2 \cdot 3 \cdot 4 + 1 = 25$, $25 = 1+3+5+7+9$ and $24 = 11+13$.

   If $n = 2$ then $2 \cdot 3 \cdot 4 \cdot 5 + 1 = 121$ and $120 = 59+61$ are odd-summing numbers.

References

[1] Olson, M., Sequentially so. *Mathematics Magazin* (1991), 297–298.

[2] Orosz, Gyuláné, Partíciók páratlan számokkal, *Acta. Acad. Paed. Agriensis, Sect. Math.* **29** (2002), 107–114.

[3] Ray, C., Harris, S., An odd sum. *Mathematics Teacher* **95**, Number 3 (2002).

Erzsébet Orosz
Department of Mathematics
Károly Eszterházy College
Leányka str. 4.
H-3300 Eger, Hungary
E-mail: ogyne@ektf.hu

ACTA ACADEMIAE PAEDAGOGICAE AGRIENSIS

SECTIO MATHEMATICAE

International journal for mathematics and computer science
Referred by Zentralblatt für Mathematik and Mathematical Reviews

The journal of the Eszterházy Károly College is open for scientific publications in any field of mathematics and computer science. Methodological papers are also welcome. Papers submitted to the journal should be written in English. Only new and unpublished material can be accepted.

Authors are kindly asked to write the final form of their manuscript in LaTeX. If you have any problems or questions, please write an e-mail to the Editor: matek@ektf.hu.

The following volumes are available at

http://www.ektf.hu/tanszek/matematika/acta.html:

Vol. 24 (1997)

Vol. 25 (1998)

Vol. 26 (1999)

Vol. 27 (2000)

Vol. 28 (2001)

Vol. 29 (2002)

Vol. 30 (2003)

Vol. 31 (2004)

Contents

Methodological papers