ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXV.

AZ ESZTERHÁZY KÁROLY TANÁRKÉPZŐ FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI

REDIGIT—SZERKESZTI
PÓCS TAMÁS, V. RAISZ RÓZSA

SECTIO MATEMATICAE

TANULMÁNYOK A MATEMATIKAI TUDOMÁNYOK KÖRÉBŐL

REDIGIT—SZERKESZTI
KISS PÉTER, RIMÁN JÁNOS

EGER, 1998

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXV.

AZ ESZTERHÁZY KÁROLY TANÁRKÉPZŐ FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI

REDIGIT—SZERKESZTI
PÓCS TAMÁS, V. RAISZ RÓZSA

SECTIO MATEMATICAE

TANULMÁNYOK A MATEMATIKAI TUDOMÁNYOK KÖRÉBŐL

REDIGIT—SZERKESZTI
KISS PÉTER, RIMÁN JÁNOS

EGER, 1998

EMTEX—JATEX

A kiadásért felelős:
az Eszterházy Károly Tanárképző Főiskola főigazgatója
Megjelent az EKTF Líceum Kiadó műszaki gondozásában
Kiadóvezető: Rimán János
Felelős szerkesztő: Zimányi Árpád
Műszaki szerkesztő: Rimán János
Megjelent: 1999. február Példányszám: 50

Készült: Molnár és Társa '2001' Kft. nyomdája, Eger
Ügyvezető igazgató: Molnár György

An application of the continued fractions for $\sqrt{D}$ in solving some types of Pell's equations

BÉLA ZAY

Abstract. In this paper we study the positive solutions of the Diophantine equation $x^2-Dy^2=N$, where D and $|N|$ are natural numbers, $|N|<\sqrt{D}$ and D is not the square of a natural number. Let $\sqrt{D}=(a_0,\overline{a_1,\ldots,a_s})$ be the representation of $\sqrt{D}$ as a simple continued fraction expansion. We prove that if the n-th convergent to $\sqrt{D}$ is $\frac{H_n}{K_n}=(a_0,\ldots,a_n)$, then

$$H_{(n+2)s+r}=2H_{s-1}H_{(n+1)s+r}+(-1)^{s+1}H_{ns+r}$$

and

$$H_{(n+2)s+r}=2H_{s-1}K_{(n+1)s+r}+(-1)^{s+1}K_{ns+r}.$$

In cases of $D=(2k+1)^2-4$ (for any $k\geq 2$), $D=(2k)^2-4$ (for any $k\geq 3$), $D=k^2-1$ (for any $k\geq 2$) and $D=k^2+1$ (for any $k\geq 1$) we give all positive solutions of $x^2-Dy^2=N$ $\left(|N|<\sqrt{D}\right)$ with the help of Binet formulae of the sequences (H_{ns+r}) and (K_{ns+r}) (for any $r=1,2,\ldots,s$).

Introduction

In this paper we consider the equation

$$x^2 - Dy^2 = N \tag{1}$$

and its solutions in natural numbers, provided D and N are rational integers, $D > 0$, furthermore D is not the square of a natural number. Many authors studied these Diophantine equations. Among others D. E. FERGUSON [1] solved the equations $x^2-5y^2 = \pm 4$, V. E. HOGATT, JR. and M. BICKNELL-JOHNSON [2] solved the equations

$$x^2 - (A^2 \pm 4)y^2 = \pm 4 \tag{2}$$

where A is a fixed natural number. K. LIPTAI [4] proved that if there is a solution to (1) then all solutions can be given with the help of finitely many, well determined second order linear recurrences.

Research supported by Foundation for Hungarian Higher Education and Research and Hungarian OTKA Foundation Grant No. T 16975 and 020295.

Auxiliary results

The purpose of this paper is to give such second order linear recurrences in case of $|N| < \sqrt{D}$ and in some special cases.

We shall use a lemma of P. KISS [3] and some theorems from [5] and [6].

Let γ be a real quadratic irrational number and let

$$\gamma = (a_0, a_1, a_2, \ldots) = (a_0, a_1, \ldots, a_{t-1}, \overline{a_t, \ldots, a_{t+s-1}}) \tag{3}$$

be the representation of γ as a simple periodic continued fraction, where s is the minimal period length of (3). P. KISS proved:

If the n-th convergent to γ is $\frac{H_n}{K_n} = (a_0, a_1, \ldots, a_n)$ and the n-th convergent to $\gamma_0 = (\overline{a_t, \ldots, a_{t+s-1}})$ is $\frac{h_n}{k_n} = (a_t, a_{t+1}, \ldots, a_{t+n})$, then (as it was proved by P. Kiss [3])

$$H_{(n+2)s+r} = (h_{s-1} + k_{s-2})H_{(n+1)s+r} + (-1)^{s+1} H_{ns+r}, \tag{4}$$

and

$$K_{(n+2)s+r} = (h_{s-1} + k_{s-2})K_{(n+1)s+r} + (-1)^{s+1} K_{ns+r}, \tag{5}$$

where $n \geq 0, r = 0, 1, \ldots, s-1$ and we assume, that $k_{-1} = 0$.

In the special case of $\gamma = \sqrt{D}$ we prove the following lemma.

Lemma 1. *Let D be a positive integer which is not a square of a natural number and let*

$$\sqrt{D} = (a_0, \overline{a_1, \ldots, a_s}) \tag{6}$$

be the representation of $\sqrt{D}$ as a simple continued fraction expansion, where s is the period length of (6). If the n-th convergent to $\sqrt{D}$ is

$$\frac{H_n}{K_n} = (a_0, a_1, \ldots, a_n)$$

then

$$H_{(n+2)s+r} = 2H_{s-1} H_{(n+1)s+r} + (-1)^{s+1} H_{ns+r} \tag{7}$$

and

$$K_{(n+2)s+r} = 2H_{s-1} K_{(n+1)s+r} + (-1)^{s+1} H_{ns+r} \tag{8}$$

for every integer $n \geq 0$ and r $(0 \leq r \leq s-1)$.

The first $2s$ terms of sequences (H_n) and (K_n) can be got from the following well known relations

$$H_m = a_m H_{m-1} + H_{m-2}, \quad H_{-1} = 1,\ H_0 = a_0, \tag{9}$$

and

$$K_m = a_m K_{m-1} + K_{m-1}, \quad K_{-1} = 0,\ K_0 = 1, \tag{10}$$

for any $m \geq 0$.

The following algorithm for representing the number $\sqrt{D}$ as a simple continued fraction is well known (see in [6], p. 319): We set $a_0 = \left[\sqrt{D}\right]$, $b_1 = a_0$, $c_1 = D - a_0^2$ and we find the numbers a_{n-1}, b_n and c_n successively using the formulae

$$a_{n-1} = \left[\frac{a_0 + b_{n-1}}{c_{n-1}}\right], \quad b_n = a_{n-1}c_{n-1} - b_{n-1}, \quad c_n = \frac{D - b_n^2}{c_{n-1}}.$$

Now consider the sequence

$$(b_2, c_2), \quad (b_3, c_3), \quad (b_4, c_4), \ldots$$

and find the smallest index s for which $b_{s+1} = b_1$ and $c_{s+1} = c_1$. Then the representation of $\sqrt{D}$ as a simple continued fraction is

$$\sqrt{D} = (a_0, \overline{a_1, a_2, \ldots, a_s}).$$

We shall use two other results from [5] (pp 158–159).

Lemma 2. *If D is a positiv integer, not a perfect square, then $H_n^2 - DK_n^2 = (-1)^{n-1}c_{n+1}$ for all integer $n \geq -1$.*

Lemma 3. *Let D be a positive integer not a perfect square, and let the convergents to the continued fraction expansion of $\sqrt{D}$ be H_n/K_n. Let N be an integer for which $|N| < D$. Then any positive solution $x = u, y = t$ of $x^2 - Dy^2 = N$ with $(u, t) = 1$ satisfies $u = H_n, t = K_n$, for some positive integer n.*

Recalling that $c_n = c_{n+s}$ in the Lemma 2., we can formulate Lemma 4. which is a consequence of the first three lemmas.

Lemma 4. *Let D be a positive integer not a perfect square, and let*

$$\sqrt{D} = (a_0, \overline{a_1, \ldots, a_s})$$

be the representation of $\sqrt{D}$ *as a simple continued fraction. Suppose that* N *is a non-zero integer with* $|N| < \sqrt{D}$, *and let*

$$H_{-1} = 1, \quad H_0 = a_0, \quad H_m = a_m H_{m-1} + H_{m-2}, \quad 1 \le m \le 2s, \tag{11}$$

$$K_{-1} = 0, \quad K_0 = 1, \quad K_m = a_m K_{m-1} + K_{m-2}, \quad 1 \le m \le 2s, \tag{12}$$

$$H_{(n+2)s+r} = 2H_{s-1}H_{(n+1)s+r} + (-1)^{s+1}H_{ns+r}, \ 1 \le r \le s, \ n \ge 0, \tag{13}$$

$$K_{(n+2)s+r} = 2H_{s-1}K_{(n+1)s+r} + (-1)^{s+1}K_{ns+r}, \ 1 \le r \le s, \ n \ge 0, \tag{14}$$

and

$$c_{ns+r+1} = (-1)^{ns+r-1}(H_r^2 - DK_r^2), \ 1 \le r \le s. \tag{15}$$

If $1 \le r \le s, c_{r+1} \ne 0$ *and* $\sqrt{\frac{(-1)^{n-1}N}{c_{r+1}}}$ *is a natural number then let* $d_r = \sqrt{\frac{(-1)^{r-1}N}{c_{r+1}}}$. *Denote by* M *the set of positive solutions* (x, y) *of* $x^2 - Dy^2 = N$. *Then*

$$M = \{(x, y) : x = d_r H_{ns+r}, \ y = d_r K_{ns+r}, \ n \ge 0, \ 1 \le r \le s\}. \tag{16}$$

This also means that: If there exists no natural numbers d_r $(1 \le r \le s)$ which satisfy the above conditions then there isn't integer solution $x = u$, $y = t$ of $x^2 - Dy^2 = N$ $(|N| < D)$, that is M is the empty set.

Theorems

Applying Lemma 4. for some special equations we obtain the following results.

Theorem 1. *Let* k $(k \ge 2)$ *be a natural number with* $D = (2k+1)^2 - 4$. *Let* α *and* β *denote the zeros of* $f_1(x) = x^2 - (2k+1)x + 1$ *and let* $\alpha > \beta$. *Denote by* M *the set of positive* (x, y) *solutions of* $x^2 - Dy^2 = N$.

(a) *If* $N = 4l^2$ *and* $l \left(1 \le l \le \sqrt{\frac{k}{2}}\right)$ *is a natural number, then*

$$M = \left\{(x, y) : x = l(\alpha^m + \beta^m), \quad y = l\frac{\alpha^m - \beta^m}{\alpha - \beta}, \ m \ge 1\right\}.$$

(b) *If* $N = (2l-1)^2$ *and* $1 \le l \le \frac{1}{2} + \sqrt{\frac{k}{2}}$ *then*

$$M = \left\{(x, y) : x = \left(l - \frac{1}{2}\right)(\alpha^{3m+3} + \beta^{3m+3}), \right.$$
$$\left. y = \left(l - \frac{1}{2}\right)\frac{\alpha^{3m+3} - \beta^{3m+3}}{\alpha - \beta}, \ m \ge 1\right\}.$$

(c) *If* $N = 1 - 2k$ *then*

$$M = \left\{(x,y)\colon x = \frac{(\alpha-1)\alpha^{3m+1} + (\beta-1)\beta^{3m+1}}{2}, \right.$$
$$\left. y = \frac{(\alpha-1)\alpha^{3m+1} - (\beta-1)\beta^{3m+1}}{2(\alpha-\beta)},\ m \geq 1\right\}.$$

(d) *If* $1 \leq |N| \leq 2k$, $N \neq 1-2k$ *and* N *isn't a square of a natural number then* $M = \emptyset$ *(empty set).*

Theorem 2. *Let* k $(k \geq 3)$ *be a natural number and* $D = (2k)^2 - 4$. *Let* α *and* β *denote the zeros of* $f_2(x) = x^2 - 2kx + 1$ *with* $\alpha > \beta$. *Denote by* M *the set of positive* (x,y) *solutions of* $x^2 - Dy^2 = N$.

(a) *If* $N = 4l^2$ *and* l $\left(1 \leq l \leq \sqrt{\frac{k-1}{2}}\right)$ *is a natural number then*

$$M = \left\{(x,y)\colon x = l(\alpha^m + \beta^m),\ \ y = l\frac{\alpha^m - \beta^m}{\alpha-\beta},\ m \geq 1\right\}.$$

(b) *If* $N = (2l-1)^2$ *and* l *is a natural number* $\left(1 \leq l < \frac{1}{2} + \sqrt{k^2-1}\right)$ *then*

$$M = \left\{(x,y)\colon x = \left(l - \frac{1}{2}\right)\left(\alpha^{2m} + \beta^{2m}\right), \right.$$
$$\left. y = \left(l - \frac{1}{2}\right)\frac{\alpha^{2m} - \beta^{2m}}{\alpha-\beta},\ m \geq 1\right\}.$$

(c) *If* $1 \leq |N| < 2k$ *and* N *isn't a square of a natural number then* $M = \emptyset$.

Theorem 3. *Let* k $(k \geq 2)$ *be a natural number and* $D = k^2 - 1$. *Let* α *and* β *denote the zeros of* $f_3(x) = x^2 - 2kx + 1$ *where* $\alpha > \beta$. *Denote by* M *the set of positive solutions of* $x^2 - Dy^2 = N$.

(a) *If* $N = l^2$ *and* $1 \leq l \leq \sqrt{k-1}$ *then*

$$M = \left\{(x,y)\colon x = \frac{l}{2}(\alpha^{n+1} + \beta^{n+1}),\ y = \frac{l\left(\alpha^{n+1} - \beta^{n+1}\right)}{2(\alpha-\beta)},\ m \geq 1\right\}.$$

(b) *If* $1 \leq |N| < 2k-1$ *and* N *isn't a square of a natural number then* $M = \emptyset$.

Theorem 4. *Let k $(k \geq 1)$ be a natural number and $D = k^2 + 1$. Let α and β denote the zeros of $f_4(x) = x^2 - 2kx - 1$ with $\alpha > \beta$. Denote by M the set of positive solutions of $x^2 - Dy^2 = N$.*
(a) *If $N = l^2$ and $1 \leq l \leq \sqrt{k}$ then*

$$M \left\{ (x,y) \colon x = \frac{l}{2}\left(\alpha^{2n+1} + \beta^{2n+1}\right),\ y = \frac{l(\alpha^{2n+1} - \beta^{2n+1})}{\alpha - \beta},\ m \geq 1 \right\}.$$

(b) *If $N = -l^2$ and $1 \leq l \leq \sqrt{k}$ then*

$$M = \left\{ (x,y) \colon x = \frac{l}{2}(\alpha^{2m} + \beta^{2m}),\ y = \frac{l\left(\alpha^{2m} - \beta^{2m}\right)}{\alpha - \beta},\ m \geq 1 \right\}.$$

(c) *If $1 \leq |N| \leq k$ and $|N|$ isn't a square of a natural number then $M = \emptyset$.*

Proofs

To prove Lemma 1. we need the following two lemmas.

Lemma 5. *Let $f_{n+2}(x_1, x_2, \ldots, x_n)$ and $g_{n+2}(x_1, x_2, \ldots, x_n)$ be the polinomials which are defined by recurring relations*

$$f_{n+2}(x_1, \ldots, x_n) = x_n f_{n+1}(x_1, \ldots, x_{n-1}) + f_n(x_1, \ldots, x_{n-2}),\ n \geq 1$$

and

$$g_{n+2}(x_1, \ldots, x_n) = x_1 g_{n+1}(x_2, \ldots, x_n) + g_n(x_3, \ldots, x_n),\ n \geq 1$$

respectively, where $f_1 = g_1 = 0$ and $f_2 = g_2 = 1$. Then

$$f_{n+2}(x_1, \ldots, x_n) = g_{n+2}(x_1, \ldots, x_n),\quad n \geq -1$$

also holds.

Proof. We can easily verify that

$$f_1 = g_1,\ f_2 = g_2,\ f_3(x_1) = x_1 = g_3(x_1)$$

and

$$f_4(x_1, x_2) = x_2 f_3(x_1) + f_2 = g_3(x_2)x_1 + g_2 = g_4(x_1, x_2).$$

Assume that $n \geq 3$ and

$$f_{n+2-i}(x_1, \ldots, x_{n-1}) = g_{n+2-i}(x_1, \ldots, x_{n-1})$$

holds for $i = 1, 2, 3, 4$.

Using the definitions and the last assumptions we can finish the proof by induction for n:

$$\begin{aligned}
&f_{n+2}(x_1,\ldots,x_n) = x_n f_{n+1}(x_1,\ldots,x_{n-1}) + f_n(x_1,\ldots,x_{n-2})\\
=&x_n g_{n+1}(x_1,\ldots,x_{n-1}) + g_n(x_1,\ldots,x_{n-2})\\
=&x_n x_1 g_n(x_2,\ldots,x_{n-1}) + x_n g_{n-1}(x_3,\ldots,x_{n-1})\\
+&x_1 g_{n-1}(x_2,\ldots,x_{n-2}) + g_{n-2}(x_3,\ldots,x_{n-2})\\
=&x_1\left(x_n f_n(x_2,\ldots,x_{n-1}) + f_{n-1}(x_2,\ldots,x_{n-2})\right)\\
+&\left(x_n f_{n-1}(x_3,\ldots,x_{n-1}) + f_{n-2}(x_3,\ldots,x_{n-2})\right)\\
=&x_1 f_{n+1}(x_2,\ldots,x_{n-1},x_n) + f_n(x_3,\ldots,x_{n-1},x_n)\\
+&x_1 g_{n+1}(x_2,\ldots,x_n) + g_n(x_3,\ldots,x_n) = g_{n+2}(x_1,\ldots,x_n).
\end{aligned}$$

Lemma 6. *If $x_i = x_{n+2-i}$ holds for every i $(1 \le i \le n+1)$ then*

$$f_{n+2}(x_1,\ldots,x_n) = f_{n+2}(x_2,\ldots,x_{n+1})$$

is also valid for every integer n $(n \ge -1)$.

Proof. This is evident for $-1 \le n \le 2$, because

$$f_1 = 0, f_2 = 1, f_3(x_1) = x_1 = x_2 = f_3(x_2)$$

and

$$f_4(x_1,x_2) = x_2x_1 + 1 = x_3x_2 + 1 = f_4(x_2,x_3) \text{ (since } x_1 = x_3).$$

Let $n > 2$. Assume that if $y_i = y_{n-i}$ holds for every i $(1 \le i \le n-1)$ then

$$f_n(y_1,\ldots,y_{n-2}) = f_n(y_2,\ldots,y_{n-1})$$

is also valid. Let $y_i = x_{i+1}$ for every i $(1 \le i \le n-1)$.

Then

$$y_i = x_{i+1} = x_{n+2-(i+1)} = x_{n-i+1} = y_{n-i}$$

and so

$$f_n(x_2,\ldots,x_{n-1}) = f_n(x_3,\ldots,x_n).$$

Using this equation, Lemma 5. and the relation $x_1 = x_{n+1}$ we obtain, that

$$\begin{aligned}
&f_{n+2}(x_1,\ldots,x_n)\\
=&g_{n+2}(x_1,\ldots,x_n) = x_1 g_{n+1}(x_2,\ldots,x_n) + g_n(x_3,\ldots,x_n)\\
=&x_{n+1} f_{n+1}(x_2,\ldots,x_n) + f_n(x_3,\ldots,x_n)\\
=&x_{n+1} f_{n+1}(x_2,\ldots,x_n) + f_n(x_2,\ldots,x_{n-1})\\
=&f_{n+2}(x_2,\ldots,x_{n+1})
\end{aligned}$$

which completes the proof of the lemma.

Proof of Lemma 1. It is well known [see in [6] p. 317] that in the representation of $\sqrt{D}$ as a simple conntinued fraction, the sequence $a_1, a_2, \ldots, a_{s-1}$ is symmetric, that is $a_i = a_{s-i}$, for every i $(1 \leq i \leq s-1)$ and

$$a_s = 2a_0. \tag{17}$$

If $\frac{h_n}{k_n}$ is the n^{th} convergent of $(a_1, a_2, \ldots) = (\overline{a_1, a_2, \ldots, a_s})$ then

$$h_{-1} = 1, \quad h_0 = a_1, \quad h_n = a_{n+1}h_{n-1} + h_{n-2}, \quad n \geq 1$$

and

$$k_{-1} = 0, \quad k_0 = 1, \quad k_n = a_{n+1}k_{n-1} + k_{n-2}, \quad n \geq 1.$$

Using this last definition and (10) by Lemma 6. we obtain, that

$$k_{s-2} = f_s(a_2, \ldots, a_{s-1}) = f_s(a_1, \ldots, a_{s-2}) = K_{s-2}.$$

It is known (and it is easy to see by induction for n) that

$$K_n = h_{n-1}, \quad n \geq 0 \tag{19}$$

and

$$H_n = a_0 h_{n-1} + k_{n-1}, \quad n \geq 0. \tag{20}$$

By (19), (12), (17), (18) and (20)

$$\begin{aligned} h_{s-1} + k_{s-2} &= K_s + k_{x-2} = a_s K_{s-1} + K_{s-2} + k_{s-2} \\ &= 2a_0 K_{s-1} + 2k_{s-2} = 2(a_0 h_{s-2} + k_{s-2}) = 2H_s. \end{aligned}$$

Using this equation we obtain (7) and (8) from (4) and (5) respectively. Thus the theorem is proved.

To proofs of the Theorem 1., Theorem 2., Theorem 3. and Theorem 4. we use the Lemma 4. and the representation of $\sqrt{D}$ as a simple continued fraction:

Lemma 7. *Let k be a rational integer. Then*

$$\sqrt{(2k+1)^2 - 4} = (2k, \overline{1, k-1, 2, k-1, 1, 4k}) \quad \text{for } k \geq 2. \tag{21}$$

$$\sqrt{(2k)^2 - 4} = (2k-1, \overline{1, k-2, 1, 4k-2}) \quad \text{for } k \geq 3, \tag{21}$$

$$\sqrt{k^2 - 1} = (k-1, \overline{1, 2k-2}) \quad \text{for } k \geq 2, \tag{23}$$

$$\sqrt{k^2 + 1} = (k, \overline{2k}) \quad \text{for } k \geq 1. \tag{24}$$

Proof. If $x = (\overline{1, k-1, 2, k-1, 1, 4k})$ then $x > 1$,

$$x = 1 + \cfrac{1}{k-1+\cfrac{1}{2+\cfrac{1}{k-1+\cfrac{1}{1+\cfrac{1}{4k+\cfrac{1}{x}}}}}}$$

and so

$$\left(\frac{1}{x}\right)^2 + 4k\frac{1}{x} - (4k-3) = 0$$

from which (using $\frac{1}{x} > 0$) we can see that

$$\sqrt{(2k+1)^2 - 4} = 2k + \frac{1}{x}$$

It is known that $\sqrt{D} = \sqrt{(2k+1)^2 - 4} = (a_0, \overline{a_1, \ldots, a_s})$ where $a_0 = \left[\sqrt{D}\right] = 2k$, and

$$\sqrt{D} = a_0 + \frac{1}{x}, \quad \text{where} \quad x = (\overline{a_1, \ldots, a_s}).$$

Every irrational number can be expessed in exactly one way as an infinite simple continued fraction. Thus the first part of the lemma is proved. The proof of other three parts is carried out analogously. We can see these formulae in [6] p. 321., too.

Proof of Theorem 1. We have only to apply the Lemma 4. and Lemma 7. By (22)

$$\sqrt{D} = \sqrt{(2k+1)^2 - 4} = (2k, \overline{1, k-1, 2, k-1, 1, 4k}), \quad k \geq 2$$

and so the representation of $\sqrt{D}$ as a simple continued fraction has a period consisting of $s = 6$ terms. This terms are

$$a_0 = 2k,\ a_1 = 1,\ a_2 = k-1,\ a_3 = 2,\ a_n = k-1,\ a_5 = 1,\ a_6 = 4k.$$

By the formulas (9), (10), (13) and (14) we can verify that

$$H_{6n+1} = \alpha^{3n+1} + \beta^{3n+1}, \qquad K_{6n+1} = \frac{\alpha^{3n+1} - \beta^{3n+1}}{\alpha - \beta},$$

$$H_{6n+2} = \frac{(\alpha-1)\alpha^{3n+1} + (\beta-1)\beta^{3n+1}}{2},$$

$$K_{6n+2} = \frac{(\alpha-1)\alpha^{3n+1} - (\beta-1)\beta^{3n+1}}{2(\alpha-\beta)},$$

$$H_{6n+3} = \alpha^{3n+2} + \beta^{3n+3}, \quad K_{6n+3} = \frac{\alpha^{3n+2} - \beta^{3n+2}}{\alpha - \beta},$$

$$H_{6n+4} = \frac{(\alpha-2)\alpha^{3n+2} + (\beta-2)\beta^{3n+2}}{2},$$

$$K_{6n+4} = (\frac{\alpha-2)\alpha^{3n+2} - (\beta-2)\beta^{3n+2}}{2(\alpha-\beta)},$$

for $n \geq 0$ and

$$H_{6n+5} = \frac{\alpha^{3n+3} + \beta^{3n+3}}{2}, \quad K_{6n+5} = \frac{\alpha^{3n+3} - \beta^{3n+3}}{2},$$

$$H_{6n+6} = \frac{(2\alpha-1)\alpha^{3n+3} + (2\beta-1)\beta^{3n+3}}{2},$$

$$K_{6n+6} = \frac{(2\alpha-1)\alpha^{3n+3} - (2\beta-1)\beta^{3n+3}}{2(\alpha-\beta)},$$

for $n \geq -1$. From these equations we obtain, that

$$H_{6n+r}^2 - DK_{6n+r}^2 = \left\{ \begin{array}{ll} 1, & \text{for } r = 5 \\ 4, & \text{for } r = 1 \text{ or } 3 \\ 1-2k, & \text{for } r = 2 \\ 3-4k, & \text{for } r = 4\ 6 \end{array} \right\} = (-1)^{\quad 1} c_{r+1}$$

for any $n \geq 0$. From (25) and (16) we can easily verify that the statements of Theorem 1. are valid.

The proofs of the Theorem 2., Theorem 3. and Theorem 4. are carried out analogously to the proof of the preceding theorem. For brevity we write only few formulas (without details) in this proofs.

Proof of Theorem 2.

$$\sqrt{D} = \sqrt{(2k)^2 - 4} = (2k-1, \overline{1, k-2, 1, k-2}), \text{ for } k \geq 3$$

$$H_{4n+1} = \alpha^{2n+1} + \beta^{2n+1}, \quad K_{4n+1} = \frac{\alpha^{2n+1} - \beta^{2n+1}}{\alpha - \beta},$$

$$H_{4n+2} = \frac{(\alpha-2)\alpha^{2n+1} + (\beta-2)\beta^{2n+1}}{2},$$
$$K_{4n+2} = \frac{(\alpha-2)\alpha^{2n+1} - (\beta-2)\beta^{2n+1}}{2(\alpha-\beta)},$$
$$H_{4n+3} = \frac{\alpha^{2n+2} + \beta^{2n+2}}{2}, \quad K_{4n+3} = \frac{\alpha^{2n+2} - \beta^{2n+2}}{2(\alpha-\beta)},$$

for $n \geq 0$ and

$$H_{4n+4} = \frac{(2\alpha-1)\alpha^{2n+2} + (2\beta-1)\beta^{2n+2}}{2},$$
$$K_{4n+4} = \frac{(2\alpha-1)\alpha^{2n+2} - (2\beta-1)\beta^{2n+2}}{2(\alpha-\beta)},$$

for $n \geq -1$ and

$$H_n^2 - DK_n^2 = \left\{ \begin{array}{ll} 1 & \text{for } r = 3 \\ 4, & \text{for } r = 1 \\ 5-4k, & \text{for } r = 2 \text{ or } 4 \end{array} \right\} = (-1)^{r-1} c_{r+1}, \ n \geq 0.$$

Proof of Theorem 3.

$$\sqrt{D} = \sqrt{k^2-1} = (k-1, \overline{1, 2k-2}), \quad \text{for } k \geq 2$$
$$H_{2n+1} = \frac{\alpha^{n+1} + \beta^{n+1}}{2}, \quad K_{2n+1} = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha-\beta},$$
$$H_{2n+2} = \frac{(\alpha-1)\alpha^{n+2} + (\beta-1)\beta^{n+2}}{2},$$
$$K_{2n+2} = \frac{(\alpha-1)\alpha^{n+2} - (\beta-1)\beta^{n+2}}{\alpha-\beta},$$

for $n \geq -1$ and

$$H_{2n+r} - DK_{2n+r}^2 = \left\{ \begin{array}{ll} 1, & \text{for } r = 1 \\ 2-2k, & \text{for } r = 0 \end{array} \right\} = (-1)^{r-1} c_{r+1}, \ n \geq 0.$$

Proof of Theorem 4.

$$\sqrt{D} = \sqrt{k^2+1} = (k, \overline{2k}), \text{ for } k \geq 1$$
$$H_n = \frac{\alpha^{n+1} + \beta^{n+1}}{2}, \quad K_n = \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha-\beta}$$

$$H_n^2 - DK_n^2 = (-1)^{n+1} = (-1)^{n-1}c_{n+1}, \text{ (that is } c_{n+1} = 1 \text{ for any } n).$$

References

[1] D. E. Ferguson, Letter to the editor, *Fibonacci Quart.*, **8** (1970), 88–89.

[2] V. E. Hogatt jr., and M. Bicknell-Johnson, A primer for the Fibonacci numbers XVII: Generalized Fibonacci numbers satisfying $U_{n+1}U_{n-1} - U_n^2 = \pm 1$, *Fibonacci Quart.*, **2** (1978), 130–137.

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

[4] K. Liptai, On a Diophantine problem, *Discuss. Math.*, (to appear).

[5] I. Niven, H. S. Zuckerman, *An introduction to the theory of numbers*, John Wiley and Sons, London · New York, 1960.

[6] W. Sierpinski, *Elementary Theory of Numbers*, PWN-Polish Scientific Publishers, Warszawa, 1987.

Béla Zay
Károly Eszterházy Teachers' Training College
Department of Mathematics
H–3301 Eger, Pf. 43
Hungary

Bounds for the zeros of Fibonacci-like polynomials

FERENC MÁTYÁS

Abstract. The Fibonacci-like polynomials $G_n(x)$ are defined by the recursive formula $G_n(x)=xG_{n-1}(x)+G_{n-2}(x)$ for $n\geq 2$, where $G_0(x)$ and $G_1(x)$ are given seed-polynomials. The notation $G_n(x)=G_n(G_0(x),G_1(x),x)$ is also used. In this paper we determine the location of the zeros of polynomials $G_n(a,x+b,x)$ and give some bounds for the absolute values of complex roots of these polynomials if $a,b\in\mathbf{R}$ and $a\neq 0$. Our result generalizes the result of P. E. RICCI who investigated this problem in the case $a=b=1$.

Introduction

Let $G_0(x)$ and $G_1(x)$ be polynomials with real coefficients. For any $n \in \mathbf{N} \setminus \{0,1\}$ the polynomial $G_n(x)$ is defined by the recurrence relation

$$G_n(x) = xG_{n-1}(x) + G_{n-2}(x) \tag{1}$$

and these polynomials are called Fibonacci-like polynomials. If it is necessary then the initial or seed polynomials $G_0(x)$ and $G_1(x)$ can also be detected and in this case we use the form $G_n(x) = G_n(G_0(x), G_1(x), x)$. Note that $G_n(0,1,1) = F_n$ where F_n is the n^{th} Fibonacci number.

In some earlier papers the Fibonacci-like polynomials and other polynomials, defined by similar recursions, were studied. G. A. MOORE [5] and H. PRODINGER [6] investigated the maximal real roots (zeros) of the polynomials $G_n(-1, x-1, x)$ $(n \geq 1)$. HONGQUAN YU, YI WANG and MINGFENG HE [2] studied the limit of maximal real roots of the polynomials $G_n(-a, x-a, x)$ if $a \in \mathbf{R}_+$ as n tends to infinity.

Under some restrictions in [3] we proved a necessary and sufficient condition for seed-polynomials when the set of the real roots of polynomials $G_n(G_0(x), G_1(x), x)$ $(n = 0, 1, 2, \ldots)$ has nonzero accumulation points. These accumulation points can be effectively determined. In [4], using this result, we proved the following

Theorem A. *If $a < 0$ or $2 < a$ then, apart from 0, the single accumulation point of the set of real roots of polynomials $G_n(a, x \pm a, x)$ $(n =$*

Research supported by the Hungarian OTKA Foundation, No. T 020295.

$1, 2, \ldots$) *is* $\pm\frac{a(2-a)}{a-1}$, *while in the case* $0 < a \leq 2$ *the above set has no nonzero accumulation point.*

According to Theorem A, apart from finitely many real roots, all of the real roots of polynomials $G_n(a, x \pm a, x)$ $(a \in \mathbf{R} \setminus \{0\}, n = 1, 2, \ldots)$ can be found in the open intervals

$$\left(\pm\frac{a(2-a)}{a-1} - \varepsilon, \pm\frac{a(2-a)}{a-1} + \varepsilon\right) \quad \text{or} \quad (-\varepsilon, \varepsilon),$$

where ε is an arbitrary positive real number.

Investigating the complex zeros of Fibonacci-like polynomials V. E. HOGATT, JR. and M. BICKNELL [1] proved that the roots of the equation $G_n(0, 1, x) = 0$ are $x_k = 2i\cos\frac{k\pi}{n}$ $(k = 1, 2, \ldots, n-1)$, i.e. apart from 0 if n is even, all of the roots are purely imaginary and their absolute values are less than 2. P. E. RICCI [7] among others studied the location of zeros of polynomials $G_n(1, x+1, x)$ and proved the following result.

Theorem B. *All of the complex zeros of polynomials* $G_n(1, x+1, x)$ $(n = 1, 2, \ldots)$ *are in or on the circle with midpoint* $(0, 0)$ *and radius 2 in the Gaussian plane.*

The purpose of this paper is to generalize the result of P. E. RICCI for the polynomials $G_n(a, x+b, x)$ where $a, b \in \mathbf{R}$ and $a \neq 0$, i.e. to give bounds for the absolute values of zeros. To prove our results we are going to use linear algebraic methods as it was applied by P. E. RICCI [7], too.

At the end of this part we list some terms of the polynomial sequence $G_n(x) = G_n(a, x+b, x)$ $(n = 2, 3, \ldots)$. We have

$$\begin{aligned}
G_2(x) &= x^2 + bx + a,\\
G_3(x) &= x^3 + bx^2 + (a+1)x + b,\\
G_4(x) &= x^4 + bx^3 + (a+2)x^2 + 2bx + a,\\
G_5(x) &= x^5 + bx^4 + (a+3)x^3 + 3bx^2 + (2a+1)x + b,\\
G_6(x) &= x^6 + bx^5 + (a+4)x^4 + 4bx^3 + (3a+3)x^2 + 3bx + a.
\end{aligned}$$

Known facts from linear algebra

To estimate the absolute values of zeros of polynomials $G_n(a, x+b, x)$ $(n \geq 1)$ we need the following notations and theorem. Let $\mathbf{A} = (a_{ij})$ be an $n \times n$ matrix with complex entries, λ_i $(i = 1, 2, \ldots, n)$ and $f(x)$ denote the eigenvalues and the charecteristic polynomial of $\mathbf{A}$, respectively. It is known that

$$f(\lambda_i) = 0 \tag{2}$$

and

$$\max |\lambda_i| \leq \|\mathbf{A}\|, \tag{3}$$

where $\|\mathbf{A}\|$ denotes a norm of the matrix $\mathbf{A}$. In this paper we apply the norms

$$\|\mathbf{A}\|_1 = n \max |a_{ij}| \tag{4}$$

and

$$\|\mathbf{A}\|_2 = \sqrt{\sum_{i,j} |a_{ij}|^2}. \tag{5}$$

Using the so called Gershgorin's theorem we can get a better estimation for the absolute values of the roots of $f(x) = 0$ and it gives the location of zeros of $f(x)$, too. Let us consider the sets C_i of complex numbers z defined by

$$C_i = \{z\colon\ |z - a_{ii}| \leq r_i\}, \tag{6}$$

where $i = 1, 2, \ldots, n$ and

$$r_i = \sum_{\substack{j=1 \\ j \neq i}}^{n} |a_{ij}| \quad (n \geq 2). \tag{7}$$

So C_i is the set of complex numbers z which are inside the circle or on the circle with midpoint a_{ii} and radius r_i in the complex plane. These sets (circles) are called to be Gershgorin-circles. Using these notations we formulate the following well-known theorem.

Gershgorin's theorem. *Let $n \geq 2$. For every i $(1 \leq i \leq n)$ there exists a j $(1 \leq j \leq n)$ such that*

$$\lambda_i \in C_j \tag{8}$$

and so

$$\{\lambda_1, \lambda_2, \ldots, \lambda_n\} \subset C_1 \cup C_2 \cup \cdots \cup C_n. \tag{9}$$

Theorems and the Main Result

Let us consider the $n \times n$ matrix

$$\mathbf{A}_n = \begin{pmatrix} -b & -ai & 0 & \cdots & 0 & 0 & 0 \\ -i & 0 & -i & \cdots & 0 & 0 & 0 \\ 0 & -i & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -i & 0 & -i \\ 0 & 0 & 0 & \cdots & 0 & -i & 0 \end{pmatrix},$$

where $b \in \mathbf{R}$ and $a \in \mathbf{R} \setminus \{0\}$.

Further on we prove the following

Theorem 1. *Let $n \geq 1$ and $a, b \in \mathbf{R}$ $(a \neq 0)$. The characteristic polynomial of matrix $\mathbf{A}_n$ is the polynomial $G_n(a, x+b, x)$.*

Let $n \geq 2$ and $a, b \in \mathbf{R}$ $(a \neq 0)$. If $\lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nn}$ denote the zeros of the polynomial $G_n(a, x+b, x)$ then, using the norms defined by (4) and (5) for the matrix $\mathbf{A}_n$, one can get the following estimations by (2),(3) and Theorem 1.

$$\max_{1 \leq i \leq n} |\lambda_{ni}| \leq n \max(|a|, |b|, 1) \tag{10}$$

and

$$\max_{1 \leq i \leq n} |\lambda_{ni}| \leq \sqrt{a^2 + b^2 + 2n - 3}. \tag{11}$$

From (10) and (11) it can be seen that these bounds depend on a, b and n but using the Gershgorin-circles we can get a more precise bound for $|\lambda_{ni}|$ and this bound depends only on a and b.

We shall prove

Theorem 2. *Let $n \geq 2$ and $a, b \in \mathbf{R}$ $(a \neq 0)$ and let us denote by K_1 the set $K_1 = \{z : |z+b| \leq |a|\}$ and by K_2 the set $K_2 = \{z : |z| \leq 2\}$ in the Gaussian plane. Then*

$$\lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nn} \in K_1 \cup K_2. \tag{12}$$

Now we are able to formulate our main result.

Main Result. *For any* $n \geq 1$ *and* $a, b \in \mathbf{R}$ $(a \neq 0)$ *if* $G_n(a, x+b, x) = 0$, *then*

$$|x| \leq \max(|a| + |b|, 2), \tag{13}$$

i.e. the absolute values of all zeros of all polynomial terms of polynomial sequence $G_n(a, x+b, x)$ $(n = 1, 2, 3, \ldots)$ *have a common upper bound, and by (13) this bound depends only on* a *and* b *in explicit way.*

We mention that Theorem B can be obtained as a special case ($a = b = 1$) of our Main Result.

Proofs

Proof of Theorem 1. It is known that the characteristic polynomial $f_n(x)$ of matrix $\mathbf{A}_n$ can be obtained by the determinant of matrix $x\mathbf{I}_n - \mathbf{A}_n$, where $\mathbf{I}_n$ is the $n \times n$ unit matrix. So

$$f_n(x) = \det(x\mathbf{I}_n - \mathbf{A}_n) = \det \begin{pmatrix} x+b & ai & 0 & \cdots & 0 & 0 & 0 \\ i & x & i & \cdots & 0 & 0 & 0 \\ 0 & i & x & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & i & x & i \\ 0 & 0 & 0 & \cdots & 0 & i & x \end{pmatrix}. \tag{14}$$

We prove the theorem by induction on n. It can be seen directly that $f_1(x) = x + b = G_1(a, x+b, x)$ and $f_2(x) = x^2 + bx + a = G_2(a, x+b, x)$. Let us suppose that $f_{n-2}(x) = G_{n-2}(a, x+b, x)$ and $f_{n-1}(x) = G_{n-1}(a, x+b, x)$ hold for an integer $n \geq 3$. Then developing (14) with respect to the last column and the resulting determinant with respect to the last row, we get

$$f_n(x) = xf_{n-1}(x) - iif_{n-2}(x) = xf_{n-1}(x) + f_{n-2}(x),$$

i.e. by our induction hipothesis

$$f_n(x) = xG_{n-1}(a, x+b, x) + G_{n-2}(a, x+b, x)$$

and so by (1)

$$f_n(x) = G_n(a, x+b, x)$$

holds for every integer $n \geq 1$.

Proof of the Theorem 2. From the matrix $\mathbf{A}_n$ we determine the so-called Gershgorin-circles. By the definition of $\mathbf{A}_n$ and (6) now there are only

two distinct Gershgorin-circles. The midpoints of these circles are $-b$ and 0 in the Gaussian plane, while by (7) their radii are $|a|$ and 2, respectively, i.e. they are the sets (circles) K_1 and K_2. (We omitted the circle with midpoint 0 and radius 1, because this circle is contained by one of the above circles.)

Since $G_n(a, x+b, x)$ is the characteristic polynomial of the matrix $\mathbf{A}_n$, and $\lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nn}$ are the zeros of it so from (8) and (9) we get that

$$\lambda_{n1}, \lambda_{n2}, \ldots, \lambda_{nn} \in K_1 \cup K_2.$$

This completes the proof.

Proof of the Main Result. We have seen in the proof of Theorem 2 that the Gershgorin-circles K_1 and K_2 don't depend on n if $n \geq 2$, therefore for any $n \geq 2$ the zeros of the polynomials $G_n(a, x+b, x)$ belong to the sets (circles) K_1 and K_2. I.e. if $G_n(a, x+b, x) = 0$ for a complex x, then

$$|x| \leq \max(|a| + |b|, 2). \tag{15}$$

Since $G_1(a, x+b, x) = 0$ if $x = -b$ therefore (15) also holds if $n = 1$. This completes our proof for every integer $n \geq 1$.

References

[1] V. E. Hoggat, Jr. and M. Bicknell, Roots of Fibonacci Polynomials, *The Fibonacci Quarterly* **11.3** (1973), 271–274.

[2] Hongquan Yu, Yi Wang and Mingfeng He, On the Limit of Generalized Golden Numbers, *The Fibonacci Quarterly* **34.4** (1996), 320–322.

[3] F. Mátyás, Real Roots of Fibonacci-like Polynomials, *Proceedings of Number Theory Conference, Eger* (1996) (to appear)

[4] F. Mátyás, The Asymptotic Behavior of Real Roots of Fibonacci-like Polynomials, *Acta Acad. Paed. Agriensis, Sec. Mat.*, **24** (1997), 55–61.

[5] G. A. Moore, The Limit of the Golden Numbers is 3/2, *The Fibonacci Quarterly* **32.3** (1994), 211–217.

[6] H. Prodinger, The Asymptotic Behavior of the Golden Numbers, *The Fibonacci Quarterly* **35.3** (1996), 224–225.

[7] P. E. Ricci, Generalized Lucas Polynomials and Fibonacci Polynomials, *Riv. Mat. Univ. Parma* (5) 4 (1995), 137–146.

Ferenc Mátyás
Károly Eszterházy Teachers' Training College
Department of Mathematics
H–3301 Eger, Pf. 43
Hungary
E-mail: matyas@ektf.hu

Representation of integers as terms of a linear recurrence with maximal index

JAMES P. JONES[1] and PÉTER KISS[2]

Abstract. For sequences $H_n(a,b)$ of positive integers, defined by $H_0=a$, $H_1=b$ and $H_n=H_{n-1}+H_{n-2}$, we investigate the problem: for a given positive integer N find positive integers a and b such that $N=H_n(a,b)$ and n is as large as possible. Denoting by $R(N)=r$ the largest integer, for which $N=H_r(a,b)$ for some a and b, we give bounds for $R(N)$ and a polynomial time algorithm for computing it. Some properties of $R(N)$ are also proved.

Introduction

Let $H_n(a,b)$ be a sequence of positive integers defined by $H_0 = a$, $H_1 = b$ and $H_n = H_{n-1} + H_{n-2}$ where a and b are arbitrary positive integers (the parameters). The sequence $H_n(a,b)$ occurs in a problem of COHN [1]: *Given a positive integer N, find positive integers a and b such that $N = H_n(a,b)$ and n is as large as possible.*

COHN [1] actually formulated the problem slightly differently, replacing 'n is as large as possible' by '$a+b$ is as small as possible'. However this makes little difference. We shall consider the problem as stated above.

Let $R = R(N)$ be the largest integer R such that $N = H_R(a,b)$ for some $a, b \geq 1$. The function R is well defined. For any $N \geq 1$, there exist integers a, b and n such that $N = H_n(a,b)$, $1 \leq a$, $1 \leq b$. Since $N = H_1(1,N)$, we can let $n = 1$, $a = 1$ and $b = N$. If $2 \leq N$, we can also let $a = 1$, $b = N-1$ and $n = 2$ so $N = H_2(1, N-1)$. Thus there always exist integers n, a and b such that $N = H_n(a,b)$, $1 \leq a$ and $1 \leq b$.

It is also easy to see that there exist a, b and r such that $N = H_r(a,b)$, $1 \leq a$, $1 \leq b$ and r is maximal. If $N = H_r(a,b)$, $1 \leq a$ and $1 \leq b$, then $r \leq H_r(a,b)$. Hence for all such r, a and b, $r \leq N$. Thus all possible values of r are bounded above by N. In fact this argument shows that $R(N) \leq N$ for all N.

[1] Research supported by National Science and Research Council of Canada Grant No. OGP 0004525.

[2] Research supported by Foundation for Hungarian Higher Education and Research and Hungarian OTKA Foundation Grant No. T 16975 and 020295.

The first few values of R are given by $R(1) = 1$, $R(2) = 2$, $R(3) = 3$, $R(4) = 3$, $R(5) = 4$, $R(6) = 3$, $R(7) = 4$, $R(8) = 5$, $R(9) = 4$, $R(10) = 4$, $R(11) = 5$, $R(12) = 4$ and $R(13) = 6$. Note that the function R is not increasing. That is, $N \leq M$ does not imply $R(N) \leq R(M)$.

Since $R(N)$ is well defined, Cohn's problem becomes one of giving an algorithm to compute $R(N)$. In this paper we shall give a simple algorithm which solves this problem. We shall also show that this algorithm is polynomial time, that is the time to find $R(N)$ is less than a polynomial in $\ln(N)$. We also prove some theorems about the number of N such that $R(N) = r$ and about the number of pairs (a, b) such that $H_r(a, b) = N$. First we need some lemmas.

1. Representation of N in the form $N = H_r(a, b)$ with r maximal

We use $\lfloor x \rfloor$ to denote the floor of x, (integer part of x). $\lceil x \rceil$ denotes the ceiling of x, $\lceil x \rceil = -\lfloor -x \rfloor$. F_n denotes the n^{th} Fibonacci number, where $F_0 = 0$, $F_1 = 1$ and $F_{i+2} = F_i + F_{i+1}$. L_n denotes the n^{th} Lucas number, defined by $L_0 = 2$, $L_1 = 1$ and $L_{i+2} = L_i + L_{i+1}$. We define $H_{-n}(a, b)$ by $H_{-n}(a, b) = (-1)^{n+1} H_n(-a, b - a)$.

Below we shall use many elementary identities and inequalities such as $L_{n+1} = 2F_n + F_{n+1}$, $L_n + 1 \leq F_{n+2}$ for $1 \leq n$ and $F_{n+1} < L_n$, for $2 \leq n$. We shall also need the following well known identity due to HORADAM [3].

Lemma 1.1. *For all integers n, a and b, $H_n(a, b) = aF_{n-1} + bF_n$.*

Proof. By induction on n using $F_{i+2} = F_i + F_{i+1}$. The result can also be seen to hold for negative n since $H_{-n}(a, b) = (-1)^n (aF_{n+1} - bF_n)$.

Lemma 1.2. $H_n(a, b) = H_n(a + F_n, b - F_{n-1})$ *and* $H_n(a, b) = H_n(a - F_n, b + F_{n-1})$.

Lemma 1.3. *For all integers n, k, a and b, we have*

(i) $\quad H_n(a, b) = H_{n-1}(b, a + b).$

(ii) $\quad H_n(a, b) = H_{n-k}(H_k(a, b), H_{k+1}(a, b)),$

(iii) $\quad H_n(a, b) = H_{n+1}(b - a, a).$

(iv) $\quad H_n(a, b) = H_{n+k}(H_{-k}(a, b), H_{1-k}(a, b)).$

Proof. They follow from the definitions.

Lemma 1.4. *If $N = H_r(a, b)$, $1 \leq a$, $1 \leq b$ and $R(N) = r$, then $b \leq a$.*

Proof. Suppose $R(n) = r$ and $N = H_r(a, b)$. If $a < b$, then by Lemma 1.3 we would have $N = H_r(a, b) = H_{r+1}(b - a, a)$ so that $r + 1 \leq R(N)$, contradicting $r = R(N)$.

Earlier we saw that $n = 1$ is realizable as a value of n such that $N = H_n(a,b)$ for $a \geq 1$, $b \geq 1$. In the next lemma we shall show that all values of $n \leq R(N)$ are realizable as values of n such that $N = H_n(a,b)$. We shall call this the Intermediate Value Lemma (IVL).

Lemma 1.5. (I.V.L.) *If $n \leq R(N)$, then there exist a, b such that $N = H_n(a,b)$, $1 \leq a$ and $1 \leq b$.*

Proof. Suppose $r = R(N)$ and $n \leq r$. There exist $a \geq 1$, $b \geq 1$ such that $N = H_r(a,b)$. Let $k = r - n$. Then $0 \leq k$. By Lemma 1.3 (ii), $N = H_r(a,b) = H_{r-k}(H_k(a,b), H_{k+1}(a,b)) = H_n(H_k(a,b), H_{k+1}(a,b))$ where $1 \leq H_k(a,b)$ and $1 \leq H_{k+1}(a,b)$, since $0 \leq k$ and $a, b \geq 1$.

Lemma 1.6. *If $n \geq 1$ then $R(F_{n+1}) = n$.*

Proof. Let $r = R(F_{n+1})$. Since $F_{n+1} = F_{n-1} + F_n = H_n(1,1), n \leq r$. Conversely, $F_{n+1} = H_r(a,b) = aF_{r-1} + bF_r \geq F_{r-1} + F_r = F_{r+1}$. Hence $n \geq r$. Therefore $n = r$.

Lemma 1.7. *If $n \geq 2$, then $R(L_{n+1}) = n + 1$.*

Proof. Here we need the inequality $L_{n+1} + 1 \leq F_{n+3}$. Let $r = R(L_{n+1})$. Since L_n may be defined by $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_n + L_{n+1}$, we have $L_n = H_n(2,1)$ and so $L_{n+1} = H_{n+1}(2,1)$. Hence $n+1 \leq r$. Conversely, $L_{n+1} = H_r(a,b) = aF_{r-1} + bF_r \geq F_{r-1} + F_r = F_{r+1}$. Hence $F_{r+1} \leq L_{n+1}$. Therefore $F_{r+1} + 1 \leq L_{n+1} + 1 \leq F_{n+3}$ and so $F_{r+1} < F_{n+3}$. Therefore $r + 1 < n + 3$. Hence $r < n + 2$. Therefore $r \leq n + 1$. So $r = n + 1$ and $R(L_{n+1}) = n + 1$.

Lemma 1.8. *If $N < F_{n+1}$, then $R(N) < n$.*

Proof. Let $R(N) = r$. Then there exist $a, b \geq 1$ such that $N = H_r(a,b)$. Hence we have $F_{n+1} > N = H_r(a,b) = aF_{r-1} + bF_r \geq F_{r-1} + F_r = F_{r+1}$. Thus $F_{n+1} > F_{r+1}$. Hence we have $n+1 > r+1$ so that $n > r$. In otherwords $n > R(N)$.

Corollary 1.9. *If $1 \leq n$ and $N \leq F_{n+1}F_{n+2}$, then $R(N) \leq 2n$.*

Proof. If $1 \leq n$, then $F_{n+2} < L_{n+1}$. Hence $F_{n+1}F_{n+2} < F_{n+1}L_{n+1} = F_{2n+2}$. Therefore $N < F_{2n+2}$. Hence by Lemma 1.8, $R(N) < 2n + 1$. Therefore $R(N) \leq 2n$.

Lemma 1.10. *Let A be an arbitrary positive integer and suppose $0 \leq n$. Then*

(i) $\quad n = R(AF_{n+1})$ *if* $A \leq F_n$,

(ii) $\quad n < R(AF_{n+1})$ *if* $F_n < A$.

Proof. $AF_{n+1} = A(F_{n-1} + F_n) = AF_{n-1} + AF_n = H_n(A, A)$ implies $n \leq R(AF_{n+1})$. For (i) suppose $A \leq F_n$ and $n+1 \leq R(AF_{n+1})$. By the Intermediate Value Lemma there exist $c \geq 1$ and $d \geq 1$ such that $AF_{n+1} = cF_n + dF_{n+1}$. Then $F_{n+1} \mid cF_n$ and $(F_n, F_{n+1}) = 1$ imply $F_{n+1} \mid c$. Hence $F_{n+1} \leq c$ so that $d = 0$. Hence $R(AF_{n+1}) = n$. For (ii) suppose $F_n < A$. Then there exist b and t such that $A = tF_n + b$, $1 \leq b$ and $1 \leq t$. Let $a = tF_{n+1}$. Then $AF_{n+1} = (tF_{n+1})F_n + bF_{n+1} = H_{n+1}(tF_{n+1}b) = H_{n+1}(a, b)$, $1 \leq a$ and $1 \leq b$. Hence $n+1 \leq R(AF_{n+1})$ so that $n < R(AF_{n+1})$.

Corollary 1.10. *For all* $n \geq 0$, $R(F_nF_{n+1}) = n$.

Lemma 1.11. *If* $F_nF_{n+1} < N$, *then* $n < R(N)$.

Proof. Suppose $F_nF_{n+1} < N$. We shall show that $n+1 \leq R(N)$ by finding a and b such that $N = H_{n+1}(a, b) = aF_n + bF_{n+1}$, $1 \leq a$ and $1 \leq b$. Let b be the least positive solution to the congruence $N \equiv bF_{n+1} \pmod{F_n}$, (taking $b = F_n$, if $F_n \mid N$, so that $b \geq 1$). We claim

$$bF_{n+1} + F_n \leq N. \tag{1.12}$$

This inequality (1.12) will be proved by considering two cases:

Case 1. $N \equiv 0 \pmod{F_n}$. Then $b = F_n$. Since $F_n \mid N$ and $F_nF_{n+1} < N$, we have $F_n(F_{n+1} + 1) \leq N$. So we have $F_{n+1}b + F_n = F_{n+1}F_n + F_n = F_n(F_{n+1} + 1) \leq N$, and so (1.12) holds.

Case 2. $N \not\equiv 0 \pmod{F_n}$. Then $1 \leq b < F_n$, so $b \leq F_n - 1$. Therefore $bF_{n+1} + F_n \leq (F_n - 1)F_{n+1} + F_n = F_nF_{n+1} + (F_n - F_{n+1}) \leq F_nF_{n+1} < N$ and so again (1.12) holds.

Now that (1.12) is established, let $a = (N - bF_{n+1})/F_n$. Then a is an integer, $N = aF_n + bF_{n+1} = H_{n+1}(a, b)$ and (1.12), implies $1 \leq a$.

Corollary 1.13. *If* $1 < n$ *and* $F_{2n} \leq N$, *then* $n < R(N)$.

Proof. By Lemma 1.11. If $1 < n$, then $F_{n+1} < L_n$ and $F_nF_{n+1} < F_nL_n = F_{2n} \leq N$.

Lemma 1.14. *If* $1 \leq N$, *then* $R(N) \leq (\lfloor 1 + 2.128 \cdot \ln(N) \rfloor)$.

Proof. Let $r = R(N)$. The inequality holds for $N = 1$, since $R(1) = 1$. Suppose $N \geq 2$. Then $2 \leq r$. Let $k = r + 1$. Then $3 \leq k$ so that we can use the inequality

$$(8/5)^{k-2} < F_k \qquad (3 \leq k). \tag{1.15}$$

(This inequality, which is well known, is easy to prove by induction on $k \geq 3$, using the fact that if $x = 8/5$, then $x^2 < x + 1$). Using the inequality

with $k = r + 1$, by Lemma 1.8 we get $(8/5)^{r-1} < F_{r+1} \leq N$. Taking logs of both sides we have $(r-1)\ln(8/5) \leq \ln(N)$. Hence we have $r - 1 \leq \ln(N)/\ln(8/5) < \ln(N)/(47/100) < \ln(N) \cdot 2.128$, proving the lemma.

Lemma 1.16. *If* $1 \leq N$, *then* $\lceil 1.5 + .893 \cdot \ln(N) \rceil \leq R(N)$.

Proof. Let $r = R(N)$. Lemma 1.11 implies $N \leq F_r F_{r+1}$. If $N \leq 6$, the inequality can be checked by cases. Suppose $7 \leq N$. Then $4 \leq r$. We will use the following elementary inequality which is easy to prove using the fact that $x^2 > x + 1$ for $x = 7/4$.

$$F_k < (7/4)^{k-2} \qquad (3 < k). \tag{1.17}$$

Using the inequality twice, with $k = r$ and $k = r + 1$, we get

$$N \leq F_r F_{r+1} < (7/4)^{r-2}(7/4)^{r-1} = (7/4)^{2r-3}. \tag{1.18}$$

Taking logs of both sides, $\ln(N) < (2r-3)\ln(7/4)$. Hence $\ln(N)/\ln(7/4) < 2(r - 1.5)$. Therefore $2^{-1} \cdot \ln(N)/\ln(7/4) < r - 1.5$. Consequently $1.5 + 2^{-1} \cdot \ln(N)/\ln(7/4) < r$. Hence $\lceil 1.5 + 2^{-1} \cdot \ln(N)/\ln(7/4) \rceil \leq r$. Therefore $\lceil 1.5 + .893 \cdot \ln(N) \rceil \leq r$.

Corollary 1.19. *For* $N \geq 1$,

$$\lceil 1.5 + .893 \cdot \ln(N) \rceil \leq R(N) \leq \lfloor 1 + 2.128 \cdot \ln(N) \rfloor.$$

Proof. By Lemma 1.14 and Lemma 1.15.

Corollary 1.20. *If* $R(N) = r$, *then* $F_{r+1} \leq N \leq F_r F_{r+1}$.

Proof. Suppose $R(N) = r$. By Lemma 1.8, $F_{r+1} \leq N$. By Lemma 1.11, $N \leq F_r F_{r+1}$.

The equation $N = H_r(a, b)$ sometimes has two solutions (a, b) in positive integers with $r = R(N)$. E.g. if $N = 6$, then $R(6) = 3$, $6 = H_3(2, 2)$ and $6 = H_3(4, 1)$.

Definition 1.21. N is called a *double number* if there exist $a, b, c, d \geq 1$ such that $N = H_r(a, b) = H_r(c, d), a \neq c$ or $b \neq d$, (equivalently if $a \neq c$ and $b \neq d$), where $r = R(N)$. If N is not a double number, then N is called a *single number*.

Examples 1.22. Some representations of N in the form $N = H_r(a, b)$ with $R = R(N)$:

$N = 1$,	$R = 1$,	$a = 1$,	$b = 1$,
$N = 10$,	$R = 4$,	$a = 2$,	$b = 2$,

$N = 100,$	$R = 7,$	$a = 6,$	$b = 4,$
$N = 1,000,$	$R = 12,$	$a = 8,$	$b = 2,$
$N = 10,000,$	$R = 12,$	$a = 80,$	$b = 20,$
$N = 100,000,$	$R = 14,$	$a = 269,$	$b = 99,$
$N = 1,000,000,$	$R = 19,$	$a = 154,$	$b = 144,$
$N = 10,000,000,$	$R = 19,$	$a = 1540,$	$b = 1440,$
$N = 100,000,000,$	$R = 23,$	$a = 5143,$	$b = 311,$
$N = 1,000,000,000,$	$R = 23,$	$a = 51430,$	$b = 3110.$

$N = 1,000,000,000$ happens to be an example of a double number. For we have $N = H_r(c,d)$ also for $c = 22773$ and $d = 20821$, besides $a = 51430$ and $b = 3110$. Other examples of double numbers are $15 = H_4(6,1) = H_4(3,3)$ and $32 = H_5(9,1) = H_5(4,4)$.

In the next section we shall prove that the equation $N = H_r(a,b)$ never has three solutions (a,b) in positive integers with $r = R(N)$. (Of course it may have other solutions when $r < R(N)$. E.g. for $N = 6$ and $r = 3$ we have $6 = H_2(1,5) = H_2(2,4) = H_2(3,3)$ where $2 < r$.) Thus there is no concept of a triple number.

2. An algorithm for $R(N)$

In this section we shall show that there exists an algorithm for computing $R(N)$. In fact we shall prove that there is a polynomial-time algorithm for computing $R(N)$. We give a procedure which finds, given N, the value of $R(N)$ and also a and b. Since the number of steps in the procedure will be less then a polynomial in $\ln(N)$, the number of bit operations needed to compute $R(N)$ will be less than a polynomial in $\ln(N)$.

Suppose N is given. To compute $R(N)$, begin with any sufficiently large value of r, satisfying $r \geq R(N)$. For example by Corollary 1.19 we can take $r = \lfloor 1 + 2.128 \cdot \ln(N) \rfloor$. Then proceed as follows.

Step 1: Find a positive solution b to the congruence

$$N \equiv bF_r \pmod{F_{r-1}}, \qquad (1 \leq b). \tag{2.1}$$

This congruence is solvable in natural numbers since $(F_r, F_{r-1}) = 1$. Hence there is a solution b in the range $1 \leq b \leq F_{r-1}$. Take the least such b in this range.

Step 2: Check whether

$$bF_r < N. \tag{2.2}$$

If this is the case, put $a = (N - bF_r)/F_{r-1}$. Then a is an integer by (2.1). Also we have $N = aF_{r-1} + bF_r$ and condition (2.2) implies $1 \leq a$. In this

case the algorithm terminates and $R(N) = r$. If (2.2) does not hold, then we decrease r by 1 and return to Step 1. We iterate steps 1 and 2, decreasing r until (2.2) holds. Since initially $R(N) \leq \lfloor 1 + 2.128 \cdot \ln(N) \rfloor \leq r$, the algorithm must terminate after at most $\lfloor 1 + 2.128 \cdot \ln(N) \rfloor$ iterations.

We claim that this computation is polynomial time. Certainly the number of operations needed at each step is less than or equal to a polynomial in $\ln(N)$. Calculation of F_r requires time exponential in $\ln(r)$, i.e. proportional to a polynomial in r. However r is less than or equal to a polynomial in $\ln(N)$, since $F_r \leq N$. So this is polynomial time.

In addition to finding r, the algorithm also finds (a, b) such that $H_r(a, b) = N$. The pair (a, b) is not uniquely dependent upon N. There is sometimes a second pair (c, d) such that $H_r(c, d) = N$. As sketched above the algorithm finds the pair (a, b) with least b. It can easily be extended also to find the second pair (c, d), when that exists. After (a, b) has been found, let $d = b + F_{r-1}$ and $c = a - F_r$. Then $N = H_r(c, d)$ by Lemma 1.2. d is positive. If $dF_r < N$, then c will also be positive and (c, d) will be a second pair. If not, then there is no second pair, i.e. N is a single.

The algorithm can be simplified to yield a more explicit formula for $r = R(N)$ and explicit formulas for a, b, c and d. For this we shall use an old identity of LUCAS [4]:

$$F_{r-1}^2 - F_{r-2} \cdot F_r = (-1)^r. \tag{2.3}$$

Multiplying both sides of (2.3) by $(-1)^r N$ and rearranging terms we get

$$(-1)^r F_{r-1} N \cdot F_{r-1} - (-1)^r F_{r-2} N \cdot F_r = N. \tag{2.4}$$

Equation (2.4) provides a solution to the linear diophantine equation $aF_{r-1} + bF_r = N$. It shows that $AF_{r-1} + BF_r = N$ will hold if we put $A = A_r(N)$ and $B = B_r(N)$, where

$$A_r(N) = (-1)^r F_{r-1} N \quad \text{and} \quad B_r(N) = -(-1)^r F_{r-2} N. \tag{2.5}$$

Thus $a = A_r(N)$ and $b = B_r(N)$ is a particular solution of the equation $aF_{r-1} + bF_r = N$. Since $(F_r, F_{r+1}) = 1$, from a particular solution we may obtain all solutions (a, b) by

$$a = A_r(N) - tF_r, \quad b = B_r(N) + tF_{r-1}, \quad (t = 0, \pm 1, \pm 2, \pm 3, \ldots). \tag{2.6}$$

Then by Lemma 1.1 $H_r(a, b) = N$ for all integers t. Now define $g_r(N)$ and $h_r(N)$ by

$$g_r(N) = \frac{(-1)^r F_{r-2} N + 1}{F_{r-1}} \tag{2.7}$$

and

$$h_r(N) = \frac{(-1)^r F_{r-1} N - 1}{F_r}. \tag{2.8}$$

Then $g_r(N)$ and $h_r(N)$ are reals. For a and b as in (2.6), we have $1 \leq a$ iff $t \leq h_r(N)$ and $1 \leq b$ iff $g_r(N) \leq t$. Hence (a, b) is a positive solution of $aF_{r-1} + bF_r = N$ iff

$$g_r(N) \leq t \leq h_r(N). \tag{2.9}$$

Since t is integer valued, condition (2.9) is equivalent to

$$g_r(N) \leq \lceil g_r(N) \rceil \leq t \leq \lfloor h_r(N) \rfloor \leq h_r(N). \tag{2.10}$$

Condition (2.9) is in turn equivalent to $\lceil g_r(N) \rceil \leq h_r(N)$ and also to $g_r(N) \leq \lfloor h_r(N) \rfloor$.

From (2.3), (2.7) and (2.8), it is easy to see that

$$h_r(N) - g_r(N) = \frac{N - F_{r+1}}{F_{r-1} F_r}. \tag{2.11}$$

The functions $g_r(N)$ and $h_r(N)$ give us a new algorithm to compute $R(N)$. We have

Theorem 2.12. *Suppose $N > 1$. Then $R(N)$ is the largest integer $r > 1$ such that*

$$\left\lceil \frac{(-1)^r F_{r-2} N + 1}{F_{r-1}} \right\rceil \leq \left\lfloor \frac{(-1)^r F_{r-1} N - 1}{F_r} \right\rfloor. \tag{2.12}$$

Furthermore, the set of $r > 1$ satisfying (2.12) is the set $\{2, 3, \ldots, R(N)\}$. Hence (2.12) can be used as an algorithm to calculate $R(N)$.

Proof. By Lemma 1.8, if $r \leq R(N)$, then $F_{r+1} < N$ and hence by (2.11), $g_r(N) \leq h_r(N)$. Thus

$$r \leq R(N) \Rightarrow g_r(N) \leq h_r(N). \tag{2.13}$$

By (2.9) and the IVL, for all $r \leq R(N)$, there exist $t\,(g_r(N) \leq t \leq h_r(N))$, and this implies $\lceil g_r(N) \rceil \leq \lfloor h_r(N) \rfloor$. On the other hand, by (2.9), when $R(N) < r$, there is no integer t such that $g_r(N) \leq t \leq h_r(N)$ and so we have not $\lceil g_r(N) \rceil \leq \lfloor h_r(N) \rfloor$.

This shows that the set of $r > 1$ satisfying (2.12) is an interval.

This approach to $R(N)$, thru $g_r(N)$ and $h_r(N)$, also gives a new algorithm to decide whether N is a single or a double. From (2.9) and (2.10) we have

(2.14) N is a single iff $\lceil g_r(N) \rceil = \lfloor h_r(N) \rfloor$.

Also

(2.15) N is a double iff $\lceil g_r(N) \rceil < \lfloor h_r(N) \rfloor$.

From (2.5), (2.6), (2.7) and (2.8) we can obtain explicit formulas for a, b, c and d:

(2.16) $a = A_r(N) - \lceil g_r(N) \rceil F_r$ and $b = B_r(N) + \lceil g_r(N) \rceil F_{r-1}$,

(2.17) $c = A_r(N) - \lfloor h_r(N) \rfloor F_r$ and $d = B_r(N) + \lfloor h_r(N) \rfloor F_{r-1}$.

If N is a single, $c = a$ and $d = b$. If N is a double, $c = a - F_r$ and $d = b + F_{r-1}$. Thus when $r = R(N)$, formulas (2.16) and (2.17) can be used as definitions of a, b, c and d. The ratio on the right side of (2.11) is not always less than 2 however, even when $r = R(N)$. In this case, when $r = R(N)$, we have only the weak inequality

$$R(N) \leq r \Longrightarrow \frac{N - F_{r+1}}{F_{r-1} F_r} < \alpha + 1. \tag{2.18}$$

Here $\alpha = (1 + \sqrt{5})/2 = 1.61803\ldots$ so that $\alpha + 1 = 2.61803\ldots$. The idea of the proof is the following: From Lemma 1.11 we see that $R(N) \leq r$ implies $N \leq F_r F_{r+1}$. Then $(F_r F_{r+1} - F_{r-1}) F_{r-1} F_r < \alpha + 1$ can be shown using $F_r^2 < \alpha F_1 F_{r-1} + F_{r+1}$.

Next we shall prove that there are no triples. The following lemmas will be used.

Lemma 2.19. *If* $1 < r$, *then* $F_r F_{r+1} < (1 + 2F_{r+1}) F_{r-1} + F_r$.

Proof. If $1 < r$, then $F_r < 1 + 2F_{r-1}$. Hence

$$\begin{aligned} F_r F_{r+1} &< (1 + 2F_{r-1}) F_{r+1} = F_{r+1} + 2F_{r-1} \cdot F_{r+1} \\ &= F_{r-1} + 2F_{r-1} \cdot F_{r+1} + F_r = (1 + 2F_{r+1}) F_{r-1} + F_r. \end{aligned}$$

Lemma 2.20. *Suppose* $1 < N$, $N = H_r(a, b)$, $R(N) = r$ *and* $1 \leq b$. *Then* $a \leq 2F_r$.

Proof. Let $r = R(N)$ and $N = H_r(a, b)$. Since $1 < N$ and $r = R(N)$, we have $1 < r$. We claim

$$a < b + 2F_{r+1}. \tag{2.21}$$

If not, then $b + 2F_{r+1} \leq a$. Since $1 \leq b$ and $N = H_r(a,b)$, by Lemma 2.19 and Lemma 1.11 we have

$$N = aF_{r-1} + bF_r \geq (b+2F_{r+1})F_{r-1} + bF_r \geq (1+2F_{r+1})F_{r-1} + F_r > F_rF_{r+1}.$$

But this contradicts Lemma 1.11 which says that $N \leq F_rF_{r+1}$, since $r = R(N)$. Hence (2.21) holds. Now it is easy to see that

$$N = aF_{r-1} + bF_r = (b + 2F_{r+1} - a)F_r + (a - 2F_r)F_{r+1}.$$

Supposing $2F_r < a$ and using (2.21), we get the contradiction $R(N) \geq r+1$. So $a \leq 2F_r$.

Theorem 2.22. *If $R(N) = r$, then the equation $N = H_r(a,b)$ has at most two solutions in positive integers a, b. There are no triples.*

Proof. Suppose the equation $N = H_r(a,b)$ has three solutions in positive integers, say $(a,b), (c,d)$ and a third solution (x,y). Then $c = a - F_r$, $d = b + F_{r-1}$, $x = a - 2F_r$ and $y = b + 2F_{r-1}$. But by Lemma 2.20, $a \leq 2F_r$. Hence $x \leq 0$, a contradiction.

From Theorem 2.22, if $r = R(N)$, then $\lfloor h_r(N) \rfloor \leq \lceil g_r(N) \rceil + 1$. And so in (2.15), when $\lceil g_r(N) \rceil < \lfloor h_r(N) \rfloor$, we have $\lceil g_r(N) \rceil + 1 = \lfloor h_r(N) \rfloor$.

Following F_nF_{n+1} there is a very long interval consisting entirely of singlels.

Suppose $R(N) = r$. Recall from Corollary 1.20 that if $R(N) = r$, then N must lie in the interval $F_{r+1} \leq N \leq F_rF_{r+1}$. We can show that most N in this interval are singles.

Theorem 2.23. *If $F_nF_{n+1} < N < F_nF_{n+1} + F_n^2 + F_{n+2}$, then N is a single.*

We won't prove this result, (Theorem 2.23.). However it will be clear how to do so after we have proved Lemma 3.1 in the next section.

Taking a limit as $n \to \infty$, one finds that the interval $[F_nF_{n+1}, F_nF_{n+1} + F_n^2 + F_{n+2}]$ occupies some 38% of the interval $[F_nF_{n+1}, F_{n+1}F_{n+2}]$. $(\beta^2 = \left((1-\sqrt{5})/2\right)^2 = (-.61803)^2 = .381966\ldots)$ Thus on average more than 28% of N are singles. Actually, in the next section, we shall prove that 92.7% of N are singles.

3. The number of N such that $R(N) = r$

In this section we consider the problem of the number of N such that $R(N) = r$. Here r is a fixed positive integer. The number of such N must

be finite. By Lemma 1.11, the number of such N must be less than or equal to F_rF_{r+1}. We shall give an exact formula for this number. First we need some lemmas.

Lemma 3.1. *Suppose $R(N) = r$ and a, b, c, d are as defined in (2.16) and (2.17). Then $N = H_r(a, b) = H_r(c, d)$. If N is a single, then $c = a, d = b$,*

$$(i) \qquad 1 \leq b \leq a \leq F_r \quad \text{and} \quad 1 \leq b \leq F_{r-1}.$$

If N is a double, then we have $c = a - F_r$, $d = b + F_{r-1}$, $b \leq a$,

$$(ii) \qquad F_{r-1} < d \leq c \leq F_r, \qquad F_{r+1} < a \leq 2F_r \quad \text{and} \quad 1 \leq b \leq F_{r-2}.$$

Proof. Suppose a, b, c and d are as above and $N > 1$. Let $r = R(N)$. Then $N = H_r(a, b) = H_r(c, d)$. Suppose first N is a single. By (2.16) and (2.17), $c = a, d = b$, $1 \leq a$ and $1 \leq b$. By Lemma 1.2, $N = H_r(a, b) = H_r(a + F_r, b - F_{r-1})$. Hence $b \leq F_{r-1}$, else N would be a double. By Lemma 1.4, $b \leq a$. By Lemma 1.2 we know $N = H_r(a, b) = H_r(a - F_r, b + F_{r-1})$. Hence $a \leq F_r$, else N would be a double. Therefore (i) holds.

Next suppose N is a double. Then by (2.15), (2.16) and (2.17), $c = a - F_r$, $d = b + F_{r-1}$, $1 \leq a, b, c, d$. By Lemma 2.20, $a \leq 2F_r$. Since $c = a - F_r$, this implies $c \leq F_r$. By Lemma 1.4, since $N = H_r(c, d)$, $d \leq c$. Hence $d \leq F_r$. Since $d \leq F_r$ and $d = b + F_{r-1}$, $b + F_{r-1} \leq F_r$, so that $b \leq F_r - F_{r-1} = F_{r-2}$, i.e. $b \leq F_{r-2}$. Since $0 < b$ and $d = b + F_{r-1}$, $F_{r-1} < d$. Since $F_{r-1} < d$ and $d \leq c$, $F_{r-1} < c$. Since $a = c + F_r$, this implies that $F_{r+1} < a$. Hence statement (ii) holds.

Lemma 3.2. *If $R(N) = r$, then there exist unique positive integers x and y satisfying*

$$(3.2) \qquad N = H_r(x, y) \quad \text{and} \quad 1 \leq y \leq x \leq F_r.$$

Proof. By Lemma 3.1. If N is a single, then we can let $x = a$ and $y = b$. If N is a double, then we can let $x = c$ and $y = d$ and we will have $\leq y \leq x \leq F_r$. x and y are unique by Theorem 2.22, to the effect that $N = H_r(x, y)$ has at most two solutions. Every N is either a single or a double. Note that if N is a double, then $x = a$ and $y = b$ won't satisfy $1 \leq y \leq x \leq F_r$ since $F_{r+1} < a$.

Lemma 3.3. *Suppose $R(N) = r$. Then all solutions (x, y) of $N = H_r(x, y)$ in positive integers satisfy either*

$$(3.3.1) \qquad 1 \leq y \leq x \leq F_r$$

or

(3.3.2) $$F_{r+1} < x \leq 2F_r, \quad 1 \leq y \leq F_{r-2} \quad \text{and} \quad y \leq x.$$

But not both.

Proof. By Theorem 2.22, N is either a double or a single. Hence there are only two cases to consider. If N is a single, then $(x, y) = (a, b)$ and condition (3.3.1) holds by Lemma 3.1. (i). If N is a double, then $(x, y) = (a, b)$ or $(x, y) = (c, d)$. In the first case, by Lemma 3.1 (ii) (3.3.2) holds. In the sceond case, by Lemma 3.1 (ii) (3.3.1) holds.

Lemma 3.4. *Suppose $R(N) = r$. Then all solutions of $N = H_r(x, y)$ in positive integers (x, y) satisfy the conditions $x \leq 2F_r$ and $y \leq F_r$.*

Proof. By Lemma 3.3, either (3.3.1) holds or (3.3.2) holds. (3.3.1) implies $x \leq F_r \leq 2F_r$ and $y \leq F_r$. (3.3.2) implies $x \leq 2F_r$ and $y \leq F_{r-2} \leq F_r$. Hence $x \leq 2F_r$ and $y \leq F_r$.

Lemma 3.5. *If $0 < k$, then for all positive integers a and b,*

$$0 < H_k(a, b) < H_{k+1}(a, b).$$

Proof. From the definition it follows that $H_n(a, b)$ is a strictly increasing sequence of positive integers.

Theorem 3.6. *There exist integers x and y such that*

(3.6) $$N = H_n(x, y) \quad \text{and} \quad 1 \leq y \leq x \leq F_n$$

iff $n = R(N)$. Furthermore x and y are unique.

Proof. To prove the first part of the theorem suppose $R(N) = n$. Then by Lemma 3.2 there exist unique integers x and y suct that $N = H_n(x, y)$ and $1 \leq y \leq x \leq F_n$, i.e. (3.6). To prove the second part suppose x and y are integers satisfying (3.6). Then $n > 0$. Let $R(N) = r$. Then $n \leq r$. Let $k = r - n$. By definition of $R(N)$ there are positive integers a and b such that $N = H_r(a, b)$. By Lemma 1.3 (ii), since $n = r - k$, we have $N = H_r(a, b) = H_n(H_k(a, b), H_{k+1}(a, b))$ so that $N = H_n(H_k(a, b), H_{k+1}(a, b))$.

Thus $x = H_k(a, b)$ and $y = H_{k+1}(a, b)$ are particular solutions to the linear diophantine equation $N = xF_{n-1} + yF_n$. Since $(F_n, F_{n+1}) = 1$, all solutions to the equation are given by

$$x = H_k(a, b) - tF_n \quad \text{and} \quad y = H_{k+1}(a, b) + tF_{n-1},$$

where t is an integer. Since $y \leq x$, we have for some t the inequality $H_{k+1}(a, b) + tF_{n-1} \leq H_k(a, b) - tF_n$. This implies

$$t \leq (H_k(a, b) - H_{k+1}(a, b))/F_{n+1},$$

so that

$$t \leq H_k(a,b) - H_{k+1}(a,b).$$

Since $x \leq F_n$, we also have the inequality $H_k(a,b) - tF_n \leq F_n$, which implies

$$H_k(a,b)/F_n \leq t+1.$$

If $0 < k$, then by Lemma 3.5 we have $t < 0$ and $0 < t+1$ so that $-1 < t < 0$. This is a contradiction since t is an integer. Hence $k = 0$. Thus $r = n$ and hence $R(N) = n$.

Remark. Condition (3.6) cannot be replaced by the weaker condition $N = H_n(x,y)$ and $1 \leq y \leq x$, This condition is not strong enough to imply $n = R(N)$. For example if $N = 96$, then $R(N) = 6$ but $N = H_5(17,9)$ and $9 \leq 17$. Also $N = H_5(12,12)$ and $12 \leq 12$.

Theorem 3.7. *Let r be fixed nonnegative integer. Then the number of N such that $R(N) = r$ is exactly*

$$\frac{F_r(F_r+1)}{2}.$$

Proof. Let r be fixed nonnegative integer. We will use Theorem 3.6 to count the number of N such that $R(N) = r$. We will count pairs (x,y) such that $1 \leq y \leq x \leq F_r$. For each such pair, we put $N = H_r(x,y)$. For each N there is only one pair (x,y) satisfying $N = H_r(x,y)$ and $1 \leq y \leq x \leq F_r$, by Theorem 2.6. How many pairs (x,y) are there such that $1 \leq x \leq F_r$? For each such x, there are x choices of y such that $1 \leq y \leq x$. Hence the number of N such that $R(N) = r$ is given by the sum

$$\sum_{x=1}^{F_r} x = \frac{F_r(F_r+1)}{2}.$$

Example 3.7. The number of N such that $R(N) = 5$ is $F_5(F_5+1)/2 = 5 \cdot 6/2 = 15$. By Corollary 1.20, these 15 N all lie in the interval $8 = F_6 \leq N \leq F_5F_6 = 40$. They are the 15 values $N = 8, 11, 14, 16, 17, 19, 20, 22, 24, 25, 27, 30, 32, 35$ and 40.

4. Double numbers

In this section we first prove that there are infinitely many double numbers. Then we give a combinatorial formula for the number of double numbers N having a fixed value of R. Last we give an asymptotic estimate for the number of double numbers up to F_nF_{n+1}.

Lemma 4.1. *For all $n > 2$, F_nF_{n+1} is a double number.*

Proof. Suppose $2 < n$. Recall that by Corollary 1.10, $R(F_nF_{n+1}) = n$. We have $F_nF_{n+1} = F_n(F_{n-1} + F_n) = F_nF_{n-1} + F_nF_n = H_n(F_n, F_n)$. On the other hand,

$$\begin{aligned} F_nF_{n+1} &= (F_n + F_n)F_{n-1} + (F_n - F_{n-1})F_n \\ &= H_n(2F_n, F_n - F_{n-1}) = H_n(2F_n, F_{n-2}). \end{aligned}$$

$0 < F_{n-2}$ since $n > 2$. The two representations of F_nF_{n+1} are distinct since $F_n \neq F_{n-2}$.

Lemma 4.2. *For $n > 4$, if $N = F_n(F_{n+1} - 1)$, then $R(N) = n$ and N is a double number.*

Proof. By an argument similar to that in the proof of Lemma 4.1 it is easy to see that

$$N = H_n(F_n, F_n - 1) = H_n(2F_n, F_{n-2} - 1). \tag{4.2}$$

To prove that $R(N) = n$ we will use the IVL. Obviously $n \leq R(N)$. Suppose that $n + 1 \leq R(n)$. Then by the IVL there exist $a \geq 1$ and $b \geq 1$ such that $N = H_{n+1}(a, b)$. Hence $F_n(F_{n+1} - 1) = aF_n + bF_{n+1}$. Then $F_n \mid b$, since $(F_n, F_{n+1}) = 1$. Let $b = eF_n$, where $1 \leq e$. Then we have $a + (e-1)F_{n+1} < 0$, a contradiction. Thus $R(N) = n$.

We give next a formula for the number of double numbers N with a fixed R value r. For this it is necessary first to characterise double numbers. From section 2 we have the following result.

Lemma 4.3. *Suppose $R(N) = r$. Then N is a double number iff*

$$\left\lceil \frac{(-1)^r F_{r-2}N + 1}{F_{r-1}} + 1 \right\rceil = \left\lfloor \frac{(-1)^r F_{r-1}N - 1}{F_r} \right\rfloor.$$

Proof. See the remark following Theorem 2.22 that N is a double iff $\lceil g_r(N) \rceil + 1 = \lfloor h_r(N) \rfloor$.

Theorem 4.4. *N is a double number and $R(N) = r$ iff there exist unique positive integers x and y such that*

$$N = H_r(x, y) \quad \text{and} \quad F_{r-1} < y \leq x \leq F_r. \tag{4.4}$$

Proof. For the proof of one part of the theorem, suppose N is a double number and $R(N) = r$. By Lemma 3.1, there exist positive integers c and

d such that $N = H_r(c,d)$ and $F_{r-1} < d \leq c \leq F_r$. Let $x = c$ and $y = d$. Then (4.4) holds. Also since the condition $F_{r-1} < y \leq x \leq F_r$ implies $1 < y \leq x \leq F_r$, x and y are unique by Lemma 3.1. For the proof of the second part, suppose (4.4) for some positive integers x and y. Then since $1 \leq r$, $1 \leq y \leq x \leq F_r$. Hence $R(N) = r$ by Theorem 3.6. N cannot be a single since in that case, by Lemma 3.1, we would have $x = a, y = b$ and $b \leq F_{r-1}$. Hence N is a double.

Note that if (x,y) satisfies $F_{r-1} < y \leq x \leq F_r$, then $(x + F_r, y - F_{r-1})$ satisfies $F_{r+1} < x \leq 2F_r$ and $1 \leq y \leq F_{r-2}$. Also if (x,y) satisfies $F_{r+1} < x \leq 2F_r$ and $1 \leq y \leq F_{r-2}$, then $(x - F_r, y + F_{r-1})$ satisfies $F_{r-1} < y \leq x \leq F_r$. So one could also prove a version of Theorem 4.4, with condition (4.4) replaced by

$$N = H_r(x,y), \quad F_{r+1} < x \leq 2F_r \quad \text{and} \quad 1 \leq y \leq F_{r-2}.$$

Theorem 4.5. *Let $r \geq 3$. The number of N such that N is a double number and $R(N) = r$ is exactly*

$$\frac{F_{r-2}(F_{r-2}+1)}{2}.$$

Proof. Suppose r is a fixed positive integer. To count the number of double numbers N such that $R(N) = r$ we will use representation (4.4) of Theorem 4.4. We can determine the number of double numbers N such that $R(N) = r$ by counting pairs of integers (x,y) such that $F_{r-1} < y \leq x \leq F_r$. For each such pair (x,y) we can let $N = H_r(x,y)$ since N depends uniquely on (x,y). How many pairs of integers (x,y) are there such that $F_{r-1} < y \leq x \leq F_r$? Since $F_r - F_{r-1} = F_{r-2}$, there are F_{r-2}, there are F_{r-2} choices for x such that $F_{r-1} < x \leq F_r$. For each choice of x, there are x choices for y such that $F_{r-1} < y \leq x$. Therefore the numbers N such that $R(N) = r$ is given by the sum

$$\sum_{x=1}^{F_{r-2}} x = \frac{F_{r-2}(F_{r-2}+1)}{2}.$$

Example. The number of N such that N is a double and $R(N) = 6$ is $F_4(F_4+1)/2 = 3 \cdot 4/2 = 6$. By Corollary 1.20 and Theorem 2.23 with $n = 5$ these N lie in the interval $18 = 5 \cdot 8 + 5^2 + 13 = F_5F_6 + F_5^2 + F_1 \leq N \leq F_6F_7 = 8 \cdot 13 = 104$. They are $N = 78, 83, 88, 91, 96$ and 104.

Lemma 4.6. *For all double numbers N, $N \leq F_nF_{n+1}$ iff $R(N) \leq n$.*

Proof. The first part of the lemma is the contrapositive of Lemma 1.11, if $R(N) \leq n$ then $N \leq F_nF_{n+1}$. For the proof of the second part

suppose N is a double and $N \leq F_n F_{n+1}$. Let $r = R(N)$. We will that $r \leq n$. Suppose not. Suppose $n < r$. Let $N = H_r(a, b)$ where a are as in (2.16). By Lemma 3.1 (ii), since N is a double, $F_{r+1} < a$. $N = H_r(a, b) = aF_{r-1} + bF_r \geq F_{r+1}F_{r-1} + F_r > F_{n+2}F_n \geq F_n$ · contradicting $N \leq F_n F_{n+1}$. Therefore $r \leq n$.

Theorem 4.7. *For $n \geq 1$, the number of double numbers $N \leq F_r$ is equal to*

$$\frac{F_{n-1}F_{n-2} + F_n - 1}{2}.$$

Proof. By Lemma 4.6 and Theorem 4.5, the number of double nu $N \leq F_n F_{n+1}$ is

$$\sum_{r=3}^{n} \frac{F_{r-2}(F_{r-2}+1)}{2} = \frac{1}{2}\sum_{r=3}^{n}(F_{r-2}^2 + F_{r-2})$$

$$= \frac{1}{2}\left(\sum_{i=1}^{n-2} F_i^2 + \sum_{i=1}^{n-2} F_i\right) = \frac{1}{2}(F_{n-2}F_{n-1} + F_n - 1).$$

What proportion of integers N are double numbers? We shall sho on average approximately 7.3% of numbers are doubles. We shall sho by proving that for n sufficiently large, approximately $\beta^4/2$ of the nu N up to $F_n F_{n+1}$ are doubles. Here $\beta = (1 - \sqrt{5})/2 = -61803\ldots$ s $\beta^4/2 = .072949016\ldots$.

Theorem 4.8. *The probability that N is a double number is a totic to $\beta^4/2$.*

Proof. Let $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. Then $\alpha\beta$ = It is known that F_n is asymptotic to $\alpha^n/\sqrt{5}$, i.e. that $\lim F_n/\alpha^n \approx$ By Lemma 4.6 and Theorem 4.7, the number of double numbers N $F_n F_{n+1}$, divided by the number of N up to $F_n F_{n+1}$ is equal to

$$(F_{n-1}F_{n-2} + F_n - 1)/2F_nF_{n+1} \approx F_{n-1}F_{n-2}/2F_nF_{n+1}$$

$$\approx \left((\alpha^{n-1}/\sqrt{5})(\alpha^{n-2}/\sqrt{5})\right) / \left(2(\alpha^n/\sqrt{5})(\alpha^{n+1}/\sqrt{5})\right)$$

$$= \alpha^{n-1}\alpha^{n-2}/2\alpha^n\alpha^{n+1} = 1/2\alpha^4 = \beta^4/2.$$

References

[1] J. H. E. COHN., Recurrent sequences including N, *Fibonacci Quarterly*, **29** (1991), 30–36.

[2] A. F. HORADAM, Generalized Fibonacci sequences, *Amer. Math. Monthly* **68** (1961), 455–459.

[3] A. F. HORADAM, Basic properties of a certain generalized sequence of numbers, *Fibonacci Quarately* **3** (1965), 161–176.

[4] E. LUCAS, Theorie des fonctions numériques simplement périodiques, *American Journal of Mathematics,* vol. 1 (1878), 184–240, 289–321. English translation: *Fibonacci Association,* Santa Clara University, 1969.

JAMES P. JONES
DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF CALGARY
CALGARY, ALBERTA T2N 1N4
CANADA

PÉTER KISS
KÁROLY ESZTERHÁZY TEACHERS' TRAINING COLLEGE
DEPARTMENT OF MATHEMATICS
LEÁNYKA U. 4.
3301 EGER, PF. 43.
HUNGARY
E-mail: kissp@ektf.hu

A sieve for all primes of the form $x^2+(x+1)^2$

PANAYIOTIS G. TSANGARIS

Abstract: All composite numbers of the form $x^2+(x+1)^2$ are determined in terms of suitable (non-homogeneous) linear recurrence sequences of order 2 (Theorem 4.12). As a consequence, all primes of the same form in a given interval can be determined by a sieving procedure (Theorem 4.13).

Introduction

The object of this study are the prime and composite numbers of the form $x^2+(x+1)^2$. Their study depends heavily on the following

Theorem 1.1. (SIERPINSKI) [3]) *The number $x^2+(x+1)^2$ is composite if and only if there exist natural numbers y, z such that:*

$$(T) \qquad T(x) = T(y) + T(z).$$

(Here $T(x), T(y), T(z)$ denote triangular numbers.)

The description of all composite numbers of the form $x^2+(x+1)^2$ is reduced to the study of the integral solutions of the following family of Diophantine equations of Fermat-Pell type:

$$(F_k) \qquad X^2 - 2Y^2 = 2k^2 - 1, \quad k = 0, 1, 2, \ldots.$$

Thus the study of equation (T) is reduced to the study of the family of equations (F_k) in terms of Gauss type transformations.

The detailed study of all solutions of (F_k) is carried on via Nagell's method of equivalence classes, thus avoiding any reference to fundamental units.

We will consider the Diophantine equation

$$(1.1) \qquad \xi^2 - d\eta^2 = -1 \quad (d \neq \square)$$

where $d \neq \square$ (non-square) is a natural number. The sequence of non-negative (that is $\xi_{2n+1} \geq 0$ and $\eta_{2n+1} \geq 0$) integral solutions of (1.1) is determined by the following recursive formulae:

$$(1.2) \qquad \begin{aligned} \xi_{2n+3} &= 2x_1\xi_{2n+1} - \xi_{2n-1}, \text{ where } \xi_1 = \xi_1 \text{ and } \xi_3 = \xi_1^3 + 3d\xi_1\eta_1^2 \\ \eta_{2n+3} &= 2x_1\eta_{2n+1} - \eta_{2n-1}, \text{ where } \eta_1 = \eta_1 \text{ and } \eta_3 = 3\xi_1^2\eta_1 + d\eta_1^3, \end{aligned}$$

$(n = 1, 2, \ldots)$ where $\xi_1 + \eta_1\sqrt{d}$ is the fundamental solution of (1.1) and $x_1 + y_1\sqrt{d}$ is the fundamental solution of

$$(P) \qquad x^2 - dy^2 = 1 \quad (d \neq \square).$$

The following Theorems can be found in [5] (cf. also [4]).

Theorem 1.2. *Consider the Diophantine equation*

$$(F) \qquad X^2 - dY^2 = C. \quad (d \neq \square,\ C > 0).$$

Let $X_r^* + Y_r^*\sqrt{d}$ be the fundamental solution of a class A_r of integral solutions of (F) with $X_r^* > 0$ Let $x_n + y_n\sqrt{d}$, where $n = 0, 1, \ldots$, be the sequence of all non-negative integral solutions of (P). Let

$$X_n + Y_n\sqrt{d} \equiv (X_r^* + Y_r^*\sqrt{d})(x_n + y_n\sqrt{d}) \text{ for all } n = 0, 1, \ldots,$$
$$X_n^{'} + Y_n^{'}\sqrt{d} \equiv (X_r^* - Y_r^*\sqrt{d})(x_n + y_n\sqrt{d}) \text{ for all } n = 1, 2, \ldots$$

(for a typical r).

Then the following hold true:

(i) $Y_{n+1} > Y_n \geq 0$ *for every* $n = 0, 1, \ldots$.

(ii) Let $Y_r^* > 0$. *Then* $Y_{n+1}^{'} \geq Y_n > Y_n^{'} > 0$ *for every* $n = 1, 2, \ldots$.

(iii) Let $Y_r^* = 0$. *Then* $Y_n = Y_n^{'}$ *for every* $n = 0, 1, \ldots$.

(iv) Let A_r be genuine (= non-ambiguous). Then

$$Y_{n+1}^{'} > Y_n > Y_n^{'} > 0 \text{ for all } n = 1, 2, \ldots.$$

(v) Let A_r be ambiguous. Then for every m there exist n such that:

$$X_m^{'} = X_n \text{ and } Y_m^{'} = Y_n.$$

(vi) Let $X_r^* + Y_r^*\sqrt{d}$, where $r = 1, 2, \ldots, m$, be the only integral solutions of (F) such that

$$0 < X_r^* \leq \sqrt{(x_1 + 1)C/2} \text{ and } 0 \leq Y_r^* \leq y_1\sqrt{C}/\sqrt{2(x_1 + 1)}.$$

Then the set of all non-negative integral solutions of (F) consists of all pairs (X_n, Y_n) together with all pairs $(X_n^{'}, Y_n^{'})$ for all respective genuine classes A_r in addition to all pairs (X_n, Y_n) for all respective ambiguous classes

B_r. Moreover, $X_n, Y_n, X_n^{'}$ and $Y_n^{'}$ are determined by the following recursive formulae:

$$\begin{aligned} X_{n+1} &= 2x_1X_n - X_{n-1} \text{ for } n = 1,2,\ldots \\ \text{with } X_0 &= X_r^*,\ X_1 = x_1X_r^* + dy_1Y_r^* \text{ and } r = 1,2,\ldots,m. \\ Y_{n+1} &= 2x_1Y_n - Y_{n-1} \text{ for } n = 1,2,\ldots \\ \text{with } Y_0 &= Y_r^*,\ Y_1 = y_1X_r^* + x_1Y_r^* \text{ and } r = 1,2,\ldots,m. \end{aligned} \tag{1.3}$$

$$\begin{aligned} X_{n+1}^{'} &= 2x_1X_n^{'} - X_{n-1}^{'} \text{ for } n = 1,2,\ldots \\ \text{with } X_0^{'} &= X_r^*,\ X_1^{'} = x_1X_r^* - dy_1Y_r^* \text{ and } r = 1,2,\ldots,m. \\ Y_{n+1}^{'} &= 2x_1Y_n^{'} - Y_{n-1}^{'} \text{ for } n = 1,2,\ldots \\ \text{with } Y_0^{'} &= -Y_r^*,\ Y_1^{'} = y_1X_r^* - x_1Y_r^* \text{ and } r = 1,2,\ldots,m. \end{aligned} \tag{1.4}$$

Theorem 1.3. *Consider the Diophantine equation (F), $C \neq 0$. Let $X_r^* + Y_r^*\sqrt{d}$ be the fundamental solution of a class A_r of integral solutions of (F). Let $x_1 + y_1\sqrt{d}$ be the fundamental solutions of (P) and*

$$\begin{aligned} X_n + Y_n\sqrt{d} &\equiv (X_r^* + Y_r^*\sqrt{d})(x_1 + y_1\sqrt{d})^n \equiv (X_r^* + Y_r^*\sqrt{d})(x_n + y_n\sqrt{d}), \\ X_n^{'} + Y_n^{'}\sqrt{d} &\equiv (X_r^* - Y_r^*\sqrt{d})(x_1 + y_1\sqrt{d})^n \quad \text{for all } n = 0,1,\ldots. \end{aligned}$$

Let $R_n \equiv Y_n^2 + k^2$ and $R_n^{'} \equiv Y_n^{'2} + k^2$, where k is a fixed integer. Then the numbers R_n and $R_n^{'}$ are determined by the following recursive formulae:

$$R_{n+1} = 2x_2R_n - R_{n-1} - 2k^2(x_2 - 1) + 2y_1^2C,$$

where $R_0 = Y_r^{*2} + k^2$ and $R_1 = (y_1X_r^* + x_1Y_r^*)^2 + k^2$.

$$R_{n+1}^{'} = 2x_2R_n^{'} - R_{n-1}^{'} - 2k^2(x_2 - 1) + 2y_1^2C,$$

where $R_0^{'} = Y_r^{*2} + k^2$ and $R_1^{'} = (y_1X_r^* - x_1Y_r^*)^2 + k^2$.

2. Reduction of the Diophantine equation $x(x+1) = y(y+1) + z(z+1)$ to a family of Fermat equations

Theorem 2.1 below aims at reducing the problem of solving the Diophantine equation

$$x(x+1) = y(y+1) + z(z+1) \tag{E}$$

to that of solving each one of the Diophantine equations (F_k).

Theorem 1.3. *Consider the Diophantine equations* (E) *and* (F_k). *Then the following hold true:*

$(i)_1$ *Let* (x, y, z) *be an integral solution of* (E) *with* $y \geq z$. *Let*

$$X \equiv 2x + 1 \text{ and } Y \equiv 2y - (k-1), \text{ where } k \equiv y - z.$$

Then $X + Y\sqrt{2}$ *is an integral solution of* (F_k).

$(i)_2$ *If* $y \neq 0, -1$ *and* $z \neq 0, -1$ *then* $|Y| \neq k \pm 1$.

$(ii)_1$ *Let* $X + Y\sqrt{2}$ *be an integral solution of* (F_k). *Let*

$$x = (X-1)/2, \; y = (Y + k - 1)/2 \text{ and } z = (Y - k - 1)/2. \tag{2.1}$$

Then (x, y, z) *is an integral solution of* (E).

$(ii)_2$ *If* $|Y| \neq k \pm 1$, *then* $y \neq 0, -1$ *and* $z \neq 0, -1$.

Proof. $(i)_1$ By direct computation.

$(i)_2$ Clear because $|Y| = k \pm 1$ implies $(y = 0, -1)$ or $(z = 0, -1)$.

$(ii)_1$ Let $X + Y\sqrt{2}$ be an integral solution of (F_k). Then it is easily proved by parity considerations that the numbers (2.1) are integers. Also

$$X = 2x + 1, \; Y = 2y - (k-1) \text{ and } k = y - z,$$

whence (F_k) implies

$$(2x+1)^2 - 2(2y - (y - z - 1))^2 = 2(y-z)^2 - 1,$$

that is

$$x(x+1) = y(y+1) + z(z+1).$$

$(ii)_2$ Is proved in a way similar to the proof of $(i)_2$, namely $(y = 0, -1)$ or $(z = 0, -1)$ imply $|Y| = k \pm 1$.

Note. The transformation leading from (E) to (F_k) emanate from GAUSS (Art. 216 in [1])

3. Determination of all integral solutions of the equation $X^2 - 2Y^2 = 2k^2 - 1$, where $k = 0, 1, \ldots$

Proposition 3.1 is crucial for the location of the fundamental solutions of (F_k). Further, Theorem 3.4 characterizes the classes of solutions of (F_k), (as regards genuiness or ambiguity) in terms of their representing fundamental solutions. Special attention is given to the case of $2k^2 - 1$ being a square

number (cf. Theorem 3.5). The set of all non-negative solutions of (F_k) is determined recursively by Theorem 3.6 together with Corollary 3.7.

Proposition 3.1. *Consider the Diophantine equation (F_k) where k is a natural number. Let $X^*+Y^*\sqrt{2}$ be a solution of (F_k). Then $X^*+Y^*\sqrt{2}$ is the fundamental solution of a class of integral solutions of (F_k) if and only if the following (equivalent) inequalities are satisfied:*

$$0 < |X^*| \leq 2k-1, \tag{3.1}$$

$$0 \leq Y^* \leq k-1. \tag{3.2}$$

Proof. By using Theorem 109 in [2].

Note. The fundamental solution of (F_0) is $X^* + Y^*\sqrt{2} = 1 + \sqrt{2}$.

Proposition 3.2. *Let k be a natural number. Then $2k-1+(k-1)\sqrt{2}$ is the fundamental solution of a class of integral solutions of (F_k).*

Proof. Evident by Proposition 3.1.

Proposition 3.3. *Let A be a class of integral solutions of the Diophantine equation (F), $C \neq 0$. Let $X + Y\sqrt{d}$ be a representative of A and*

$$L = (-X^2 - dY^2)/C \quad \text{and} \quad M = -2XY/C.$$

Then the following hold true:

(i) A is a genuine if and only if at least one of the numbers L, M is not integral.

(ii) A is ambiguous if and only if both numbers L and M are integral.

Proof. Immediate by using Nagell's criterion (p. 205, [2]).

Theorem 3.4. *Let $X^* + Y^*\sqrt{2}$ be the fundamental solution of a class A of integral solutions of (F_k), where $k = 1, 2, \ldots$. Then the following hold true:*

(i) A is genuine if and only if $Y^* > 0$.

(ii) A is ambiguous if and only if $Y^* = 0$.

Proof. (i) (a) If A is genuine, then the previous Proposition 3.3 easily implies $Y^* > 0$.

(b) Let now $Y^* > 0$ and assume that A is ambiguous. Then, by the same Proposition, the numbers

$$L = (-X^{*2} - 2Y^{*2})/(2k^2-1) \quad \text{and} \quad M = -2X^*Y^*/(2k^2-1)$$

are integers. In particular, because L is an integer it follows that

$$(2k^2 - 1) \mid X^{*^2} + 2Y^{*^2} = 4Y^{*^2} + 2k^2 - 1.$$

Thus

$$(2k^2 - 1) \mid 4Y^{*^2}.$$

Also, $Y^* \leq \sqrt{(2k^2 - 1)/2}$, i.e.

$$4Y^{*^2} < 2(2k^2 - 1).$$

Hence

$$2k^2 - 1 < 4Y^{*^2} = h(2k^2 - 1) < 2(2k^2 - 1),$$

where h is a natural number. Hence $1 < h < 2$, which is impossible. Hence A is genuine.

(ii) Immediate by (i).

Note: (F_0) has only one class of integral solutions, which is ambiguous.

Theorem 3.5. *Let k be a natural number. Then the following are equivalent:*

(i) $2k^2 - 1$ *is a square number.*

(ii) The totality of ambiguous classes of integral solutions of (F_k) *consists of a single class.*

In consequence, if $2k^2 - 1$ *is not a square number, then every class of integral solutions of* (F_k) *is genuine.*

Proof. By using Proposition 3.1 and Theorem 3.4.

Theorem 3.6. *Consider the Diophantine equation (F_k), where k is a natural number. Let $x_n + y_n\sqrt{2}$, where $n = 0, 1, 2, \ldots$, be the sequence of all non-negative integral solutions of*

$$x^2 - 2y^2 = 1.$$

Let $X_r^* + Y_r^*\sqrt{2}$, (where $r = 1, 2, \ldots, m$), be the only integral solutions of (F_k) such that:

$$0 < X_r^* \leq 2k - 1 \quad \text{and} \quad 0 \leq Y_r^* \leq k - 1.$$

Let

$$X_n + Y_n\sqrt{2} \equiv (X_r^* + Y_r^*\sqrt{2})(x_n + y_n\sqrt{2}) \text{ for all } n = 0, 1, \ldots,$$
$$X_n^{'} + Y_n^{'}\sqrt{2} \equiv (X_r^* - Y_r^*\sqrt{2})(x_n + y_n\sqrt{2}) \text{ for all } n = 1, 2, \ldots,$$

(for a typical r). Then the following hold true:

(i) Let $Y_r^* > 0$ and $k \geq 2$. (Case of genuine classes of integral solutions of (F_k)). Then the pairs (X_n, Y_n) and (X_n', Y_n') are determined by (1.3) and (1.4) (for $x_1 = 3$, $y_1 = 2$ and $d = 2$).

(ii) Let $Y_r^* = 0$. (Case of ambiguous classes). Then the pairs (X_n, Y_n) are determined by (1.3).

Moreover, in case (i) all pairs (X_n, Y_n) together with all pairs (X_n', Y_n') constitute the set of all non-negative integral solutions of (F_k) which belong to the class with typical fundamental solution $X_r^* + Y_r^*\sqrt{2}$. Also, in case (ii) all pairs (X_n, Y_n) constitute the set of all non-negative integral solutions of (F_k) which belong to the class with typical fundamental solution $X_r^* + 0\sqrt{2}$.

Proof. By using Theorems 3.4, 3.5, 1.2(vi) and Proposition 3.1.

Corollary 3.7. *The sequence of all positive integral solutions (X_n, Y_n) of (F_0) is determined by (1.2) (for $X_n \equiv \xi_{2n+1}, Y_n \equiv \eta_{2n+1}, \xi_1 = 1, \xi_3 = 7, \eta_1 = 1$ and $\eta_3 = 5$).*

4. Determination of all prime and composite numbers of the form $x^2 + (x+1)^2$.

In Theorem 4.2 it is shown that every positive (integral) solution of (T) leads to a non-negative solution of a certain (F_k) and vice-versa. Theorems 4.6, 4.7 together with Corollary 4.8 determine all (F_k) whose non-negative solutions (taken together) lead to all positive solutions of (T).

In Theorem 1.1 a primality criterion is given for numbers of the form $N(x) = x^2+(x+1)^2$. Composite numbers of the form $N(x)$ are characterized (in terms of a suitable solution of (F_k)) in Theorem 4.9. The recursive determination of all composite numbers of the form $N(x)$ is given by Theorems 4.10, 4.11 and 4.12. This leads to our final Theorem 4.13, which constitutes an algorithm (sieve) for the determination of all primes of the form $N(x)$.

Lemma 4.1. *Let $X + Y\sqrt{2}$ be a non-negative integral solution of (F_k). Let*

$$x \equiv (X-1)/2, \quad y \equiv (Y+k-1)/2 \quad \text{and} \quad z \equiv (Y-k-1)/2.$$

Then x, y, z are natural numbers if and only if $Y > k+1$.

Proof. Easy and so omitted.

Theorem 4.2. *Consider the Diophantine equations (F_k) and (T). Then the following hold true:*

(i) Let $X + Y\sqrt{2}$ be a (non-negative) integral solution of (F_k), with $Y > k + 1$. Let

$$x \equiv (X - 1)/2, \ y \equiv (Y + k - 1)/2 \ \text{ and } \ z \equiv (Y - k - 1)/2.$$

Then (x, y, z) is a triad of positive integral solutions of (T).

(ii) Let (x, y, z) be a triad of positive integral solutions of (T) with $y \geq z$. Let

$$k \equiv y - z, \ X \equiv 2x + 1 \ \text{ and } \ Y \equiv 2y - (k - 1).$$

Then $X + Y\sqrt{2}$ is a (non-negative) integral solution of (F_k) with $Y > k + 1$.

Proof. By using Theorem 2.1, Lemma 4.1 and the fact that the Diophantine equation (T) is equivalent to the equation (E).

Proposition 4.3. *Let k be a natural number. Let $X + Y\sqrt{2}$ be a non-negative integral solution of (F_k). Then the following hold true:*

(i) Let $0 \leq Y \leq k - 1$. Then $X + Y\sqrt{2}$ is a fundamental solution of a class of integral solutions of (F_k).

(ii) $Y \neq k$.

(iii) Let $Y = k + 1$. Then $X = 2k + 1$. Moreover, $X + Y\sqrt{2} = (2k + 1) + (k + 1)\sqrt{2}$ is obtained from the fundamental solution $(X^* = 2k - 1, Y^* = k - 1)$ as follows:

$$X + Y\sqrt{2} = (2k - 1 + (k - 1)\sqrt{2})(3 + 2\sqrt{2}) \text{ for } k = 1 \text{ and}$$
$$X + Y\sqrt{2} = (2k - 1 - (k - 1)\sqrt{2})(3 + 2\sqrt{2}) \text{ for } k > 1.$$

Proof. By direct computations.

Proposition 4.4. *Consider the Diophantine equation (F_k), where $k > 1$. Let $X^* + Y^*\sqrt{2}$ be the fundamental solution of a class A of (F_k) with $X^* > 0$. Let $3 + 2\sqrt{2}$ be the fundamental solution of the equation*

$$x^2 - 2y^2 = 1.$$

Let

$$Z_n \equiv X_n + Y_n\sqrt{2} \equiv (X^* + Y^*\sqrt{2})(3 + 2\sqrt{2})^n \text{ for all } n = 0, 1, \ldots, \text{ and}$$
$$Z_n' \equiv X_n' + Y_n'\sqrt{2} \equiv (X^* - Y^*\sqrt{2})(3 + 2\sqrt{2})^n \text{ for all } n = 1, 2, \ldots.$$

Then the following hold true:

(i) Let A be genuine. Then the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k) which belong to A or to $\overline{A}$ and satisfy the inequality $Y > k + 1$ are the following:

(a) $Z_n \in A$ *and* $Z_n^{'} \in \overline{A}$ *for all* $n \geq 1$ *if and only if* $Y^* < k-1$.

(b) $Z_n \in A$ *for all* $n \geq 1$ *and* $Z_n^{'} \in \overline{A}$ *for all* $n \geq 2$ *if and only if* $Y^* = k-1$.

(ii) Let A be ambiguous, (whence $Y^* = 0$, while $2k^2-1$ is a square number). Then the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k) which belong to A and satisfy the inequality $Y > k+1$ are all Z_n for every $n \geq 1$.

Proof. (i) By Theorem 1.2 (iv) we have:

$$Y_{n+1}^{'} > Y_n > Y_n^{'} > 0 \quad \text{for all } n \geq 1, \text{ where } Y_1^{'} = 2X^* - 3Y^*.$$

(a) Hence, we have $Y_1^{'} = 2X^* - 3Y^* > k+1$ if and only if $(2X^*)^2 > (3Y^* + k + 1)^2$, that is if and only if $(Y^* - (k-1))(Y^* + 7k + 5) < 0$, and so if and only if $Y^* < k-1$.

Consequently, by Proposition 4.3, the only (non-negative) integral solution $X + Y\sqrt{2}$ of (F_k), which belong to A or $\overline{A}$ and satisfy the inequality $Y > k+1$ are all $Z_n \in A$ and all $Z_n^{'} \in \overline{A}$, $n = 1, 2, \ldots$, for which $Y^* < k-1$.

(b) Hence, $Y_1^{'} = 2X^* - 3Y^* = k+1$ if and only if $Y^* = k-1$.

Thus, the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k), which belong to A or $\overline{A}$ and satisfy the inequality $Y > k+1$ are all $Z_n \in A$ for all $n \geq 1$ and all $Z_n^{'} \in \overline{A}$ for all $n \geq 2$ if and only if $Y^* = k-1$.

(ii) By Theorem 1.2 (i) the following hold true: $Y_{n+1} > Y_n \geq 0$ for all $n = 0, 1, \ldots$, while $Y^* = Y_0 = 0$ and $Y_1 = 2\sqrt{2k^2-1}$.

Also, (by direct computations) we show that $Y_1 > k+1$. Consequently, the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k), which belong to A and satisfy the inequality $Y > k+1$ are all Z_n for every $n \geq 1$.

Proposition 4.5. *Consider the Diophantine equation (F_1). Let*

$$X_n + Y_n\sqrt{2} \equiv (1 + 0\sqrt{2})(3 + 2\sqrt{2})^n \quad \text{for all } n = 0, 1, \ldots.$$

Then the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_1), such that $Y > 2$, are all $X_n + Y_n\sqrt{2}$ for every $n \geq 2$.

Proof. By using Theorem 1.2 (i).

Theorem 4.6. *Let k be a natural number. Consider the Diophantine equation (F_k). Let $Z_r^* \equiv X_r^* + Y_r^*\sqrt{2}$, (where $r = 1, 2, \ldots, m$) be the only integral solutions of (F_k) such that:*

$$X_r^* > 0 \quad \text{and} \quad 0 \leq Y_r^* \leq k-1.$$

Let A_r be the corresponding classes of integral solutions of (F_k) with fundamental solutions Z_r^*. Let

$$Z_n \equiv X_n + Y_n\sqrt{2} \equiv (X_r^* + Y_r^*\sqrt{2})(3+2\sqrt{2})^n \text{ for all } n = 0, 1, \ldots,$$
$$Z_n^{'} \equiv X_n^{'} + Y_n^{'}\sqrt{2} \equiv (X_r^* - Y_r^*\sqrt{2})(3+2\sqrt{2})^n \text{ for all } n = 1, 2, \ldots.$$

for an (arbitrary) typical r. Then the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k), which satisfy the inequality $Y > k+1$, are the following:

(i) All $Z_n \in A_r$ and all $Z_n^{'} \in \overline{A}_r$ for every $n \geq 1$ if and only if $0 < Y_r^* < k-1$.

(ii) All $Z_n \in A_r$ for every $n \geq 1$ and all $Z_n^{'} \in \overline{A}_r$ for every $n \geq 2$ if and only if $0 < Y^* = k-1$.

(iii) All $Z_n \in A_r$ for every $n \geq 1$ if and only if $Y_r^* = 0$ for $k \geq 2$.

(iv) All $Z_n \in A_r$ for every $n \geq 2$ if and only if $Y_r^* = 0$ for $k = 1$.

Proof. By using Propositions 4.4, 4.5 and Theorem 3.6.

Theorem 4.7. *Let k be a natural number. Consider the Diophantine equation (F_k). Let $X_r^* + Y_r^*\sqrt{2}$, (where $r = 1, 2, \ldots, m$) be the only integral solutions of (F_k) such that:*

$$X_r^* > 0 \text{ and } 0 \leq Y_r^* \leq k-1.$$

Let

$$X_n + Y_n\sqrt{2} \equiv (X_r^* + Y_r^*\sqrt{2})(3+2\sqrt{2})^n \text{ for all } n = 0, 1, \ldots \text{ and } r = 1, 2, \ldots, m,$$
$$X_n^{'} + Y_n^{'}\sqrt{2} \equiv (X_r^* - Y_r^*\sqrt{2})(3+2\sqrt{2})^n \text{ for all } n = 1, 2, \ldots \text{ and } r = 1, 2, \ldots, m.$$

Then the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_k) such that $Y > k+1$ are the following:

(i) All $X_n + Y_n\sqrt{2}$ and all $X_n^{'} + Y_n^{'}\sqrt{2}$ (with $n \geq 1$) for every Y_r^* with $0 < Y_r^* < k-1$, when $k \geq 2$.

(ii) All $X_n + Y_n\sqrt{2}$ (with $n \geq 1$) and all $X_n^{'} + Y_n^{'}\sqrt{2}$ (with $n \geq 2$) for $0 < Y_r^* = k-1$, when $k \geq 2$.

(iii) All $X_n + Y_n\sqrt{2}$ (with $n \geq 1$) for $Y_r^* = 0$, when $k \geq 2$.

(iv) All $X_n + Y_n\sqrt{2}$ (with $n \geq 2$) for $Y_r^* = 0$, when $k = 1$.

Proof. By using Theorems 3.6 and 4.6.

By Corollary 3.7 it follows that

Corollary 4.8. *The only non-negative integral solutions $X + Y\sqrt{2}$ of (F_0) such that $Y > 1$ are:*

$$X_n + Y_n\sqrt{2} \text{ for every } n = 1, 2, \ldots.$$

Theorem 4.9. *Consider the Diophantine equation* (F_k), $k = 0, 1, \ldots$. *Let* $X + Y\sqrt{2}$ *be a non-negative integral solution of* (F_k). *Let* $x \equiv (X-1)/2$ *and* $N(x) \equiv x^2 + (x+1)^2$. *Then* $N(x) = Y^2 + k^2$. *Moreover, the following are equivalent:*

(i) $N(x)$ *is composite.*

(ii) $Y > k + 1$.

Proof. The equality $N(x) = Y^2 + k^2$ follows by direct computations, while the equivalence of (i) and (ii) follows from Theorems 4.2 and 1.1.

Theorem 4.10. *Let* $N(x) \equiv x^2 + (x+1)^2$. *Consider the Diophantine equation* (F_k), $k = 0, 1, \ldots$. *Let* $X_r^* + Y_r^*\sqrt{2}$, *(where* $r = 1, 2, \ldots, m$*) be the only non-negative integral solutions of* (F_k) *such that:*

$$0 \leq Y_r^* \leq k - 1 \quad \text{for } k \geq 1,$$

while, for $k = 0$ *we have:* $X_r^* = Y_r^* = 1$ *for all* $r = 1, 2, \ldots, m$. *Let*

$$X_n + Y_n\sqrt{2} \equiv (X_r^* + Y_r^*\sqrt{2})(3 + 2\sqrt{2})^n,$$
$$X_n^{'} + Y_n^{'}\sqrt{2} \equiv (X_r^* - Y_r^*\sqrt{2})(3 + 2\sqrt{2})^n \text{ for all } n = 0, 1, \ldots,$$

(for a typical r*). Let* $\tilde{x}_n \equiv (X_n - 1)/2$ *and* $\tilde{x}_n^{'} \equiv (X_n^{'} - 1)/2$ *for every* $n = 0, 1, \ldots$. *Let* R_n, $R_n^{'}$, *where* $n = 0, 1, \ldots$, *be the sequences defined by the recursive formmulae:*

$$R_{n+1} = 34R_n - R_{n-1} - 8(2k^2 + 1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0 = Y_r^{*2} + k^2$, $R_1 = (2X_r^* + 3Y_r^*)^2 + k^2$ *(for a typical* r*).*

$$R_{n+1}^{'} = 34R_n^{'} - R_{n-1}^{'} - 8(2k^2 + 1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0^{'} = Y_r^{*2} + k^2$, $R_1^{'} = (2X_r^* - 3Y_r^*)^2 + k^2$ *(for a typical* r*).*

Then the following hold true:

(i) Let $k = 0$. *The for every integer* n *there exists an integer* m *such that:*

$$R_n = R_m^{'} = N(\tilde{x}_n) \quad \text{for every } n \geq 0.$$

Moreover, the numbers $R_1, R_2, \ldots$, *are all composite.*

(ii) Let $k = 1$, *whence* $X_r^* = 1$, $Y_r^* = 0$ *for every* $r = 1, 2, \ldots, m$. *Then*

$$R_n = R_n^{'} = N(\tilde{x}_n) \quad \text{for every } n \geq 0.$$

Moreover, the numbers $R_2, R_3, \ldots$, *are all composite.*

(iii) Let $k \geq 2$ *and* $Y_r^* = 0$ *Then*

$$R_n = R_n^{'} = N(\tilde{x}_n) \quad \textit{for every } n \geq 0.$$

Moreover, the numbers $R_1, R_2, \ldots$, *are all composite.*

(iv) Let $k \geq 2$ *and* $Y_r^* = k - 1$. *Then*

$$R_n = N(\tilde{x}_n) \quad \textit{and} \quad R_n^{'} = N(\tilde{x}_n^{'}) \quad \textit{for every } n \geq 0.$$

Moreover, the numbers $R_1, R_2, \ldots$, *and also the numbers* $R_2^{'}, R_3^{'}, \ldots$, *are all composite.*

(v) Let $k \geq 2$ *and* $0 < Y_r^* < k - 1$. *Then*

$$R_n = N(\tilde{x}_n) \quad \textit{and} \quad R_n^{'} = N(\tilde{x}_n^{'}) \quad \textit{for every } n \geq 0.$$

Moreover, the numbers $R_1, R_2, \ldots$, *and also the numbers* $R_1^{'}, R_2^{'}, \ldots$, *are all composite.*

Note: For the cases (iv) and (v) we have:

$$R_m \neq R_n^{'} \quad \textit{for any } m, n.$$

Proof. (i) The unique class of integral solutions of (F_0) is ambiguous. By Theorem 2.4 in [5] and Corollary 4.8 we have:

$$X_n + Y_n\sqrt{2} \equiv \xi_{2n+1} + \eta_{2n+1}\sqrt{2} = (1+\sqrt{2})(x_n + y_n\sqrt{2}) = (1+\sqrt{2})^{2n+1}$$

for all $n = 0, 1, \ldots$.

Hence, by the definition of ambiguous class and Theorem 1.3, for every integer n there exists an integer m such that:

$$R_n = R_m^{'} = N(\tilde{x}_n), \text{ where } \tilde{x}_n = (\xi_{2n+1} - 1)/2.$$

According to Corollary 4.8, the only (non-negative) integral solutions $X + Y\sqrt{2}$ of (F_0) such that $Y > 1$ are all $Y_{n+1} = \eta_{2n+3}$ for every $n \geq 0$. Hence by Theorem 4.9, the numbers $R_1, R_2, \ldots$ are all composite.

(ii) Obviously $X_r^* = 1$, $Y_r^* = 0$ for every $r = 1, 2, \ldots, m$ because $k = 1$. Hence, $R_n = R_n^{'}$ for all $n = 0, 1, \ldots$. Now, Theorem 1.3 implies

$$R_n = N(\tilde{x}_n) = Y_n^2 + k^2 = Y_n^2 + 1 \quad \text{for all } n \geq 0.$$

Also, by Theorem 4.7 (iv), we deduce that $X_{n+1}+Y_{n+1}\sqrt{2}$, where $n \geq 1$, are the only (non-negative) integral solutions of (F_1) such that $Y_{n+1} > k+1 = 2$. Hence, according to Theorem 4.9, the numbers $R_2, R_3, \ldots$ are all composite.

(iii) We have $R_n = R_n^{'}$ for every $n = 0, 1, \ldots$ because $Y_r^* = 0$. By Theorem 4.7 (iii) the numbers $X_{n+1} + Y_{n+1}\sqrt{2}$, where $n \geq 0$, are the only (non-negative) integral solutions of (F_k) such that $Y_{n+1} > k+1$. This completes the proof by invoking Theorems 1.3 and 4.9.

(iv) By Theorem 4.7 (ii) the numbers $X_{n+1}+Y_{n+1}\sqrt{2}$ with $n \geq 0$, together with the numbers $X_{n+1}^{'} + Y_{n+1}^{'}\sqrt{2}$, with $n \geq 1$, are the only (non-negative) integral solutions of (F_k) such that $Y_{n+1} > k+1$ and $Y_{n+1}^{'} > k+1$. Thus the proof is completed by Theorem 1.3 and 4.9.

(v) By Theorem 4.7 (i), the numbers $X_{n+1} + Y_{n+1}\sqrt{2}$ together with the numbers $X_{n+1}^{'} + Y_{n+1}^{'}\sqrt{2}$, where $n \geq 0$, are the only (non-negative) integral solutions of (F_k) such that $Y_{n+1} > k+1$ and $Y_{n+1}^{'} > k+1$. This finishes the proof of the whole Theorem, again in view of Theorems 1.3 and 4.9.

Theorem 4.11. *Consider the Diophantine equation (F_k), $k = 0, 1, \ldots$. Let $X_r^* + Y_r^*\sqrt{2}$, (where $r = 1, 2, \ldots, m$) be the only non-negative integral solutions of (F_k) such that:*

$$0 \leq Y_r^* \leq k-1 \quad \text{for } k \geq 1,$$

While, for $k = 0$ we have: $X_r^* = Y_r^* = 1$ for all $r = 1, 2, \ldots, m$. Let $R_n, R_n^{'}$ be the sequences, defined by the recursive formulae:

$$R_{n+1} = 34R_n - R_{n-1} - 8(2k^2+1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0 = Y_r^{*2} + k^2$, $R_1 = (2X_r^* + 3Y_r^*)^2 + k^2$ (for a typical r).

$$R_{n+1}^{'} = 34R_n^{'} - R_{n-1}^{'} - 8(2k^2+1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0^{'} = Y_r^{*2} + k^2$, $R_1^{'} = (2X_r^* - 3Y_r^*)^2 + k^2$ (for a typical r).

Suppose that the number $N(x) \equiv x^2 + (x+1)^2$ is composite. Then $N(x)$ is equal to some of the composite numbers R_n or $R_n^{'}$, for a suitable index, as stated in cases (i)–(v) of Theorem 4.10 (for some value of k).

Proof. Since $N(x)$ is composite it follows from Theorem 1.1 that there exist natural numbers y, z such that

$$T(x) = T(y) + T(z).$$

Let $y \geq z$. Let also $k \equiv y - z$, $X \equiv 2x + 1$ and $Y \equiv 2y - (k-1)$. Then, according to Theorem 4.2 (ii), $X + Y\sqrt{2}$ is a (non-negative) integral solution of (F_k), with $Y > k + 1$. Hence, $X + Y\sqrt{2}$ is a solution of type (i) or (ii) or (iii) or (iv) of Theorem 4.7 or it is a solution $X + Y\sqrt{2}$ of (F_0) with $Y > 1$ (see Corollary 4.8). Also, $N(x) = Y^2 + k^2$. Hence, by Theorem 1.3 $N(x)$ is equal to some R_n or some $R_n^{'}$. Finally, the appropriate index n for which $N(x) = R_n$ or $N(x) = R_n^{'}$ is obtained by applying Theorem 4.6 to the respective case as in (i)-(v) of Theorem 4.10. This ends the proof of the Theorem.

Theorem 4.12. (*Determination of all composites of the form* $N(x) \equiv x^2 + (x+1)^2$) *Consider the Diophantine equations*

$$(F_k) \qquad X^2 - 2Y^2 = 2k^2 - 1, \quad \text{where } k = 0, 1, \ldots.$$

Let $X_r^* + Y_r^*\sqrt{2}$, *(where* $r = 1, 2, \ldots, m$*), be the only non-negative integral solutions of* (F_k) *such that:*

$$0 \leq Y_r^* \leq k - 1 \quad \text{for } k \geq 1,$$

While, for $k = 0$ *we have:* $X_r^* = Y_r^* = 1$ *for all* $r = 1, 2, \ldots, m$. *Let* $R_n, R_n^{'}$ *be the sequences defined by the recursive formulae:*

$$R_{n+1} = 34R_n - R_{n-1} - 8(2k^2 + 1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0 = Y_r^{*2} + k^2$, $R_1 = (2X_r^* + 3Y_r^*)^2 + k^2$ *(for a typical* r*).*

$$R_{n+1}^{'} = 34R_n^{'} - R_{n-1}^{'} - 8(2k^2 + 1) \quad \text{for all } n = 1, 2, \ldots,$$

where $R_0^{'} = Y_r^{*2} + k^2$, $R_1^{'} = (2X_r^* - 3Y_r^*)^2 + k^2$ *(for a typical* r*).*

Then, the only composite numbers of the form $N(x) \equiv x^2 + (x+1)^2$ *are the following:*

(i) $R_1, R_2, \ldots$ *(for* $k = 0$*).*
(ii) $R_2, R_3, \ldots$ *(for* $k = 1$ *and* $Y_r^* = 0$*).*
(iii) $R_1, R_2, \ldots$ *(for* $k \geq 2$ *and* $Y_r^* = 0$*).*
(iv) $R_1, R_2, \ldots$ *together with* $R_2^{'}, R_3^{'}, \ldots$ *(for* $k \geq 2$ *and* $Y_r^* = k - 1$*).*
(v) $R_1, R_2, \ldots$ *together with* $R_1^{'}, R_2^{'}, \ldots$ *(for* $k \geq 2$ *and for all* Y_r^* *such that* $0 < Y_r^* < k - 1$*).*

Proof. By using Theorems 4.10 and 4.11.

Theorem 4.13. (*Sieve-algorithm for the determination of all primes of the form* $N(x) \equiv x^2 + (x+1)^2$ *in an Interval [5,M], where* M *is a (positive) integer*)

Step 1: Determine all numbers $N(x)$ for $x = 1, 2, \ldots, \left[(-1+\sqrt{2M-1})/2\right]$.

Step 2: Determine all R_n and R'_n, as in Theorem 4.12 obtained from the Diophantine equations

$$X^2 - 2Y^2 = 2k^2 - 1, \quad \text{where } k = 0, 1, \ldots, \left[\sqrt{M}\right].$$

Step 3: Delete from the table of the numbers in Step 1, all numbers of Step 2. The remaining numbers are the only prime numbers of the form $N(x)$ in the interval [5,M].

Proof. By using Theorem 4.12.

References

[1] C. F. Gauss, *Disqusitiones Arithmeticae*, (English transl. A. A. Clarke, Yale University Press, New Haven, Connecticut, London, 1966.)

[2] T. Nagell, *Introduction to Number Theory*, Chelsea, New York, 1964.

[3] W. Sierpinski, Sur les nombres triangularies qui sont sommes de deux nombres triangularies, *Elem. Math.*, **17** (1962), 63–65.

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

[5] P. G. Tsangaris, Fermat–Pell Equation and the Numbers of the form $w^2+(w+1)^2$, *Publ. Math. Debrecen*, **47** (1995), 127–138.

Panayiotis G. Tsangaris
Department of Mathematics, Athens University
Panepistimiopolis, 157 84 Athens, Greece.

Quasi multiplicative functions with congruence property

BUI MINH PHONG

Abstract. We prove that if an integer-valued quasi multiplicative function f satisfies the congruence $f(n+p)\equiv f(n) \pmod{p}$ for all positive integers n and all primes $p\neq\pi$, where π is a given prime, then $f(n)=n^{\alpha}$ for some integer $\alpha\geq 0$.

An arithmetical function $f(n) \not\equiv 0$ is said to be multiplicative if $(n, m) = 1$ implies

$$f(nm) = f(n)f(m)$$

and it is called completely multiplicative if this holds for all pairs of positive integers n and m. In the following we denote by $\mathcal{M}$ and $\mathcal{M}^*$ the set of all integer-valued multiplicative and completely multiplicative functions, respectively. Let $\mathbf{N}$ be the set of all positive integers and $\mathcal{P}$ be the set of all primes.

The problem concerning the characterization of some arithmetical functions by congruence properties was studied by several authors. The first result of this type was found by M. V. Subbarao [7], namely he proved in 1966 that if $f \in \mathcal{M}$ satisfies

$$f(n + m) \equiv f(m) \pmod{n} \quad \text{for all} \quad n, m \in \mathbf{N}, \tag{1}$$

then there is an $\alpha \in \mathbf{N}$ such that

$$f(n) = n^{\alpha} \quad \text{for all} \quad n \in \mathbf{N}. \tag{2}$$

A. Iványi [2] extended this result proving that if $f \in \mathcal{M}^*$ and (1) holds for a fixed $m \in \mathbf{N}$ and for all $n \in \mathbf{N}$, then $f(n)$ has also the same form (2). It is shown in [4] that the result of Subbarao continues to hold if the relation (1) is valid for $n \in \mathcal{P}$ instead for all positive integers. In [6] we improved the results of Subbarao and Iványi mentioned above by proving that if $M \in \mathbf{N}$, $f \in \mathcal{M}$ satisfy $f(M) \neq 0$ and

$$f(n + M) \equiv f(M) \pmod{n} \quad \text{for all} \quad n \in \mathbf{N},$$

It was financially supported by OTKA 2153 and T 020295

then (2) holds. Later, in the papers [3]–[5] we obtained some generalizations of this result, namely we have shown that if integers $A > 0$, $B > 0$, $C \neq 0$, $N > 0$ with $(A, B) = 1$ and $f \in \mathcal{M}$ satisfy the relation

$$f(An + B) \equiv C \pmod{n} \quad \text{for all} \quad n \geq N,$$

then there are a positive integer α and a real-valued Dirichlet character $\chi \pmod{A}$ such that $f(n) = \chi(n)n^{\alpha}$ for all $n \in \mathbf{N}$, $(n, A) = 1$.

In 1985, Subbarao [8] introduced the concept of weakly multiplicative arithmetic function $f(n)$ (later renamed quasi multiplicative arithmetic functions) as one for which the property

$$f(np) = f(n)f(p)$$

holds for all primes p and positive integers n which are relatively prime to p. In the following let $\mathcal{QM}$ denote the set of all integer-valued quasi multiplicative functions. In [1] J. Fabrykowski and M. V. Subbarao proved that if $f \in \mathcal{QM}$ satisfies

$$f(n + p) \equiv f(n) \pmod{p} \tag{3}$$

for all $n \in \mathbf{N}$ and all $p \in \mathcal{P}$, then $f(n)$ has the form (2). They also conjectured that this result continues to hold even if the relation (3) is satisfied for an infinity of primes instead of for all primes. This conjecture is still open.

Let $\mathcal{A} \subset \mathcal{P}$, and assume that the congruence (3) holds for all $n \in \mathbf{N}$ and for all $p \in \mathcal{A}$. For each positive integer n let $H(n)$ denote the product of all prime divisors p of n for which $p \in \mathcal{A}$. It is obvious from the definition that $H(n) \mid H(mn)$ holds for all positive integers n and m, furthermore one can deduce that if $f \in \mathcal{QM}$ satisfies the congruence (3) for all $n \in \mathbf{N}$ and for all $p \in \mathcal{A}$, then

$$f(n + m) \equiv f(m) \pmod{H(n)} \quad \text{for all} \quad n,\ m \in \mathbf{N}.$$

Thus the conjecture of Fabrykowski and Subbarao is contained in the following

Conjecture. *Let A, B be fixed positive integers with the condition $(A, B) = 1$ and $\mathcal{A}$ is an infinite subset of $\mathcal{P}$. If a function $f \in \mathcal{QM}$ and integer $C \neq 0$ satisfy the congruence*

$$f(An + B) \equiv C \pmod{H(n)} \quad \textit{for all} \quad n \in \mathbf{N},$$

then there are a positive integer α *and a real-valued Dirichlet character* χ (mod A) *such that*

$$f(n) = \chi(n)n^{\alpha} \quad \text{for all} \quad n \in \mathbf{N},\ (n, A) = 1.$$

In this note we prove this conjecture for a special case, when $A = B = 1$ and $\mathcal{P} = \mathcal{A} \cup \{\pi\}$, where π is a fixed prime.

Theorem. *Let* π *be a given prime and let* $H(n)$ *be the product of all prime divisors* p *of* n *for which* $p \neq \pi$. *If a function* $f \in \mathcal{QM}$ *and an integer* $C \neq 0$ *satisfy the congruence*

$$f(n+1) \equiv C \pmod{H(n)} \tag{4}$$

for all $n \in \mathbf{N}$, *then there is a non-negative integer* α *such that*

$$f(n) = n^{\alpha} \quad \text{for all} \quad n \in \mathbf{N}.$$

We shall use some lemmas in the proof of our theorem.

Lemma 1. *Assume that the conditions of the theorem are satisfied. Then* $f \in \mathcal{M}^*$, *i.e*

$$f(ab) = f(a)f(b)$$

holds for all $a,\ b \in \mathbf{N}$. *Furthermore* $C = 1$.

Proof. Assume that a and b are fixed positive integers. Let q be a prime with the condition

$$q > \max(a,\ b,\ |C|,\ |Cf(ab) - f(a)f(b)|) \quad \text{and} \quad q \neq \pi. \tag{5}$$

Since $(ab, q) = 1$, one can deduce from Dirichlet's theorem that there are positive integers x, y, u and v such that

$$ax = qy + 1, \quad (x, ab) = 1, \quad x \in \mathcal{P}$$

and

$$bu = qv + 1, \quad (u, abx) = 1, \quad u \in \mathcal{P}.$$

Then we have

$$abxu = qT + 1,$$

where $T := y + v + qyv$. Thus, we infer from (4) and the fact $f \in \mathcal{QM}$, that

$$f(a)f(x) = f(ax) = f(qy + 1) \equiv C \pmod{q},$$

$$f(b)f(u) = f(bu) = f(qv+1) \equiv C \pmod{q}$$

and

$$f(ab)f(x)f(u) = f(abxu) = f(qT+1) \equiv C \pmod{q}.$$

These and (5) show that $f(x)f(u) \not\equiv 0 \pmod{q}$, consequently

$$f(a)f(b) \equiv Cf(ab) \pmod{q}.$$

Hence, we infer from the last relation together and the fact $q > |Cf(ab) - f(a)f(b)|$ that

$$Cf(ab) = f(a)f(b). \tag{6}$$

Thus, we have proved that (6) holds for all positive integers a and b. By applying (6) with $a = b = 1$, we have $C = 1$ and so the proof of Lemma 1 is finished.

Lemma 2. *Assume that the conditions of the theorem are satisfied. Let Q be a positive integer. Then for each prime divisor q of $f(Q)$ we have $q|\pi Q$.*

Proof. Let Q be a positive integer and assume on the contrary that there exists a prime q such that $q|f(Q)$ and $\left(q, \pi Q\right) = 1$.

Since $(Q, q) = 1$, we infer that there are positive integers x and y such that

$$Qx = qy + 1.$$

By using Lemma 1, it follows from (4) and the fact $q \neq \pi$ that

$$0 \equiv f(Q)f(x) = f(Qx) = f(qy+1) \equiv 1 \pmod{q},$$

which is a contradiction. Thus the proof of Lemma 2 is finished.

Lemma 2 shows that for each prime p, we can write $f(p)$ as follows:

$$|f(p)| = p^{\alpha(p)}\pi^{\beta(p)},$$

consequently

$$|f(\pi)| = \pi^{\alpha}, \tag{7}$$

for some non-negative integer α.

Now we can prove our theorem.

Proof of the theorem. We shall prove that $f(n) = n^\alpha$ is satisfied for all $n \in \mathbf{N}$, where $\alpha \geq 0$ is given in (7).

Let n, s be positive integers. By (4), we have

$$f(n\pi^{2s}) = f\left((n\pi^{2s} - 1) + 1\right) \equiv 1 \pmod{H(n\pi^{2s} - 1)}.$$

On the other hand, it follows from Lemma 1 and (7) that

$$n^\alpha f(n\pi^{2s}) = n^\alpha f(n)\pi^{2\alpha s} = f(n)(n\pi^{2s})^\alpha \equiv f(n) \pmod{H(n\pi^{2s} - 1)}.$$

These imply

$$f(n) \equiv n^\alpha \pmod{H(n\pi^{2s} - 1)},$$

therefore, by setting $s \to \infty$, we have $H(n\pi^{2s} - 1) \to \infty$ and so $f(n) = n^\alpha$. This holds for each positive integer n, consequently it also holds for all $n \in \mathbf{N}$. The theorem is proved.

References

[1] J. Fabrykowski and M. V. Subbarao, A class of arithmetic functions satisfying a congruence property, *Journal Madras University, Section B* **51** (1988), 48–51.

[2] A. Iványi, On multiplicative functions with congruence property, *Ann. Univ. Sci. Budapest, Sect. Math.* **15** (1972), 133–137.

[3] I. Joó and B. M. Phong, Arithmetical functions with congruence properties, *Ann. Univ. Sci. Budapest, Sect. Math.* **35** (1992), 151–155.

[4] B. M. Phong, Multiplicative functions satisfying a congruence property, *Periodica Math. Hungar.* **26** (1991), 123–128.

[5] B. M. Phong, Multiplicative functions satisfying a congruence property V, *Acta Math. Hungar.* **62** (1993), 81–87.

[6] B. M. Phong and J. Fehér, Note on multiplicative functions satisfying congruence property, *Ann. Univ. Sci. Budapest, Sect. Math.* **33** (1990), 261–265.

[7] M. V. Subbarao, Arithmetic functions satisfying congruence property, *Canad. Math. Bull.*, **9** (1966), 143–146.

[8] M. V. Subbarao, *Amer. Math. Soc. Abstract*, **86** # T-11-15, p. 324.

Bui Minh Phong
Eötvös Loránd University
Department of Computer Algebra
Pázmány Péter sét. 2. Inf. ép.
H-1117 Budapest, Hungary
E-mail: bui@compalg.elte.hu

On a conjecture about the equation
$A^{mx} + A^{my} = A^{mz}$

ALEKSANDER GRYTCZUK

Abstract. Let A be a given integral 2×2 matrix. We prove that the equation

$$(\star) \qquad A^{mx}+A^{my}=A^{mz}$$

has a solution in positive integers x,y,z and $m>2$ if and only if the matrix A is a nilpotent matrix or the matrix A has an eigenvalue $\alpha=\frac{1+i\sqrt{3}}{2}$.

1. Introduction

First we note that $(\star)$ is equivalent to the following Fermat's equation

$$(1) \qquad X^m + Y^m = Z^m, \quad m > 2,$$

where $X = A^x$, $Y = A^y$ and $Z = A^z$.

It has been recently proved by A. WILES [12], R. TAYLOR and A. WILES [11] that (1) has no solution in nonzero integers X, Y, Z if $m > 2$. But, in contrast to the classical case, the Fermat's equation (1) has infinitely many solutions in 2×2 integral matrices X, Y, Z for $m = 4$. This fact was discovered by R. Z. DOMIATY [2] in 1966. Namely, he proved that, if

$$X = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 0 & 1 \\ c & 0 \end{pmatrix},$$

where a, b, c are integer solutions of the Pythagorean equation $a^2 + b^2 = c^2$, then

$$X^4 + Y^4 = Z^4.$$

Other results connected with Fermat's equation in the set of matrices are given in monograph [10] by P. RIBENBOIM. In these investigations it is an important problem to give a necessary and sufficient condition for the solvability of (1) in the set of matrices. Such type results were proved recently by A. KHAZANOV [7], when the matrices X, Y, Z belong to $SL_2(Z)$, $SL_3(Z)$ or $GL_3(Z)$. In particular, he proved that there are solutions of (1) in $X, Y, Z \in SL_2(Z)$ if and only if m is not a multiple of 3 or 4. We proved

in [4] a necessary condition for the solvability of (1) in 2×2 integral matrices X, Y, Z having a determinant form. More precisely, we proved (see [4], Thm. 2) that the equation $(\star)$ does not hold in positive integers x, y, z and $m \geq 2$, if $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Another proof of this cited result was given by D. Frejman [3].

M. H. Le and Ch. Li [8] proved the following generalization of our result: Let $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ be a given integral matrix such that $r = \operatorname{Tr} A = a + d > 0$ and $\det A = ad - bc < 0$, then $(\star)$ does not hold.

In their paper they posed the following

Conjecture. Let A be an integral 2×2 matrix. The equation $(\star)$ has a solution in natural numbers x, y, z and $m > 2$ if and only if the matrix A is a nilpotent matrix.

A corrected version of this Conjecture was proved by the same authors in [9].

In the present paper we prove the following

Theorem. *The equation $(\star)$ has a solution in positive integers x, y, z and $m > 2$ if and only if the matrix A is a nilpotent matrix or the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$.*

We note that the condition matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$ is equivalent to $\operatorname{Tr} A = \det A = 1$ (cf. [9]). On the other hand it is easy to see that the condition $\det A = 1$ implies that the matrix A cannot be a nilpotent matrix, thus the original Conjecture of M. H. Le and Ch. Li is not true.

We also note that X. Chen [1] proved that if A_n is the companion matrix for the polynomial $f(x) = x^n - x^{n-1} - \ldots - x - 1$ then the equation $(\star)$ with $A = A_n$ has no solution in positive integers x, y, z and $m \geq 2$ for any fixed integer $n \geq 2$.

Futher result of this type is contained by [5]. Namely, we proved the following:

Let $A = (a_{ij})_{n \times n}$ be a matrix with at least one real eigenvalue $\alpha > \sqrt{2}$. If the equation

$$A^r + A^s = A^t \tag{2}$$

has a solution in positive integers r, s and t then $\max\{r - t, s - t\} = -1$.

From this cited result one can obtain the corresponding results of the papers [1], [3], [4], [8] as particular cases.

2. Basic Lemmas

Lemma 1. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an integral matrix such that* $\operatorname{Tr} A \neq 0$ *or* $\det A \neq 0$ *and let*

$$r = a + d = \operatorname{Tr} A, \quad s = -\det A, \quad A_0 = r, \quad A_1 = rA_0 + s$$

and

$$A_n = rA_{n-1} + sA_{n-2} \quad \text{if} \quad n \geq 2.$$

Then for every natural number $n \geq 2$, *we have*

$$A^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = \begin{pmatrix} aA_{n-2} + sA_{n-3} & bA_{n-2} \\ cA_{n-2} & dA_{n-2} + sA_{n-3} \end{pmatrix},$$

where we put $A_{-1} = 1$.

The proof of this Lemma immediately follows from Theorem 1 of [6].

Lemma 2. *Let* A *be an integral matrix satisfying the assumptions of Lemma 1 and let* A_n *be the recurrence sequence associated with the matrix* A *as in Lemma 1. Moreover, let* Δ_n *be the discriminant of the characteristic polynomial of* A^n *if* $n \geq 2$ *and let* $\Delta_1 = \Delta = r^2 + 4s$. *Then for every natural number* $n \geq 2$ *we have* $\Delta_n = \Delta A_{n-2}^2$.

The proof of Lemma 2 is given in [4].

Lemma 3. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an integral matrix and let* $f(x) = x^2 - (\operatorname{Tr} A)x + \det A$ *be the characteristic polynomial of* A *with the roots* $\alpha, \beta \neq \frac{1+i\sqrt{3}}{2}$ *and the discriminant* $\Delta = r^2 + 4s$, *where* $r = a + d = \operatorname{Tr} A$ *and* $s = -\det A$. *If* $s \neq 0$ *and* $\Delta \neq 0$ *then the equation* $(\star)$ *has no solutions in natural numbers* x, y, z *and* $m > 2$.

Proof. If $x = z$ and $(\star)$ is satisfied then $A^{my} = 0$, thus $\det A = 0$, which contradicts to our assumption. Similarly we obtain a contradiction when $y = z$. If $x = y$ then by $(\star)$ it follows that $2A^{mx} = A^{mz}$, hence $4(\det A)^{mx} = (\det A)^{mz}$ and so we obtain a contradiction, because the last equality is impossible in natural numbers x, y, z and $m > 2$ with integer $\det A \neq 0$.

Further on we can assume that if $(\star)$ is satisfied, then x, y and z are distinct natural numbers. Since $s = -\det A \neq 0$, therefore there exists the inverse matrix A^{-1} and from $(\star)$ we obtain

$$A^{m(x-z)} + A^{m(y-z)} = I, \quad \text{if} \quad \min\{x, y, z\} = z \tag{3}$$

$$A^{m(x-y)} + I = A^{m(z-y)}, \quad \text{if} \quad \min\{x, y, z\} = y, \tag{4}$$

$$I + A^{m(y-x)} = A^{m(z-x)}, \quad \text{if} \quad \min\{x, y, z\} = x, \tag{5}$$

where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $\{A_n\}$ be the recurrence sequence associated with the matrix A. Then applying Lemma 1 to (3) we obtain

$$(6)\quad \begin{aligned} &a\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) - (\det A)\left(A_{m(x-z)-3} + A_{m(y-z)-3}\right) = 1,\\ &b\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) = 0,\\ &c\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) = 0,\\ &d\left(A_{m(x-z)-2} + A_{m(y-z)-2}\right) - (\det A)\left(A_{m(x-z)-3} + A_{m(y-z)-3}\right) = 1. \end{aligned}$$

From Lemma 1, (4) and (5) we obtain similar formulae to (6).

Suppose that $b \neq 0$ or $c \neq 0$. Then from (6) we get $\det A = \pm 1$. On the other hand since $\Delta \neq 0$, therefore from Lemma 2 we can deduce that

$$(7)\qquad A_{n-2} = \frac{1}{\sqrt{\Delta}}\left(\alpha^n - \beta^n\right).$$

Substituting (7) to (6) we obtain

$$(8)\qquad \alpha^{m(x-z)} + \alpha^{m(y-z)} = \beta^{m(x-z)} + \beta^{m(y-z)} = 1.$$

By (4) and (5) we similarly have

$$(9)\qquad \alpha^{m(z-y)} - \alpha^{m(x-y)} = \beta^{m(z-y)} - \beta^{m(x-y)} = 1$$

and

$$(10)\qquad \alpha^{m(z-x)} - \alpha^{m(y-x)} = \beta^{m(z-x)} - \beta^{m(y-x)} = 1.$$

From (8)–(10) it follows that in all cases

$$(11)\qquad \alpha^{mx} + \alpha^{my} = \alpha^{mz} \quad \text{and} \quad \beta^{mx} + \beta^{my} = \beta^{mz}$$

for natural numbers x, y, z and $m > 2$, which can be written in the forms

$$(12)\qquad \alpha^{m(x-z)} + \alpha^{m(y-z)} = 1 \quad \text{and} \quad \beta^{m(x-z)} + \beta^{m(y-z)} = 1.$$

Since $\Delta \neq 0$, thus we consider two cases: $\Delta > 0$ or $\Delta < 0$. Let us suppose that $\Delta > 0$. Since $\Delta = r^2 + 4s$ and $s = -\det A = \pm 1$, so we have $\Delta \geq 5$. If $r > 0$ then we obtain

$$(13)\qquad \alpha = \frac{r + \sqrt{\Delta}}{2} \geq \frac{1 + \sqrt{5}}{2} > \sqrt{2} > 1.$$

From (13) and (12) it follows that both exponents $m(x-z)$ and $m(y-z)$ must be negative. On the other hand fom (13) we have $\alpha^{-2} < \frac{1}{2}$ and by (12) it follows that it cannot happen that both exponents $m(x-z)$ and $m(y-z)$ are ≤ -2. Therefore one of them must be equal to -1 and we obtain $m(x-z) = -1$ or $m(y-z) = -1$. But this is impossible, because $m > 2$ and x, y, z are positive integers.

After this we consider the case $r \leq 0$. Let us suppose that $r < 0$ and put $r = -r'$, where $r' > 0$. Then we have

$$\beta = \frac{r - \sqrt{\Delta}}{2} = -\frac{r' + \sqrt{\Delta}}{2} = -\beta$$

and

$$\beta = r' + \sqrt{\frac{\Delta}{2}} \geq \frac{1+\sqrt{5}}{2} > \sqrt{2} > 1.$$

Substituting $\beta = -\beta$ to the second equation of (12) we obtain

$$(14) \qquad (-1)^{m(x-z)}(\beta')^{m(x-z)} + (-1)^{m(y-z)}(\beta')^{m(y-z)} = 1.$$

If m is even then as in our previous case we obtain a contradiction. So, we can assume that m is an odd natural number greater than 2. If $x-z$ and $y-z$ are odd then it is easy to see that (14) does not hold. Therefore one of them must be even and from (14) we obtain

$$(15) \quad (\beta')^{m(x-z)} - (\beta')^{m(y-z)} = 1, \quad \text{if} \quad x-z \quad \text{is even and} \quad y-z \quad \text{is odd}$$

and

$$(16) \quad (\beta')^{m(y-z)} - (\beta')^{m(x-z)} = 1, \quad \text{if} \quad y-z \quad \text{is even and} \quad x-z \quad \text{is odd.}$$

Because of the symmetry, it is sufficient to consider one of these equations. Let us suppose that (15) is satisfied. If $x-z > 0$ and $y-z > 0$ then, by(15), it follows that $x-z > y-z$. On the other hand, (15) can be represented in the form

$$(17) \qquad (\beta')^{m(y-z)}\left((\beta')^{m(x-z)} - 1\right) = 1.$$

The condition $x-z > y-z$ implies $x > y$ and since $\beta' > \sqrt{2}, m > 2, x-z > 0$ and $y-z > 0$, therefore (17) is impossible. Hence we get that one of the differences $x-z$ so $y-z$ must be negative. Suppose that $x-z < 0$ and $y-z > 0$. Then from (15)

$$(18) \qquad (\beta')^{m(x-z)} = (\beta')^{m(y-z)} + 1$$

follows. It is easy to see that $(\beta')^{m(x-z)} = \left((\beta')^{-2}\right)^{\frac{m(z-x)}{2}}$. On the other hand we have $(\beta')^{-2} < \frac{1}{2}$ and we obtain

$$(\beta')^{m(x-z)} = \left((\beta')^{-2}\right)^{\frac{m(z-x)}{2}} < \left(\frac{1}{2}\right)^{\frac{m(z-x)}{2}} < \frac{1}{2},$$

because $\frac{m(z-x)}{2} > 1$. Therefore from (18) we get

$$(\beta')^{m(y-z)} + 1 = (\beta')^{m(x-z)} < \frac{1}{2},$$

which is impossible. In a similar way we obtain a contradiction in the case $x-z > 0$ and $y-z < 0$. It remains to consider the case when both differences $x - z$ and $y - z$ are negative. From (15) we have

$$1 = \left|(\beta')^{m(x-z)} - (\beta')^{m(y-z)}\right| \leq (\beta')^{m(x-z)} + (\beta')^{m(y-z)}. \tag{19}$$

On the other hand we have

$$(\beta')^{m(x-z)} = \left((\beta')^{-2}\right)^{\frac{m(z-x)}{2}} < \left(\frac{1}{2}\right)^{\frac{m(z-x)}{2}} < \frac{1}{2} \tag{20}$$

and

$$(\beta')^{m(y-z)} + \left((\beta')^{-2}\right)^{\frac{m(z-y)}{2}} < \left(\frac{1}{2}\right)^{\frac{m(z-y)}{2}} < \frac{1}{2}. \tag{21}$$

Hence, by (19)–(21), we get a contradiction.

Further on we have to consider the case $r = 0$. But in this case we have $\alpha = 1, \beta = -1$ and we can can observe that (12) is impossible.

Now, we can consider the case $\Delta < 0$. Since $s = -\det A = \pm 1$ and $\Delta = r^2 + 4s < 0$, therefore we have $s = -1$ and the inequality $r^2 - 4 < 0$ implies $-2 < r < 2$, that is, $r = -1, 0, 1$.

The case $r = 1$ is impossble by the assumptions on the eigenvalues of the matrix A.

If $r = 0$ then we obtain that $\alpha = i, \beta = -i$ and it is easy to check that (12) does not hold.

If $r = -1$ then $\alpha = \frac{-1+i\sqrt{3}}{2}$ is the third root of unity. Analyzing the exponents $m(x - z)$ and $m(y - z)$ modulo 3 in (12) we get a contradiction.

Summarizing, we obtain that in the case $b \neq 0$ or $c \neq 0$ the equation $(\star)$ has no solution in positive integers x, y, z and $m > 2$. So, $b = c = 0$ and the matrix A can be reduced to a diagonal matrix of the form $A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. On the other hand for every natural number k we have

$$A^k = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}^k = \begin{pmatrix} a^k & 0 \\ 0 & d^k \end{pmatrix}. \tag{22}$$

If $(\star)$ is satisfied then, by (22), it follfows that

$$a^{mx} + a^{my} = a^{mz}, \quad d^{mx} + d^{my} = d^{mz}. \tag{23}$$

From the assumption of Lemma 3 we have $s = -\det A \neq 0$. This condition implies $ad \neq 0$, because $\det A = \det \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = ad$. Therefore (23) does not hold.

Considering all of the cases the proof of Lemma 3 is complete.

Now, we can prove the following.

Lemma 4. *Let* $A = \begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ *be an integral matrix and let* $r = \operatorname{Tr} A, s = -\det A$ *and* $\Delta = r^2 + 4s$. *If* $s \neq 0$ *and* $\Delta = 0$, *then* $(\star)$ *has no solutions in positive integers* x, y, z *and* $m > 2$.

Proof. Since $s \neq 0$, therefore using Lemma 1 in similar way as in the proof of Lemma 3, for the case $b \neq 0$ or $c \neq 0$ we obtain $s = -\det A = \pm 1$. Since, $\Delta = r^2 + 4s = 0$, thus $s = -1$ and consequently $r^2 - 4 = 0$, so we have $r = \pm 2$. Therefore we get $\alpha = \beta = \frac{r}{2} = 1$ if $r = 2$ and $\alpha = \beta = -1$ if $r = -2$. From the well-known theorem of Schur it follows that for any given matrix A there is an unitary matrix P such that

$$A = P^* T P, \tag{24}$$

where T is the upper triangular matrix having on the main diagonal the eigenvalues of the matrix A.

Suppose that the matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries has the eigenvalues α, β.

From (24) by easy induction we obtain

$$A^k = P^* T^k P \tag{25}$$

for every natural number k, where T^k is the upper triangular matrix with the eigenvalues α^k, β^k on the main diagonal. If $(\star)$ is satisfied then, by (25), it follows that

$$T^{mx} + T^{my} = T^{mz} \tag{26}$$

and from (26) we have

$$\alpha^{mx} + \alpha^{my} = \alpha^{mz}, \quad \beta^{mx} + \beta^{my} = \beta^{mz}. \tag{27}$$

Since in our case $\alpha = \beta = \pm 1$ so we can see that (27) does not hold. Therefore we have $b = c = 0$ and we get a contradiction as we have got it in the last step of the proof of Lemma 3. So the proof of Lemma 4 is complete.

Lemma 5. *Let* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *be an itegral matrix and let* $r = \operatorname{Tr} A, s = -\det A$ *and* $\Delta = r^2 + 4s$. *If* $s = 0$ *and* $\Delta \neq 0$ *then the equation* $(\star)$ *has no solution in positive integers* x, y, z *and* $m > 2$.

Proof. From the assumptions of Lemma 5 it follows that $r \neq 0$ and therefore we can use Lemma 1. Since $s = 0$ so, by Lemma 1, it follows that

$$A^k = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^k = \begin{pmatrix} ar^{k-1} & br^{k-1} \\ cr^{k-1} & dr^{k-1} \end{pmatrix} = r^{k-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = r^{k-1} A. \tag{28}$$

If $(\star)$ is satisfied then from (28) we obtain

$$r^{mx} + r^{my} = r^{mz}. \tag{29}$$

Being $r \neq 0$, it is easy to see that the equation (29) is impossible in positive integers x, y, z and $m > 2$. This proves Lemma 5.

3. Proof of the Theorem

Suppose that the equation $(\star)$ has a solution in postive integers x, y, z and $m > 2$. Then by Lemma 3, Lemma 4 and Lemma 5 it follows that $s = \det A = 0$ and $r = \operatorname{Tr} A = 0$ or the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$. In the case $s = r = 0$ we have $a = -d$ and $s = -\det A = -(ad - bc) = -\left(-d^2 - bc\right) = d^2 + bc = 0$ and also putting $d = -a$ we have $a^2 + bc = 0$. On the other hand we have

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = \begin{pmatrix} a^2 + bc & b(a+d) \\ c(a+d) & d^2 + bc \end{pmatrix} = \begin{pmatrix} a^2 + bc & br \\ cr & d^2 + bc \end{pmatrix}. \tag{30}$$

Substituting

$$r = 0, a^2 + bc = d^2 + bc = 0$$

to (30) we obtain that $A^2 = 0$, that is the matrix A is a nilpotent matrix with nilpotency index two.

Now, we suppose that the matrix A is nilpotent matrix, i.e. $A^k = 0$ for some natural number $k \geq 2$. Then it is easy to see that $(\star)$ is satisfied for all positive integers $x, y, z, m > 2$ such that $mx \geq k, my \geq k, mz \geq k$.

Suppose that the matrix A has an eigenvalue $\alpha = \frac{1+i\sqrt{3}}{2}$. Then it is easy to check that $\alpha^2 = \frac{-1+i\sqrt{3}}{2} = \varepsilon$ is a third root of unity. By an easy calculation we obtain

$$\alpha^n = \begin{cases} 1, & \text{if} \quad n = 6k, \\ -\varepsilon^2, & \text{if} \quad n = 6k+1, \\ \varepsilon, & \text{if} \quad n = 6k+2, \\ -1, & \text{if} \quad n = 6k+3, \\ \varepsilon^2, & \text{if} \quad n = 6k+4, \\ -\varepsilon, & \text{if} \quad n = 6k+5. \end{cases} \tag{31}$$

Applying (31) we obtain that $(\star)$ is satisfied if and only if the following relations are satisfied

$$mx \equiv r_1 (\bmod\ 6), \quad my \equiv r_2 (\bmod\ 6), \quad mz \equiv r_3 (\bmod\ 6), \tag{32}$$

where

$$\langle r_1, r_2, r_3 \rangle = \langle 0,2,1 \rangle, \langle 0,4,5 \rangle, \langle 1,3,2 \rangle, \langle 1,5,0 \rangle, \langle 2,4,3 \rangle, \langle 2,0,1 \rangle,$$

$$\langle 3,1,2 \rangle, \langle 3,5,4 \rangle, \langle 4,0,5 \rangle, \langle 4,2,3 \rangle, \langle 5,0,1 \rangle, \langle 5,3,4 \rangle.$$

The proof of Theorem is complete.

From the proof of Theorem we get the following

Corollary. *All soluitions of the equation*$(\star)$ *in natural numbers* x, y, x *and* $m > 2$, *when the matrix* A *has an eigennvalue* $\alpha = \frac{1+i\sqrt{3}}{2}$ *are given by the congruence formulas (32) with the above restrictions on* $\langle r_1, r_2, r_3 \rangle$ *and if the matrix* A *is a nilpotent matrix with nilpotency index* $k \geq 2$ *then* $(\star)$ *is satisfied by all positive integers* $x, y, z, m > 2$ *such that* $mx \geq k, my \geq k$ *and* $mz \geq k$.

Remark. We note that Theorem with Corollary is equivalent to the result presented by M. H. Le and Ch. Li in [9], but our proof is given in another way and it gives more information about the impossibility of the solvability of $(\star)$ in the cases mentioned in Lemma 3, 4, 5.

References

[1] X. CHEN, On Fermat's equation in the set of generalized Fibonacci matrices, *Discuss. Math., Algebra and Stochastic Methods* **17** (1997), 5–8.

[2] R. Z. DOMIATY, Solutions of $x^4+y^4=z^4$ in 2×2 integral matrices, *Amer. Math. Monthly.* **73** (1966), 631.

[3] D. FREJMAN, On Fermat's equation in the set of Fibonacci matrices, *Discuss. Math.* **13** (1993), 61–64.

[4] A. GRYTCZUK, On Fermat's equation in the set of integral 2×2 matrices, *Period. Math. Hungar.* **30** (1995), 67–72.

[5] A. GRYTCZUK, Note on Fermat's type equation in the set of $n\times n$ matrices, *Discuss. Math., Algebra and Stochastic Methods*, **17** (1997), 19–23.

[6] A. GRYTCZUK and K. GRYTCZUK, *Functional recurrences Applications of Fibonacci Numbers*, Ed. G. E. Bergum et al., by Kluwer Acad. Publ., Dordrecht, 1990, 115–121.

[7] A. KHAZANOV, Fermat's equation in matrices, *Serdica Math. J.* **21** (1995), 19–40.

[8] M. H. LE and CH. LI, A note on Fermat's equation in integral 2×2 matrices, *Discuss. Math., Algebra and Stochastic Methods*, **15** (1995), 135–136.

[9] M. H. LE and CH. LI , On Fermat's equation in integral 2×2 matrices, *Period. Math. Hungar.* **31** (1995), 219–222.

[10] P.RIBENBOIM, *13 Lectures on Fermat's Last Theorem*, Springer Verlag, 1979.

[11] R. TAYLOR and A. WILES, Ring-theoretic properties of certain Hecke algebras, *Annals of Math.* **141** (1995), 553–572.

[12] A. WILES, Modular elliptic curves and Fermat's Last Theorem, *Annals of Math.* **141** (1995), 443–551.

ALEKSANDER GRYTCZUK
INSTITUTE OF MATHEMATICS
DEPARTMENT OF ALGEBRA AND NUMBER THEORY
T. KOTARBINSKI PEDAGOGICAL UNIVERSITY
65-069 ZIELONA GÓRA, POLAND

Egy euklidészi gyűrű

KIRÁLY BERTALAN,* OROSZ GYULÁNÉ

Abstract. We showe in this paper that the polynomial ring over a field of the infinite cyclic group is an Euclidean one.

Legyen $R\langle g\rangle$ a $\langle g\rangle$ végtelen ciklikus csoport T test fölötti csoportgyűrűje. A $T\langle g\rangle$ minden eleme felírható

$$x = \sum_{i\in Z} \alpha_i g^i, \qquad \alpha_i \in T \tag{1}$$

alakban, ahol csak véges sok $\alpha_i \neq 0$. Könnyű belátni, hogy a $T[g]$ és $T[g^{-1}]$ polinomgyűrűk (ha úgy tekintünk a g-re, ill. a g^{-1}-re mint határozatlanokra) a $T\langle g\rangle$ részgyűrűi.

Ismeretes, hogy a test fölötti egyhatározatlanú polinomok gyűrűje euklidészi gyűrű. Az euklidészi gyűrűk fontos szerepet játszanak a matematikában, többek között az algebrában és a számelméletben is. Ez annak tulajdonítható, hogy egész sor olyan tulajdonsággal rendelkeznek, amelyek megkönnyítik alkalmazásukat (pl. az euklidészi gyűrűk főideálgyűrűk, érvényes bennük az egyértelmű prímfaktorizáció tétele, legnagyobb közös osztó létezése stb.). Az is ismeretes, hogy a test fölötti kéthatározatlanú polinomok gyűrűje nem euklidészi gyűrű. A $T\langle g\rangle$ csoportgyűrűt nem tekinthetjük sem egyhatározatlanú, sem pedig kéthatározatlanú polinomgyűrűnek. Bebizonyítjuk, hogy ennek ellenére a $T\langle g\rangle$ euklidészi gyűrű.

Tétel. *A végtelen ciklikus csoport test fölötti csoportgyűrűje euklidészi gyűrű.*

A tétel bizonyításához szükségünk lesz néhány jól ismert fogalomra és állításra.

Ismeretes, hogy a gyűrű egységeinek halmaza a szorzásra nézve csoportot alkot amelyet $U(R)$-rel fogunk jelölni és az R gyűrű egységcsoportjának fogunk nevezni.

A továbbiakban R integritástartományt fog jelölni, azaz kommutatív, egységelemes, nullosztómentes gyűrűt.

* A kutatást az OTKA T16432 sz. pályázata támogatta.

Az a elemet a b $(a, b \in R)$ *asszociáltjának* nevezzük, ha $a = \varepsilon b$ valamely $\varepsilon \in U(R)$ elem esetén. Ezt $a \sim b$-vel jelöljük. Könnyű belátni, hogy a $\sim$ ekvivalenciareláció az R-en. Ezért a továbbiakban úgy is mondhatjuk, hogy az a és b elemek asszociáltak.

Definíció. A $T\langle g\rangle$ csoportgyűrű

$$x' = 1 + \sum_{0<i\in Z} \alpha_i g^i, \qquad \alpha_i \in T$$

alakú elemeit normált elemeknek nevezzük.

Világos, hogy ha x' normált elem, akkor $x' \in T[g] \subset T\langle g\rangle$.

1. Lemma. *A $T\langle g\rangle$ csoportgyűrűben igazak a következő állítások:*

1. Minden $x \neq 0$ $T\langle g\rangle$-beli elemhez létezik olyan egyértelműen meghatározott x' normált elem, hogy $x \sim x'$ és egy megfelelő α $(\alpha \in T)$ és egy meghatározott k egész számmal teljesül az

$$x = \alpha g^k x' \tag{2}$$

egyenlőség. Az x' elemet az x normáltjának fogjuk nevezni.

2. Ha x' és y' normált elemek, akkor az $x'y'$ is normált elem.

3. Tetszőleges nem nulla x, y $T\langle g\rangle$-beli elemek esetén igaz az

$$(xy)' = x'y',$$

egyenlőség.

Bizonyítás. 1. Legyen $x \in T\langle g\rangle$. Akkor az (1) szerint x előállítható

$$x = \sum_{i\in Z} \alpha_i g^i, \qquad \alpha_i \in T$$

alakban, ahol csak véges sok $\alpha_i \neq 0$. Legyen

$$k = \min_{\alpha_i \neq 0} \{i\}$$

és

$$x' = \alpha_k^{-1} g^{-k} x = \alpha_k^{-1} g^{-k} \sum_{i\in Z} \alpha_i g^i = 1 + \sum_{\substack{i\in Z \\ i\neq k}} \alpha_k^{-1} g^{-k} \alpha_i g^{i-k}.$$

Mivel $i - k \geq 0$, az x' elem felírásában a g-nek csak nemnegatív hatványai szerepelnek. Így

$$x' = 1 + \sum_{0<j\in Z} \delta_i g^i$$

alakú, vagyis x' normált elem. Az

$$x' = \alpha_k^{-1} g^{-k} x$$

egyenlőségekből nyerjük, hogy

$$x = \alpha_k g^k x'.$$

Tehát x előállítható (2) alakban és $x \sim x'$.

2. Legyen $x' = 1 + \sum_{0<i\in Z} \alpha_i g^i$ és $y' = 1 + \sum_{0<i\in Z} \beta_i g^i$. Az x', y' a $T[g]$ polinomgyűrű elemei és

$$x'y' = 1 + \sum_{0<i\in Z} \gamma_i g^i \in T[g],$$

azaz $x'y'$ normált elem.

3. A (2) szerint x és y felírható

$$x = \alpha g^k x' \qquad \text{és} \qquad y = \beta g^n y', \qquad (\alpha, \beta \in T,\ k, n \in Z)$$

alakban. Ezért

$$xy = \alpha\beta g^{k+n} x'y' = \alpha\beta g^{k+n}(1 + \sum_{0<i\in Z} \delta_i g^i) \in T[g]. \tag{3}$$

Innen következik, hogy $(xy)' = x'y'$.

A továbbiakban a (2)-re való hivatkozás nélkül is fogjuk alkalmazni a $T\langle g\rangle$-beli elemek (2) alakú előállítását.

2. Lemma. *A $T\langle g\rangle$ egységcsoportjának elemei γg^i $(\gamma \in R, i \in Z)$ alakúak.*

Bizonyítás. Legyen $x \in U(T\langle g\rangle)$. Az előző Lemma értelmében x és x^{-1} előállíthatók

$$x = \alpha g^k x' \qquad \text{és} \qquad x^{-1} = \beta g^n y' \qquad (\alpha, \beta \in T, \qquad k, n \in Z)$$

alakban. Ekkor figyelembe véve azt, hogy x' és y' normált elemek az

$$x'y' = 1 + \sum_{0<i\in Z} \delta_i g^i \in T[g]$$

egyenlőségből kapjuk, hogy

$$1 = xx^{-1} = \alpha\beta g^{k+n}x'y' = \alpha\beta g^{k+n}(1 + \sum_{0<i\in Z} \delta_i g^i). \tag{4}$$

Mivel x', y' és $x'y'$ a $T[g]$ elemei a (4) csak abban az esetben teljesül, ha $x' = y' = 1$. Tehát $x = \alpha g^k$ és $y = \beta g^n$.

3. Lemma. *A $T\langle g\rangle$ csoportgyűrűben az asszociált elemek normáltja megegyezik. Azaz, ha $x \sim y$, akkor $x' = y'$.*

Bizonyítás. Ha $x \sim y$, akkor található olyan ε ($\varepsilon \in U(T\langle g\rangle)$), hogy $x = \varepsilon y$ A 2. Lemma szerint $\varepsilon = \gamma g^m$ ($\gamma \in T, m \in Z$). Evidens, hogy $\varepsilon' = 1$. Ekkor az 1. Lemma értelmében

$$x' = (\varepsilon y)' = \varepsilon' y' = y'.$$

4. Lemma. *A $T\langle g\rangle$ nullosztómentes gyűrű.*

Bizonyítás. Tegyük fel, hogy x és y nem nulla $T\langle g\rangle$-beli elemek és $xy = 0$. Ekkor felhasználva az x és y elemek $x = \alpha g^k x'$ és $y = \beta g^n y'$ ($\alpha\beta \in T$, $k, n \in Z$) előállítását normáltjaik segítségével, az $xy = 0$-ból az

$$xy = \alpha\beta g^{k+n}x'y' = 0$$

következik. Mivel $\alpha\beta g^{k+n} \in U(T\langle g\rangle)$, innen az $x'y' = 0$ egyenlőséget kapjuk. Ez ellentmondás, mert $x' \neq 0$, $y' \neq 0$ és $x', y' \in T[g]$.

Jelöljük Z^+-szal a nemnegatív egész számok halmazát.

Definíció. Az R integritástartomány euklidészi gyűrűnek nevezzük, ha létezik olyan

$$\varphi: R \setminus \{0\} \to Z^+$$

leképezés, hogy minden $a, b \in R \setminus \{0\}$ elempárra igaz a $\varphi(ab) \geq \varphi(a)$ egyenlőtlenség. Továbbá, tetszőleges a és $b \neq 0$ R-beli elemekre teljesül a következő egyenlőség:

$$a = bq + r, \qquad \text{ahol vagy } r = 0, \text{ vagy } \varphi(r) < \varphi(b), \ (r, q \in R). \tag{5}$$

A φ leképezést euklidészi normának, az (5)-öt pedig euklidészi osztásnak nevezzük.

Legyen $x = \sum_{0<i\in Z} \alpha_i g^i \in T[g] \subset T\langle g\rangle$. Ekkor $x = \alpha_k g^k x'$. Evidens, hogy $k \geq 0$. Jelöljük x°-rel az x polinom fokát. Figyelembe véve, hogy $k \geq 0$ az előző egyenlőségből következik, hogy

$$x^\circ \geq (x')^\circ. \tag{6}$$

A Tétel bizonyítása. Legyen $x \in T\langle g\rangle \setminus \{0\}$ és legyen

$$x' = 1 + \sum_{0<i\in Z} \alpha_i g^i$$

az x normáltja. Nyilván $x' \in T[g]$. Legyen $\deg x = (x')^\circ$. A $\deg x$-et az x *elem módosított fokszámának* fogjuk nevezni. Könnyű belátni, hogy a $\deg v = \deg w$ egyenlőség pontosan akkor teljesül, ha $v \sim w$, és a $\deg x = 0$ egyenlőség akkor és csak akkor igaz, ha $x \in U(T\langle g\rangle)$.

Legyen $x, y \in T\langle g\rangle \setminus \{0\}$. Akkor $x = \varepsilon x'$ és $y = \delta y'$, ahol x', y' megfelelően az x, ill. az y normáltja és $\varepsilon, \delta \in U(T\langle g\rangle)$. Az 1. Lemma 3. pontja szerint $(xy)' = x'y'$, és mivel $x'y' \in T[g]$,

$$\deg(xy) = ((xy)')^\circ = (x'y')^\circ = (x')^\circ + (y')^\circ = \deg x + \deg y. \tag{7}$$

Legyen

$$\varphi: T\langle g\rangle \setminus \{0\} \to Z^+, \qquad \varphi(x) = \deg x. \tag{8}$$

Megmutatjuk, hogy φ a $T\langle g\rangle$ euklidészi normája. Ha $x, y \in T\langle g\rangle \setminus \{0\}$, akkor a (7)-ből kapjuk, hogy

$$\varphi(xy) = \deg(xy) = \deg x + \deg y \geq \deg x = \varphi(x).$$

és így a φ euklidészi norma a $T\langle g\rangle$-n.

Legyen $x, y \in T\langle g\rangle$ és $y \neq 0$. Írjuk fel az x-et és az y-t $x = \varepsilon x'$ és $y = \delta y'$ $(\varepsilon, \delta \in U(T\langle g\rangle)$ alakban. Ha $x = 0$, vagy $\varphi(x) < \varphi(y)$, akkor $x = y \cdot 0 + x$ és az (5) teljesül.

Legyen most $\varphi(x) \geq \varphi(y)$. Ekkor $\varphi(x) = \varphi(x') \geq \varphi(y) = \varphi(y')$. A $T[g]$ polinomgyűrűben érvényes az euklidészi osztás, és mivel x', y' $T[\langle g\rangle$-beli elemek, igaz a következő egyenlőség:

$$x' = y'q + r, \quad \text{ahol} \quad r = 0 \quad \text{vagy} \quad r^\circ < (y')^\circ \qquad (q, r \in T[g] \subset T\langle g\rangle).$$

Ekkor a (6)-ból következik, hogy $\deg r = (r')^\circ \leq (y')^\circ = \deg y$ és így $\varphi(r) \leq \varphi(y')$. Tehát

$$x' = y'q + r, \quad \text{ahol} \quad r = 0 \quad \text{vagy} \quad \varphi(r) < \varphi(y'). \tag{9}$$

Ha $x = \varepsilon x'$ és $y = \delta y'$ $(\varepsilon, \delta \in U(T\langle g \rangle))$, akkor a (9)-ből kapjuk, hogy $\delta\varepsilon x' = \delta x = \delta\varepsilon y' q + \delta\varepsilon r$ és így

$$x = y\overline{q} + \overline{r},$$

ahol $\overline{q} = \varepsilon\delta^{-1}q, \overline{r} = \varepsilon r$. Mivel $\overline{q} \sim q$ és $\overline{r} \sim r$, és az asszociált elemek módosított fokszáma megegyezik, a (9)-ből következik, hogy az előző egyenlőségben vagy $\overline{r} = 0$, vagy $\varphi(\overline{r}) < \varphi(y)$. Tehát a $T\langle g \rangle$ euklidészi gyűrű.

Irodalom

[1] B. L. Van der Warden, *Algebra I.*, Berlin · Heidelberg · New York.

Király Bertalan
Eszterházy Károly Tanárképző Főiskola
Matematika Tanszék
Leányka u. 4.
3301 Eger, Pf. 43.
E-mail: kiraly@ektf.hu

Dr. Orosz Gyuláné
Eszterházy Károly Tanárképző Főiskola
Matematika Tanszék
Leányka u. 4.
3301 Eger, Pf. 43.

Functions having quadratic differences in a given class

GYULA MAKSA

Abstract. Starting from a problem of Z. Daróczy we define the quadratic difference property and show that the class of all real-valued continuous functions on $\mathbf{R}$ and some of its subclasses have this property while the class of all bounded functions does not have.

1. Introduction

For a function $f: \mathbf{R} \to \mathbf{R}$ (the reals) and for a fixed $y \in \mathbf{R}$ define the function $\Delta_y f$ on $\mathbf{R}$ by $\Delta_y f(x) = f(x+y) - f(x)$, $x \in \mathbf{R}$. The functions $A, N: \mathbf{R} \to \mathbf{R}$ are said to be additive and quadratic if

$$A(x+y) = A(x) + A(y) \qquad x, y \in \mathbf{R}$$

and

$$N(x+y) + N(x-y) = 2N(x) + 2N(y) \qquad x, y \in \mathbf{R},$$

respectively. It is well-known (see [1], [5], [2]) that, if an additive function is bounded from one side on an interval of positive length then $A(x) = cx$, $x \in \mathbf{R}$ for some $c \in \mathbf{R}$ and there are discontinuous additive functions. Similarly, if a quadratic function is bounded on an interval of positive length then $N(x) = dx^2$, $x \in \mathbf{R}$ for some $d \in \mathbf{R}$ and there are discontinuous quadratic functions.

In [4] Z. DARÓCZY asked that for which properties T the following statement is true:

$(*)$ Let $f: \mathbf{R} \to \mathbf{R}$ be a function such that for all fixed $y \in \mathbf{R}$ the function $\Delta_y \Delta_{-y} f$ has the property T. Then

$$f = f^* + N + A \qquad \text{on} \quad \mathbf{R} \tag{1}$$

This research has been supported by grants from the Hungarian National Foundation for Scientific Research (OTKA) (No. T-016846) and from the Hungarian High Educational Research and Development Fund (FKFP) (No. 0310/1997).

where f^* has the property T, N is a quadratic function and A is an additive function.

In this note we prove that, if T is the k-times continuously differentiability ($k \geq 0$ integer) or k-times differentiability ($k > 0$ integer or $k = +\infty$) or being polynomial then the statement $(*)$ is true while if T is the boundedness then $(*)$ is not true.

2. Preliminary results

The following lemma will play an important role in our investigations.

Lemma 1. *For all functions $f: \mathbf{R} \to \mathbf{R}$ and for all $u, v, x \in \mathbf{R}$ we have*

$$\begin{aligned}\Delta_u \Delta_v f(x) = {} & \Delta_{\frac{u-v}{2}} \Delta_{-\frac{u-v}{2}} f\left(x + \frac{u+v}{2}\right) \\ & - \Delta_{\frac{u+v}{2}} \Delta_{-\frac{u+v}{2}} f\left(x + \frac{u+v}{2}\right).\end{aligned} \tag{2}$$

The proof is a simple computation therefore it is omitted.

An other basic tool we will use is the following result of DE BRUIJN ([3] Theorem 1.1.)

Theorem 1. *Suppose that $f: \mathbf{R} \to \mathbf{R}$ is a function such that the function $\Delta_y f$ is continuous for all fixed $y \in \mathbf{R}$. Then $f = f^* + A$ on $\mathbf{R}$ with some continuous $f^*: \mathbf{R} \to \mathbf{R}$ and additive $A: \mathbf{R} \to \mathbf{R}$.*

Finally we will need the following two lemmata.

Lemma 2. *Let $f: \mathbf{R} \to \mathbf{R}$ be a function such that $\Delta_u \Delta_v f$ is continuous for all fixed $u, v \in \mathbf{R}$. Define*

$$H(x, u, v) = \Delta_u \Delta_v f(x) - f(u + v) + f(u) + f(v) \qquad x, u, v \in \mathbf{R}. \tag{3}$$

Then the function $(x, u) \to H(x, u, v)$, $(x, u) \in \mathbf{R}^2$ is continuous for all fixed $v \in \mathbf{R}$.

Proof. Let $v \in \mathbf{R}$ be fixed. Since $\Delta_u(\Delta_v f)$ is continuous for all fixed $u \in \mathbf{R}$, Theorem 1 implies that $\Delta_v f = f_v^* + A_v$ on $\mathbf{R}$ where $f_v^*: \mathbf{R} \to \mathbf{R}$ is continuous and A_v is additive. Thus, by (3),

$$\begin{aligned} H(x, u, v) &= \Delta_v f(x + u) - \Delta_v f(x) - \Delta_v f(u) + f(v) \\ &= f_v^*(x + u) - f_v^*(x) - f_v^*(u) + f(v) \end{aligned}$$

whence the continuity of $(x, u) \to H(x, u, v)$, $(x, u) \in \mathbf{R}^2$ follows.

Lemma 3. *Suppuse that L is one of the classes of the real-valued functions defined on $\mathbf{R}$ which are k-times continuously differentiable for some $k \geq 0$ integer or k-times differentiable for some $1 \leq k \leq +\infty$ or polynomials. If $f: \mathbf{R} \to \mathbf{R}$ is continuous and $\Delta_y f \in L$ for all fixed $y \in \mathbf{R}$ then $f \in L$.*

Proof. If L is the class of the continuous functions ($k = 0$) or of the polynomials, furthermore f is continuous and $\Delta_y f \in L$ for all fixed $y \in \mathbf{R}$ then, by Theorem 1 and by [3] page 203, respectively, $f = f^* + A$ for some $f^* \in L$ and additive function A. Therefore, by continuity of f, $A(x) = cx$, $x \in \mathbf{R}$ with some $c \in \mathbf{R}$ whence $f \in L$ follows.

The remaining statement of Lemma 3 is just Lemma 3.1. in [3].

3. The main results

For the formulation of our main results let us begin with the following

Definition. A subset E of the set of all functions $f: \mathbf{R} \to \mathbf{R}$ is said to have the quadratic difference property if for all $f: \mathbf{R} \to \mathbf{R}$, with $\Delta_y \Delta_{-y} f \in E$ for all $y \in \mathbf{R}$, the decomposition (1) holds true on $\mathbf{R}$ where $f^* \in E$, N is a quadratic function and A is an additive function.

First we prove the following

Theorem 2. *The class of all continuous functions $f: \mathbf{R} \to \mathbf{R}$ has the quadratic difference property.*

Proof. By (2) in Lemma 1 we have that $\Delta_u \Delta_v f$ is continuous for all fixed $u, v \in \mathbf{R}$. In particular, $\Delta_u(\Delta_1 f)$ is continuous for all fixed $u \in \mathbf{R}$. Applying Theorem 1 to $\Delta_1 f$ we have

$$\Delta_1 f = f_0 + a \qquad \text{on } \mathbf{R} \tag{4}$$

with some continuous $f_0: \mathbf{R} \to \mathbf{R}$ and additive $a: \mathbf{R} \to \mathbf{R}$. Define the function B on $\mathbf{R}^2$ by

$$B(u,v) = \int_0^1 \Delta_u \Delta_v f - \int_0^{u+v} f_0 + \int_0^u f_0 + \int_0^v f_0, \qquad (u,v) \in \mathbf{R}^2. \tag{5}$$

Obviously, B is symmetric. Now we show that B is additive in its first variable. For all u, t and v, we have

$$B(u+t,v) - B(u,v) = \int_0^1 \Delta_{u+t} \Delta_v f - \int_0^{u+t+v} f_0 + \int_0^{u+t} f_0 + \int_0^v f_0$$

$$-\int_0^1 \Delta_u\Delta_v f + \int_0^{u+v} f_0 - \int_0^u f_0 - \int_0^v f_0$$
$$= \int_u^{u+1} \Delta_t\Delta_v f - \int_0^{u+t+v} f_0 + \int_0^{u+t} f_0 + \int_0^{u+v} f_0 - \int_0^u f_0.$$

Since $\Delta_t\Delta_v f$ and f_0 are continuous functions, the right hand side is continuously differentiable with respect to u then so is the left hand side. Differentiating both sides with respect to u and taking into consideration (4) we obtain that

$$\begin{aligned}\frac{\partial}{\partial u}[B(u+t,v) - B(u,v)] &= \Delta_t\Delta_v\Delta_1 f(u) - f_0(u+t+v) + f_0(u+t)\\ &\quad + f_0(u+v) - f_0(u)\\ &= \Delta_t\Delta_v(f_0+a)(u) - \Delta_t\Delta_v f_0(u)\\ &= \Delta_t\Delta_v a(u) = 0 \qquad (a \text{ being additive}).\end{aligned}$$

Therefore

$$B(u+t,v) - B(u,v) = B(t,v) - B(0,v) = B(t,v),$$

that is, B is additive in its first (and by the symmetry also in its second) variable. Thus, it is well-known (see [2]) and easy to see that, the function $N:\mathbf{R} \to \mathbf{R}$ defined by $N(u) = \frac{1}{2}B(u,u)$, $u \in \mathbf{R}$ is quadratic and

$$B(u,v) = N(u+v) - N(u) - N(v) \qquad u,v \in \mathbf{R}. \tag{6}$$

Define the function $H:\mathbf{R}^3 \to \mathbf{R}$ by (3) and apply Lemma 2 to get the continuity of the function $(x,u) \to H(x,u,v)$, $(x,u) \in \mathbf{R}^2$ for all fixed $v \in \mathbf{R}$. This implies that the function $s:\mathbf{R}^2 \to \mathbf{R}$ defined by

$$s(u,v) = \int_0^1 H(x,u,v)dx \qquad (u,v) \in \mathbf{R}^2$$

is continuous in its first variable (for all fixed $v \in \mathbf{R}$). Therefore, by (3), (5) and (6) we have

$$s(u,v) = \int_0^1 \Delta_u\Delta_v f - f(u+v) + f(u) + f(v)$$

$$= B(u,v) + \int_0^{u+v} f_0 - \int_0^{u} f_0 - \int_0^{v} f_0 - f(u+v) + f(u) + f(v)$$

$$= N(u+v) - f(u+v) - (N(u) - f(u)) - (N(v) - f(v))$$

$$+ \int_0^{u+v} f_0 - \int_0^{u} f_0 - \int_0^{v} f_0$$

$$= -\Delta_v(f-N)(u) - (N(v) - f(v)) + \int_0^{u+v} f_0 - \int_0^{u} f_0 - \int_0^{v} f_0.$$

This implies that $\Delta_v(f-N)$ is continuous for all fixed $v \in \mathbf{R}$ and Theorem 1 can be applied again to get the decomposition $f - N = f^* + A$ on $\mathbf{R}$ with some continuous $f^*: \mathbf{R} \to \mathbf{R}$ and additive function A, that is, (1) holds and the proof is complete.

Theorem 3. *Let L be as in Lemma 3. Then L has the quadratic difference property.*

Proof. If L is the class of all continuous functions then the statement is proved by Theorem 2. In the remaining cases, since all functions in L are continuous, Theorem 2 implies the decomposition (1) with continuous f^*, quadratic N and additive A. We now prove that $f^* \in L$. For all $y \in \mathbf{R}$ we get from (1) that

$$\Delta_y \Delta_{-y} f = \Delta_y \Delta_{-y} f^* + 2N(y). \tag{7}$$

Therefore $\Delta_y \Delta_{-y} f^* \in L$ for all fixed $y \in \mathbf{R}$. Applying (2) in Lemma 1 we obtain that $\Delta_u(\Delta_v f^*) \in L$ for all fixed $u, v \in \mathbf{R}$. Obviously $\Delta_v f^*$ is continuous thus, by Lemma 3, $\Delta_v f^* \in L$. Since f^* is continuous, Lemma 3 can be applied again to get $f^* \in L$.

Remark. The set of all bounded functions $f: \mathbf{R} \to \mathbf{R}$ does not have the quadratic difference property. Indeed, let

$$f(x) = x \ln(x^2+1) + 2 \operatorname{arc\,tg} x - 2x, \qquad x \in \mathbf{R}.$$

Applying the Lagrangian mean value theorem with fixed $u, v, x \in \mathbf{R}$ we have

$$\Delta_u \Delta_v f(x) = u \Delta_v f'(\xi) = uv f''(\eta) \tag{8}$$

for some $\xi, \eta \in \mathbf{R}$. Since $|f''(\eta)| = \frac{2|\eta|}{\eta^2+1} \leq 1$, (8) implies that $|\Delta_y \Delta_{-y} f(x)| \leq y^2$ for all $x, y \in \mathbf{R}$, that is, $\Delta_y \Delta_{-y} f$ is bounded for all fixed $y \in \mathbf{R}$. Suppose that f has the decomposition (1) for some bounded $f^\star: \mathbf{R} \to \mathbf{R}$, quadratic N and additive A. Then $N + A$ must be bounded on any bounded interval. Thus $N(x) + A(x) = \alpha x^2 + \beta x$, $x \in \mathbf{R}$ for some $\alpha, \beta \in \mathbf{R}$. This and (1) imply that

$$(9) \qquad f^\star(x) = x \ln(x^2 + 1) + 2 \operatorname{arc\,tg} x - \alpha x^2 - (2 + \beta)x, \qquad x \in \mathbf{R}.$$

Since $f^\star$ is bounded, $0 = \lim\limits_{x \to +\infty} \frac{f^\star(x)}{x^2} = -\alpha$ and thus

$$0 = \lim_{x \to +\infty} \frac{f^\star(x) - 2 \operatorname{arc\,tg} x}{x} = \lim_{x \to +\infty} \left(\ln(x^2 + 1) - (2 + \beta) \right),$$

which is a contradiction. This shows that the set of all bounded functions does not have the quadratic difference property.

References

[1] Aczél, *Lectures on Functional Equations and Their Applications*, Academic Press, New York and London, 1966.

[2] J. Aczél, The general solution of two functional equations by reduction to functions additive in two variables and with the aid of Hamel bases, *Glasnik Mat.-Fiz. Astr.*, **20** (1965), 65–73.

[3] N. G. de Bruijn, Functions whose differences belong to a given class, *Nieuw Arch. Wisk.*, **23** no. 2 (1951), 194–218.

[4] Z. Daróczy, 35. Remark, *Aequationes Math.*, **8** (1972), 187–188.

[5] M. Kuczma, *An Introduction to the Theory of Functional Equations and Inequalities, Cauchy's Equation and Jensen's Inequality*, Panstowowe Wydawnictwo Naukowe, Warszawa · Kraków · Katovice, 1985.

Gyula Maksa
Lajos Kossuth University
Institute of Mathematics and Informatics
4010 Debrecen P.O. Box 12.
Hungary
E-mail: maksa@math.klte.hu

On a theorem of type Hardy–Littlewood with respect to the Vilenkin-like systems

GYÖRGY GÁT

Abstract. In this paper we give a convergence test for generalized (by the author) Vilenkin–Fourier series. This convergence theorem is of type Hardy–Littlewood for the ordinary Vilenkin system is proved in 1954 by Yano.

Introduction and the result

First we introduce some necessary definitions and notations of the theory of the Vilenkin systems. The Vilenkin systems were introduced by N. JA. VILENKIN in 1947 (see e.g. [7]). Let $m := (m_k, k \in \mathbf{N})$ $(\mathbf{N} := \{0, 1, \ldots\})$ be a sequence of integers each of them not less than 2. Let Z_{m_k} denote the m_k-th discrete cyclic group. Z_{m_k} can be represented by the set $\{0, \ldots, m_k - 1\}$, where the group operation is the mod m_k addition and every subset is open. The measure on Z_{m_k} is defined such that the measure of every singleton is $1/m_k$ $(k \in \mathbf{N})$. Let

$$G_m := \bigtimes_{k=0}^{\infty} Z_{m_k}.$$

This gives that every $x \in G_m$ can be represented by a sequence $x = (x_i, i \in \mathbf{N})$, where $x_i \in Z_{m_i}$ $(i \in \mathbf{N})$. The group operation on G_m (denoted by $+$) is the coordinate-wise addition (the inverse operation is denoted by $-$), the measure (denoted by μ) and the topology are the product measure and topology. Consequently, G_m is a compact Abelian group. If $\sup_{n \in \mathbf{N}} m_n < \infty$, then we call G_m a bounded Vilenkin group. If the generating sequence m is not bounded, then G_m is said to be an unbounded Vilenkin group. The boundedness of the group G_m is supposed over all of this paper and denote by $\sup_{n \in \mathbf{N}} m_n < \infty$. c denotes an absolute constant (may depend only on $\sup_n m_n$) which may not be the same at different occurences.

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

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

Research supported by the Hungarian National Research Science Foundation, Operating Grant Number OTKA F020334.

for $x \in G_m$, $n \in \mathbf{P} := \mathbf{N} \setminus \{0\}$. Let $0 = (0, i \in \mathbf{N}) \in G_m$ denote the nullelement of G_m, $I_n := I_n(0)$ $(n \in \mathbf{N})$. Let $\mathcal{I} := \{I_n(x) : x \in G_m,\ n \in \mathbf{N}\}$. The elements of $\mathcal{I}$ are called intervals on G_m.

Furthermore, let $L^p(G_m)$ $(1 \leq p \leq \infty)$ denote the usual Lebesgue spaces ($|\ .\ |_p$ the corresponding norms) on G_m, $\mathcal{A}_n$ the σ algebra generated by the sets $I_n(x)$ $(x \in G_m)$ and E_n the conditional expectation operator with respect to $\mathcal{A}_n$ $(n \in \mathbf{N})$ $(f \in L^1$.)

Let $M_0 := 1$, $M_{n+1} := m_n M_n$ $(n \in \mathbf{N})$ be the generalized powers. Then each natural number n can be uniquely expressed as

$$n = \sum_{i=0}^{\infty} n_i M_i \quad (n_i \in \{0, 1, \ldots, m_i - 1\},\ i \in \mathbf{N}),$$

where only a finite number of n_i's differ from zero. The generalized Rademacher functions are defined as

$$r_n(x) := \exp(2\pi \imath \frac{x_n}{m_n}) \quad (x \in G_m,\ n \in \mathbf{N},\ \imath := \sqrt{-1}).$$

Then

$$\psi_n := \prod_{j=0}^{\infty} r_j^{n_j} \quad (n \in \mathbf{N})$$

the nth Vilenkin function. The system $\psi := (\psi_n : n \in \mathbf{N})$ is called a Vilenkin system. Each ψ_n is a character of G_m and all the characters of G_m are of this form. Define the m-adic addition as

$$k \oplus n := \sum_{j=0}^{\infty} (k_j + n_j \pmod{m_j}) M_j \quad (k, n \in \mathbf{N}).$$

Then, $\psi_{k \oplus n} = \psi_k \psi_n$, $\psi_n(x + y) = \psi_n(x)\psi_n(y)$, $\psi_n(-x) = \bar{\psi}_n(x)$, $|\psi_n| = 1$ $(k, n \in \mathbf{N},\ x, y \in G_m)$.

Let functions $\alpha_n, \alpha_j^{(k)} : G_m \to \mathbf{C}$ $(n, j, k \in \mathbf{N})$ satisfy:

(i) $\alpha_j^{(k)}$ is measurable with respect to $\mathcal{A}_j$ $(j, k \in \mathbf{N})$,

(ii) $|\alpha_j^{(k)}| = \alpha_j^{(k)}(0) = \alpha_0^{(k)} = \alpha_j^{(0)} = 1$ $(j, k \in \mathbf{N})$,

(iii) $\alpha_n := \prod_{j=0}^{\infty} \alpha_j^{(n^{(j)})}$, $n^{(j)} := \sum_{i=j}^{\infty} n_i M_i$ $(n \in \mathbf{N})$.

Let $\chi_n := \psi_n \alpha_n$ $(n \in \mathbf{N})$. The system $\{\chi_n : n \in \mathbf{N}\}$ is called a Vilenkin-like (or $\psi\alpha$) system ([2]–[4]).

We mention some examples.

1. If $\alpha_j^{(k)} = 1$ for each $k, j \in \mathbf{N}$, then we have the "ordinary" Vilenkin systems.

2. If $m_j = 2$ for all $j \in \mathbf{N}$ and $\alpha_j^{(n^{(j)})} = (\beta_j)^{(n_j)}$, where

$$\beta_j(x) = \exp\left(2\pi\imath\left(\frac{x_{j-1}}{2^2} + \cdots + \frac{x_0}{2^{j+1}}\right)\right) \quad (n, j \in \mathbf{N},\ x \in G_m),$$

then we have the character system of the group of 2-adic integers (see e.g. [5], [4]).

3. If

$$t_n(x) := \exp\left(2\pi\imath\left(\sum_{j=0}^{\infty}\frac{n_j}{M_{j+1}}\right)\sum_{j=0}^{\infty}x_jM_j\right) \quad (x \in G_m,\ n \in \mathbf{N}),$$

then we have a Vilenkin-like system which is usefull in the approximation theory of limit periodic, almost even arithmetical functions ([2], [4]).

In [3] we proved that a Vilenkin-like system is orthonormal and complete in $L^1(G_m)$. Define the Fourier coefficients, the partial sums of the Fourier series, the Dirichlet kernels with respect to the Vilenkin-like system χ as follows.

$$\hat{f}^{\chi}(n) = \hat{f}(n) := \int_{G_m} f\bar{\chi}_n, \qquad S_n^{\chi}f = S_nf := \sum_{k=0}^{n-1}\hat{f}^{\chi}(k)\chi_k,$$

$$D_n^{\chi}(y,x) = D_n(y,x) := \sum_{k=0}^{n-1}\chi_n(y)\bar{\chi}_n(x),$$

It is known ([2]) that

$$D_{M_n}(y,x) = D_{M_n}(y-x) = \begin{cases} M_n, & \text{if } y-x \in I_n(0), \\ 0, & \text{if } y-x \notin I_n(0), \end{cases}$$

$$S_{M_n}f(y) = M_n\int_{I_n(y)} f\,d\mu = E_nf(y) \quad (f \in L^1(G_m),\ n \in \mathbf{N})$$

and

$$D_n(y,x) = \chi_n(y)\bar{\chi}_n(x)\sum_{j=0}^{\infty}D_{M_j}(y-x)\sum_{p=m_j-n_j}^{m_j-1}r_j^p(x)$$

($x \in G_m$, $n \in \mathbf{N}$, $f \in L^1(G_m)$). Then, $y - x \notin I_s$ gives

$$|D_n(y,x)| \leq cM_s \ (s \in \mathbf{N}) \tag{1}$$

([2]). It is also known ([2]) that for $y - x \notin I_s$

$$\sum_{t=0}^{M_s-1} \chi_{jM_s+t}(y)\bar{\chi}_{jM_s+t}(x) = 0 \ (j \in \mathbf{N}). \tag{2}$$

Moreover,

$$S_n^{\chi} f(y) = \int_{G_m} f(x) D_n(y,x)\, d\mu$$

($n \in \mathbf{N}$, $y \in G_m$). For more details on Vilenkin-like systems see e.g. [2]–[4].

The following theorem of type Hardy–Littlewood for the ordinary Vilenkin system is proved in 1954 by YANO ([8]). We generalize this result for Vilenkin-like systems.

Theorem. *Suppose that the following two conditions hold for function $f \in L^1(G_m)$ and for a $y \in G_m$.*

(1) $M_n log M_n \int_{I_n} |f(x+y) - f(y)|\, d\mu(x) \to 0$ $(n \to \infty)$,

(2) $|\hat{f}(k)| \leq ck^{-\delta}$ for some $\delta > 0$.

Then $S_n f(y)$ converges to $f(y)$.

Proof. Denote by

$$M_n \log M_n \int_{I_n} |f(x+y) - f(y)|\, d\mu(x) =: \varepsilon_n \to 0. \tag{3}$$

(3) implies that

$$|S_{M_n} f(y) - f(y)| = M_n \left| \int_{I_n(y)} f(x) - f(y)\, d\mu(x) \right| \leq \frac{\varepsilon_n}{\log M_n} \tag{4}$$

for $n \in \mathbf{N}$. Let $k \in \mathbf{N}$ and $n \in \mathbf{N}$ for which $M_n \leq k < M_{n+1}$. Also, let $n \geq n_0 \in \mathbf{N}$ be some integer depend on n for which $r \leq n/n_0$ that is the ratio of n and n_0 has a lower bound, where constant $r \in \mathbf{N}$ is discussed later.

$$\begin{aligned} S_k f(y) &= \int_{G_m} f(x) \sum_{j=0}^{k-1} \chi_j(y)\bar{\chi}_j(x)\, d\mu(x) \\ &= \int_{G_m} f(x+y) \sum_{j=0}^{k-1} \chi_j(y)\bar{\chi}_j(x+y)\, d\mu(x) \end{aligned}$$

and

$$\int_{G_m} f(y) \sum_{j=M_n}^{k-1} \chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x) = 0$$

gives

$$(5)\quad S_k f(y) - S_{M_n} f(y) = \int_{G_m} (f(x+y) - f(y)) \sum_{j=M_n}^{k-1} \chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x).$$

In (5) we integrate over G_m which is the disjoint union of I_n, $I_{n_0} \setminus I_n$ and $G_m \setminus I_{n_0}$. Since sequence m is bounded, then we have

$$(6)\quad \begin{aligned} &\left| \int_{I_n} (f(x+y) - f(y)) \sum_{j=M_n}^{k-1} \chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x) \right| \\ &\leq (k - M_n) \int_{I_n} |f(x+y) - f(y)|\,d\mu(x) \leq c\varepsilon_n / \log M_n. \end{aligned}$$

By (1) we have

$$(7)\quad \begin{aligned} &\left| \int_{I_{n_0} \setminus I_n} (f(x+y) - f(y)) \sum_{j=M_n}^{k-1} \chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x) \right| \\ &\leq \sum_{s=n_0}^{n-1} cM_s \int_{I_s \setminus I_{s+1}} |f(x+y) - f(y)|\,d\mu(x) \leq \sum_{s=n_0}^{n-1} \frac{c\varepsilon_s}{\log M_s}. \end{aligned}$$

Finally, we have $x \in G_m \setminus I_{n_0}$. This by (2) implies

$$\sum_{s=n_0}^{n} \sum_{j=0}^{k_s-1} \sum_{l=0}^{M_s-1} \bar{\chi}_{k^{(s+1)}+jM_s+l}(x+y)\chi_{k^{(s+1)}+jM_s+l}(y) = 0.$$

Denote by

$$J(x+y, y) := \sum_{s=0}^{n_0-1} \sum_{j=0}^{k_s-1} \sum_{l=0}^{M_s-1} \bar{\chi}_{k^{(s+1)}+jM_s+l}(x+y)\chi_{k^{(s+1)}+jM_s+l}(y).$$

Then,

$$\begin{aligned}
&\left|\int_{G_m\setminus I_{n_0}}(f(x+y)-f(y))\sum_{j=M_n}^{k-1}\chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x)\right| \\
&=\left|\int_{G_m\setminus I_{n_0}}(f(x+y)-f(y))J(x+y,y)\,d\mu(x)\right| \\
&\le\left|\int_{I_{n_0}}(f(x+y)-f(y))J(x+y,y)\,d\mu(x)\right| \\
&+\left|\int_{G_m}(f(x+y)-f(y))J(x+y,y)\,d\mu(x)\right| \qquad (8)\\
&\le cM_{n_0}\int_{I_{n_0}}|f(x+y)-f(y)|\,d\mu(x) \\
&+\left|\int_{G_m}f(x+y)J(x+y,y)\,d\mu(x)\right| \\
&\le c\varepsilon_{n_0}/\log M_{n_0}+\sum_{s=0}^{n_0-1}\sum_{j=0}^{k_s-1}\sum_{l=0}^{M_s-1}|\hat{f}(k^{(s+1)}+jM_s+l)| \\
&\le c\varepsilon_{n_0}+c^{n_0}2^{-\delta n}\le c\varepsilon_{n_0}+\left(\frac{c}{2^{\delta r}}\right)^{n_0}.
\end{aligned}$$

At last by (4), (6), (7), (8), we get

$$\begin{aligned}
&|S_kf(y)-S_{M_n}f(y)|\le|S_{M_n}f(y)-f(y)| \\
&+\left|\int_{I_n}(f(x+y)-f(y))\sum_{j=M_n}^{k-1}\chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x)\right| \\
&+\left|\int_{I_{n_0}\setminus I_n}(f(x+y)-f(y))\sum_{j=M_n}^{k-1}\chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x)\right| \\
&+\left|\int_{G_m\setminus I_{n_0}}(f(x+y)-f(y))\sum_{j=M_n}^{k-1}\chi_j(y)\bar{\chi}_j(x+y)\,d\mu(x)\right| \\
&\le c\frac{\varepsilon_n}{\log M_n}+c\varepsilon_n/\log M_n+\sum_{s=n_0}^{n-1}\frac{c\varepsilon_s}{\log M_s}+c\varepsilon_{n_0}+\left(\frac{c}{2^{\delta r}}\right)^{n_0} \\
&\le c\varepsilon_{n_0}+c\varepsilon_n+\sup_{s\ge n_0}\varepsilon_s(1/n_0+\cdots+1/n)+\left(\frac{\tilde{c}}{2^{\delta r}}\right)^{n_0}\to 0
\end{aligned}$$

as $n \to \infty$, where constant $r \in \mathbf{N}$ is given as $\frac{\tilde{c}}{2^{\delta r}} < 1$ and $n_0 \to \infty$ (as $n \to \infty$) provided that $r \leq n/n_0$. That is the proof of the theorem is complete.

References

[1] AGAEV, G. H., VILENKIN, N. JA., DZHAFARLI, G. M., RUBINSTEIN, A. I., *Multiplicative systems of functions and harmonic analysis on 0-dimensional groups* (in Russian), Izd. ("ELM"), Baku, 1981.

[2] GÁT, G., Vilenkin–Fourier series and limit periodic arithmetic functions, *Colloq. Math. Soc. János Bolyai* **58**, Approx. Theory, Kecskemét, Hungary, 1990, 316–332.

[3] GÁT, G., Orthonormal systems on Vilenkin groups, *Acta Math. Hungar.*, **58** (1–2) (1991), 193–198.

[4] GÁT, G., On almost even arithmetical functions via orthonormal systems on Vilenkin groups, *Acta Arith.*, **49** (2) (1991), 105–123.

[5] HEWITT, E., ROSS, K., *Abstract Harmonic Analysis*, Springer-Verlag, Heidelberg, 1963.

[6] SCHIPP, F., WADE, W. R., SIMON, P., PÁL, J., *Walsh series, Introduction to dyadic harmonic analysis*, Adam Hilger, Bristol and New York, 1990.

[7] VILENKIN, N. JA., On a class of complete orthonormal systems (in Russian), *Izv. Akad. Nauk. SSSR, Ser. Math.* **11** (1947), 363 400.

[8] YANO, S., A convergence test for Walsh–Fourier series, *Tohoku Math. J.*, **6** (2–3) (1954), 226–230.

BESSENYEI COLLEGE
DEPARTMENT OF MATHEMATICS
NYÍREGYHÁZA, P.O. BOX 166.
H–4400 HUNGARY
E-mail: gatgy@ny2.bgytf.hu

*P-Finsler spaces with vanishing Douglas tensor

S. BÁCSÓ, I. PAPP

Abstract. The purpose of the present paper is to prove that a *P-Randers space with vanishing Douglas tensor is a Riemannian space if the dimension is greater then three.

1. Introduction

Let $F^n(M^n, L)$ be an n-dimensional Finsler space, where M^n is a connected differentiable manifold of dimension n and $L(x, y)$ is the fundamental function defined on the manifold $T(M)\backslash 0$ of nonzero tangent vectors. Let us consider a geodesic curve $x^i = x^i(t)$,[1] $(t_0 \leq t \leq t_1)$. The system of differential equations for geodesic curves of F^n with respect to canonical parameter t is given by

$$\frac{d^2x^i}{dt^2} = -2G^i(x, y), \quad y^i = \frac{dx^i}{dt},$$

where

$$G^i = \frac{1}{4}g^{ir}\left(y^s\left(\frac{\partial L^2_{(r)}}{\partial x^s}\right) - \frac{\partial L^2}{\partial x^r}\right),$$

$$g_{ij} = \frac{1}{2}L^2_{(i)(j)}, \quad (i) = \frac{\partial}{\partial y^i}, \text{ and } \left(g^{ij}\right) = \left(g_{ij}\right)^{-1}.$$

The Berwald connection coefficients $G^i_j(x, y)$, $G^i_{jk}(x, y)$ can be derived from the function G^i, namely $G^i_j = G^i_{(j)}$ and $G^i_{jk} = G^i_{j(k)}$. The Berwald covariant derivative with respect to the Berwald connection can be written as

$$T^i_{j;k} = \partial T^i_j/\partial x^k - T^i_{j(r)}G^r_k + T^r_j G^i_{rk} - T^i_r G^r_{jk}. \tag{1}$$

(Throughout the present paper we shall use the terminology and definitions described in Matsumoto's monograph [6].)

This work was partially supported by the Ministry of Culture and Education of Hungary under Grant No. FKFP 0457.

[1] The Roman indices run over the range 1,...,n.

2. Douglas tensor, Randers metric, *P-space

Let us consider two Finsler space $F^n\left(M^n, L\right)$ and $\overline{F}^n\left(M^n, \overline{L}\right)$ on a common underlying manifold M^n. A diffeomorphism $F^n \to \overline{F}^n$ is called geodesic if it maps an arbitrary geodesic of F^n to a geodesic of $\overline{F}^n$. In this case the change $L \to \overline{L}$ of the metric is called projective. It is well-known that the mapping $F^n \to \overline{F}^n$ is geodesic iff there exist a scalar field $p(x,y)$ satisfying the following equation

$$\overline{G}^i = G^i + p(x,y)y^i, \quad p \neq 0. \tag{2}$$

The projective factor $p(x,y)$ is a positive homogeneous function of degree one in y. From (2) we obtain the following equations

$$\overline{G}^i_j = G^i_j + p\delta^i_j + p_j y^i, \quad p_j = p_{(j)}, \tag{3}$$

$$\overline{G}^i_{jk} = G^i_{jk} + p_j\delta^i_k + p_k\delta^i_j + p_{jk}y^i, \quad p_{jk} = p_{j(k)}, \tag{4}$$

$$\overline{G}^i_{jkl} = G^i_{jkl} + p_{jk}\delta^i_l + p_{jl}\delta^i_k + p_{kl}\delta^i_j + p_{jkl}y^i, \quad p_{jkl} = p_{jk(l)}. \tag{5}$$

Substituting $p_{ij} = \left(\overline{G}_{ij} - G_{ij}\right)/(n+1)$ and $p_{ijk} = \left(\overline{G}_{ij(k)} - G_{ij(k)}\right)/(n+1)$ into (5) we obtain the so called Douglas tensor which is invariant under geodesic mappings, that is

$$D^i_{jkl} = G^i_{jkl} - \left(y^i G_{jk(l)} + \delta^i_j G_{kl} + \delta^i_k G_{jl} + \delta^i_l G_{jk}\right)/(n+1), \tag{6}$$

which is invariant under geodesic mappings, that is

$$D^i_{jkl} = \overline{D}^i_{jkl}. \tag{7}$$

We now consider some notions and theorems for special Finsler spaces.

Definition 1. ([1]) In an n-dimensional differentiable manifold M^n a Finsler metric $L(x,y) = \alpha(x,y) + \beta(x,y)$ is called Randers metric, where $\alpha(x,y) = \sqrt{a_{ij}(x)y^i y^j}$ is a Riemannian metric in M^n and $\beta(x,y) = b_i(x)y^i$ is a differential 1-form in M^n. The Finsler space $F^n = (M^n, L) = \alpha + \beta$ with Randers metric is called Randers space.

Definition 2. ([1]) The Finsler metric $L = \alpha^2/\beta$ is called Kropina metric. The Finsler space $F^n = (M^n, L) = \alpha^2/\beta$ with Kropina metric is called Kropina space.

Definition 3. ([1], [6]) A Finsler space of dimension $n > 2$ is called C-reducible, if the tensor $C_{ijk} = \frac{1}{2} g_{ij(k)}$ can be written in the form

$$C_{ijk} = \frac{1}{n+1} (h_{ij} C_k + h_{ik} C_j + h_{jk} C_i), \tag{8}$$

where $h_{ij} = g_{ij} - l_i l_j$ is the angular metric tensor and $l_i = L_{(i)}$.

Theorem 1. ([7]) *A Finsler space F^n, $n \geq 3$, is C-reducible iff the metric is a Randers metric or a Kropina metric.*

Definition 4. ([4], [5]) A Finsler space F^n is called *P-Finsler space, if the tensor $P_{ijk} = \frac{1}{2} g_{ij;k}$ can be written in the form

$$P_{ijk} = \lambda(x, y) C_{ijk}. \tag{9}$$

Theorem 2. ([4]) *For $n > 3$ in a C-reducible *P-Finsler space $\lambda(x, y) = k(x) L(x, y)$ holds and $k(x)$ is only the function of position.*

3. *P-Randers space with vanishing Douglas tensor

Definition 5. ([3]) A Finsler space is said to be of Douglas type or Douglas space, iff the functions $G^i y^j - G^j y^i$ are homogeneous polynomials in (y^i) of degree three.

Theorem 3. ([3]) *A Finsler space is of Douglas type iff the Douglas tensor vanishes identically.*

Theorem 4. ([5]) *For $n > 3$, in a C-reducible *P-Finsler space $D^i_{jkl} = 0$ holds.*

If we consider a Randers change

$$\overline{L}(x, y) \to L(x, y) + \beta(x, y),$$

where $\beta(x, y)$ is a closed one-form, then this change $\overline{L} \to L$ is projective.

Definition 6. ([1]) A Finsler space is called Landsberg space if the condition $P_{ijk} = 0$ holds.

Theorem 5. ([2]) *If there exist a Randers change with respect to a projective scalar $p(x, y)$ between a Landsberg and a *P-Finsler space (fulfilling the condition $\overline{P}_{ijk} = p(x, y) \overline{C}_{ijk}$), then $p(x, y)$ can be given by the equation*

$$p(x, y) = e^{\varphi(x)} \overline{L}(x, y). \tag{10}$$

It is well-known that the Riemannian space is a special case of the Landsberg space. In a Riemannian space we have $D^i_{jkl} = 0$, and a *P-Randers space with a closed one-form $\beta(x, y)$ is a Finsler space with vanishing Douglas tensor

Theorem 6. ([3]) *A Randers space is a Douglas space iff $\beta(x, y)$ is a closed form. Then*

$$2G^i = \gamma^i_{jk} y^j y^k + \frac{r_{lm} y^l y^m}{\alpha + \beta} y^i, \tag{11}$$

where $\gamma^i_{jk}(x)$ is the Levi–Civita connection of a Riemannian space, r_{lm} is equal to $b_{i;j}$ hence r_{lm} depends only on position.

From the Theorem 6. and (10) follows that

$$\frac{r_{lm} y^l y^m}{\alpha + \beta} = e^{\varphi(x)}(\alpha + \beta)$$

that is

$$\frac{r_{lm} y^l y^m}{\overline{L}} = e^{\varphi(x)} \overline{L}.$$

From the last equation we obtain

$$r_{lm} y^l y^m = e^{\varphi(x)} \overline{L}^2.$$

Differentiating twice this equation by y^l and y^m we get

$$b_{i;j} = e^{\varphi(x)} \overline{g}_{ij}.$$

This means that the metrical tensor $\overline{g}_{ij}$ depends only on x, so we get the following

Theorem. *A *P-Randers space with vanishing Douglas tensor is a Riemannian space if the dimension is greater than three.*

4. Further possibilities

From Theorem 1, Theorem 4 and our Theorem follows that only the *P-Kropina spaces can be *P-C reducible spaces with vanishing Douglas tensor which are different from Riemannian spaces. We would like to investigate this letter case in a forthcoming paper.

References

[1] P. L. Antonelli, R. S. Ingarden, M. Matsumoto, *The Theory of Sprays and Finsler Spaces with Applications in Physics and Biology*, Kluwer Acad. Publ., Dordrecht, Boston, London, 1993.

[2] S. Bácsó, On geodesic mapping of special Finsler spaces, *Rendiconti Palermo* (to appear).

[3] S. Bácsó, M. Matsumoto, On Finsler spaces of Douglas type, A generalisation of the notion of Berwald space, *Publ. Math. Debrecen*, **51** (1997), 385–406.

[4] H. Izumi, On *P-Finsler spaces I., II. *Memoirs of the Defense Academy, Japan*, **16** (1976), 133–138, **17** (1977), 1–9.

[5] H. Izumi, On *P-Finsler spaces of scalar curvature, *Tensor*, N. S. **38** (1982), 220–222.

[6] M. Matsumoto, S. Hojo, A conclusive theorem on C-reducible Finsler spaces, *Tensor*, N. S. **32** (1978), 225–230.

Sándor Bácsó
Lajos Kossuth University
Institute of Mathematics and Informatics
4010 Debrecen P.O. Box 12
Hungary
E-mail: sbacso@math.klte.hu

Ildikó Papp
Lajos Kossuth University
Institute of Mathematics and Informatics
4010 Debrecen P.O. Box 12
Hungary
E-mail: ipapp@math.klte.hu

On a class of differential equations connected with number-theoretic polynomials

KRYSTYNA GRYTCZUK

Abstract. In this paper we consider the special class of differential equations of second order. For this class we find a general solution which is strictly connected with some number-theoretic polynomials such as Dickson, Chebyschev, Pell and Fibonacci.

1. Introduction

Consider the following class of the polynomials:

$$W_n(x,c) = \left(\frac{x+\sqrt{x^2+c}}{2}\right)^n + \left(\frac{x-\sqrt{x^2+c}}{2}\right)^n \tag{1}$$

with respect to c, where $n \geq 1$ is the degree of the polynomial $W_n(x,c)$. It is known (see[2], p. 94) that the Dickson polynomial $D_n(x,a)$ of degree $n \geq 1$ and integer parameter a can be represent in the form:

$$D_n(x,a) = \left(\frac{x+\sqrt{x^2-4a}}{2}\right)^n + \left(\frac{x-\sqrt{x^2-4a}}{2}\right)^n. \tag{D}$$

We note that the Dickson polynomial belongs to class (1) if we take $c = -4a$. Taking $c = -1$ in (1) we obtain the Chebyschev polynomial of the second kind. For $c = 1$ we get the Pell polynomial and for $c = 4$ the Fibonacci polynomial.

We prove the following:

Theorem. The general solution of the differential equation

$$\left(x^2+c\right)y'' + xy' - n^2 y = 0; \quad x^2+c > 0 \tag{*}$$

is of the form

$$y = C_1\left(\frac{x+\sqrt{x^2+c}}{2}\right)^n + C_2\left(\frac{x-\sqrt{x^2+c}}{2}\right)^n, \tag{**}$$

where C_1, C_2 are arbitrary constants.

We remark that the general solution $(**)$ is strictly connected with the polynomials $W_n(x,c)$ defined by (1).

2. Basic Lemmas

Lemma 1. (see [1], Thm. 2.) Let the real-valued functions $s_0, t_0 u, v \in C^2(J)$, where $J \subset \mathbf{R}$ and $u \neq 0, v \neq 0$. Then the functions

$$y_1 = s_0 u^\lambda, \quad y_2 = t_0 v^\lambda, \tag{2}$$

where λ is non-zero real constant, are the particular solutions of the differential equation

$$D_0 y'' + D_1 y' + D_2 y = 0, \tag{3}$$

where

$$D_0 = \det \begin{pmatrix} s_0 & s_1 \\ t_0 & t_1 \end{pmatrix}, \quad D_1 = \det \begin{pmatrix} s_2 & s_0 \\ t_2 & t_0 \end{pmatrix}, \quad D_2 = \det \begin{pmatrix} s_1 & s_2 \\ t_1 & t_2 \end{pmatrix} \tag{4}$$

and

$$s_1 = s_0' + \lambda s_0 \frac{u'}{u}, \quad t_1 = t_0' + \lambda t_0 \frac{v'}{v} \tag{5}$$

$$s_2 = s_1' + \lambda s_1 \frac{u'}{u}, \quad t_2 = t_1' + \lambda t_1 \frac{v'}{v}. \tag{6}$$

Lemma 2. Let λ, s_0, t_0 be non-zero real constants and let non-zero real functions $u, v \in C^2(J)$, $J \subset \mathbf{R}$ be linearly independent over the real number field $\mathbf{R}$. Then the general soltution of the differential equation:

$$\det \begin{pmatrix} 1 & \frac{u'}{u} \\ 1 & \frac{v'}{v} \end{pmatrix} y'' + \det \begin{pmatrix} g & 1 \\ h & 1 \end{pmatrix} y' + \lambda \det \begin{pmatrix} \frac{u'}{u} & g \\ \frac{v'}{v} & h \end{pmatrix} y = 0, \tag{$***$}$$

where

$$g = \frac{u''}{u} - (1-\lambda)\left(\frac{u'}{u}\right)^2, \quad h = \frac{v''}{v} - (1-\lambda)\left(\frac{v'}{v}\right)^2 \tag{7}$$

is of the form

$$y = C_1 s_0 u^\lambda + C_2 t_0 v^\lambda, \tag{8}$$

where C_1, C_2 are arbitrary constants.

Proof. By the assumptions of Lemma 1 and Lemma 2 it follows that

$$s_1 = \lambda s_0 \frac{u'}{u}, \quad t_1 = \lambda t_0 \frac{v'}{v}. \tag{9}$$

From (9) and (6) we obtain

$$s_2 = s_1' + \lambda s_1 \frac{u'}{u} = \lambda s_0 \left(\frac{u''}{u} - (1-\lambda) \left(\frac{u'}{u} \right)^2 \right) \tag{10}$$

and

$$t_2 = t_1' + \lambda t_1 \frac{v'}{v} = \lambda t_0 \left(\frac{v''}{v} - (1-\lambda) \left(\frac{v'}{v} \right)^2 \right). \tag{11}$$

Let us denote by $g = \frac{u''}{u} - (1-\lambda)\left(\frac{u'}{u}\right)^2$ and by $h = \frac{v''}{v} - (1-\lambda)\left(\frac{v'}{v}\right)^2$. Then the formulae (10) and (11) have the form:

$$s_2 = \lambda s_0 g, \quad t_2 = \lambda t_0 h. \tag{12}$$

By (12), (9) and Lemma 1 it follows that the differential equation (3) reduce to $(***)$. On the other hand from Lemma 1 it follows that the functions $y_1 = s_0 u^\lambda$ and $y_2 = t_0 v^\lambda$ are the particular solutions of $(***)$. Now we observe that the functions u, v are linearly independent over $\mathbf{R}$ if and only if the functions u^λ and v^λ are linearly independent over $\mathbf{R}$. Indeed, denote by $W(u^\lambda, v^\lambda)$ the Wronskian of the functions u^λ and v^λ and let

$$D_0 = \det \begin{pmatrix} 1 & \frac{u'}{u} \\ 1 & \frac{v'}{v} \end{pmatrix}.$$

Then we have

$$D_0 = (uv)^{-1} \det \begin{pmatrix} u & v \\ u' & v' \end{pmatrix}, \tag{13}$$

and

$$W\left(u^\lambda, v^\lambda\right) = \det \begin{pmatrix} u^\lambda & v^\lambda \\ \left(u^\lambda\right)' & \left(v^\lambda\right)' \end{pmatrix} = \lambda (uv)^\lambda \det \begin{pmatrix} 1 & 1 \\ \frac{u'}{u} & \frac{v'}{v} \end{pmatrix}. \tag{14}$$

Since $\det\begin{pmatrix} 1 & 1 \\ \frac{u'}{u} & \frac{v'}{v} \end{pmatrix} = \det\begin{pmatrix} 1 & \frac{u'}{u} \\ 1 & \frac{v'}{v} \end{pmatrix}$, from the definition of D_0, (13) and (14) we get

$$W\left(u^\lambda, v^\lambda\right) = \lambda(uv)^\lambda D_0 = \lambda(uv)^{\lambda-1} \det\begin{pmatrix} u & v \\ u' & v' \end{pmatrix}. \tag{15}$$

From (15) easily follows that the functions u^λ, v^λ are linearly independent over $\mathbf{R}$ if and only if the functions u, v have the same property. Using the assumption of Lemma 2 about the functions u, v we obtain that the functions u^λ, v^λ and also $y_1 = s_0 u^\lambda, y_2 = t_0 v^\lambda$ are linearly independent over $\mathbf{R}$. Since the functions y_1, y_2 are the particular solutions of $(***)$, the function $y = C_1 y_1 + C_2 y_2 = C_1 s_0 u^\lambda + C_2 t_0 v^\lambda$ is a general solution of $(***)$. The proof of Lemma 2 is complete.

3. Proof of the Theorem

Let $\lambda = n$ be natural number and let $s_0 = t_0 = 1$. Moreover, let $u = a(x)+b(x)\sqrt{k}$ and $v = a(x)-b(x)\sqrt{k}$, where k is fixed non-zero constant. If the functions u, v are linearly independent over $\mathbf{R}$ then by Lemma 2 it follows that the general solution of the differential equation

$$\det\begin{pmatrix} 1 & \frac{u'}{u} \\ 1 & \frac{v'}{v} \end{pmatrix} y'' + \det\begin{pmatrix} g & 1 \\ h & 1 \end{pmatrix} y' + n \det\begin{pmatrix} \frac{u'}{u} & g \\ \frac{v'}{v} & h \end{pmatrix} y = 0 \tag{16}$$

is of the form

$$y = C_1\left(a(x) + b(x)\sqrt{k}\right)^n + C_2\left(a(x) - b(x)\sqrt{k}\right)^n, \tag{17}$$

where $g = \frac{u''}{u} - (1-n)\left(\frac{u'}{u}\right)^2$ and $h = \frac{v''}{v} - (1-n)\left(\frac{v'}{v}\right)^2$ and C_1, C_2 are arbitrary constants. Now, we put $a(x) = \frac{x}{2}$, $b(x) = \frac{\sqrt{x^2+c}}{2}$, $k = 1$, where $x^2 + c > 0$. Then we have

$$u = \frac{x + \sqrt{x^2+c}}{2}, \quad v = \frac{x - \sqrt{x^2+c}}{2}. \tag{18}$$

From (18) we obtain

$$u' = \frac{1}{2}\left(\frac{x + \sqrt{x^2+c}}{\sqrt{x^2+c}}\right), \quad v' = -\frac{1}{2}\left(\frac{x - \sqrt{x^2+c}}{\sqrt{x^2+c}}\right). \tag{19}$$

By (18) and (19) easily follows that the functions u, v are linearly independent over $\mathbf{R}$, because the Wronskian $W(u,v) \neq 0$. On the other hand from (19) we obtain

$$u'' = \frac{1}{2}\frac{c}{(x^2+c)\sqrt{x^2+c}}, \quad v'' = -\frac{1}{2}\frac{c}{(x^2+c)\sqrt{x^2+c}}. \tag{20}$$

From (19) and (18) we get

$$\frac{u'}{u} = \frac{1}{\sqrt{x^2+c}}, \quad \frac{v'}{v} = -\frac{1}{\sqrt{x^2+c}}, \tag{21}$$

hence by (21) it follows that

$$\left(\frac{u'}{u}\right)^2 = \left(\frac{v'}{v}\right)^2 = \frac{1}{x^2+c}. \tag{22}$$

Simlarly from (20) and (18) we obtain

$$\frac{u''}{u} = \frac{c}{(x^2+c)\left(x+\sqrt{x^2+c}\right)\sqrt{x^2+c}},$$

(23)

$$\frac{v''}{v} = -\frac{c}{(x^2+c)\left(x-\sqrt{x^2+c}\right)\sqrt{x^2+c}}.$$

From (21) we calculate that

$$D_0 = \det\begin{pmatrix} 1 & \frac{u'}{u} \\ 1 & \frac{v'}{v} \end{pmatrix} = \frac{v'}{v} - \frac{u'}{u} = -\frac{2}{\sqrt{x^2+c}}. \tag{24}$$

In similar way from (22) and (23) we get

$$D_1 = \det\begin{pmatrix} g & 1 \\ h & 1 \end{pmatrix} = g - h = -\frac{2x}{(x^2+c)\sqrt{x^2+c}}. \tag{25}$$

On the other hand by (21) and (23) it follows that

$$D_2 = \det\begin{pmatrix} \frac{u'}{u} & g \\ \frac{v'}{v} & h \end{pmatrix} = h\frac{u'}{u} - g\frac{v'}{v} = \frac{2n}{(x^2+c)\sqrt{x^2+c}}. \tag{26}$$

Now, we see that from (24), (25) and (26) the differential equation (16) has the following form:

$$(x^2+c)\,y'' + xy' - n^2 y = 0, \tag{27}$$

so denote that (27) is the same equation as in our Theorem. Thus, by Lemma 2 it follows that the general solution of (27) is given by the formula

$$y = C_1 \left(\frac{x+\sqrt{x^2+c}}{2} \right)^n + C_2 \left(\frac{x-\sqrt{x^2+c}}{2} \right)^n$$

and the proof of the Theorem is complete.

Remark. Consider the following functional matrix;

$$M(x) = \frac{1}{2} \begin{pmatrix} x & \sqrt{x^2+c} \\ \sqrt{x^2+c} & x \end{pmatrix}.$$

Then we can calculate that the functions $u = \frac{x+\sqrt{x^2+c}}{2}$ and $v = \frac{x-\sqrt{x^2+c}}{2}$ are the characteristic roots of this matrix. Hence, we observe that the general solution of the differential equation (16) is linear combination of the powers such roots.

References

[1] A. Grytczuk and K. Grytczuk, *Functional recurrences, Applications of Fibonacci Numbers*, Ed. by G. E. Bergum et al., Kluwer Acad. Publ., Dordrecht, 1990, 115–121.

[2] P. Moree and G. L. Mullen, Diskson polynomial discriminators, *J. Number Theory*, **59** (1996), 88–105.

Institute of Mathematics
Technical University
Zielona Góra, ul. Podgórna 50
Poland

Interpolation possibilities using rational B-spline curve

MIKLÓS HOFFMANN and EMŐD KOVÁCS

Abstract. The aim of this paper is to solve some interesting interpolation problems using rational B-spline curve. If a sequence of planar points and vectors are given then a free-form curve can calculated which interpolates the points and has the given tangent vectors in these points. Our method gives a fast interpolation of these data using extra control points. Then we provide a method which allows to interpolate the same set of data without any predefined order of the points, i.e. a set of scattered points with the vectors. In this latter problem we use an artificial neural network to order the data.

Introduction

Rational B-spline curves and surfaces (or simply called NURBS), as the generalization of B-spline curve and surface, are widely used in CAD/CAM, and free-from design [4]. Basicly these methods have been developed for approximating points, but they can be used as interpolating curves or surfaces as well. In this paper we will use the rational B-spline curve for a special interpolation problem, where beside the points the tangent vectors of the future curve are also given. The method is similar to the case of B-spline: the control points of the future curve is calculated from the given data, so finally it will be an approximating curve, but given points will be on the curve and it will have the given tangent vectors.

This problem can also be fomulated without giving the order of points. Since all the basic free-form methods are defined with a sequence of points as input data, in this case we use an artificial neural network, the Kohonen net, to order the points and then we apply the method mentioned above.

Interpolation of a sequence of points and vectors

At first we define the rational B-spline curve as an approximating curve. If a sequence of points $V_i, i = 1, \ldots, n$ (called control points) and positive real numbers $w_i, i = 1, \ldots, n$ (called weights) are given, then the third order

This research was supported by the Hungarian National Foundation for Scientific Research (OTKA), grant No. F019395.

uniform rational B-spline curve can be defined as follows:

$$Q_i(u) = \frac{\sum_{r=-1}^{2} V_{i+r} w_{i+r} b_r(u)}{\sum_{r=-1}^{2} w_{i+r} b_r(u)} \qquad u \in [0,1]$$

where the functions b_r are the well-known basic functions:

$$b_{-1}(u) = \frac{1 - 3u + 3u^2 - u^3}{6}$$
$$b_0(u) = \frac{4 - 6u^2 + 3u^3}{6}$$
$$b_1(u) = \frac{1 + 3u + 3u^2 - 3u^3}{6}$$
$$b_2(u) = \frac{u^3}{6}$$

Note, that the curve consists of segments, and the parameter u runs over the interval $[0,1]$ in every segment. This fact will be strongly used in the basic idea of the interpolation.

Now let a sequence of points $P_i, i = 1, \ldots, m$ and a sequence of vectors $t_i, i = 1, \ldots, m$ be given. Find a sequence of contol points V_j and weights w_j (at this moment the number of points and weights is unknown) such that the curve using these control points and weights interpolates the points P_i and has the tangent vectors t_i in these points.

Suppose, that the points P_i will be the starting points of the segments of the future curve. Considering the properties of the segments mentioned above, this assumption can be formulated as follows:

$$Q_i(0) = P_i \qquad i = 1, \ldots, m-1$$
$$Q_m(1) = P_m$$

The last equation means that the last point P_m would be the end point of the last segment.

On the other hand, the given vectors have to be equal to the derivatives of the curve in the starting points of the segments:

$$\dot{Q}_i(0) = t_i \qquad i = 1, \ldots, m-1$$
$$\dot{Q}_m(1) = t_m$$

Unfortunately these equations yield a second order system of equations for the control points V_j and the weights w_j. To reduce the complication and

save computing time, some control points will be defined in advance with unit weight. Let these points be the intersections of the line of the tangent vectors t_i, t_{i+1} or, if this point would be too far from the points P_i, simply be the midpoint of the section P_i, P_{i+1}. The position of these contol points are not important because later on they can be modified without disturbing the interpolation.

Hence the system of equations has to be solved is the following:

$$\frac{\frac{1}{6}w_{i-1}V_{i-1} + \frac{4}{6}w_iV_i + \frac{1}{6}w_{i+1}V_{i+1}}{\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1}} = P_i$$

$$\frac{(-\frac{1}{2}w_{i-1}V_{i-1} + \frac{1}{2}w_{i+1}V_{i+1})(\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1})}{(\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1})^2} -$$

$$-\frac{(\frac{1}{6}w_{i-1}V_{i-1} + \frac{1}{6}w_iV_i + \frac{1}{6}w_{i+1}V_{i+1})(-\frac{1}{2}w_{i-1} + \frac{1}{2}w_{i+1})}{(\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1})^2} = t_i$$

In these equations only V_i and w_i are unknown, since $V_{i-1}, V_{i+1}, w_{i-1}, w_{i+1}$ are predefined. Coefficients can be calculated by the functions $b_i(u)$ and $\dot{b}_i(u)$ in $u = 0$.

Now the solutions of these equations and the predefined control points and weights form a control poligon and a sequence of weights, with which the rational B-spline curve can be drawn, and it will pass through the points P_i and will have the tangent vectors t_i.

Interpolation of scattered points with tangent vectors

This problem is similar to the previous one, but the given points have no predefined order, i.e. we do not know which point has to be the first and which one is the last one. Since the rational B-spline method can be applied only on a sequence of points (and weights), first of all we have to order the points. For this purpose an artificial neural network will be used. After this step the same procedure described above can be applied. Now after a short description of the applied net, the Kohonen network [2], the ordering process and the interpolation will be discussed. For more detailed discussion of the ordering method by Kohonen network see [1]–[2], [5].

The Kohonen neural network is a two-layered non-supervised learning neural network. Self organizing networks, like the applied Kohonen net, organize the input data during the so called learning phase without any supervision. The most important part of the algorithm is the training rule, which modifies the network according ot the input points.

Let a set of points $P_i(i = 1, \ldots, n)$ (scattered data) and a set of vectors $t_i(i = 1, \ldots, n)$ be given on the plane. Our first task is to determine the order of the points for the interpolation problem.

The Kohonen net is used to order the points. The first layer of neurons is called input layer and contains the two input neurons which pick up the data, the planar points. The input neurons are entirely interconnected to a second, competitive layer, containing m neurons (where $m \geq n$, usually $m = 4n$). The weights associated with the connections are adjusted during training by the following rule:

— Coordinates of the scattered points: $P_i(x_{1i}, x_{2i}, x_{3i})$ $(i = 1, \ldots, n)$

— Coordinates of the output points: $Q_j(w_{1j}, w_{2j}, w_{3j})$ $(j = 1, \ldots, m)$

STEP 1. Initialize the weights w_{sj}, $(s = 1, 2, 3 \quad j = 1, \ldots, m)$ as small random values around the average of the coordinates of the input points. Let the training time $t = 1$

STEP 2. Present new input values $(x_{1i_0}, x_{2i_0}, x_{3i_0})$, as the coordinates of a randomly selected input point p_{i_0}

STEP 3. Compute the Euclidean distance of all output nodes to the input point:

$$d_j = \sum_{s=1}^{3} (x_{si_0} - w_{sj})^2$$

STEP 4. Find the winning unit q_{j_0} as the node which has the minimum distance to the input point, so where j_0 is the value for which $d_{j_0} = min(d_j)$

STEP 5. Compute the neighborhood $N(t) = (j_0, j_1, \ldots, j_k)$

STEP 6. Update the weights (i.e.the coordinates) of the nodes in the neighborhood by the following equation:

$$w_{sj}(t+1) = w_{sj}(t) + \eta(t)(x_{si_0} - w_{sj}(t)) \quad \forall j \in N(t)$$

where $\eta(t)$ is a so called gain term, a Gaussian function decreasing in time.

STEP 7. Let $t = t + 1$. Repeat STEP 2-7 until the network is trained.

The network is said to be trained if all the input points are on the polygon, that is for all the input points $P_i(i = 1, \ldots, m)$ there is an output vector o_j such that after a certain time t_0 the Euclidean distance of o_j and P_i is smaller thane a predefined limit. A stronger convergence can be obtained if we require that the output vectors which do not converge to an input vector be on the line determined by its two neighbouring output vectors. This stronger convergence is important especially in term of the smoothness of the future curve. For the detailed description and evaluation of this problem see [2].

After the ordering process the same algorithm can be applied to calculate the interpolation curve as we described above. At this part of the process it is irrelevant, that the input points were scattered.

Conclusions

In the free-form design there are several different method according to the problem (approximation or interpolation) and the type of data (ordered or scattered). In this paper we provided two algorithms, with the help of which all kinds of problems and types of data can be handled by the rational B-spline curve. Even if parts of the data are scattered and others have to be interplated or approximated, the final result (joining the calculated control polygons) will be a unique curve.

References

[1] M. Hoffmann, L. Várady, Free-form curve design by neural networks, *Acta. Acad. Paed. Agriensis*, Tom. XXIV., 1997, 99–104.

[2] M. Hoffmann, L. Várady, Free-form surface design by neural networks, *Journal for Geometry and Graphics*, Vol. 2. N.1., 1998., 1–6.

[3] T. Kohonen: *Self-organization and associative memory*, Springer-Verlag, 1984.

[4] L. Piegl, W. Tiller: *The NURBS Book*, Springer Verlag, 1997.

[5] L. Várady: Analysis of the Dynamic Kohonen Network Used for Approximating Scattered Data, *Proceedings of the 7th ICECGDG*, Cracow, 1996, 433–436.

Miklós Hoffmann and Emőd Kovács
Institute of Mathematics and Computer Science
Károly Eszterházy Teachers' Training College
Leányka u. 4.
3300 Eger, Hungary
e-mail: hofi@ektf.hu, emod@ektf.hu

Módszertani cikkek
Methodological papers

A matematikai problémamegoldó gondolkodás vizsgálata 13—14 éves korú tanulóknál

OROSZ GYULÁNÉ

Abstract. In this paper is an experimental investigation of the mathematical problem-solving at the age of 13 and 14. It consists of an introduction, the framework of the study, research methods and problems, results and conclusions, a model.

1. Bevezetés, a témaválasztás indoklása

A NAT bevezetését megelőző években a matematikaoktatáshoz kapcsolódó hazai és nemzetközi kutatásokban igen nagy hangsúlyt kapott és kap ma is a tanulói teljesítmények mérése, összehasonlítása, a tantervi aspektusok vizsgálata (IEA, Monitor).

A MAWI-csoport (1994) széles körű vizsgálatot folytat annak feltárására, hogy a matematikatanulásának sikerességére milyen hatást gyakorol a tanulókban a matematikáról kialakított nézet. Ezen vizsgálatok eredményeit figyelembe kell venni a matematikaoktatással kapcsolatos fejlesztéseknél.

Ugyanakkor ezek mellett fontos feltárni a matematikai problémamegoldás életkori jellemzőit, az esetleges alacsony teljesítményszint okait, az előforduló hibákat, hiányosságokat.

E gondolatok inspiráltak bennünket kutatásunk megkezdésekor. Vizsgálatunk célja a 13-14 éves tanulók matematikában nyújtott problémamegoldó gondolkodásának feltérképezése. Számos felvetés és válaszra váró kutatási kérdés fogalmazható meg ezen a területen. Milyen önálló és céltudatos a tanulók ezirányú tevékenysége? Milyen jellemző hibákat követnek el? Milyen következtetéseket vonhatunk le az előforduló hibák lehetséges okaira vonatkozóan? Mi jellemzi a 7. és mi a 8. osztályos tanulók teljesítményét? Milyen a részmegoldások teljesítése? Elakadás esetén milyen arányú a segítségnyújtás? Milyen megoldási módszereket alkalmaznak a tanulók? Mi jelenti a feladatban a tanulók számára a problémát? Végül ebben az egyáltalán nem teljes sorban a legnehezebben megválaszolható kérdés, hogy milyen összefüggésben vannak a tanulói teljesítmények a külső és belső motiváló tényezőkkel? Cikkünkben egy olyan elővizsgálat eredményeiről számolunk be, mely adatokat nyújt és segít abban, hogy egy szélesebb körű vizsgálat hipotéziseit, kérdéseit körültekintőbben és hatékonyabban tudjuk megfogalmazni.

2. A vizsgálatok tervezése, metodikai vonatkozásai

A gondolkodás vizsgálatának módszerére vonatkozó tudományos követelményeknek munkánk során igyekeztünk eleget tenni és teljes egészében elfogadtuk Lénárd Ferenc (1978) megállapításait:

1. Problémákat, feladatokat adunk a kísérleti személyeknek annak érdekében, hogy ezek a gondolkodási tevékenységet kiváltsák.
2. Elakadás esetén segítséget, ún. kisegítő feladatokat alkalmazunk.
3. Megvizsgáljuk, hogy a megoldási menetekben az ismeretek milyen szerepet játszanak.
4. Közvetlen rávezetéseket alkalmazunk.
5. A gondolkodási menet lépéseit gondosan feljegyezzük és elemezzük.
6. A gondolkodási tevékenység közben elkövetett hibák tanulmányozására nagy gondot fordítunk.
7. Sohasem tévesztjük szem elől, hogy a gondolkodási tevékenység kölcsönhatás a személy és a probléma között.

A feladatok összeállításának pszichológiai szempontjai közül figyelembe vettük (Kelemen, 1970) azon megállapítását, hogy „olyan feladatokat kell adni, amelyek bizonyos nehézségeket okoznak, a megoldásuk aktív tevékenységet igényel. A feladat olyan fokig legyen újszerű, hogy lehetséges legyen a múltbeli tapasztalatokhoz való kapcsolódása. Annyi elemet kell tartalmaznia, amennyi feltétlenül szükséges a pontos megértéshez; de kellő hézagokat is kell hagyni, hogy teret biztosítson az önálló tanulói műveletvégzés számára." A témakör kiválasztásánál elfogadtuk Lénárd (1978) azon megállapítását, miszerint olyan feladatokat kell adnunk, amelyek elindítják „és egy bizonyos ideig - minden külső beavatkozás nélkül aktiválják a kísérleti személyek gondolkodási tevékenységét". Az elemi számelméleti feladatok több okból is alkalmasnak látszottak erre. Egyrészt a Nemzeti Alaptanterv tananyagában a 10-16 éves korosztály minden évfolyamán előfordulnak számelméleti alapismeretek. Másrészt a számelméleti feladatokkal való foglalkozás felkelti a tanulók matematika iránti érdeklődését, rámutat a matematika tudomány szépségeire, kutatásra ösztönzi a tehetséges tanulókat (fontos motiváló tényezők), alkalmas lehet a matematikai képességek strukturájának feltárására.

3. Vizsgálati módszer

Vizsgálatunkat Egerben 12 általános iskolában végeztük, amelybe 373 14 éves és 241 13 éves tanulót vontunk be. A vizsgálatokban a feladatlapos és az egyéni felmérés módszerét alkalmaztuk.

Jelen dolgozatunkban a feladatlapos méréshez kapcsolódó tapasztalatainkat vázoljuk. Két számelméleti feladatot választottunk ki, amelyet a

7. és 8. osztályos tanulók problémamegoldó gondolkodásának vizsgálatához egyaránt felhasználtunk.

A feladatok a következők voltak:

1. Hány olyan egyenlőszárú háromszög van, amelyeknek oldalhosszai egész számok, és leghosszabb oldalának mérőszáma 1997?

2. Egy sakktábla minden mezőjébe beírjuk rendre az $1, 2, 3, \ldots, 64$ természetes számokat a bal felső sarokból indulva, balról jobbra, felülről lefelé haladva, majd minden lehetséges módon letakarjuk egy 2×2-es négyzettel. Hány esetben lesz a letakart számok összege osztható 3-mal?

Feladatválasztásunkat gyakorlati, tanítási tapasztalataink, valamint egy elővizsgálat eredménye is megerősítí. A matematikai versenyfeladatok megoldásainak javítása során azt tapasztaltuk, hogy az elemi számelméleti feladatok e korosztály számára nehéznek bizonyultak (a teljesítmények alacsony szintje jelezte e tényt), így valóban igazi problémát jelentettek. Az elővizsgálat során a tanulók 12 feladat rangsorolását végeztették el nehézségi sorrendjük szerint, s e rangsorban az általunk kiválasztott két számelméleti feladat került az utolsó két ranghelyre.

4. A feladatok értékelése

Mindkét feladatnál a következő csoportosítást tudtuk elvégezni:
— önállóan, jól oldja meg,
— önállóan, hibásan oldja meg,
— részmegoldások, sok hibával,
— nem képes megoldani a problémát.

A tanulók 1. és 2. feladatban nyújtott teljesítményét összegezve az alábbi eredményt kaptuk:

7. osztály

	1. feladat	2. feladat
Önállóan, jól oldja meg	3,2%	0,8%
Önállóan, hibásan oldja meg	12,4%	4,6%
Részmegoldások, sok hibával	15,8%	16,4%
Nem képes megoldani a problémát	68,6%	78,2%

1. táblázat

8. osztály

	1. feladat	2. feladat
Önállóan, jól oldja meg	4,5%	1,2%
Önállóan, hibásan oldja meg	13,3%	5,5%
Részmegoldások, sok hibával	21,4%	18,6%
Nem képes megoldani a problémát	60,8%	74,7%

2. táblázat

A táblázatok adatai egyértelműen arra hívják fel a figyelmünket, hogy a tanulók önállósága igen alacsony szintű. A tanulók megoldásainak elemzéseiből nem tudunk következtetéseket levonni a sikertelenség okára vonatkozóan, mert ehhez további vizsgálatok szükségesek. A hetedik és nyolcadik osztályosok között nincs lényeges különbség az önállóság mértékét összehasonlítva. Ezért a 7. osztályosok első feladatának megoldásait elemezzük részletesen.

A 7. osztály első feladatának tartalmi, metodikai elemzése

A feladat megoldásához szükséges előismeretek:

Egyenlő szárú háromszög, alap, szár fogalmak ismerete — háromszög-egyenlőtlenség összefüggése, leghosszabb oldal értelmezése, oldalhossz mérőszáma, a háromszög oldalának mérőszáma egész szám, az összes lehetséges adott tulajdonságú háromszög megkeresése, egész számok összehasonlítása, rendezése.

Problémát jelentett a tanulók számára:

Nem volt megadva melyik a háromszög leghosszabb oldala (alapja vagy a szára). Az értelmezésnél is jelentkeztek gondok. A feladatot — tömör megfogalmazásából adódóan — a tanulók első olvasásra nem értették meg, ezért hozzá sem kezdtek a megoldásához, melyet a teljesítmények is igazolnak. Hibátlan megoldást mindössze két tanuló adott (1,2%), egyetlen számolási hibával egy tanuló oldotta meg jól a problémát, sok hibával helytelen megoldást adott a tanulók 28,2%. Nem foglakozott a feladattal a tanulók 68,6%-a. A feladat összetettsége is nehézséget okozott.

Az előforduló hibák, s azok lehetséges okai:

Figyelmetlenségből adódó hiba, hogy a tanulók 18%-a felületesen olvasta el a feladatot és elsiklott az **egész számok**, szavak felett, ami fontos feltétel volt, s ezért jutottak a helytelen következtetésre, miszerint végtelen sok ilyen tulajdonságú háromszög van. A tanulók 3%-a nem értette a mérőszám szó jelentését, s ezért nem tudta értelmezni a feladatot, s kérte, hogy konkrét mértékegységben legyen adott az oldal hossza.

Hiányos előismeretből adódó hiba volt, hogy a háromszög-egyenlőtlenséget nem tudták alkalmazni a feladatban, csupán reprodukálni voltak képesek ezen összefüggést.

Az elemi gondolkodási műveletvégzésben való járatlanságot mutatta, hogy azon tanulók, akik foglalkoztak a feladattal, csak a feladat egyik részét oldották meg, amikor az alap a leghosszabb, s a másik résszel egyáltalán nem foglalkoztak.

A kombinatorikus gondolkodásmód kialakulatlansága is okozott hibákat: sokan felismertek a háromszög-egyenlőtlenség szerepét a feladatban, megállapították mennyi lehet a meg nem adott oldal maximális és minimális hossza, de nem tudtak mit kezdeni a kapott számadatokkal, s így nem jutottak el a megoldásig, mert nem voltak képesek előállítani a meghatározott egész számokat két egész szám összegeként.

A fenti hibákból arra következtethetünk, hogy a probléma e korosztály számára nehéznek bizonyult és csak a matematikából jó képességű tanulók tudták megoldani. Véleményünk szerint a sikertelen megoldásokat adó tanulók számára megfelelő egyéni segítséget nyújtva rávezethetjük őket a helyes megoldásra.

Fenti észrevételeink olyan feltételezések, amelyek a tanulói munkák elemzésén alapulnak. További vizsgálatok szükségesek azonban annak eldöntésére, hogy mi az oka az alacsony teljesítményszintnek. Ezért végeztünk egyéni vizsgálatokat is, amelyekkel egy következő tanulmányokban foglalkozunk részletesen. A tanulói munkák elemzését figyelembe véve kidolgoztunk egy-egy elméleti modellt a tanulók segítésére, s az egyéni vizsgálatok során ezeket kipróbáltuk.

Az egyéni vizsgálatokban az általunk kidolgozott modellt használtunk. A 2. feladat megoldásához ilyen módon adtunk segítséget a tanulóknak, ha önállóan nem voltak képesek megoldani a problémát.

Mindkét osztálynál az (a) és a (b) tevékenységet alkalmaztuk. A további konstrukciókat — (c) és (d) — a felsőbb évfolyamok számára dolgoztuk ki.

5. Elemi számelméleti problémák négyzetrácsra írt számok lefedésével

(a) *Tevékenység:*

Rajzolj egy 4 × 4-es négyzetrácsot! A négyzetekbe írd be rendre az $1, 2, 3, \ldots, 16$ természetes számokat a bal felső sorokból indulva, balról jobbra, felülről lefelé haladva.

Vágj ki átlátszó fóliából egy 2 × 2-es négyzetet.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Feladatok:

1. Takard le minden lehetséges módon a számozott négyzetrácsot a 2 × 2-es négyzettel. Hány különböző letakarás lehetséges?

2. Határozd meg minden esetben a a letakart számok összegét!

3. Hány esetben lesz a letakart számok összege osztható 3-mal?

4. Hány esetben lesz a letakart számok összege osztható 5-tel?

5. Van-e olyan letakarás, amikor az összeg osztható 15-tel?

6. Írd fel a négy szám összegét általánosan!

7. Az általánosan felírt összeg segítségével fogalmazz meg további problémákat!

(b) *Tevékenység:*

Rajzolj egy 8 × 8-as négyzetrácsot! Az előző feladat feltételei szerint írd be az egyes négyzetekbe rendre az $1, 2, 3, \ldots, 64$ természetes számokat! Ismét az átlátszó fóliából kivágott 2 × 2-es négyzettel dolgozz!

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
19	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Feladatok:

1. Takard le a négyzetrácsot a 2 × 2-es négyzettel úgy, hogy a letakart négy szám összege osztható legyen 3-mal. Keress minél több megoldást!

2. Ha minden lehetséges módon elvégezzük a letakarást, akkor hány esetben lesz a letakart számok összege osztható 3-mal?

3. Írd fel általánosan a négy szám összegét!

4. A letakarások elvégzése nélkül próbálj választ adni a kérdésre az általános alak segítségével! Hány esetben lesz a letakart számok összege osztható 9-cel?

5. Igaz-e, hogy az összeg mindig osztható 4-gyel? Miért?

6. Fogalmazz meg további problémákat!

(c) **Gondolati konstrukciók:** (Szükség esetén rajzos modell készítése)

— Képzelj el egy 11 × 11-es négyzetrácsot, amelybe rendre beírtuk az $1, 2, 3, \ldots, 121$ természetes számokat az előző feladatok feltételei szerint, majd minden lehetséges módon letakartuk a 2 × 2-es négyzettel.

Feladatok:

1. Írd fel a letakart számok összegét általánosan!

2. Hány esetben lesz a letakart számok összege osztható 8-cal?

3. Hány esetben lesz a a letakart számok összege osztható 3-mal?

4. Igazold, hogy az összeg mindig osztható 4-gyel!

5. Hány letakarás esetén lesz az összeg osztható 12-vel?

(d) **További gondolati konstrukciók:** (modell segítségével vagy attól elvonatkoztatva)

— Képzelj el egy 1997 × 1997-es négyzetrácsot, amelyre beírtuk a számokat az előző feltételek szerint és minden lehetséges módon letakartuk a 2 × 2-es négyzettel.

Feladatok:

1. Írd fel a letakart számok összegét általánosan!

2. Bizonyítsd be, hogy bármely letakarás esetén teljesül, hogy az összeg osztható 4-gyel!

3. Fogalmazz meg ezen lefedésekhez kapcsolódó további problémákat!

A további problémák konstruálásához célszerű tanári segítséget nyújtani. Például: A négyzetrácsba prímszámokat páros vagy páratlan számokat írjunk, lefedő alakzatként 3 × 3-as négyzetet, 3 × 3-as vagy 2 × 2-es téglalapot használhatunk.

Következő tanulmányunkban a modellek alkalmazásához kapcsolódó tapasztalatainkról számolunk be.

Irodalom

[1] Ambrus András: *Matematikadidaktikai tanulmányok,* Tankönyvkiadó, Budapest, 1989.

[2] Balogh László: *Feladatrendszerek és gondolkodásfejlesztés,* Tankönyvkiadó, Budapest, 1987.

[3] Balogh László—Herskovits Mária—Tóth László: *Tehetség és képességek,* KLTE Pedagógiai-Pszichológiai Tanszék Debrecen, 1995.

[4] Czeglédy István: *Matematika tantárgypedagógia I.,* Calibra, Budapest, 1997.

[5] Kelemen László: *A 10—14 éves tanulók tudásszintje és gondolkodása,* Akadémiai Kiadó, Budapest, 1963.

[6] Lénárd Ferenc: *A problémamegoldó gondolkodás,* Akadémiai Kiadó, Budapest, 1978.

[7] Pólya György: *A gondolkodás iskolája,* Gondolat, Budapest, 1971.

[8] Pólya György: *A problémamegoldás iskolája I-II.,* Tankönyvkiadó, Budapest, 1971.

[9] Salamon Jenő: *A megismerő tevékenység fejlődéslélektana,* Nemzeti Tankönyvkiadó, Budapest, 1996.

Dr. Orosz Gyuláné
Eszterházy Károly Tanárképző Főiskola
Matematika Tanszék
Leányka u. 4.
3301 Eger, Pf. 43.

Tartalom (Contents)

ZAY, B., An application of the continued fractions for $\sqrt{D}$ in solving some types of Pell's equations 3

MÁTYÁS, F., Bounds for the zeros of Fibonacci-like polynomials 15

JONES, J. P. and KISS, P., Representation of integers as terms of a linear recurrence with maximal index 21

TSANGARIS, PANAYIOTIS G., A sieve for all primes of the form $x^2+(x+1)^2$ 39

PHONG, B. M., Quasi multiplicative functions with congruence property 55

GRYTCZUK, A., On a conjecture about the equation $A^{mx}+A^{my}=A^{mz}$ 61

KIRÁLY B. ÉS OROSZ GYULÁNÉ: Egy euklidészi gyűrű 71

MAKSA, GY., Functions having quadratic differences in a given class 77

GÁT, G., On a theorem of type Hardy–Littlewood with respect to the Vilenkin-like systems 83

BÁCSÓ, S. and PAPP, I., *P-Finsler spaces with vanishing Douglas tensor 91

GRYTCZUK, K., On a class of differential equations connected with number-theoretic polynomials 97

HOFFMANN, M. and KOVÁCS, E., Interpolation possibilities using rational B-spline curve 103

Methodological papers (Módszertani cikkek)

OROSZ GYULÁNÉ: A matematikai problémamegoldó gondolkodás vizsgálata 13—14 éves korú tanulóknál 111

Molnár és Társa '2001' Kft. Nyomda Eger Tel.: 36/422-946