ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS

NOVA SERIES TOM. XXX.

SECTIO MATHEMATICAE

REDIGIT
KÁLMÁN GYŐRY, FERENC MÁTYÁS

EGER, 2003

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXX.

SECTIO MATHEMATICAE

REDIGIT
KÁLMÁN GYŐRY, FERENC MÁTYÁS

EGER, 2003

Professor Péter Kiss (1937-2002)

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 7–22*

PÉTER KISS AND THE LINEAR RECURSIVE SEQUENCES

Kálmán Liptai, Ferenc Mátyás (Eger, Hungary)

Dedicated to the memory of Professor Péter Kiss

Péter Kiss was born in Nagyréde in 1937. He attended secondary school in Gyöngyös and in 1955 he entered the Eötvös Lóránd University Faculty of Science in Budapest. He took his teacher's diploma in mathematics and physics. After finishing university, he taught at the Gárdonyi Géza Secondary School in Eger for 12 years.

He began to teach at what is now called the Eszterházy Károly College at the Department of Mathematics in 1972 and taught there until his death in 2002. He took a special interest in Number Theory. His doctoral thesis "Second order linear recurrence and pseudoprime numbers" was submitted in 1977. He obtained the candidate's degree in 1980, the title of his dissertation was "Second order linear recursive sequences and their applications in diophantine problems". In 1995 Péter Kiss habilitated at the Kossuth Lajos University of Debrecen and he was inaugurated as professor. He got the Szent-Györgyi Albert prize in 1997. He got the title of doctor of mathematical science of Hungarian Academy of Sciences in 1999.

His lectures were lucid and meticulously crafted and through him many of his students grew to like mathematics and research. He brought into existence a research group in Number Theory and supported the work of his inquiring students and colleagues. One of his students, Bui Minh Phong, was awarded the Rényi Kató prize in 1976. He was the supervisor of the doctoral theses of the following colleagues: Ferenc Mátyás, Sándor Molnár, Béla Zay, Kálmán Liptai, László Szalay, and helped Bui Minh Phong, László Gerőcs and Pham Van Chung in writing of their theses.

He took an enthusiastic part in the everyday world of mathematics. He held several county and national posts in the János Bolyai Mathematical Society. He was a contributor to the abstracting journals Mathematical Reviews and Zentralblatt für Mathematik and he was also a permanent member of organizing committee of the Fibonacci Conference. He was a highly respected member of the community of mathematicians. This was proved by many joint papers, invitations to conferences and friends all over the world.

This paper is devoted to the summary of his academic achievements.

Research has been supported by the Hungarian Research Fund (OTKA) Grant T-032898.

1. Introduction

In 1202 Leonardo Pisano, or Fibonacci, employed the recurring sequence $1, 2, 3, 5, 8, 13, \ldots$ in a problem on the number of offspring of a pair of rabbits. Let's denote by F_n and F_{n+1} the n-th and $(n+1)$-th term of this sequence, respectively. In this case $F_{n+2} = F_{n+1} + F_n$, where $F_0 = 0$ and $F_1 = 1$. Simple generalizations of the Fibonacci sequence are the second order linear recurrences. The sequence $\{R_n\}_{n=0}^{\infty} = R(A, B, R_0, R_1)$ is called a second order linear recurrence if the recurrence relation

$$R_n = AR_{n-1} + BR_{n-2} \qquad (n > 1)$$

holds for its terms, where A, $B \neq 0$, R_0 and R_1 are fixed rational integers and $|R_0| + |R_1| > 0$. The sequence $R(A, B, 2, A)$ is called the associate sequence of the sequence $R(A, B, 0, 1)$.

The polynomial $x^2 - Ax - B$ is called the companion polynomial of the second order linear recurrence $R = R(A, B, R_0, R_1)$. The zeros of the companion polynomial will be denoted by α and β. In the sequel we assume that the sequence is not degenerate, i.e. α/β is not a root of unity, and we order α and β so that $|\alpha| \geq |\beta|$. Using this notation, we get that

$$R_n = \frac{a\alpha^n - b\beta^n}{\alpha - \beta},$$

where $a = R_1 - R_0\beta$ and $b = R_1 - R_0\alpha$.

Consider now a generalization of second order linear recurrences.

The sequence $G(A_1, A_2, \ldots, A_k, G_0, G_1, \ldots, G_{k-1}) = \{G_n\}_{n=0}^{\infty}$ is called a k-th order linear recursive sequence of rational integers if

$$G_n = A_1G_{n-1} + A_2G_{n-2} + \cdots + A_kG_{n-k} \qquad (n > k-1),$$

for certain fixed rational integers $A_1, A_2, \ldots, A_k$ with $A_k \neq 0$ and $G_0, G_1, \ldots, G_{k-1}$ not all zero. The companion polynomial of a recurrence with coefficients $A_1, A_2, \ldots, A_k$ is given by $x^k - A_1x^{k-1} - A_2x^{k-2} - \cdots - A_k$. Denote by $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_s$ the distinct zeros of the companion polynomial. Assume that $\alpha, \alpha_2, \ldots, \alpha_s$ has multiplicity $1, m_2, \ldots, m_s$ respectively and that $|\alpha| > |\alpha_i|$ for $i = 2, \ldots, s$. The zero α is called the dominating root of the polynomial. It is known that in this case the terms of the sequence can be written in the form

$$G_n = a\alpha^n + r_2(n)\alpha_2^n + \cdots + r_s(n)\alpha_s^n \qquad (n \geq 0)\,,$$

where the r_i's $(i = 2, \ldots, s)$ are polynomials of degree $m_i - 1$ and the coefficients of these polynomials as well as a are elements of the algebraic number field $\mathbf{Q}(\alpha, \alpha_2, \ldots, \alpha_s)$.

2. Common terms and difference of the terms of linear recurrences

Let $G(A_1, \ldots, A_k, G_0, \ldots, G_{k-1})$ and $H(B_1, \ldots, B_r, H_0, \ldots, H_{r-1})$ be linear recurrence sequences having dominating roots. Let $p_1 < p_2 < \cdots < p_s$ be different primes and denote by S the set of rational integers which have only these primes as prime factors. We suppose that $1 \in S$.

M. Mignotte (1978) studied the common terms of linear recurrences, that is, the equation

$$G_x = H_y.$$

P. Kiss proved the following theorem in [19].

Theorem 2.1. *Let G and H be linear recurrence sequences with dominating roots α and β, respectively. In this case*

$$G_n = a\alpha^n + g_2(n)\alpha_2^n + \cdots + g_s(n)\alpha_s^n,$$

and

$$H_n = b\beta^n + q_2(n)\beta_2^n + \cdots + q_t(n)\beta_t^n.$$

We suppose that $G_i \neq a\alpha^i$, $H_j \neq b\beta^j$ and $s_1 a\alpha^i \neq s_2 b\beta^j$ for any $s_1, s_2 \in S$ if $\max(i, j) > n_0$. If

$$s_1 G_x = s_2 H_y$$

for some $s_1, s_2 \in S$, then $\max(x, y) < n_1$, where n_1 is effectively computable and depends on S, n_0 and the parameters of the sequences G and H.

P. Erdős asked whether the terms of the recurrence sequences could be close to each other. P. Kiss answered this question in [30].

Theorem 2.2. *Suppose that G and H are linear recurrences satisfying the conditions of Theorem 2.1. Then for any integers $s_1, s_2 \in S$*

$$\big||s_1 G_x| - |s_2 H_y|\big| > \exp\big\{c \cdot \max(x, y)\big\}$$

for all integers $x, y > n_2$, where c and n_2 are effectively computable positive numbers depending only on S, n_0 and the parameters of G and H.

P. Kiss generalized a result of Shorey and Stewart in [30].

Theorem 2.3. *Let G be a linear recurrence sequence satisfying the conditions of Theorem 2.1. If*

$$sx^q = G_n$$

for some positive integers $s \in S, q, n$ and $x > 1$, then $q < n_3$, where n_3 is an effectively computable positive number depending only on S, n_0 and the parameters of G.

A similar result was proved in the same paper.

Theorem 2.4. *Let G be a linear recurrence sequence as in Theorem 2.1. Furthermore assume that $k > 2$, $|\alpha_2| \neq 1$, $|\alpha_2| > |\alpha_3| \geq |\alpha_j| \quad (j > 3)$ and $g_2(i) \neq 0$, if $i > n_0$. Then*

$$|sx^q - G_n| > e^{cn}$$

for all positive integers $s \in S, x, q, n$ and with $q, n > n_4$, where n_4 is an effectively computable positive number depending only on S, n_0 and the parameters of G.

3. Prime divisors of second order linear recurrences

Let $R(A, B, 0, 1)$ be a non-degenerate second order linear recurrence sequence where $R_0 = 0, R_1 = 1$ and $(A, B) = 1$. If p is a prime with $p \nmid B$, then there are terms R_n of R (different from $R_0 = 0$) which are divisible by p. The least index of these terms is called the rank of apparition of p in the sequence R and is denoted by $r(p)$. Thus $p \mid R_{r(p)}$, but $p \nmid R_m$ if $0 < m < r(p)$. If $r(p) = n$, then we say that p is a primitive divisor of R_n. If p is a primitive divisor of R_n and $p^k \mid R_n$ $(k \geq 1)$, but $p^{k+1} \nmid R_n$, then we say p^k is a primitive prime power divisor of R_n. P. Kiss proved the following theorem in [36].

Theorem 3.1. *Let $\mathcal{R}_n$ be the product of primitive prime power divisors of R_n. Then*

$$\sum_{n \leq x} \log \mathcal{R}_n = \frac{3 \cdot \log |\alpha|}{\pi^2} x^2 + O(x \log x),$$

provided that x sufficiently large. (The constant involved in $O()$ depends on the parameters of the sequence.)

In the joint paper [45] P. Kiss and B. M. Phong studied the reciprocal sum of primitive prime divisors of the terms of second order linear recurrences. To formulate this, let $R(A, B, 0, 1)$ be a second order linear recurrence and

$$p(n) = \sum_{r(p)=n} \frac{1}{p}$$

the reciprocal sum of primitive prime divisors of R_n $(n > 0)$, $(p(n) = 0$, if there is no primitive prime divisor of $R_n)$. Furthermore let

$$f(n) = \sum_{p \mid R_n} \frac{1}{p}$$

be the reciprocal sum of all prime divisors of the term R_n, $(f(n) = 0$, if there is no prime divisor). Using this notation they proved that

$$f(n) < \log \log \log n + c$$

for sufficiently large n. This is the best possible result apart from the constant c.

The average of the previous functions was studied in Kiss [47]. The main results are the following.

Theorem 3.2. *There exists a constant $c > 0$ depends on the sequence R such that*

$$\sum_{n \le x} f(n) = cx + O(\log\log x)$$

for sufficiently large x.

Theorem 3.3. *There exists an absolute constant $c > 0$ such that*

$$p(n) < c\frac{(\log\log n)^2}{n}$$

for sufficiently large n. Furthermore

$$\sum_{n \le x} p(n) = \sum_{r(p) \le x} \frac{1}{p} = \log\log x + O(1).$$

4. Approximation problems

Let $G(A, B, R_0, R_1)$ be a nondegenerate second order linear recurrence, and $D = A^2 + 4B$ denote the discriminant of its companion polynomial. If $D > 0$ then the quotion R_{n+1}/R_n is a convergent of the irrational number α. The sharpness of the convergent was studied in Kiss [16].

Theorem 4.1. *Suppose that $D > 0$, $G_0 = 0$, $G_1 = 1$ and that α is an irrational number. Then the inequality*

$$\left|\alpha - \frac{G_{n+1}}{G_n}\right| < \frac{1}{c \cdot G_n^2}$$

holds for some $c > 0$ and infinitely many n if and only if $|B| = 1$ and $c \le \sqrt{D}$. Moreover if $|B| = 1$ and the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{D}q^2}$$

holds for some rational number p/q then $p/q = G_{n+1}/G_n$ for some positive integer n.

In general G_{n+1}/G_n is a weaker convergent of α. In the joint paper [55] P. Kiss and Zs. Sinka proved the following theorem.

Theorem 4.2. *Let G be a non-degenerate second order linear recurrence with $D > 0$. Define the numbers k_0 and c_0 by*

$$k_0 = 2 - \frac{\log|B|}{\log|\alpha|} \quad \text{and} \quad c_0 = \frac{\sqrt{D}^{k_0-1}}{|a^{k_0-1}b|}$$

and let k and c positive real numbers (a and b were defined in the introduction). Then

$$\left|\alpha - \frac{G_{n+1}}{G_n}\right| < \frac{1}{cG_n^k}$$

holds for infinetely many integer n if and only if $k < k_0$ and c is arbitrary, or $k = k_0$ and $c < c_0$, or $k = k_0$, $c = c_0$ and $B > 0$, or $k = k_0$, $c = c_0$, $B < 0$ and $b/a > 0$.

P. Kiss and R. F. Tichy [39], [40] have dealt with the convergent of $|\alpha|$ by rational numbers of the forms $\left|\frac{G_{n+1}}{G_n}\right|$.

Theorem 4.3. *Let G be a non-degenerate second order linear recurrence. If $D < 0$ then there is a positive number c, depending only on the parameters of the sequence G, such that*

$$\left||\alpha| - \left|\frac{G_{n+1}}{G_n}\right|\right| < \frac{1}{n^c}$$

for infinitely many n.

Furthermore they showed that apart from the constant c, it is the best possible approximation.

Theorem 4.4. *Let G be a non-degenerate second order linear recurrence. If $D < 0$ then there is a positive number c', such that*

$$\left||\alpha| - \left|\frac{G_{n+1}}{G_n}\right|\right| > \frac{1}{n^{c'}}$$

for any sufficiently large n.

For the Fibonacci sequence Y. V. Matijasevich and R. K. Guy proved that

$$\lim_{n\to\infty} \sqrt{\frac{6 \cdot \log(F_1 \cdot F_2 \cdots F_n)}{\log[F_1, F_2, \ldots, F_n]}} = \pi.$$

In the joint paper [38] P. Kiss and F. Mátyás generalized this result. They showed that the Fibonacci sequence can be replaced by any non-degenerate second order linear recurrence sequence G with $G_0 = 0, G_1 = 1$ and $(A, B) = 1$. Using a Baker type result, they also gave an error term of the form $O\left(1/\log n\right)$.

5. Recursive sequences and diophantine equations

The equation

$$x^2 - Dy^2 = N,$$

with given integers D and N and variables x and y, is called Pell's equation. If D is negative, it can have only a finite number of rational integer solutions. If D is a perfect square, say $D = a^2$, the equation reduces to

$$(x - ay)(x + ay) = N$$

and again there are only a finite number of solutions. The most interesting case arises when D is a positive integer and not a perfect square.

In [8] P. Kiss and F. Várnai proved that the solutions (x, y) of the equation

$$x^2 - 2y^2 = N$$

can be given with the help of terms of finitely many second order linear recurrences $P(2, 1, P_0, P_1)$, such that

$$(x, y) = (\pm(P_{2n} + P_{2n+1}), \pm P_{2n+1}).$$

P. Kiss [25] generalized this result in the following form.

Theorem 5.1. *If the equation*

$$x^2 - (a^2 + 1)y^2 = N$$

has a solution for a fixed integer $a > 0$, then all solutions (x, y) can be given with the help of finitely many linear recurring sequences $G(2a, -1, G_0, G_1)$ such that

$$(x, y) = (\pm(G_{2n} + aG_{2n+1}) \pm G_{2n+1}),$$

where

$$0 \le G_1 < 2a\sqrt{N} \quad \text{for} \quad N > 0$$

and

$$0 \le G_1 < (2a^2 + 1)\sqrt{\frac{-N}{a^2 + 1}} \quad \text{for} \quad N < 0.$$

In the same paper P. Kiss proved the following theorem.

Theorem 5.2. *If the equation*

$$x^2 - (a^2 - 4)y^2 = 4N$$

has a solution for a fixed integer $a > 0$, then all solutions (x, y) can be given with the help of finitely many second order linear recurring sequences $G(a, -1, G_0, G_1)$ such that

$$(x, y) = (\pm H_{2n}, \pm G_{2n}),$$

where H is the associate sequence of G and

$$0 \leq G_1 < \sqrt{N} \quad \text{for} \quad N > 0$$

and

$$0 \leq G_1 < a\sqrt{\frac{-N}{a^2 - 4}} \quad \text{for} \quad N < 0.$$

In their joint paper [77] P. Kiss and K. Liptai found relationships between Fibonacci numbers and solutions of special diophantine equations.

Theorem 5.3. *All positive integer solutions of the equation*

$$x^2 + x(y - 1) - y^2 = 0$$

are of the form

$$(x, y) = (F_{2h+1}^2, F_{2h+1}F_{2h+2}),$$

where F_i is the i-th Fibonacci number.

List of publications of Péter Kiss

[1] Magasabbfokú egyenletek tárgyalásának egy módja a számítástechnika elemeinek felhasználásával,(A treatment of higher degree equations by means of computers), (with B. Szepessy). *Acta Acad. Paed. Agriensis*, Eger, **11** (1973), 287–303.

[2] Egy számelméleti probléma általánosítása, (A generalization of a problem of number theory), *Mat. Lapok.*, **25** (1974), 145–149.

[3] Néhány számelméleti probléma vizsgálata számítógép felhasználásával, (Solutions of some problems of number theory using computer), *Acta Acad. Paed. Agriensis*, Eger, **13** (1975), 379–393.

[4] One way of making automorphic numbers, *Publ. Math. Debrecen*, **22** (1975), 199–203.

[5] A generalization of a problem in number theory, *Mat. Sem. Not. (Kobe Univ., Japan)*, **5** (1977), 313—317.

[6] On the connection between the rank of apparition of a prime p in Fibonacci sequence and the Fibonacci primitive roots, (with B. M. Phong), *Fibonacci Quart.,* **15** (1977), 347–349.

[7] Egy binom kongruenciáról, (On a binom congruence), *Acta Acad. Paed. Agriensis*, Eger, **14** (1978), 457–464.

[8] On generalized Pell numbers, (with F. Várnai) *Mat. Sem. Not. (Kobe Univ. Japan),* **6** (1978), 259–267.

[9] On a function cencerning second order recurrences, (with B. M. Phong), *Ann. Univ. Sci. Budapest. Etvs,* **21** (1978), 119–122.

[10] A Pell sorozat néhány tulajdonságáról, (Some properties of Pell sequences), (with F. Mátyás and F. Várnai), *Acta Acad. Paed. Agriensis*, Eger, **15** (1979), 411–417.

[11] Divisibility properties in second order recurrences, (with B. M. Phong), *Publ. Math. Debrecen,* **26** (1979), 187–198.

[12] Zero terms in second order linear recurrences, *Math. Sem. Not. (Kobe Univ., Japan),* **7** (1979), 145–152.

[13] Diophantine representation of generalized Fibonacci numbers, *Elem. Math.,* **34** (1979), 129–132.

[14] A method for solving diophantine equations, *Amer. Math. Monthly,* **86** (1979), 384–387.

[15] Connection between second order recurrences and Fermat's last theorem, *Period. Mat. Hungar.,* **11** (1980), 151–157.

[16] Diophantine approximative property of the second order linear recurrences, *Period. Math. Hungar.,* **11** (1980), 281–287.

[17] On Lucas and Lehmer sequences and their applications to Diophantine equations, (with K. Győry and A. Schinzel), *Coll. Math.,* **45** (1981), 75–80.

[18] Közös elemek másodrendű rekurzív sorozatokban, (On common terms of second order linear recurrences), *Acta Acad. Paed. Agriensis*, Eger, **16** (1982), 539–546.

[19] On common terms of linear recurrences, *Acta Math. Acad. Sci. Hungar.,* **40** (1982), 119–123.

[20] On second order recurrences and continued fractions, *Bull. Malaysian Math. Soc. (2),* **5** (1982), 33–41.

[21] Note on super pseudoprime numbers, (with J. Fehér) *Ann. Univ. Sci. Budapest. Etvs,* **26** (1983), 157–159.

[22] On some properties of linear recurrences, *Publ. Math. Debrecen,* **30** (1983), 273–281.

[23] On linear recurrences, *Coll. Math. Soc. J. Bolyai,* Topics in classical number theory, Budapest, **1981** (1984), 855–861.

[24] On distribution of linear recurrences mod 1, (with S. Molnár), *Stud. Sci. Math. Hungar.,* **17** (1982), 113–127.

[25] Pell egyenletek megoldása lineáris rekurzív sorozatok segítségével, (Solutions of the Pell equations with the help of linear recurrences), *Acta Acad. Paed. Agriensis*, Eger, **17** (1984), 813–824.

[26] Note on distribution of the sequence $n\theta$ modulo a linear recurrence, *Discussiones Mathematicae,* **7** (1985), 135–139.

[27] A distribution property of second-order linear recurrences, *Fibonacci numbers and their applications* (ed. A. N. Philippou, G. E. Bergum, A. F. Horadam), *D. Riedel Publ. Comp.,* (1986), 121–130.

[28] On Lucas pseudoprimes which are products of s primes, (with B. M. Phong and E. Lieuwens), *Fibonacci numbers and their applications* (ed. by A. N. Philippou, G. E. Bergum, A. F. Horadam), *Riedel Publ. Comp.*, (1986), 131—139.

[29] Distribution of the ratios of the terms of a second order linear recurrence, (with R. F. Tichy), *Proc. of the Koninkl. Nederlandse Acad. van Wetensch.,* A **89** (1986), 79–86.

[30] Differences of the terms of linear recurrences, *Studia Sci. Math. Hungar.,* **20** (1985), 285–293.

[31] Some results on Lucas pseudoprimes, *Ann. Univ. Sci. Budapest, Etvs,* **28** (1985), 153–159.

[32] On a problem of A. Rotkiewicz, (with B. M. Phong) *Math. Comp.,* **48** (1987), 751–755.

[33] On uniform distribution of sequences, (with R. Tichy) *Proc. Japan Acad.,* **63** ser. A, No. 6 (1987), 205–207.

[34] A Lucas számok prímosztóiról, (Prime divisors of Lucas numbers), *Acta Acad. Paed. Agriensis*, Eger, **18/11** (1987), 17–25.

[35] Kombinatorika és gráfelmélet, (Combinatorics and graph theory), (with G. Hetyei), *Jegyzet, Eger–Pcs,* (1988)

[36] Primitive divisors of Lucas numbers, *Applications of Fibonacci Numbers,* (ed. by A. N. Philippon et al.), *Kluwer Acad. Publ.,* (1988), 29–38.

[37] A lower bound for the counting function of Lucas pseudoprimes, (with P. Erdős and A. Sárközy), *Math. Comp.,* **51** (1988), 315–323.

[38] An asymptotic formula for π, (with F. Mátyás) *J. Number Theory,* **31** (1989), 255–259.

[39] A discrepancy problem with applications to linear recurrences I., (with R. F. Tichy) *Proc. Japan Acad.,* **65** (ser. A), No. 5 (1989), 135–138.

[40] A discrepancy problem with applications to linear recurrences II., (with R. F. Tichy), *Proc. Japan Acad.,* **65** (ser. A), No. 6 (1989), 131–194.

[41] Weakly composite Lucas number, (with B. M. Phong) *Ann. Univ. Sci. Budapest. Etvs, Sect. Math.,* **31** (1988), 179–182.

[42] On the number of solutions of the diophantine equation $\binom{x}{p} = \binom{y}{2}$, *Fibonacci Quart.,* **26** No. 2 (1988), 127–130.

[43] On primitive prime power divisors of Lucas numbers, *Coll. Math. Soc. J. Bolyai, Number Theory*, Budapest, **51** (1987), 773–786.

[44] On rank of apparition of primes in Lucas sequences, *Publ. Math. Debrecen,* **36** (1989), 147–151.

[45] Reciprocal sum of prime divisors of Lucas numbers, (with B. M. Phong) *Acta Acad. Paed. Agriensis*, Eger, **19** (1989), 47–54.

[46] Results on the ratios of the terms of second order linear recurrences, *Conference Report of 9th Czechoslovak Colloquium on Number Theory,* Rackova Dolina, (1989), 28–33.

[47] On prime divisors of the terms of second order linear recurrence sequences, *Applications of Fibonacci numbers,* (ed. by G. E. Bergum et al.), *Kluwer Acad. Publ.,* (1990), 203–207.

[48] On asymptotic distribution modulo a subdivision, (with R. F. Tichy), *Publ. Math. Debrecen,* **37** (1990), 187–191.

[49] Results and problems concerning prime divisors of Lucas numbers, *Algebra and Number Theory,* (ed. by A. Grytczuk), *Pedagogical Univ. Zielona Gra,* (1990), 43–48.

[50] On prime divisors of Mersenne numbers, (with P. Erdős and C. Pomerance), *Acta Arithm.,* **57** (1991), 267–281.

[51] A Lucas-számok prímosztóinak egy tulajdonságáról, (On properties of prime divisors of Lucas numbers), *Acta Acad. Paed. Agriensis, Sect. Math.,* **20** (1991), 15—20.

[52] Results on the ratios of the terms of second order linear recurrences, *Math. Slovaca,* **41** (1991), 257–260.

[53] Lucas-számok Wieferich-típusú prímosztói, (Prime divisors of Wieferich type Lucas numbers), *Mat. Lapok,* **34** (1987), 93–98. (1991.)

[54] Average order of logarithms of terms in binary recurrences, (with B. Tropak), *Discuss. Math.,* **10** (1990), 29–39.

[55] On the ratios of the terms of second order linear recurrences, (with Zs. Sinka), *Period. Math. Hungar.,* **23** (1991), 139–143.

[56] On a generalization of a recursive sequence, (with B. Zay), *Fibonacci Quart.,* **30** (1992), 103–109.

[57] Linear recursive sequence and power series, (with J. P. Jones), *Publ. Math. Debrecen.,* **41** (1992), 295–306.

[58] Some Diophantine approximation results concerning linear recurrences, (with J. P. Jones), *Math. Slovaca,* **42** (1992), 583–591.

[59] On reciprocal sum of terms of linear recurrences, (with J. Hancl), *Math. Slovaca,* **43** (1993), 31–37.

[60] Exponential Diophantine representation of binomial coefficients, factorials and Lucas sequences, (with J. P. Jones), *Discuss. Math.,* **12** (1992), 53–65.

[61] Average order of the terms of a recursive sequence, *sterr.–Ung.–Slow. Koll. ber Zahlentheorie, Graz,* (1992) *Grazer Math. Ber.,* **318** (1992), 45–52.

[62] An asymptotic formula concerning Lehmer numbers, (with J. P. Jones), *Publ. Math. Debrecen,* **42** (1993), 199–213.

[63] Some results concerning the reciprocal sum of prime divisors of a Lucas number, *Applications of Fibonacci Numbers* (eds by G. E. Bergum et al.), *Kluwer Acad. Publ., Netherland,* **5** (1993), 417–420.

[64] Properties of the least common multiple function, (with J. P. Jones), *Acta Acad. Paed. Agriensis, Sect. Math.,* **21** (1993), 65–72.

[65] On points whose coordinates are terms of a linear recurrence, *Fibonacci Quart.,* **31** (1993), 239–245.

[66] On sequences of zeros and ones, (with B. Zay), *Studia Sci. Math. Hungar.,* **29** (1994), 437–442.

[67] Pure powers and power classes in recurrence sequences, *Math. Slovaca,* **44** (1994), 525–529.

[68] Teljes hatványok lineáris rekurzív sorozatokban, (Perfect powers in linear recursive sequences), (with J. P. Jones), *Acta Acad. Paed. Agriesis, Sect. Mat.,* **22** (1994), 55–60.

[69] Diophantine approximation in terms of linear recurrent sequences, (with J. P. Grabner and R. F. Tichy), *Number Theory, Proceedings of the fourth Conf. of the Canadian Number Theory Association, Halifax,* 1994 (1995), 187–195.

[70] Some identities and congruences for a special family of second order recurrences, (with J. P. Jones), *Acta Acad. Paed. Agriensis, Sect. Mat.,* **23** (1995–96), 3–9.

[71] A note on the prime divisors of Lucas numbers, (with B. Zay), *Acta Acad. Paed. Agriensis, Sect. Mat.,* **23** (1995–96), 17–21.

[72] Some congruences concerning second order linear recurrences (with J. P. Jones), *Acta Acad. Paed. Agriensis*, Sect. Mat., **24** (1997), 29–33.

[73] On sums of the reciprocals of prime divisors of terms of a linear recurrence, *Applications of Fibonacci Numbers*, vol. 7, ed by G. E. Bergum et al., *Kluwer Acad. Publ.,* 1998, 215–220.

[74] An approximation problem concerning linear recurrences, *Number Theory, Diophantine, Computational and Algebraic Aspects* (Proc. of the International Conference, Eger, July 29–August 2, 1996), Walter de Gruyter GmBH & Co., 1998, 289–293.

[75] Some new identities and congruences for Lucas sequences (with J.P. Jones), *Discuss. Math.*, **18** (1998), 39–47.

[76] Representation of integers as terms of a linear recurrence with maximal index (with J. P. Jones), *Acta Acad. Paed. Agriensis, Sect. Mat.,* **25** (1998), 21–37.

[77] Solution of Diophantine equations by second order linear recurrences (with K. Liptai), *Ann. Univ. Sci. Budapest., Sect. Comp.,* **18** (1999) 109–114.

[78] On a problem concerning perfect powers in linear recurrences, *Acta Acad. Paed. Agriensis, Sect. Math.,* **26** (1999), 25–30.

[79] Note on a result of I. Nemes and A. Pethő concerning polynomial values in linear recurrences, *Publ. Math. Debrecen,* **56** (2000), 451–455.

[80] Results concerning products and sums of the terms of linear recurrences, *Acta Acad. Paed. Agriensis, Sect. Math.,* **27** (2000), 1–7.

[81] On sums of the terms of linear recurrences, *Acta Math. (Univ. Nitra),* **4** (2000), 27–31.

[82] On a simultaneous approximation problem concerning binary recurrences, *Acta Math. Acad. Paed. Nyiregyhaziensis,* **17/2** (2001), 71–76.

[83] Perfect powers from the sums of terms linear recurrences (with F. Mátyás), *Period. Math. Hungar.,* **42** (2001), 163–168.

[84] On products and sums of the terms of linear recurrences (with F. Mátyás), *Acta Acad. Paed. Agriensis Sect. Math.*, **28** (2001), 3–11.

[85] Product of the terms of linear recurrences (with F. Mátyás), *Studia Sci. Math. Hungar.,* **37** (2001), 355–362.

Lectures in conferences

[1] On linear recurrences, International Number Theory Conference, Budapest, 1981.

[2] On distributions of sequences, Austrian–Hungarian Number Theory Conference, Visegrád, 1983.

[3] Linear recurrences mod m, Austrian–Hungarian Number Theory Conference, Budapest, 1983.

[4] Distributions of some sequences mod 1, Austrian–Hungarian Number Theory Conference, Viena, 1984.

[5] Some properties of linear recurrrences, Fibonacci Conference, Patras (Greek), 1984.

[6] Distribution properties of linear recuerrences, Polish Mathematical Conference, Zielona Góra–Zagan, 1985. VI. 24–27.

[7] Prime divosors of Lucas numbers, Austrian–Hungarian Number Theory Conference, Viena, 1986. V. 2–3.

[8] Primitive prime divisors of Lucas numbers, International Number Theory Conference, Miskolc, 1986. VI. 22.

[9] On divisors of Lucas numbers, Polish Mathematical Conference, Zagan, 1986. IX. 8–11.

[10] On greatest prime power divisors of the terms of linear recurrences, Fibonacci numbers and reccurence sequence, International Number Theory Conference, Eger, 1986. IX. 19–20.

[11] Prime power divisors of Lucas numbers, Fibonacci numbers and recurrence sequences, International Conference, Eger, 1987. V. 16–17.

[12] On primitive prime power divisors of Lucas Numbers, Colloquium on Number Theory, Budapest, 1987. VII. 20–25.

[13] On divisors of Mersenne numbers and their generalizations, University Number Theory Conference, Patras (Greek), 1987. IX. 16.

[14] Reciprocal sum of prime divisors of Lucas number, III. International Number Theory Conference, Eger, 1988. V. 17–18.

[15] On prime divisors of the terms of second order linear recurrence sequences, (Third International Conference on Fibonacci Numbers and their Applications,) Pisa, 1988. VII. 25–29.

[16] Results and problems concerning prime divisors of Lucas numbers, 7. Polish Mathematical Conference, Kalsk–Zielona Góra, 1988. IX. 19–22.

[17] Approximation properties of linear recurrences, IV. International Number Theory Conference, Eger, 1989. V. 23–24.

[18] Results on the ratios of the terms of second order linear recurrences, IX. Czechoslovak Number Theory Coll., (Rackova Dolina), 1989. IX. 11–15.

[19] Some asymptotic formulas concerning linear recursive sequences, International Conference on Sets, Graphs and Numbers, Budapest, 1991. I. 20–26.

[20] Some diophantine approximative results concerning linear recurrences, 10^{th} Czechoslovak Number Theory Conference, Myto pod Dumbierom, 1991. IX. 2–8.

[21] On a recurrence sequence, Austrian–Hungarian–Czechoslovak Number Theory Conference, Graz, 1992. VI. 15–17.

[22] Some results concerning reciprocas sum of prime divisors of Lucas numbers, 5^{th} International Conference on Fibonacci Numbers and their Applications, St. Andrews (Scotland), 1992. VIII. 20–24.

[23] On prime divisors of Lucas numbers, Polish Mathematical Conference, Lubiatow–Zielona Góra, 1992. IX. 21–24.

[24] Perfect powers and power classes in recurrence sequences, 11^{th} Czecho-Slovak International Conference on Number Theory, Rackova Dolina, 1993. Sept. 5–11.

[25] Connection between Diophantine equations and linear recurrences, Conference in the memory of Kovács–Környei, Mátraháza, 1995. márc. 16–18.

[26] On sums of the reciprocals of prime divisors of terms of a linear recurrence, Seventh Internat. Conf. on Fibonacci Numbers and their Applications, Graz, July 15–19., 1996.

[27] An approximation problem concerning linear recurrences, International Conference on Number Theory, Eger, 1996. jul. 29.–aug. 02.

[28] Perfect powers from products and sums of the terms of linear recurrences, Number Theory Conference, Eger, 2000. nov. 8.

[29] Results concerning products and sums of the terms of linear recurrences, Colloquium on Number Theory in honor of the 60th birthday of Professors Kálmán Győry and András Sárközy, Institute of Mathematics and Informatics, Debrecen, 2000, July 03–07.

[30] On a simultaneous approximation problem concerning binary recurrences, Ninth International Conference on Fibonacci Numbers and Their Applications, Luxembourg, 2000, July 17–22.

Kálmán Liptai
Department of Applied Mathematics
Károly Eszterházy College
H-3301, Eger, P.O. Box 43.
Hungary
e-mail: liptaik@ektf.hu

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

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 23–30*

ON SOME SPECIAL FINSLER METRICS IN PSYCHOMETRY

Sándor Bácsó, Erika Gyöngyösi, Ildikó Papp (Debrecen, Hungary)
Brigitta Szilágyi (Budapest, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. An expansive use of Finsler metrics can be observed in physics, biology, geology, financial mathematics. It is a great improvement for us dealing with Finsler geometry to know that Finsler metrics can be applied even in psychology. The aim of this present paper is to show some Finsler metrics being important even in applications such as Hilbert metric. These classical Finsler metrics have been formulated since the beginning of 1900 and they are even projects of current research, too. Since the book entitled "An Introduction to Riemann–Finsler Geometry" (Springer-Verlag, 2000) written by D. Bao, S. S. Chern and Z. Shen was published, the previous names of concepts of Finsler geometry and Finsler metric were replaced by Riemann–Finsler geometry and Riemann–Finsler metric.

1. Introduction

First of all let us give the concept of Riemann-Finsler metric.

Definition 1. Let an n-dimensional differentiable manifold M be given with a tangent space T_xM in the point (x^i) $(i = 1, 2, \ldots, n)$ of M. Let us denote the coordinates of vectors of T_xM by (y^i). The function $L(x, y)$: $TM(= \bigcup_x T_xM) \to \mathbf{R}$ is Riemann–Finsler metric, if the following properties hold:

(1) **Regularity**: $L(x, y)$ is a function C^∞ on the manifold $TM\backslash O$ of nonzero tangent vectors.

(2) **Positive homogeneity**: $L(x, \lambda y) = \lambda L(x, y)$ for all $\lambda > 0$.

(3) **Strong convexity**: the $n \times n$ matrix $g_{ij}(x, y) = \frac{\partial^2 L^2}{\partial y^i \partial y^j}(x, y)$ is positive definit at every $y \neq 0$.

Remark. In some situations, the Riemann–Finsler metric $L(x, y)$ satisfies the criterion $L(x, y) = L(x, -y)$. In general, we consider this property to be too restrictive. In Example 1 we present an original Finsler metric, which has not this symmetric property.

This definition mentioned above can be found in the doctoral dissertation of Paul Finsler "Über Kurven und Flächen in allgemeinen Räumen", 1918, Göttingen.

Essentially the same definition was given by Riemann in his famous habilitation dissertation "Über die Hypothesen, welche der Geometrie zugrund liegen", 1854.

Since this definition was considered to be too general in determining the tensor of curvature, Riemann chose a well-known special case

$$L^2(x, y) = g_{ij}(x)y^i y^j,$$

and he stated *"we will now stick to the case ellipsoids (quadratic forms), because if not, the computation would become very complicated"*.

An American–Chinese professor Shiing-Shen Chern who is one of the living geometers with the most significant scientific achievements in differential geometry denies Riemann's statement. He wrote in his latest two papers where he pointed out:

"In fact, the general case is just as simple and a main point went unnoticed by Riemann and his successors" [1].

"I believe a major part of differential geometry in the 21th century should be Riemann–Finsler geometry" [2].

2. Randers metrics

It is not difficult to construct an non-trivial (i.e. non-Riemannian) Riemann-Finsler metric. G. Randers studied the following metric in 1941:

$$L(x, y) = \alpha(x, y) + \beta(x, y)$$

where $\alpha^2(a, y) = a_{ij}(x)y^i y^j$ is a Riemann metric, $\beta(x, y) = b_i(x)y^i$ is an 1-form [3].

We can illustrate this metric in two-dimensional case in the following way:

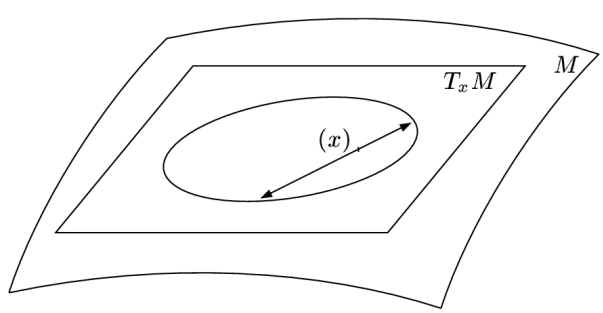


Figure 1

In the tangent space T_xM the indicatrix is an ellipse whose focus is the origin. So we get an original Riemann–Finsler metric, where

$$L(x, y) \neq L(x, -y).$$

We can consider the generalization of a Randers metric as Funk metric from which the Hilbert metric can be derived.

3. Funk distance function

Let $\mathbf{E}^n$ be an n-dimensional Euclidean space, and D be a strictly convex domain in $\mathbf{E}^n$, and in $\mathbf{E}^n$ let ∂D denote the border of D.

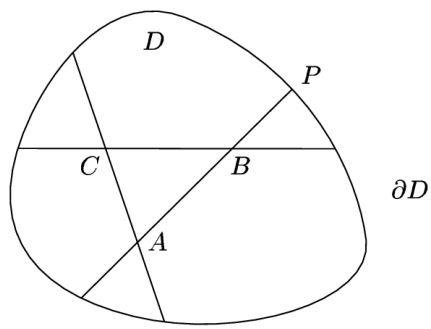


Figure 2

Consider two arbitrary points A and B of D and let the line $|AB|$ meet ∂D in a point P and let the order of the points be A, B, P.

Definition 2. ([4]) Given a positive constant k the **Funk distance function** $f(A, B)$ can be defined as follows:

$$f(A, B) = \frac{1}{k} \log(AP/BP)$$

where AP and BP denote Euclidean distances.

From this definition it follows that the Funk distance function has the properties:

(1) $f(A, B) \geq 0$ for every two points A and B of D;
(2) $f(A, B) = 0$ if and only if $A = B$;
(3) $f(A, B)+f(B, C) \geq f(A, C)$ holds for every three points A, B, C of D. Equality holds if and only if B is on the line $|AC|$;
(4) Generally $f(A, B) \neq f(B, A)$, but $f(A, A_n) \to 0$ if and only if $f(A_n, A) \to 0$.

4. Hilbert distance function

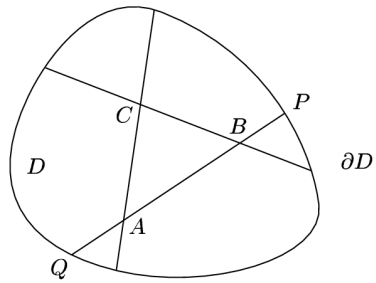


Figure 3

Definition 3. ([5]) The Hilbert distance function is obtained by the symmetrisation of the Funk distance function:

$$h(A,B) = \frac{1}{2}\{f(A,B) + f(B,A)\} = \frac{1}{2k}\log(AP/BP \times BQ/AQ).$$

Here the line $|AB|$ meets the border of D in the points P and Q and the order of the points is Q, A, B, P.

The Hilbert distance function has the following properties:

(1) $h(A,B) \geq 0$ for every two points A and B of D;

(2) $h(A,B) = 0$ if and only if $A = B$;

(3) $h(A,B)+h(B,C) \geq h(A,C)$ holds for every three points A, B, C of the domain D. Equality holds if and only if the point B is on the line $|AC|$ provided if D is strictly convex;

(4) $h(A,B) = h(B,A)$.

5. Funk and Hilbert metrics

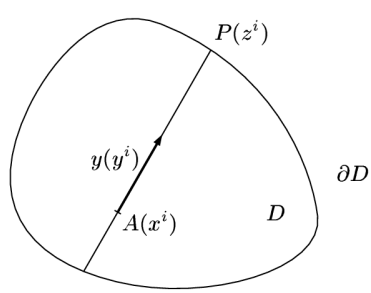


Figure 4

Let (x^i) be the coordinates of the point A, (y^i) be the coordinates of the vector $y \neq 0$. Let us define the function $r(x^i, y^i)$ by the following equality

$$r(x, y) = AP/\|y\|,$$

where AP is an Euclidean distance, $\|y\|$ is the Euclidean norm of the vector y.

The function $r(x, y)$ has the following properties:

(1) $r(x, y) > 0$ for every pair (x, y);
(2) $r(x, y)$ is of degree (-1) positively homogeneous in y;
(3) If $\partial D = \{z^i : \phi(z^i) = 0\}$ then $\phi(x^i + ry^i) = 0$. Namely, if we denote the coordinates of P by (z^i) then $z^i = x^i + r(x, y)y^i$;
(4) $r(x, y) \in C^\infty$.

Definition 4. [6] $L_f = \frac{1}{kr(x,y)}$ and $L_h = \frac{1}{2k[r(x,y)+r(x,-y)]}$ are Funk metric and Hilbert metric respectively.

Theorem 5. 1. *[7] The Funk metric and the Hilbert metric are original Riemann-Finsler metrics.*

Theorem 5. 2. *[8] The Funk space (D, L_f) and Hilbert space (D, L_h) have constant curvatures with the values $(-k^2/4)$ and $(-k^2)$ respectively.*

An interesting special case follows:

Let the border ∂D of the strictly convex domain D be given by a curve of second order, which is non-degenerated as follows:

$$\partial D : \varphi(z^i) = 0,$$

where

$$\varphi(z^i) = b_{ij}z^i z^j + c_i z^i + d, b_{ij} = b_{ji}.$$

then $L_f = \frac{1}{k}[(a_{ij}(x)y^i y^j)^{d\frac{1}{2}} + b_i(x)y^i]$ and $L_h = \frac{1}{2}[a_{ij}(x)y^i y^j]^{d\frac{1}{2}}$.

So in this case (D, L_f) is a Randers space with a negative constant curvature $(-k^2/4)$, and (D, L_h) is a Riemannian space with a negative constant curvature $(-k^2)$. If D is a unit circle then (D, L_h) gives the well-known Klein model of the hyperbolic space.

6. Some application in physics, in biology and in psychology

Let $\mathbf{R}^n = (M, \alpha)$ be an n-dimensional Riemannian space with a Riemannian metric α, $\alpha^2 = a_{ij}(x)y^i y^j$, and with a differential one-form $\beta = b_i(x)y^i$ on M.

Definition 5. An (α, β)-metric is a Finsler metric $L(\alpha, \beta)$ on M which is a positively homogeneous function of degree one the arguments (α, β).

The Randers metric $L = \alpha + \beta$ and the Kropina metric $L = \alpha^2/\beta$ have played a central role in the theory of (α, β)-metrics, and have been the bases of various branches of theoretical physics [9].

In biology there are a lot of Finsler metrics which are suitable to describe biological models and now we intend to show only one of them which arises in coral reef ecology:

If we consider the following local coordinate system in two-dimensional case $\underline{x} = (x^1, x^2) = (x, y)$ and $\underline{u} = (y^1, y^2) = (h, v)$, then this metric has the following form

$$L(x, y, h, v) = e^{\phi(x,y)} N(h, v),$$

where N is a special Minkowski metric (the main scalar is constant, which is a very restrictive condition for the metric) [10].

This metric is very similar to the metric, which is used in psychometry when a psychometric function has radial symmetry. Then the applicable Finsler metric is of the following form:

$$(\star)\ F(\underline{x}, \underline{u}) = \xi(\underline{x})|\underline{u}|,$$

where $\xi(\underline{x}) > 0$ and $|\underline{u}|$ denotes the Minkowski norm [11], [12].

This type of Finsler metrics are called conform Minkowski, or conform flat metrics. Properties of this type of metrics are being worked out presently. Consider the following Finsler metrics with the property $(\star)$ which are defined as in the paper mentioned above:

(1) $F(\underline{x}, \underline{u}) = e^{ax+by} \sqrt[4]{h^4 + v^4 + h^2v^2}$

(2) $F(\underline{x}, \underline{u}) = e^{cxy} \sqrt[4]{h^4 + v^4 + h^2v^2}$

(3) $F(\underline{x}, \underline{u}) = e^{ax+by} \sqrt[4]{(h^2 + v^2 + hv)(h^2 + v^2)}$

(4) $F(\underline{x}, \underline{u}) = e^{cxy} \sqrt[4]{(h^2 + v^2 + hv)(h^2 + v^2)}$, where $a, b, c \in \mathbf{R}$ are constants.

The Gaussian curvature of the first of these two dimensional Finsler metrics is as follows [13]

$$-72\sqrt{u^4 + v^4 + u^2v^2}(4b^2u^{14} - 4abvu^{13} - 40u^{12}b^2v^2 + u^{12}a^2v^2 + 34av^3u^{11}$$

$$-83u^{10}b^2v^4 - 7u^{10}a^2v^4 + 146av^5bu^9 - 50u^8a^2v^6 - 95u^8b^2v^6 + 188av^7bu^7$$

$$-50u^6b^2v38 - 95u^6a^2v^8 + 146av^9bu^5 - 7u^4b^2v^{10} - 83u^4a^2v^{10} + 34av^{11}bu^3$$

$$+u^2b^2v^{12} - 40u^2a^2v^{12} - 4av^{13}bu + 4a^2v^{14})e^{(-2\alpha x - 2by)}/(2u^4 + 11u^2v^2 + 2v^4)^4.$$

The Gaussian curvature of the others is much more complicated.

It would be interesting studied under what conditions a Randers metric applied in so many fields could be applied in psychometry as Finsler metric. One can even examine under what conditions a Randers metric is conform flat (conform Minkowski). This means a rather complicated examination. A necessary

and sufficient condition is known for a Randers metric to be conform Minkowski. Meanwhile this result is too complicated in respect of applications.

Determining the differential equations of the geodetics of the metrics mentioned above could provide an important problem ($n = 2$).

It may be interesting to examine under what conditions a Finsler metric applied in pscyhometry is of Douglas type. That is, it occurs if and only if the differential equations of the geodetics ($y = y(x)$) in two dimension is as follows:

$$y'' = \frac{d^2y}{dx^2} = a(x,y)(y')^3 + b(x,y)(y')^2 + c(x,y)y' + d(x,y),$$

that is the differential equation of the geodetics is a polynom of degree three in $y' = \frac{dy}{dx}$ [14], [15], [16].

This result may be of importance because the psychometric metric can be measured along the geodesics.

Remark 2. Certainly Randers metric can only be applied in psychometry if nonsymmetrical metrics are also allowed in studies of some psychometric problems. We can find a refrence to this possibility in the paper [11]. We hope that in the near future we can characterize the metric functions which is useful in psychometry and which we described in the present paper.

References

[1] Shiing-Shen Chern, Finsler Geometry is Just Riemann Geometry Without Quadratic Restrictions, *Notices of AMS*, **46** (1996), 959–962.

[2] Shiing-Shen Chern, Back to Riemann, *Mathematics: Frontiers and Perspectives*, (2000), 33–34.

[3] Randers, G., On an assymetric metric in the four-space of general relativity, *Phys. Rev.*, (2) **59** (1941), 195–199.

[4] Funk, P., Über Geometrien, bei denen die Geraden die Kürzesten sind, *Math. Ann.*, **101** (1929), 226–237.

[5] Hilbert, D., Über die gerade Linie als kürzeste Verbindung zweier Punkte, *Math. Ann.*, **46** (1901), 91–96.

[6] Okada, T., On models of projectively flat Finsler spaces of constant negative curvature, *Tensor N. S.*, **40** (1983), 117–124.

[7] Busemann, H., *The geometry of geodesics*, Academic Press, New York, 1955.

[8] Shen, Z., *Differential Geometry of Spray and Finsler Spaces,* Kluwer Academic Publishers, 2001.

[9] Asanov, G. S., *Finsler geometry, relativity and gauge therioes*, D. Reidel Publ. Comp., Dordrecht, 1985.

[10] Antonelli, P. L., Ingarden, R. and Matsumoto, M., *The theory of sprays and Finsler spaces with application in physics and biology*, Kluwer Academic Publishers, 1993.

[11] Dzhafarov, E. N. and Colonius, H., Fechnerian metrics in unidimensional and multidimensional stimulus spaces, *Psychonomic Bulletin and Review*, **6(2)** (1999), 239–268.

[12] Dzhafarov, E. N. and Colonius, H., Multidimensional Fechnerian Scaling: Basics, *Journal of Mathematical Psychology*, **45** (2001), 670–719.

[13] Kozma, L. Verbal communications.

[14] Bácsó, S. and Matsumoto, M., On Finsler spaces of Douglas type, I, II, IV, *Publ. Math. Debrecen*, **51** (1997), 385–406, **53** (1998), 423–438, **56** (2000), 213–221.

[15] Bácsó, S. and Matsumoto, M., On Finsler spaces of Douglas type, III, *Kluwer Academic Publishers,* (2000), 89–94.

[16] Arnold, V. I., *Geometrical Methods in the Theory of Ordinary Differential Equations,* Springer-Verlag, 1983.

Sándor Bácsó, Erika Gyöngyösi, Ildikó Papp
Institute of Informatics
University of Debrecen
H-4010 Debrecen, P.O. Box. 12
Hungary
e-mail: bacsos@math.klte.hu
gyerika@hotmail.com
pappi@math.klte.hu

Brigitta Szilágyi
Budapest University of Technology and Economics
H-1111 Budapest, Műegyetem rkp. 3–9.
Hungary

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 31–36*

A NOTE ON NON-NEGATIVE INFORMATION FUNCTIONS

Béla Brindza and Gyula Maksa (Debrecen, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. The purpose of the present paper is to make a first step to prove the conjecture, namely, that not every non-negative information function coincides with the Shannon's one on the algebraic elements of the closed unit interval.

1. Introduction

The characterization of the Shannon entropy, based upon its recursive and symmetric properties is strongly connected with the so-called fundamental equation of information, which is

$$f(x)+(1-x)f\left(\frac{y}{1-x}\right)=f(y)+(1-y)f\left(\frac{x}{1-y}\right) \tag{1.1}$$

where $f\colon[0,1]\to\mathbb{R}$ and (1.1) holds for all $x,y\in[0,1[$, $x+y\le 1$.

The solutions of (1.1) satisfying $f(0)=f(1)$ and $f(\frac{1}{2})=1$ are the information functions. The basic monography Aczél and Daróczy [1] contains several results on these functions, like, if f is non-negative and bounded, then $f=S$, where

$$S(x)=-x\log_2 x-(1-x)\log_2(1-x),\qquad x\in[0,1],$$

($0\log_2 0$ is defined by 0). (See also Daróczy–Kátai [2]). A related result is

Theorem 1. (Daróczy–Maksa [3]). *If f is a non-negative information function, then*

$$f(x)\ge S(x),\qquad x\in[0,1] \tag{1.2}$$

moreover, there exists a non-negative information function different from S.

This research has been supported by the Hungarian Research Fund (OTKA) Grant T-030082 and by the Higher Educational Research and Development Fund (FKFP) Grant 0215/2001.

The proof of the second part of this theorem is based upon the existence of a non-identically zero real derivation $d\colon \mathbb{R} \to \mathbb{R}$ which is additive, that is

$$d(x+y) = d(x) + d(y) \qquad (x, y \in \mathbb{R})$$

and satisfies the equation

$$d(xy) = xd(y) + yd(x), \qquad (x, y \in \mathbb{R})$$

and different from 0 at some point. (See for example Kuczma [4]).

A computation shows that the function

$$f(x) = \begin{cases} S(x) + \dfrac{d(x)^2}{x(1-x)} & \text{if } \ x \in \,]\,0,1[\\ 0 & \text{if } \ x \in \{0,1\} \end{cases} \tag{1.3}$$

is a non-negative information function and different from S if d is a real derivation different from 0. (See Daróczy–Maksa [3]).

After this result some other natural questions arose, namely, the characterization of the non-negative information functions and (or at least) their Shannon kernel $\{x \in [0,1]\colon f(x) = S(x)\}$ where f is a fixed non-negative information function. (See Lawrence–Mess–Zorzitto [6], Maksa [7] and Lawrence [5].)

It is known that the real derivations are vanishing over the field of algebraic numbers (se Kuczma [4]), hence

$$f(\alpha) = S(\alpha) \tag{1.4}$$

if f is given by (1.3). It is noted that (1.4) holds for all non-negative information functions f and for all rational $\alpha \in [0,1]$. (See Daróczy–Kátai [2].)

Our conjecture is that there are non-negative information functions that are different from the Shannon's one at some algebraic element of $[0,1]$. In the next section we prove a partial result in this direction.

2. Results

The base of our investigations is the following theorem.

Theorem 2. *A function $f\colon [0,1] \to \mathbb{R}$ is a non-negative information function, if and only if, there exists an additive function $a\colon \mathbb{R} \to \mathbb{R}$ such that $a(1) = 1$,*

$$-xa(\log_2 x) - (1-x)a(\log_2(1-x)) \geq 0 \qquad \textit{if} \quad x \in \,]\,0,1[\,, \tag{2.1}$$

and

$$f(x) = \begin{cases} -xa(\log_2 x) - (1-x)a(\log_2(1-x)) & \text{if } x \in]\,0,1[\\ 0 & \text{if } x \in \{0,1\}. \end{cases} \tag{2.2}$$

Furthermore $f = S$ holds, if and only if, there is a real derivation $d\colon \mathbb{R} \to \mathbb{R}$ such that

$$a(x) = x + 2^x d(2^{-x}) \qquad \text{if} \quad x \in \mathbb{R}. \tag{2.3}$$

Proof. The first part of the theorem is an easy consequence of Theorem 1 of Daróczy–Maksa [3]. To prove the second part, first suppose that the non-negative information function f coincides with S on $[0,1]$. Therefore, by the definition of S and by (2.2), we get that

$$-xa(\log_2 x) - (1-x)a(\log_2(1-x)) = -x\log_2 x - (1-x)\log_2(1-x) \tag{2.4}$$

holds for all $x \in]\,0,1[$ where a is an additive function that exists by the first part of the theorem. Define the function $\varphi\colon]\,0,+\infty[\to \mathbb{R}$ by

$$\varphi(x) = -xa(\log_2 x) + x\log_2 x. \tag{2.5}$$

An easy calculation shows that

$$\varphi(xy) = x\varphi(y) + y\varphi(x) \qquad \text{if} \quad x > 0,\ y > 0 \tag{2.6}$$

and, because of (2.4),

$$\varphi(x) + \varphi(1-x) = 0 \qquad \text{if} \quad 0 < x < 1.$$

This implies that

$$\varphi\left(\frac{x}{x+y}\right) + \varphi\left(\frac{y}{x+y}\right) = 0$$

for all $x > 0$, $y > 0$ whence, applying (2.6), we have that

$$\begin{aligned} 0 &= x\varphi\left(\frac{1}{x+y}\right) + \frac{1}{x+y}\varphi(x) + y\varphi\left(\frac{1}{x+y}\right) + \frac{1}{x+y}\varphi(y) \\ &= (x+y)\varphi\left(\frac{1}{x+y}\right) + \frac{1}{x+y}(\varphi(x) + \varphi(y)) \\ &= \varphi(1) - \frac{1}{x+y}(\varphi(x+y) - \varphi(x) - \varphi(y)). \end{aligned}$$

Since $\varphi(1) = 0$, we dotain that

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{if} \quad x > 0,\ y > 0. \tag{2.7}$$

If $x \in \mathbb{R}$ define the function $d\colon \mathbb{R} \to \mathbb{R}$ by

$$d(x) = \varphi(u) - \varphi(v)$$

where $u > 0$, $v > 0$ and $x = u - v$. Equation (2.7) garantees that the definition of d is correct, d is additive, and moreover, by (2.6) and (2.7), d is a real derivation that is an extension of φ to $\mathbb{R}$. Thus, by (2.5),

$$d(x) = -xa(\log_2 x) + x \log_2 x \qquad \text{if} \quad x > 0$$

whence we obtain (2.3) replecing x by 2^{-x}.

Finally, if d is an arbitrary real derivation then the function a defined by (2.3) is additive, $a(1) = 1$ and the function f given in (2.2) coincides with S on $[0, 1]$.

Since every real derivation vanishes at all algebraic points (see, for example Kuczma [4]), in order to prove our conjecture, by (2.3), we have to construct an additive function a for which $a(1) = 1$, $a(\log_2 \beta) \neq \log_2 \beta$ for some positive algebraic number β and (2.1) holds for all $x \in]\,0, 1[$.

Instead of this we can proof the following weaker result only.

Theorem 3. *Let $\mathbb{Q}(\alpha)$ be a real algebraic extension of $\mathbb{Q}$ of degree $n > 1$. If $\mathbb{Q}[\alpha]$ (the ring of algebraic integers in $\mathbb{Q}(\alpha)$) is a unique factorization domain then there exists an additive $a\colon \mathbb{R} \to \mathbb{R}$ with $a(1) = 1$ satisfying*

$$-xa(\log_2 x) - (1-x)a(\log_2(1-x)) \geq S(x) \qquad \text{if} \quad x \in]\,0, 1[\, \cap \mathbb{Q}[\alpha] \tag{2.8}$$

and

$$a(\log_2 \beta) \neq \log_2 \beta \tag{2.9}$$

for some positive algebraic number β.

Proof. Let U be the unitgroup of $\mathbb{Q}[\alpha]$ generating by a set of fundamental units $\{\varepsilon_1, \ldots, \varepsilon_{n-1}\}$ and $P = \{\pi_1, \ldots, \pi_s, \ldots\}$ be the set of primes in $\mathbb{Q}[\alpha]$. Since the group of the roots of unity is $\{-1, 1\}$, only, we may assume that

$$0 < \varepsilon_i, \quad i = 1, \ldots, n-1; \qquad 0 < \pi_j, \quad j = 1, 2, \ldots .$$

and every non-zero element x of $\mathbb{Q}[\alpha]$ can uniquely be written in the form

$$x = \pm \left(\prod_{i=1}^{n-1} \varepsilon_i^{k_i} \right) \left(\prod_{j=1}^{\infty} \pi_j^{\ell_j} \right) \tag{2.10}$$

where the exponents are (rational) integers and $\ell_j \geq 0$, $j = 1, 2, \ldots$. The set P is multiplicatively independent, hence the set $\{\log_2 \pi : \pi \in P\}$ is linearly independent (over $\mathbb{Q}$). Therefore there is a Hamel basis $\mathcal{H} \subset \mathbb{R}$ for which $1 \in \mathcal{H}$ and $\log_2 \pi \in \mathcal{H}$ if $\pi \in P$.

Let $\pi_1 \in P$ be fixed. We may assume that $\pi_1 \neq 2$. Define the function a_0 on $\mathcal{H}$ by $a_0(\log_2 \pi_1) = \log_2 \frac{\pi_1}{2}$, $a_0(h) = h$ if $h \in \mathcal{H}$, $h \neq \log_2 \pi_1$, and let a be the additive extension of a_0 to $\mathbb{R}$. It is obvious that $a(1) = 1$ and (2.9) is satisfied by $\beta = \pi_1$. To prove (2.8) first suppose that the exponent of π_1 is positive in the decomposition (2.10) of $x \in]\,0, 1[\, \cap \mathbb{Q}[\alpha]$. Then the exponent of π_1 in the decomposition of $(1-x)$ is zero. Of course, the same is true also for $(1-x)$ instead of x. Therefore

$$a(\log_2(1-x)) = \log_2(1-x) \tag{2.11}$$

or

$$a(\log_2 x) = \log_2 x \tag{2.12}$$

holds for all $x \in]\,0, 1[\, \cap \mathbb{Q}[\alpha]$. Supposing (2.11) we have that

$$\begin{aligned}
&- xa(\log_2 x) - (1-x)a(\log_2(1-x)) \\
&= -xa\left(\log_2 \frac{x}{\pi_1^{\ell_1}} + \log_2 \pi_1^{\ell_1}\right) - (1-x)\log_2(1-x) \\
&= -xa\left(\log_2 \frac{x}{\pi_1^{\ell_1}}\right) - xa(\log_2 \pi_1^{\ell_1}) - (1-x)\log_2(1-x) \\
&= -x\log_2 \frac{x}{\pi_1^{\ell_1}} - x\ell_1 a(\log_2 \pi_1) - (1-x)\log_2(1-x) \\
&= -x\log_2 x - (1-x)\log_2(1-x) + x\ell_1\big[\log_2 \pi_1 - a(\log_2 \pi_1)\big] \\
&= -x\log_2 x - (1-x)\log_2(1-x) + x\ell_1\big[\log_2 \pi_1 - \log_2 \frac{\pi_1}{2}\big] \\
&> -x\log_2 x - (1-x)\log_2(1-x) = S(x).
\end{aligned}$$

Thus (2.8) holds. In case (2.12) the proof is similar. Finally, if the exponent of π_1 is zero in the decompositions of both x and $(1-x)$ then, of course, the equality is valid in (2.8).

Remark. According to the classical approximation result of Dirichlet the set $D = \{\, x \in]0, 1[\cap \mathbb{Q}[\alpha] : \ell_1 > 0 \text{ in } (2.10)\}$ is dense in $[0, 1]$. Thus the strict inequality holds on the dense set D in (2.8).

References

[1] Aczél, J. and Daróczy, Z., *On measures of information and their characterizations,* Academic Press, New York, 1975.

[2] Daróczy, Z. and Kátai, I., Additive zahlentheoretische Funktionen und das Mass der Information, *Ann. Univ. Sci. Budapest, Eötvös Sect. Math.*, **13** (1970), 83–88.

[3] Daróczy, Z. and Maksa, Gy., *Nonnegative information functions.* In: Proc. Colloqu. Methods of Complex Anal. in the Theory of Probab. and Statist., Debrecen, 1977, Colloquia Mathematica Societatis János Bolyai Vol. 21, North-Holland, Amsterdam, 1979, 67–68.

[4] Kuczma, M., *An Introduction to the Theory of Functional Equations and Inequalities*, Państwowe Wydawnictwo Naukowe, Warszawa–Kraków–Katowice, 1985.

[5] Lawrence, J., The Shannon kernel of non-negative information function, *Aequationes Math.*, **23** (1981), 233–235.

[6] Lawrence, J., Mess, G. and Zorzitto, F., Near-derivations and information functions, *Proc. Amer. Math. Soc.*, **76** (1979), 117–122.

[7] Maksa, Gy., On near-derivations, *Proc. Amer. Math. Soc.*, **81**, (1981), 406–408.

Béla Brindza
University of Debrecen
Institute of Mathematics
4010 Debrecen P.O. Box 12.
Hungary
e-mail: brindza@math.klte.hu

Gyula Maksa
University of Debrecen
Institute of Mathematics
4010 Debrecen P.O. Box 12.
Hungary
e-mail: maksa@math.klte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 37–43*

ON ACCUMULATION POINTS OF GENERALIZED RATIO SETS OF POSITIVE INTEGERS

József Bukor (Trnava, Slovakia)
János T. Tóth (Ostrava, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. The paper deals with a generalized ratio set of positive integers defined as

$$R_n(A)=\{a_1a_2...a_n/(b_1b_2...b_n);a_1,a_2,...,a_n,b_1,b_2,...,b_n\in A\}, \qquad \text{where } A\subset\mathbf{N}.$$

There are characterized the accumulation points of $R_n(A)$. Further it is proved that if $A\subset\mathbf{N}$ has positive lower asymptotic density then for sufficiently large positive integer n the set $R_n(A)$ is dense in $\mathbf{R}^+$.

AMS Classification Number: 11B05

1. Introduction

Denote by $\mathbf{R}$ ($\mathbf{R}^+$) the set of all real (positive real) numbers and by $\mathbf{N}$ the set of all positive integer numbers, respectively. The *ratio set* of $A \subset \mathbf{N}$ is denoted by $R(A) = \{\frac{a}{b}; a, b \in A\}$ (see [3], [5]). The symbol X^d will stand for the set of all accumulation points of $X \subset \mathbf{R}^+$. It is easy to see that for any infinite subset A of positive integers $\{0, +\infty\} \subset R(A)^d$. The set $R(A)$ is everywhere dense in $\mathbf{R}^+$ if $R(A)^d = [0, +\infty]$.

It is known that if $\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$ for the set $A = \{a_1 < a_2 < \cdots\} \subset \mathbf{N}$ then $R(A)$ is dense in $\mathbf{R}^+$ [5], on the other hand if $\underline{\lim}_{n\to\infty} \frac{a_{n+1}}{a_n} = c > 1$ then $R(A)$ is not dense in $\mathbf{R}^+$, moreover $R(A)^d \cap \left(\frac{1}{c}, c\right) = \emptyset$ [6].

The lower and upper asymptotic density of A, denoted by $\underline{d}(A)$ and $\overline{d}(A)$ respectively, are defined as

$$\underline{d}(A) = \underline{\lim}_{x\to\infty} \frac{A(x)}{x}, \qquad \overline{d}(A) = \overline{\lim}_{x\to\infty} \frac{A(x)}{x},$$

This research was supported by Grant GAAV A 1187, 101.

where $A(x) = \#\{a \le x : a \in A\}$. If $\underline{d}(A) = \overline{d}(A) = d(A)$ then the number $d(A)$ is called the asymptotic density of the set A.

We mention some known results on the topics density of ratio sets. Šalát [5] showed that $\underline{d}(A) = \overline{d}(A) > 0$ or $\overline{d}(A) = 1$ implies that $R(A)$ is everywhere dense in $\mathbf{R}^+$ and for every sufficiently small $\varepsilon > 0$ there exists a subset of $A \subset \mathbf{N}$ such that $\overline{d}(A) = 1 - \varepsilon$ and $R(A)$ is not everywhere dense in $\mathbf{R}^+$. He gave an example of $A \subset \mathbf{N}$ for which $\underline{d}(A) = \frac{1}{4}$ and $R(A)$ is not everywhere dense in $\mathbf{R}^+$. Strauch and Tóth [4] proved that $\frac{1}{2}$ is the lower bound of γ's for which $\underline{d}(A) \ge \gamma$ implies that $R(A)$ is everywhere dense in $\mathbf{R}^+$.

We define the *generalized ratio set*

$$R_n(A) = \{\frac{a_1 a_2 \dots a_n}{b_1 b_2 \dots b_n};\ a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in A\}.$$

Clearly, $R_1(A) = R(A)$ and $R_n(A) \subset R_m(A)$ for $m \ge n$.

In [2] was asked: For which sets $B \subset \mathbf{R}$ does there exist a set $A \subset \mathbf{N}$ such that $R(A)^d = B$? It is evident that $B \ne \emptyset$ provided A is infinite. On the other hand, $\{0, +\infty\} \subset R(A)^d$ for any infinite $A \subset \mathbf{N}$. Further, if some positive $t \in R(A)^d$, then $\frac{1}{t} \in R(A)^d$, since $\frac{a}{b} \in R(A)$ always implies that $\frac{b}{a} \in R(A)$. Notice also, that the accumulation points of any linear set constitute a closed set in $\mathbf{R}$. Consequently, the nonempty set B must be a closed subset of $[0, +\infty] = \mathbf{R}^+ \cup \{0, +\infty\}$, it must contain 0 and $+\infty$, and if $b \in B$ ($b \in \mathbf{R}^+$) then $\frac{1}{b} \in B$. In [1] was proved that these conditions are also sufficient for the existence of an $A \subset \mathbf{N}$ for that $R(A)^d = B$. We show that the same assertion is valid if we consider the generalized ratio set $R_n(A)$ instead of the ratio set $R(A)$.

2. Theorems and proofs

Theorem 1. *Let $\emptyset \ne B \subset [0, +\infty]$ and n be a positive integer. The followings are equivalent:*

(i) There exists an $A \subset \mathbf{N}$ such that $R_n(A)^d = B$;

(ii) $B \cap \mathbf{R}$ is closed in $\mathbf{R}$, $\{0, +\infty\} \subset B$ and $b \in B$ implies $\frac{1}{b} \in B$.

Proof. As the implication (i) $\Rightarrow$ (ii) is trivial it suffices to prove only (ii) $\Rightarrow$ (i). The case $n = 1$ was considered in [1]. Let us suppose that $n > 1$ and suppose $\emptyset \ne B \subset [0, +\infty]$ satisfies (ii). Let $\mathcal{S}$ stand for the system of intervals $(1 + \frac{i-1}{n}, 1 + \frac{i+1}{n})$ where $n \in \mathbf{N}$ and $i = 1, 2, \dots, n^2$. The length of intervals tends to zero with increasing n and every real number greater than 1 can be covered with infinitely many elements of $\mathcal{S}$. Denote by $((c_k - \delta_k, c_k + \delta_k))_{k=1}^{\infty}$ the sequence of those intervals from $\mathcal{S}$ which meet B (i.e. which contain at least one element from B).

Define the set $A = \{a_0 < a_1 < a_2 < \ldots\} \subset \mathbf{N}$ as follows:
Let $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, further

$$a_{3k} = \lfloor (a_{3k-1})^{n^2}.(c_k + 1) \rfloor, a_{3k+1} = (a_{3k})^{n^2}, a_{3k+2} = \left\lceil \frac{c_k.(a_{3k+1})^n}{(a_{3k})^{n-1}} \right\rceil \text{for } k = 1, 2, \ldots$$

We will show that $R_n(A)^d = B$.

(1) $B \subset R_n(A)^d$: Let $t \in B$ be a positive real number. We may suppose that $t > 1$. Let $((c_{m_k} - \delta_{m_k}, c_{m_k} + \delta_{m_k}))_{k=1}^{\infty}$ be a sequence of intervals containing t. Then $\lim\limits_{k\to\infty} c_{m_k} = t$ since $\lim\limits_{k\to\infty} \delta_{m_k} = 0$. Accordingly the sequence

$$(1) \qquad \frac{a_{3m_k+2} \cdot (a_{3m_k})^{n-1}}{(a_{3m_k+1})^n} = \left\lceil \frac{c_{m_k} \cdot (a_{3m_k+1})^n}{(a_{3m_k})^{n-1}} \right\rceil \cdot \frac{(a_{3m_k})^{n-1}}{(a_{3m_k+1})^n} \qquad (k = 1, 2, \ldots)$$

converges to t; thus, $t \in R(A)^d$.

(2) $R_n(A)^d \subset B$: Let us consider the fraction

$$r = \frac{a_{i_1} a_{i_2} \ldots a_{i_m}}{a_{j_1} a_{j_2} \ldots a_{j_m}} \in R_n(A),$$

where $m \leq n$, $a_{i_1}, \ldots, a_{i_m}, a_{j_1}, \ldots, a_{j_m} \in A$ further $a_{i_1} \geq a_{i_2} \geq \cdots \geq a_{i_m}$, $a_{i_1} > a_{j_1} \geq a_{j_2} \geq \cdots \geq a_{j_m}$ and the fraction r cannot be simplified. Our aim is to show that only a sequence like (1) from $R_n(A)$ can have finite limit. To prove this we consider the following possibilities:

(a) $i_1 = 3k$ or $i_1 = 3k + 1$. In this case we have

$$r \geq \frac{a_{i_1}}{(a_{i_1-1})^n} \geq (a_{i_1-1})^{n^2-n}.$$

(b) $m < n$, $i_1 = 3k + 2$, $j_1, \ldots, j_m \leq 3k + 1$ or $m = n$, $j_1, \ldots, j_{n-1} \leq 3k + 1$, $j_n \leq 3k$. Now we have

$$r \geq \frac{a_{3k+2}}{(a_{3k+1})^{n-1} \cdot a_{3k}} = \frac{\left\lceil \frac{c_k \cdot (a_{3k+1})^n}{(a_{3k})^{n-1}} \right\rceil}{(a_{3k+1})^{n-1} \cdot a_{3k}} \geq \frac{a_{3k+1}}{(a_{3k})^n} = (a_{3k})^{n^2-n}.$$

(c) $i_1 = 3k + 2$, $i_2, \ldots, i_{n-1} \leq 3k$, $i_n \leq 3k - 1$, $j_1 = j_2 = \cdots = j_n = 3k + 1$. Then we have the following estimation

$$r \leq \frac{a_{3k+2} \cdot (a_{3k})^{n-2} \cdot a_{3k-1}}{(a_{3k+1})^n} < \frac{(c_k + 1) \cdot (a_{3k+1})^n}{(a_{3k})^{n-1}} \cdot \frac{(a_{3k})^{n-2} \cdot a_{3k-1}}{(a_{3k+1})^n} \cdot \frac{(c_k + 1) \cdot a_{3k-1}}{a_{3k}}$$

$$\leq (a_{3k-1})^{1-n^2}.$$

The last case we have to consider is related to (1)

(d) $i_1 = 3k+2$, $i_2 = \cdots = i_n = 3k$, $j_1 = \cdots = j_n = 3k+1$.

Let now $t \in R(A)^d$ and $t > 1$. Then there exist sequences $(s_{i,l})_{l=1}^{\infty}$ and $(r_{i,l})_{l=1}^{\infty}$, $i = 1, 2, \ldots, n$ of positive integers such that

$$\lim_{l\to\infty} \frac{a_{s_{1,l}} \cdot a_{s_{2,l}} \cdots a_{s_{n,l}}}{a_{r_{1,l}} \cdot a_{r_{2,l}} \cdots a_{r_{n,l}}} = t. \tag{2}$$

Observe that if the fractions in (2) are of the form (a) and (b) then their limit is $+\infty$ and if these fractions are of the form (c) then their limit is 0. So (2) can hold only if for sufficiently large numbers we have the case (d). Therefore for some subsequence $(m_k)_{k=1}^{\infty}$ of positive integers we have

$$\lim_{k\to+\infty} c_{m_k} = t.$$

Taking into account that every interval $(c_{m_k} - \delta_{m_k}, c_{m_k} + \delta_{m_k})$ contains some $t_k \in B$, therefore $\lim\limits_{k\to\infty} t_k = t$. Finally, the closedness of $B \cap \mathbf{R}$ in $\mathbf{R}$ ensures that $t \in B$.

Remark. As a consequence of the theorem we immediately have that for each $n \geq 1$ there exists a set $A \subset \mathbf{N}$ such that $R_n(A)$ is not dense in $\mathbf{R}^+$, but R_{n+1} is already dense in $\mathbf{R}^+$. Indeed, there is a set A such that the set of all accumulation points of $R_n(A)$ is equal to $B = \{n, \frac{1}{n}; n = 1, 2, \ldots\}$. Obviously, then $R_{n+1}(A)$ is dense in $\mathbf{R}^+$.

Strauch and Tóth [4] have proved that for any $A \subset \mathbf{N}$ and the interval (α, β), $0 \leq \alpha < \beta \leq 1$ if $(\alpha, \beta) \cap R(A) = \emptyset$ then $\overline{d}(A) \leq 1 - (\beta - \alpha)$. The following lemma generalizes this result and it is basic for the proof of the theorem below.

Lemma. *Let $A \subset \mathbf{N}$ and the pairwise disjoint intervals (α_i, β_i), $0 \leq \alpha_i < \beta_i \leq 1$ are such that $(\alpha_i, \beta_i) \cap R(A) = \emptyset$, $i = 1, 2, \ldots, m$. Then*

$$\overline{d}(A) \leq 1 - \sum_{i=1}^{m} (\beta_i - \alpha_i)$$

Proof. In the cases $\overline{d}(A) = 0$ or $\overline{d}(A) = 1$ the assertion is trivial (it was proved by Šalát [5] that $\overline{d}(A) = 1$ implies that $R(A)$ is everywhere dense in $\mathbf{R}^+$), so we can suppose that the set A is infinite and A has infinite complement in $\mathbf{N}$. Thus A can be expressed as the set of integer points lying in the intervals

$$[b_1, c_1],\ [b_2, c_2], \ldots, [b_n, c_n], \ldots,$$

whose endpoints are ordered as

$$b_1 \le c_1 < b_2 \le c_2 < \cdots < b_n \le c_n < \cdots$$

Obviously,

$$\overline{d}(A) = \overline{\lim}_{n\to+\infty} \frac{1}{c_n} \sum_{i=1}^{n} (c_i - b_i + 1).$$

Let us consider the fractions $\frac{a}{c_n}$, where $a \in A$, $a \le c_n$. All these fractions are contained in the union of the intervals

$$\left[\frac{b_1}{c_n}, \frac{c_1}{c_n}\right], \left[\frac{b_2}{c_n}, \frac{c_2}{c_n}\right], \cdots, \left[\frac{b_n}{c_n}, \frac{c_n}{c_n}\right]. \tag{3}$$

The distance of any two neighbouring fractions lying in the same interval of (3) is $\frac{1}{b_n} \to 0$ as $n \to +\infty$. Therefore, for sufficiently large n, each interval $(\alpha_i, \beta_i) \subset [0,1]$, $i = 1, 2, \ldots, m$ must lie in the complement of

$$\left[\frac{b_k}{c_n}, \frac{c_k}{c_n}\right], \quad k = 1, 2, \ldots, n.$$

This complement is formed by the pairwise disjoint intervals

$$\left(\frac{c_k}{c_n}, \frac{b_{k+1}}{c_n}\right), \quad k = 1, 2, \ldots, n-1.$$

Hence

$$\cup_{i=1}^{m} (\alpha_i, \beta_i) \subset \cup_{k=1}^{n} \left(\frac{c_k}{c_n}, \frac{b_{k+1}}{c_n}\right)$$

and therefore

$$\sum_{i=1}^{m} (\beta_i - \alpha_i) \le \sum_{k=1}^{n} \frac{b_{k+1} - c_k}{c_n}.$$

The upper asymptotic density of the set A we can write as

$$\overline{d}(A) = \overline{\lim}_{n\to+\infty} \left(\frac{c_n - b_1}{c_n} + \frac{n}{c_n} - \frac{1}{c_n} \left[(b_2 - c_1) + (b_3 - c_2) + \cdots + (b_n - c_{n-1}) \right] \right)$$

whence

$$\overline{d}(A) - \overline{d}(C) \le 1 - \sum_{i=1}^{m} (\beta_i - \alpha_i),$$

where C is the range of c_n. Now, for a positive integer t, transform $[b_n, c_n] \to [tb_n, tc_n + t - 1]$ and denote by A_t the set of all integer points lying in $[tb_n, tc_n + t - 1]$,

$n = 1, 2, \ldots$. Analogously, C_t is the set of all $tc_n + t - 1$. Then we have $\overline{d}(A_t) = \overline{d}(A)$ and $\overline{d}(C_t) = \overline{d}(C)/t$, which gives

$$\overline{d}(A) - \frac{\overline{d}(C)}{t} \leq 1 - \sum_{i=1}^{m} (\beta_i - \alpha_i)$$

and the assertion of the lemma follows.

Theorem 2. *For arbitrary $A = \{a_1 < a_2 < \cdots\} \subset \mathbf{N}$ having positive lower asymptotic density ($\underline{d}(A) > 0$) there exists a positive integer n such that the set $R_n(A)$ is dense in $\mathbf{R}^+$.*

Proof. First, we claim that $\underline{d}(A) > 0$ implies that for some interval $[\gamma, \delta]$, $1 \leq \gamma < \delta$ the set $R(A)$ is dense in $[\gamma, \delta]$. Indeed, if such interval $\gamma, \delta]$ does not exist, then there exist pairwise disjoint intervals (α_i, β_i), $0 \leq \alpha_i < \beta_i \leq 1$ such that $(\alpha_i, \beta_i) \cap R(A) = \emptyset$, $i = 1, 2, \ldots, m$ and the sum of the length of these intervals can be arbitrary near to 1, i.e.

$$\sum_{i=1}^{m} (\beta_i - \alpha_i) > 1 - \underline{d}(A)$$

which is a contradiction with the lemma.

From the condition $\underline{d}(A) > 0$ follows that for sufficiently large K we have

$$\frac{a_{k+1}}{a_k} < K, \quad k = 1, 2, \ldots$$

If $R(A)$ is dense in $[\gamma, \delta]$, $(1 \leq \gamma < \delta)$ then $R_2(A)$ is dense in $[1, \frac{\delta}{\gamma}]$ and $R_4(A)$ is dense in $[1, (\frac{\delta}{\gamma})^2], \ldots$. To see this, we remark that

$$R_{2^{n+1}}(A) = R(R_{2^n}(A)), \quad n = 1, 2, \ldots$$

Evidently $(\frac{\delta}{\gamma})^n \to +\infty$ for $n \to +\infty$, therefore for sufficiently large n we have that $R_{n-1}(A)$ is dense in $[1, K]$. Using this fact we have that the set

$$\left\{ t \cdot \frac{a_k}{a_1};\ t \in R_{n-1}(A) \right\} \subset R_n(A)$$

is dense in each $[\frac{a_k}{a_1}, \frac{a_{k+1}}{a_1}]$, $k = 1, 2, \ldots$, hence $R_n(A)$ is dense in $\mathbf{R}^+$.

To conclude this paper, let us describe some open problems associated with this topic.

Let $\gamma(n)$ be the least value of γ for which $\underline{d}(A) \geq \gamma$ implies that $R_n(A)$ is dense in $\mathbf{R}^+$, $n = 1, 2, \ldots$. It is known that $\gamma(1) = 1/2$. Determine the exact value of $\gamma(2)$. What can be said about the function $\gamma(n)$?

References

[1] Bukor, J. and Tóth, T. J., On accumulation points of ratio sets of positive integers *Amer. Math. Monthly*, **103** (1996), 502–504.

[2] Hobby, D., and Silberger, D. M., Quotients of primes, *Amer. Math. Monthly*, **100**, (1993), 50–52.

[3] Narkiewicz, W. and Šalát, T., A theorem of H. Steinhaus and (R)-dense sets of positive integers, *Czechoslovak Math. Journal*, **34** (109) (1984), 355–361.

[4] Strauch, O. and Tóth, T. J., Asymptotic density of $A \subset \mathbf{N}$ and the density of the ratio set $R(A)$, *Acta Arith.* **LXXXVII.1** (1998), 67–77.

[5] Šalát, T., On ratio sets of natural numbers, *Acta Arith.*, **15** (1969) 273–278. Corrigendum: *Acta Arith.* **16** (1969).

[6] Tóth, T. J. and Zsilinszky, L., On density of ratio sets of powers of primes, *Nieuw Archive voor Wiskunde*, **13** (1995), 205–208.

József Bukor
Slovak University of Technology
Faculty of Material Science and Technology
Department of Mathematics
Paulinska 16, 91724 Trnava
Slovakia
e-mail: bukor@selye.sk

János T. Tóth
University of Ostrava
Department of Mathematics
30 dubna 22, 70103 Ostrava
Czech Republic
e-mail: toth@osu.cz

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 45–54*

RECENT RESULTS ON POWER INTEGRAL BASES OF COMPOSITE FIELDS

István Gaál and Péter Olajos (Debrecen, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. We consider the problem of existence of power integral bases in orders of composite fields. Completing our former results we show that under certain congruence conditions on the defining polynomial of the generating elements of the fields, the composite of the polynomial orders does not admit power integral basis. As applications we provide several examples involving also infinite parametric families of fields.

AMS Classification Number: 11D57, 11Y50

Keywords and phrases: power integral basis, composite field, index form equations.

1. Introduction

Let K be an algebraic number field of degree n with ring of integers $\mathbb{Z}_K$. It is a classical problem in algebraic number theory to decide if there is an element α in K such that

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

is an integral basis. Such an integral basis is called *power integral basis*. A further problem is to find all elements which generate power integral bases.

The index of a primitive algebraic integer α of K is defined as the module-index

$$I(\alpha) = (\mathbb{Z}_K^+ : \mathbb{Z}^+[\alpha]).$$

Obviously α generates a power integral basis if and only if $I(\alpha) = 1$.

Note that

$$I(\alpha) = \frac{\left|\prod_{1 \le j < k \le n} (\alpha^{(j)} - \alpha^{(k)})\right|}{\sqrt{|D_K|}} \tag{1}$$

Research of the first author is supported by Grants T-037367 and T-042985, of the second author by Grant T-037367 from the Hungarian National Foundation for Scientific Research.

where $\alpha^{(i)}$ $(i = 1, \ldots, n)$ are the conjugates of α and D_K is the discriminant of K.

Let $\{1, \omega_2, \ldots, \omega_n\}$ be an integral basis of K. Then the discriminant of the linear form $l(X) = X_1 + \omega_2 X_2 + \cdots + \omega_n X_n$ can be written as

$$D_{K/\mathbb{Q}}(l(X)) = I(x_2, \ldots, x_n)^2 \cdot D_K,$$

where $I(x_2, \ldots, x_n)$ is the *index form* corresponding to the integral basis $\{1, \omega_2, \ldots, \omega_n\}$ (see I. Gaál [4]).

For any

$$\alpha = x_1 + \omega_2 x_2 + \cdots + \omega_n x_n \in \mathbb{Z}_K$$

we have

$$I(\alpha) = |I(x_2, \ldots, x_n)|.$$

Hence if we want to determine all generators of power integral bases, we have to solve the *index form equation*

$$I(x_2, \ldots, x_n) = \pm 1 \quad (x_2, \ldots, x_n \in \mathbb{Z}). \tag{2}$$

Using Baker's method the first effective upper bounds for the solutions of (2) were given by K. Győry [10]. This upper bound implies that (2) has only finitely many solutions.

There are efficient algorithms for determining all generators of power integral bases in lower degree number fields cf. I. Gaál and N. Schulte [9] for cubic, I. Gaál, A. Pethő and M. Pohst [7] for quartic fields. A general algorithm for quintic fields was given by I. Gaál and K. Győry [5], which already requires several hours of CPU time. For algorithms for solving index form equations in certain special sextic, octic, nonic fields see I. Gaál [1], [3], I.Gaál and M. Pohst [8], I. Járási [11]. For a more complete overview on the topic see the monograph [4].

For higher degree number fields this problem is very complicated because of the high degree and the large number of variables of equation (1). The resolution of this equation is only hopeful if K has proper subfields, because in this case the index form is reducible.

Higher degree fields having subfields are very often given as composites of certain subfields. This is the case that we investigated in [2] and [6]. The purpose of this paper is to add some recent results to this area. In order to make it easier for the reader to compare our (old and new) results, we first summarize our former results, then we detail the new results that can be used in some important cases not covered by our former statements.

2. Coprime discriminants

In [2] we considered the problem of existence of power integral bases in case K is the composite of two subfields L and M with coprime discriminants. Let L be of degree r with integral basis $\{l_1 = 1, l_2, \dots, l_r\}$ and discriminant D_L. Denote the index form corresponding to the integral basis $\{l_1 = 1, l_2, \dots, l_r\}$ of L by $I_L(x_2, \dots, x_r)$. Similarly, let M be of degree s with integral basis $\{m_1 = 1, m_2, \dots, m_s\}$ and discriminant D_M. Denote the index form corresponding to the integral basis $\{m_1 = 1, m_2, \dots, m_s\}$ of M by $I_M(x_2, \dots, x_s)$. Assume, that the discriminants are coprime, that is $\gcd(D_L, D_M) = 1$.

Set $K = L \cdot M$ the composite of L and M. As it is known (cf. W. Narkiewicz [12]) the discriminant of K is $D_K = D_L^s \cdot D_M^r$ and an integral basis of K is given by $\{l_i \cdot m_j : 1 \le i \le r,\ 1 \le j \le s\}$. Hence, any integer α of K can be represented in the form

$$\alpha = \sum_{i=1}^{r} \sum_{j=1}^{s} x_{ij} \cdot l_i \cdot m_j \tag{3}$$

with $x_{ij} \in \mathbb{Z}$ $(1 \le i \le r,\ 1 \le j \le s)$.

I. Gaál [2] formulated a general necessary condition for $\alpha \in \mathbb{Z}_K$ to be a generator of a power integral basis of K.

Theorem 1. (I. Gaál, [2]) *Assume* $\gcd(D_L, D_M) = 1$. *If* α *of (3) generates a power integral basis in* $K = L \cdot M$ *then*

$$N_{M/Q}\left(I_L\left(\sum_{i=1}^{s} x_{2i} \cdot m_i, \dots, \sum_{i=1}^{s} x_{ri} \cdot m_i\right)\right) = \pm 1 \tag{4}$$

and

$$N_{L/Q}\left(I_M\left(\sum_{i=1}^{r} x_{i2} \cdot l_i, \dots, \sum_{i=1}^{r} x_{is} \cdot l_i\right)\right) = \pm 1. \tag{5}$$

This statement was applied e.g. for nonic fields [3].

3. Non-coprime discriminants

A sufficient condition for the non-existence of power integral bases in K was formulated by I. Gaál, P. Olajos and M. Pohst [6] in the case when D_L and D_M are usually not coprime.

Let $f, g \in \mathbb{Z}[x]$ be distinct monic irreducible polynomials (over $\mathbb{Q}$) of degrees m and n, respectively. Let φ be a root of f and let ψ be a root of g. Set $L = \mathbb{Q}(\varphi)$, $M = \mathbb{Q}(\psi)$ and assume that the composite field $K = LM$ has degree mn. We also assume that there is a prime number q, $(q \geq 2)$ such that both f and g have a multiple linear factor (at least square) modulo q, that is, there exist a_f and a_g in $\mathbb{Z}$ such that

$$\begin{cases} f(a_f) \equiv f'(a_f) \equiv 0 & (\text{mod } q), \\ g(a_g) \equiv g'(a_g) \equiv 0 & (\text{mod } q). \end{cases} \tag{6}$$

Note that our assumption implies that q divides both the discriminant $d(f)$ of the polynomial f and the discriminant $d(g)$ of g. In our case the fields we consider are composites of subfields whose discriminants are usually not coprime. This is the case in many interesting examples.

Consider the order $\mathcal{O}_f = \mathbb{Z}[\varphi]$ of the field L, the order $\mathcal{O}_g = \mathbb{Z}[\psi]$ of the field M and the composite order $\mathcal{O}_{fg} = \mathcal{O}_f\mathcal{O}_g = \mathbb{Z}[\varphi, \psi]$ in the composite field $K = ML$. Note that $\{1, \varphi, \ldots, \varphi^{m-1}\}$, $\{1, \psi, \ldots, \psi^{n-1}\}$ and $\{1, \varphi, \ldots, \varphi^{m-1}, \psi, \varphi\psi, \ldots, \varphi^{m-1}\psi, \ldots, \psi^{n-1}, \varphi\psi^{n-1}, \ldots, \varphi^{m-1}\psi^{n-1}\}$ are $\mathbb{Z}$ bases of $\mathcal{O}_f$, $\mathcal{O}_g$ and $\mathcal{O}_{fg}$, respectively.

Theorem 2. (I. Gaál, P. Olajos, M. Pohst [6]) *Under the above assumptions the index of any primitive element of the order $\mathcal{O}_{fg}$ is divisible by q.*

As a consequence we have:

Theorem 3. (I. Gaál, P. Olajos, M. Pohst [6]) *Under the above assumptions the order $\mathcal{O}_{fg}$ has no power integral basis.*

In [6] we applied the above theorem to the parametric family of simplest sextic fields.

4. New results on composite fields

We are going to formulate a further sufficient condition for the non-existence of power integral bases in composite fields.

Let $f, g \in \mathbb{Z}[x]$ be monic, irreducible polynomials of degrees $m, n \in \mathbb{Z}$, respectively. Let α be a root of f, and let β be a root of g. Denote the discriminants of these polynomials by $d(f), d(g)$. The conjugates of α and β will be denoted by α_k $(k = 1, \ldots, m)$ and β_l $(l = 1, \ldots, n)$, respectively. Further, let $L = \mathbb{Q}(\alpha)$, $\mathcal{O}_{\mathcal{L}} = \mathbb{Z}[\alpha]$ with discriminant $D_{\mathcal{O}_{\mathcal{L}}} = d(f)$ and $M = \mathbb{Q}(\beta)$, $\mathcal{O}_{\mathcal{M}} = \mathbb{Z}\S^{\Updownarrow}[\beta]$ with discriminant $D_{\mathcal{O}_{\mathcal{M}}} = d(g)$. We assume that there are square-free numbers $p, q \in \mathbb{Z}$ $(p, q \geq 2)$ such that

$$(A) \qquad f(x) \equiv x^m \pmod{p},$$

or

$$(B) \qquad g(x) \equiv x^n \pmod{q}.$$

This condition is of course restrictive, but (as we can see in the examples) it holds in many cases which are important for the applications.

Let $K = L \cdot M$ and $\mathcal{O}_\mathcal{K} = \mathcal{O}_\mathcal{L} \cdot \mathcal{O}_\mathcal{M} = \mathbb{Z}[\alpha, \beta]$. Then $D_{\mathcal{O}_\mathcal{K}} = D^n_{\mathcal{O}_\mathcal{L}} \cdot D^m_{\mathcal{O}_\mathcal{M}}$ and any $\vartheta \in \mathcal{O}_\mathcal{K}$ can be written in the form

$$\vartheta = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot \alpha^i \cdot \beta^j$$

with conjugates

$$\vartheta_{kl} = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot \alpha_k^i \cdot \beta_l^j$$

$(1 \le k \le m,\ 1 \le l \le n)$.

Our main result is the following:

Theorem 4. *Assume that there exists a power integral basis in $\mathcal{O}_\mathcal{K}$. If (A) is satisfied, then*

$$(7) \qquad (d(g))^{m(m-1)/2} \equiv \pm 1 \pmod{p}.$$

If (B) is satisfied, then

$$(8) \qquad (d(f))^{n(n-1)/2} \equiv \pm 1 \pmod{q}.$$

As a consequence we have:

Theorem 5. *If (A) is satisfied, but (7) does not hold, then $\mathcal{O}_\mathcal{K}$ does not admit any power integral basis. If (B) is satisfied, but (8) does not hold, then $\mathcal{O}_\mathcal{K}$ does not admit any power integral basis.*

Proof of Theorem 4. If ϑ generates a power integral basis in K, then we have

$$(9) \qquad I(\vartheta) = \frac{1}{\sqrt{|D_{\mathcal{O}_\mathcal{K}}|}} \cdot \prod\nolimits_{(k_1,l_1)<(k_2,l_2)} |\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2}| = 1.$$

where the pairs $(k_1, l_1) < (k_2, l_2)$ are ordered lexicographically.

This product splits into three factors taking integer values. The first and second are the following:

$$F_1 = \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{\vartheta_{kl_1} - \vartheta_{kl_2}}{\beta_{l_1} - \beta_{l_2}},$$

$$F_2 = \prod_{l=1}^{n} \prod_{1 \le k_1 < k_2 \le m} \frac{\vartheta_{k_1 l} - \vartheta_{k_2 l}}{\alpha_{k_1} - \alpha_{k_2}}.$$

The factors in these products are algebraic integers. By using symmetric polynomials we can see that both F_1 and F_2 are complete norms, hence $F_1, F_2 \in \mathbb{Z}$. These factors absorb completely the discriminant $\sqrt{|D_{\mathcal{O}_\mathcal{K}}|}$, thus the third factor F_3 consist of the remaining factors $(\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2})$ of the product (9), and also takes integer value.

Assume that $f(x) \equiv x^m \pmod{p}$. Denote by N the smallest normal extension of K, let p_0 be a prime factor of p and let $\mathfrak{p}_0$ be a prime ideal of N lying above p_0. Since $f(x) \equiv x^m \pmod{p_0}$, hence $f(x) = \prod_{j=1}^{m}(x - \alpha_j) \equiv x^m \pmod{\mathfrak{p}_0}$. This means that for any root α_j we have
$0 = f(\alpha_j) \equiv \alpha_j^m \pmod{\mathfrak{p}_0}$ that is the roots of f are zero modulo $\mathfrak{p}_0$.

Let us consider the factors F_1 and $F_3 \pmod{\mathfrak{p}_0}$. Using $\alpha_j \equiv 0 \pmod{\mathfrak{p}_0}$ for $j = 1, \ldots, m$ we have

$$F_1 = \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \left(\frac{\vartheta_{kl_1} - \vartheta_{kl_2}}{\beta_{l_1} - \beta_{l_2}} \right)$$

$$= \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_k^i \cdot \beta_{l_1}^j - \alpha_k^i \cdot \beta_{l_2}^j)$$

$$\equiv \prod_{k=1}^{m} \prod_{1 \le l_1 < l_2 \le n} \frac{1}{\beta_{l_1} - \beta_{l_2}} \sum_{j=0}^{n-1} x_{0j} \cdot (\beta_{l_1}^j - \beta_{l_2}^j)$$

$$= \left(\prod_{1 \le l_1 < l_2 \le n} \sum_{j=0}^{n-1} x_{0j} \cdot \left(\frac{\beta_{l_1}^j - \beta_{l_2}^j}{\beta_{l_1} - \beta_{l_2}} \right) \right)^m \pmod{\mathfrak{p}_0}.$$

For similar reasons for F_3 we have

$$F_3 = \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} (\vartheta_{k_1 l_1} - \vartheta_{k_2 l_2})$$

$$= \prod_{k_1 \ne k_2} \prod_{1 \le l_1 < l_2 \le n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} x_{ij} \cdot (\alpha_{k_1}^i \cdot \beta_{l_1}^j - \alpha_{k_2}^i \cdot \beta_{l_2}^j)$$

$$\equiv \prod_{k_1\neq k_2}\prod_{1\le l_1<l_2\le n}\sum_{j=0}^{n-1} x_{0j}\cdot(\beta_{l_1}^j-\beta_{l_2}^j)$$

$$= \prod_{k_1\neq k_2}\prod_{1\le l_1<l_2\le n}(\beta_{l_1}-\beta_{l_2})\cdot\sum_{j=0}^{n-1} x_{0j}\cdot\left(\frac{\beta_{l_1}^j-\beta_{l_2}^j}{\beta_{l_1}-\beta_{l_2}}\right)$$

$$= (D_{\mathcal{O}_\mathcal{M}})^{m(m-1)/2}\cdot\left(\prod_{1\le l_1<l_2\le n}\sum_{j=0}^{n-1} x_{0j}\cdot\left(\frac{\beta_{l_1}^j-\beta_{l_2}^j}{\beta_{l_1}-\beta_{l_2}}\right)\right)^{m^2-m}$$

$$= (d(g))^{m(m-1)/2}\cdot\left(\prod_{1\le l_1<l_2\le n}\sum_{j=0}^{n-1} x_{0j}\cdot\left(\frac{\beta_{l_1}^j-\beta_{l_2}^j}{\beta_{l_1}-\beta_{l_2}}\right)\right)^{m^2-m} \pmod{\mathfrak{p}_0}.$$

In the case when $\vartheta\in\mathcal{O}_\mathcal{K}$ generates a power integral basis in $\mathcal{O}_\mathcal{K}$ then this means that $F_i=\varepsilon_i\quad(i=1,2,3)$, where $\varepsilon_i=1$ or -1. This implies

$$F_1\equiv\varepsilon_1 \pmod{\mathfrak{p}_0},\ F_2\equiv\varepsilon_2 \pmod{\mathfrak{p}_0},\ F_3\equiv\varepsilon_3 \pmod{\mathfrak{p}_0}.$$

Comparing the above congruences for F_1 and $F_3 \pmod{\mathfrak{p}_0}$ we conclude

$$(d(g))^{m(m-1)/2}\cdot\varepsilon_1^{m-1}\equiv\varepsilon_3 \pmod{\mathfrak{p}_0}.$$

But this is a congruence with integers, hence it must also hold modulo p_0 in $\mathbb{Z}$ (if an integer is divisible by a prime ideal then by taking norms it follows that a certain power of the prime number under the prime ideal divides a power of the integer, that is the prime number divides the integer):

$$(d(g))^{m(m-1)/2}\cdot\varepsilon_1^{m-1}\equiv\varepsilon_3 \pmod{p_0}.$$

This is satisfied for all prime factors p_0 of (the square-free) p hence we become

$$(d(g))^{m(m-1)/2}\cdot\varepsilon_1^{m-1}\equiv\varepsilon_3 \pmod{p},$$

that is

$$(d(g))^{m(m-1)/2}\equiv\pm1 \pmod{p}. \tag{10}$$

Performing a similar calculation in the case $g(x)\equiv x^n \pmod{q}$ for F_2 and $F_3 \pmod{q}$ we obtain

$$(d(f))^{n(n-1)/2}\equiv\pm1 \pmod{q}. \tag{11}$$

This theorem gives a simple condition to exclude the existence of power integral bases in $\mathcal{O}_\mathcal{K}$. If the congruences (7) and (8) are both valid and the discriminants D_L, D_M are coprime (this means that we can not apply Theorem 4) then we have to use Theorem 1 for finding the generator elements. On the other hand, if the discriminants D_L, D_M are coprime and if Theorem 4 is applicable, then we can exclude the existence of power integral bases without any tedious computations.

5. Examples

In the examples we use the polynomial orders $\mathcal{O}_{\mathcal{L}}$ and $\mathcal{O}_{\mathcal{M}}$ in the same meaning as in Theorem 2, and similarly $\mathcal{O}_{\mathcal{K}} = \mathcal{O}_{\mathcal{L}}\mathcal{O}_{\mathcal{M}}$.

Example I. Let p, q be square-free integers (≥ 2). One of the most straightforward and frequently used applications of Theorem 4 is the case when $f(x) = x^m - p$ and $g(x) = x^n - q$. Assume that $K = \mathbb{Q}(\sqrt[m]{p}, \sqrt[n]{q})$ is of degree mn. We have

$$d(f) = (-1)^{(m-1)(m-2)/2} \cdot m^m \cdot p^{m-1},$$

$$d(g) = (-1)^{(n-1)(n-2)/2} \cdot n^n \cdot q^{n-1}.$$

By Theorem 4 if one of the congruences

$$\left(n^n \cdot q^{n-1}\right)^{m(m-1)/2} \equiv \pm 1 \pmod{p},$$

$$\left(m^m \cdot p^{m-1}\right)^{n(n-1)/2} \equiv \pm 1 \pmod{q}.$$

is not satisfied, then $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\sqrt[m]{p}, \sqrt[n]{q}]$ has no power integral basis.

I.1. In the special case if $m = 3,\ n = 2$, the field $K = L \cdot M$ is an algebraic number field of degree 6. We have $d(f) = D_{\mathcal{O}_{\mathcal{L}}} = -27 \cdot p^2, d(g) = D_{\mathcal{O}_{\mathcal{M}}} = 4 \cdot q$.

The above congruences are of the form

$$64 \cdot q^3 \equiv \pm 1 \pmod{p}. \tag{12}$$

$$-27 \cdot p^2 \equiv \pm 1 \pmod{q}. \tag{13}$$

If for example $p = 7,\ q = 5$ then $\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1$. We have

$$64 \cdot 5^3 = 8000 \equiv 6 \equiv -1 \pmod{7}, \tag{14}$$

$$-27 \cdot 7^2 = -1323 \equiv 2 \equiv -3 \pmod{5}. \tag{15}$$

Theorem 4 implies that there is no power integral basis in $\mathcal{O}_{\mathcal{K}}$.

I.2. In the special case when $m = 22,\ n = 15$ and $[K : \mathbb{Q}] = 22 \cdot 15 = 330$, we have

$$d(f) = D_{\mathcal{O}_{\mathcal{L}}} = 22^{22} \cdot p^{21},\ \ d(g) = D_{\mathcal{O}_{\mathcal{M}}} = -15^{15} \cdot q^{14}.$$

If for example we take $p = 31,\ q = 17$ then

$$\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 4, either

$$(-15^{15} \cdot 17^{14})^{231} \equiv 4 \equiv -27 \pmod{31}$$

or

$$(22^{22} \cdot 31^{21})^{105} \equiv 10 \equiv -7 \pmod{17}$$

implies that there exist no power integral basis in $\mathcal{O}_{\mathcal{K}}$.

Example II. To consider a different example let $f(x) = x^5 - p^3x^3 - p^2x^2 - px - p$ and $g(x) = x^3 - q^2x^2 - qx - q$ $(m = 5,\ n = 3)$. If $\mathcal{O}_{\mathcal{K}}$ has power integral bases, then the following congruences must be satisfied:

$$d(g)^{10} \equiv \pm 1 \pmod{p},$$

$$d(f)^3 \equiv \pm 1 \pmod{q},$$

where

$$d(g) = -q^2(-4q - q^4 + 18q^2 + 4q^5 + 27)$$

and

$$d(f) = -p^4(108p^{13} - 56p^{12} + 12p^{11} + 75p^8 - 38p^7 + 11p^6 - 3750p^4 +$$

$$4250p^3 - 1600p^2 + 256p - 3125).$$

If one of these congruences is not satisfied, $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\alpha, \beta]$ (α and β are being roots of f, g respectively) has no power integral basis.

II.1. Let $p = 7,\ q = 29$. Then $[K : \mathbb{Q}] = 5 \cdot 3 = 15$, and we have

$$d(f) = D_{\mathcal{O}_{\mathcal{L}}} = -23320969892806663 = -(7)^4(11)^2(5208131)(15413),$$

$$d(g) = D_{\mathcal{O}_{\mathcal{M}}} = -68417338124 = -(2)^2(29)^2(41)(496051)$$

and

$$\gcd(D_{\mathcal{O}_{\mathcal{L}}}, D_{\mathcal{O}_{\mathcal{M}}}) = 1,$$

hence Theorem 1 would be applicable. But by applying Theorem 4, either

$$d(g)^{10} \equiv 2 \equiv -5 \pmod{7}$$

or

$$d(f)^3 \equiv 6 \equiv -23 \pmod{29}$$

implies that there exist no power integral basis in $\mathcal{O}_{\mathcal{K}}$.

References

[1] Gaál, I., Computing elements of given index in totally complex cyclic sextic fields, *J. Symbolic Comput.,* **20** (1995), 61–69.

[2] Gaál, I., Power integral bases in composits of number fields, *Canad. Math. Bulletin*, **41** (1998), 158–165.

[3] Gaál, I. Solving index form equations in fields of degree nine with cubic subfields, *J. Symbolic Comput.*, **30** (2000), 181–193.

[4] Gaál, I., *Diophantine equations and power integral bases,* Birkhäuser, Boston, 2002.

[5] Gaál, I. and Győry, K., Index form equations in quintic fields, *Acta Arith.*, **89** (1999), 379–396.

[6] Gaál, I., Olajos, P. and Pohst, M., Power integral bases in orders of composit fields, *Experimental Math.*, **11** (2002), 87–90.

[7] Gaál, I., Pethő, A., and Pohst, M., On the resolution of index form equations in quartic number fields, *J. Symbolic Comput.*, **16** (1993), 563–584.

[8] Gaál, I. and Pohst, M., On the resolution of index form equations in sextic fields with an imaginary quadratic subfield, *J. Symbolic Comput.*, **22** (1996), 425–434.

[9] Gaál, I. and Schulte, N., Computing all power integral bases of cubic number fields, *Math. Comput.*, **53** (1989), 689–696.

[10] Győry, K., Sur les polynômes à coefficients entiers et de discriminant donné III., *Publ. Math. Debrecen*, **23** (1976), 141–165.

[11] Járási, I., Power integral bases in sextic fields with a cubic subfield, *Acta Sci. Math. Szeged*, to appear.

[12] Narkiewicz, W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1974.

István Gaál
University of Debrecen
Institute of Mathematics
H–4010 Debrecen, P.O. Box 12.
Hungary
e-mail: igaal@math.klte.hu

Péter Olajos
University of Debrecen
Institute of Mathematics
H–4010 Debrecen, P.O. Box 12.
Hungary
e-mail: olaj@math.klte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 55–65*

ON THE L^1 NORM OF THE WEIGHTED MAXIMAL FUNCTION OF THE WALSH–KACZMARZ–DIRICHLET KERNELS

György Gát (Nyíregyháza, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. In this paper we investigate the integral of the weighted maximal function of the Walsh–Paley–Dirichlet, and the Walsh–Kaczmarz–Dirichlet kernels. We find necessary and sufficient conditions for the finiteness of the integrals. The conditions are quite different for the two rearrangements of the Walsh system.

AMS Classification Number: 42C10

Keywords and phrases: Walsh–Paley, Walsh–Kaczmarz system, Dirichlet kernels, weighted maximal functions, integral.

1. Introduction

The Walsh system in the Kaczmarz enumeration was studied by a lot of authors (see [4], [5], [8], [7], [1], [6], [9]). In [2] it has been pointed out that the behavior of the Dirichlet kernel of the Walsh–Kaczmarz system is worse than of the kernel of the Walsh–Paley system considered more often. Namely, it is proved [2]that for the Dirichlet kernel $D_n(x)$ of the Walsh–Kaczmarz system the inequality $\limsup_{n\to\infty} \frac{|D_n(x)|}{\log n} \geq C > 0$ holds a.e. This "spreadness" of this system makes easier to construct examples of divergent Fourier series [1].

A number of pathological properties is due to this "spreadness" property of the kernel. For example, for Fourier series with respect to the Walsh–Kaczmarz system it is impossible to establish any local test for convergence at a point or on an interval, since the principle of localization does not hold for this system.

On the other hand, the global behavior of the Fourier series with respect to this system is similar in many aspects to the case of the Walsh–Paley system. Schipp [5] and Wo–Sang Young [9] proved that the Walsh–Kaczmarz system is a convergence system. Skvorcov [8] verified the everywhere (and uniform) convergence of the Fejér

Research supported by the Hungarian "Művelődési és Közoktatási Minisztérium", grant no. FKFP 0182/2000, by the Hungarian National Foundation for Scientific Research (OTKA), grant no. M 36511/2001.

means of continuous functions, and Gát proved [3] that the Fejér–Lebesgue theorem also holds for the Walsh–Kaczmarz system.

Beyond the convergence theorems of the Fourier series one can often find some boundedness properties of the Dirichlet kernel functions. For instance, for the Walsh–Paley system we have $\sup_{n\in\mathbb{N}} |D_n(x)| < \infty$ for each $x \neq 0$. This —as we have seen above— is not the case for the Kaczmarz rearrangement. What can be said for the norm of maximal functions? It is easy to have that the L^1 norm of $\sup_{n\in\mathbb{N}} |D_n|$ with respect to both systems is infinite. What happens if we apply some weight function α? That is, on what conditions find we the inequality

$$\left\| \sup_{n\in\mathbb{N}} \left| \frac{D_n}{\alpha(n)} \right| \right\|_1 < \infty$$

valid? The aim of this paper is to find the necessary and sufficient conditions for the both rearrangement of the Walsh system.

Let P denote the set of positive integers, $N := P \cup \{0\}$ the set of nonnegative integers and Z_2 the discrete cyclic group of order 2, respectively. That is, $Z_2 = \{0, 1\}$ the group operation is the mod 2 addition and every subset is open. Haar measure is given in a way that the measure of a singleton is 1/2. Set

$$G := \times_{\infty}^{k=0} Z_2$$

the complete direct product. Thus, every $x \in G$ can be represented by a sequence $x = (x_i, i \in \mathbb{N})$, where $x_i \in \{0, 1\}\, (i \in \mathbb{N})$. The group operation on G is the coordinate-wise addition, (which is the so-called logical addition) the measure (denoted by μ) and the topology are the product measure and topology. The compact Abelian group G is called the Walsh group. Set $e_i := (0, 0, \ldots, 1, 0, 0, \ldots) \in G$ the i-th coordinate of which is 1, the rest are zeros.

A base for the neighborhoods of G can be given as follows

$$I_0(x) := G, \quad I_n(x) := \{y = (y_i, i \in \mathbb{N}) \in G : y_i = x_i \,\text{for}\, i < n\}$$

for $x \in G, n \in \mathbb{P}$. Let $0 = (0, i \in \mathbb{N}) \in G$ denote the nullelement of $G, I_n := I_n(0)\, (n \in \mathbb{N})$. Let $\mathcal{I} := \{I_n(x) : x \in G, n \in \mathbb{N}\}$. The elements of $\mathcal{I}$ are called the dyadic intervals on G. Furthermore, let $L^p(G)\, (1 \leq p \leq \infty)$ denote the usual Lebesgue spaces ($|\,.\,|_p$ the corresponding norms) on G, $\mathcal{A}_n$ the σ algebra generated by the sets $I_n(x)\, (x \in G_m)$ and E_n the conditional expectation operator with respect to $\mathcal{A}_n\, (n \in \mathbb{N})\, (f \in L^1)$.

Let $n \in \mathbb{N}$. Then $n = \sum_{i=0}^{\infty} n_i 2^i$, where $n_i \in \{0, 1\}\, (n \in \mathbb{N})$, i.e. n is expressed in the number system based 2. Denote by $|n| := \max(j \in \mathbb{N} : n_j \neq 0)$, that is, $2^{|n|} \leq n < 2^{|n|+1}$. The Rademacher functions are defined as:

$$r_n(x) := (-1)^{x_n} \quad (x \in G,\, n \in \mathbb{N}).$$

The Walsh–Paley system is defined as the sequence of the Walsh–Paley functions:

$$\omega_n(x) := \prod_{k=0}^{\infty} (r_k(x))^{n_k} = (-1)^{\sum_{k=0}^{|n|} n_k x_k}, \quad (x \in G,\, n \in \mathbb{N}).$$

That is, $\omega := (\omega_n, n \in \mathbb{N})$. The n-th Walsh–Kaczmarz function is

$$\kappa_n(x) := r_{|n|}(x) \prod_{k=0}^{|n|-1} \big(r_{|n|-1-k}(x)\big)^{n_k} = r_{|n|}(x)(-1)^{\sum_{k=0}^{|n|-1} n_k x_{|n|-1-k}},$$

for $n \in \mathbb{P}$, $\kappa_0(x) := 1, x \in G$. The Walsh–Kaczmarz system $\kappa := (\kappa_n, n \in \mathbb{N})$ can be obtained from the Walsh–Paley system by renumbering the functions within the dyadic "block" with indices from the segment $[2^n, 2^{n+1} - 1]$. That is, $\{\kappa_n : 2^k \le n < 2^{k+1}\} = \{\omega_n : 2^k \le n < 2^{k+1}\}$ for all $k \in \mathbb{N}$, $\kappa_0 = \omega_0$.

By means of the transformation $\tau_A : G \to G$

$$\tau_A(x) := (x_{A-1}, x_{A-2}, \dots, x_1, x_0, x_A, x_{A+1}, \dots) \in G,$$

which is clearly measure-preserving and such that $\tau_A(\tau_A(x)) = x$ we have

$$\kappa_n(x) = r_{|n|}(x)\omega_n(\tau_{|n|}(x)) \quad (n \in \mathbb{N}).$$

Let us consider the Dirichlet kernel functions:

$$D_n^{\phi} := \sum_{k=0}^{n-1} \phi_k,$$

where ϕ is either κ or ω and $n \in \mathbb{P}$.

Let function $\alpha : [0, +\infty) \to [1, +\infty)$ be monotone increasing, and define the weighted maximal function of the Dirichlet kernels:

$$D_{\alpha}^{\phi}(x) := \sup_{n \in \mathbb{N}} \frac{|D_n^{\phi}(x)|}{\alpha(\lfloor \log n \rfloor)} \quad (x \in G),$$

where ϕ is either the Walsh–Paley, or the Walsh–Kaczmarz system. If it does not cause confusion the notation ϕ is omitted. First we discuss the Walsh–Paley case.

Proposition 1. *$D_{\alpha}^{\omega} \in L^1$ if and only if $\sum_{A=0}^{\infty} \frac{1}{\alpha(A)} < \infty$. Moreover,*

$$\frac{1}{2} \sum_{A=0}^{\infty} \frac{1}{\alpha(A)} \le \| D_{\alpha}^{\omega} \|_1 \le 2 \sum_{A=0}^{\infty} \frac{1}{\alpha(A)}.$$

Proof. In [6] one can read that for arbitrary $x \in I_A \setminus I_{A+1}$, and $A \in \mathbb{N}$ the inequality

$$|D_n(x)| \leq \min\{n, 2^A\}.$$

This immediately follows

$$D_\alpha(x) \leq 2 \sum_{k=0}^{A} \frac{2^k}{\alpha(k)}.$$

That is,

$$\begin{aligned} || D_\alpha ||_1 &= \sum_{A=0}^{\infty} \int_{I_A \setminus I_{A+1}} D_\alpha(x) d\mu(x) \\ &\leq 2 \sum_{A=0}^{\infty} \frac{1}{2^{A+1}} \sum_{k=0}^{A} \frac{2^k}{\alpha(k)} \\ &= \sum_{k=0}^{\infty} \sum_{A=k}^{\infty} \frac{1}{2^A} \frac{2^k}{\alpha(k)} \\ &\leq 2 \sum_{k=0}^{\infty} \frac{1}{\alpha(k).} \end{aligned}$$

That is, we have proved that $(1/\alpha(n)) \in l^1$ implies $D_\alpha \in L^1$. On the other hand, in the same way as above we have

$$\begin{aligned} | D_\alpha |_1 &= \sum_{A=0}^{\infty} \int_{I_A \setminus I_{A+1}} D_\alpha(x) d\mu(x) \\ &\geq \sum_{A=0}^{\infty} \int_{I_A \setminus I_{A+1}} \frac{D_{2^A}(x)}{\alpha(A)} d\mu(x) \\ &= \sum_{A=0}^{\infty} \frac{1}{2^{A+1}} \frac{2^A}{\alpha(A)}. \end{aligned}$$

In the case of the Walsh–Kaczmarz system the situation changes. Namely, we prove the following two propositions:

Proposition 2. *If* $\sum_{A=1}^{\infty} \frac{A}{\alpha(A)} < \infty$, *then* $D_\alpha^\kappa \in L^1$. *Moreover,* $|| D_\alpha^\kappa ||_1 \leq 4 \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} + C$, *where* C *is some constant, such that may depend on* α *(but anyway it is a finite real).*

Proposition 3. *There exists a positive constant* C *(which may depend on* α*) such that*

$$| D_\alpha^\kappa |_1 \geq \frac{1}{25} \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} - C.$$

These propositions give

Corollary 4. *$D_\alpha^\kappa \in L^1$ if and only if $\sum_{A=1}^{\infty} \frac{A}{\alpha(A)} < \infty$.*

That is, in the case of the Kaczmarz rearrangement we have to divide by a "greater" weight function α if we want the maximal function D_α^κ to be integrable. Besides, by the method of the proof of Proposition 3 one can prove that if $D_\alpha^\kappa \notin L^1$ (that is, $\sum_{A=1}^{\infty} \frac{A}{\alpha(A)} = \infty$), then it is not integrable on any dyadic interval. This is quite different in the Walsh–Paley case. Since for this system even the maximal function $\sup_n |D_n^\omega|$ is bounded by 2^A on $G \setminus I_A$. In order to prove Proposition 2 we use to following lemma. Let

$$L_\alpha(x) := \sup\{\frac{D_{2^j}(\tau_A(x))}{\alpha(A)} : j \le A, j, A \in \mathbb{N}\}, \quad x \in G.$$

Lemma 5. *We prove $|| L_\alpha ||_1 \le 2 \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} + C$.*

Proof.

$$| L_\alpha |_1 \le \sum_{A=0}^{\infty} \sum_{j=0}^{A} \frac{| D_{2^j} \circ \tau_A |_1}{\alpha(A)} = \sum_{A=1}^{\infty} \frac{A+1}{\alpha(A)} + C.$$

Proof of Proposition 2. It is known ([6]) that for $1 \le n \in \mathbb{N}$

$$D_n^\kappa = D_{2^{|n|}} + r_{|n|} D_{n-2^{|n|}}^\omega \circ \tau_{|n|}.$$

Since in [6] one can find the inequality

$$|D_n^\omega(x)| \le 2^j = D_{2^j}(x)$$

for any $x \in I_j \setminus I_{j+1}$, then

$$\sup_{|n|=A} |D_n^\kappa(x)| \le D_{2^A}(x) + \sup_{|n|<A} |D_n^\omega(\tau_A(x))| \le D_{2^A}(x) + \sup\{D_{2^j}(\tau_A(x)) : j < A\}.$$

This gives

$$D_\alpha^\kappa(x) = \sup_A \sup_{|n|=A} \frac{|D_n^\kappa(x)|}{\alpha(A)} \le \sup_A \frac{|D_{2^A}(x)|}{\alpha(A)} + L_\alpha(x) \le D_\alpha^\omega(x) + L_\alpha(x).$$

By Proposition 1 we have

$$| D_\alpha^\omega |_1 \le 2 \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} + C,$$

and by Lemma 5, that is, by

$$| L_\alpha |_1 \leq 2 \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} + C$$

the proof of the inequality

$$| D_\alpha^\kappa |_1 \leq 4 \sum_{A=1}^{\infty} \frac{A}{\alpha(A)} + C,$$

that is, the proof of Proposition 2 is complete.

Proof of Proposition 3. Introduce the following notations:

$$L_{\alpha,N} := \sup_{\substack{A \leq N \\ j \leq A}} \left| \frac{D_{2^j} \circ \tau_A}{\alpha(A)} \right|, \quad a_N := | L_{\alpha,N} |_1 \ \ (N \in \mathbb{N}).$$

First, we prove that

$$a_N \leq CN^2. \tag{1}$$

This in equality can be proved in the following way.

$$a_N \leq \sum_{A=0}^{N} \sum_{j=0}^{A} \left\| \frac{D_{2^j} \circ \tau_A}{\alpha(0)} \right\|_1 \leq \sum_{A=0}^{N} \sum_{j=0}^{A} C \leq CN^2.$$

Next, for $N \in \mathbb{N}$, and $k \in \mathbb{N}, 1 \leq k$ denote by $J_{N,k}$ the following subset of G.

$$J_{N,k} := \begin{cases} \{x \in G : x_{N-k} = 1, x_{N-k+1} = \cdots = x_{N-1} = 0\} & \text{if } N \geq k \geq 2, \\ \{x \in G : x_{N-1} = 1\} & \text{if } N \geq k = 1. \end{cases}$$

Since for fixed N the sets$J_{N,k}$, I_N are disjoint, and $\cup_{k=1}^{N} J_{N,k} \cup I_N = G$, then we have

$$a_N = \sum_{k=1}^{N} \int_{J_{N,k}} L_{\alpha,N} \, d\mu + \int_{I_N} L_{\alpha,N} \, d\mu. \tag{2}$$

We give another upper bound for a_N, a different one from the inequality (1). Investigate the function $L_{\alpha,N}$ on the set $J_{N,k}$.

If $A = N$, then for $y = \tau_A(x)$ we have $y_0 = \cdots = y_{k-2} = 0, y_{k-1} = 1$.

Thus, $\sup_{j \leq A} D_{2^j}(\tau_A(x))/\alpha(A) = 2^{k-1}/\alpha(N)$.

For $A = N - 1$ we have $\sup_{j \leq A} D_{2^j}(\tau_A(x))/\alpha(A) = 2^{k-2}/\alpha(N-1)$.

And so on ...
Finally, if $A = N - k + 1$ we have $\sup_{j\le A} D_{2^j}(\tau_A(x))/\alpha(A) = 1/\alpha(N-k+1)$. That is, for $x \in J_{N,k}$

$$\sup_{\substack{N-k<A\le N\\ j\le A}} \left|\frac{D_{2^j}\circ\tau_A(x)}{\alpha(A)}\right| = \max\left\{\frac{2^{k-1}}{\alpha(N)}, \frac{2^{k-2}}{\alpha(N-1)}, \dots, \frac{1}{\alpha(N-k+1)}\right\}.$$

This, and

$$\int_{J_{N,k}} \sup_{\substack{A\le N-k\\ j\le A}} \left|\frac{D_{2^j}\circ\tau_A(x)}{\alpha(A)}\right| d\mu = \frac{1}{2^k} a_{N-k}$$

implies

$$\int_{J_{N,k}} L_{\alpha,N}(x)\, d\mu(x) = \max\left\{\frac{1}{2\alpha(N)}, \frac{1}{2^2\alpha(N-1)}, \dots, \frac{1}{2^k\alpha(N-k+1)}, \frac{1}{2^k} a_{N-k}\right\}.$$

Consequently, by (2) we have

$$\begin{aligned} a_N &\le \sum_{k=1}^{N} \sup_{l\in[1,\dots,k]} \frac{1}{2^l\alpha(N-l+1)} + \sum_{k=1}^{N}\frac{1}{2^k}a_{N-k} + \int_{I_N} L_{\alpha,N}\, d\mu \\ &\le \sum_{k=1}^{N} \sup_{l\in[1,\dots,k]} \frac{1}{2^l\alpha(N-l+1)} + \sum_{k=1}^{N}\frac{1}{2^k}a_{N-k} + \frac{1}{2^N}L_{\alpha,N}(0) \\ &\le N \sup_{A\in[1,\dots,N]} \frac{1}{2^{N-A+1}\alpha(A)} + \sum_{k=1}^{N}\frac{1}{2^k}a_{N-k} + \sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)} \\ &\le \left(\frac{N}{2}+1\right) \sup_{0<A\le N} \frac{1}{2^{N-A}\alpha(A)} + \sum_{k=1}^{N}\frac{1}{2^k}a_{N-k} + \frac{1}{2^N\alpha(0)}. \end{aligned} \tag{3}$$

Next, we prove the inequality below (constant C depends on the function α).

$$\sum_{n=1}^{N}\frac{n}{2}\sup\left\{\frac{1}{\alpha(n)}, \frac{1}{2\alpha(n-1)}, \dots, \frac{1}{2^{n-1}\alpha(1)}\right\} \le C + \frac{2}{3}\sum_{n=1}^{N}\frac{n}{\alpha(n)}. \tag{4}$$

If

$$\sup\left\{\frac{1}{\alpha(n)}, \frac{1}{2\alpha(n-1)}, \dots, \frac{1}{2^{n-1}\alpha(1)}\right\} = \frac{1}{2^k\alpha(n-k)}$$

for some $1 \le k < n$, then we have

$$\sup\left\{\frac{1}{\alpha(n)}, \frac{1}{2\alpha(n-1)}, \dots, \frac{1}{2^{n-1}\alpha(1)}\right\} = \frac{1}{2^k\alpha(n-k)}$$
$$\sup\left\{\frac{1}{\alpha(n-1)}, \frac{1}{2\alpha(n-2)}, \dots, \frac{1}{2^{n-2}\alpha(1)}\right\} = \frac{1}{2^{k-1}\alpha(n-k)}$$
$$\vdots$$
$$\sup\left\{\frac{1}{\alpha(n-k)}, \frac{1}{2\alpha(n-k-1)}, \dots, \frac{1}{2^{n-k-1}\alpha(1)}\right\} = \frac{1}{\alpha(n-k)}.$$

Consequently, for the left side of (4) we have the following upper bound.

$$\frac{1}{2}\sum_{i=1}^{K}\left(\frac{n_i}{\alpha(n_i)} + \frac{n_i+1}{2\alpha(n_i)} + \frac{n_i+2}{2^2\alpha(n_i)} + \dots + \frac{n_{i+1}-1}{2^{n_{i+1}-n_i-1}\alpha(n_i)}\right),$$

where for the strictly monotone increasing sequence (n_i) we have $n_1 = 1$, and $K \in \mathbb{N}$ is defined as $n_{K+1} - 1 = N$. If

$$\{i \in \mathbb{N}\colon n_i + 1 < n_{i+1}\} = \emptyset,$$

then the left side of (4) is bounded by

$$\frac{1}{2}\sum_{n=1}^{K}\frac{n}{\alpha(n)} = \frac{1}{2}\sum_{n=1}^{N}\frac{n}{\alpha(n)}.$$

On the other hand, if

$$\{i \in \mathbb{N}\colon n_i + 1 < n_{i+1}\} \neq \emptyset,$$

then let ρ denote its minimal element. That is, $n_1 = 1, n_2 = 2, \dots, n_\rho = \rho, n_{\rho+1} \ge \rho + 2$. Consequently for the left side of (4) we have

$$\begin{aligned}
&\sum_{n=1}^{N}\frac{n}{2}\sup\left\{\frac{1}{\alpha(n)}, \frac{1}{2\alpha(n-1)}, \dots, \frac{1}{2^{n-1}\alpha(1)}\right\}\\
&= \frac{1}{2}\left(\frac{1}{\alpha(1)} + \frac{2}{\alpha(2)} + \dots + \frac{\rho-1}{\alpha(\rho-1)}\right)\\
&+ \frac{1}{2}\left(\frac{n_\rho}{\alpha(n_\rho)} + \frac{n_\rho+1}{2\alpha(n_\rho)} + \dots + \frac{n_{\rho+1}-1}{2^{n_{\rho+1}-n_\rho-1}\alpha(n_\rho)}\right)\\
&+ \frac{1}{2}\sum_{i=\rho+1}^{K}\left(\frac{n_i}{\alpha(n_i)} + \frac{n_i+1}{2\alpha(n_i)} + \frac{n_i+2}{2^2\alpha(n_i)} + \dots + \frac{n_{i+1}-1}{2^{n_{i+1}-n_i-1}\alpha(n_i)}\right) \qquad (5)\\
&\le C + \frac{1}{2}\sum_{i=\rho+1}^{K}\left(\frac{n_i}{\alpha(n_i)} + \frac{1}{\alpha(n_i)}\left(n_i + \sum_{j=1}^{\infty}\frac{j}{2^j}\right)\right)\\
&\le C + \frac{1}{2}\sum_{i=\rho+1}^{K}\left(\frac{n_i}{\alpha(n_i)} + \frac{n_i+2}{\alpha(n_i)}\right)
\end{aligned}$$

(C depends on α). Since the function $\alpha\colon[0,+\infty)\to[1,+\infty)$ is monotone increasing, then we have

$$\begin{aligned}
&\sum_{n=1}^{N}\frac{n}{2}\sup\left\{\frac{1}{\alpha(n)},\frac{1}{2\alpha(n-1)},\dots,\frac{1}{2^{n-1}\alpha(1)}\right\}\\
&\le C+\frac{1}{2}\sum_{i=\rho+1}^{K}\left(\frac{n_i}{\alpha(n_i-1)}+\frac{n_i+2}{\alpha(n_i)}\right)\\
&\le C+\frac{1}{2}\sum_{n=n_{\rho+1}-1}^{N}\frac{n+2}{\alpha(n)}\\
&\le C+\frac{1}{2}\cdot\frac{4}{3}\sum_{n=1}^{N}\frac{n}{\alpha(n)}.
\end{aligned}$$

That is, the inequality (4) is verified. On the other hand, (2) also implies

$$\begin{aligned}
a_N&\ge\sum_{k=1}^{N}\max\left\{\frac{1}{2\alpha(N)},\frac{1}{2^k}a_{N-k}\right\}+\sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)}\\
&\ge\sum_{k=\lfloor N/4\rfloor+1}^{N}\frac{1}{2\alpha(N)}+\sum_{k=1}^{\lfloor N/4\rfloor}\frac{1}{2^k}a_{N-k}+\sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)}\\
&\ge\frac{3N/8}{\alpha(N)}+\frac{a_{N-1}}{2}+\frac{a_{N-2}}{2^2}+\dots+\frac{a_{\lceil 3N/4\rceil}}{2^{\lfloor N/4\rfloor}}+\sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)}.
\end{aligned}$$

By this inequality we have

$$2a_N-a_{N-1}\ge\frac{3N/4}{\alpha(N)}+\frac{a_{N-2}}{2}+\frac{a_{N-3}}{2^2}+\dots+\frac{a_{\lceil 3N/4\rceil}}{2^{\lfloor N/4\rfloor-1}}+2\sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)}.$$

Consequently, (3) gives

$$\begin{aligned}
&2a_N-2a_{N-1}\ge\frac{3N/4}{\alpha(N)}+\frac{a_{N-2}}{2}+\frac{a_{N-3}}{2^2}+\dots+\frac{a_{\lceil 3N/4\rceil}}{2^{\lfloor N/4\rfloor-1}}+2\sup_{A\le N}\frac{1}{2^{N-A}\alpha(A)}\\
&-\frac{N-1}{2}\sup_{A\le N-1}\frac{1}{2^{N-1-A}\alpha(A)}-\sum_{k=1}^{N-1}\frac{1}{2^k}a_{N-1-k}-\sup_{A\le N-1}\frac{1}{2^{N-A}\alpha(A)}\\
&\ge\frac{3N/4}{\alpha(N)}-\frac{N-1}{2}\sup_{A\le N-1}\frac{1}{2^{N-1-A}\alpha(A)}-\sum_{k=\lfloor N/4\rfloor}^{N-1}\frac{1}{2^k}a_{N-1-k}.
\end{aligned}$$

At last by (1) and (4) we have the following lower bound for a_N.

$$\begin{aligned}
2a_N &= \sum_{n=1}^{N}(2a_n - 2a_{n-1}) \\
&\geq \sum_{n=1}^{N}\frac{3n/4}{\alpha(n)} - \sum_{n=0}^{N-1}\frac{n}{2}\sup_{A\leq n}\frac{1}{2^{n-A}\alpha(A)} - C\sum_{n=1}^{N}\frac{n^2}{2^{n/4}} \\
&\geq \left(\frac{3}{4}-\frac{2}{3}\right)\sum_{n=1}^{N}\frac{n}{\alpha(n)} - C.
\end{aligned}$$

Apply Proposition (1), or more exactly, the method its proof, and the inequality given for a_N above.

$$\begin{aligned}
&|| D_\alpha^\kappa ||_1 = \sup_{N\in\mathbb{N}}\sup\left\{\left|\left|\frac{D_n^\kappa}{\alpha(\log(\lfloor n\rfloor))}\right|\right|_1 : n\leq N\right\} \\
&\geq \sup_{N\in\mathbb{N}}\sup\left\{\left|\left|\frac{D_{2^A+2^j}^\kappa}{\alpha(A)}\right|\right|_1 : j<A\leq N, (j,A,N\in\mathbb{N})\right\} \\
&\geq \sup_{N\in\mathbb{N}}\sup\left\{\left|\left|\frac{D_{2^j}^\omega\circ\tau_A}{\alpha(A)} - \frac{D_{2^A}}{\alpha(A)}\right|\right|_1 : j<A\leq N, (j,A,N\in\mathbb{N})\right\} \\
&\geq \sup_{N\in\mathbb{N}}\left(a_N - 2\sum_{A=0}^{N}\frac{1}{\alpha(A)}\right) \\
&\geq \sup_{N\in\mathbb{N}}\left(\frac{1}{24}\sum_{n=1}^{N}\frac{n}{\alpha(n)} - 2\sum_{A=1}^{N}\frac{1}{\alpha(A)} - C\right) \\
&\geq \frac{1}{25}\sum_{n=1}^{\infty}\frac{n}{\alpha(n)} - C.
\end{aligned}$$

This completes the proof of Proposition (3).

References

[1] Balašov, L. A., Series with respect to the Walsh system with monotone coefficients, *Sibirsk Math. Ž*, **12** (1971), 25–39.

[2] Šneider, A. A., On series with respect to the Walsh functions with monotone coefficients, *Izv. Akad. Nauk SSSR, Ser. Mat.*, **12** (1948), 179–192.

[3] Gát, Gy., On $(C,1)$ summability of integrable functions with respect to the Walsh–Kaczmarz system, *Studia Math.*, **130** (1998), No. 2, 135–148.

[4] Schipp, F., Certain rearrangements of series in the Walsh series, *Mat. Zametki*, **18** (1975), 193–201.

[5] Schipp, F., Pointwise convergence of expansions with respect to certain product systems, *Analysis Math.*, **2** (1976), 63–75.

[6] Schipp, F., Wade, W. R., Simon, P. and Pál, J., *Walsh series: an introduction to dyadic harmonic analysis*, Adam Hilger, Bristol and New York, 1990.

[7] Skvorcov, V. A., Convergence in L_1 of Fourier series with respect to the Walsh–Kaczmarz system, *Vestnik Mosk. Univ. Ser. Mat. Meh.*, **6** (1981), 3–6.

[8] Skvorcov, V. A., On Fourier series with respect to the Walsh–Kaczmarz system, *Analysis Math.,* **7** (1981), 141–150.

[9] Young, W. S., On the a. e. convergence of Walsh–Kaczmarz–Fourier series, *Proc. Amer. Math. Soc.,* **44** (1974), 353–358.

György Gát
Inst. of Math. and Comp. Sci.
College of Nyíregyháza
H-4400, Nyíregyháza, P.O. Box 166.
Hungary
e-mail: gatgy@zeus.nyf.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 67–73*

ON SOME ARITHMETICAL PROPERTIES OF LUCAS AND LEHMER NUMBERS, II.

Kálmán Győry* **(Debrecen)**

Dedicated to the memory of Professor Péter Kiss

Abstract. Denote by S the set of non-zero integers composed only of finitely many given primes. We proved with Kiss and Schinzel [7] that if u_n is a Lucas or Lehmer number with $n>6$ and $u_n \in S$, then $|u_n|$ can be estimated from above in terms of S. An explicit upper bound for $|u_n|$ was given later in our article [5]. In the present paper a significant improvement of this bound is established which implies, among other things, that $P(u_n) > \frac{1}{4}(\log\log|u_n|)^{1/2}$ if $n>30$ or if $30 \geq n > 6$ and $|u_n|$ is sufficiently large.

AMS Classification Number: 11B39, 11D61

1. Introduction

The Lucas numbers u_n are defined by

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad n > 0,$$

where $\alpha + \beta$ and $\alpha\beta$ are relatively prime non-zero rational integers and α/β is not a root of unity, while the Lehmer numbers u_n satisfy

$$u_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{if n is odd,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{if n is even,} \end{cases}$$

where $(\alpha + \beta)^2$ and $\alpha\beta$ are relatively prime non-zero rational integers and α/β is not a root of unity. The Lucas and Lehmer numbers are non-zero rational integers.

*Supported in part by the Netherlands Organization for Scientific Research, the Hungarian Academy of Sciences and by grants 29330, 38225 and 42985 of the Hungarian National Foundation for Scientific Research.

Let $p_1, \dots, p_s$ be rational primes with $\max_i p_i = P$, and denote by S the set of non-zero rational integers not divisible by primes different from $p_1, \dots, p_s$. We proved with Kiss and Schinzel [7] that if u_n is a Lucas number or a Lehmer number with $n > 6$ and $u_n \in S$ then

$$n \le \max\{C_1, P+1\} \tag{1}$$

with $C_1 = e^{452}4^{67}$ and

$$\max\{|\alpha|, |\beta|, |u_n|\} < C_2, \tag{2}$$

where C_2 is an effectivelly computable positive number depending only on P and s. The proof of (1) was based on a result of Stewart [15] which asserts that for $n > C_1$, the Lucas and Lehmer numbers u_n always have a primitive prime divisor. To prove (2), we reduced the problem to Thue–Mahler equations and used the bound available at that time for the solutions of such equations. Later, in [5], I made C_2 completely explicit by means of an explicit and improved bound from [4] on the solutions of Thue–Mahler equations. As a consequence, I showed in [5] that if u_n is a Lucas or Lehmer number with $n > 6$ and $|u_n| > \exp\exp\{4C_1^3 \log C_1\}$ then

$$4sP^2 \log P > \log\log|u_n| \tag{3}$$

and

$$P > \frac{1}{2}(\log\log|u_n|)^{1/3}, \tag{4}$$

where $P = P(u_n)$ and $s = \omega(u_n)$. Here $P(u_n)$ and $\omega(u_n)$ signify the greatest prime factor and the number of distinct prime factors of u_n (with the convention that $P(\pm 1) = 1, \omega(\pm 1) = 0$).

As is known, there are various lower bounds for $P(u_n)$ in terms of n, valid for all or "almost all" n, see e.g. [3], [16], [12], [14], [13], [8], [17] and the references given there. However, these estimates do not imply (3) and (4), because the lower bounds in (3) and (4) depend on u_n and not on n. Theorem 2 of [8] gives also a lower bound of the form

$$c(\log\log|u_n|)^2 \log\log\log|u_n|, \text{ if } |u_n| > c'.$$

for $P(u_n)$. In contrast with (4), the constants c, c' depend, however, on α, β and S as well.

Recently, Bilu, Hanrot and Voutier [1] significantly improved Stewart's result [15] by showing that for $n > 30$, u_n has a primitive prime divisor. This will enable us to prove (1) with C_1 replaced by 30. Furthermore, in 1998 I succeeded (cf. [6]) to improve upon the previous bound of [4] on the solutions of Thue–Mahler equations, that is, in another formulation, on the S-integral solutions of Thue equations. Using

this improvement from [6] and following the arguments of [5], we shall derive (2) with an explicit bound C_2 which is much better than the previous one in [5]. As a consequence, we obtain also some improvements of (3) and (4).

Keepeng the above notation, let $\varphi(n)$ denote Eurler's function.

Theorem. *Let u_n be a Lucas number or a Lehmer number defined as above with $n > 6$. If $u_n \in S$ then*

$$n \leq \max\{30, P+1\}. \tag{5}$$

Further,

$$\max\{|\alpha|, |\beta|, |u_n|\}$$

is bounded above by

$$\exp\{(k(s+1))^{9k(s+2)} P^k (\log P)^{sk+2}\}, \tag{6}$$

where $k = \varphi(n)/2$.

The inequality (5) is a significant improvement of (1), while (6) improves upon considerably (3) of [5].

From (5) and (6) we deduce the following improvements of (3) and (4).

Corollary. *Let u_n be a Lucas or a Lehmer number with $n > 30$, or with $30 \geq n > 6$ and $|u_n| > \exp\exp\{7040\}$. Then we have*

$$9(s+2)P \log P > \log\log|u_n| \tag{7}$$

and

$$P > \frac{1}{4}(\log\log|u_n|)^{1/2}, \tag{8}$$

where $P = P(u_n)$ and $s = \omega(u_n)$.

2. Proofs

Proof of the Theorem. We follow the proof of Theorem 1 of [5]. Let $u_n \in S$ be a Lucas number or a Lehmer number with $n > 6$. Then (5) follows in the same way as (1) was proved in [7] if we raplace Stewart's result [15] by the above-mentioned theorem of Bilu, Hanrot and Voutier [1] on primitive prime divisors.

To prove (6), we first introduce some notation. Put $\alpha\beta = B$ and $\alpha + \beta = A$ or $(\alpha+\beta)^2 = A$ according as u_n is a Lucas or a Lehmer number. Setting $\alpha^2 + \beta^2 = E$, we get $E = A^2 - 2B$ or $E = A - 2B$ and $\gcd(E, B) = 1$.

Denote by $\Phi_d(x,y)$ the d-th cyclotomic polynomial in homogeneous form. Then we have

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{\substack{d|n \\ d>1}} \Phi_d(\alpha,\beta), \text{ if } n > 0,$$

or

$$u_n = \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} = \prod_{\substack{d|n \\ d\geq 3}} \Phi_d(\alpha,\beta), \text{ if } n \text{ is even.}$$

If $\zeta = e^{2\pi i/d}$ and $d \geq 3$, then

$$\Phi_d(\alpha,\beta) = F_d(E,B),$$

where

$$F_d(z,1) = \prod_{\substack{\gcd(t,d)=1 \\ 1\leq t<d/2}} (z - (\zeta^t + \zeta^{-t})) \tag{9}$$

is an irreducibile polynomial of degree $\varphi(d)/2$ with coefficients from $\mathbf{Z}$. We infer now in both cases that there are non-negative integers $z_1, \ldots, z_s$ such that

$$G(E,B) = \prod_{\substack{d|n \\ d\geq 3}} F_d(E,B) = \pm p_1^{z_1} \cdots p_s^{z_s}. \tag{10}$$

Here $G(x,y)$ is a homogeneous polynomial with coefficients from $\mathbf{Z}$. Further, in view of $n > 6$, the degree of G, denoted by g, satisfies

$$3 \leq g \leq \frac{n-1}{2}.$$

We note that $G(x,y)$ is not irreducibile in general, but its linear factors over $\bar{\mathbf{Q}}$ are pairwise linearly independent. Putting

$$z_i = gz_i' + z_i'' \text{ with integers } z_i' \geq 0, 0 \leq z_i'' < g, 1 \leq i \leq s,$$

and

$$D = p_1^{z_1'} \cdots p_s^{z_s'}, b = \pm p_1^{z_1''} \cdots p_s^{z_s''},$$

(10) implies

$$G\left(\frac{E}{D}, \frac{B}{D}\right) = b \tag{11}$$

which can be regarded as a Thue equation in the S-integers $\frac{E}{D}, \frac{B}{D}$.

We apply *) now Theorem 1 of [6] with $m = 2$ to equation (11). Denote by $K = K_n$ the maximal real subfield of the n-th cyclotomic field. Its degree is $k = \varphi(n)/2$. Let h_K, R_K, D_K and R_S be the class number, regulator, discriminant and $S-$regulator (for its definition see e.g. [6]) of K. Further, we write $\log^* \alpha$ for $\max\{\log \alpha, 1\}$. Then using Theorem 1 of [6], one can deduce the estimate

$$\begin{aligned} &\max(|E|, |B|) < \exp\{c_1 P^k R_S (\log^* R_S). \\ &(\log^*(PR_S)/\log^* P)(R_K + h_K \log Q + 2g + \log|b|)\}, \end{aligned} \tag{12}$$

where

$$c_1 = n(k(s+1))^{8ks+9k+11}.$$

As is known, (see e.g. [6])

$$\log^*(PR_S)/\log^* P \le 2\log^* R_S \text{ and } R_S \le h_K R_K (k^s W)^k,$$

where $W = (\log p_1) \cdots (\log p_s)$. Further, we use as in [5] that

$$h_K R_K < 4|D_K|^{1/2} (\log|D_K|)^{k-1}$$

and

$$R_K \ge 0.373, \quad |D_K| \le n^k.$$

For $n \ge 3$, we also have (cf. [10]),

$$n/\varphi(n) < e^\gamma \log\log n + 5/(2\log\log n),$$

where γ denotes Euler's constant.
Finally, we have

$$\log Q \le s \log P \text{ and } \log|b| \le gs \log P.$$

Now it is easy to verify that (12) gives the bound (6) for $\max\{|\alpha|, |\beta|, |u_n|\}$.

Proof of the Corollary. First suppose that $k \le P/2$. In view of $k \le \frac{n-1}{2}$ and (5), this is always the case if $n > 30$. In this case (7) can be easily deduced from (6) by using

$$s \le 1.25506 P/\log P \text{ for } s \ge 1 \tag{13}$$

(cf. [10]). Further, one can easily check that

$$s + 2 \le 1.777777 P/\log P \text{ if } 1 \le s \le 7. \tag{14}$$

*) We remark that in case of $\phi(n)/2 \ge 3$, i.e. except for the cases n=8,10,12,(10) could also be reduced to an irreducibile Thue–Mahler equation to which a recent theorem of Bugeaud and the author [2] also applies.

Now using (13) if $s \geq 8$ and (14) if $1 \leq s \leq 7$, we get from (7) the estimate (8).

Next suppose that $P/2 < k$. Then, by (5), it follows that $n \leq 30$ and hence $k \leq 14$. This gives $P \leq 23$ and so $s \leq 9$. Now we infer from (6) that $\log\log|u_n| \leq 7040$. Hence, if $6 < n \leq 30$ and

$$|u_n| > \exp\exp\{7040\},$$

then we must have $k \leq P/2$ and, as was proved above, (7) and (8) follow.

References

[1] Bilu, Yu., Hanrot, G. and Voutier, P. M., Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.*, **539**, (2001), 75–122.

[2] Bugeaud, Y. and Győry, K., Bounds for the solutions of Thue–Mahler equations and norm form equations, *Acta Arithmetica*, **74**, (1996), 273–292.

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

[4] Győry, K., Explicit upper bounds for the solutions of some diophantine equations, *Ann. Acad. Sci. Fenn. Ser. A. I. Math.*, **5**, (1980), 3–12.

[5] Győry, K., On some arithmetical properties of Lucas and Lehmer numbers, *Acta Arithmetica*, **40**, (1982), 369–373.

[6] Győry, K., Bounds for the solutions of decomposable form equations, *Publ. Math. Debrecen*, **52**, (1998), 1–31.

[7] Győry, K., Kiss, P. and Schinzel, A., On Lucas and Lehmer sequences and their applications to diophantine equations, *Colloqu. Math.*, **45**, (1981), 75–80.

[8] Győry, K., Mignotte, M. and Shorey, T. N., On some arithmetical properties of weighted sums of S-units, *Math. Pannonica*, **1**/2, (1990), 25–43.

[9] Robin, G., Estimation de la fonction de Tchebycheff Θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$, nombre de diviseurs premiers de n, *Acta Arithmetica*, **42**, (1983), 367–389.

[10] Rosser, J. B. and Schoenfeld, L., Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6**, (1962), 64–94.

[11] Rosser, J. B. and Schoenfeld, L., Sharper bounds for the Chebyshev functions $\Theta(x)$ and $\Psi(x)$, *Math. Comp.*, **29**, (1975), 243–296.

[12] Schinzel, A., The intrinsic divisors of Lehmer numbers in the case of negative discriminant, *Arkiv Mat.*, **4**, (1962), 413–416.

[13] Shorey, T. N. and Stewart, C. L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers II., *J. London Math. Soc.*, **23**, (1981), 17–23.

[14] Stewart, C. L., On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, *Proc. London Math. Soc.*, **24**, (1977), 425–447.

[15] Stewart, C. L., *Primitive divisors of Lucas and Lehmer numbers,* In: *Transcendence theory: Advances and applications*, Acad. Press, London, New York, San Francisco, 1977, 79–92.

[16] Ward, M., The intrinsic divisors of Lehmer numbers, *Annals of Math.*, (2), **62**, (1955), 230–236.

[17] Kunrui, Yu. and Ling-kei Hung., On binary recurrence sequences, *Indag. Math. N. S.*, **6** (3), (1995), 341–354.

Kálmán Győry
Number Theory Research Group of the
Hungarian Academy of Sciences,
Institute of Mathematics
University of Debrecen
H–4010 Debrecen P.O. Box 12.
Hungary
e-mail: gyory@math.klte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 75–86*

REPRESENTATION OF SOLUTIONS OF PELL EQUATIONS USING LUCAS SEQUENCES

James P. Jones (Calgary, Canada)

Dedicated to the memory of Professor Péter Kiss

Abstract. We consider classes of Pell equations of the form $x^2-dy^2=c$ where $d=a^2\pm 4$ or $d=a^2\pm 1$ and $c=\pm 4$ or $c=\pm 1$. We show that all the solutions are expressible in terms of Lucas sequences and we give the Lucas sequences which solve the equations explicitly.

AMS Classification Number: 11B39, 11B37

1. Introduction

The purpose of this paper is to collect together results concerning the solutions of the Pell equations $x^2-(a^2\pm 4)y^2=\pm 4$, $x^2-(a^2\pm 4)y^2=\pm 1$, $x^2-(a^2\pm 1)y^2=\pm 4$ and $x^2-(a^2\pm 1)y^2=\pm 1$. We show that the solutions to these Pell equations can all be expressed in terms of Lucas sequences $U_n(a,\pm 1)$ and $V_n(a,\pm 1)$ of E. Lucas [20], [21].

The solutions of the Pell equations $x^2-(a^2+4)y^2=\pm a$, $x^2-(a^2-4)y^2=5-2a$, $x^2-(a^2-4)y^2=2-a$ and $x^2-(a^2-1)y^2=2-2a$ can also be represented as Lucas sequences. This is more difficult to prove however and will be shown in a subsequent paper.

The above Pell equations are important to logicians since the sequences of solutions have many elegant divisibility properties which make them useful for diophantine representation of recursively enumerable sets. The above mentioned Pell equations can be found in the papers Y. Matiyasevich [22], [25], M. Davis [1], J. Robinson [26], [27], [28], M. Davis, H. Putnam, J. Robinson [3] and Davis, Matiyasevich and Robinson [2]. Also in the author's papers [4], [5], [6], [7], and in Jones and Matiyasevich [8], [10]. The above Pell equations also have application to the problem of singlefold diophantine representation of recursively enumerable sets. See Matiyasevich [25] for an explanation, also the paper of Sun Zhiwei [29] and Jones and Matiyasevich [8], [9].

Let A and B be integers with $A\geq 1$ and $B=\pm 1$. Put $D=A^2-4B$. The Pell equation,

$$V^2-DU^2=\pm 4, \tag{1}$$

is closely connected with the Lucas identity,

$$V_n^2 - DU_n^2 = 4B^n \tag{2}$$

which is satisfied by the Lucas sequences U_n and V_n. In the theory developed by E. Lucas [20], [21] and D. H. Lehmer [18], [19], the sequences $U_n = U_n(A, B)$ and $V_n = V_n(A, B)$ satisfying equation (2) are definable as second order linear recurrences:

$$V_0 = 2,\ V_1 = A,\ V_{n+2} = AV_{n+1} - BV_n, \tag{3}$$

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = AU_{n+1} - BU_n. \tag{4}$$

The Lucas sequences V_n and U_n satisfy a large number of other identities as well. We shall need:

$$(i)\ \ 2V_{n+1} = AV_n + DU_n, \qquad (ii)\ \ 2U_{n+1} = AU_n + V_n, \tag{5}$$

$$(i)\ \ 2BV_{n-1} = AV_n - DU_n, \qquad (ii)\ \ 2BU_{n-1} = AU_n - V_n. \tag{6}$$

The above four identities are easy to derive, by induction on n, from the recurrence equations (3) and (4). Using identity (5) (i) it is then easy to show that U_n and V_n satisfy the Lucas identity (2). For plainly $V_n^2 - DU_n^2 = 4B^n$ holds for $n = 0$. Suppose it holds for n. By (5) (i),

$$4V_{n+1}^2 - 4DU_{n+1}^2 = (AV_n + DU_n)^2 - D(AU_n + V_n)^2$$

$$= A^2V_n^2 + D^2U_n^2 - DA^2U_n^2 - DV_n^2 = (A^2 - D)V_n^2 - (A^2 - D)DU_n^2$$

$$= 4BV_n^2 - 4BDU_n^2 = 4B(V_n^2 - DU_n^2) = 4B4B^n = 16B^{n+1}.$$

Hence the Lucas identity (2) holds for $n + 1$ and so by induction (2) holds for all $n \geq 0$.

One of the main theorems we shall need is that all solutions of $V^2 - DU^2 = \pm 4$ are given by the Lucas sequences $V = V_n(A, B)$ and $U = U_n(A, B)$. And we shall need to know exactly for which pairs (A, B) this holds. We therefore give a careful proof and an exact statement. We will prove the theorem in the following form:

Theorem 1.1. *Suppose $D = A^2 - 4B$, $B = 1$ and $3B + 5 \leq 2A$. Then for all nonnegative integers U and V,*

$$V^2 - DU^2 = \pm 4 \iff (\exists n \geq 0)[V = V_n(A, B) \text{ and } U = U_n(A, B)]$$

Before giving the proof we mention that the purpose of the hypothesis $3B+5 \leq 2A$ is to exclude some pairs such as $B = 1$ and $A = 3$ for which the theorem does not hold, yet include others such as $B = -1$ and $A = 1$ for which it does hold. If $B = 1$ and $A = 3$, then $D = 5$. $x^2 - 5y^2 = -4$ has infinitely many nonnegative integer solutions (x, y). But they are not all of the form $x = V_n(3, 1)$ and $y = U_n(3, 1)$. For example the solution $(x, y) = (1, 1)$ is not of the form $x = V_n(3, 1)$ and $y = U_n(3, 1)$. Rather $x = V_n(1, -1)$ and $y = U_n(1, -1)$ where $n = 1$. (x, y) lies within the Fibonacci sequence.

Care is therefore necessary in the statement of Theorem 1.1. Not only can Theorem 1.1 fail to hold when $B = 1$ and $A = 3$, the result can fail to hold when we try to generalize it beyond $|B| = 1$. Consider for example the case of $B = 2$. If $A = 4$, then $D = A^2 - 4B = 8$. Now $V = 20$ and $U = 7$ is a solution of $V^2 - 8U^2 = 4B^1$. But $\forall n$ $20 \neq V_n(4, 2)$ and $\forall n$ $7 \neq U_n(4, 2)$. Thus Theorem 1.1 does not hold for $B = 2$ and $A = 4$.

2. Descent

Our main tool in the proof we shall give here of Theorem 1.1 will be Fermat's method of descent. We will apply the method to equation (1). We will need the following lemmas:

Lemma 2.1. (Parity Lemma) *Suppose A is a positive integer and $|B| = 1$.*
If A is even: $V_n(A, B)$ is even, and $U_n(A, B)$ is even iff $2|n$.
If A is odd: $V_n(A, B) \equiv U_n(A, B) \pmod 2$, and $V_n(A, B)$ and $U_n(A, B)$ are even iff $3|n$.

Proof. By induction on n using equations (3) and (4).

Lemma 2.2. *For all $n \geq 0$, $V_{2n}(1, -1) = V_n(3, +1)$ and $U_{2n}(1, -1) = U_n(3, +1)$, $(n = 0, 1, 2, \ldots)$.*

Proof. The proof of this for V_n is the same as that for U_n so we shall give only the proof for U_n. For this we use induction on n. If $n = 0$ or $n = 1$, then $U_{2n}(1, -1) = U_n(3, 1)$ and $U_{2(n+1)}(1, -1) = U_{n+1}(3, 1)$. Suppose these hold for n and $n+1$. By (4), $U_{2(n+2)}(1, -1) = U_{2n+4}(1, -1) = U_{2n+3}(1, -1) + U_{2n+2}(1, -1) =$
$U_{2n+2}(1, -1) + U_{2n+1}(1, -1) + U_{2n+2}(1, -1) =$
$U_{2n+2}(1, -1) + U_{2n+2}(1, -1) - U_{2n}(1, -1) + U_{2n+2}(1, -1) =$
$3U_{2n+2}(1, -1) - U_{2n}(1, -1) = 3U_{2(n+1)}(1, -1) - U_{2n}(1, -1) =$
$3U_{n+1}(3, 1) - U_n(3, 1) = U_{n+2}(3, 1)$.

Lemma 2.3. *Let A and V be non-negative integers. Then*
If $V^2 - A^2 = +8$, then $A = 1$ and $V = 3$.

If $V^2 - A^2 = -8$, then $A = 3$ and $V = 1$.

Proof. $1 \le |V^2 - A^2| \le 8 \ \Rightarrow 1 \le |V - A|(V + A) \le 8 \ \Rightarrow 1 \le V + A \le 8$. Hence, if $V^2 - A^2 = +8$, then $A = 1$ and $V = 3$. If $V^2 - A^2 = -8$, then $A = 3$ and $V = 1$.

Lemma 2.4.

(Descent Lemma) Suppose $D = A^2 - 4B$, $B = \pm 1$, $B + 2 \le A$ and U and V are integers such that $0 \le V$, $2 \le U$ and $V^2 - DU^2 = \pm 4$. If V' and U' are defined by

$$(7) \qquad (i) \ \ V' = \frac{AV - DU}{2B}, \qquad (ii) \ \ U' = \frac{AU - V}{2B},$$

then V' and U' are integers and satisfy $V'^2 - DU'^2 = \pm 4B$. Also V' and U' satisfy

$$(8) \qquad (i) \ \ 2V = AV' + DU, \qquad (ii) \ \ 2U = AU' + V'.$$

Furthermore $1 \le V'$ and $1 \le U' < U$.

Proof. First we show that $2U \le V$. Since $D = A^2 - 4B$, $B = \pm 1$ and $B + 2 \le A$, $5 \le D$. Since $2 \le U$ we have $4 \le U^2$ and so $4U^2 \le 5U^2 \pm 4 \le DU^2 \pm 4 = V^2$. Therefore $2U \le V$.

Next we show that V' and U' are integers. $D = A^2 - 4B \Rightarrow D \equiv A^2 \equiv A \pmod 2$. Also $V^2 - DU^2 = \pm 4 \Rightarrow V^2 \equiv A^2U^2 \pmod 2 \Rightarrow V \equiv AU \pmod 2$. Hence $AU - V \equiv 0 \pmod 2$ and so U' is an integer. Also since $V \equiv AU \pmod 2$ and $D \equiv A \pmod 2$, $AV - DU \equiv A^2U - AU \equiv AU - AU = 0 \pmod 2$ so V' is an integer.

Next we show that $(V')^2 - D(U')^2 = \pm 4B$. From the definitions of V' and U' we have

$$V'^2 - DU'^2 = \frac{(AV - DU)^2}{4B^2} - D\frac{(AU - V)^2}{4B^2} =$$

$$\frac{A^2V^2 - DV^2 - DA^2U^2 + D^2U^2}{4B^2} =$$

$$\frac{(A^2 - D)(V^2 - DU^2)}{4B^2} = \frac{(4B)(\pm 4)}{4B^2} = \frac{\pm 4}{B} = \pm 4B.$$

Next we show that $2V = AV' + DU'$ and $2U = AU' + V'$. From the definitions of V' and U',

$$AV' + DU' = A\frac{AV - DU}{2B} + D\frac{AU - V}{2B} = \frac{A^2V - DV}{2B} = \frac{V(A^2 - D)}{2B} = \frac{V4B}{2B} = 2V.$$

Also

$$AU' + V' = A\frac{AU - V}{2B} + \frac{AV - DU}{2B} = \frac{A^2U - DU}{2B} = \frac{U(A^2 - D)}{2B} = \frac{U4B}{2B} = 2U.$$

Next we show that $1 \le U' < U$. $V^2 - DU^2 = \pm 4 \Rightarrow (A^2 - 4B)U^2 - V^2 = \mp 4 \Rightarrow A^2U^2 - V^2 = 4BU^2 \mp 4 \Rightarrow (AU - V)(AU + V) = 4B(U^2 \mp B)$. Since $2BU' = AU - V \Rightarrow 2BU'(AU + V) = 4B(U^2 \mp B) \Rightarrow U'(AU + V) = 2(U^2 \mp B) = 2U^2 \mp 2B$, we have

$$\frac{2U^2 - 2}{AU + V} \le U' = \frac{2U^2 \mp 2B}{AU + V} \le \frac{2U^2 + 2}{AU + V} \le \frac{2U^2 + 2}{U + V}, \tag{9}$$

using $B + 2 \le A \Rightarrow 1 \le A$. Since $2 \le U \Rightarrow 2 < 2U^2 \Rightarrow 0 < 2U^2 - 2$, equation (9) $\Rightarrow 0 < U'$. Hence $1 \le U'$. Now we can show $U' < U$. Using $2U \le V$, shown earlier, $2U \le V \Rightarrow 3U \le U + V$. Also $2 \le U \Rightarrow 2 < U^2$. Hence by (9),

$$U' \le \frac{2(U^2 + 2)}{U + V} \le \frac{2U^2 + 2}{3U} \le \frac{2U^2 + U^2}{3U} = U. \tag{10}$$

Therefore $U' < U$. Finally we can show that $1 \le V'$. Since $V' = (AV - DU)/2B$, we have

$$UV' = \frac{AUV - DU^2}{2B} = \frac{AUV - V^2 \pm 4}{2B} = \frac{AUV - V^2}{2B} \pm 2B = VU' \pm 2B. \tag{11}$$

Since $1 \le U'$ and $4 \le 2U \le V$, we have $2 \le 4 \pm 2B \le 2U \pm 2B \le 2UU' \pm 2B \le VU' \pm 2B = UV'$ by (11). Hence $2 \le UV'$ and so $1 \le V'$. This completes the proof of the Descent Lemma.

Proof of Theorem 1.1. Suppose $3B + 5 \le 2A$. In the direction $\Leftarrow$ Theorem 1.1 has already been proven by our establishing identity (2). For the direction $\Rightarrow$ we use the Descent Lemma and induction on U. Suppose $0 \le U$, $0 \le V$ and $V^2 - DU^2 = \pm 4$. If $U = 0$, then $V^2 = \pm 4 \Rightarrow V^2 = 4 \Rightarrow V = 2$ and so we can let $n = 0$. Suppose $U = 1$. Then $V^2 - DU^2 = \pm 4 \Rightarrow V^2 - (A^2 - 4B) = \pm 4 \Rightarrow V^2 - A^2 = \pm 4 - 4B$. We consider two cases:

Case 1. $B = -1$. Here we have $V^2 - A^2 = 0$ or $V^2 - A^2 = 8$. If $V^2 - A^2 = 0$, then $V = A$ and so we can let $n = 1$ since $V_1(A, B) = A = V$ and $U_1(A, B) = 1 = U$. If $V^2 - A^2 = 8$, then by Lemma 2.3, $A = 1$ and $V = 3$ so we can let $n = 2$ since $V_2(A, B) = A^2 - 2B = 3 = V$ and $U_2(A, B) = A = 1 = U$.

Case 2. $B = +1$. Here $V^2 - A^2 = 0$ or $V^2 - A^2 = -8$. If $V^2 - A^2 = -8$, then by Lemma 2. 3, $A = 3$ and $V = 1$. Since $B = 1$, $A = 3$ contradicts $3B + 5 \le 2A$. Hence $V^2 - A^2 = 0$. In this case $V = A$ and so we can let $n = 1$ since $V_1(A, B) = A = V$ and $U_1 = 1 = U$.

Now we can suppose $2 \le U$ and that the implication $\Rightarrow$ of Theorem 1. 1 holds for all pairs V', U' such that $0 \le U' < U$ and $0 \le V'$. Since $B = \pm 1$, the hypothesis $3B + 5 \le 2A$ implies $B + 2 \le A$ and so we can apply the Descent lemma. Define V' and U' from V and U as indicated in the Descent Lemma: $V' = (AV - DU)/2B$ and $U' = (AU - V)/2B$. The Descent Lemma then asserts

that V' and U' are integers, $1 \leq V'$, $1 \leq U' < U$ and $V'^2 - DU'^2 = \pm 4$. Hence by the induction hypothesis $\exists n \geq 0$ such that $V' = V_n(A, B)$ and $U' = U_n(A, B)$. Consequently using equations (8) in the Descent Lemma and identity (5) (i) we have, $2V = AV' + DU' = AV_n + DU_n = 2V_{n+1}$ and so $V = V_{n+1}$. By (8) and identity (5) (ii) we also have $2U = AU' + V' = AU_n + V_n = 2U_{n+1}$ and so $U = U_{n+1}$. Thus the implication $\Rightarrow$ holds for U. By induction the implication $\Rightarrow$ holds for all U. Thus Theorem 1. 1 is proved.

Corollary 2.5. *If $4 \leq A$, $B = 1$, $D = A^2 - 4$, then $V^2 - DU^2 = -4$ has no solutions U, V.*

Proof. Of course this follows immediately from Theorem 1. 1 and Lucas Identity (2). But there is a more interesting proof using the Descent Lemma: Suppose $4 \leq A$, $B = +1$ and $D = A^2 - 4$. Then $B + 2 \leq A$ so we can use the Descent Lemma. Suppose $V^2 - DU^2 = -4$ for some V, U. Let (V, U) be the pair with smallest U such that $0 \leq V$ and $0 \leq U$. Then $U \neq 0$. By Lemma 2. 3, $U = 1$ would imply $A = 3$. Hence $2 \leq U$ and so by the Descent Lemma $\exists V'$, U' such that $1 \leq V'$, $1 \leq U' < U$ and $V^2 - DU^2 = -4$. But this contradicts the original choice of U and V. Thus V and U such that $V^2 - DU^2 = -4$ do not exist.

Remark. If $A = 3$, then $V^2 - (A^2 - 4)U^2 = -4$ does have solutions, e.g. $V = 1$ and $U = 1$.

Corollary 2.6. *If $4 \leq A$, then $x^2 - (a^2 - 4)y^2 = -4$ has no solutions.*

Corollary 2.7. *If $4 \leq A$, then all solutions of $x^2 - (a^2 - 4)y^2 = +4$ are given by $x = V_i(a, +1)$ and $y = U_i(a, +1)$, $(i = 0, 1, 2, \ldots)$.*

Corollary 2.8. *If $1 \leq A$, then all solutions of $x^2 - (a^2 + 4)y^2 = -4$ are given by $x = V_{2i+1}(a, -1)$ and $y = U_{2i+1}(a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Corollary 2.9. (Matiyasevich equation [22]) *If $1 \leq A$, then all solutions of $x^2 - (a^2 + 4)y^2 = +4$ are given by $x = V_{2i}(a, -1)$ and $y = U_{2i}(a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Remark. In [22] Y. V. Matiyasevich used the above equation $x^2 - (a^2 + 4)y^2 = 4$ with $a = 1$, to solve Hilbert's Tenth Problem. (I.e. he used the sequence of Fibonacci numbers with even subscripts, $U_{2i}(1, -1) = U_i(3, 1)$.)

3. Solutions of Pell equations with $d = a^2 \pm 4$ and $c = \pm 1$.

In this section we give the solutions of Pell equations of the form $x^2 - (a^2 \pm 4)y^2 = \pm 1$.

Lemma 3.1. *If $4 \leq a$, then $x^2 - (a^2 - 4)y^2 = -1$ has no solutions.*

Proof. Suppose $4 \leq a$ and $x^2 - (a^2 - 4)y^2 = -1$. Multiplying by 4 we obtain $(2x)^2 - (a^2 - 4)(2y)^2 = -4$, which, since $4 \leq a$, has no solutions by Corollary 2.6.

Remark. If $a = 3$, then $x^2 - (a^2 - 4)y^2 = -1$ has infinitely many solutions, $x = V_{6i+3}(1,-1)/2$ and $y = U_{6i+3}(1,-1)/2$, $(i = 0, 1, 2, \ldots)$. This is shown by the next theorem since $a^2 - 4 = 5 = 1^2 + 4$.

Theorem 3.2. *If $1 \leq a$ and a is odd, then all solutions of $x^2 - (a^2 + 4)y^2 = -1$ are given by $x = \frac{V_{6i+3}(a,-1)}{2}$ and $y = \frac{U_{6i+3}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

Proof. Using Corollary 2.8, since $1 \leq a$, we have $x^2 - (a^2 + 4)y^2 = -1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = -4 \iff 2x = V_n(a,-1)$ and $2y = U_n(a,-1)$ for some odd n. As a is odd, by the Parity Lemma $2|V_n(a,-1)$ and $2|U_n(a,-1) \iff 3|n$. $3|n$ and n is odd $\iff \exists i\ n = 6i + 3$, $(i = 0, 1, 2, \ldots)$.

Lemma 3.3. *For any even integer a, $x^2 - (a^2 + 4)y^2 = -1$ has no solutions.*

Proof. Suppose a is even. Then $4|a^2 \Rightarrow 4|a^2 - 4$. But $x^2 \neq -1 \pmod 4$.

Theorem 3.4. *If $4 \leq a$ and a is even, then all solutions of $x^2 - (a^2 - 4)y^2 = +1$ are given by $x = \frac{V_{2i}(a,+1)}{2}$ and $y = \frac{U_{2i}(a,+1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

Proof. Using Corollary 2.7, since $4 \leq a$, we have $x^2 - (a^2 - 4)y^2 = +1 \iff (2x)^2 - (a^2 - 4)(2y)^2 = +4 \iff \exists\, n \geq 0$, $2x = V_n(a,+1)$ and $2y = U_n(a,+1)$. Since $2|a$, the Parity Lemma implies $2|V_n(a,+1)$ and $2|U_n(a,+1) \iff 2|n$, i.e. $n = 2i$, $(i = 0, 1, 2, \ldots)$.

Theorem 3.5. *If $3 \leq a$ and a is odd, then all solutions of $x^2 - (a^2 - 4)y^2 = +1$ are given by $x = \frac{V_{3i}(a,+1)}{2}$ and $y = \frac{U_{3i}(a,+1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

Proof. Suppose $3 \leq a$ and a is odd. $x^2 - (a^2 - 4)y^2 = +1 \iff (2x)^2 - (a^2 - 4)(2y)^2 = +4$. If $3 < a$, then by Corollary 2.7, $2x = V_n(a,+1)$ and $2y = U_n(a,+1)$, where, by the Parity Lemma, $n = 3i$, $(i = 0, 1, 2, \ldots)$. If $3 = a$, then, since $a^2 - 4 = 5 = 1^2 + 4$, Corollary 2.9, $\Rightarrow 2x = V_{2j}(1,-1)$ and $2y = U_{2j}(1,-1)$, where $j = 3i$, $(i = 0, 1, 2, \ldots)$ by the Parity Lemma, so that $x = V_{6i}(1,-1)/2$ and $y = U_{6i}(1,-1)/2$, $(i = 0, 1, 2, \ldots)$. However by Lemma 2.2, $V_{6i}(1,-1) = V_{3i}(3,+1)$ and $U_{6i}(1,-1) = U_{3i}(3,+1)$, $(i = 0, 1, 2, \ldots)$ as required

Theorem 3.6. *If $2 \leq a$ and a is even, then all solutions of $x^2 - (a^2 + 4)y^2 = +1$ are given by $x = \frac{V_{2i}(a,-1)}{2}$ and $y = \frac{U_{2i}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

Proof. By Corollary 2.9, since $1 \leq a$, we have $x^2 - (a^2 + 4)y^2 = +1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = +4 \iff 2x = V_n(a,-1)$ and $2y = U_n(a,-1)$ for some even n. Since $2|a$ and n is even, the Parity Lemma implies $2|V_n(a,-1)$ and $2|U_n(a,-1)$.

Theorem 3.7. *If $1 \leq a$ and a is odd, then all solutions of $x^2 - (a^2 + 4)y^2 = +1$ are given by $x = \frac{V_{6i}(a,-1)}{2}$ and $y = \frac{U_{6i}(a,-1)}{2}$, $(i = 0, 1, 2, \ldots)$.*

Proof. By Corollary 2.9, since $1 \leq a$, we have $x^2 - (a^2 + 4)y^2 = +1 \iff (2x)^2 - (a^2 + 4)(2y)^2 = +4 \iff 2x = V_n(a,-1)$ and $2y = U_n(a,-1)$ for some even n. Since

a is odd, the Parity Lemma implies $2|V_n(a,-1)$ and $2|U_n(a,-1) \iff 3|n$. $2|n$ and $3|n \iff 6|n$. Hence $n = 6i$ $(i = 0, 1, 2, \ldots)$.

4. Solutions of Pell equations with $d = a^2 \pm 1$ and $c = \pm 1$.

In this section we consider solutions of Pell equations of the form $x^2 - (a^2 \pm 1)y^2 = \pm 1$.

Lemma 4.1. *If $2 \leq a$, then $x^2 - (a^2 - 1)y^2 = -1$ has no solutions.*

Proof. Suppose $2 \leq a$ and $x^2 - (a^2 - 1)y^2 = -1$. Multiplying by 4 we obtain $(2x)^2 - ((2a)^2 - 4)y^2 = -4$. Since $4 \leq 2a$, this equation has no solutions by Corollary 2. 6.

[Another proof is also possible. Let $d = a^2 - 1$. The continued fraction expansion of $\sqrt{d}$ is $\sqrt{d} = [a-1;\ \overline{1,\ 2a-2}]$ with period length 2 (even). Hence $x^2 - dy^2 = -1$ is unsolvable.]

Theorem 4.2. (Julia Robinson's equation [26], [27]) *If $2 \leq a$, then all solutions of $x^2 - (a^2 - 1)y^2 = +1$ are given by $x = \frac{V_i(2a,+1)}{2}$ and $y = U_i(2a, +1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Suppose $2 \leq a$. Using Corollary 2.7, since $4 \leq 2a$ we have $x^2 - (a^2 - 1)y^2 = +1 \iff (2x)^2 - ((2a)^2 - 4)y^2 = +4 \iff \exists\ n \geq 0,\ 2x = V_n(2a, +1)$ and $y = U_n(2a, +1)$. Since $2a$ is even, the Parity Lemma implies $V_n(2a, +1)$ is even. Hence $2|V_n(2a, +1)$.

Theorem 4.3. *If $1 \leq a$, then all solutions of $x^2 - (a^2 + 1)y^2 = +1$ are given by $x = \frac{V_{2i}(2a,-1)}{2}$ and $y = U_{2i}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Using Corollary 2.9, since $1 \leq 2a$, we have $x^2 - (a^2 + 1)y^2 = +1 \iff (2x)^2 - ((2a)^2 + 4)y^2 = +4 \iff 2x = V_n(2a, -1)$ and $y = U_n(2a, -1)$ for some even n, $n = 2i$, $(i = 0, 1, 2, \ldots)$. Since $2a$ is even, the Parity Lemma implies $2|V_n(2a, -1)$.

Theorem 4.4. *If $1 \leq a$, then all solutions of $x^2 - (a^2 + 1)y^2 = -1$ are given by $x = \frac{V_{2i+1}(2a,-1)}{2}$ and $y = U_{2i+1}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Using Corollary 2.8, since $1 \leq 2a$, we have $x^2 - (a^2 + 1)y^2 = -1 \iff (2x)^2 - ((2a)^2 + 4)y^2 = -4 \iff 2x = V_n(2a, -1)$ and $y = U_n(2a, -1)$ for some odd n, $n = 2i + 1$, $(i = 0, 1, 2, \ldots)$. The Parity Lemma implies $2|V_n(2a, -1)$, since $2a$ is even.

5. Solutions of Pell equations with $d = a^2 \pm 1$ and $c = \pm 4$.

In this section we consider solutions of Pell equations of the form $x^2 - (a^2 \pm 1)y^2 = \pm 4$.

Lemma 5.1. *If $2 \leq a$, $a \neq 3$ and $x^2 - (a^2 - 1)y^2 = \pm 4$, then y is even.*

Proof. Let $d = a^2 - 1$. Suppose $2 \leq a$, $a \neq 3$ and $x^2 - dy^2 = \pm 4$. If a is even, then $4|a^2$ and so $d \equiv -1 \pmod 4$. Hence $x^2 - dy^2 = \pm 4 \Rightarrow x^2 + y^2 \equiv 0 \pmod 4 \Rightarrow y \equiv x \equiv 0 \pmod 2$. Therefore we can suppose a is odd and $5 \leq a$. Then $4|d$ and so x is even. Suppose y is odd, and without loss of generality that y is the least such odd $y > 0$. Since $3 < a$, $(a-1)^2 < a^2 - 5 < a^2 + 3 < (a+1)^2$. Hence $d \pm 4$ is not a square and so $y \neq 1$. Therefore $2 < y$. Let $x' = ax - dy$ and $y' = ay - x$. Then

$$x'^2 - dy'^2 = (ax - dy)^2 - d(ay - x)^2 = (a^2 - d)x^2 - d(a^2 - d)y^2 = x^2 - dy^2 = \pm 4.$$

Hence (x', y') is also a solution. Since x is even and a and y are both odd, y' is odd. Now $5 \leq a$ and $2 < y \Rightarrow 2y^2(1-a) < \pm 4 < y^2 \iff$

$$2y^2 - 2ay^2 < \pm 4 < y^2 \iff y^2 - 2ay^2 < -y^2 \pm 4 < 0 \iff$$
$$a^2y^2 - 2ay^2 + y^2 < a^2y^2 - y^2 \pm 4 < a^2y^2 \iff$$
$$(a^2 - 2a + 1)y^2 < (a^2 - 1)y^2 \pm 4 < a^2y^2 \iff$$
$$(a-1)^2y^2 < x^2 < a^2y^2 \iff (a-1)y < x < ay \iff$$

$0 < ay - x < y \iff 0 < y' < y$. But since $x'^2 - dy'^2 = \pm 4$ and y' is odd, this contradicts the choice of y. Hence no such odd y exists.

Lemma 5.2. *If $1 \leq a$, $a \neq 2$ and $x^2 - (a^2 + 1)y^2 = \pm 4$, then y is even.*

Proof. Let $d = a^2 + 1$. Suppose $1 \leq a$, $a \neq 2$ and $x^2 - dy^2 = \pm 4$. If a is odd, then $a^2 \equiv 1 \pmod 4$ and so $d \equiv 2 \pmod 4$. Hence $x^2 - dy^2 = \pm 4 \Rightarrow x^2 + 2y^2 \equiv 0 \pmod 4 \Rightarrow y \equiv x \equiv 0 \pmod 2$. Consequently we can suppose a is even and since $a \neq 2$, that $4 \leq a$. Suppose y is odd and y is the least such odd $y > 0$. Since d is odd and y is odd, x must be odd. Since $2 < a$, $(a-1)^2 < a^2 - 3 < a^2 + 5 < (a+1)^2$ so that $d \pm 4$ is not a square and hence $y \neq 1$. Thus $2 < y$. Put $x' = dy - ax$ and $y' = x - ay$. As in the proof of Lemma 5.1, $x'^2 - dy'^2 = \pm 4$. Since $y' = x - ay$, x is odd and a is even, y' is odd. Now $2 < a$ and $2 < y \Rightarrow -y^2 < \pm 4 < 2ay^2 \iff 0 < y^2 \pm 4 < 2ay^2 + y^2 \iff$

$$a^2y^2 < a^2y^2 + y^2 \pm 4 < a^2y^2 + 2ay^2 + y^2 \iff$$
$$a^2y^2 < (a^2 + 1)y^2 \pm 4 < (a+1)^2y^2 \iff$$
$$a^2y^2 < x^2 < (a+1)^2y^2 \iff ay < x < (a+1)y \iff$$

$0 < x - ay < y \iff 0 < y' < y$. But since $x'^2 - dy'^2 = \pm 4$ and y' is odd, this contradicts the choice of y. Hence no such odd y exists.

Theorem 5.3. *If $2 \leq a$ and $a \neq 3$, then all solutions of $x^2 - (a^2-1)y^2 = +4$ are given by $x = V_i(2a, +1)$ and $y = 2U_i(2a, +1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Suppose $2 \leq a$, $a \neq 3$ and $x^2 - (a^2-1)y^2 = +4$. By Lemma 5.l, $2|y$. Let $y = 2u$. $x^2 - (a^2-1)y^2 = +4 \iff x^2 - (a^2-1)4u^2 = +4 \iff x^2 - ((2a)^2-4)u^2 = +4 \iff x = V_i(2a, +1)$ and $u = U_i(2a, +1)$ for some i, by Corollary 2.7, since $4 \leq 2a$.

Theorem 5.4. *If $1 \leq a$ and $a \neq 2$, then all solutions of $x^2 - (a^2+1)y^2 = +4$ are given by $x = V_{2i}(2a, -1)$ and $y = 2U_{2i}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Suppose $1 \leq a$, $a \neq 2$ and $x^2 - (a^2+1)y^2 = +4$. By Lemma 5.2, $2|y$. Let $y = 2u$. $x^2 - (a^2+1)y^2 = +4 \iff x^2 - (a^2+1)4u^2 = +4 \iff x^2 - ((2a)^2+4)u^2 = +4 \iff x = V_{2i}(2a, -1)$ and $u = U_{2i}(2a, -1)$ for some i, $(i = 0, 1, \ldots)$, by Corollary 2.9, since $1 \leq 2a$.

Theorem 5.5. *If $1 \leq a$ and $a \neq 2$, then all solutions of $x^2 - (a^2+1)y^2 = -4$ are given by $x = V_{2i+1}(2a, -1)$ and $y = 2U_{2i+1}(2a, -1)$, $(i = 0, 1, 2, \ldots)$.*

Proof. Suppose $1 \leq a$, $a \neq 2$ and $x^2 - (a^2+1)y^2 = -4$. By Lemma 5.2, $2|y$. Let $y = 2u$. $x^2 - (a^2+1)y^2 = -4 \iff x^2 - (a^2+1)4u^2 = -4 \iff x^2 - ((2a)^2+4)u^2 = -4 \iff x = V_{2i+1}(2a, -1)$ and $u = U_{2i+1}(2a, -1)$ for some i, $(i = 0, 1, \ldots)$, by Corollary 2.8, since $1 \leq 2a$.

Theorem 5.6. *If $2 \leq a$ and $a \neq 3$, then $x^2 - (a^2-1)y^2 = -4$ has no solutions.*

Proof. Suppose $2 \leq a$, $a \neq 3$ and $x^2 - (a^2-1)y^2 = -4$. By Lemma 5.1, $2|y$. Let $y = 2u$. Then $x^2 - (a^2-1)y^2 = -4 \Rightarrow x^2 - (a^2-1)4u^2 = -4 \Rightarrow x^2 - ((2a)^2-4)u^2 = -4$. But this equation has no solutions by Corollary 2.6, since $4 \leq 2a$.

References

[1] Davis, M., Hilbert's tenth problem is unsolvable, *Amer. Math. Monthly*, **80** (1973), 233–269.

[2] Davis, M., Matijasevich, Y., V. and Robinson, J., Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution, Mathematical developments arising from Hilbert problems, *Proc. of Symposia in Pure Math.*, **28**, Amer. Math. Soc., Providence, Rhode Island, (1976), 323–378.

[3] Davis, M., Putnam, H. and Robinson, J., The decision problem for exponential diophantine equations, *Annals of Math.*, Series 2, **74** (1961), 425–436.

[4] Jones, J. P., Diophantine representation of the Fibonacci numbers, *Fibonacci Quarterly,* **13** (1975), 84–88.

[5] Jones, J. P., Satao, D., Wada, H. and Wiens, D., Diophantine representation of the set of prime numbers, *Amer. Math. Monthly*, **83** (1976), 449–464.

[6] Jones, J. P., Diophantine representation of Mersenne and Fermat primes, *Acta Arithmetica*, **35** (1979), 209–221.

[7] Jones, J. P., Universal diophantine equation, *Jour. Symbolic Logic*, **47** (1982), 549–571.

[8] Jones, J. P. and Matiyasevich, Y. V., A New Representation for the Symmetric Binomial Coefficient and its Applications, *Annales des Sciences Mathematiques du Quebec*, **6** (1982), 81–97.

[9] Jones, J. P. and Matiyasevich, Y. V., *Exponential Diophantine Representation of Recursively Enumerable Sets*, Proceedings of the Herbrand Symposium, Logic Colloquium 1981, Marseilles, France. Studies in Logic, Vol. 107, North Holland Publishers, Amsterdam, 1982, 159–177.

[10] Jones, J. P. and Matiyasevich, Y. V., Proof of recursive unsolvability of Hilbert's Tenth Problem, *Amer. Math. Monthly*, **98** (1991), 689–709.

[11] Kiss, P. and Jones, J. P., Some diophantine approximation results concerning second order linear recurrences, *Math. Slovaca*, **42** (1992), No. 5, 583–591.

[12] Jones, J. P. and Kiss, P., On points whose coordinates are terms of a linear recurrence, *Fibonacci Quarterly,* **31** (1993), 239–245.

[13] Jones, J. P. and Kiss, P., Some identities and congruences for a special family of second order recurrences, *Acta Academiae Paedagogicae Agriensis, New Series,* **23** (1995-96), 3–9.

[14] Jones, J. P. and Kiss, P., Some congruences concerning second order recurrences, *Acta Academiae Paedagogicae Agriensis, New Series*, **24** (1997), 29–33.

[15] Kiss, P. and Jones, J. P., Some new identities and congruences for Lucas sequences, *Discussiones Math.*, **18** (1998), 39–47.

[16] Kiss, P., A diophantine approximative property of second order linear recurrences, *Period. Math.*, **11** (1980), 281–287.

[17] Kiss, P., Diophantine representation of generalized Fibonacci numbers, *Elemente der Mathematik,* **34** (1979), 129–132.

[18] Lehmer, D. H., On the multiple solutions of the Pell Equation, *Annals of Math.*, **30** (1928), 66–72.

[19] Lehmer, D. H., An extended theory of Lucas functions, *Annals of Math*, **31** (1930), 419–448.

[20] Lucas, E., Sur les congruences des nombres euleriens et des coefficients differentiels des fonctions trigonom triques suivant un module premier, *Bulletin de la Societe Mathematique de France*, **6** (1877–78), 49–54.

[21] Lucas, E., Theorie des fonctions numeriques simplement periodiques, *Amer. Jour. of Math.*, **1** (1878), 184–240, 289–321. English translation: Fibonacci Association, Santa Clara University, 1969.

[22] Matiyasevich, Y. V., Enumerable sets are diophantine, *Doklady Akademii Nauk SSSR,* **191** (1970), 279–282 (Russian). English transl. Soviet Math. Doklady **11** (1970), 354–357.

[23] Yuri Matiyasevich and Julia Robinson, Reduction of an arbitrary diophantine equation to one in 13 unknowns, *Acta Arithmetica*, **27** (1975), 521–553.

[24] Yuri Matiyasevich, Algorithmic unsolvability of exponential diophantine equations in three unknowns, *Studies in the Theory of Algorithms and Mathematical Logic, Akad. Nauk.*, Moscow, (1979), 69–78.

[25] Yuri V. Matiyasevich, *Hilbert's Tenth Problem,* Foundations of Computing series, M. I. T. Press, Cambridge, Massachusetts, 1993.

[26] Julia Robinson, Existential definability in arithmetic, *Trans. Amer. Mathematical Society,* **72** (1952), 437–449.

[27] Julia Robinson, Diophantine decision problems, *Studies in Number Theory (W. J. LeVeque, ed.), MAA Studies in Mathematics*, **6** (1969), 76–116.

[28] Julia Robinson, Unsolvable diophantine problems, *Proc. Amer. Math. Soc.*, **22** (1969), 534–538.

[29] Sun Zhiwei, *Singlefold diophantine representation of the sequence* $u_0 = 0$, $u_1 = 1$ *and* $u_{n+2} = m \cdot u_{n+1} + u_n$, Pure and Applied Logic (Zhang Jinwen ed.), Beijing University Press, (1992), 97–101.

James P. Jones
University of Calgary
Department of Mathematics and Statistics
Calgary Alberta, T2N1N4 Canada
e-mail: jpjones@math.ucalgary.ca

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 87–100*

ON SOME RESEARCH PROBLEMS IN MATHEMATICS

Imre Kátai (Budapest, Hungary)

Dedicated to the memory of Professor Péter Kiss

I. Introduction

The problem presented here is originated during our joint research activity with Z. Daróczy and some others for the Rényi–Parry expansions [1–11].

Let $\mathbb{C}^\infty$ denote the space of sequences $\underline{c} = (c_0, c_1, \ldots)$ the coordinates c_ν of which are complex numbers. The shift operator $\sigma\colon \mathbb{C}^\infty \to \mathbb{C}^\infty$ is defined by

$$\sigma(\underline{c}) = (c_1, c_2, \ldots).$$

Let $t_0 = 1,\ t_\nu \in \mathbb{C} \quad (\nu = 1, 2, \ldots)$ be bounded, and $\underline{t} = (t_0, t_1, \ldots)$. We define

$$R(z) = t_0 + t_1 z + \cdots. \tag{1.1}$$

Let l_1 be the linear space of the sequences $\underline{b} \in \mathbb{C}^\infty$, for which $\sum |b_\nu| < \infty$ holds.

The scalar product of a bounded sequence $\underline{c}$ and a $\underline{b} \in \mathbb{C}^\infty$ is defined as

$$\underline{c}\,\underline{b} = \underline{b}\underline{c} = \sum_{\nu=0}^{\infty} b_\nu c_\nu.$$

Let

$$\mathcal{H}_{\underline{t}} = \left\{ \underline{b} \in l_1 \mid \sigma^l(\underline{b})\underline{t} = 0, \quad l = 0, 1, 2, \ldots \right\}. \tag{1.2}$$

It is clear that $\mathcal{H}_t$ is a closed linear subspace of l_1.

Let $\mathcal{H}_{\underline{t}}^{(0)} \subseteq \mathcal{H}_{\underline{t}}$ be the set of those $\underline{b} \in \mathcal{H}_t$ for which

$$|b_\nu| \le C(\varepsilon, \underline{b}) e^{-\varepsilon\nu} \quad (\nu \ge 0) \tag{1.3}$$

holds with suitable $\varepsilon > 0$ and $C(\varepsilon, \underline{b}) \quad (< \infty)$.

Financially supported by the Research Group of Applied Number Theory of HAS, and by OTKA T 031877.

If ρ is a root of $R(z)$, $|\rho|<1$, then $b_\nu=\rho^\nu$ satisfies $\sigma^l(\underline{b})\underline{t}=0 \quad (l=0,1,2,\dots)$ and even $|b_\nu|\le Ce^{-\varepsilon\nu}$, where ε can be defined from $e^{-\varepsilon}=|\rho|$, and $C=1$.

If ρ is a root of $R(z)$ of multiplicity m, then $b_\nu=\nu^j\rho^\nu \quad (\nu\ge 0)$ are solutions of $\sigma^l(\underline{b})\underline{t}=0 \quad (l\ge 0)$ for every $j=0,\dots,m-1$, furthermore (1.3) holds with suitable ε, and constant $C(\varepsilon,\underline{b})$. The sequences $b_\nu=\nu^j\rho^\nu \quad (\nu\ge 0)$ are called elementary solutions.

Let $\mathcal{H}_{\underline{t}}^{(e)}$ be the space of finite linear combinations of elementary solutions.

Let furthermore $\overline{\mathcal{H}}_t^{(e)}$ be the closure of $\mathcal{H}_t^{(e)}$.

It is obvious that $\overline{\mathcal{H}}_t^{(e)}\subseteq\mathcal{H}_t$.

Conjecture 1. $\overline{\mathcal{H}}_t^{(e)}=\mathcal{H}_t$.

Conjecture 2. *Assume that $R(z)\ne 0$ in $|z|<1$. Then $\mathcal{H}_{\underline{t}}=\{\underline{0}\}$.*

Theorem 1. *We have*

$$\mathcal{H}_{\underline{t}}^{(0)}=\mathcal{H}_{\underline{t}}^{(e)}.$$

Proof. $\mathcal{H}_{\underline{t}}^{(e)}\subseteq\mathcal{H}_{\underline{t}}^{(0)}$ obviously holds. We shall prove that $\mathcal{H}_t^{(0)}\subseteq\mathcal{H}_t^{(e)}$, i.e. that if $\sigma^l(\underline{b})\underline{t}=0 \quad (l=0,1,2,\dots)$, and

$$|b_\nu|<C(\underline{b},\varepsilon)\cdot e^{-\varepsilon\nu},$$

then there exist $\rho_1,\dots,\rho_k$ suitable roots of $R(z)$, $|\rho_s|\le 1/e^\varepsilon \quad (s=1,\dots,k)$ such that

$$b_\nu=\sum_{s=1}^{k}p_s(\nu)\rho_s^\nu \quad (\nu=0,1,2,\dots),$$

p_s are polynomials, $\deg p_s=m_s-1$, where m_s is the multiplicity of the root ρ_s for $R(z)$.

Let $\underline{b}$ be a solution of

$$\sigma^l(\underline{b})\underline{t}=0 \quad (l=0,1,2,\dots), \qquad |b_\nu|\le C(\varepsilon,\underline{b})\cdot e^{-\varepsilon\nu}. \tag{1.4}$$

Let furthermore $\rho_1,\dots,\rho_p$ be all the roots of $R(z)$ in the disc $|z|<\dfrac{1}{e^\varepsilon}+\varepsilon_1$, where ε_1 is an arbitrary small positive number. Let m_s be the multiplicity of ρ_s, i.e.

$$R^{(j)}(\rho_s)=0 \quad (j=0,\dots,m_s-1), \qquad R^{(m_s)}(\rho_s)\ne 0.$$

Let $\varphi(z)=\prod_{j=1}^{p}(z-\rho_j)^{m_j}$, $\psi(z)=\prod_{j=1}^{p}(1-\rho_j z)^{m_j}$, and E be defined for a sequence $a_0a_1\dots$ such that $Ea_m=a_{m+1}$.

If $\underline{b}$ is a solution of the equation (1.4), and p is an arbitrary polynomial in $C[z]$, then $e_n = p(E)b_n$ is a solution of (1.4) as well.

Let

$$c_n := \psi(E)b_n \quad (n \in \mathbb{N}_0).$$

Let furthermore

$$B(z) = \sum_{\nu=0}^{\infty} \frac{b_\nu}{z^\nu}, \quad C(z) = \sum_{\nu=0}^{\infty} \frac{c_\nu}{z^\nu}. \tag{1.5}$$

Observe that

$$C(z) = \prod \left(1 - \frac{\rho_\nu}{z}\right)^{m_\nu} B(z) = \psi\left(\frac{1}{z}\right) B(z), \tag{1.6}$$

and that

$$\psi\left(\frac{1}{z}\right) z^M = \varphi(z), \quad M = m_1 + \cdots + m_p. \tag{1.7}$$

The function $B(z)$ is regular outside $|z| \le e^{-\varepsilon}$, and bounded in $|z| \ge \dfrac{1}{e^\varepsilon} + \varepsilon_2$, where $\varepsilon_2 > 0$ is an arbitrary constant. We assume that $\dfrac{1}{e^\varepsilon} + \varepsilon_2 < 1$. In the ring $\dfrac{1}{e^\varepsilon} + \varepsilon_2 < |z| < 1$ we have

$$R(z)B(z) = \left(\sum_{u=0}^{\infty} t_u z^u\right)\left(\sum_{v=0}^{\infty} b_\nu \cdot z^{-v}\right) = \sum_{r=-\infty}^{\infty} \kappa_r z^r,$$

where

$$\kappa_r = \sum_{\substack{u-v=r \\ u,v\ge 0}} t_u b_v.$$

Due to (1.4), $\kappa_r = 0$ if $r < 0$, and $\kappa_r = O(1)$, for $r > 0$. Thus

$$R(z)B(z) = K(z), \quad K(z) = \kappa_0 + \kappa_1 z + \cdots,$$

$K(z)$ is regular in $|z| < 1$. Consequently, $B(z) = \dfrac{K(z)}{R(z)}$,

$$C(z) = \frac{K(z)\psi\left(\frac{1}{z}\right)}{R(z)}. \tag{1.8}$$

The right hand side of (1.8) is regular in $|z| < \frac{1}{e^{\varepsilon}} + \varepsilon_1$, and bounded there. Otherhand $B(z)$ and so $C(z)$ is bounded in $|z| \geq \frac{1}{e^{\varepsilon}} + \varepsilon_2$. If we choose $\varepsilon_2 < \varepsilon_1$, we conclude that $C(z)$ is bounded on the whole plane and so, it is constant, $C(z) = D$, $\sum \frac{b_\nu}{z^\nu} = B(z) = \frac{D}{\psi(1/z)}$, and so

$$\sum_{\nu=0}^{\infty} b_\nu z^\nu = \frac{D}{\prod (1-\rho_\nu z)^{m_\nu}}.$$

The right hand side can be splitted into partial fractions,

$$\frac{D}{\prod (1-\rho_\nu z)^{m_\nu}} = \sum_{\nu=1}^{p} \sum_{j=0}^{m_\nu} \frac{e_{\nu,j}}{(1-\rho_\nu z)^j}, \quad (e_{\nu,j} \in \mathbb{C}),$$

whence we obtain immediately that

$$c_n = \sum_{\nu=1}^{p} p_\nu(n) \rho_\nu^n \quad \deg p_\nu \leq m_\nu - 1,$$

and so the theorem holds.

II.

Let $\{\lambda_n\}_{n=1}^{\infty}$ be a strictly monotonic sequence of positive numbers, $\lambda_1 > \lambda_2 > \cdots (> 0)$, and assume that $L_n = \lambda_{n+1} + \ldots$ is finite, furthermore that

$$\lambda_n \leq L_n \quad (n = 0, 1, 2, \ldots). \tag{2.1}$$

The condition (2.1) implies that

$$H = \left\{ x \;\middle|\; x = \sum \varepsilon_n \lambda_n, \quad \varepsilon_n \in \{0, 1\} \right\}$$

is the whole interval $[0, L_0]$. This assertion is due to Kakeya.

In some of our papers with Daróczy, we have investigated expansions generated by λ_n satisfying (2.1).

A sequence $\{\lambda_n\}$ is called interval filling, if (2.1) holds.

In a paper written jointly with Z. Daróczy and G. Szabó [12] we proved the following assertion.

Theorem 2. *Let λ_n be an interval filling sequence. Let $\{a_n\}_{n=1}^{\infty} \in l_1$ be a sequence with the following property: if*

$$\sum_{n=1}^{\infty} \varepsilon_n \lambda_n = 0, \quad \varepsilon_n \in \{-1, 0, 1\},$$

then

$$\sum \varepsilon_n a_n = 0.$$

We have $a_n = c\lambda_n$ with some constant c.

Conjecture 3. *Let $\{\lambda_n\}_{n=1}^{\infty}$ be such a sequence of positive numbers for which $\lambda_1 > \lambda_2 > \cdots$, $\sum \lambda_n < \infty$, and $H = \{x \mid x = \sum \varepsilon_n \lambda_n, \quad \varepsilon_n \in \{0, 1\}\}$ contains an interval. Assume furthermore that $\{a_n\}_{n=1}^{\infty} \in l_1$ such a sequence for which $\sum \delta_n \lambda_n = 0, \quad \delta_n \in \{-1, 0, 1\}$ implies that $\sum \delta_n a_n = 0$.*

Then $a_n/\lambda_n =$ constant.

Remarks. 1. If $H = \{\sum \varepsilon_n \lambda_n \mid \varepsilon_n \in \{0, 1\}\}$ is totally disconnected, then each $x \in H$ has a unique expansion, therefore

$$\delta_1 \lambda_1 + \delta_2 \lambda_2 + \cdots = 0, \qquad \delta_j \in \{-1, 0, 1\}$$

implies that $\delta_1 = \delta_2 = \cdots = 0$, consequently every $\{a_n\} \in l_1$ is a solution.

2. Assume that $\Lambda := \{\lambda_n\}$ is interval filling and even that there is a non-trivial subsequence $\lambda_{n_j} (= w_j)$ for which $\Omega = \{w_j\}$ is interval-filling.

Let $\mathcal{M}$ denote the set of the following sequences $(e_1, e_2, \ldots) = \underline{e}$.

1. If $e_\nu \in \{-1, 0, 1\}$ for every ν and $e_\nu = 0$ for $\nu \notin \{n_1, n_2, \ldots\}$, then $\underline{e} \in \mathcal{M}$.

2. For every n, let λ_n be expanded in the system Ω with some digits $\{0, 1\}$:

$$\lambda_n = \sum_{j=1}^{\infty} \delta_{n+j}^{(n)} \lambda_{n+j},$$

where $\delta_m^{(n)} = 0$ if $m \notin \{n_1, n_2, \ldots\}$.

Then

$$\left(0, 0, \ldots, 0, \overset{n}{-1}, \delta_{n+1}^{(n)}, \delta_{n+2}^{(n)}, \ldots\right) \in \mathcal{M},$$

if $n \geq n_1$, where n_1 is a constant.

3. For every $n = 1, \ldots, n_1 - 1$ choose an arbitrary sequence $\left(e_1^{(n)}, e_2^{(n)}, \ldots\right)$ such that

(a) $e_l^{(n)} = 0$ if $l < n$,

(b) $e_u^{(n)} \neq 0$,

(c) $e_m^{(n)} \in \{-1,0,1\}$.

Let $\left(e_1^{(n)}, e_2^{(n)}, \dots\right) \in \mathcal{M}$.

Assertion: *Let* $\{a_n\} \in l_1$ *be a sequence for which*

$$\sum \varepsilon_n a_n = 0$$

whenever

$$\sum \varepsilon_n \lambda_n = 0$$

and $(\varepsilon_1, \varepsilon_2, \dots) \in \mathcal{M}$.

Then $a_n = c\lambda_n \quad (n \in \mathbb{N})$.

The assertion is an easy consequence of our Theorem 2.

Indeed, by using Theorem 2 for Ω, we obtain that $a_{n_j} = c\lambda_{n_j} \quad (j = 1, 2, \dots)$.

Let now $j \geq 1$ be fixed and consider the set of the integers $n \in [n_j+1, n_{j+1}-1]$. Since Ω is interval filling, therefore $\lambda_{n_j} \leq \lambda_{n_{j+1}} + \lambda_{n_{j+2}} + \cdots$ consequently for every n there is a suitable sequence defined in (ii).

We have $a_n = \sum \delta_{n+j}^{(n)}\ a_{n+j} = c \sum \delta_{n+j}^{(n)}\ \lambda_{n+j} = c\lambda_n$. Thus $a_n = c\lambda_n$ if $n \geq n_1$. From (*iii*), we obtain that $a_n = c\lambda_n$ for $n = n_1 - 1,\ n_1 - 2, \dots, 1$.

The assertion is proved.

Let $\lambda_n := \Theta^n,\ \Theta \in \left(\frac{1}{2}, 1\right),\ L_0 = \frac{\Theta}{1-\Theta}$. A sequence $\varepsilon_1, \dots, \varepsilon_N \in \{-1,0,1\}$ is said to be continuable if

$$\left|\varepsilon_1\Theta + \cdots + \varepsilon_N\Theta^N\right| \leq \Theta^N L_0.$$

Let $t(0) = 2,\ t(\pm 1) = 1$ and

$$\tau(\varepsilon_1, \dots, \varepsilon_N) = \prod_{j=1}^{N} t(\varepsilon_j).$$

Let $m_N(\Theta) = \sum \tau(\varepsilon_1, \dots, \varepsilon_N)$, where the summation is extended over the continuable sequences. One can see easily that

$$m_N(\Theta) \geq c(4\Theta)^N, \quad c > 0.$$

Let $\mathcal{F}$ be a set of sequences $\underline{\varepsilon} = \varepsilon_1\varepsilon_2 \dots,\ \varepsilon_\nu \in \{-1,0,1\}$, furthermore let $\mathcal{F}_N$ be the set of those sequences $\delta_1 \dots \delta_N \in \{-1,0,1\}^N$, which can be continued with suitable $\varepsilon_\nu \in \{-1,0,1\} \quad (\nu \geq N+1)$ such that $\delta_1 \dots \delta_N\ \varepsilon_{N+1}\varepsilon_{N+2} \dots\ \in \mathcal{F}$.

Let

$$\pi_N(\Theta|\mathcal{F}) = \sum_{\delta_1 \dots \delta_N \in \mathcal{F}_N} \tau(\delta_1, \dots, \delta_N).$$

Conjecture 4. *If* $\underline{a} = a_1 a_2 \ldots \in l_1$ *and*

$$\sum \varepsilon_n a_n = 0 \quad \textit{whenever}$$

$\underline{\varepsilon} \in \mathcal{F}$, *and*

$$\pi_N(\Theta|\mathcal{F}) \to \infty \quad (N \to \infty)$$

then $a_n = c\Theta^n \quad (n = 1, 2, \ldots)$.

III.

Let $\Theta \in \left(\frac{1}{2}, 1\right)$, $q = 1/\Theta$, $L = \frac{\Theta}{1-\Theta}$. Let $\eta \in [\Theta, \Theta L]$ and $T = T_\eta$ be the mapping $[0, L] \to [0, L]$ defined as follows.

If $x \in [0, L]$, then let

$$\varepsilon_1 = \varepsilon_1(x) = \begin{cases} 0, & \text{if } x < \eta, \\ 1, & \text{if } x \geq \eta, \end{cases}$$

and let $x_1 = Tx$ be defined from

$$x = \varepsilon_1 \Theta + \Theta x_1.$$

Continuing this process, $x_n = \varepsilon_{n+1}\Theta + \Theta x_{n+1} \quad (n = 1, 2, \ldots)$, an expansion of x

$$x = \varepsilon_1 \Theta + \varepsilon_2 \Theta^2 + \cdots \tag{3.1}$$

is given. We say that it is a representation of level η of x.

We can see that $T\colon [0, q\eta) \to [0, q\eta)$. Let us consider the expansion of level η of $q\eta$, and η:

$$q\eta = t_1\Theta + t_2\Theta^2 + \ldots, \quad \eta = \pi_1\Theta + \pi_2\Theta^2 + \cdots. \tag{3.2}$$

Let $\underline{t} = t_1 t_2 \ldots$, $\underline{\pi} = \pi_1 \pi_2 \ldots$.

Let

$$\mathcal{E} := \{\underline{\varepsilon}(\S) \mid \S \in [\prime, \amalg\eta)\}.$$

Let furthermore $\mathcal{F}$ be the set of those sequences $\underline{f} = f_1 f_2 \ldots \in \{0, 1\}^\infty$ for which:

(1) $\sigma^j(\underline{f}) < \underline{t} \quad (j = 0, 1, 2, \ldots)$,

(2) if $f_\nu = 1$, then

$$\sigma^{\nu-1}(\underline{f}) = f_\nu f_{\nu+1} \ldots \geq \underline{\pi}.$$

Theorem 3. *We have* $\mathcal{E} = \mathcal{F}$.

Remark. The expansion T for $\eta = \Theta$ was defined by A. Rényi [1]. W. Parry proved the relation $\mathcal{E} = \mathcal{F}$ for $\eta = \Theta$ in [2].

Proof of Theorem 3. The relation $\mathcal{E} \subseteq \mathcal{F}$ is obvious. Let $x = \varepsilon_1(x)\Theta + \cdots$, $x \in [0, q\eta]$. Since for every couples y_1, y_2, if $0 \leq y_1 < y_2 \leq q\eta$, then $\underline{\varepsilon}(y_1) < \underline{\varepsilon}(y_2)$, thus $\underline{\varepsilon}(x) < \underline{t}$. Since $x_n = \varepsilon_{n+1}(x)\Theta + \cdots < q\eta$, therefore $\sigma^n(\underline{\varepsilon}(x)) < \underline{t}$. If $\varepsilon_n(x) = 1$, then $x_{n-1} = \varepsilon_n(x)\Theta + \cdots \geq \eta$, thus $(\varepsilon_n(x), \ldots) \geq \pi$. Thus $\mathcal{E} \subseteq \mathcal{F}$ is true.

Let $\underline{f} \in \mathcal{F}$, $y : T = f_1\Theta + f_2\Theta^2 + \cdots$. We shall prove that $y \leq q\eta$ and that if $f_k = 1$, then $f_k\Theta + \cdots \geq \eta$. Hence it would follow that $\underline{\varepsilon}(y) = \underline{f}$.

Let $f_j = t_j \quad (j = 1, \ldots, k_1 - 1)$, $f_{k_1} = 0$, $t_{k_1} = 1$. Furthermore let $f_{k_1+j} = t_j$ for $(j = 1, \ldots, k_2 - 1)$, $f_{k_2} = 0$, $t_{k_2} = 1$, and so on. We allow the choice $k_\nu = 1$, when $(j = 1, \ldots, k_\nu - 1)$ is an empty condition.

Thus we have

$$y = t_1\Theta + \cdots + t_{k_1-1}\Theta^{k_1-1} + \Theta^{k_1}\left(t_1\Theta + \cdots + t_{k_2-1}\Theta^{k_2-1}\right) + \\ + \Theta^{k_1+k_2}\left(t_1\Theta + \cdots + t_{k_3-1}\Theta^{k_3-1}\right) + \cdots . \tag{3.3}$$

If $t_k = 1$, then $t_k\Theta + t_{k+1}\Theta^2 + \cdots \geq \eta$, and so $t_1\Theta + \cdots + t_{k-1}\Theta^{k-1} \leq (q\Theta)(1 - \Theta^k)$.

From (3.3) we obtain that

$$y \leq (q\Theta)(1 - \Theta^{k_1}) + (q\Theta) \cdot \Theta^{k_1}(1 - \Theta^{k_2}) + \cdots = q\Theta.$$

The estimation from below is the same. Assume that $f_1 = \pi_1$, $f_j = \pi_j \quad j = 1, \ldots, (k_1 - 1)$, $f_{k_1} = 1$, $\pi_{k_1} = 0$, $f_{k_1+j} = \pi_j$, $j = 1, \ldots, k_2 - 1$, $f_{k_1+k_2} = 1$, $\pi_{k_2} = 0$, and so on. Then

$$y = \left(\pi_1\Theta + \cdots + \pi_{k_1-1}\Theta^{k_1-1}\right) + \Theta^{k_1-1}\left(\pi_1\Theta + \cdots + \pi_{k_2-1}\Theta^{k_2-1}\right) + \\ + \Theta^{(k_1-1)+(k_2-1)}\left(\pi_1\Theta + \ldots + \pi_{k_3-1}\Theta^{k_3-1}\right) + \cdots$$

If k is such an integer for which $\pi_k = 0$, then $\eta = \pi_1\Theta + \cdots + \pi_{k-1}\Theta^{k-1} + \Theta^{k-1}\xi, \quad \xi < \eta$, and so

$$\pi_1\Theta + \cdots + \pi_{k-1}\Theta^{k-1} \geq \eta\left(1 - \Theta^{k-1}\right).$$

Therefore

$$y \geq \eta\left(1 - \Theta^{k_1-1}\right) + \eta\Theta^{k_1-1}\left(1 - \Theta^{k_2-1}\right) + \ldots = \eta.$$

Hence the assertion easily follows.

Theorem 4. *Let $\eta_1 < \eta_2,\ \eta_1, \eta_2 \in [\Theta, \Theta L]$. Furthermore let $\mathcal{H}(\eta_1, \eta_2)$ be the set of those $x \in [0, L]$ for which their expansions of level η_1 and of level η_2 are the same. Then the Lebesgue measure of $\mathcal{H}(\eta_1, \eta_2)$ is zero.*

We shall not prove this theorem presently.

IV.

Let $q > 1$ be a Pisot number, $\Theta = 1/q,\ k = [q],\ \mathcal{A} = \{0, 1, \ldots, k\}$,

$$H := \left\{ \sum \varepsilon_n \Theta_n \;\middle|\; \varepsilon_n \in \mathcal{A} \right\} = [0, kL], \quad L = \frac{\Theta}{1 - \Theta}.$$

Let $\underline{\varepsilon}(x) = \varepsilon_1(x)\varepsilon_2(x)\ldots$ be the sequence of digits in the regular (that is the Rényi–Parry) expansion of $x\,(= \sum \varepsilon_n(\Theta)\Theta^n)$. Let $\underline{t} = t_1 t_2 \ldots$ be the sequence of digits in the quasi-regular expansion of 1.

The digit $\varepsilon_1(x)$ for the regular expansion of x is defined as

$$\varepsilon_1(x) = [qx],$$

while in the quasi-regular expansions by $[qx]$, if qx is not an integer, and by $qx - 1$ if it is an integer. Since q is a Pisot number, therefore $\sigma^k(\underline{t}) \quad (k = 0, 1, \ldots)$ is ultimately periodic, that is

$$\sigma^{k+p}(\underline{t}) = \sigma^k(\underline{t}) \tag{4.1}$$

holds with suitable $p > 0,\ k > 0$.

Let $\mathcal{B} = \{\lfloor_\prime, \lfloor_\infty, \ldots, \lfloor_\nabla\}$ be a set of distinct integers such that $b_0 = 0,\ -K_1 = \min b_\nu < 0,\ K_2 = \max b_\nu > 0$.

We would like to find those sequences $f_1, f_2, \ldots \in \mathcal{B}$ for which

$$O = f_1\Theta + f_2\Theta^2 + \cdots \tag{4.2}$$

holds.

Let $\gamma_0 = 0,\ \gamma_1 = -f_1,\ \gamma_j = q\gamma_{j-1} - f_j \quad (j = 1, 2, \ldots)$.

Then

$$\gamma_j = f_{j+1}\Theta + f_{j+2}\Theta^2 + \cdots \in [-K_1 L, K_2 L]. \tag{4.3}$$

The numbers γ_j are integers in $Q(q)$. Let the conjugates of q be $q = q_1,\ q_2, \ldots, q_n$. We have $|q_\nu| < 1 \quad (\nu = 2, \ldots, n)$.

Consequently,

$$\gamma_j(q_l) = -\left(f_1 q_l^{j-1} + \cdots + f_j\right), \quad |\gamma_j(q_l)| \le \frac{\max(K_1, K_2)}{1 - |q_l|}$$

$(j = 2, \dots, n),\ \gamma_j \in [-K_1 L, K_2 L]$.

Since the vectorials $\{\gamma_j(q_l) \mid l = 1, \dots, n\}$ belong to a bounded domain, therefore they are taken from a finite set which is denoted by $\mathcal{F}$:

$$\mathcal{F} = \left\{\rho,\ \rho \text{ integer in } Q(q),\ |\rho(q_l)| \le \frac{\max(K_1, K_2)}{1 - |q_l|} \quad (l \ge 2), \quad \rho \in [-K_1 L, L_2 L]\right\}.$$

The construction of the graph $G(\mathcal{F})$

The edges of the graph are the elements of $\mathcal{F}$. We shall draw an edge from $\rho \in \mathcal{F}$ to $\rho q - f$ if $\rho q - f \in \mathcal{F}$. This (directed) edge is labeled with f.

It is clear that all solutions $f_1, f_2, \dots$ of (4.2) can be getting by walking on the graph starting from 0, and noting the sequence of the labels of the graph.

By using this construction we can solve some interesting problems.

Problem. Let $\mathcal{A} = \{0, 1, \dots, k\}$, $\underline{\varepsilon}(x)$ be the sequence of digits in the regular expansion of x. Let us determine those sequences $(\delta_1, \dots, \delta_N) \in \mathcal{A}^N$ which can be continued appropriately, by $\delta_{N+j} \in \mathcal{A}$ $(j = 1, 2, \dots)$ such that $x = \sum_1 \delta_\nu \Theta^\nu$.

This can be done as follows. We consider the set $\mathcal{B} = \mathcal{A} - \mathcal{A} = \{\sqcap - \sqsubseteq \mid \sqcap, \sqsubseteq \in \mathcal{A}\}$ and define $\mathcal{F}$ as earlier, then $G(\mathcal{F})$ by drawing the edge $\rho_1 \to \rho_2$, if $\rho_2 = q\rho_1 - f$. After then we delete the edge labeled with f, and substitute it with as many edges as many solutions $f = u - v,\ u, v \in \mathcal{A}$ has, and we label them with (u, v). Let $G^*(\mathcal{F})$ be this directed multigraph.

Let us walk on $G^*(\mathcal{F})$ starting from 0 and note the sequence of labels:

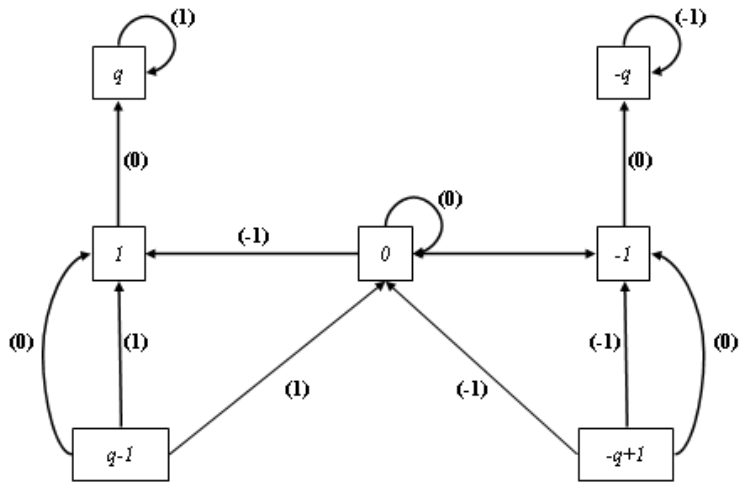
$$(u_1, v_1), (u_2, v_2), \dots .$$

Let us consider only those routes for which $u_j = \varepsilon_j(x) \quad (j = 1, \dots, N)$. Then the sequence of the second components will give a suitable continuable sequence $\delta_1, \dots, \delta_N$, and all appropriate sequences can be getting on this way.

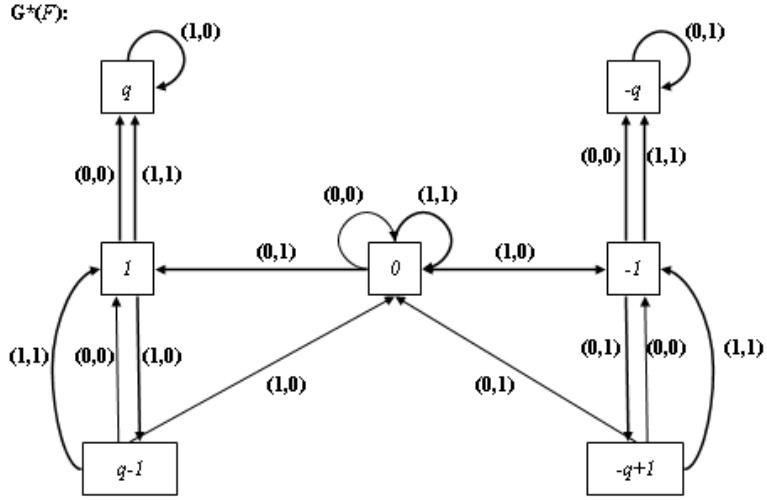
Let us see $G(\mathcal{F})$ and $G^*(\mathcal{F})$ in the simplest case

$$\Theta = \frac{\sqrt{5} - 1}{2}, \quad q = \frac{\sqrt{5} + 1}{2}, \quad \mathcal{A} = \{0, 1\}, \quad \mathcal{B} = \{-\infty, \prime, \infty\}.$$

G(*F*):


(1)
(-1)
q
-q
(0)
(0)
(0)
1
(-1)
0
-1
(0)
(1)
(1)
(-1)
(-1)
(0)
q-1
-q+1

G*(*F*):


(1,0)
(0,1)
q
-q
(0,0)
(1,1)
(0,0)
(1,1)
(0,0)
(1,1)
1
(0,1)
0
(1,0)
-1
(1,1)
(0,0)
(1,0)
(1,0)
(0,1)
(0,1)
(0,0)
(1,1)
q-1
-q+1

V.

Let $f: \mathbb{N} \to \mathbb{C}$ be a completely multiplicative arithmetical function, $|f(n)| = 1 \quad (n \in \mathbb{N})$, and let $\delta_f(n) = f(n+1)\overline{f}(n)$.

E. Wirsing proved in 1984 that if $\delta_f(n) \to 1 \quad (n \to \infty)$, then $f(n) = n^{i\tau}$ [13], [14].

Daróczy and I proved the following assertion [15].

If G is a compact Abelian group, $f: \mathbb{N} \to G$ is completely additive, i.e. $f(mn) = f(m) + f(n)$ for every $m, n \in \mathbb{N}$, and $f(n+1) - f(n) \to 0 \quad (n \to \infty)$, then there is a continuous homomorphism $\Phi: \mathbb{R}_x \to G$ such that

$$f(n) = \phi(n) \quad (n \in \mathbb{N}).$$

Conjecture 5. *Let G be a compact Abelian group, $f: \mathbb{N} \to G$ be completely additive, and closure $f(\mathbb{N}) = G$ (closure $f(\mathbb{N})$ always is a closed subgroup in G). Let U be the set of those u for which there exists an infinite sequence of integers $n_\nu \nearrow$, such that $f(n_\nu + 1) - f(n_\nu) \to u$.*

Then U is a subspace in G, furthermore

$$f(n) := \Phi(n) + V(n),$$

where Φ is a continuous homomorphism, $\phi: \mathbb{R}_x \to G$, $V(\mathbb{N}) \subseteq U$, clos $V(\mathbb{N}) = U$.

We formulate our conjecture for complex valued completely multiplicative functions.

Conjecture 6. *Let f be completely multiplicative, $|f(n)| = 1 \quad (n \in \mathbb{N})$, $\delta_f(n) = f(n+1)\overline{f}(n)$. Let $\mathcal{A}_k = \{\alpha_1, \dots, \alpha_k\}$ be the set of limit points of $\{\delta_f(n) \mid n = 1, 2, \dots\}$. Then $\mathcal{A}_k = \{w | w^k = 1\}$, furthermore $f(n) = n^{i\tau} F(n)$, and*

$$(i) \qquad F(\mathbb{N}) = \mathcal{A}_k,$$

(ii) for every $w \in \mathcal{A}_k$ there is some infinite sequence n_ν such that $F(n_\nu + 1)\overline{F}(n_\nu) = w \quad (\nu = 1, 2, \dots)$.

A weaker conjecture, namely that under the conditions of Conjecture 6 there is an s such that $F(\mathbb{N}) = \{\omega \mid \omega^s = 1\}$, was proved by E. Wirsing [18] in his brilliant paper.

VI.

Let $\mathcal{P}_k$ be the set of integers $n = p_1 \cdots p_k$ where $p_1, \dots, p_k$ are distinct primes. Let α be a fixed irrational number. Let $e(\beta) := e^{2\pi i \beta}$. Let $q_1 < q_2 < \cdots < q_r$

be the whole sequence of the primes up to x. Let $X_{q_j} \quad (j = 1, \dots, r)$ be complex numbers,

$$Q_k(X_{q_1}, \dots, X_{q_r}) := \left| \sum_{\substack{n \in \mathcal{P}_k \\ n = p_1 \dots p_k < x}} X_{p_1} \cdots X_{p_k} e(n\alpha) \right|.$$

Let us define

$$\delta_k(x) = \max_{|X_{q_1}| \le 1, \dots, |X_{q_r}| \le 1} \frac{Q_k(X_{q_1}, \dots, X_{q_r})}{\pi_k(x)},$$

$$\delta_k = \limsup_{x \to \infty} \delta_k(x).$$

Conjecture 7. *We have $\delta_k < 1$ if $k \ge 2$. Furthermore $\delta_k \to 0 \quad (k \to \infty)$.*

H. Daboussi proved several years ago that for every irrational α, for every multiplicative function f, such that $|f(n)| \le 1 \quad (n \in \mathbb{N})$, the relation

$$\frac{1}{x} \left| \sum_{n \le x} f(n) e(n\alpha) \right| \to 0 \quad (x \to \infty).$$

The order of the convergence may depend on α, but does not depend on f. In our recent paper written jointly with Indlekofer [19] we proved:

If α is irrational, $w(n)$ is the number of the prime divisors of n, $\tilde{\mathcal{P}}_k = \{n \mid w(n) = k\}$, $\tilde{\pi}_k(x) = \#\left\{\tilde{\mathcal{P}}_k(x) \cap [1, x]\right\}$, $\eta > 0$ is a small constant, then uniformly for multiplicative functions f restricted by the conditions $|f(n)| \le 1 \quad (n \in \mathbb{N})$ we have

$$\max_k \frac{1}{\tilde{\pi}_k(x)} \left| \sum_{\substack{n \le x \\ n \in \tilde{\mathcal{P}}_K}} f(n) e(n\alpha) \right| \to 0 \quad \text{as} \quad \eta < \frac{k}{x_2} < 2 - \eta \qquad x \to \infty.$$

I hope that Conjecture 7 is true.

References

[1] Rényi, A., Representations for real numbers and their ergodic properties, *Acta Math. Acad. Sci. Hungar.*, **8** (1957), 477–493.

[2] Parry, W., On the β-expansions of real numbers, *Acta Math. Acad. Sci. Hungar.*, **11** (1960), 401–416.

[3] Daróczy, Z., Járai, A. and Kátai, I., Intervalfüllende Folgen und volladditive Funktionen, *Acta Sci. Math. (Szeged)*, **50** (1986), 337–350.

[4] Daróczy, Z. and Kátai, I., Additive functions, *Analysis Math.*, **12**, (1986), 85–96.

[5] Daróczy, Z. and Kátai, I., Interval filling sequences and additive functions, *Acta Sci. Math. (Szeged)*, **52**, (1988), 337–347.

[6] Daróczy, Z., Járai, A. and Kátai, I., Interval filling sequences, *Annales Univ. Eötvös L. Sectio Computatorica*, **6** (1985), 53–63.

[7] Daróczy, Z. and Kátai, I., On differentiable additive funcitons, *Annales Univ. Eötvös L., Sectio Computatorica*, **6** (1985), 53–63.

[8] Daróczy, Z. and Kátai, I., Continuous additive functions and difference equations of infinite order, *Analysis Math.*, **12** (1986), 237–249.

[9] Daróczy, Z. and Kátai, I., On functions additive with respect to interval filling sequences, *Acta Math. Hungar.*, **51** (1988), 185–200.

[10] Daróczy, Z. and Kátai, I., Univoque sequences, *Publ. Math. Debrecen*, **42**, (1993), 397–407.

[11] Daróczy, Z. and Kátai, I., On the structure of univoque numbers, *Publ. Math. Debrecen*, **46** (1995), 385–408.

[12] Daróczy, Z., Kátai, I. and Szabó, T., On completely additive functions related to interval filling sequences, *Archiv Math.*, **54** (1990), 173–179.

[13] Wirsing, E., *A proof is given in a letter to me*, 1984.

[14] Wirsing, E., Tang Yuansheng and Shao Pintsung, On a conjecture of Kátai for additive functions, *J. Number Theory*, **56** (1996), 391–395.

[15] Daróczy, Z. and Kátai, I., On additive arithmetical functions with values in topological groups, *Publ. Math. Debrecen*, **33** (1986), 287–292.

[16] Kátai, I. and Subbarao, M. V., The characterization of $n^{i\tau}$ as a multiplicative function, *Acta Math. Hungar.*

[17] Kátai, I. and Subbarao, M. V., On the multiplicative function $n^{i\tau}$, *Studia Sci. Math.*, **34** (1998), 211–218.

[18] Wirsing, E., *On a problem of Kátai and Subbarao*, (unpublished manuscript).

[19] Indlekofer, K.-H. and Kátai, I., *A note on a theorem of Daboussi*, (manuscript).

Imre Kátai
Eötvös Loránd University
Department of Computer Algebra
H-1117 Budapest
Pázmány Péter sétány I/C.
Hungary
e-mail: katai@compalg.inf.elte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 101–108*

RECIPROCAL INVARIANT DISTRIBUTED SEQUENCES CONSTRUCTED BY SECOND ORDER LINEAR RECURRENCES

Sándor H.-Molnár (Budapest, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. In this paper we determine necessary and sufficient conditions for the sequence $(G_{n+1}/G_n)_{n=0}^{\infty}$ to become a reciprocal invariant distributed sequence modulo 1, where G_n is the n-th term of a non-degenerate second order linear recurrence of real numbers.

1. Introduction

Let $G = G(A, B, G_0, G_1) = (G_n)_{n=0}^{\infty}$ be a second order linear recursive sequence of real numbers defined by the recursion

$$G_n = AG_{n-1} + BG_{n-2} \qquad (n > 1), \tag{1}$$

where A, B and the initial terms G_0, G_1 are fixed real numbers with restrictions $AB \neq 0$, $D = A^2 + 4B \neq 0$ and $G_0^2 + G_1^2 > 0$. It is well-known that the terms of G can be written in the form

$$G_n = a\alpha^n - b\beta^n, \tag{2}$$

where α and β are the roots of the characteristic polynomial $x^2 - Ax - B$ of the sequence G and $a = \frac{G_1 - G_0\beta}{\alpha - \beta}, b = \frac{G_1 - G_0\alpha}{\alpha - \beta}$ (see e.g. I. Niven and H. S. Zuckerman [9], p. 91).

Troughout this paper we assume $|\alpha| \geq |\beta|$ and the sequence is non-degenerate, i.e. α/β is not a root of unity and $ab \neq 0$. If $G_{n_0} = 0$ we may also suppose that $G_n \neq 0$ for $n \neq n_0$, since P. Kiss [2] proved that a non-degenerate sequence G has at most one zero term.

Distribution properties of the Fibonacci sequence $G = G(1, 1, 0, 1)$ and more general integer valued and real valued recurrences were studied by several authors. Here we only mention the papers [4], [3], [5] and [7], connected with our topic.

The object of this paper is to determine necessary and sufficient conditions for the sequence $(G_{n+1}/G_n)_{n=0}^{\infty}$ to become a reciprocal invariant distributed sequence modulo 1. (The definition of reciprocal invariant will be given later.)

The sequence $\omega = (x_n)_{n=1}^{\infty}$ is said to have asymptotic distribution function modulo 1 (a.d.f. mod 1) F if

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \chi(x, x_n) = F(x) \quad \text{for} \quad 0 \le x \le 1,$$

where the function χ is defined by

$$\chi(x, y) = \begin{cases} 1, & \text{if } 0 \le \{y\} < x, \\ 0, & \text{if } x \le \{y\} \end{cases}$$

and $\{y\}$ denotes the fractional part of the real number y.

In [8] the following definition was introduced.

Definition. Let $\omega = (x_n)_{n=1}^{\infty}$ and $\xi = (f(x_n))_{n=1}^{\infty}$ be sequences of real numbers, where f is a real–valued function. If the sequences ω and ξ have a.d.f. mod 1 and these functions are identical, then we say ω is f invariant distributed sequence modulo 1. (i.d. mod 1 to f.)

In special cases:

(i) if ω is i.d. mod 1 to $f(x) = \frac{1}{x}$, we say ω is reciprocal invariant distributed sequence mod 1,

(ii) if ω is i.d. mod 1 to $f(x) = \sqrt{x}$ we say ω is a square root invariant distributed sequence mod 1.

P. Kiss and R. F. Tichy in [4] investigated the asymptotic distribution function modulo 1 of the sequence $(G_{n+1}/G_n)_{n=1}^{\infty}$ when $D < 0$. Their theorem can be extended to any sequence $(G_{n+k}/G_n)_{n=1}^{\infty}$, where k is a nonzero integer. We prove:

Theorem 1. *Let $G = (G_n)_{n=0}^{\infty}$ be a linear recurring sequence defined by $G_n = AG_{n-1} + BG_{n-2}, \quad (n > 1)$ with nonzero real coefficients A and B, real initial values G_0, G_1 (not both G_0 and G_1 are zero) and with negative discriminant $D = A^2 + 4B$. Let $k \neq 0$ be an integer. If the number $\Theta = \frac{1}{\pi} \arctan \frac{\sqrt{-D}}{A}$ is irrational, then the asymptotic distribution function modulo 1 H of the sequence $(G_{n+k}/G_n)_{n=1}^{\infty}$ is given by*

$$H(x) = H_1(x - \{c\}) + H_1(\{c\}) \tag{3}$$

with

$$H_1(x) = x + \frac{1}{\pi} \arctan \frac{\sin(2\pi x)}{\exp(2\pi|d|) - \cos(2\pi x)}, \tag{4}$$

$c = r^k \cos(k\pi\Theta), \quad d = -r^k \sin(k\pi\Theta)$ *and* $r = |\alpha| = \left| \frac{A+\sqrt{A^2+4B}}{2} \right|$.

Theorem 2. *Let $G = (G_n)_{n=0}^{\infty}$ be a non-degenerate second order linear recursive sequence defined by $G_n = AG_{n-1} + BG_{n-2} \quad (n > 1)$ with nonzero real coefficients A and B, real initial values G_0, G_1 (where $G_0^2 + G_1^2 \neq 0$) and negative discriminant $D = A^2 + 4B$. The sequence $\omega = (G_{n+1}/G_n)_{n=1}^{\infty}$ is reciprocal invariant distributed modulo 1 if and only if $B = -1$.*

Theorem 3. *Let $G = (G_n)_{n=0}^{\infty}$ be a non-degenerate second order linear recursive sequence defined by the recursion $G_n = AG_{n-1} + BG_{n-2} \quad (n > 1)$ with nonzero integer coefficients A and B, integer initial values G_0, G_1 (where $G_0^2 + G_1^2 \neq 0$) and with positive discriminant $D = A^2 + 4B$. The sequence $\omega = (G_{n+1}/G_n)_{n=1}^{\infty}$ is reciprocal invariant distributed modulo 1 if and only if $B = 1$.*

2. Proofs

Proof of Theorem 1. Let G be a second order linear recursive sequence satisfying the conditions of Theorem 1. We know from [2] that the zero multiplicity of G is at most one and one element is not relevant for the asymptotic distribution function therefore without loss of generality we may assume that $G_n \neq 0$ for $n \geq 0$. In (2) α, β and a, b are complex conjugate numbers since $D = A^2 + 4B < 0$ and we can write

$$\alpha = r\exp(i\pi\Theta), \qquad \beta = r\exp(-i\pi\Theta) \tag{5}$$

and

$$a = r_1\exp(i\pi\omega), \qquad b = r_1\exp(-i\pi\omega), \tag{6}$$

where $\exp(x)$ denotes the usual exponential function and

$$0 < \Theta = \frac{1}{\pi}\arctan\frac{\sqrt{-D}}{A} < 1, \quad \omega = \frac{1}{\pi}\arctan\frac{AG_0 - 2G_1}{G_0\sqrt{-D}},$$

while r and r_1 are positive real numbers, $a \neq 0$ and $b \neq 0$. Since G is a non-degenerate sequence we have Θ is an irrational number.

By (2), (5) and (6) we obtain for all $n \geq \max\{0, -k\} = n_0$ that

$$\frac{G_{n+k}}{G_n} = \frac{r_1 r^{n+k}\exp(i\pi(\omega + (n+k)\Theta)) + r_1 r^{n+k}\exp(-i\pi(\omega + (n+k)\Theta))}{r_1 r^n\exp(i\pi(\omega + n\Theta)) + r_1 r^n\exp(-i\pi(\omega + n\Theta))}$$

$$= r^k\frac{\cos(\pi(\omega + (n+k)\Theta))}{\cos(\pi(\omega + n\Theta))} = r^k(\cos(\pi k\Theta) - \sin(\pi k\Theta)\cdot\tan(\pi(\omega + n\Theta)))$$

$$= c + d\tan(\pi(\omega + n\Theta)),$$

where $c = r^k \cos(k\pi\Theta), d = -r^k \sin(k\pi\Theta)$ are nonzero real numbers independent on n. Note that the proof of the inequality

$$\left| \frac{1}{N} \sum_{n=n_0}^{N+n_0-1} \chi\left(x, \frac{G_{n+k}}{G_n}\right) - \int_0^1 \chi(x, c + d\tan(\pi(y+\omega))dy \right|$$

$$\leq 4\sqrt{|r^k \sin(k\pi\Theta)|}\sqrt{\Delta_N} + 6\Delta_N,$$

where $\Delta_N = \Delta_N(\Theta n)$ denotes the discrepancy of the sequence $(\Theta n)_{n=1}^{\infty}$ which is analogous to described in [4] by P. Kiss and R. F. Tichy. Since we only need a.d.f. mod 1, we omit the proof.

In the following we compute the integral

$$H(x) = \int_0^1 \chi(x, c + d\tan(\pi(y+\omega))dy = \int_{-1/2}^{1/2} \chi(x, c + d\tan(\pi(y+\omega))dy \tag{7}$$

in the case $c = 0$. By the substitution $u = d\tan(\pi y)$ we get

$$H_1(x) = \frac{|d|}{\pi} \int_{-\infty}^{\infty} \frac{\chi(x,u)}{d^2+u^2} du. \tag{8}$$

We use the Fourier series expansion of the characteristic function

$$\chi(x,u) = x + \frac{1}{\pi}\sum_{m=1}^{\infty} \frac{\sin(2\pi mx)}{m}\cos(2\pi mu) + \frac{1}{\pi}\sum_{m=1}^{\infty} \frac{1-\cos(2\pi mx)}{m}\sin(2\pi mu)$$

and the integral formulae

$$\int_{-\infty}^{\infty} \frac{\cos(2\pi mu)}{d^2+u^2} du = \frac{\pi}{|d|}\exp(-2\pi m|d|), \int_{-\infty}^{\infty} \frac{\sin(2\pi mu)}{d^2+u^2} du = 0 \quad \text{(see e.g. [1])}.$$

By swapping summation and integration and applying Lebesgue's theorem on dominated convergence we have

$$H_1(x) = x + \frac{1}{\pi}\sum_{m=1}^{\infty} \frac{\sin(2\pi mx)}{m}\exp(-2\pi m|d|) = x + \frac{1}{\pi}\Im\left(\sum_{m=1}^{\infty} \frac{w^m}{m}\right),$$

where $w = \exp(2\pi(-|d| + ix))$. Since $-|d| < 0$, we have $|w| < 1$ and $\Re(1-w) > 0$, so $\sum\limits_{m=1}^{\infty} \frac{w^m}{m} = -\log(1-w)$. Since

$$\Im(1-w) = \exp(-2\pi|d|)\sin(2\pi x) \text{ and } \Re(1-w) = 1 - \exp(-2\pi|d|)\cos(2\pi x)$$

it follows that

$$H_1(x) = x + \frac{1}{\pi}\arctan\frac{\exp(-2\pi|d|)\sin(2\pi x)}{1-\exp(-2\pi|d|)\cos(2\pi x)}$$

$$= x + \frac{1}{\pi}\arctan\frac{\sin(2\pi x)}{\exp(2\pi|d|) - \cos(2\pi x)}.$$

Since $H_1(-x) = -H_1(x), H(x) = H_1(x-c) - H_1(-c) = H_1(x-c) + H_1(c)$, the proof of the theorem is complete.

Proof of Theorem 2. Let G be a second order linear recursive sequence satisfying the conditions of Theorem 2. By [4] the a.d.f. mod 1 of the sequence $(G_{n+1}/G_n)_{n=1}^{\infty}$ is $F(x) = F_1(x - \{A/2\}) + F_1(\{A/2\})$, where

$$F_1(x) = x + \frac{1}{\pi}\arctan\frac{\sin(2\pi x)}{\exp(\pi\sqrt{-D}) - \cos(2\pi x)}.$$

One can check that $\omega = (G_n/G_{n+1})_{n=0}^{\infty} = (G_{n-1}/G_n)_{n=1}^{\infty} = \xi$. The a. d. f. mod 1 ω and ξ are identical which is easy to derive by Theoem 1. Indeed, if $k = -1$ and $c = r^{-1}\cos(-\pi\Theta) = \frac{r\cos(\pi\Theta)}{r^2} = -\frac{A}{2B}$ and $d = -r^{-1}\sin(-\pi\Theta) = \frac{r\sin(\pi\Theta)}{r^2} = -\frac{\sqrt{-D}}{2B}$ then

$$H(x) = H_1\left(x - \left\{\frac{-A}{2B}\right\}\right) + H_1\left(\left\{\frac{-A}{2B}\right\}\right),$$

where

$$H_1(x) = x + \frac{1}{\pi}\arctan\frac{\sin(2\pi x)}{\exp\left(\frac{\pi\sqrt{-D}}{-B}\right) - \cos(2\pi x)}.$$

We have to decide some necessary and sufficient conditions for the equality

$$F(x) = H(x) \quad 0 \le x \le 1. \tag{9}$$

A straightforward calculation shows that the derivate of $F(x)$ and $H(x)$ is given by

$$F'(x) = 1 + 2\frac{E_1\cos\left(2\pi\left(x - \left\{\frac{A}{2}\right\}\right)\right) - 1}{E_1^2 - 2E_1\cos\left(2\pi\left(x - \left\{\frac{A}{2}\right\}\right)\right) + 1} \tag{10}$$

and

$$H^{'}(x) = 1 + 2\frac{E_2 \cos\left(2\pi\left(x - \left\{\frac{-A}{2B}\right\}\right)\right) - 1}{E_2^2 - 2E_2 \cos\left(2\pi\left(x - \left\{\frac{-A}{2B}\right\}\right)\right) + 1}, \tag{11}$$

where

$$E_1 = \exp(\pi\sqrt{-D}) \quad \text{and} \quad E_2 = \exp\left(\frac{\pi\sqrt{-D}}{B}\right).$$

This yields that the graph of $F(x)$ is steepest at $\{A/2\}$ and the graph of $H(x)$ is steepest at $\left\{\frac{-A}{2B}\right\}$. By (9) we get $x_0 = \{A/2\} = \left\{\frac{-A}{2B}\right\}$ and thus

$$F(x_0) = F_1(0) + F_1\left(\left\{\frac{A}{2}\right\}\right) = F_1\left(\left\{\frac{A}{2}\right\}\right)$$

and

$$H(x_0) = H_1(0) + H_1\left(\left\{\frac{-A}{2B}\right\}\right) = H_1\left(\left\{\frac{A}{2}\right\}\right).$$

On the other hand,

$$F_1\left(\left\{\frac{A}{2}\right\}\right) = H_1\left(\left\{\frac{A}{2}\right\}\right)$$

implies

$$\exp(\pi\sqrt{-D}) = \exp\left(\frac{\pi\sqrt{-D}}{-B}\right)$$

and $B = -1$. If $B = -1$ then $F(x) = H(x) \quad (0 \le x \le 1)$ is trivially true. Therefore $B = -1$ is a necessary and sufficient condition for $(G_{n+1}/G_n)_{n=0}^{\infty}$ to be reciprocal invariant distributed mod 1.

Proof of Theorem 3. Suppose $|\alpha| \ge |\beta|$, where α and β are the roots of the characteristic polynomial of G. By the conditions of Theorem 3, $D > 0$, therefore $|\alpha| > |\beta|$. From $\alpha\beta = -B \in \mathbf{Z}$ and $B \neq 0$ it follows that $|\alpha| > 1$. Then $(G_{n+1}/G_n)_{n=0}^{\infty}$ and $(G_n/G_{n+1})_{n=0}^{\infty}$ is convergent (c.f. [7]).

Indeed,

$$\lim_{n\longrightarrow\infty}\frac{G_{n+1}}{G_n} = \lim_{n\longrightarrow\infty}\frac{a\alpha^{n+1} - b\beta^{n+1}}{a\alpha^n - b\beta^n} = \lim_{n\longrightarrow\infty}\alpha\frac{1 - (b/a)(\beta/\alpha)^{n+1}}{1 - (b/a)(\beta/\alpha)^n} = \alpha$$

and

$$\lim_{n\longrightarrow\infty}\frac{G_n}{G_{n+1}} = \frac{1}{\alpha}.$$

The sequence $(G_{n+1}/G_n)_{n=0}^{\infty}$ can only be reciprocal invariant distributed mod 1 if $\alpha \equiv \frac{1}{\alpha} \pmod 1$.

If $\alpha > 1$ then $0 < \frac{1}{\alpha} < 1$, therefore there is a positive integer c, for which $\alpha - c = \frac{1}{\alpha}$. By multiplying the equality by α, we have

$$\alpha^2 - c\alpha - 1 = 0. \tag{12}$$

If $\alpha < -1$ then $-1 < \frac{1}{\alpha} < 0$, therefore

$$\alpha^2 + (c-1)\alpha - 1 = 0. \tag{13}$$

So there exists an integer A, such that α is a root of the equation

$$x^2 - Ax - 1 = 0. \tag{14}$$

The constants in (1), by the condition of Theorem 3, are integers and at the same time (14) is the characteristic equation of the sequence G, so therefore the condition $B = 1$ is necessary.

An easy calculation shows that if $|\alpha| > 1$ and $B = 1$ then the sequence $(G_{n+1}/G_n)_{n=0}^{\infty}$ and $(G_n/G_{n+1})_{n=0}^{\infty}$ are such ones that their limit points are greater and smaller, alternately. Then there exists and a.d.f. mod 1 for both sequences, which is the function

$$F(x) = \begin{cases} 0, & \text{if } 0 \le x < \{\alpha\}, \\ \frac{1}{2}, & \text{if } x = \{\alpha\}, \\ 1, & \text{if } \{\alpha\} < x \le 1. \end{cases}$$

The proof is complete.

References

[1] Dwight, H. B., *Tables of integrals and other mathematical data*, 4th edition, Macmillan Company, 1961.

[2] Kiss, P., Zero terms in second order linear recurrences, *Math. Sem. Notes (Kobe Univ.)*, **7** (1979), 145–152.

[3] Kiss, P. and H.-Molnár, S. On distribution of linear recurrences modulo 1, *Studia Sci. Math. Hungar.*, **17** (1982), 113–127.

[4] Kiss, P. and Tichy, R. F., Distribution of the ratios of the terms of a second order linear recurrence, *Indag Math.*, **48** (1986), 79–86.

[5] Kiss, P. and Tichy, R. F., A discrepancy problem with applications to linear recurrences I., *Proc. Japan Acad.*, 65, **5** (1989), 135–138.

[6] Kuipers, L. and Niederreiter, H., *Uniform distribution of sequences,* Wiley, New York, 1974.

[7] Mátyás, F., Másodrendű lineáris rekurzív sorozatok elemeinek hányadosáról (On the quotients of the elements of linear recursive sequence of second order), *Mat. Lapok*, **27** (1976/79), 379–389 (In Hungarian).

[8] H.-Molnár, S., Sequences and their transforms with identical asymptotic distribution function modulo 1, *Studia Sci. Math. Hungarica*, **29** (1994), 315–322.

[9] Niven, I. and Zuckerman, H. S., *An introduction to the theory of numbers,* Wiley, New York, 1960.

Sándor H.-Molnár
Department of Mathematics
Budapest Business School
Department of Mathematics
H–1149 Budapest, Buzogány str. 10–12.
Hungary
e-mail: s.molnar@freemail.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 109–114*

A NOTE ON THE CORRELATION COEFFICIENT OF ARITHMETIC FUNCTIONS

Milan Păstéka, Robert F. Tichy (Bratislava, Slovakia – Graz, Austria)

Dedicated to the memory of Professor Péter Kiss

1. Introduction

The statistical independence was studied by G. Rauzy [9], and later in the papers [3], [5]. We remark that two arithmetical functions F, G with values in $[0, 1]$ are called statistically independent if and only if

$$\frac{1}{N}\sum_{n=1}^{N} F(f(n))G(g(n)) - \frac{1}{N^2}\sum_{n=1}^{N} F(f(n))\sum_{n=1}^{N} G(g(n)) \to 0,$$

as $N \to \infty$ for all continuous real valued functions f, g defined on $[0, 1]$ (cf. [9]). In the papers [3], [5] a characterization of this type of independence is given in terms of the L^p-discrepancy.

The aim of the present note is to give a "statistical" condition of linear dependence of some type of functions. We consider two polyadically continuous functions f and g. Such functions can be uniformly approximated by the periodic functions (cf. [8]). Let Ω be the space of polyadic integers, constructed as a completion of positive integers with respect to the metric $d(x, y) = \sum_{n=1}^{\infty} \frac{\varphi_n(x-y)}{2^n}$, where $\varphi_n(z) = 0$ if $n|z$ and $\varphi_n(z) = 1$ otherwise, (see the paper [7]). For a survay on the properties of this metric ring we refer also to the monograph [8]. The functions f, g can be extended to uniformly continuous functions $\tilde{f}, \tilde{g}$ defined on Ω. The space Ω is equipped with a Haar probability measure P, thus $\tilde{f}, \tilde{g}$ can be considered as random variables on Ω. Put

$$\tilde{\rho} = \frac{|E(\tilde{f} \cdot \tilde{g}) - E(\tilde{f}) \cdot E(\tilde{g})|}{D^2(\tilde{f}) \cdot D^2(\tilde{g})},$$

where $E(\cdot)$ is the mean value and $D^2(\cdot)$ is the dispersion (variance) (cf. [1], [10]). The value $\tilde{\rho}$ is called the correlation coefficient of $\tilde{f}, \tilde{g}$, thus if $\tilde{\rho} = 1$ then $\tilde{g} = A\tilde{f} + B$ for some constants A, B. In the following we will prove a similar result for a greater class of functions.

2. Correlation on a set with valuation

Let $\mathbf{M}$ be a set with valuation

$$|\cdot|\colon \mathbf{M} \to [\mathbf{0}, \infty)$$

such that

(i) The set $\mathbf{M}(\mathbf{x}) = \{\mathbf{a} \in \mathbf{M} : |\mathbf{a}| \leq \mathbf{x}\}$ is finite for every $x \in [0, \infty)$,

(ii) If $N(x) = \operatorname{card} \mathbf{M}(\mathbf{x})$, then $N(x) \to \infty$ as $x \to \infty$.

Let $S \subseteq \mathbf{M}$ and put for $x > 0$

$$\gamma_x(S) = \frac{\operatorname{card}(S \cap \mathbf{M}(\mathbf{x}))}{N(x)}.$$

Then γ_x is an atomic probability measure with atoms $\mathbf{M}(\mathbf{x})$. If for some $S \subseteq \mathbf{M}$ there exists the limit

$$\lim_{x \to \infty} \gamma_x(S) := \gamma(S), \tag{2.1}$$

then the value $\gamma(S)$ will be called the asymptotic density of S.

If h is a real-valued function defined on $\mathbf{M}$, then it can be considered as a random variable with respect to γ_x for $x > 0$ with mean value

$$E_x(h) := \frac{1}{N(x)} \sum_{|a| \leq x} h(a)$$

and dispersion

$$D_x^2(h) = \frac{1}{N(x)} \sum_{|a| \leq x} (h(a) - E_x(h))^2 = \frac{1}{N(x)} \sum_{|a| \leq x} h^2(a) - (E_x(h))^2$$

(cf. [1]).

Remark. In the case $\mathbf{M} = \mathbf{N}$ (the set of positive integers) we obtain by (2.1) the well known asymptotic density. Various examples of such sets $\mathbf{M}$ with valuations satisfying (i),(ii) are special arithmetical semigroups equipped with absolute value $|\cdot|$ in the sense of Knopfmacher [6].

Let f, g be two real-valued functions defined on $\mathbf{M}$ and $D_x^2(f) > 0, D_x^2(g) > 0$ for sufficiently large x. Consider their correlation coefficient with respect to γ_x given as follows

$$\rho_x = \rho_x(f, g) = \frac{|E_x(f \cdot g) - E_x(f) E_x(g)|}{D_x(f) \cdot D_x(g)}. \tag{2.2}$$

Clearly, if $\rho_x = 1$, then for every $\alpha \in \mathbf{M}(\mathbf{x})$ we have

$$g(\alpha) = A_x f(\alpha) + B_x,$$

where

$$A_x = \frac{E_x(f \cdot g) - E_x(f)E_x(g)}{D_x^2(f)},$$

and

$$B_x = E_x(g) - A_x E_x(f)$$

(cf. [1], [10]).

Note that if $\mathbf{M} = \mathbf{N}$ and f, g are statistically independent arithmetic functions, then

$$\rho_x(f, g) \to 0, x \to \infty.$$

The line $\beta = A_x\alpha + B_x$ is well known as the regression line of f, g on $\mathbf{M}(\mathbf{x})$ (cf. [1], [10]). Consider now the function $g - A_x f$. By some calculations we derive

$$E_x(g - A_x f) = B_x,$$

and

$$D_x^2(g - A_x f) = (1 - \rho_x^2)D_x^2(g),$$

where ρ_x is given by (2.2). Thus from Tchebyschev's inequality we get

$$\gamma_x\left(\{a : |g(a) - A_x f(a) - B_x| \geq \varepsilon\}\right) \leq \frac{(1 - \rho_x^2)D_x^2(g)}{\varepsilon^2}. \tag{2.3}$$

Suppose now that there exist some A, B such that $A_x \to A, B_x \to B$.

We have

$$|g(a) - Af(a) - B| \leq |g(a) - A_x f(a) - B_x| + |f(a)||A_x - A| + |B_x - B|.$$

Thus if f is bounded we obtain for $\varepsilon > 0$ and sufficiently large x

$$|g(a) - Af(a) - B| \geq \varepsilon \Rightarrow |g(a) - A_x f(a) - B_x| \geq \frac{\varepsilon}{2},$$

and so (2.3) yields

$$\gamma_x(\{a : |g(a) - Af(a) - B| \geq \varepsilon\}) \leq \frac{4(1 - \rho_x^2)D_x^2(g)}{\varepsilon^2}. \tag{2.4}$$

Now we can state our main result.

Theorem 1. *Let f, g be two bounded real-valued functions on $\mathbf{M}$.*

(1) Suppose that $D_x^2(f) > 0, D_x^2(g) > 0$ for sufficiently large x and $A_x \to A, B_x \to B$ and $\rho_x \to 1$ (as $x \to \infty$). Then for every $\varepsilon > 0$

$$\gamma(\{a : |g(a) - Af(a) - B| \geq \varepsilon\}) = 0. \tag{2.5}$$

(2) Let $D_x^2(g) > K > 0$ for some K and assume (2.5) for every $\varepsilon > 0$ and suitable constants A, B. Then $\rho_x \to 1$ (as $x \to \infty$).

Proof. If g is bounded, then also $D_x^2(g)$ is bounded and the assertion (1) follows directly from (2.4).

Put $g_1 := Af + B$. The assumptions of (2) imply that $A \neq 0$ and $D_x^2(f) > K_1 > 0, D_x^2(g_1) > K_2 > 0$ for some constants K_1, K_2. Then we have

$$\rho_x(g_1, f) = 1 \tag{2.6}$$

for each x.

Denote for two bounded real-valued functions h_1, h_2:

$$h_1 \sim h_2 \Longleftrightarrow \gamma(\{a : |h_1(a) - h_2(a)| \geq \varepsilon\}) = 0.$$

It can be verified easily that $\sim$ is an equivalence relation compatible with addition and multiplication, moreover for each uniformly continuous function F it follows from (ii)

$$h_1 \sim h_2 \Rightarrow E_x(F(h_1)) - E_x(F(h_2)) \to 0$$

as $x \to \infty$. In the case (2) we have $g \sim g_1$. This yields

$$D_x^2(g) - D_x^2(g_1) \to 0, x \to \infty, \tag{2.7}$$

but (2.6) gives

$$D_x(g_1)D_x(f) = |E_x(g_1 f) - E_x(g_1)E_x(f)|.$$

Hence, observing that $D_x(f)$ is bounded we obtain from (2.7).

$$D_x(g)D_x(f) - |E_x(g_1 f) - E_x(g_1)E_x(f)| \to 0, x \to \infty \ .$$

Therefore

$$D_x(g)D_x(f) - |E_x(gf) - E_x(g)E_x(f)| \to 0, x \to \infty \ ,$$

and the assertion follows.

The Besicovitch functions. Consider now the case $\mathbf{M} = \mathbf{N}$. An arithmetic function h is called almost periodic if for each $\varepsilon > 0$ there exists a periodic function h_ε such that

$$\overline{\lim_{N\to\infty}} \frac{1}{N} \sum_{n \leq N} |h(n) - h_\varepsilon(n)| < \varepsilon.$$

(These functions are also called Besicovitch functions). The class of all such arithmetic functions will be denoted by B^1. For a survey of the properties of B^1 we refer to [8] or [2]. For each $h \in B^1$ there exist the limits

$$\lim_{N\to\infty} E_N(h) := E(h)$$

and

$$\lim_{N\to\infty} D_N^2(h) := D^2(h).$$

If $f, g \in B^1$ are bounded then also $f + g, f \cdot g \in B^1$.

Thus, if $D^2(f), D^2(g) > 0$ then the limits $\lim_{x\to\infty} A_x$, $\lim_{x\to\infty} B_x$ and $\lim_{x\to\infty} \rho_x$ always exist.

The relation $h \sim L$ for an arithmetic function h and some constant L, used in the proof of Theorem 1, is defined in [4] as the statistical convergence of h to L. Šalát [11] gives the following characterisation of the statistical convergence:

Theorem 2. *Let h be an arithmetic function, and L a constant. Then $h \sim L$ if and only if there exists a subset $K \subset \mathbf{N}$ such that the asymptotic density of K is 1 and $\lim_{n\to\infty, n\in K} h(n) = L$.*

Denote by B^2 the set of all Besicovitch functions of h, such that h is bonded and $D^2(h) > 0$. Thus for two functions $f, g \in B^2$ there exists the limit $\rho(f, g) := \lim_{n\to\infty} \rho_N(f, g)$. Theorem 1 and Theorem 2 immediately imply:

Theorem 3. *Let $f, g \in B^2$. Then $\rho(f, g) = 1$ if and only if there exist some constants A, B and a set $K \subset \mathbf{N}$ of asymptotic density 1 such that*

$$\lim_{n\to\infty, n\in K} f(n) - Ag(n) - B = 0.$$

Let us conclude this note by the remarking that the statistical convergence of the real valued function on $\mathbf{M}$ can be characterized analogously as in the paper [11], using the same ideas. Let h be a real valued function on $\mathbf{M}$ and L a real constant. Consider $K \subset \mathbf{M}$, then we write

$$\lim_{a\in K} h(a) = L \Leftrightarrow \forall \varepsilon > 0 \exists x_0 \forall a \in K : |a| > x_0 \Longrightarrow |h(a) - L| < \varepsilon.$$

Theorem 4. *Let h be a real valued function on $\mathbf{M}$ and L a constant. Then $h \sim L$ if and only if there exists a set $K \subset \mathbf{M}$ such that $\gamma(K) = 1$ and $\lim_{a\in K} h(a) = L$.*

Sketch of proof. Put $K_n = \{a \in \mathbf{M} : |h(a) - L| < \frac{1}{n}\}$ for $n \in \mathbf{N}$. Clearly it holds that $\gamma(K_n) = 1, n = 1, 2, \ldots$. Thus it can be selected such an increasing sequence of positive integers $\{x_n\}$ that for $x > x_n$ we have

$$\gamma_x(K_n) > \left(1 - \frac{1}{n}\right), \quad n = 1, 2, \ldots.$$

Put

$$K = \bigcup_{n=1}^{\infty} K_n \cap \Big(M(x_{n+1}) \setminus M(x_n) \Big).$$

Using the fact that the sequence of sets K_n is non increasing it can be proved that $\gamma(K) = 1$, and $\lim_{a \in K} h(a) = L$, by a similary way as in [11].

References

[1] Billingsley, P., *Measure and Probability*, John Willey.

[2] Besicovitch, A. S., *Almost periodic functions,* Dover, New York, 1954.

[3] Grabner, P. J. and Tichy, R. F., Remarks on statistical independence of sequences, *Math. Slovaca*, **44**, No. 1, (1994), 91–94.

[4] Fast, H., Sur la convergence statistique, *Coll. Math.*, **2** (1951), 241–244.

[5] Grabner, P. J., Strauch, O. and Tichy, R. F., L^p-discrepancy and statistical independence of sequences, *Czech. Math. Journal*, **49**, (124), (1999), 97–110.

[6] Knopfmacher, J., *Abstract analytic number theory,* Dover Publications, INC, New York, 1975.

[7] Novoselov, E. V., Topological theory of divisibility, (Russian), *Uchen. Zap. Elabuz.* PI **8** (1960), 3–23.

[8] Postnikov, R. G., *Introduction to analytic number theory,* Nauka, Moscow, 1971, (in Russian), english translation Amer. Math. Soc., Providence, R. I., 1988.

[9] Rauzy, G., *Propriétés statistiques de suites arithmetiques,* Le Mathematicien, **15**, Collection SVP, Presses Universitaires de France, Paris, 1976.

[10] Rényi, A., *Wahrscheinlichkeitstheorie,* Teubner Verlag, VEB, Berlin.

[11] Šalát, T., On statistically convergent sequences of real numbers, *Math. Slovaca*, **30**, (1980), No. 2, 139–150.

[12] Waerden, v. d. B. L., *Mathematische Statistik,* Springer-Verlag, Berlin–Göttingen–Heidelberg, 1957.

Milan Păstéka
Slovac Academy of Sciences
Stefanikova 49, SK-814 73 Bratislava
Slovakia
e-mail: pasteka@mat.savba.sk

Robert F. Tichy
Institut für Mathematik TU Graz
Steyrergasse 30, A-801 Graz
Austria
e-mail: tichy@tugraz.at

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 115–122*

EGY NEGYEDRENDŰ REKURZÍV SOROZATCSALÁDRÓL

Pethő Attila (Debrecen, Hungary)

Emlékül Kiss Péternek, a rekurzív sorozatok fáradhatatlan kutatójának.

Abstract. Let $a,b\in\mathbf{Z}$ and $\delta\in\{1,-1\}$ such that $a^2-4(b-2\delta)\neq 0$, $b\delta\neq 2$ and if $\delta=1$, then $b\neq 2a-2$. We define the fourth order recursive sequence $G_n=G_n(a,b,\delta)$, $n\geq 0$ by the initial terms $G_0=0$, $G_1=1$, $G_2=a$, $G_3=a^2-b-\delta$ and by the recursion

$$G_{n+4}=aG_{n+3}-bG_{n+2}+\delta aG_{n+1}-G_n,\quad n\geq 0.$$

Similarly, the sequence $\widehat{G}_n=\widehat{G}_n(a,b,\delta)$, $n\geq 0$ is defined by the same recursive relation but with initial terms $\widehat{G}_0=4$, $\widehat{G}_1=a$, $\widehat{G}_2=a^2-2b$, $\widehat{G}_3=a^3-3ab+3a\delta$. It is shown that G_n behaves in some sense similarly as the Fibonacci sequence and $\widehat{G}_n$ as the Lucas sequence. More precisely we prove that G_n is a divisibility sequence and $\widehat{G}_n$ divides $\widehat{G}_m$ whenever n is odd and divides m. We prove further that these sequences are closely related to the second order sequences defined by the initial terms $g_0=0$, $g_1=1$, as well as $\widehat{g}_0=2$, $\widehat{g}_1=a$ and by the recursion

$$g_{n+2}=ag_{n+1}-(b-2\delta)g_n,\quad n\geq 0.$$

We show for example that if p is a prime then

$$G_p(a,b,\delta)\equiv g_p(a,b,\delta)\pmod p\quad\text{and}\quad \widehat{G}_p(a,b,\delta)\equiv\widehat{g_p}(a,b,\delta)\pmod p.$$

1. Bevezetés

Legyenek $a,b\in\mathbf{Z}$ és $\delta\in\{1,-1\}$ olyanok, hogy $a^2-4(b-2\delta)\neq 0$, $b\delta\neq 2$, és ha $\delta=1$, akkor $b\neq 2a-2$. Legyen továbbá a $G_n=G_n(a,b,\delta)$, $n\geq 0$ sorozat a $G_0=0$, $G_1=1$, $G_2=a$, $G_3=a^2-b-\delta$ kezdőértékkel és a

$$G_{n+4}=aG_{n+3}-bG_{n+2}+\delta aG_{n+1}-G_n,\quad n\geq 0 \tag{1}$$

rekurzióval definiálva.

Hasonlóképpen legyen a $\widehat{G}_n=\widehat{G}_n(a,b,\delta)$, $n\geq 0$ sorozat a $\widehat{G}_0=4$, $\widehat{G}_1=a$, $\widehat{G}_2=a^2-2b$, $\widehat{G}_3=a^3-3ab+3a\delta$ kezdőtagokkal és ugyancsak az (1) rekurzióval definiálva.

A dolgozat az OTKA T42985 és T38225 pályázatok támogatásával készült.

Dolgozatunkban megmutatjuk, hogy a $\{G_n\}_{n=0}^{\infty}$ sorozat bizonyos szempontból hasonlóképpen viselkedik, mint a Fibonacci, míg a $\widehat{G}_n$, mint a Lucas-sorozat. Pontosabban igaz az

1. Tétel. A $\{G_n\}_{n=0}^{\infty}$ *oszthatósági sorozat, azaz ha* $d|n$, *akkor* $G_d|G_n$.

2. Tétel. *Ha* n *páratlan és* $d|n$, *akkor* $\widehat{G}_d|\widehat{G}_n$.

Az 1. Tételt a $b = 1, 3$, $\delta = 1$ speciális esetekben a [2] dolgozatban bizonyítottuk.

A fenti negyedfokú sorozatok szoros kapcsolatban állnak a $g_0 = 0$, $g_1 = 1$, illetve a $\widehat{g}_0 = 2$, $\widehat{g}_1 = a$ kezdőértékekkel és a

$$g_{n+2} = ag_{n+1} - (b - 2\delta)g_n, \quad n \geq 0 \tag{2}$$

rekurzióval definiált másodrendű rekurzív sorozatokkal. A pontos összefüggéseket a 4. Tételben fogalmazzuk meg.

Végezetül megmutatjuk, hogy a $\{G_n\}$ és $\{g_n\}$, illetve a $\{\widehat{G}_n\}$ és $\{\widehat{g}_n\}$ sorozatok p prímszám szerinti redukáltjai is összefüggnek.

3. Tétel. *Legyen* p *prímszám. Akkor*

$$G_p(a, b, \delta) \equiv g_p(a, b, \delta) \pmod{p} \quad \textit{és} \tag{3}$$

$$\widehat{G}_p(a, b, \delta) \equiv \widehat{g}_p(a, b, \delta) \pmod{p}. \tag{4}$$

Az 5. tételben megfogalmazott kongurenciák prímszámok tesztelésére is alkalmasak, erre a kérdésre azonban most nem térünk ki.

2. Kapcsolat a $\{G_n\}$ és $\{g_n\}$ sorozatok karakterisztikus polinomjai között

A $\{G_n\}$ és persze a $\{\widehat{G}_n\}$ karakterisztikus polinomja

$$P_G(x) = x^4 - ax^3 + bx^2 - \delta ax + 1.$$

Könnyen belátható, hogy

$$\frac{1}{x^2}P_G(x) = \left(x + \frac{\delta}{x}\right)^2 - a\left(x + \frac{\delta}{x}\right) + b - 2\delta,$$

azaz az $\frac{1}{x^2}P_G(x)$ racionális törtfüggvényben az $y = x + \frac{\delta}{x}$ helyettesítést végrehajtva a

$$P_g(y) = y^2 - ay + b - 2\delta$$

polinomot kapjuk, amelyik a $\{g_n\}$ és $\{\widehat{g}_n\}$ sorozatok karakterisztikus polinomja. Az $a^2-4(b-2\delta)\neq 0$ feltétel miatt $P_g(y)$-nak két különböző gyöke van, melyeket ε és ε'-vel fogunk jelölni. A $b\delta\neq 2$ feltétel miatt $b-2\delta\neq 0$, így $\varepsilon\varepsilon'\neq 0$.

A kezdőértékek megválasztása miatt

$$g_n=\frac{\varepsilon^n-\varepsilon'^n}{\varepsilon-\varepsilon'} \quad \text{és} \quad \widehat{g}_n=\varepsilon^n+\varepsilon'^n \tag{5}$$

teljesül minden $n\geq 0$-ra.

Ha η a $P_G(x)$ gyöke, akkor $\eta\neq 0$ és $\frac{\delta}{\eta}$ is gyöke $P_G(x)$-nek. A $b\neq 2a-2$, ha $\delta=1$ feltétel miatt $\eta\neq\frac{\delta}{\eta}$. A $P_G(x)$ és $P_g(y)$ polinomok közötti összefüggés miatt $\eta+\frac{\delta}{\eta}$ gyöke $P_g(y)$-nak. Feltehető, hogy $\eta+\frac{\delta}{\eta}=\varepsilon$. Mivel $\varepsilon\neq\varepsilon'$, így $P_G(x)$-nek van olyan ϑ-val jelölt gyöke, amelyre $\vartheta+\frac{\delta}{\vartheta}=\varepsilon'$. Eredményeinket az alábbi állításokban foglaljuk össze.

1. Lemma. *Legyenek $a,b,\in\mathbf{Z}$ és $\delta\in\{1,-1\}$ olyanok, hogy $a^2-4(b-2\delta)\neq 0$, $b\delta\neq 2$, és $b\neq 2a-2$, ha $\delta=1$. Ekkor*

(i) $P_g(x)$-nek két nullától különböző gyöke van: ε és ε'.

(ii) $P_G(x)$-nek négy különböző gyöke van: η, $\frac{\delta}{\eta}$, ϑ és $\frac{\delta}{\vartheta}$.

(iii) Teljesül, hogy

$$\varepsilon=\eta+\frac{\delta}{\eta} \quad \text{és} \quad \varepsilon'=\vartheta+\frac{\delta}{\vartheta}.$$

Az 1. Lemmában megfogalmazott tulajdonságokat, valamint a $\{G_n\}$ és a $\{\widehat{G}_n\}$ sorozatok kezdőértékeit felhasználva könyen belátható, hogy

$$G_n=\frac{\eta^n+\left(\frac{\delta}{\eta}\right)^n-\vartheta^n-\left(\frac{\delta}{\vartheta}\right)^n}{\eta+\frac{\delta}{\eta}-\vartheta-\frac{\delta}{\vartheta}} \tag{6}$$

és

$$\widehat{G}_n=\eta^n+\left(\frac{\delta}{\eta}\right)^n+\vartheta^n+\left(\frac{\delta}{\vartheta}\right)^n \tag{7}$$

teljesül minden $n\geq 0$-ra.

3. A tételek bizonyítása

Az 1. tétel bizonyítása. Vegyük észre először az

$$\eta^n+\left(\frac{\delta}{\eta}\right)^n-\vartheta^n-\left(\frac{\delta}{\vartheta}\right)^n=(\eta^n-\vartheta^n)\left(1-\left(\frac{\delta}{\eta\vartheta}\right)^n\right)$$

relációt, amelyik minden $n \geq 0$-ra teljesül. Ebből és (6)-ból következik, hogy

$$G_n = \frac{\eta^n - \vartheta^n}{\eta - \vartheta} \cdot \frac{1 - \left(\frac{\delta}{\eta^\vartheta}\right)^n}{1 - \frac{\delta}{\eta^\vartheta}}. \tag{8}$$

Az η és ϑ a $P_G(x)$ gyökei, így egységek valamely algebrai számtestben. Ebből következik, hogy $\frac{\delta}{\eta^\vartheta}$ is egység.

A definícióból nyilvánvaló, hogy $G_n \in \mathbf{Z}$ minden $n \geq 0$-ra. Legyen $d \in \mathbf{N}$ olyan, hogy $d \mid n$. Akkor $G_n/G_d \in \mathbf{Q}$.

Másrészt (8)-ból következik, hogy

$$\frac{G_n}{G_d} = \frac{\eta^n - \vartheta^n}{\eta^d - \vartheta^d} \cdot \frac{1 - \left(\frac{\delta}{\eta^\vartheta}\right)^n}{1 - \left(\frac{\delta}{\eta^\vartheta}\right)^d}.$$

Elemi algebrai azonosság szerint

$$\frac{\eta^n - \vartheta^n}{\eta^d - \vartheta^d} = \eta^{n-d} + \eta^{n-2d}\vartheta^d + \cdots + \eta^d\vartheta^{n-2d} + \vartheta^{n-d}.$$

A jobb oldali összeadandók mindegyike algebrai egész, így az összegük is az. Ugyanígy látható be, hogy a második faktor is algebrai egész, így G_n/G_d olyan algebrai egész szám, amelyik $\mathbf{Q}$-ban van. Ez pedig csak akkor lehetséges, ha $G_n/G_d \in \mathbf{Z}$.

2. tétel bizonyítása. Ez hasonló az 1. Tétel bizonyításához. Azt kell csak észrevennünk, hogy

$$\eta^n + \left(\frac{\delta}{\eta}\right)^n + \vartheta^n + \left(\frac{\delta}{\vartheta}\right)^n = (\eta^n + \vartheta^n)\left(1 + \left(\frac{\delta}{\eta\vartheta}\right)^n\right), \tag{9}$$

valamint ha n páratlan és $d \mid n$, akkor

$$\frac{\eta^n + \vartheta^n}{\eta^d + \vartheta^d}, \quad \text{illetve} \quad \frac{1 + \left(\frac{\delta}{\eta\vartheta}\right)^n}{1 + \left(\frac{\delta}{\eta\vartheta}\right)^d}$$

algebrai egészek.

1. Megjegyzés. Az osztható rekurzív sorozatokat Bézivin, Pethő és van der Poorten [1] karakterizálták. Az általunk definiált $\{G_n\}$ és $\{\widehat{G}_n\}$ sorozatoknak az az érdekessége, hogy bár (8), illetve (9) szerint felbomlanak két másodrendű lineáris

rekurzív sorozat szorzatára, a faktorok azonban általában nem racionális egészek. Ez történik például, ha $b = -1$ vagy -3 és $\delta = -1$.

Az $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ kezdőértékekkel, illetve rekurzióval definiált Fibonacci-sorozat jelenti az iskolapéldát osztható rekurzív sorozatokra. Erre könyű olyan bizonyítást adni (ld. pl. [3]), amelyik csak az egész számok aritmetikáját használja. Hasonló bizonyítást a $\{G_n\}$ és a $\{\widehat{G}_n\}$ sorozatokra nem sikerült találnunk.

2. Megjegyzés. A Fibonacci-sorozatokra, sőt az általánosabb $R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ sorozatokra, ahol α és β az $\alpha x^2 - r_1 x - r_0$, $r_1, r_0 \in \mathbf{Z}$ polinom gyökei, az 1. tételnél erősebb $(R_n, R_d) = R_{(n,d)}$ reláció is teljesül.

Ez általában nem igaz az általunk definiált $\{G_n\}$ sorozatokra. Tekintsük például az

n	0	1	2	3	4	5	6	7	8	9	10
G_n	0	1	1	5	7	20	35	83	161	355	720

sorozatot, amelyik a

$$G_{n+4} = G_{n+3} + 3G_{n+2} - G_{n+1} - G_n$$

rekurziónak tesz eleget. Ekkor például $(G_3, G_5) = 5 \neq G_1$ és $(G_4, G_6) = 7 \neq G_2$. Könnyen lehet persze további példákat is találni, ezért érdekes kérdés a $\{G_n\}$ és $\{\widehat{G}_n\}$ sorozatokra a tagok legnagyobb közös osztójának jellemzése.

A 3. tétel bizonyítása. A (8), (9) valamint az 1. lemma (iii) relációkat használjuk a bizonyításban. Legyen p prímszám. Ha $p = 2$, akkor (3) és (4) a sorozatok kezdőértékei megválasztása miatt teljesül. A továbbiakban tehát feltehető, hogy p páratlan. Ekkor

$$\begin{aligned}
\frac{\varepsilon^p - \varepsilon'^p}{\varepsilon - \varepsilon'} &= \frac{\left(\eta + \frac{\delta}{\eta}\right)^p - \left(\vartheta + \frac{\delta}{\vartheta}\right)^p}{\varepsilon - \varepsilon'} \\
&= \frac{\sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i} \delta^i \left(\eta^{p-2i} + \left(\frac{\delta}{\vartheta}\right)^{p-2i} - \vartheta^{p-2i} - \left(\frac{\delta}{\vartheta}\right)^{p-2i}\right)}{\varepsilon - \varepsilon'} \\
&= \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i} \delta^i \frac{\eta^{p-2i} + \left(\frac{\delta}{\eta}\right)^{p-2i} - \vartheta^{p-2i} - \left(\frac{\delta}{\vartheta}\right)^{p-2i}}{\eta + \frac{\delta}{\eta} - \vartheta - \frac{\delta}{\vartheta}} \\
&= \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i} \delta^i G_{p-2i}.
\end{aligned}$$

Mivel $\binom{p}{i}$ minden $1 \le i \le p-i$-re osztható p-vel, így az előző azonosságból

$$g_p \equiv G_p \pmod{p},$$

azaz (3) következik.

A (4) kongruencia hasonlóképpen ellenőrizhető.

3. Megjegyzés. A (3) és (4) kongruenciák nem prímkritériumok, azaz vannak olyan összetett számok, amelyekre (3), illetve (4) teljesül. A Fibonacci-sorozat és a 2. megjegyzésben megadott sorozat például az $(a, b, \delta) = (1, -3, -1)$ paraméterekkel van definiálva. A $0 \le n \le 10000$ intervallumban az $n = 15, 25, 45, 121, 125, 375, 525, 625, 1125, 1605, 2205, 2375, 3125, 4375, 5425, 8925, 9375$ összetett számokra is teljesül (3).

4. További összefüggések a $\{G_n\}$ és $\{g_n\}$, illetve a $\{\widehat{G}_n\}$ és $\{\widehat{g}_n\}$ sorozatok között

Az előbbiekben láthattuk, hogy a $\{G_n\}$ és $\{g_n\}$, illetve $\{\widehat{G}_n\}$ és $\{\widehat{g}_n\}$ sorozatok között szoros kapcsolat van. A 3. részben például beláttuk, hogy páratlan p egészre g_p kifejezhető $G_p, G_{p-2}, \dots, G_1$ egész együtthatós lineáris kombinációjaként. Most az ellenkező irányú kapcsolatot vizsgáljuk, azaz G_p-t ($\widehat{G}_p - t$) szeretnénk kifejezni a $\{g_n\}$ ($\{\widehat{g}_n\}$) sorozat elemei lineáris kombinációjaként. A következő állítás biztosan ismert, de nem sikerült referenciát találnunk.

2. Lemma. *Definiáljuk a* $\{\lambda_i^{(j)}\}_{\substack{i\ge 0\\ j\ge 2}}$ *sorozatot a következőképpen:*

$$\lambda_0^{(0)} = 2,\ \lambda_1^{(0)} = 0,\ \lambda_0^{(1)} = 1,\ \lambda_1^{(1)} = 0 \quad \textit{és}$$
$$\lambda_0^{(2k+2)} = -\lambda_0^{(2k)},\ \lambda_{k+1}^{(2k+2)} = \lambda_k^{(2k+1)},\ \lambda_i^{(2k+2)} = \lambda_{i-1}^{(2k+1)} - \lambda_i^{(2k)},\ 1 \le i \le k \quad \textit{és}$$
$$\lambda_0^{(2k+3)} = 0,\ \lambda_{k+1}^{(2k+3)} = \lambda_{k+1}^{(2k+2)},\ \lambda_i^{(2k+3)} = \lambda_i^{(2k+2)} - \lambda_i^{(2k+1)},\ 1 \le i \le k.$$

Ha $0 \le n = 2k + e$, *ahol* $e \in \{0, 1\}$, *akkor*

$$X^n + Y^n = \sum_{i=0}^{k} \lambda_i^{(n)} (X+Y)^{2i+e} (XY)^{k-i}.$$

Bizonyítás. Egyszerű teljes indukció, felhasználva az

$$X^{n+1} + Y^{n+1} = (X^n + Y^n)(X+Y) - XY(X^{n-1} + Y^{n-1})$$

azonosságot.

3. Lemma. *Bármely $n \geq 0$ és $0 \leq i \leq [\frac{n}{2}]$-re* $\lambda_i^{(n)}(-1)^{[\frac{n}{2}]-i} \geq 0$.

Bizonyítás. A 2. lemmában leírtak miatt

$$\lambda_{[n/2]}^{(n)} = 1 \quad \text{és} \quad \lambda_0^{(n)} = \begin{cases} 2(-1)^{[n/2]}, & \text{ha } n \text{ páros,} \\ 0, & \text{ha } n \text{ páratlan.} \end{cases}$$

Így az állítás igaz minden n-re és $i = 0$, $[\frac{n}{2}]$-re. Tegyük fel, hogy igaz minden $m < n$-re, és legyen $0 < i < [\frac{n}{2}]$.

Ha n páros, mondjuk $n = 2k + 2$, és $0 < i < k + 1$, akkor

$$\begin{aligned} \lambda_i^{(2k+2)}(-1)^{k+1-i} &= \lambda_{i-1}^{(2k+1)}(-1)^{k+1-i} - \lambda_i^{(2k)}(-1)^{k+1-i} \\ &= \lambda_{i-1}^{(2k+1)}(-1)^{[\frac{2k+1}{2}]-(i-1)+2} + \lambda_i^{(2k)}(-1)^{k-i+2}. \end{aligned}$$

A jobb oldalon álló kifejezésben az indukciós hipotézis szerint mindkét összeadandó nem negatív, így az összegük is az.

Ha pedig n páratlan, például $n = 2k + 3$, és $0 < i < k + 1$, akkor

$$\begin{aligned} \lambda_i^{(2k+3)}(-1)^{k+1-i} &= \lambda_i^{(2k+2)}(-1)^{k+1-i} - \lambda_i^{(2k+1)}(-1)^{k+1-i} \\ &= \lambda_i^{(2k+2)}(-1)^{[\frac{2k+2}{2}]-i} + \lambda_i^{(2k+1)}(-1)^{[\frac{2k+1}{2}]-i+2}, \end{aligned}$$

és az előbbi esethez hasonlóan következtethetünk arra, hogy a kifejezés nem negatív.

4. Tétel. *Legyenek a, b, δ a Bevezetésben megfogalmazott feltételeknek eleget tevő egész számok és $0 \leq n = 2k + e$, ahol $e \in \{0, 1\}$. Akkor*

$$G_n(a,b,\delta) = \begin{cases} \sum\limits_{i=0}^{k} \lambda_i^{(n)}\, g_{2i+e}(a,b,\delta), & \text{ha } \ de = 1, \\ \sum\limits_{i=0}^{k} |\lambda_i^{(n)}|\, g_{2i+e}(a,b,\delta), & \text{ha } \ \delta = -1, \end{cases}$$

és

$$\widehat{G}_n(a,b,\delta) = \begin{cases} \sum\limits_{i=0}^{k} \lambda_i^{(n)}\, \widehat{g}_{2i+e}(a,b,\delta), & \text{ha } \ \delta = 1, \\ \sum\limits_{i=0}^{k} |\lambda_i^{(n)}|\, \widehat{g}_{2i+e}(a,b,\delta), & \text{ha } \ \delta = -1. \end{cases}$$

Bizonyítás. Csak az első állítást bizonyítjuk, mert a második bizonyítása teljesen hasonló. Az a, b és δ argumentumokat elhagyjuk a továbbiakban. A (6) azonosságot és a 2. lemma állítását felhasználva

$$
\begin{aligned}
G_n &= \frac{\eta^n + \left(\frac{\delta}{\eta}\right)^n - \left(\vartheta^n + \left(\frac{\delta}{\vartheta}\right)^n\right)}{\varepsilon - \varepsilon'} \\
&= \frac{1}{\varepsilon - \varepsilon'} \left(\sum_{i=0}^{k} \lambda_i^{(n)} \left(\eta + \frac{\delta}{\eta}\right)^{2i+e} \left(\eta \frac{\delta}{\eta}\right)^{k-i} - \sum_{i=0}^{k} \lambda_i^{(n)} \left(\vartheta + \frac{\delta}{\vartheta}\right)^{2i+e} \left(\vartheta \frac{\delta}{\vartheta}\right)^{k-i} \right) \\
&= \frac{1}{\varepsilon - \varepsilon'} \sum_{i=0}^{k} \lambda_i^{(n)} \delta^{k-i} \left(\varepsilon^{2i+e} - \varepsilon'^{2i+e}\right) \\
&= \sum_{i=0}^{k} \lambda_i^{(n)} \delta^{k-i} g_{2i+e}.
\end{aligned}
$$

Végül felhasználva a 3. lemmát, kapjuk az állítást.

Irodalom

[1] J.-P. Bézivin, A. Pethő and A. J. van der Poorten, A full characterization of divisibility sequences, *Amer. J. Math.*, **112** (1990), 985–1001.

[2] A. Pethő, Complete solutions to a family of quartic diophantine equations, *Math. Comp.*, **57** (1991), 777–798.

[3] N. N. Vorobjev, *Fibonacci Numbers* (in Russian, sixth edition), Nauka Moskau, 1978.

Pethő Attila
Debreceni Egyetem
Számítógéptudományi Tanszék
H-4010 Debrecen, Pf. 12
e-mail: pethoe@math.klte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 123–132*

ON ADDITIVE FUNCTIONS SATISFYING CONGRUENCE PROPERTIES

Bui Minh Phong (Budapest, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. In this paper, we consider those integer-valued additive functions f_1 and f_2 for which the congruence $f_1(an+b) \equiv f_2(cn)+d \pmod{n}$ is satisfied for all positive integers n and for some fixed integers $a \geq 1$, $b \geq 1$, $c \geq 1$ and d. Our result improve some earlier results of K. Kovács, I. Joó, I. Joó & B. M. Phong and P. V. Chung concerning the above congruence.

1. Introduction

The problem concerning the characterization of some arithmetical functions by congruence properties initiated by Subbarao [10] was studied later by several authors. M. V. Subbarao proved that if an integer-valued multiplicative function $g(n)$ satisfies the congruence

$$g(n+m) \equiv g(m) \pmod{n}$$

for all positive integers n and m, then there is a non-negative integer α such that

$$g(n) = n^{\alpha}$$

holds for all positive integers n. Recently some authors generalized and improved this result in a variety of ways. A. Iványi [3] obtained that the same result holds when m is a fixed positive integer and g is an integer-valued completely multiplicative function. For further results and generalizations of this problem we refer to the works of B. M. Phong [7]–[8], B. M. Phong & J. Fehér [9], I. Joó [4] and I. Joó & B. M. Phong [5]. For example, it follows from [8] that if an integer-valued multiplicative function $g(n)$ satisfies the congruence

$$g(An+B) \equiv C \pmod{n}$$

for all positive integers n and for some fixed integers $A \geq 1$, $B \geq 1$ and $C \neq 0$ with $(A, B) = 1$, then there are a non-negative integer α and a real-valued Dirichlet character $\chi_A \pmod{A}$ such that

$$g(n) = \chi_A(n) n^{\alpha}$$

It was financially supported by OTKA T 043657

holds for all positive integers n which are prime to A.

In the following let $\mathcal{A}$ and $\mathcal{A}^*$ denote the set of all integer-valued additive and completely additive functions, respectively. Let $\mathbb{N}$ denote the set of all positive integers. A similar problem concerning the characterization of a zero-function as an integer-valued additive function satisfying a congruence property have been studied by K. Kovács [6], P. V. Chung [1]–[2], I. Joó [4] and I. Joó & B. M. Phong [5]. It was proved by K. Kovács [6] that if $f \in \mathcal{A}^*$ satisfies the congruence

$$f(An + B) \equiv C \pmod{n}$$

for some integers $A \geq 1$, $B \geq 1$, C and for all $n \in \mathbb{N}$, then

$$f(n) = 0$$

holds for all $n \in \mathbb{N}$ which are prime to A. This result was extended in [1], [2], [4] and [5] for integer-valued additive functions f. It follows from the results of [2] and [4] that for integers $A \geq 1$, $B \geq 1$, C and functions $f_1 \in \mathcal{A}$, $f_2 \in \mathcal{A}^*$ the congruence

$$f_1(An + B) \equiv f_2(n) + C \pmod{n} \quad (\forall n \in \mathbb{N})$$

implies that $f_2(n) = 0$ for all $n \in \mathbb{N}$ and $f_1(n) = 0$ for all $n \in \mathbb{N}$ which are prime to A.

Our purpose in this paper is to improve the above results by showing the following

Theorem 1. *Assume that $a \geq 1$, $b \geq 1$, $c \geq 1$ and d are fixed integers and the functions f_1, f_2 are additive. Then the congruence*

$$f_1(an + b) \equiv f_2(cn) + d \pmod{n} \tag{1}$$

is satisfied for all $n \in \mathbb{N}$ if and only if the equation

$$f_1(an + b) = f_2(cn) + d \tag{2}$$

holds for all $n \in \mathbb{N}$.

Theorem 2. *Assume that $a \geq 1$, $b \geq 1$, $c \geq 1$ and d are fixed integers. Let $a_1 = \frac{a}{(a,\, b)}$, $b_1 = \frac{b}{(a,\, b)}$ and*

$$\mu := \begin{cases} 1 & \text{if } 2 \mid a_1 b_1 \\ 2 & \text{if } 2 \nmid a_1 b_1. \end{cases}$$

If the additive functions f_1 and f_2 satisfy the equation (2) for all $n \in \mathbb{N}$, then

$$f_1(n) = 0 \quad \text{for all} \quad n \in \mathbb{N},\ (n, \mu a b_1) = 1$$

and

$$f_2(n) = 0 \quad \text{for all} \quad n \in \mathbb{N},\ (n, \mu c b_1) = 1.$$

2. Lemmas

Lemma 1. *Assume that $f^* \in \mathcal{A}^*$ satisfies the congruence*

$$f^*(An + B) \equiv f^*(n) + D \pmod{n}$$

for some fixed integers $A \geq 1$, $B \geq 1$ and D. Then $f^*(n) = 0$ holds for all $n \in \mathbb{N}$.

Proof. Lemma 1 follows from Theorem 2 of [4].

Lemma 2. *Assume that $f \in \mathcal{A}$ satisfies the congruence*

$$f(An + B) \equiv D \pmod{n}$$

for some fixed integers $A \geq 1$, $B \geq 1$ and D. Then $f(n) = 0$ holds for all $n \in \mathbb{N}$ which are prime to A.

Proof. This is the result of [1].

Lemma 3. *Assume that f_1, $f \in \mathcal{A}$ satisfy the congruence*

$$f_1(An + 1) \equiv f(Cn) + D \pmod{n} \tag{3}$$

holds for all $n \in \mathbb{N}$ with some integers $A \geq 1$, $C \geq 1$ and D. Then

$$f(n) = f[(n, 6C^2)] \quad \text{for all} \quad n \in \mathbb{N}$$

and $f_1(m) = 0$ holds for all $m \in \mathbb{N}$, which are prime to $6AC$. Here (x, y) denotes the greatest common divisor of the integers x and y.

Proof. In the following we shall denote by n^* the product of all distinct prime divisors of positive integer n.

For each positive integer M let $P = P(M)$ be a positive integer for which

$$(M^2 - 1)^* | ACP. \tag{4}$$

It is obvious from (4) that

$$(ACM(M+1)Pn + 1, AC(M+1)Pn + 1) = 1,$$

$$\left(C^2(M+1)^2 Pn, ACMPn + 1\right) = 1$$

and

$$(ACM(M+1)Pn+1)\,(AC(M+1)Pn+1) = AC(M+1)^2Pn[ACMPn+1]+1$$

hold for all $n \in I\!N$. Using these relations and appealing to the additive nature of the functions f_1 and f, we can deduce from (3) that

$$f(ACMPn+1) \tag{5}$$

$$\equiv -f\left(C^2(M+1)^2Pn\right)+f\left(C^2M(M+1)Pn\right)+f\left(C^2(M+1)Pn\right)+D \pmod n$$

is satisfied for all n, $M \in I\!N$, where $P = P(M)$ satisfies the condition (4).

Let $M = 2$, $P(2) = 3$ and $M = 3$, $P(3) = 2$. In these cases (4) is true and so it follows from (5) that

$$f(6ACn+1) \equiv -f(27C^2n)+f(18C^2n)+f(9C^2n)+D \pmod n \tag{6}$$

and

$$f(6ACn+1) \equiv -f(32C^2n)+f(24C^2n)+f(8C^2n)+D \pmod n \tag{7}$$

are satisfied for all $n \in I\!N$. Let N and n be positive integers with the condition

$$(N(N+1), 6ACn+1) = 1. \tag{8}$$

By using the relation

$$(6ACn+1)(6^2A^2C^2Nn^2+1) = 6ACn\,[6ACNn(6ACn+1)+1]+1$$

and that

$$\left(6ACn+1, 6^2A^2C^2Nn^2+1\right) = (6ACn+1, N+1) = 1,$$

$$(6ACNn, 6ACn+1) = (6ACn+1, N) = 1,$$

it follows from (6) and (7) that

$$-f\left(162AC^3Nn^2\right)+f\left(108AC^3Nn^2\right)+f\left(54AC^3Nn^2\right) \equiv -f\left(27C^2Nn\right) \tag{9}$$

$$+f\left(18C^2Nn\right)+f\left(9C^2Nn\right)-f\left(27C^2n\right)+f\left(18C^2n\right)+f\left(9C^2n\right)+D \pmod n$$

and

$$-f\left(192AC^3Nn^2\right)+f\left(144AC^3Nn^2\right)+f\left(48AC^3Nn^2\right) \equiv -f\left(32C^2Nn\right) \tag{10}$$

$$+f\left(24C^2Nn\right)+f\left(8C^2Nn\right)-f\left(32C^2n\right)+f\left(24C^2n\right)+f\left(8C^2n\right)+D \pmod n$$

hold for all n, $N \in I\!N$ satisfying (8).

Let Q be a fixed positive integer. First we apply (9) when $N = 1$, $n = Qm$, $(m, Q) = 1$ and $m \to \infty$. It is obvious that (8) holds, and so by (9) we have

$$f\left(Q^2\right) = 2f(Q) \quad \text{for} \quad Q \in I\!N, (Q, 6AC) = 1. \tag{11}$$

Now let $N = Q$ and $n = Q^k(6CQm + 1)$ with k, $m \in I\!N$. It is obvious that (8) holds for infinity many integers m, because $\left(36AC^2Q^{k+1}, 6ACQ^k + 1\right) = 1$. These with (9) show that

$$f\left(Q^{2k+1}\right) = f\left(Q^k\right) + f\left(Q^{k+1}\right) \quad \text{for all} \quad Q \in I\!N, (Q, 6AC) = 1. \tag{12}$$

From (11) and (12) we obtain that

$$f\left(Q^k\right) = kf(Q) \quad \text{for all} \quad Q \in I\!N, (Q, 6AC) = 1. \tag{13}$$

Thus, by using the additivity of f it follows from (8) and (13) that (9) and (10) hold for all N, $n \in I\!N$, and they with $n = Qm$, $(m, 6ACNQ) = 1$, $m \to \infty$ imply that

$$-f\left(162AC^3NQ^2\right) + f\left(108AC^3NQ^2\right) + f\left(54AC^3NQ^2\right) = -f\left(27C^2NQ\right)$$

$$+f\left(18C^2NQ\right) + f\left(9C^2NQ\right) - f\left(27C^2Q\right) + f\left(18C^2Q\right) + f\left(9C^2Q\right) D$$

and

$$-f\left(192AC^3NQ^2\right) + f\left(144AC^3NQ^2\right) + f\left(48AC^3NQ^2\right) = -f\left(32C^2NQ\right)$$

$$+f\left(24C^2NQ\right) + f\left(8C^2NQ\right) - f\left(32C^2Q\right) + f\left(24C^2Q\right) + f\left(8C^2Q\right) + D$$

hold for all N, $Q \in I\!N$. Consequently

$$-f\left(27C^2NQ\right) + f\left(18C^2NQ\right) + f\left(9C^2NQ\right) - f\left(27C^2Q\right) + f\left(18C^2Q\right) + f\left(9C^2Q\right)$$

$$-f\left(27C^2NQ^2\right) + f\left(18C^2NQ^2\right) + f\left(9C^2NQ^2\right) - f\left(27C^2\right) + f\left(18C^2\right) + f\left(9C^2\right) \tag{14}$$

and

$$-f\left(32C^2NQ\right) + f\left(24C^2NQ\right) + f\left(8C^2NQ\right) - f\left(32C^2Q\right) + f\left(24C^2Q\right) + f\left(8C^2Q\right)$$

$$= -f\left(32C^2NQ^2\right) + f\left(24C^2NQ^2\right) + f\left(8C^2NQ^2\right) - f\left(32C^2\right) + f\left(24C^2\right) + f\left(8C^2\right) \tag{15}$$

are satisfied for all N, $Q \in I\!N$.

For each prime p let $e = e(p)$ be a non-negative integer for which $p^e \parallel C^2$.

First we consider the case when $(p,6)=1$. By applying (14) with $Q=p$, $N=p^l$ $(l\geq 0)$, we have

$$f\left(p^{l+e(p)+2}\right)-f\left(p^{l+e(p)+1}\right)=f\left(p^{e(p)+1}\right)-f\left(p^{e(p)}\right) \quad \text{for all} \quad l\geq 0,$$

which shows that for all integers $\beta\geq e(p)$

$$f\left(p^{\beta+1}\right)-f\left(p^{\beta}\right)=f\left(p^{e(p)+1}\right)-f\left(p^{e(p)}\right). \tag{16}$$

Now we consider the case $p=2$. Applying (14) with $Q=2$ and $n=2^l$, $(l\geq 0)$ one can check as above that

$$f\left(2^{\beta+1}\right)-f\left(2^{\beta}\right)=f\left(2^{e(2)+2}\right)-f\left(2^{e(2)+1}\right). \tag{17}$$

Finally, we consider the case $p=3$. Applying (15) with $Q=3$ and $N=3^l$, $l\geq 0$ we also get

$$f\left(3^{\beta+1}\right)-f\left(3^{\beta}\right)=f\left(3^{e(3)+2}\right)-f\left(3^{e(3)+1}\right). \tag{18}$$

Now we write

$$f(n)=f^*(n)+F(n),$$

where f^* is a completely additive function defined as follows:

$$f^*(p):=\begin{cases} f\left(p^{e(p)+1}\right)-f\left(p^{e(p)}\right) & \text{for } (p,6)=1 \\ f\left(p^{e(p)+2}\right)-f\left(p^{e(p)+1}\right) & \text{for } p=2 \text{ or } p=3 \end{cases}. \tag{19}$$

Then, from (16)-(19) it follows that

$$F\left(p^k\right)=F\left[(p^k,6C^2)\right] \quad \text{for} \quad (k=0,1,\ldots).$$

Thus, we have proved that

$$F(n)=F\left[(n,6C^2)\right] \tag{20}$$

is satisfied for all $n\in I\!N$.

We shall prove that $f^*(n)=0$ for all $n\in I\!N$ and $f_1(m)=0$ for all $m\in I\!N$ which are prime to $6AC$.

We note that, by considering $n=2m$ and taking into account (6), we have

$$f(12ACm+1)\equiv -f(54C^2m)+f(36C^2m)+f(18C^2m)+D \pmod m$$

Since $f = f^* + F$, from the last relation and (20) we get

$$f^*(12ACm + 1) \equiv f^*(m) + [f^*(12C^2) + F(6C^2) + D] \pmod{m},$$

which with Lemma 1 shows that $f^*(n) = 0$ for all $n \in \mathbb{N}$. This shows that $f \equiv F$, i.e.

$$f(n) = f[(n, 6C^2)]$$

holds for all $n \in \mathbb{N}$. Now, by applying (3) with $n = 6Cm$ and using the last relation and Lemma 2, we have that $f_1(n) = 0$ holds for all $n \in \mathbb{N}$ which are prime to $6AC$.

The proof of Lemma 3 is completed.

3. Proof of Theorem 1

It is obvious that (1) follows from (2). We shall prove that if (1) is true, then (2) holds.

Assume that the functions f_1 and $f_2 \in \mathcal{A}$ satisfy the congruence (1) for some integers $a \geq 1$, $b \geq 1$, $c \geq 1$ and d. It is obvious that (1) implies the fulfilment of

$$f_1(abn + 1) \equiv f_2(b^2cn) + d - f_1(b) \pmod{n}$$

for all $n \in \mathbb{N}$. By Lemma 3,

$$f_2(n) = f_2[(n, 6b^4c^2)] \quad \text{for all} \quad n \in \mathbb{N} \tag{21}$$

and

$$f_1(n) = 0 \tag{22}$$

for all $n \in \mathbb{N}$ which are prime to $6abc$.

We shall prove that

$$f_1(an + b) = f_2(cn) + d \tag{23}$$

is true for all $n \in \mathbb{N}$.

Let K be a positive integer. By (21) and (22), we have

$$f_1(6ab^4ct + 1) = 0,$$

$$f_2[6b^4c^2(aK + b)t + cK] = f_2(cK)$$

hold for all positive integers t, consequently

$$f_1(aK+b) - f_2(cK) - d = f_1(aK+b) + f_1(6ab^4ct+1) - f_2(cK) - d$$
$$= f_1[a(6b^4c(aK+b)t+K)+b] - f_2[6b^4c^2(aK+b)t+cK] - d$$

holds for every positive integer t. Thus, by applying (1) with $n = 6b^4c(aK+b)t+K$, the last relation proves that (23) holds for $n = K$.

This completes the proof of Theorem 1.

4. Proof of Theorem 2

As we have shown in the proof of Theorem 1, if the functions $f_1,\ f_2 \in \mathcal{A}$ satisfy (2), then (21) and (22) imply

$$f_1(m) = 0 \quad \text{for all} \quad m \in I\!N,\ (m, 6abc) = 1 \tag{24}$$

and

$$f_2(n) = 0 \quad \text{for all} \quad n \in I\!N,\ (m, 6bc) = 1. \tag{25}$$

Let $D = (a,b)$, $a_1 = \frac{a}{D}$, $b_1 = \frac{b}{D}$. It is clear that for each positive integer $M,\ (M, a_1) = 1$ there are $m_0, n_0 \in I\!N$ such that

$$Mm_0 = a_1n_0 + b_1,\ \ (m_0,\ a_1) = 1 \ \text{ and } \ (M,\ n_0) = (M,\ b_1). \tag{26}$$

Let

$$u(M) := \begin{cases} 1, & \text{if} \quad 2 \mid a_1 \frac{M}{(M,\ b_1)} \frac{b_1}{(M,\ b_1)}, \\ 2, & \text{if } 2 \ \not| \ a_1 \frac{M}{(M,\ b_1)} \frac{b_1}{(M,\ b_1)}. \end{cases} \tag{27}$$

By applying the Chinese Remainder Theorem and using (26)–(27), we can choose a positive integer t_1 such that $m_1 = a_1t_1 + m_0,\ n_1 = Mt_1 + n_0$ satisfy the following conditions:

$$Mm_1 = a_1n_1 + b_1 \ \ ,$$

$$\frac{n_1}{u(M)(M,\ b_1)} \ \text{ is an integer,}$$

and

$$(m_1,\ 6abc) = \left(\frac{n_1}{u(M)(M,\ b_1)},\ 6bc\right) = 1.$$

Hence, we infer from (2) and (24)-(25) that

$$f_1(DM) = f_1(DMm_1) = f_1(an_1 + b) = f_2(cn_1) + d = f_2\left[cu(M)(M, b_1)\right] + d,$$

consequently

$$f_1[DM] = f_2[cu(M)(M, b_1)] + d \tag{28}$$

hold for all $M \in I\!N$, $(M,\ a_1) = 1$. This implies that

$$f_1(n) = 0 \quad \text{for all} \quad n \in I\!N, \quad (n,\ \mu a b_1) = 1, \tag{29}$$

where $\mu \in \{1,\ 2\}$ such that $2|\ \mu a_1 b_1$.

Now we prove that

$$f_2(n) = 0 \quad \text{for all} \quad n \in I\!N, \quad (n,\ \mu c b_1) = 1. \tag{30}$$

For each positive integer n, let $M(n) := a_1 n + b_1$ and $U(n) := u(a_1 n + b_1)$. Since $(M(n),\ b_1) = (n,\ b_1)$ and

$$a_1 \frac{M(n)}{(M(n),\ b_1)} \frac{b_1}{(M(n),\ b_1)} \equiv a_1 \frac{b_1}{(n,\ b_1)} \left[\frac{n}{(n,\ b_1)} + 1\right] \pmod 2,$$

we have

$$U(n) := \begin{cases} 1, & \text{if} \quad 2 \mid a_1 \frac{b_1}{(n,\ b_1)} \left[\frac{n}{(n,\ b_1)} + 1\right], \\ 2, & \text{if } 2 \not| \ a_1 \frac{b_1}{(n,\ b_1)} \left[\frac{n}{(n,\ b_1)} + 1\right]. \end{cases}$$

Hence, (2) and (28) show that

$$f_2(cn) = f_1(an + b) - d = f_1[DM(n)] - d = f_2[cU(n)(n, b_1)]$$

is satisfied for all $n \in I\!N$, which implies (29). Thus, (29) is proved.

By (29) and (30), the proof of Theorem 2 is completed.

References

[1] Chung, P. V., Note on additive functions satisfying some congruence properties I.–II., *Studia Math. Hungar.*, **28** (1993), 359–362, 427–429.

[2] Chung, P. V., Note on additive functions satisfying some congruence properties III., *Ann. Univ. Sci. Budapest. Eötvös, Sect. Math.*, **37** (1994), 263–266.

[3] Iványi, A., On multiplicative functions with congruence property, *Ann. Univ. Sci. Budapest. Eötvös, Sect. Math.*, **5** (1972), 151–155.

[4] Joó, I., Arithmetical functions satisfying a congruence property, *Acta Math. Hungar.*, **63** (1994), 1–21.

[5] Joó, I. and Phong, B. M., Arithmetical functions with congruence properties, *Ann. Univ. Sci. Budapest. Eötvös, Sect. Math.*, **35** (1992), 151–155.

[6] Kovács, K., On additive functions satisfying some congruence properties, *Periodica Math. Hungar.*, **23** (3) (1991), 227–231.

[7] Phong, B. M., Multiplicative functions satisfying a congruence property, *Studia Sci. Math. Hungar.*, **26** (1991), 123–128.

[8] Phong, B. M., Multiplicative functions satisfying a congruence property V., *Acta Math. Hungar.*, **62** (1–2)(1993), 81–87.

[9] Phong, B. M. and Fehér, J., Note on multiplicative functions satisfying congruence property, *Ann. Univ. Sci. Budapest. Eötvös, Sec. Math.*, **33** (1990), 261–265.

[10] Subbarao, M. V., Arithmetic functions satisfying congruence property, *Canad. Math. Bull.*, **9** (1966), 143–146.

Bui Minh Phong
Eötvös Loránd University
Department of Computer Algebra
Pázmány Péter sét. I/C
H-1117 Budapest
Hungary
e-mail: bui@compalg.inf.elte.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 133–145*

STRUCTURE OF THE GROUP OF QUASI MULTIPLICATIVE ARITHMETICAL FUNCTIONS

Štefan Porubský (Prague, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. The structure of the group of quasi multiplicative arithmetical functions such that $f(1)\neq 0$ with respect to Dirichlet and the more general Davison convolution via an isomorphism to a subgroup of upper triangular and Toeplitz matrices will be described.

AMS Classification Number: 11A25

1. Introduction

In what follows unless contrary is stated **K** denotes a field between the field of complex **C** and the field of rational numbers **Q**. Let Arit(**K**) denote the set of all **K**-valued arithmetical functions (i.e. functions defined on the set **N** of positive integers with values in **K**), and Mult(**K**) the set of *nonzero* (i.e. non identically vanishing) **multiplicative** arithmetical functions f, that is functions such that $f(nm) = f(n)f(m)$ whenever $(m, n) = 1$. The sets Arit(**K**) and Mult(**K**) endowed with the **Dirichlet convolution**

$$(f \star_D g)(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$$

are of basic importance in various number-theoretical considerations.

Given an $f \in \mathrm{Arit}(\mathbf{K})$ we can assign it the formal Dirichlet series

$$f \mapsto T(f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}. \tag{1}$$

The author was supported by the Grant Agency of the Czech Republic, Grant # 201/01/0471.

If we define the multiplication of formal Dirichlet series by

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \cdot \sum_{n=1}^{\infty} \frac{g(n)}{n^s} = \sum_{n=1}^{\infty} \frac{(f \star_D g)(n)}{n^s},$$

then for the set of all formal Dirichlet series

$$\mathcal{D}(\mathbf{K}) = \left\{ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ : \ a_n \in \mathbf{K} \right\}$$

with multiplication defined above we have:

Lemma 1. ([13, Theorem 4.6.1]) *The map T defined by (1) gives an isomorphism between the semigroups* $(\mathrm{Arit}(\mathbf{K}), \star_D)$ *and* $(\mathcal{D}(\mathbf{K}), .)$.

The underlying property for the investigation that follows is the following result due to Bell:

Lemma 2. *(a) The set of arithmetical functions $f \in \mathrm{Arit}(\mathbf{K})$ for which $f(1) \neq 0$ forms a commutative group with respect to Dirichlet convolution $\star_D$.*
(b) The set $(\mathrm{Mult}(\mathbf{K}), \star_D)$ *forms a subgroup of the group* $(\mathrm{Arit}(\mathbf{K}), \star_D)$.

Dehaye [5] analyzed the structure of the group $(\mathrm{Mult}(\mathbf{R}), \star_D)$ of real valued non-zero multiplicative functions with respect to the Dirichlet convolution $\star_D$. He proved (among other) that $(\mathrm{Mult}(\mathbf{R}), \star_D)$ is isomorphic to the complete direct[1] product $\widetilde{\prod}_{i \in \mathbf{N}} \mathrm{D}^1_{\mathbf{R}}$ of countably many copies of $\mathrm{D}^1_{\mathbf{R}}$, where $\mathrm{D}^1_{\mathbf{R}}$ is the set of all matrices

$$\begin{pmatrix} 1 & a & b & c & d & \cdots \\ 0 & 1 & a & b & c & \cdots \\ 0 & 0 & 1 & a & b & \cdots \\ 0 & 0 & 0 & 1 & a & \cdots \\ 0 & 0 & 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

which all entries on descending diagonals are equal real numbers while the main diagonal entries are equal to 1. In what follows we show using more number theoretical arguments that his results can be extended to more general types of arithmetical functions and convolutions.

[1] For the definition of the complete (or Cartesian) direct product the reader is referred to [6] or [5] or sources quoted [5], if necessary.

2. Quasi multiplicative functions

If $f \in \mathrm{Arit}(\mathbf{K})$ is a multiplicative arithmetical function, then $f(m)f(n) = f((m,n))f\Big(\frac{m.n}{(m,n)}\Big)$ for all $m, n \in \mathbf{N}$. An arithmetical function f is called **quasi multiplicative** ([11,14]) if $f(1) \neq 0$ and

$$f(1)f(mn) = f(m)f(n) \quad \text{whenever} \quad (m,n) = 1. \tag{2}$$

The set of nonzero $\mathbf{K}$-valued quasi multiplicative functions will be denoted by $\mathrm{Quas}(\mathbf{K})$. The analogue of the second part of Theorem 2 for nonzero quasi multiplicative can be verified by a direct computation:

Lemma 3. *The set* $\mathrm{Quas}(\mathbf{K})$ *forms a commutative group with respect to Dirichlet convolution* $\star_D$.

Note that an f with $f(1) \neq 0$ is quasi multiplicative if, and only if, $f^- = \frac{1}{f(1)}f$ is multiplicative.[2] There follows from this observation (or directly from (2)) that

$$f^-(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \prod_{i=1}^{k} \frac{f(p_i^{\alpha_i})}{f(1)} = \prod_{i=1}^{k} f^-(p_i^{\alpha_i}), \tag{3}$$

or

$$f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = f(1)^{1-k} \prod_{i=1}^{k} f(p_i^{\alpha_i}) = f(1) \prod_{i=1}^{k} f^-(p_i^{\alpha_i}), \tag{4}$$

whenever $p_1, \ldots, p_k$ are distinct primes and $\alpha_i \in \mathbf{N}$. The next two results follow from well known properties of multiplicative functions:

Lemma 4. *If* $f \in \mathrm{Arit}(\mathbf{K})$ *with* $f(1) \neq 0$, *then* f *is quasi multiplicative if and only if (3) or (4) holds for all* k *tuples* $p_1, \ldots, p_k$ *of distinct primes and all* $\alpha_i \in \mathbf{N}$.

If f is multiplicative then under the isomorphism of Lemma 1 the image $T(f)$ is a Dirichlet series admitting the so called Euler factorization. Therefore if $f \in \mathrm{Quas}(\mathbf{K})$, then applying this fact to the multiplicative function f^- we get:

Lemma 5. *If* $f \in \mathrm{Quas}(\mathbf{K})$ *then* $T(f)/f(1)$ *is the formal product of the series*

$$1 + \frac{f(p)}{f(1)p^s} + \frac{f(p^2)}{f(1)p^{2s}} + \frac{f(p^3)}{f(1)p^{3s}} + \cdots, \tag{5}$$

where the product runs over all primes p.

[2] If f is multiplicative, so is $f(Mn)/f(M)$, where M is any positive integer.

The series (5) is in a one-to-one relation to a formal power series called **Bell series** $f_p(x)$ of an $f \in \mathrm{Arit}(\mathbf{K})$ with $f(1) \neq 0$ modulo the prime p

$$f_p(x) = f(1) + f(p)x + f(p^2)x^2 + \cdots = \sum_{n=0}^{\infty} f(p^n)x^n.$$

In terms of Bell series we can characterize the quasi multiplicative functions as follows:

Lemma 6. *Let $f, g \in \mathrm{Quas}(\mathbf{K})$. Then $f = g$ if, and only if,*

$$f_p(x) = g_p(x) \quad \textit{for all primes } \ p,$$

or equivalently

$$f(p^\alpha) = g(p^\alpha) \quad \textit{for all primes } p \textit{ and integers } \alpha \geq 0.$$

The next result shows a close relation between Bell series and Dirichlet multiplication:

Lemma 7. ([1, Theorem 2.25]) *For any two arithmetical functions f and g let $h = f \star_D g$. Then for every prime p we have*

$$h_p(x) = f_p(x)g_p(x).$$

Perhaps a most natural proof of this result can be modelled using matrix multiplication of infinite upper triangular matrices of the type

$$f_p(x) \mapsto m_{\mathbf{K},D}(f_p) = \begin{pmatrix} f(1) & f(p) & f(p^2) & f(p^3) & \cdots \\ 0 & f(1) & f(p) & f(p^2) & \cdots \\ 0 & 0 & f(1) & f(p) & \cdots \\ 0 & 0 & 0 & f(1) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \tag{6}$$

Let $\mathcal{P}$ denote the set of all (rational) primes.

Theorem 8. *Let $\mathrm{D}_{\mathbf{K}}$ be the set of matrices of the type*[3]

$$T(a,b,c,d,e,\ldots) = \begin{pmatrix} a & b & c & d & e & \cdots \\ 0 & a & b & c & d & \cdots \\ 0 & 0 & a & b & c & \cdots \\ 0 & 0 & 0 & a & b & \cdots \\ 0 & 0 & 0 & 0 & a & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \quad \textit{with } a \neq 0, b, c, d, e, \ldots \in \mathbf{K}.$$

[3] *That is upper triangular (semi-definite) matrices that are constant along all diagonals parallel to the principal diagonal. Matrices possessing the later property are also called* **Toeplitz matrices**.

Then
(a) $\mathrm{D}_{\mathbf{K}}$ *is a group with respect to the matrix multiplication,*
(b) The group $(\mathrm{Quas}(\mathbf{K}), \star_D)$ *is isomorphic to a subgroup of the complete direct product* $\widetilde{\prod}_{p\in\mathcal{P}}\mathrm{D}_{\mathbf{K}}$*, defined by the condition that the diagonal value* a *is a common number in all components of an element of the direct product.*

Proof. (a) The proof can be based either on standard tools from matrix algebra or using our arithmetical background. Using the matrix algebra language let $A(m,n)$, $m,n \in \{1,2,3,\ldots\}$ be the (m,n)th entry of a matrix A. Then $A \in \mathrm{D}_{\mathbf{K}}$ if and only if

(1) if $n > m$ then $A(m,n) = 0$, i.e. A is upper triangular,
(2) $A(m+k, n+k) = A(m,n)$ for all indices $m,n \in \mathbf{N}, k \in \mathbf{Z}$ such that $\min\{m,n,n+k,m+k\} \geq 1$, i.e. A is Toeplitz.

Let $A_i \in \mathrm{D}_{\mathbf{K}}$, $i = 1,2$ and $A = A_1A_2$. Then $A(m,n) = \sum_{t=1}^{\infty} A_1(m,t)A_2(t,n)$. That A is upper triangular is easy to see. What concerns the second property it suffices to prove it for $k = 1$ only. Let $n \leq m$. Then[4]

$$A(m+1,n+1) = \sum_{t=1}^{\infty} A_1(m+1,t)A_2(t,n+1) = \sum_{t=n+1}^{m+1} A_1(m+1,t)A_2(t,n+1)$$
$$= \sum_{t=n}^{m} A_1(m,t)A_2(t,n) = A(m,n),$$

where in the second equality we used the fact that the matrices under consideration are upper triangular. The case $n > m$ is even easier to verify, for in this case at least one of the factors in the first sum vanishes. This shows that $D_{\mathbf{K}}$ is closed under the multiplication of matrices.

The presence of the identity element in $D_{\mathbf{K}}$ is clear. To prove the existence of inverse elements we switch to our arithmetical background.[5]

If $f \in \mathrm{Mult}(\mathbf{K})$, then also $f^{-1} \in \mathrm{Mult}(\mathbf{K})$. Lemma 7 implies that the Bell series modulo p of f^{-1} is given by

$$f_p^{-1}(x) = \frac{1}{f_p(x)}.$$

[4] Another form of the following rearrangement of the summands gives [3, p. 96–97] the **product matrix formula** for an $(m+1,n+1)$ entry of the product of two general Toeplitz matrices saying that $A(m+1,n+1) = A_1(m+1,1)A_2(1,n+1) + A(m,n)$.

[5] For another proof we refer to [3, Corollary of Theorem 2] where it is proved that *the only Toeplitz matrices with Toeplitz inverses are the triangular ones.*

Consequently, $f_p^{-1}(x)$ can be found by formal power series inversion and the corresponding element in $D_{\mathbf{K}}$ can be found for $\ell = f^{-1}$ noting that if

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots \\ 0 & 0 & 1 & 0 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & 0 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

and E is the infinite identity matrix, then

$$\ell_p(H) = \ell(1)E + \ell(p)H + \ell(p^2)H^2 + \cdots = \begin{pmatrix} \ell(1) & \ell(p) & \ell(p^2) & \ell(p^3) & \cdots \\ 0 & \ell(1) & \ell(p) & \ell(p^2) & \cdots \\ 0 & 0 & \ell(1) & \ell(p) & \cdots \\ 0 & 0 & 0 & \ell(1) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

This proves (a) and simultaneously that if $h = f \star_D g$, then

$$m_{\mathbf{K},D}(h_p) = h_p(H) = f_p(H)g_p(H) = m_{\mathbf{K},D}(f_p)m_{\mathbf{K},D}(g_p),$$

that is that the mapping (6) is a homomorphism. That this mapping is also a bijection follows from the fact that the (quasi) multiplicative functions are uniquely determined by its values at all prime powers arguments (including 1). Since the product of two Bell series modulo p of two quasi multiplicative functions is a Bell series modulo p of a quasi multiplicative function modulo p, (b) follows using the isomorphism which is the composition of the isomorphism described in part (a) and that of of Lemma 1taking into account the Euler factorization from Lemma 5.

If f is a nonzero multiplicative function then $f(1) = 1$ and Dehaye's result mentioned in the introduction for $\mathbf{K} = \mathbf{R}$ follows immediately. Dehaye proved this result via subsets

$$\mathbf{F}^p = \{f \in \mathrm{Mult}(\mathbf{R}) : f(n) = 0 \text{ for every } n > 1 \text{ not divisible by } p\}$$

for each $p \in \mathcal{P}$. However, the multiplicativity of f implies that

$$\mathbf{F}^p = \{f \in \mathrm{Mult}(\mathbf{R}) : f(n) = 0 \text{ for every } n > 1 \text{ which is not a power of } p\}.$$

Consequently, the Euler factorization of an $f \in \mathbf{F}^p$ reduces to one factor only, namely

$$T(f) = 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \frac{f(p^3)}{p^{3s}} + \cdots,$$

This observation immediately implies, first of all, the result extending [5, Theorem 2.2, Theorem 5.2] to an arbitrary $\mathbf{K}$:

Lemma 9. *For any prime p, $\mathbf{F}^p$ is a group which is isomorphic to $\mathrm{D}^1_{\mathbf{K}}$.*

Secondly, we have more generally:

Theorem 10. *If $P \subset \mathcal{P}$ is any set of primes then the set*

$$\{f \in \mathrm{Quas}(\mathbf{K}) : f(n) = 0 \text{ for every } n > 1 \text{ not divisible by a } p \in P\}.$$

is a group which is isomorphic to a subgroup of the complete direct product $\widetilde{\prod}_{p\in\mathcal{P}}\mathrm{D}_{\mathbf{K}}$, defined by the condition that the diagonal value a is a common number in all components of an element of the direct product. Its subset

$$\mathbf{F}^P = \{f \in \mathrm{Mult}(\mathbf{K}) : f(n) = 0 \text{ for every } n > 1 \text{ not divisible by a } p \in P\}$$

forms a subgroup which is isomorphic to $\widetilde{\prod}_{p\in P}\mathrm{D}^1_{\mathbf{K}}$.

Other results proved by Dehaye state that the group $\mathrm{Mult}(\mathbf{R})$ is torsion-free [5, Theorem 2.1] and divisible [5, Theorem 7.1]. To extend these results the following simple result will be useful:

Lemma 11. *Let $g \in \mathrm{Arit}(\mathbf{C})$ such that $g(1) \neq 0$. Then the equation $f^{(n)} = g$, where $f^{(n)} = \overbrace{f \star_D \ldots \star_D f}^{n \text{ times}}$, is soluble in $\mathrm{Arit}(\mathbf{C})$ and has n solutions here.*

Proof. The equation of the theorem can be solved inductively either by starting with the equation $(T(f))^n = T(g)$, or equivalently setting

$$\begin{aligned} &f(1) = \sqrt[n]{g(1)}, \quad \text{and} \\ &f(k) = \frac{1}{n(f(1))^{n-1}}\left(g(k) - \sum_{\substack{d_1\ldots d_n=k \\ d_1,\ldots,d_n\neq k}} f(d_1)\ldots f(d_n)\right), \quad \text{for } k > 1. \end{aligned} \tag{7}$$

Clearly if f is one solution of our equation, then all solutions of this equation are given by $\omega_i f$, where ω_i runs over all nth roots of unity.

A group $(G, .)$ is called **divisible** if the equation $x^n = a$ has a solution in G for every $a \in G$.

Theorem 12. *(a) The group $\{f \in \mathrm{Arit}(\mathbf{C}) : f(1) \neq 0\}$ is divisible and has torsion. Its torsion part is isomorphic to the group of all complex roots of unity, that is to group $\mathbf{Q}/\mathbf{Z}$.*
(b) If $\mathbf{C} \supset \mathbf{K} \supset \mathbf{Q}$, then $\mathrm{Mult}(\mathbf{K})$ is divisible and torsion-free.
(c) The groups $\mathrm{Arit}^+(\mathbf{R}) = \{f \in \mathrm{Arit}(\mathbf{R}) : f(1) > 0\}$ and $\mathrm{Quas}^+(\mathbf{R}) = \{f \in \mathrm{Quas}(\mathbf{R}) : f(1) > 0\}$ are divisible and torsion-free.

Proof. The proof follows easily from the previous Lemma. The verification that the solution given by (7) is (quasi) multiplicative can be proved directly.

The groups like Arit($\mathbf{K}$), Quas($\mathbf{K}$) or Mult($\mathbf{K}$) are not the only groups of arithmetical functions. In [14] infinite chains of subgroups of Arit($\mathbf{C}$) are constructed. The solvability of the equation $f^{(n)} = g$ which was investigated in many papers, cf. [8] and the papers quoted here, has an interesting grouptheoretic consequence ([6, §20]):

Corollary 13. *The groups* Arit($\mathbf{C}$), Arit$^+$($\mathbf{R}$), Quas$^+$($\mathbf{R}$) *and* Mult($\mathbf{K}$) *with* $\mathbf{C} \supset \mathbf{K} \supset \mathbf{Q}$ *have no maximal proper subgroup.*

Another consequence is the solvability of more general systems of compatible equations

$$\prod_{j\in J} x_j^{n_{ij}} = g_i, \qquad g_i \in G, i \in I$$

where among the integers n_{ij} only finitely many are nonzero for every j (cf. [6, §22]).

3. Davison convolution

The Dirichlet convolution has many possible generalizations. The following one was introduced in [4]. Let K be a $\mathbf{K}$-valued function defined on the set of the all ordered couples (n, d) of positive integers n, d satisfying $d|n$. Let $f, h \in$ Arit($\mathbf{K}$) be two arithmetical functions. By **(Davison) K-convolution** $f \star_K g$ we shall mean the operation

$$(f \star_K g)(n) = \sum_{d|n} K(n,d) f(d) g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} K(d_1 d_2, d_1) f(d_1) g(d_2).$$

The function K is called **kernel (of the convolution)**.

As already mentioned the set of non-zero multiplicative functions f endowed with Dirichlet' s convolution $\star_D$ forms a commutative group (cf. [1, Chapt. 2] or [12, Theorem 4.12]). To ensure a similar property with respect to the Davison convolution $\star_K$ some properties should be imposed on the kernel function K (cf. [4]):

(i) *The Davison convolution* $\star_K$ *is associative if and only if we have*

$$K(abc, bc)K(bc, c) = K(abc, c)K(ab, b) \text{ for every } a,\ b,\ c \in \mathbf{N},$$

or equivalently,

$$K(n,d)K(d,e) = K(n,e)K\left(\frac{n}{e}, \frac{d}{e}\right) \text{ for every } n, d,\ e \in \mathbf{N} \text{ with } d|n \text{ and } e|d.$$

(ii) *The Davison convolution* $\star_K$ *is commutative if and only if for every couple of elements* $a,\, b \in \mathbf{N}$ *there holds*

$$K(ab,a) = K(ab,b) \text{ for every } a,b \in \mathbf{N},$$

or equivalently,

$$K(n,d) = K\left(n, \frac{n}{d}\right) \text{ for every } n,\, d \in \mathbf{N} \text{ with } d|n.$$

The Davison convolution as operation does not possess the neutral element in general.

(iii) *The identity function* δ_1 *defined by* $\delta_1(n) = \delta_{1n}$*, where* δ_{ij} *is the Kronecker delta, is the unit element with respect to* $\star_K$ *if and only if*

$$K(n,n) = K(n,1) = 1 \text{ for every } n \in \mathbf{N}.$$

The next important question is the keeping up of the multiplicativity of arithmetical functions under the influence of the Davison convolution.

(iv) *The Davison convolution* $f \star_K g$ *of two multiplicative functions* f, g *is a multiplicative function if and only if*

$$K(abcd,ac) = K(ab,a)K(cd,c) \text{ for every } a,b,c,d \in \mathbf{N} \text{ with } (ab,cd) = 1.$$

The question about the existence of the inverse function f^{-1} to a given $f \in \mathrm{Arit}(\mathbf{K})$ with respect to the Davison convolution can be solved surprisingly quickly:

(v) *the inverse function* f^{-1} *of* f *with respect to* $\star_K$ *exists if and only if* $f(1) \neq 0$.
When this condition is fulfilled then f^{-1} can be defined recursively by

(j) If $n = 1$ then $f^{-1}(1) = \frac{1}{K(1,1)f(1)} = \frac{1}{f(1)}$.

(jj) Let $n > 1$ and suppose that $f^{-1}(m)$ is already defined for the all $m < n$. Then put

$$\begin{aligned} f^{-1}(n) &= \frac{-1}{K(n,n)f(1)} \sum_{\substack{bc=n \\ c\neq n}} f(b)f^{-1}(c)K(n,b) \\ &= \frac{-1}{f(1)} \sum_{\substack{bc=n \\ c\neq n}} f(b)f^{-1}(c)K(n,b). \end{aligned}$$

The first part of Lemma 2 can be now reproved using (v) in the following form:

Lemma 14. *The set of $f \in \mathrm{Arit}(\mathbf{K})$ for which $f(1) \neq 0$ forms a commutative group with respect to a K-convolution satisfying conditions (i)–(iii).*

Given a prime $p \in \mathcal{P}$ and a $\mathbf{K}$–valued function K defined on the set of all ordered couples (n,d) of positive integers n,d satisfying $d|n$, define $\mathrm{D}_{\mathbf{K},K,p}$ as the set of matrices of the type

$$\begin{pmatrix} aK(1,1) & bK(p,p) & cK(p^2,p^2) & dK(p^3,p^3) & eK(p^4,p^4) & \cdots \\ 0 & aK(p,1) & bK(p^2,p) & cK(p^3,p^2) & dK(p^4,p^3) & \cdots \\ 0 & 0 & aK(p^2,1) & bK(p^3,p) & cK(p^4,p^2) & \cdots \\ 0 & 0 & 0 & aK(p^3,1) & bK(p^4,p) & \cdots \\ 0 & 0 & 0 & 0 & aK(p^4,1) & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \tag{8}$$

where $a \neq 0$ and $a,b,c,d,e,\ldots \in \mathbf{K}$. If we put $a=1$ in elements of $\mathrm{D}_{\mathbf{K},K,p}$ we get a subset, say $\mathrm{D}^1_{\mathbf{K},K,p}$. As a generalization of Theorem 8 we get:

Theorem 15. *Let $\star_K$ be a Davison convolutions satisfying properties (i)–(iv). Then*

(a) $\mathrm{D}_{\mathbf{K},K,p}$ is a group with respect to the matrix multiplication,

(b) The group $(\mathrm{Quas}(\mathbf{K}),\star_K)$ is isomorphic to the subgroup of $\widetilde{\prod}_{p\in\mathcal{P}}\mathrm{D}_{\mathbf{K},K,p}$ defined by the condition that the diagonal value a is a common number in all components (8) of an element of the direct product.

(c) The group $(\mathrm{Mult}(\mathbf{K}),\star_K)$ is isomorphic to the group $\widetilde{\prod}_{p\in\mathcal{P}}\mathrm{D}^1_{\mathbf{K},K,p}$.

Proof. Since a quasi multiplicative function f is uniquely determined by values $f(1)\neq 0$, $f(p)$, $f(p^2)$, ... for every $p\in\mathcal{P}$, instead of working with indices of entries of matrices we can suppose without loss of generality that the elements of $\mathrm{D}_{\mathbf{K},K,p}$ are of the form

$$m_{\mathbf{K},K,}(f_p) = \begin{pmatrix} f(1)K(1,1) & f(p)K(p,p) & f(p^2)K(p^2,p^2) & f(p^3)K(p^3,p^3) & f(p^4)K(p^4,p^4)\cdots \\ 0 & f(1)K(p,1) & f(p)K(p^2,p) & f(p^2)K(p^3,p^2) & f(p^3)K(p^4,p^3)\cdots \\ 0 & 0 & f(1)K(p^2,1) & f(p)K(p^3,p) & f(p^2)K(p^4,p^2)\cdots \\ 0 & 0 & 0 & f(1)K(p^3,1) & f(p)K(p^4,p) \ \cdots \\ 0 & 0 & 0 & 0 & f(1)K(p^4,1) \ \cdots \\ \vdots & \vdots & \vdots & 0 & \vdots \quad \ddots \end{pmatrix}$$

where $f\in\mathrm{Quas}(\mathbf{K})$. Then the (i,j), $j\geq i$, entry of the product $m_{\mathbf{K},K,}(g_p)m_{\mathbf{K},K,}(f_p)$ is

$$\sum_{k=i}^{j} g(p^{k-i})f(p^{j-k})K(p^{k-1},p^{k-i})K(p^{j-1},p^{j-k}) =$$
$$\sum_{k=0}^{j-i} g(p^{k})f(p^{j-i-k})K(p^{i+k-1},p^{k})K(p^{j-1},p^{j-i-k}),$$

while its expected value is

$$(g \star_K f)(p^{j-i})K(p^{j-1},p^{j-i}) = \left(\sum_{k=0}^{j-i} g(p^k)f(p^{j-i-k})K(p^{j-i},p^k)\right) K(p^{j-1},p^{j-i}).$$

To prove that our multiplication is well defined we have to prove that

$$K(p^{j-1},p^{j-i})K(p^{j-i},p^k) = K(p^{j-1},p^{j-i-k})K(p^{i+k-1},p^k). \tag{9}$$

There follows from (i) that

$$K(p^{a+b+c},p^{b+c})K(p^{b+c},p^c) = K(p^{a+b+c},p^c)K(p^{a+b},p^b), \quad a,b,c \in \{0,1,2,\ldots\}.$$

Taking $a = i-1$, $b = k$, and $c = j-i-k$ we get

$$K(p^{j-1},p^{j-i})K(p^{j-i},p^{j-i-k}) = K(p^{j-1},p^{j-i-k})K(p^{i-1+k},p^k),$$

but (ii) implies $K(p^{j-i},p^{j-i-k}) = K(p^{j-i},p^k)$ and (9) follows.

The existence of the identity element and the inverse one in $D_{\mathbf{K},k,p}$ follows now from the fact that such elements exist in the set of quasi multiplicative functions.

There follows from the above lines that the mapping

$$f \in \mathrm{Quas}(\mathbf{K}) \mapsto \prod_{p\in\mathcal{P}} m_{\mathbf{K},K}(f_p)$$

is the desired isomorphism from $(\mathrm{Quas}(\mathbf{K}),\star_K)$ onto the subgroup of $\widetilde{\prod}_{p\in\mathcal{P}}\mathrm{D}_{\mathbf{K},K,p}$ defined by the condition that the diagonal value a is a common number in all components of an element of the direct product, thereby proving statement (b). The statement (c) follows in turn.

The definition of the quasi multiplicativness depends only on the ordinary multiplication between positive integers and the elements of $\mathbf{K}$, therefore the next corollary might be surprising at the first sight:

Corollary 16. [(81, p.191)] *Let $\star_L$ and $\star_K$ be two Davison convolutions satisfying properties (i)–(iv). Then the couples groups $(\mathrm{Quas}(\mathbf{K}),\star_L)$ and $(\mathrm{Quas}(\mathbf{K}),\star_K)$, and $(\mathrm{Mult}(\mathbf{K}),\star_K)$ and $(\mathrm{Mult}(\mathbf{K}),\star_L)$ are isomorphic.*

Proof. Using the above ideas an alternative proof (to that given in 81) can be given as follows.

If $f, g \in \mathrm{Quas}(\mathbf{K})$ then the mapping

$$m_{\mathbf{K},K}(f_p) \mapsto m_{\mathbf{K},L}(f_p)$$

is one–to–one and maps $D_{\mathbf{K},K,p}$ onto $D_{\mathbf{K},L,p}$ while

$$m_{\mathbf{K},K}(f_p \star_K g_p) \mapsto m_{\mathbf{K},L}(f_p \star_L g_p).$$

This induces an isomorphism between the subgroups of $\widetilde{\prod}_{p\in\mathcal{P}} \mathrm{D}_{\mathbf{K},K,p}$ and $\widetilde{\prod}_{p\in\mathcal{P}} \mathrm{D}_{\mathbf{K},L,p}$ defined by the condition that the diagonal value a is a common number in all components of an element of the direct product.

The reformulation of the remaining results of previous section for Davison convolutions due to the above isomorphism is left to the reader.

4. Concluding generalization

In the previous reasoning we used from the properties of positive integer only the unique factorization property. Thus all previous results can be lifted to arithmetical functions defined on the so called arithmetical semigroups.

Let G denote a free commutative semigroup relative to a multiplication operation denoted by juxtaposition, with identity element 1_G and with at most countably many generators. Such a semigroup will be called **arithmetical semigroup** if in addition a real-valued **norm** $|\cdot|$ is defined on G such that

(1) $|1_G| = 1, |a| > 1$ for all $a \in G$,

(2) $|ab| = |a|.|b|$ for all $a, n \in G$,

(3) the total number

$$N_G(x) = \sum_{\substack{|a|\le x \\ a\in G}} 1$$

of elements $a \in G$ of norm not exceeding x is finite for each real x.

The role of primes take over the generators of G.

More details on abstract approach to the theory of arithmetical functions via the notion of arithmetical semigroup can be found in [9] or [10], where the interested reader may also find many instances of arithmetical semigroups.

5. Acknowledgement

The author thanks the referee for corrections and many useful comments.

References

[1] Apostol, T. M., *Introduction to Analytic number Theory*, Springer-Verlag, New York – Heidelberg – Berlin, 1976.

[2] Bell, E. T., *Arithmetical Theory of Numerical Functions*, University of Washington 1915.

[3] Brown, A., Halmos, P. R., Algebraic properties of Toeplitz operators, *J. Reine Angew. Math.*, **213** 1963, 89–102.

[4] Davison, T. M. K., On arithmetical convolution, *Canad. Math. Bull.*, **9** (1966), 287–296.

[5] Dehaye, P. O., On the structure of the group of multiplicative arithmetical functions, *Bull. Belg. Math. Soc.*, **9** (2002), 15–21.

[6] Fuchs, L., *Infinite Abelian Groups*, Vol. I, Academic Press, New York and London, 1970.

[7] Haukkanen, P., Some classes of quasi–fields having isomorphic additive and multiplicative groups, *Rend. Mat. Appl.*, (7) **7** (1987), 181–191.

[8] Haukkanen, P., On the Davison convolution of arithmetical functions, *Canad. Math. Bull.*, **32** (4) (1989), 467–473.

[9] Knopfmacher, J., *Abstract Analytic Number Theory*, North-Holland Mathematical Library Vol.12, North-Holland & American Elsevier, Amsterdam – Oxford – New York, 1975.

[10] Knopfmacher, J., Recents developments and applications of abstract analytic number theory, *Quaest. Math.*, **24**, (2001), 291–3070.

[11] Lahiri, D. B., Hypo-multiplicative number-theoretic functions, *Aequationes Math.*, **9** (1973), 184–192.

[12] Niven, I., Zuckerman, H. S., *An Introduction to the Theory of Numbers* (Third Edition), J. Wiley & Sons, New York – London – Sydney – Toronto, 1972.

[13] Shapiro, H. N., *Introduction to the Theory of Numbers*, Wiley, 1983.

[14] Succi, F., Sul gruppo moltiplicativo delle funzioni aritmetiche regolari, *Rend. Mat. Appl.*, (5) **19** (1960), 458–472.

Štefan Porubský
Institute of Computer Science
Academy of Sciences of the Czech Republic
Pod Vodárenskou věží 2, 18207 Prague 8
Czech Republic
e-mail: Stefan.Porubsky@cs.cas.cz

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 147–165*

ON THE CONGRUENCE $u_n \equiv c \pmod{\mathfrak{p}}$, WHERE u_n IS A RECURRING SEQUENCE OF THE SECOND ORDER

Andrzej Schinzel (Warsaw, Poland)

Dedicated to the memory of Professor Péter Kiss

1. Introduction

The following assertion has been proved in [1] as a by-product of a study of exponential congruences (Corollary to Theorem 5). Let a sequence u_n of rational integers satisfy the recurrence relation $u_{n+1} = au_n + bu_{n-1}$, where $a^2 + 4b \neq 0$. If the congruence $u_n \equiv c \pmod{p}$ is soluble for almost all primes p and either $b = 0, -1$ or $b = 1$, $a \neq d^3 + 3d$ (d integer), then $c = u_m$ for an integer m.

The aim of this paper is to extend this result as follows.

Theorem 2. *Let K be a number field, u_n a sequence of elements of K satisfying the relation*

$$u_{n+1} = au_n + bu_{n-1}, \quad \text{where } a^2 + 4b \neq 0. \tag{1}$$

If $c \in K$, the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is soluble for almost all prime ideals $\mathfrak{p}$ of K and either $b = 0, -1$ or $b = 1$, $a = 0$ or $b = 1$, $a^2 + 4 \neq d^2$ (d an integer of K), then $c = u_m$, where m is an integer.

Corollary 1. *Let a sequence u_n of rationals satisfy the recurrence relation* (1). *If $c \in \mathbf{Q}$, the congruence $u_n \equiv c \pmod{p}$ is soluble for almost all primes p and $b = 0$, or ± 1, then $c = u_m$ for an integer m.*

Comparing Corollary 1 with Corollary quoted above from [1] we see that now u_n need not be integers and the condition $a \neq d^3 + 3d$ has disappeared.

Corollary 2. *Let K be an imaginary quadratic field and u_n a sequence of elements of K satisfying the recurrence relation* (1). *If $c \in K$, the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is soluble for almost all prime ideals $\mathfrak{p}$ of K and $b = 0$, or ± 1, then $c = u_m$ for an integer m.*

Theorem 2 is a consequence of the following theorem concerning exponential congruences.

Theorem 1. *Let K be a number field, $\alpha \in K^*$, $f \in K[z]$, $\deg f \leq 4$. The congruence*

$$f(\alpha^x) \equiv 0 \pmod{\mathfrak{p}}$$

is soluble for almost all prime ideals $\mathfrak{p}$ *of* K*, if and only if one of the following cases holds for a* β *in the splitting field of* f

$$z - \alpha^r \mid f(z), \quad r \in \mathbf{Z} \tag{2}$$

$$\alpha = \beta^2,\ \left(z - \beta^{2r_1+1}\right)\left(z + \beta^{2r_2}\right)\left(z + \beta^{2r_3+1}\right) \mid f(z),\ r_i \in \mathbf{Z}; \tag{3}$$

$$\alpha = \beta^2,\ \left(z - \beta^{2r_1+1}\right)\left(z - \zeta_4^{e_2}\beta^{2r_2}\right)\left(z + \beta^{2r_3+1}\right)\left(z - \zeta_4^{e_4}\beta^{2r_4+1}\right) \mid f(z), \quad r_i \in \mathbf{Z},\ e_2e_4 \text{ odd}; \tag{4}$$

$$\alpha = \beta^3,\ (z - \beta^{r_1})(z - \zeta_3^{e_2}\beta^{r_2})(z - \zeta_3^{e_3}\beta^{r_3})(z - \zeta_3^{e_4}\beta^{r_4}) \mid f(z),\ r_i \in \mathbf{Z}, \quad e_2r_1 \not\equiv 0,\ r_2 \equiv 0,\ e_3r_3 \equiv -1,\ e_4r_4 \equiv 1 \pmod 3; \tag{5}$$

$$\alpha = \beta^4,\ \left(z - \beta^{2r_1+1}\right)\left(z + \beta^{4r_2}\right)\left(z + \beta^{2r_3+1}\right)\left(z + \beta^{4r_4+2}\right) \mid f(z),\ r_i \in \mathbf{Z}; \tag{6}$$

ζ_q *denotes a root of unity of order* q*.*

Remark. In principle one could obtain a similar result for degree f bounded by any number b. However, the number of possibilities increases fast with b and the matter gets out of hand (cf. Theorem 5 in [1]).

Definition. A system of congruences $A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod{m_h}$ $(1 \le h \le g)$ is covering, if every integer vector $[t_0, t_1]$ satisfies at least one of these congruences.

Lemma 1. *A system of congruences*

$$A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod m \quad (1 \le h \le 4) \tag{7}$$

is covering, if and only if one of the following cases holds:

$$\text{for an } h_0 \le 4 : m \mid (A_{h_0 0}, A_{h_0 1})\,; \tag{8}$$

$$2 \mid m \text{ and for three distinct indices } h_1, h_2, h_3 \le 4 \tag{9}$$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod m,$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod m,$$
$$A_{h_3 0} \equiv 0, \quad A_{h_3 1} \equiv \frac{m}{2} \pmod m;$$

(10) $3 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \varepsilon_1 \frac{m}{3} \pmod{m},$$
$$A_{h_2 0} \equiv \varepsilon_2 \frac{m}{3}, \quad A_{h_2 0} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \varepsilon_3 \frac{m}{3} \pmod{m},$$
$$A_{h_4 0} \equiv -A_{h_4 1} \equiv \varepsilon_4 \frac{m}{3} \pmod{m};$$

where $[\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4] \in \{-1, 1\}^4$.

(11) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \varepsilon_3 \frac{m}{4} \pmod{m},$$
$$A_{h_4 0} \equiv -A_{h_4 1} \equiv \varepsilon_4 \frac{m}{4} \pmod{m},$$

where $[\varepsilon_3, \varepsilon_4] \in \{1, -1\}^2$;

(12) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_2 0} \equiv \varepsilon_2 \frac{m}{4}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_4 0} \equiv \varepsilon_4 \frac{m}{4}, \quad A_{h_4 1} \equiv \frac{m}{2} \pmod{m},$$

where $[\varepsilon_2, \varepsilon_4] \in \{-1, 1\}^2$;

(13) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \varepsilon_1 \frac{m}{4} \pmod{m},$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_4 0} \equiv \frac{m}{2}, \quad A_{h_4 1} \equiv \varepsilon_4 \frac{m}{4} \pmod{m},$$

where $[\varepsilon_1, \varepsilon_4] \in \{-1, 1\}^2$.

Proof necessity. Since each of the vectors $[1, 0]$ and $[0, 1]$ satisfies one of the congruences (7) we have for some h_1, h_2

$$A_{h_1 0} \equiv 0, \quad A_{h_2 1} \equiv 0 \pmod m.$$

If $h_1 = h_2 = h$ we have the case (8), thus assume $h_2 \neq h_1$. Since each of the vectors $[1, -1]$ and $[1, 1]$ satisfies one of the congruences (7) we have for some j_1, j_2

$$A_{j_1 0} - A_{j_1 1} \equiv 0, \quad A_{j_2 0} + A_{j_2 1} \equiv 0 \pmod m. \tag{14}$$

If $j_i \in \{h_1, h_2\}$ ($i = 1$ or 2), we have the case (9) with $h_3 = j_i$, thus we assume $j_i \notin \{h_1, h_2\}$ ($i = 1, 2$) and distinguish two cases:

$$j_1 \neq j_2 \tag{15}$$

and

$$j_1 = j_2. \tag{16}$$

In the case (15) excluding the case (8) we infer that $A_{h_1 1} \not\equiv 0 \pmod m$, $A_{h_2 0} \not\equiv 0 \pmod m$, $A_{j_1 0} \not\equiv 0 \pmod m$, $A_{j_2 0} \not\equiv 0 \pmod m$. Since each of the vectors $[\pm 2, 1]$, $[1, \pm 2]$ satisfies one of the congruences (7) for $h \in \{h_1, h_2, j_1, j_2\}$ we infer that either

$$2 \mid m, \quad A_{h_1 1} \equiv A_{h_2 0} \equiv \frac{m}{2} \pmod m, \tag{15.1}$$

or

$$3 \mid m, \quad A_{j_i 0} \equiv \varepsilon_{i+2} \frac{m}{3} \pmod m, \quad [\varepsilon_3, \varepsilon_4] \in \{-1, 1\}^2. \tag{15.2}$$

In the case (15.1), since each of the vectors $[\pm 3, 1]$ satisfies one of the congruences (7) for $h \in \{j_1, j_2\}$, we infer that either for an $i \leq 2$, $A_{j_i 0} \equiv \frac{m}{2} \pmod m$, or $4 \mid m$ and $A_{j_i 0} \equiv \varepsilon_{i+2} \frac{m}{4} \pmod m$ ($i = 1, 2$) where $[\varepsilon_3, \varepsilon_4] \in \{-1, 1\}^2$. In the former case we have (9) with $h_3 = j_i$, in the latter case we have (11) with $h_i = j_{i-2}$ ($i = 3, 4$). In the case (15.2), since each of the vectors $[3, 1]$, $[1, 3]$ satisfies one of the congruences (7) for $h \in \{h_1, h_2\}$ we infer that

$$A_{h_1 1} \equiv \varepsilon_1 \frac{m}{3} \pmod m, \quad A_{h_2 0} \equiv \varepsilon_2 \frac{m}{3} \pmod m$$

where $[\varepsilon_1, \varepsilon_2] \in \{-1, 1\}^2$, thus we have the case (10) with $h_i = j_{i-2}$ for $i = 3, 4$.

Consider now the case (16). Excluding (8) we infer that

$$A_{h_1 1} \not\equiv 0 \pmod m,$$
$$A_{h_2 0} \not\equiv 0 \pmod m,$$
$$A_{j_1 0} \equiv A_{j_1 1} \equiv \frac{m}{2} \pmod m.$$

Let $\{j_3\} = \{1,2,3,4\} \setminus \{h_1, h_2, j_1\}$. Since each of the vectors $[1, \pm 2]$, $[\pm 2, 1]$ satisfies one of the congruences (7) we infer that either

$$2 \mid m, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod m, \tag{16.1}$$

or

$$2 \mid m, \quad A_{h_2 0} \equiv \frac{m}{2} \pmod m \tag{16.2}$$

or

$$\begin{aligned} A_{j_{3,0}} \pm 2A_{j_{3,1}} &\equiv 0 \pmod m, \\ \pm 2A_{j_{3,0}} + A_{j_{3,1}} &\equiv 0 \pmod m. \end{aligned} \tag{16.3}$$

The conditions (16.3) lead to (8) with $h = j_3$, the conditions (16.1) and (16.2) together lead to (9) with $h_3 = j_1$. If (16.1) holds but (16.2) does not, then since each of the vectors $[\pm 2, 1]$ satisfies one of congruences (7) for $h \in \{h_2, j_3\}$, we have

$$\pm 2A_{j_{3,0}} + A_{j_{3,1}} \equiv 0 \pmod m, \tag{17}$$

hence

$$\pm 4A_{j_{3,0}} \equiv 2A_{j_{3,1}} \equiv 0 \pmod m.$$

If

$$A_{j_{3,1}} \equiv 0 \pmod m,$$

then either $A_{j_{3,0}} \equiv 0 \pmod m$, which gives (8) with $h = j_3$, or $A_{j_{3,0}} \equiv \frac{m}{2} \pmod m$, which gives (9) with $h_2 = j_3$, $h_3 = j_1$. If $A_{j_{3,1}} \equiv \frac{m}{2} \pmod m$, then (17) implies $4 \mid m$,

$$A_{j_{3,0}} \equiv \varepsilon_4 \frac{m}{4} \pmod m,$$

which gives (12) with $h_3 = j_1$, $h_4 = j_3$. If (16.2) holds but (16.1) does not, then by symmetry we have (8) or (9) or (13).

Sufficiency of the condition follows from the easily verified fact, that the following systems of congruences are covering:
$0 \equiv 0 \pmod 1$; $t_1 \equiv 0$, $t_0 \equiv 0$, $t_0 + t_1 \equiv 0 \pmod 2$; $t_1 \equiv 0$, $t_0 \equiv 0$, $t_0 + t_1 \equiv 0$, $t_0 - t_1 \equiv 0 \pmod 3$; $t_1 \equiv 0$, $t_0 \equiv 0 \pmod 2$, $t_0 + t_1 \equiv 0$, $t_0 - t_1 \equiv 0 \pmod 4$;

$t_1 \equiv 0,\ t_0 + t_1 \equiv 0 \pmod 2,\ t_0 \equiv 0,\ t_0 + 2t_1 \equiv 0 \pmod 4;\ t_0 \equiv 0,\ t_0 + t_1 \equiv 0 \pmod 2,\ t_1 \equiv 0,\ 2t_0 + t_1 \equiv 0 \pmod 4$.

Lemma 2. *If K is a number field, $\alpha \in K$, $\beta_j \in \overline{\mathbf{Q}}$ $(1 \le j \le l)$, the congruence*

$$\prod_{j=1}^{l} (\alpha^x - \beta_j) \equiv 0 \pmod{\mathfrak{p}} \tag{18}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of the field $K(\beta_1, \dots, \beta_l) =: K_1$ and w is the number of roots of unity contained in K_1, then there exist $\gamma \in K_1$ and a subset H of $\{1, \dots, l\}$ such that

$$\alpha = \zeta_w^a \gamma^e, \tag{19}$$

$$\beta_h = \zeta_w^{b_h} \gamma^{d_h} \quad (h \in H) \tag{20}$$

and the system of congruences

$$t_0 (ad_h - eb_h) + wd_h t_1 \equiv 0 \pmod{we} \quad (h \in H) \tag{21}$$

is covering.

Proof. Let

$$\alpha = \zeta_w^{a_0} \prod_{s=1}^{t} \pi_s^{a_s}, \quad \beta_j = \zeta_w^{b_{j0}} \prod_{s=1}^{t} \pi_s^{b_{js}} \quad (1 \le j \le l), \tag{22}$$

where π_s are elements of the multiplicative basis of the field K_1 (see [1], Lemma 9). Let Q be a unimodular matrix such that

$$[a_1, \dots, a_t]\, Q = [e, 0, \dots, 0], \quad e = (a_1, \dots, a_t) \tag{23}$$

and put

$$[b_{j1}, \dots, b_{jt}]\, Q = [d_{j1}, \dots, d_{jt}]. \tag{24}$$

We choose integers $\eta_2, \dots, \eta_t$ divisible by w such that for all $j \le l$

$$\sum_{s=2}^{t} d_{js}\eta_s = 0 \text{ implies } d_{j_s} = 0 (2 \le s \le t) \tag{25}$$

and set

$$m = \max_{1 \le j \le l} \left| \sum_{s=2}^{t} d_{js}\eta_s \right| + 1. \tag{26}$$

Further we set

$$n = 2^\tau wme \operatorname*{l.c.m.}_{\substack{q \le m+e \\ q \text{ prime}}} (q-1),\ \eta_1 = \frac{n}{e}t_1 + a_0\frac{n}{ew}t_0, \tag{27}$$

where τ is the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K_1$,

$$\varepsilon_0 = -t_0, \quad \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_t \end{bmatrix} = Q \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_t \end{bmatrix}. \tag{28}$$

By Theorem 4 of [1] there exist infinitely many prime ideals $\mathfrak{P}$ of $K_1(\zeta_n)$ such that

$$\left(\frac{\zeta_w}{\mathfrak{P}}\right)_n = \zeta_w^{\varepsilon_0}, \quad \left(\frac{\pi_s}{\mathfrak{P}}\right)_n = \zeta_n^{\varepsilon_s} \quad (1 \le s \le t). \tag{29}$$

Let H be the set of these indices $h \le l$ that for some integers x, t_0, t_1 and for some prime ideal $\mathfrak{P}$ satisfying (29) we have

$$\alpha^x \equiv \beta_h \pmod{\mathfrak{P}}. \tag{30}$$

The congruence (30) gives

$$\left(\frac{\alpha^x}{\mathfrak{P}}\right)_n = \left(\frac{\beta_h}{\mathfrak{P}}\right)_n,$$

hence

$$x\left(\frac{n}{w}a_0\varepsilon_0 + \sum_{s=1}^{t} a_s\varepsilon_s\right) \equiv \frac{n}{w}b_{h0}\varepsilon_0 + \sum_{s=1}^{t} b_{hs}\varepsilon_s \pmod{n}$$

and by (24) and (28)

$$x\left(-\frac{n}{w}a_0t_0 + e\eta_1\right) \equiv -\frac{n}{w}b_{h0}t_0 + \sum_{s=1}^{t} d_{hs}\eta_s \pmod{n}.$$

Substituting the value of η_1 from (27) we obtain

$$0 \equiv nxt_1 \equiv -\frac{n}{w}b_{h0}t_0 + \frac{n}{w}d_{h1}\left(\frac{w}{e}t_1 + \frac{a_0}{e}t_0\right) + \sum_{s=2}^{t} d_{hs}\eta_s \pmod{n}. \tag{31}$$

It follows that

$$\sum_{s=2}^{t} d_{hs}\eta_s \equiv 0 \pmod{m}$$

and, by (26) and (25),

$$\sum_{s=2}^{t} d_{hs}\eta_s = 0, \quad d_{hs} = 0 \ (2 \le s \le t). \tag{32}$$

Hence, by (23) and (24),

$$b_{hs} = \frac{d_{h1}}{e} a_{hs}$$

and putting $a_0 = a$, $b_{h0} = b_h$, $d_{h1} = d_h$

$$\gamma = \prod_{s=1}^{t} \pi_s^{a_s/e}$$

we obtain (20) and (21). Moreover, since the congruence (18) is soluble for almost all prime ideals $\mathfrak{p}$ of K_1 the system of congruences, resulting from (31) and (32)

$$(ad_h - eb_h)\, t_0 + wd_h t_1 \equiv 0 \pmod{we} \quad (h \in H) \tag{33}$$

must be covering.

Remark. The above proof is modelled on the proof of Theorem 5 in [1].

Lemma 3. *If a system of congruences*

$$A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod{m} \quad (1 \le h \le g) \tag{34}$$

is covering, $w \mid m$, $d = (m, A_{11}, \dots, A_{g1})$ and $\alpha = \beta^{m/d}$, then the alternative of congruences

$$\alpha^x \equiv \zeta_w^{A_{h0}} \beta^{A_{h1}/d} \pmod{\mathfrak{p}} \quad (1 \le h \le g)$$

is soluble for all prime ideals $\mathfrak{p}$ of $\mathbf{Q}(\zeta_w, \beta)$ for which β is a $\mathfrak{p}$-adic unit.

Proof. Since the system (34) is covering, for every prime ideal $\mathfrak{p}$ there exists an $h \le g$ such that

$$A_{h0} \frac{d\frac{N\mathfrak{p}-1}{w}}{\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)} + A_{h1} \frac{\operatorname{ind}\beta}{\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)} \equiv 0 \pmod{m},$$

hence

$$A_{h0}\frac{N\mathfrak{p}-1}{w} + \frac{A_{h1}}{d}\operatorname{ind}\beta \equiv 0 \left(\operatorname{mod} \frac{m}{d}\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)\right).$$

However

$$\frac{m}{d}\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right) \equiv 0 \ (\operatorname{mod}(\operatorname{ind}\alpha, N\mathfrak{p}-1)),$$

hence the congruence

$$A_{h0}\frac{N\mathfrak{p}-1}{w}+\frac{A_{h1}}{d}\operatorname{ind}\beta \equiv x \operatorname{ind}\alpha \pmod{N\mathfrak{p}-1}$$

is soluble for x and we obtain

$$\alpha^x \equiv \zeta_w^{A_{h0}}\beta^{A_{h1}/d} \pmod{\mathfrak{p}}.$$

Proof of Theorem 1. Necessity.

By Lemma 2 the system (33) is covering, hence we apply Lemma 1 with

$$A_{h0} = ad_h - eb_h, \quad A_{h1} = wd_h.$$

If the case (8) holds, then for a certain $h \in H$

$$ad_h - eb_h \equiv wd_h \equiv 0 \pmod{we},$$

hence $e \mid d_h$ and $b_h \equiv a\frac{d_h}{e} \pmod{w}$, which gives

$$\beta_h = \alpha^{d_h/e}$$

hence (2) holds with $r = d_h/e$.

If the case (9) holds, then for some distinct indices h_1, h_2, h_3

$$ad_{h_1} - eb_{h_1} \equiv 0, \quad wd_{h_1} \equiv \frac{we}{2} \pmod{we},$$

hence $2 \mid e$, $d_{h_1} \equiv \frac{e}{2}c_1$, c_1 odd, $2 \mid a$, $b_{h_1} \equiv \frac{a}{2}c_1 \pmod{w}$;

$$ad_{h_2} - eb_{h_2} \equiv \frac{we}{2}, \quad wd_{h_2} \equiv 0 \pmod{we},$$

hence $d_{h_2} = ec_2$, $c_2 \in \mathbf{Z}$, $b_{h_2} \equiv \frac{w}{2} + ac_2 \pmod{w}$;

$$ad_{h_3} - eb_{h_3} \equiv wd_{h_3} \equiv \frac{we}{2} \pmod{we},$$

hence $d_{h_3} = \frac{e}{2}c_3$, c_3 odd, $b_{h_3} \equiv \frac{w}{2} + ac_3 \pmod{w}$.

This gives (3) with

$$\beta = \zeta_w^{a/2}\gamma^{e/2}, \quad 2r_1 + 1 = c_1, \quad r_2 = c_2, \quad 2r_3 + 1 = c_3.$$

If the case (10) holds, $3 \mid we$ and without loss of generality we may assume that

$$ad_1 - eb_1 \equiv 0, \quad wd_1 \equiv \varepsilon_1\frac{we}{3} \pmod{we},$$

hence $3 \mid e$, $d_1 \equiv \frac{e}{3}\varepsilon_1 \pmod e$, $3 \mid a$, $b_1 \equiv \frac{a}{3}\frac{3d_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{3}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $e \mid d_2$, $3 \mid w$, $b_2 \equiv \frac{d_2}{e} - \varepsilon_2 \frac{w}{3} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \varepsilon_3 \frac{we}{3} \pmod{we},$$

hence $d_3 \equiv \varepsilon_3 \frac{e}{3} \pmod e$, $b_3 \equiv \frac{a}{3}\frac{3d_3}{e} - \varepsilon_3 \frac{w}{3} \pmod w$;

$$ad_4 - eb_4 \equiv -wd_4 \equiv \varepsilon_4 \frac{we}{3} \pmod{we},$$

hence $d_4 \equiv -\varepsilon_4 \frac{e}{3} \pmod e$, $b_4 \equiv \frac{a}{3}\frac{3d_4}{e} - \varepsilon_4 \frac{w}{3} \pmod w$.

This gives (5) with

$$\beta = \zeta_w^{a/3}\gamma^{e/3}, \quad r_i = \frac{3d_i}{e} \quad (1 \le i \le 4), \quad e_i \equiv -\varepsilon_i \pmod 3 \quad (2 \le i \le 4).$$

If the case (11) holds, $4 \mid we$ and without loss of generality we may assume that

$$ad_1 - eb_1 \equiv 0, \quad wd_1 \equiv \frac{we}{2} \pmod{we}, \tag{35}$$

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{2}, \quad wd_2 \equiv 0 \pmod{we}, \tag{36}$$

$$ad_3 - eb_3 \equiv wd_3 \equiv \varepsilon_3 \frac{we}{4} \pmod{we}, \tag{37}$$

$$ad_4 - eb_4 \equiv -wd_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we}. \tag{38}$$

(35) implies $2 \mid e$ and $d_1 \equiv \frac{e}{2} \pmod e$, $2 \mid a$, $b_1 \equiv \frac{a}{2} \cdot \frac{2d_1}{e} \pmod w$, (36) implies $d_2 \equiv 0 \pmod e$, $b_2 \equiv a\frac{d_2}{e} - \frac{w}{2} \pmod w$, (37) implies $4 \mid e$, $a \equiv w \pmod 4$. Now, we distinguish two subcases

$$w \equiv 2 \pmod 4 \tag{39.1}$$

and

$$w \equiv 0 \pmod 4. \tag{39.2}$$

In the case (39.1) we take

$$\beta = \zeta_w^{\frac{a(w+2)}{8}}\gamma^{e/4}$$

and find

$$\begin{aligned}
\alpha &= \zeta_w^a \gamma^e = \beta^4,\\
\beta_1 = \zeta_w^{b_1}\gamma^{d_1} &= \zeta_w^{\frac{a}{2}\cdot\frac{2d_1}{e}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_1}{e}} \beta^{4d_1}\\
&= \zeta_w^{\frac{2d_1}{e}\left(\frac{a}{2}-\frac{a(w+2)}{4}\right)} \beta^{4d_1/e} = \zeta_w^{-\frac{awd_1}{2e}} \beta^{4d_1/e} = \zeta_w^{\frac{w}{2}} \beta^{4d_1/e} = -\beta^{\frac{4d_1}{e}},\\
\beta_2 = \zeta_w^{b_2}\gamma^{d_2} &= -\zeta_w^{a\frac{d_2}{e}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_2}{e}} \beta^{4d_2}\\
&= -\zeta_w^{\frac{d_2}{e}\left(a-\frac{a(w+2)}{2}\right)} \beta^{4d_2/e} = -\zeta_w^{r-\frac{d_2}{e}\cdot\frac{aw}{2}} \beta^{4d_2/e} = -\beta^{\frac{4d_2}{e}}.
\end{aligned}$$

(37) implies $4 \mid e$, $d_3 \equiv \varepsilon_3\frac{e}{4} \pmod{e}$, $b_3 \equiv \frac{ac_3-\varepsilon_3 w}{4} \pmod{w}$, $c_3 = \frac{4d_3}{e} \equiv \varepsilon_3 \pmod 4$,

$$\begin{aligned}
\beta_3 = \zeta_w^{b_3}\gamma^{d_3} &= \zeta_w^{\frac{ac_3-\varepsilon_3 w}{4}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_3}{e}} \beta^{\frac{4d_3}{e}}\\
&= \zeta_w^{\left(-\frac{a}{2}c_3-\varepsilon_3\right)\frac{w}{4}} \beta^{4d_3/e} = (-1)^{\frac{a+2}{4}} \beta^{\frac{4d_3}{e}}.
\end{aligned}$$

(38) implies $4 \mid e$, $d_4 \equiv -\varepsilon_4\frac{e}{4} \pmod{e}$, $b_4 \equiv \frac{ac_4-\varepsilon_4 w}{4} \pmod{w}$, $c_4 = \frac{4d_4}{e} \equiv -\varepsilon_4 \pmod 2$,

$$\begin{aligned}
\beta_4 = \zeta_w^{b_4}\gamma^{d_4} &= \zeta_w^{\frac{ac_4-\varepsilon_4 w}{4}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_4}{e}} \beta^{\frac{4d_4}{e}}\\
&= \zeta_w^{\left(-\frac{a}{2}c_4-\varepsilon_4\right)\frac{w}{4}} \beta^{4d_4/e} = (-1)^{\frac{a-2}{4}} \beta^{\frac{4d_4}{e}}
\end{aligned}$$

and we obtain the case (6).

Consider now the case (39.2). Here (37) implies $4 \mid a$, we take

$$\beta = \zeta_w^{\frac{a-w}{4}} \gamma^{e/4}$$

and find

$$\begin{aligned}
&\alpha = \zeta_w^a \gamma^e = \beta^4,\\
&\beta_1 = \zeta_w^{b_1}\gamma^{d_1} = \zeta_w^{ad_1/e}\gamma^{d_1} = -\beta^{4d_1/e},\\
&\beta_2 = \zeta_w^{b_2}\gamma^{d_2} = -\zeta_w^{ad_2/e}\gamma^{d_2} = -\beta^{4d_2/e}.
\end{aligned}$$

Moreover, (37) gives $d_3 \equiv \varepsilon_3\frac{e}{4} \pmod{e}$, $b_3 \equiv \frac{ad_3}{e} - \varepsilon_3\frac{w}{4} \pmod{w}$, hence

$$\beta_3 = \zeta_4^{-\varepsilon_3}\zeta_w^{ad_3/e}\gamma^{d_3} = \beta^{4d_3/e};$$

(38) gives $d_4 \equiv -\varepsilon_4 \frac{e}{4} \pmod e$, $b_4 \equiv \frac{ad_4}{e} - \varepsilon_4 \frac{w}{4} \pmod w$, hence

$$\beta_4 = \zeta_4^{-\varepsilon_4} \zeta_w^{ad_4/e} \gamma^{d_4} = -\beta^{4d_4/e}$$

and we obtain again the case (6).

Consider now the case (12). Here we have

$$ad_1 - eb_1 \equiv 0 \pmod{we}, \quad wd_1 \equiv \varepsilon_1 \frac{we}{4} \pmod{we},$$

hence $4 \mid e$, $d_1 \equiv \varepsilon_1 \frac{e}{4} \pmod e$, $4 \mid a$, $b_1 \equiv \frac{ad_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \frac{we}{2} \pmod{we}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $d_2 \equiv 0 \pmod e$, $b_2 \equiv \frac{ad_2}{e} - \frac{a}{2} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \frac{we}{2} \pmod{we},$$

hence $d_3 \equiv \frac{e}{2} \pmod e$, $b_3 \equiv \frac{ad_3}{e} - \frac{w}{2} \pmod w$;

$$ad_4 - eb_4 \equiv \frac{we}{2} \pmod{we}, \quad wd_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we},$$

hence $d_4 \equiv \varepsilon_4 \frac{e}{4} \pmod e$, $b_4 \equiv \frac{ad_4}{e} - \frac{w}{2} \pmod w$.

Therefore, setting

$$\beta = \zeta_w^{a/4} \gamma^{e/4}$$

we obtain

$$\alpha = \beta^4,\ \beta_1 = \beta^{4d_1/e},\ \beta_2 = -\beta^{4d_2/e},\ \beta_3 = -\beta^{4d_3/e},\ \beta_4 = -\beta^{4d_4/e},$$

which is again the case (6).

Consider now the case (13). Here we have

$$ad_1 - eb_1 \equiv 0 \pmod{we}, \quad wd_1 \equiv \frac{we}{4} \pmod{we},$$

hence $2 \mid e$, $d_1 \equiv \frac{e}{4} \pmod e$, $2 \mid a$, $b_1 \equiv \frac{ad_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{4} \pmod{we}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $d_2 \equiv 0 \pmod e$, $4 \mid w$, $b_2 \equiv ad_2 - \varepsilon_2 \frac{a}{2} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \frac{we}{2} \pmod{we},$$

hence $d_3 \equiv \frac{e}{2} \pmod{e}$, $b_3 \equiv ad_3 - \frac{w}{2} \pmod{w}$;

$$ad_4 - eb_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we}, \quad wd_4 \equiv \frac{we}{2} \pmod{we},$$

hence $d_4 \equiv \frac{e}{2} \pmod{e}$, $b_4 \equiv \frac{ad_4}{e} - \varepsilon_4 \frac{w}{4} \pmod{w}$.

Therefore, setting

$$\beta = \zeta_w^{a/4} \gamma^{e/4}$$

we obtain

$$\alpha = \beta^2,\ \beta_1 = \beta^{2d_1/e},\ \beta_2 = \zeta_4^{-\varepsilon_2} \beta^{2d_2/e},\ \beta_3 = -\beta^{2d_3/e},\ \beta_4 = \zeta_4^{-\varepsilon_4} \beta^{2d_4/e},$$

which is the case (4).

Sufficiency of the condition follows from Lemma 3 and the covering property of the relevant systems of congruences, which in turn follows from Lemma 1. Indeed, a prime ideal $\mathfrak{p}$ of K is divisible by a prime ideal $\mathfrak{P}$ of $K(\zeta_w, \beta)$, which in turn divides a prime ideal $\mathfrak{q}$ of $\mathbf{Q}(\zeta_w, \beta)$. Solubility of the congruence

$$\prod_{h=1}^{g} \left(\alpha^x - \zeta_w^{A_{h0}} \beta^{A_{h1}/d} \right) \equiv 0 \pmod{\mathfrak{q}}$$

implies solubility of the congruence $f(\alpha^x) \equiv 0 \pmod{\mathfrak{P}}$, and this, since $f \in K[z]$, solubility of $f(\alpha^x) \equiv 0 \pmod{\mathfrak{p}}$.

Lemma 4. *If $u_n = \lambda_1 \alpha^n + \lambda_2 (-\alpha^{-1})^n$ is a recurring sequence in K and α is a root of unity, then solubility of the congruence*

$$u_n \equiv c \pmod{\mathfrak{p}}$$

for infinitely many prime ideals $\mathfrak{p}$ of K implies $c = u_m$, where m is an integer.

Proof. If α is a root unity of order q we have $u_n \in \{u_1, \ldots, u_{2q}\}$, hence if $c \neq u_m$ the congruence in question is soluble for only finitely many prime ideals $\mathfrak{p}$ dividing

$$\prod_{m=1}^{2q} (u_n - c).$$

Proof of Theorem 2. If $b = 0$ we have $u_n = \lambda \alpha^n$ and the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda z - c$.

If $b = -1$, we have $u_n = \lambda_1 \alpha^n + \lambda_2 \alpha^{-n}$ and the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda_1 z^2 - cz + \lambda_2$.

If $b = 1$, $a = 0$ we have $\alpha = \pm 1$ and the assertion follows by virtue of Lemma 4.

If $b = 1$, $c = 0$ or $\lambda_1 = 0$ or $\lambda_2 = 0$ the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda_1 z + \lambda_2$ or $\lambda_2 z - c$ or $\lambda_1 z - c$, respectively. Therefore, assume $b = 1$, $ac\lambda_1\lambda_2 \neq 0$.

Solubility of the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is equivalent to solubility of the congruence

$$f\left(\alpha^{2n}\right) \equiv 0 \pmod{\mathfrak{p}},$$

where

$$f(z) = \left(\lambda_1 z^2 - cz + \lambda_2\right)\left(\lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2\right).$$

We apply Theorem 1 with α^2 in stead of α, considering successively the cases (2)–(6).

In the case (2) we have $z - \alpha^{2r} \mid f(z)$, hence either $z - \alpha^{2r} \mid \lambda_1 z^2 - cz + \lambda_2$, or $z - \alpha^{2r} \mid \lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2$. In the former case $u_n = c$ has the solution $n = 2r$, in the latter case $n = 2r + 1$.

In the case (3) we have one of the following six cases:

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;
\end{aligned} \tag{40.1}$$

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0;
\end{aligned} \tag{40.2}$$

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;
\end{aligned} \tag{40.3}$$

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0;
\end{aligned} \tag{40.4}$$

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;
\end{aligned} \tag{40.5}$$

$$\begin{aligned}
&\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\
&\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0.
\end{aligned} \tag{40.6}$$

Since $c\lambda_1\lambda_2 \neq 0$ at least one of the determinants $\Delta_1, \ldots, \Delta_6$ is 0, where

$$\Delta_1 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix},$$

$$\Delta_3 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_4 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix},$$

$$\Delta_5 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_6 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix}.$$

Suppose first that α is not an algebraic integer. Then in the expanded form of the determinant Δ_i the highest power of α must occur at least twice. However, the exponents in the first column of Δ_i are twice the exponents in the second column. Denoting the latter by $\delta_{i1}, \delta_{i2}, \delta_{i3}$ in the decreasing order, we infer that the greatest power of α in Δ_i is $\alpha^{2\delta_{i1}+\delta_{i2}}$ and it is not repeated unless two of the numbers δ_{ij} $(j = 1, 2, 3)$ are equal. This gives the following possibilities:

(41.1) $\quad i = 1, \quad r_2 = r_3 + 1;$

(41.2) $\quad i = 2, \quad r_2 = r_1, \quad \text{or} \quad r_3 = r_1, \quad \text{or} \quad r_3 = r_2;$

(41.3) $\quad i = 3, \quad r_2 = r_1;$

(41.4) $\quad i = 4, \quad r_2 = r_1 + 1;$

(41.5) $\quad i = 5, \quad r_2 = r_1 + 1, \quad \text{or} \quad r_3 = r_1, \quad \text{or} \quad r_2 = r_3 + 1;$

(41.6) $\quad i = 6, \quad r_3 = r_2$

and in each case the equation $\Delta_i = 0$ gives α as 0 or a root of unity, contrary to the assumption, that α is not an algebraic integer.

Assume now that α is an algebraic integer. Since $a^2 + 4 \neq d^2$ (d an integer of K) we have $\alpha \notin K$. Hence α is conjugate over K to $-\alpha^{-1}$ and λ_2 is conjugate to λ_1. By (40.1)–(40.6) we have for an $\varepsilon \in \{1, -1\}$,

$$\lambda_1 \left(\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}\right)^2 - c\left(\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}\right) + \varepsilon\lambda_2 = 0, \tag{42}$$

hence

$$\lambda_1 \alpha^{2r_1+1+\frac{1-\varepsilon}{2}} = \frac{c \mp \sqrt{c^2 - 4\varepsilon\lambda_1\lambda_2}}{2}. \tag{43}$$

If $\lambda_1\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} =: \mu \in K$ then

$$\lambda_1 = \mu\alpha^{-2r_1-1-\frac{1-\varepsilon}{2}}, \quad \lambda_2 = \mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}(-1)^{\frac{1+\varepsilon}{2}}$$

and from (42)

$$0 = \mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} - c\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} + \varepsilon(-1)^{\frac{1+\varepsilon}{2}}\mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} = -c\alpha^{2r_1+1+\frac{1-\varepsilon}{2}},$$

contrary to $c \neq 0$.

If $\lambda_1\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} \notin K$, then from (43) on taking conjugates we obtain

$$\lambda_2(-1)^{\frac{1-\varepsilon}{2}}\alpha^{-2r_1-1-\frac{1-\varepsilon}{2}} = \frac{c \pm \sqrt{c^2 - 4\varepsilon\lambda_1\lambda_2}}{2},$$

hence on multiplication side by side with (43)

$$\lambda_1\lambda_2(-1)^{\frac{1+\varepsilon}{2}} = \varepsilon\lambda_1\lambda_2,$$

contrary to $\lambda_1\lambda_2 \neq 0$.

In the case (4) there exists a permutation $(\zeta_4^{\varepsilon_1}\alpha^{\delta_1}, \dots, \zeta_4^{\varepsilon_4}\alpha^{\delta_4})$ of $(\alpha^{2r_1+1}, !\zeta_4^{e_2}\alpha^{2r_2}, -\alpha^{2r_3+1}, \zeta_4^{e_4}\alpha^{2r_4+1})$ such that

$$\frac{\lambda_2}{\lambda_1} = \zeta_4^{\varepsilon_1+\varepsilon_2}\alpha^{\delta_1+\delta_2} = -\zeta_4^{\varepsilon_3+\varepsilon_4}\alpha^{\delta_3+\delta_4+2}. \tag{44}$$

If $\delta_1+\delta_2 = \delta_3+\delta_4+2$, then $2(\delta_1+\delta_2) = \delta_1+\delta_2+\delta_3+\delta_4+2 = 2r_1+2r_2+2r_3+2r_4+5$, which is impossible mod 2. If $\delta_1+\delta_2 \neq \delta_3+\delta_4+2$, then α is a root of unity and the assertion follows by virtue of Lemma 4.

In the case (5) we have

$$\alpha = \gamma^3, \quad \beta = \gamma^2, \quad \text{where } \gamma = \alpha/\beta$$

and there exists a permutation

$$(\zeta_3^{\varepsilon_1}\gamma^{\delta_1}, \dots, \zeta_3^{\varepsilon_4}\gamma^{\delta_4}) \text{ of } (\gamma^{2r_1}, \zeta_3^{e_2}\gamma^{2r_2}, \zeta_3^{e_3}\gamma^{2r_3}, \zeta_3^{e_4}\gamma^{2r_4})$$

such that

$$\frac{\lambda_2}{\lambda_1} = \zeta_3^{\varepsilon_1+\varepsilon_2}\gamma^{\delta_1+\delta_2} = -\zeta_3^{\varepsilon_3+\varepsilon_4}\gamma^{\delta_3+\delta_4+6}.$$

If $\delta_1+\delta_2 = \delta_3+\delta_4+6$, we obtain $\zeta_3^{\varepsilon_1+\varepsilon_2-\varepsilon_3-\varepsilon_4} = -1$, which is impossible. If $\delta_1+\delta_2 \neq \delta_3+\delta_4+6$, then γ is a root of unity and so is α; the assertion follows by virtue of Lemma 4.

In the case (6) we have

$$\alpha = \varepsilon_0\beta^2, \quad (\varepsilon_0 = \pm 1)$$

and there exists a permutation

$(\varepsilon_1\beta^{\delta_1}, \varepsilon_2\beta^{\delta_2}, \varepsilon_3\beta^{\delta_3}, \varepsilon_4\beta^{\delta_4})$ of $(\beta^{2r_1+1}, -\beta^{4r_2}, -\beta^{2r_3+1}, -\beta^{4r_4+2})$ such that $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) \in \{1, -1\}^4$ and

$$\frac{c}{\lambda_1} = \varepsilon_1\beta^{\delta_1} + \varepsilon_2\beta^{\delta_2} = \varepsilon_0\varepsilon_3\beta^{\delta_3+2} + \varepsilon_0\varepsilon_4\beta^{\delta_4+2}, \tag{45}$$

$$\frac{\lambda_2}{\lambda_1} = \varepsilon_1\varepsilon_2\beta^{\delta_1+\delta_2} = -\varepsilon_3\varepsilon_4\beta^{\delta_3+\delta_4+4}. \tag{46}$$

If β is not an algebraic integer, then it follows from (45) that the greatest term of the sequence $(\delta_1, \delta_2, \delta_3+2, \delta_4+2)$ occurs in this sequence at least twice and from (46) that $\delta_1 + \delta_2 = \delta_3 + \delta_4 + 4$. Hence

$$\delta_1 = \delta_3 + 2, \quad \delta_2 = \delta_4 + 2 \quad \text{or} \quad \delta_1 = \delta_4 + 2, \quad \delta_2 = \delta_3 + 2. \tag{47}$$

This gives the following possibilities:

$$\{\delta_1, \delta_2\} = \{2r_1 + 1, 4r_2\}, \quad \{\delta_3, \delta_4\} = \{2r_3 + 1, 4r_4 + 2\};$$

$$\{\delta_1, \delta_2\} = \{2r_1 + 1, 4r_4 + 2\}, \quad \{\delta_3, \delta_4\} = \{2r_3 + 1, 4r_2\};$$

$$\{\delta_1, \delta_2\} = \{4r_2, 2r_3 + 1\}, \quad \{\delta_3, \delta_4\} = \{2r_1 + 1, 4r_4 + 2\};$$

$$\{\delta_1, \delta_2\} = \{2r_3 + 1, 4r_4 + 2\}, \quad \{\delta_3, \delta_4\} = \{2r_1 + 1, 4r_2\}$$

and we obtain from (45) the following equations

$$\beta^{2r_1+1} - \beta^{4r_2} = -\varepsilon_0\beta^{2r_3+3} - \varepsilon_0\beta^{4r_4+4},$$

$$\beta^{2r_1+1} - \beta^{4r_4+2} = -\varepsilon_0\beta^{2r_3+3} - \varepsilon_0\beta^{4r_2+2},$$

$$-\beta^{4r_2} - \beta^{2r_3+1} = \varepsilon_0\beta^{2r_1+3} - \varepsilon_0\beta^{4r_4+4},$$

$$-\beta^{2r_3+1} - \beta^{4r_4+2} = \varepsilon_0\beta^{2r_1+3} - \varepsilon_0\beta^{4r_4+2}.$$

By (47) the exponents on both sides are equal in pairs, which gives for each value of ε_0 : $\beta = 0$, hence $\alpha = 0$, contrary to $b = 1$.

If β is an algebraic integer so is α. Since $a^2+4 \neq d^2$ (d an integer of K) we have $\alpha \notin K$, hence α is conjugate over K to α^{-1} and λ_1 is conjugate to λ_2. On the other hand, we have

$$\lambda_1 \left(\alpha^{2r_4+1+\frac{1-\varepsilon}{2}}\right)^2 - c\alpha^{2r_4+1+\frac{1-\varepsilon}{2}} + \varepsilon\lambda_2 = 0, \quad \varepsilon \in \{1,-1\}, \tag{48}$$

which differs from (42) only by permutation of r_1 and r_4 and hence leads to contradiction.

Proof of Corollary 1. If $a \in \mathbf{Q}$, then either $a=0$ or $a^2+4 \neq d^2$, $d \in \mathbf{Z}$ hence the assumptions of Theorem 2 are fulfilled.

Proof of Corollary 2. If $a \in K$ and

$$a^2+4 = d^2, \quad d \text{ an integer of } K \tag{49}$$

the zeros of z^2-az-1 are units of K. However, since K is quadratic imaginary, the only units of K are roots of unity and the assertion follows by virtue of Lemma 4.

Example. The following example shows that the assumption $a^2+4 \neq d^2$ (d an integer of K) cannot be altogether omitted. Let $K=\mathbf{Q}(\alpha)$, where $\alpha^3+\alpha^2-\alpha+1=0$ and take

$$u_n = \lambda_1\alpha^n + \lambda_2\left(-\alpha^{-1}\right)^n, \quad \lambda_1 = -\left(1+\alpha^2\right), \quad \lambda_2 = \alpha^2-\alpha^4, \quad c = \alpha^4+1.$$

As observed in the proof of Theorem 2 solubility of the congruence

$$u_n \equiv c \pmod{\mathfrak{p}}, \tag{50}$$

is equivalent to solubility of the congruence

$$f\left(\alpha^{2n}\right) \equiv 0 \pmod{\mathfrak{p}}, \tag{51}$$

where

$$f(z) = \left(\lambda_1 z^2 - cz + \lambda_2\right)\left(\lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2\right).$$

Now

$$f(z) = \lambda_1^2(z-\alpha)(z+1)(z+\alpha)\left(\alpha^2 z+1\right), \tag{52}$$

hence by Theorem 1, case (3), the congruence (51) is soluble for almost all prime ideals $\mathfrak{p}$ of K and so is the congruence (50). On the other hand,op solubility of the equation $u_n = c$ would imply solubility of the equation $f(\alpha^{2n})=0$, hence, by (52), α would be a root of unity, which contradicts $\alpha^3+\alpha^2-\alpha-1=0$.

The author thanks the Department of Mathematics of the University of Colorado at Boulder, where a part of the paper has been written.

References

[1] Schinzel, A., Abelian binomials, power residues and exponential congruences, *Acta Arith.*, **32** (1977), 245–274, Addendum and corrigendum, ibid., **36** (1980), 101–104.

Andrzej Schinzel
Institute of Mathematics PAN
P.O. Box 21, 00-956 Warszawa 10,
e-mail: A.Schinzel@impan.gov.pl

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 167–171*

ON INTERSECTION OF NORMAL FITTING CLASSES OF FINITE GROUPS

V. V. Shpakov, N. N. Vorob'ev and N. T. Vorob'ev (Vitebsk, Belarus)

Dedicated to the memory of Professor Péter Kiss

Abstract. Intersections of $\mathfrak{X}$-normal Fitting classes are studied for Fischer class $\mathfrak{X}$ of partially soluble groups.

AMS Classification Number: 20D10

Introduction

When describing Fitting classes of finite soluble groups structure and their classification the basic result is Blessenohl–Gaschütz's theorem [1]: the intersection of any set of non-identity normal Fitting classes is non-identity normal Fitting class again.

Remind that a class $\mathfrak{F}$ of finite groups is called a Fitting class if the following two conditions hold:

(i) if $G \in \mathfrak{F}$ and $N \triangleleft G$, then $N \in \mathfrak{F}$;

(ii) if M, $N \triangleleft G = MN$ with M and N in $\mathfrak{F}$, then $G \in \mathfrak{F}$.

We note from the definition of a Fitting class it follows that every finite group G has a unique maximal normal $\mathfrak{F}$-subgroup called the $\mathfrak{F}$-radical of G denoting $G_{\mathfrak{F}}$.

A Fitting class $\mathfrak{F}$ is called normal in a class of finite groups $\mathfrak{X}$ or $\mathfrak{X}$-normal [4] if $\mathfrak{F} \subseteq \mathfrak{X}$ and $G_{\mathfrak{F}}$ is maximal among subgroups of G belonging to $\mathfrak{F}$ for all groups $G \in \mathfrak{X}$. In the case when $\mathfrak{X} = \mathfrak{S}$ ($\mathfrak{S}$ is the class of all finite soluble groups) $\mathfrak{F}$ is called $\mathfrak{S}$-normal or simply normal Fitting class.

In this paper we develop and extend the above-mentioned result by Blessenohl–Gaschütz in two directions. In the first place, we prove an analog of Blessenohl–Gaschütz's theorem for $\mathfrak{X}$-normal Fitting classes where $\mathfrak{X}$ is a Fischer class (in particular $\mathfrak{X} \subseteq \mathfrak{S}$). In the second place, we replace a solvability condition for the groups of the class $\mathfrak{X}$ with a partially solvability condition. In the course of this paper we consider only finite groups. We use the terminology and notations of [2].

1. Some notations and lemmas

Let $\mathfrak{F}$ be a Fitting class. A subgroup V of a group G is called an $\mathfrak{F}$-injector of G if $V \bigcap N$ is maximal in N from the subgroups in $\mathfrak{F}$ for any subnormal subgroup

N of G. A famous Fischer–Gaschütz–Hartley's theorem [3] that every group $G \in \mathfrak{S}$ has a unique class of conjugate $\mathfrak{F}$-injectors is a synthesis of well-known Sylow's and Hall's theorems.

We note that if $\mathfrak{F}$ and $\mathfrak{H}$ are Fitting classes then their product $\mathfrak{F}\mathfrak{H}$ is the class of groups $(G \mid G/G_{\mathfrak{F}} \in \mathfrak{H})$ which is a Fitting class. In particular $\mathfrak{F}\mathfrak{S}$ is the class of all groups G such that factor group by the $\mathfrak{F}$-radical of G is soluble.

The following lemma extends Fischer–Gaschütz–Hartley's theorem.

Lemma 1.1. (V. Sementovskii [5]) *If $G \in \mathfrak{F}\mathfrak{S}$ then*

(a) G has a unique class of conjugate $\mathfrak{F}$-injectors;

(b) if V is an $\mathfrak{F}$-injector of G and $V \subseteq H \subseteq G$, then V is also an $\mathfrak{F}$-injector of H.

We shall use the definition of $\mathfrak{X}$-normal Fitting class which is equivalent to above-mentioned (in introduction) Laue's definition [4].

Definition 1.2. Let $\mathfrak{F}$ and $\mathfrak{X}$ be Fitting classes such that $\mathfrak{F} \subseteq \mathfrak{X} \subseteq \mathfrak{F}\mathfrak{S}$. We call the Fitting class $\mathfrak{F}$ an $\mathfrak{X}$-normal or normal in $\mathfrak{X}$ if for any group $G \in \mathfrak{X}$ its $\mathfrak{F}$-injector is a normal subgroup of G. We denote this by $\mathfrak{F} \lhd \mathfrak{X}$.

The following example gives a construction procedure of wide family of $\mathfrak{X}$-normal Fitting classes.

Example 1.3. Let $\mathfrak{F}$ be any non-empty Fitting class and $\mathfrak{X} = \mathfrak{F}\mathfrak{N}$ where $\mathfrak{N}$ is the class of all nilpotent groups. Then for any group $G \in \mathfrak{X}$ its $\mathfrak{F}$-injector $V = G_{\mathfrak{F}}$. In fact since $G/G_{\mathfrak{F}}$ is nilpotent, then $V/G_{\mathfrak{F}}$ is a subnormal subgroup of $G/G_{\mathfrak{F}}$. Therefore V is subnormal in G and $V = G_{\mathfrak{F}}$.

We shall use the result by J. Tits.

Lemma 1.4. ([2, Lemma A 1.2]) *Let U, V and W be subgroups of a group G. Then the following statements are equivalent:*

(a) $U \bigcap VW = (U \bigcap V)(U \bigcap W)$;

(b) $U \bigcap UW = U(V \bigcap W)$.

2. The main result

Remind that a Fitting class $\mathfrak{F}$ is called a Fischer class if $G \in \mathfrak{F}$, $K \lhd G$, $K \subseteq H \subseteq G$ and H/K is a p-group (p is a prime number) implies $H \in \mathfrak{F}$.

Theorem 2.1. *Let $\mathfrak{X}$ be a Fisher class and $\{\mathfrak{F}_i \mid i \in I\}$ be the set of $\mathfrak{X}$-normal Fitting classes. If $\mathfrak{F} = \bigcap_{i \in I} \mathfrak{F}_i$ and $\mathfrak{F} \subseteq \mathfrak{X} \subseteq \mathfrak{F}\mathfrak{S}$, then $\mathfrak{F}$ is an $\mathfrak{X}$-normal Fitting class.*

Proof. We proceed by induction on the order of groups in $\mathfrak{X}$. Suppose that the theorem fails to hold. Let $G \in \mathfrak{X}$ be a counter example of minimal order. Since

$G/G_{\mathfrak{F}}$ is soluble by hypothesis then by Lemma 1.1 there exist $\mathfrak{F}$-injectors in G. Let V be an $\mathfrak{F}$-injector of G, such that V is not normal in G. Since $\mathfrak{F} \subseteq \mathfrak{F}_i$ for all $i \in I$, then $G_{\mathfrak{F}} \subseteq G_{\mathfrak{F}_i}$ and by the isomorphism $G/G_{\mathfrak{F}}/G_{\mathfrak{F}_i}/G_{\mathfrak{F}} \cong G/G_{\mathfrak{F}_i}$, we have $G/G_{\mathfrak{F}_i}$ is soluble.

Consequently by Lemma 1.1 there exists an $\mathfrak{F}_i$-injector V_i in G. By hypothesis $V_i \triangleleft G$ for all $i \in I$. Therefore $\bigcap_{i\in I} V_i \triangleleft G$. Evidently $\bigcap_{i\in I} V_i \in \mathfrak{F}$. Hence $\bigcap_{i\in I} V_i \subseteq G_{\mathfrak{F}}$.

On the other hand for every $i \in I$ we have the inclusion

$$G_{\mathfrak{F}} \subseteq G_{\mathfrak{F}_i} = V_i.$$

Consequently $G_{\mathfrak{F}} = \bigcap_{i\in I} V_i$ and $\bigcap_{i\in I} V_i \subset V$.

Let M be an arbitrary maximal normal subgroup of G. Since V is an $\mathfrak{F}$-injector of G then the subgroup $V \bigcap M$ is an $\mathfrak{F}$-injector of the group M. Then since $M \in \mathfrak{X}$ it follows that $V \bigcap M \triangleleft M$ by induction.
We obtain $V \bigcap M = M_{\mathfrak{F}} = G_{\mathfrak{F}} \bigcap M$. Hence for any maximal normal subgroup M of G we have

$$V \bigcap M = \left(\bigcap_{i\in I} V_i\right) \bigcap M. \tag{1}$$

We note that V is not contained in any subnormal subgroup N of G. If this assertion fails to hold i.e. $V \subseteq N \triangleleft\triangleleft G$ then there exists an $\mathfrak{F}$-injector in N. By Lemma 1.1 the subgroup V is an $\mathfrak{F}$-injector of N. Then by induction $V \triangleleft N$. Therefore $V \triangleleft\triangleleft G$ and $V = G_{\mathfrak{F}}$. A contradiction because V is not normal subgroup of G.

We show that $G = RV$ for any normal subgroup R of G such that G/R is nilpotent. Let $RV \neq G$. Then a subgroup RV/R is subnormal in G/R. Hence RV is subnormal in G. Consequently V is contained in the subgroup $H = RV$ and $H \triangleleft\triangleleft G$, a contradiction.

Now we prove that G is comonolithic. Let G be not comonolithic and M_1 and M_2 be maximal normal subgroups of G. Without loss of generality we consider $M_1 \supseteq G_{\mathfrak{F}}$ and $M_2 \not\supseteq G_{\mathfrak{F}}$. Then $G = M_2 G_{\mathfrak{F}}$. Besides $M_1 \supseteq G_{\mathfrak{F}}$ and $G \in \mathfrak{F}\mathfrak{S}$. It follows that G/M_1 is nilpotent. From above $G = VM_1$. Consequently by the isomorphisms $G/M_1 \cong V/(V \bigcap M_1)$ and $G/M_2 \cong V/(V \bigcap M_2)$ the subgroups $V \bigcap M_1$ and $V \bigcap M_2$ are maximal normal of V.

Suppose $V \bigcap M_1 \neq V \bigcap M_2$. Then $V = (V \bigcap M_1)(V \bigcap M_2)$. Hence by (1)

$$V = \left(\left(\bigcap_{i\in I} V_i\right) \bigcap M_1\right) \left(\left(\bigcap_{i\in I} V_i\right) \bigcap M_2\right)$$

and $V \subseteq G_{\mathfrak{F}}$. Consequently $V = G_{\mathfrak{F}}$. A contradiction because the subgroup V is not normal in G. Therefore $V \bigcap M_1 = V \bigcap M_2$. Then

$$G/M_1 \cong V/V \bigcap M_1 = V/V \bigcap M_2 \cong G/M_2$$

and $G/M_2 \in \mathfrak{N}$. Thus the group $G/(M_1 \bigcap M_2)$ is nilpotent. Hence $G = V(M_1 \bigcap M_2)$. From the other hand $G = VM_1 \bigcap VM_2$. Consequently

$$V\left(M_1 \bigcap M_2\right) = VM_1 \bigcap VM_2.$$

By Lemma 1.2 we have the equality

$$V = \left(V \bigcap M_1\right)\Big)V \bigcap M_2\Big) = V \bigcap M_1.$$

It follows that $V \subseteq M_1$. A contradiction because V is not contained in any subnormal subgroup of G. Thus $M_1 = M_2 = M$ and G is comonolithic. Consequently for every $i \in I$ we have $V_i \subseteq M$. Hence by (1)

$$V \bigcap M = \bigcap_{i \in I} V_i. \tag{2}$$

Then by the isomorphism

$$G/M \cong V/\left(\bigcap_{i \in I} V_i\right)$$

the group $V/(\bigcap V_i)$ is cyclic of prime order p.

Now we show $V_i V \neq G$ for some $i \in I$. Suppose for any $i \in I$ the equality holds $V_i V = G$. If for all $j \in I$ we have $V_j = G$ then $G \in \mathfrak{F}$ and G is an $\mathfrak{F}$-injector for itself. Hence $G = V \triangleleft G$. A contradiction because V is not normal in G. Consequently $V_j \neq G$ for some $j \in I$. Since by hypothesis $V_j \triangleleft G$ then

$$G/V_j \cong V/V \bigcap V_j.$$

By the equality (2)

$$V \bigcap V_j \subseteq V \bigcap M = \bigcap_{i \in I} V_i \subseteq V_j \bigcap V.$$

Then $V_j \bigcap V = \bigcap_{i \in I} V_i$. Since $V/(\bigcap_{i \in I} V_i) \cong G/V_j$ it follows that G/V_j is a cyclic group of prime order p. Hence V_j is a maximal normal subgroup of G. Therefore $V_j = M$.

It is easily seen that $V_j \in \mathfrak{F} = \bigcap_{i \in I} \mathfrak{F}_i$. In fact if for $i \neq j$ $(i \in I)$ we have $V_i \neq G$ then we analogously conclude $V_i = M = V_j$ and $V_j \in \mathfrak{F}_i$.

If $V_i = G$ then $V_j \lhd V_i \in \mathfrak{F}_i$ and $V_j \in \mathfrak{F}_i$. Consequently $V_j \in \mathfrak{F}_i$ for all $i \neq j$. Therefore $V_j \in \mathfrak{F}$. Hence $V_j \subseteq G_{\mathfrak{F}} \subseteq V$. By hypothesis $V_j V = G$ and we obtain $V = G$ and $G \in \mathfrak{F}$. A contradiction because V is not normal in G.

Thus there exists $i \in I$ such that $V_i V \neq G$. We prove that $V_i V \in \mathfrak{X}$. In fact since a group $\overline{V} = V/(\bigcap_{i\in I} V_i)$ is simple then its normal subgroup $(V \bigcap V_i)/(\bigcap_{i\in I} V_i)$ either coincides with $\overline{V}$ or $(V \bigcap V_i)/(\bigcap_{i\in I} V_i)$ is the identity group. In the first case we have $V = V \bigcap V_i \subseteq V_i$. A contradiction because V is not contained in any subnormal subgroup of G. Thus we conclude $V \bigcap V_i = \bigcap_{i\in I} V_i$. Then by the isomorphism $V_i V/V_i \cong V/V \bigcap V_i$ the group $V_i V/V_i$ is a p-group.

Consequently since $G \in \mathfrak{X}$ and $\mathfrak{X}$ is a Fischer class if follows that $V_i V \in \mathfrak{X}$. We have $|V_i V| < |G|$ and by Lemma 1.1 V is an $\mathfrak{F}$-injector of $V_i V$. Hence by induction $V \lhd V_i V$. Since $V \in \mathfrak{F}_i$ then $V \subseteq (V_i V)_{\mathfrak{F}_i}$. By Lemma 1.1 V_i is an $\mathfrak{F}_i$-injector of $V_i V$. Hence $(V_i V)_{\mathfrak{F}_i} = V_i$. Thus $V \subseteq V_i$. A contradiction because V is not contained in any subnormal subgroup of G. The contradiction indicates that $\mathfrak{F}$ is an $\mathfrak{X}$-normal Fitting class. The theorem is proved.

We note by [1, Theorem 5.1] that every non-identity $\mathfrak{S}$-normal Fitting class contains the class of all nilpotent groups $\mathfrak{N}$. Therefore in the case $\mathfrak{X} = \mathfrak{S}$ we have the Blessenohl–Gaschütz's result.

Corollary 2.2. [1, Theorem 6. 2] *In the set of all non-identity normal Fitting classes there exists a unique minimal element by inclusion.*

References

[1] Blessenohl, D. and Gaschütz, W., Über normale Schunk und Fittingklassen, *Math. Z.*, **148** (1970), 1–8.

[2] Doerk, K. and Hawkes, T. O., *Finite Soluble Groups*, Berlin–New York, Walter de Gruyter, 1992.

[3] Fischer, B., Gaschütz, W. and Hartley, B., Injectoren endlicher auflösbaren Gruppen, *Math. Z.*, **102** (1967), 337–339.

[4] Laue, H., Über nichtauflösbare normalen Fittingklassen, *J. Algebra*, **45** (1977), 274–283.

[5] Sementovskii, V. G., *Injectors of finite groups*, Minsk, Nauka i Tekhnika, 1984, 166–170 (in Russian).

V. V. Shpakov, N. N. Vorob'ev and N. T. Vorob'ev
Department of Mathematics,
P. Masherov Vitebsk State University,
210038, Vitebsk, Belarus
e-mail: nicholas@vsu.by

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 173–177*

A NOTE ON BINOMIAL COEFFICIENTS AND EQUATIONS OF PYTHAGOREAN TYPE

László Szalay (Sopron, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. The aim of this paper is to solve three diophantine equations of Pythagorean type.

1. Introduction

In [1] LUCA determined all consecutive binomial coefficients satisfying the equation

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

His nice work leads to those Fibonacci numbers which are square or twice a square. In this note we apply LUCA's method to find all the solutions (n, k) of

$$a\binom{n}{k}^2 + b\binom{n}{k+1}^2 = \binom{n}{k+2}^2, \tag{1}$$

where $(a, b) = (1, 2)$ and $(a, b) = (2, 1)$. Moreover, the solutions of the diophantine equation

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

are also provided. The results are the following.

Theorem 1. *If $n \in \mathbf{N}$, $n \geq 2$ and $k \in \mathbf{N}$, $k \leq n-2$ satisfy equation (1) with $(a, b) = (1, 2)$ then $(n, k) = (14, 4)$.*

Theorem 2. *Equation (1) with $(a, b) = (2, 1)$ has no solution in $n \in \mathbf{N}$ and $k \in \mathbf{N}$ $(n \geq 2\ ,\ k \leq n-2)$.*

Theorem 3. *If $n \in \mathbf{N}$ and $k \in \mathbf{N}$, $k \leq n$ satisfy equation (2) then $(n, k) = (3, 1)$.*

Obviously, one can gain similar type of results as Theorem 1–3 if the symmetry of Pascal triangle is considered. For the proofs we follow paper [1] and go into details in only one case. The general case (1) seems to be more complicated. Even if $a = 1$ or $b = 1$, though the analogous equation to (6) exists, but the corresponding equation (11) or (12) is more difficult, where one should determine special figurate numbers in second order recurrences.

At the end of this paper we summarize some computational results in case $1 \leq a, b \leq 25$.

2. Proofs

Proof of Theorem 1. If $(a, b) = (1, 2)$ then equation (1) in natural numbers n and k leads to

$$(y+1)^2 \left(y^2 + 2x^2\right) = x^2 (x-1)^2 , \tag{3}$$

where $y = k + 1$ and $x = n - k$ are positive integers. Equation (3) implies that $y^2 + 2x^2$ is a square. It is well known (see, for example, [3]), that all the solutions of the diophantine equation $y^2 + 2x^2 = z^2$ in positive integers x, y and z can be expressed as

$$y = d\left|u^2 - 2v^2\right|, \quad x = 2duv, \quad z = d\left(u^2 + 2v^2\right), \tag{4}$$

with the conditions $d, u, v \in \mathbf{Z}^+$, $\gcd(u, v) = 1$ and $u \equiv 1 \pmod 2$. It is easy to see that $\gcd(u^2 + 2v^2, 2uv) = 1$. Therefore the consequence

$$\left(d|u^2 - 2v^2| + 1\right)\left(u^2 + 2v^2\right) = 2uv\,(2duv - 1) \tag{5}$$

of equation (3) together with (4) implies that

$$e = \frac{2duv - 1}{u^2 + 2v^2} = \frac{d|u^2 - 2v^2| + 1}{2uv} \tag{6}$$

is a positive integer. The system of two linear equations

$$\left.\begin{array}{rcrcr} (u^2 + 2v^2)e & - & (2uv)d & = & -1 \\ (2uv)e & - & |u^2 - 2v^2|d & = & 1 \end{array}\right\} \tag{7}$$

in variables e and d has a unique solution, namely

$$\left\{ e = \frac{|u^2 - 2v^2| + 2uv}{D},\ d = \frac{u^2 + 2v^2 + 2uv}{D} \right\} \tag{8}$$

with

$$D = -(u^2 + 2v^2)|u^2 + 2v^2| + 4u^2v^2 = \pm\left(u^4 - 4v^4\right) + 4u^2v^2.$$

Obviously, D is odd. If D has an odd prime divisor p then by (8) we conclude that p divides both $|u^2 - 2v^2| + 2uv$ and $u^2 + 2v^2 + 2uv$. But this is impossible because $\gcd(u, v) = 1$. Consequently $|D| = 1$. Here we must distinguish two cases. Depending on the sign of $u^2 - 2v^2$ either

$$4D = \left(2u^2 + 4v^2\right)^2 - 8\left(u^2\right)^2 = \pm 4, \tag{9}$$

or

$$4D = \left(2u^2 + 4v^2\right)^2 - 8\left(2v^2\right)^2 = \pm 4. \tag{10}$$

Both cases are connected with the Pell sequence $\{P_n\}_{n=0}^{\infty}$ defined by $P_s = 2P_{s-1} + P_{s-2}$, $P_0 = 0$, $P_1 = 1$, and its associate sequence $\{R_n\}_{n=0}^{\infty}$ given by the same recurrence relation and having initial values $R_0 = R_1 = 2$. These recurrences provide all the solutions of the equation $X^2 - 8Y^2 = \pm 4$. Therefore, by (9) or (10) it follows that

$$\left\{ P_s = u^2\ ,\ R_s = 2u^2 + 4v^2 \right\}$$

or, in the second case

$$\left\{ P_s = 2v^2,\ R_s = 2u^2 + 4v^2 \right\}.$$

Fortunately, the squares and twice a squares have already been determined in the Pell sequence (see [2] and [4]):

$$\left.\begin{array}{rcrcl} P_s = u^2 & \Leftrightarrow & (s,u) & = & (0,0);(1,1);(7,13); \\ P_s = 2v^2 & \Leftrightarrow & (s,v) & = & (0,0);(2,1). \end{array}\right\} \tag{11}$$

Among them only $(s, v) = (2, 1)$ provides a solution of the original problem, namely $(n, k) = (14, 4)$.

Proof of Theorem 2. This proof is very similar to the previous one, therefore we only indicate the crucial point of it. Equation (1) with $(a, b) = (2, 1)$ and later by $y = k + 1 = 2duv$, $x = n - k = d|u^2 - 2v^2|$ implies that

$$D = \left(u^2 + 2v^2 - uv\right)^2 - (3uv)^2 = \pm 1,$$

which contradicts that $u, v \in \mathbf{Z}^+$.

Proof of Theorem 3. Apply again the procedure of Luca. Equation (2) implies that

$$(y+1)^2 \left(y^2 + x^2\right) = x^2 (x+1)^2 \tag{12}$$

with $x = n$, $y = n - k$. The unknowns x and y are two entries of a Pythagorean triple, hence we have two cases. If

$$x = 2duv, \quad y = d(u^2 - v^2)$$

$(d, u, v \in \mathbf{Z}^+$, $\gcd(u, v) = 1$, $u \geq v$ and $u \not\equiv v \pmod{()2}$ then (12) leads to

$$\left(4u^2 + 2v^2\right)^2 - 5\left(2u^2\right)^2 = \pm 4,$$

otherwise, if we interchange the role of x and y in the equation $x^2 + y^2 = z^2$, it follows that

$$\left(2u^2 + 2v^2 - 2uv\right)^2 - 5\left(2uv\right)^2 = \pm 4.$$

As in [1], we must know the square and twice a square Fibonacci numbers. In the first case $F_s = 2u^2$, $L_s = 4u^2 + 2v^2$ provide the only solution $(n, k) = (3, 1)$. From $F_s = 2uv$, $L_s = 2u^2 + 2v^2 - uv$ we conclude that $F_{s-1} = (u - v)^2$ and it gives no more binomial coefficients satisfying (2) (see [1].

Computational results

If $1 \leq a, b \leq 25$, applying a simple computer search, we found all the solutions of equation (1) in the intervals $2 \leq n \leq 250$, $0 \leq k \leq n - 2$. The results are shown in the following table.

a	1	1	1	1	1	2	3	4	4	4	4	5	7	9	9	9	9
b	1	2	7	14	23	8	24	2	5	12	21	1	2	3	6	7	19
n	62	14	43	98	173	26	64	4	19	44	83	14	7	11	6	14	53
k	26	4	10	18	28	5	9	0	4	8	13	4	1	2	0	2	8

a	10	11	11	13	13	13	16	16	16	16	16	16	16	17	18	19
b	6	4	14	1	4	23	1	3	4	8	12	13	14	13	2	5
n	43	118	23	25	19	34	7	134	76	19	8	13	28	94	11	43
k	10	33	3	7	4	4	1	38	20	3	0	1	4	18	2	10

a	20	20	22	22	23	25	25	25	25	25	25	25
b	1	11	3	9	1	3	6	8	15	20	22	23
n	4	44	19	89	229	5	14	11	29	10	22	46
k	0	8	4	19	68	0	2	1	4	0	2	6

References

[1] Luca, F., Consecutive binomial coefficents in Pythagorean triples and squares in the Fibonacci sequence, *Fibonacci Quart.*, **40** (2002), 76–78.

[2] Ljunggren, W., Über die Gleichung $x^4 - Dy^2 = 1$, *Arch. Mat. Naturvid.*, **45** (1942), 61–70.

[3] Niven, I., Zuckerman, H., S.,*Bevezetés a számelméletbe*, Műszaki Kiadó, Budapest, 1978.

[4] Ribenboim, P., Pell numbers, squares and cubes, *Publ. Math. Debrecen*, **54** (1999), 131–152.

László Szalay
Institute of Mathematics and Statistics
University of West Hungary
Erzsébet str. 9, H-9400 Sopron
Hungary
e-mail: laszalay@ktk.nyme.hu

Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 179–190*

RELATIONSHIPS BETWEEN TRANSLATION AND ADDITIVE RELATIONS

Árpád Száz (Debrecen, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. According to our former papers, a relation F on a groupoid X is called a translation relation if $x+F(y)\subset F(x+y)$ for all $x,y\in X$. Moreover, a relation F on one groupoid X to another Y is called an additive relation if $F(x)+F(y)\subset F(x+y)$ for all $x,y\in X$.

In particular, a reflexive additive relation on a groupoid is a translation relation. Moreover, translation relations play important roles in the extensions and uniformizations of semigroups and groups, respectively. Therefore, it is of some interest to investigate the relationships between translation and additive relations.

In particular, we show that a normal translation relation on a group is odd (additive) if and only if it is symmetric (transitive). Moreover, if F is an odd additive relation of one group X into another Y and S is a translation relation on Y, then $R=F^{-1}\circ S\circ F$ is a translation relation on X such that $R=F^{-1}\circ S\circ f$ for any selection f of F.

A translation relation F on a group X is called normal if $F(0)+x\subset x+F(0)$ for all $x\in X$. Moreover, a relation F on one group X to another Y is called odd if $-F(x)\subset F(-x)$ for all $x\in X$. In particular, we also show that an additive function on one group to another is odd if and only if its domain is symmetric.

AMS Classification Number: 04A05, 20L13

Keywords and phrases: Translation, additive and odd relations on groups

1. A few basic facts on relations and groupoids

A subset F of a product set $X\times Y$ is called a relation on X to Y. In particular, the relations $\Delta_X=\{(x,x):\ x\in X\}$ and $X^2=X\times X$ are called the identity and universal relations on X, respectively.

Namely, if in particular $F\subset X^2$, then we may simply say that F is a relation on X. Note that if F is a relation on X to Y, then F is also a relation on $X\cup Y$. Therefore, it is frequently not a severe restriction to assume that $X=Y$.

The work has been supported by the grant OTKA T-030082.

If F is a relation on X to Y, then for any $x \in X$ and $A \subset X$ the sets $F(x) = \{y \in Y : (x,y) \in F\}$ and $F[A] = \bigcup_{x \in A} F(x)$ are called the images of x and A under F, respectively. Whenever $A \in X$ seems unlikely, we may write $F(A)$ in place of $F[A]$.

If F is a relation on X to Y, then the values $F(x)$, where $x \in X$, uniquely determine F since $F = \bigcup_{x \in X} \{x\} \times F(x)$. Therefore, the inverse F^{-1} of F can be defined such that $F^{-1}(y) = \big\{x \in X : \ \ y \in F(x)\big\}$ for all $y \in Y$.

Moreover, if F is a relation on X to Y and G is a relation on Y to Z, then the composition $G \circ F$ of G and F can be defined such that $(G \circ F)(x) = G\big(F(x)\big)$ for all $x \in X$. Note that thus we have $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.

If F is a relation on X to Y, then the sets $D_{_F} = F^{-1}(X)$ and $R_{_F} = F(X)$ are called the domain and range of F, respectively. If in particular $X = D_{_F}$ (and $Y = R_{_F}$) , then we say that F is a relation of X into (onto) Y.

A relation F on X to Y is called a function if for each $x \in D_{_F}$ there exists $y \in Y$ such that $F(x) = \{y\}$. In this case, by identifying singletons with their elements, we usually write $F(x) = y$ in place of $F(x) = \{y\}$.

If F is a relation on X to Y, then a function f of $D_{_F}$ into Y is called a selection of F if $f \subset F$. In terms of selections, the axiom of choice can be briefly reformulated by saying that every relation has a selection.

A relation F on X is called reflexive, symmetric and transitive if $\Delta_{_F} \subset F$, $F^{-1} \subset F$ and $F \circ F \subset F$, respectively. Note that if F is a symmetric relation, then we actually have $F = F^{-1}$.

If X is nonvoid set and $+$ is a function of X^2 into X, then the ordered pair $X(+) = (X,+)$ is called a groupoid. In this case, we may also naturally write $x + y = +(x,y)$ for all $x, y \in X$.

Moreover, if X is a groupoid, then we may also naturally write $A+B = \big\{x+y : x \in A, \ y \in B\big\}$ for all $A, B \subset X$. Thus, the family $\mathcal{P}(\mathcal{X})$ of all subsets of X is also a groupoid.

Note that if X is, in particular, a group, then $\mathcal{P}(\mathcal{X})$ is, in general, only a semigroup with zero element $\{0\}$. However, we can still naturally use the notations $-A = \big\{-x : \ x \in A\big\}$ and $A - B = A + (-B)$.

A subset A of a groupoid X is called additive and normal if $A + A \subset A$ and $A + x \subset x + A$ for all $x \in X$, respectively. Moreover, a subset A of a group X is called symmetric if $-A \subset A$.

Note that if A is a symmetric set, then we also have $A \subset -A$. Moreover, if A is a normal subset of a group X, then we also have $x + A = x + (A - x) + x \subset x + (-x + A) + x = A + x$ for all $x \in X$.

2. A few basic facts on translation relations

Definition 2.1. A relation F on a groupoid X is called a translation relation if

$$x + F(y) \subset F(x + y)$$

for all $x, y \in X$.

Remark 2.2. Note that thus we have $X + D_{_F} \subset D_{_F}$. Therefore, $D_{_F}$ is an ideal of X whenever $F \neq \emptyset$.

Hence, it is clear that $D_{_F} = X + D_{_F}$ whenever X has a zero element. Moreover, $D_{_F} = X$ whenever X is a group and $F \neq \emptyset$.

Remark 2.3. Moreover, it is also worth mentioning that, by using the notation xFy instead of $y \in F(x)$, the inclusion $x + F(y) \subset F(x + y)$ can be expressed by saying that yFz implies $(x + y)F(x + z)$.

Example 2.4. Clearly, the identity function $\Delta_{_X}$ of a groupoid X is a translation relation on X.

Moreover, the order relation $\leq$ of a left-ordered group X [5, p. 127] is, in particular, a translation relation on X.

Example 2.5. More generally, we can also note that if Y is a subset of a semigroup X and F is a relation on X such that $F(x) = x + Y$ for all $x \in X$, then F is a translation relation on X.

Moreover, we can also easily establish the following

Theorem 2.6. *If F is a relation on a group X, then the following assertions are equivalent :*

(1) F is a translation; *(2) $F(x) = x + F(0)$ for all $x \in X$.*

Proof. If (1) holds, then $x + F(0) \subset F(x + 0) = F(x)$ and $F(x) = x - x + F(x) \subset x + F(-x + x) = x + F(0)$ for all $x \in X$. Therefore, (2) also holds. Moreover, by Example 2.5, the converse implication (2) $\Longrightarrow$ (1) is also true.

Remark 2.7. In this respect, it is also worth mentioning that if F is a relation on a group X such that $F(x + y) \subset x + F(y)$ for all $x, y \in X$, then we also have $F(x) = x + F(0)$ for all $x \in X$. Therefore, F is a translation relation on X.

Example 2.8. If $X = [0, +\infty]$ and F is a relation on X such that $F(x) = [0, x]$ for all $x \in X$, then F is a translation (and a total order) relation on X such that $F(x) \neq x + F(0)$ for all $x \in X \setminus \{0\}$.

Example 2.9. More generally, we can also note that if p is a function on a group X to $[0, +\infty]$, and moreover $r \in [0, +\infty]$ and F is a relation on X such that

$F(x) = \{y \in X : \ p(-x+y) \leq r\}$ for all $x \in X$, then F is a translation relation on X. Therefore, $F(x) = x + F(0)$ for all $x \in X$.

Concerning translation relations, we shall also need the following theorems which have been mostly proved in [13].

Theorem 2.10. *If F is a relation on a groupoid X, then the following assertions are equivalent :*

(1) F is a translation ; *(2)* $\Delta_X + F \subset F$.

Remark 2.11. If F is a translation relation on a groupoid X with a zero element, then the equality $F = \Delta_X + F$ is also true.

Theorem 2.12. *If F is a translation relation on a groupoid X and $A, B \subset X$, then*

$$A + F(B) \subset F(A + B).$$

Moreover, if X is a group, then the corresponding equality is also true.

Remark 2.13. In this respect, it is also worth noticing that if F is a normal translation relation on a group X in the sense that $F(0)$ is a normal subset of X, then we also have $F(A + B) = F(A) + B$.

Theorem 2.14. *If F is a translation relation on a groupoid X, then F^{-1} is also a translation relation on X.*

Theorem 2.15. *If F is a normal translation relation on a group X and $A \subset X$, then*

$$F^{-1}(A) = -F(-A).$$

Remark 2.16. The equality $F^{-1}(0) = -F(0)$ is true even if the translation relation F is not normal.

Theorem 2.17. *If F and G are translation relations on a groupoid X, then $G \circ F$ is also a translation relation on X.*

Theorem 2.18. *If F is a normal and G is an arbitrary translation relation on a group X and $A, B \subset X$, then*

$$(G \circ F)(A + B) = F(A) + G(B).$$

Remark 2.19. The equality $(G \circ F)(0) = F(0) + G(0)$ is true even if F is an arbitrary relation on X.

Moreover, the equality $(G \circ F)(A) = F(A) + G(0)$ is true even if the translation relation F is not normal.

Therefore, under the conditions of Theorem 2.18, we also have $(G \circ F)(x) = (F \circ G)(x)$ for all $x \in X$, and hence $G \circ F = F \circ G$.

3. A few basic facts on additive relations

Definition 3.1. A relation F on one groupoid X to another Y is called additive if

$$F(x) + F(y) \subset F(x + y)$$

for all $x, y \in X$.

Remark 3.2. Note that thus we have $D_F + D_F \subset D_F$. Therefore, D_F is a subgroupoid of X whenever $F \neq \emptyset$.

Remark 3.3. Moreover, it is also worth noticing that, by using the notation xFy instead of $y \in F(x)$, the inclusion $F(x) + F(y) \subset F(x + y)$ can be expressed by saying that xFz and yFw imply $(x + y)F(z + w)$.

Example 3.4. Note that the order relation $\leq$ of an ordered group X [3, p. 9] is, in particular, an additive relation on X.

Example 3.5. More generally, we can also note that if X is a groupoid and Z is an additive and normal subset of a semigroup Y, and moreover f is an additive function on X to Y and F is a relation on X to Y such that $F(x) = f(x) + Z$ for all $x \in X$, then F is an additive relation on X to Y.

Moreover, we can also easily establish the following

Theorem 3.6. *If F is an additive relation on one group X to another Y and f is a selection for F such that $-f(x) \in F(-x)$ for all $x \in D_F$, then for all $x \in D_F$ we also have*

$$F(x) = f(x) + F(0).$$

Proof. Namely, we evidently have $f(x) + F(0) \subset F(x) + F(0) \subset F(x)$ and

$$F(x) = f(x) - f(x) + F(x) \subset f(x) + F(-x) + F(x) \subset f(x) + F(0)$$

for all $x \in X$. Therefore, the required equality is also true.

Remark 3.7. Quite similarly, we can also prove that $F(x) = F(0) + f(x)$ for all $x \in D_F$.

Example 3.8. If X and F are as in Example 2.8, then F is an additive relation on X such that for any function f of X and $Z \subset X$, with $F(0) = f(0) + Z$, we have $F(x) \neq f(x) + Z$ for all $x \in X \setminus \{0\}$.

Example 3.9. More generally, we can also note that if $X = [0, +\infty]$, p is a subadditive function on a groupoid Y to X, and F is a relation on X to Y such that $F(x) = \{y \in Y : \ p(y) \leq x\}$ for all $x \in X$, then F is an additive relation on X to Y.

Concerning additive relations, we can also easily prove the following counterparts of the corresponding results of [14].

Theorem 3.10. *If F is a relation on one groupoid X to another Y, then the following assertions are equivalent:*

(1) F is additive ; *(2) $F + F \subset F$.*

Theorem 3.11. *If F is an additive relation on one groupoid X to another Y and $A, B \subset X$, then*

$$F(A) + F(B) \subset F(A + B).$$

Theorem 3.12. *If F is an additive relation on one groupoid X to another Y, then F^{-1} is an additive relation on Y to X.*

Theorem 3.13. *If F is an additive relation on one groupoid X to another Y and G is an additive relation on Y to a groupoid Z, then $G \circ F$ is an additive relation on X to Z.*

The relationship between translation and additive relations can be cleared up by the following

Theorem 3.14. *If F is a normal translation relation on a group X, then the following assertions are equivalent :*

(1) F is additive ; *(2) F is transitive.*

Proof. If (1) holds, then by Remark 2.19 we have $(F \circ F)(x) = F(x) + F(0) \subset F(x)$ for all $x \in X$ even if F is not normal. Therefore, $F \circ F \subset F$, and thus (2) also holds.

While, if (2) holds, then by Theorem 2.18 we have $F(x) + F(y) = (F \circ F)(x + y) \subset F(x + y)$ for all $x, y \in X$. Therefore, (1) also holds.

Remark 3.15. Quite similarly, we can also prove that a translation relation F on a group X is transitive if and only if the set $F(0)$ is additive.

Moreover, in addition to Theorem 3.14, it is also worth noticing that a reflexive and additive relation F on a groupoid X is a translation relation.

4. A few basic facts on odd relations

Definition 4.1. A relation F on one group X to another Y is called odd if

$$-F(x) \subset F(-x)$$

for all $x \in X$.

Remark 4.2. Note that thus we have $-D_{_F} \subset D_{_F}$. Therefore, $D_{_F}$ is a symmetric subset of X, and we have $D_{_F} = -D_{_F}$.

Remark 4.3. Moreover, it is also worth noticing that, by using the notation xFy instead of $y \in F(x)$, the inclusion $-F(x) \subset F(-x)$ can be expressed by saying that xFy implies $(-x)F(-y)$.

Example 4.4. Note that the order relation $\leq$ of an ordered group X is odd if and only if $\leq$ coincides with $\Delta_{_X}$.

Concerning odd relations, we can also easily prove the following theorems.

Theorem 4.5. *If F is a relation on one group X to another Y, then the following assertions are equivalent :*

(1) F is odd; *(2) $-F = F$.*

Theorem 4.6. *If F is an odd relation on one group X to another Y and $A \subset X$, then*

$$F(-A) = -F(A).$$

Proof. If $y \in -F(A)$, then $-y \in F(A)$. Therefore, there exists $x \in A$ such that $-y \in F(x)$. Hence, we can already see that $y \in -F(x) \subset F(-x) \subset F(-A)$. Therefore, $-F(A) \subset F(-A)$.

Now, by writing $-A$ in place of A, we can also see that $-F(-A) \subset F(A)$, and hence $F(-A) \subset -F(A)$ is also true.

Theorem 4.7. *If F is an odd relation on one group X to another Y, then F^{-1} is an odd relation on Y to X.*

Theorem 4.8. *If F is odd relation on one group X to another Y and G is an odd relation on Y to a group Z, then $G \circ F$ is an odd relation on X to Z.*

The relationship between odd and translation relations can be cleared up by the following

Theorem 4.9. *If F is a normal translation relation on a group X, then the following assertions are equivalent :*

(1) F is odd; *(2) F is symmetric.*

Proof. If (1) holds, then by Theorems 2.15 and 4.6 we have $F^{-1}(x) = -F(-x) = -\big(-F(x)\big) = F(x)$ for all $x \in X$. Therefore, $F^{-1} = F$, and thus (2) also holds.

While, if (2) holds, then only by Theorem 2.15 we have $-F(x) = -F^{-1}(x) = -\big(-F(-x)\big) = F(-x)$ for all $x \in X$. Therefore, (1) also holds.

Remark 4.10. Quite similarly, we can also prove that a translation relation F on a group X is symmetric if and only if the set $F(0)$ is symmetric.

Concerning the relationship between odd and additive relations, we can only prove the following theorems.

Theorem 4.11. *If F is an additive relation on one group X to another Y and f is an odd selection for F, then for all $x \in D_F$ we have*

$$F(x) = f(x) + F(0).$$

Proof. Namely, $-f(x) = f(-x) \in F(-x)$ for all $x \in D_F$. Therefore, Theorem 3.6 can be applied.

Theorem 4.12. *If f is an additive function on one group X to another Y, then the following assertions are equivalent:*

(1) f is odd; *(2) D_f is symmetric.*

Proof. By Remark 4.2, it is clear that the implication (1)$\Longrightarrow$(2) is true even if f is not additive.

Moreover, if (2) holds, then for any $x \in D_f$, we also have $-x \in D_f$. Hence, by the additivity of f, it follows that $f(x) + f(-x) = f(0)$. Now, by writing 0 in place of x, we can see that $f(0) + f(0) = f(0)$, and thus $f(0) = 0$. Therefore, we actually have $f(x) + f(-x) = 0$, and hence $-f(x) = f(-x)$. That is, (1) also holds.

Example 4.13. If X is a group and Z is an additive and normal subset of a group Y, and moreover f is an additive function on X to Y, with a symmetric domain, and F is a relation on X to Y such that $F(x) = f(x) + Z$ for all $x \in X$, then F is an odd additive relation on X to Y.

5. A few basic facts on odd additive relations

Theorem 5.1. *If F is a nonvoid odd additive relation on one group X to another Y, then $0 \in F(0)$.*

Proof. Since $F \neq \emptyset$, there exist $x \in X$ and $y \in Y$ such that $y \in F(x)$. Hence, by the assumed properties of F, it is clear that $0 = y - y \in F(x) - F(x) = F(x) + F(-x) \subset F(0)$.

Corollary 5.2. *If F is an odd additive relation on one group X to another Y and f is a function of D_F into Y such that $F(x) = f(x) + F(0)$ for all $x \in D_F$, then f is a selection for F.*

Theorem 5.3. *If F is an odd additive relation on one group X to another Y and f is a selection for F, then for all $x \in D_F$ we have*

$$F(x) = f(x) + F(0).$$

Proof. Namely, $-f(x) \in -F(x) = F(-x)$ for all $x \in D_F$. Therefore, Theorem 3.6 can be applied.

Theorem 5.4. *If F is an odd additive relation on one group X to another Y and $A \subset D_F$ and $B \subset X$, then*

$$F(A+B) = F(A) + F(B).$$

Proof. Since $A \subset D_F$, for each $x \in A$ there exists $y \in F(x)$. Hence, by Theorem 3.11, it is clear that

$$\begin{aligned} F(x+B) &= y - y + F(x+B) \subset F(x) - F(x) + F(x+B) \\ &= F(x) + F(-x) + F(x+B) \subset F(A) + F(-x+x+B) = F(A) + F(B). \end{aligned}$$

Therefore, we also have

$$F(A+B) = F\Big(\bigcup_{x\in A}(x+B)\Big) = \bigcup_{x\in A} F(x+B) \subset F(A) + F(B).$$

Thus, by Theorem 3.11, the corresponding equality is also true.

Remark 5.5. If $A \subset X$ and $B \subset D_F$, then we can quite similarly see that the equality $F(A+B) = F(A) + F(B)$ is also true.

Example 5.6. If $F = \Delta_{\Delta_{\mathbf{R}}}$, then F is a linear relation on $\mathbf{R}^2$. Moreover, if $A = \mathbf{R} \times \{0\}$ and $B = \{0\} \times \mathbf{R}$, then

$$F(A+B) = \Delta_{\mathbf{R}}, \quad \text{but} \quad F(A) + F(B) = \{(0,0)\}.$$

Remark 5.7. A relation F on one vector space X to another Y over the same field K is called linear [15] if in addition to the additivity of F we also have $\lambda F(x) \subset F(\lambda x)$ for all $\lambda \in K$ and $x \in X$.

6. Projective generation of translation relations

Theorem 6.1. *If F is an additive relation of one groupoid X into another Y and S is a translation relation on Y, then $R = F^{-1} \circ S \circ F$ is a translation relation on X.*

Proof. If $x, y \in X$ and $z \in R(y)$, then by the corresponding definitions we also have $z \in \big(F^{-1} \circ S \circ F\big)(y) = F^{-1}\big(S\big(F(y)\big)\big)$. Therefore, there exists $w \in S\big(F(y)\big)$ such that $z \in F^{-1}(w)$, and hence $w \in F(z)$. Consequently, we also have $F(z) \cap S\big(F(y)\big) \neq \emptyset$. Hence, since $F(x) \neq \emptyset$, it follows that

$$\big(F(x) + F(z)\big) \cap \big(F(x) + S\big(F(0)\big)\big) \neq \emptyset.$$

Hence, by using that $F(x)+F(z)\subset F(x+z)$ and

$$F(x)+S\big(F(y)\big)\subset S\big(F(x)+F(y)\big)\subset S\big(F(x+y)\big),$$

we can infer that

$$F(x+z)\cap S\big(F(x+y)\big)\neq\emptyset.$$

Therefore, there exists $\omega\in S\big(F(x+y)\big)$ such that $\omega\in F(x+z)$, and hence $x+z\in F^{-1}(\omega)$. Consequently, we also have

$$x+z\in F^{-1}\left(S\big(F(x+y)\big)\right)=\big(F^{-1}\circ S\circ F\big)(x+y)=R(x+y).$$

Therefore, the inclusion $x+R(y)\subset R(x+y)$ is also true.

Theorem 6.2. *If F is a relation on one group X to another Y such that*

(1) $0\in F(0)$, *(2)* $-F(0)\subset F(0)$,

(3) $F(0)+F(x)\subset F(x)$ *for all* $x\in X$,

and S is a translation relation on Y, then

$$F^{-1}\big(S(0)\big)=F^{-1}\left(S\big(F(0)\big)\right).$$

Proof. Because of hypothesis (1), we evidently have $S(0)\subset S\big(F(0)\big)$, and hence $F^{-1}\big(S(0)\big)\subset F^{-1}\left(S\big(F(0)\big)\right)$.

To prove the converse inclusion, note that if $x\in F^{-1}\left(S\big(F(0)\big)\right)$, then there exists $y\in S\big(F(0)\big)$ such that $x\in F^{-1}(y)$, and hence $y\in F(x)$. Moreover, there exists $z\in F(0)$ such that $y\in S(z)$. Hence, by using the translation property of S, we can see that

$$-z+y\subset -z+S(z)\subset S(-z+z)=S(0).$$

Moreover, by using hypotheses (2) and (3), we can see that

$$-z+y\in -F(0)+F(x)\subset F(0)+F(x)\subset F(x),$$

and hence $x\in F^{-1}(-z+y)$. Therefore, we also have $x\in F^{-1}\big(S(0)\big)$.

Corollary 6.3. *If F is an odd additive relation on one group X to another Y and S is a translation relation on Y, then* $F^{-1}\big(S(0)\big)=F^{-1}\left(S\big(F(0)\big)\right)$.

Proof. If $F=\emptyset$, then the required assertion trivially holds. While, if $F\neq\emptyset$, then by Theorem 5.1 we have $0\in F(0)$. Thus, Theorem 6.2, can be applied.

Theorem 6.4. *If F is an odd additive relation on one group X to another Y and S is a translation relation on Y, then for any selection f of F we have*

$$F^{-1}\circ S\circ f=F^{-1}\circ S\circ F.$$

Proof. In this case, by Theorems 4.7 and 3.12, it is clear that F^{-1} is an odd additive relation on Y to X. Moreover, by using Theorems 3.11, 5.3 and 5.4 and Corollary 6.3, we can see that

$$\begin{aligned}
&\big(F^{-1}\circ S\circ f\big)(x) = F^{-1}\big(S\big(f(x)\big)\big) = F^{-1}\big(f(x)+S(0)\big)\\
&= F^{-1}\big(f(x)\big) + F^{-1}\big(S(0)\big) = F^{-1}\big(f(x)\big) + F^{-1}\big(S\big(F(0)\big)\big)\\
&= F^{-1}\big(f(x)+S\big(F(0)\big)\big) = F^{-1}\big(S\big(f(x)+F(0)\big)\big)\\
&= F^{-1}\big(S\big(F(x)\big)\big) = \big(F^{-1}\circ S\circ F\big)(x)
\end{aligned}$$

for all $x\in D_{_F}$. Therefore, the required equality is also true.

Remark 6.5. If F and S are in Theorem 6.4, then as a more direct generalization of Corollary 6.3, we can also prove that $F^{-1}\big(S(y)\big)= F^{-1}\big(S\big(F(x)\big)\big)$ for all $x\in D_{_F}$ and $y\in F(x)$.

However, the latter statement can also be easily derived from Theorem 6.4 since by the axiom of choice for any $x\in D_{_F}$ and $y\in F(x)$ there exists a selection f of F such that $f(x)=y$.

References

[1] Arens, R., Operational calculus of linear relations, *Pacific J. Math.*, **11** (1961), 9–23.

[2] Cross, R., *Multivalued Linear Operators*, Marcel Dekker, New York, 1998.

[3] Fuchs, L., *Partially Ordered Algebraic Systems*, Pergamon Press, Oxford, 1963.

[4] Godini, G., Set-valued Cauchy functional equation, *Rev. Roumaine Math. Pures Appl.*, **20** (1975), 1113–1121.

[5] Mura, R. B. and Rhemtulla, A., *Orderable Groups*, Marcel Dekker, New York, 1977.

[6] Nikodem, K., Additive selections of additive set-valued functions, *Univ. u Novom Sadu Zb. Rad. Pirod.-Mat. Fak. Ser. Mat.*, **18** (1988), 143–148.

[7] Száz, Á., Projective generation of preseminormed spaces by linear relations, *Acta Sci. Math. Hungar.*, **23** (1988), 297–313.

[8] Száz, Á., Projective and inductive generations of relator spaces, *Acta Math. Hungar.*, **53** (1989), 407–430.

[9] Száz, Á., Pointwise limits of nets of multilinear maps, *Acta Sci. Math. (Szeged)*, **55** (1991), 103–117.

[10] Száz, Á., The intersection convolution of relations and the Hahn–Banach type theorems, *Ann. Polon. Math.*, **69** (1998), 235–249.

[11] Száz, Á., Preseminorm generating relations and their Minkowski functionals, *Publ. Elektrotehn. Fak., Univ. Beograd, Ser. Mat.*, **12** (2001), 16–34.

[12] Száz, Á., Partial multipliers on partially ordered sets, *Novi Sad J. Math.* , **32** (2002), 25–45.

[13] Száz, Á., Translation relations, the building blocks of compatible relators, *Math. Montisnigri*, to appear.

[14] Száz, Á. and Száz, G., Additive relations, *Publ. Math. Debrecen*, **20** (1973), 259–272.

[15] Száz, Á. and Száz, G., Linear relations, *Publ. Math. Debrecen*, **27** (1980), 219–227.

Árpád Száz
Institute of Mathematics
University of Debrecen
H-4010 Debrecen, P.O. Box 12
Hungary
e-mail: szaz@math.klte.hu