ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXI/11

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

EGER
1993

1.002.436

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXI.

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

EGER
1993

ISSN 1216-6014

Felelős kiadó: dr. Orbán Sándor
főiskolai főigazgató

Készült az Eszterházy Károly Tanárképző Főiskola
nyomdaüzemében

TARTALOM

TÓMÁCS TIBOR

A REKURZÍV SOROZATOK EGY ALKALMAZÁSÁRÓL

ABSTRACT: *(On an application of second order linear recurrences)* Let $ax^2+bx-c=0$ be an equation such that a,b,c are positive integers and successive terms of an arithmetic sequence in any order. Let these numbers be of the form $n, n+r, n+2r$, where n and r positive integers. M. K. Mahanthappa [2] investigated the rational roots of the equation, provided that $r=1$ and n positive integer. In the paper we generalize this problem for the case $r>1$.

Legyen az $ax^2+bx-c=0$ másodfokú egyenletben a, b és c valamilyen sorrendben egy pozitív egészekből álló számtani sorozat egymást követő tagjai. Tekintsük ezeket $n, n+r, n+2r$, alakban, ahol n és r pozitív egészek.

M. K. Mahanthappa [2] azt a problémát vetette fel, hogy $r=1$ esetén, mely pozitív egész n-ekre lesznek racionális gyökei az egyenletnek. Ez egész együtthatók esetén akkor és csak akkor teljesül, ha az egyenlet diszkriminánsa négyzetszám. Rögzített n és r esetén a három együttható sorrendjétől függően hat különböző egyenletet kapunk, de

csak három különböző diszkriminánst. Ezért elég a következő egyenleteket vizsgálni:

(1) $$nx^2+(n+2r)x-(n+r)=0\ ,$$

(2) $$(n+r)x^2+nx-(n+2r)=0\ ,$$

(3) $$nx^2+(n+r)x-(n+2r)=0\ .$$

Mahanthappa [2] $r=1$ esetén megadta az összes olyan n pozitív egészet, melyekre racionálisak a gyökök. Ezek az (1) egyenlet esetén $n=F_{2m}F_{2m+3}$, a (2) egyenlet esetén $n=F_{2m}F_{2m+1}-1$, és a (3) egyenlet esetén $n=F_{2m+1}-1$, ahol $m\geq 1$ egész, és F_k a Fibonacci sorozat k-adik tagja.

Most tekintsük az $r>1$ esetet. Ekkor egyszerű következményként kapjuk, hogy az (1) egyenletbe $n=rF_{2m}F_{2m+3}$, a (2) egyenletbe $n=rF_{2m}F_{2m+1}-r$, és a (3) egyenletbe $n=rF_{2m+1}-r$ helyettesítve, ahol $m\geq 1$ egész, racionálisak lesznek a gyökök. Nevezzük ezeket triviális választásoknak.

A dolgozat célja, hogy találjunk nem triviális pozitív egész n-eket, melyekre szintén racionálisak a gyökök.

A következő tételeket bizonyítjuk:

1. Tétel: Legyen az $r>1$ egész $r=u^2-uv-v^2$ alakú, ahol u és v pozitív valós számok. Legyen $\{R_k\}(k=0,1,2,\ldots)$ egy másodrendű lineáris rekurzív sorozat, melyet az $R_0=v, R_1=u$ kezdőelemek és az $R_k=R_{k-1}+R_{k-2}$ rekurzió definiál, ahol $k>1$ egész. Legyen továbbá $N_m=R_{2m}R_{2m+3}$, ahol $m\geq 0$ egész.

Ha N_m egész és r nem osztója N_m-nek, akkor $n = N_m$ esetén (1) egyenletnek racionálisak a gyökei, és n nem triviális választás.

2. Tétel: Az előző tételben definiált r és R_k esetén legyen $T_m = R_{2m}R_{2m+1}$, ahol $m \geq 1$ egész.

Ha T_m egész és r nem osztója T_m-nek, akkor $n = n = T_m - r$ esetén (2) egyenletnek racionálisak a gyökei, és n nem triviális választás.

3. Tétel: Legyen az $r > 1$ egész és $r^2 = u^2 - uv - v^2$, ahol u és v pozitív egészek. Legyen $\{R_k\}(k = 0,1,2,\ldots)$ egy másodrendű lineáris rekurzív sorozat, melyet az $R_0 = v, R_1 = u$ kezdőelemek és az $R_k = R_{k-1} + R_{k-2}$ rekurzió definiál, ahol $k > 1$ egész.

Ha r nem osztója R_{2m+1}-nek, ahol $m \geq 0$ egész, akkor $n = R_{2m+1} - r$ esetén (3) egyenletnek racionálisak a gyökei, és n nem triviális választás.

A tételek bizonyításához szükségünk lesz a következő lemmákra:

1. Lemma: Legyen $\{R_m\}(m = 0,1,2,\ldots)$ egy másodrendű lineáris rekurzív sorozat, melyet az R_0, R_1 nem mindkettő zérus valós kezdőelemek, A, B konstans egészek és az $R_m = AR_{m-1} + BR_{m-2}$ rekurzió definiál, ahol $m > 1$ egész. Legyenek a sorozat $x^2 - Ax - B$ karakterisztikus polinomjának a gyökei

$$\alpha = \frac{A + \sqrt{A^2 + 4B}}{2} \quad \text{és} \quad \beta = \frac{A - \sqrt{A^2 + 4B}}{2}.$$

Legyen továbbá $a = R_1 - R_0\beta$ és $b = R_1 - R_0\alpha$.

Tegyük fel, hogy a karakterisztikus polinom $D = A^2 + 4B$ diszkriminánsa nem nulla. Definiáljuk az $\{R_m\}$ sorozat $\{G_m\}$ asszociált sorozatát a

$$G_m = a\alpha^m + b\beta^m$$

formulával, ahol $m \geq 1$ egész. Ekkor

(4) $$R_m = \frac{a\alpha^m - b\beta^m}{\alpha - \beta} \qquad (m \geq 0),$$

(5) $$G_m = R_{m+1} + BR_{m-1} \qquad (m \geq 1),$$

és

(6) $$G_m^2 - DR_m^2 = 4(-B)^m(R_1^2 - AR_0R_1 - BR_0^2) \qquad (m \geq 1)$$

teljesül.

Megjegyzés: $A = B = 1$, $R_0 = 0$ és $R_1 = 1$ esetén az $\{R_m\}$ sorozat az ismert Fibonacci sorozatot szolgáltatja. Az $\{F_m\}$ Fibonacci sorozat asszociált sorozatát Lucas sorozatnak nevezzük és $\{L_m\}$-el jelöljük.

2. Lemma: Legyen az n pozitív egész olyan tulajdonságú, hogy az (1), (2), vagy (3) egyenlet gyökei racionálisak. Ekkor az n akkor és csak akkor triviális, ha r osztója n-nek.

1. Lemma bizonyítása: A (4) egyenlőség jól ismert, de teljes indukcióval is egyszerűen bizonyíthatjuk. (Lásd például D. Jarden [1].)

Az (5) egyenlőség az

$$a\alpha^m + b\beta^m = \frac{a\alpha^{m+1} - b\beta^{m+1}}{\alpha - \beta} - \alpha\beta\frac{a\alpha^{m-1} - b\beta^{m-1}}{\alpha - \beta}$$

és a $B = -\alpha\beta$ azonosságokból, továbbá a (4) egyenlőségből következik.

A (6) egyenlőséget $\alpha - \beta = \sqrt{D}$, $\alpha + \beta = A$ és $\alpha\beta = -B$ azonosságok segítségével, továbbá a (4) egyenlőséggel bizonyíthatjuk, hiszen

$$G_m^2 - DR_m^2 = \left(a\alpha^m + b\beta^m\right)^2 - D\left(\frac{a\alpha^m - b\beta^m}{\alpha - \beta}\right)^2 = 4ab(\alpha\beta)^m =$$

$$= 4(-B)^m(R_1 - R_0\beta)(R_1 - R_0\alpha) = 4(-B)^m\left(R_1^2 - AR_0R_1 - BR_0^2\right).$$

2. Lemma bizonyítása: Legyen az (1) egyenletnek racionálisak a gyökei. Ha r triviális választás, akkor $n = rF_{2m}F_{2m+3}$ $(m \geq 1)$, így r osztója n-nek. Ha $n = tr$, ahol $t \geq 1$ egész, akkor

$$trx^2 + (tr + 2r)x - (tr + r) = 0$$
$$tx^2 + (t + 2)x - (t + 1) = 0$$

aminek a feltétel miatt racionálisak a gyökei, így Mahanthappa említett eredményei alapján

$$t = F_{2m}F_{2m+3} \quad (m \geq 1)$$

és

$$n = rF_{2m}F_{2m+3} \quad (m \geq 1),$$

ami triviális választás. Hasonlóan bizonyíthatjuk az állítást a (2) és (3) egyenletekre is.

1. Tétel bizonyítása: Az (1) egyenlet diszkriminánsa

$$D_1 = (n+2r)^2 + 4n(n+r) = n^2 + (2(n+r))^2$$

Racionális gyökök esetén, és csak akkor D_1 négyzetszám, $D_1 = t^2$, ahol t egy pozitív egész. Ekkor $[n, 2(n+r), t]$ pitagoraszi számhármas.

Reprezentáljuk $[g^2 - h^2, 2gh, g^2 + h^2]$ alakban.

Ekkor $n = g^2 - h^2$ és $2(n+r) = 2gh$ miatt

$$g^2 - gh - (h^2 - r) = 0 \tag{7}$$

következik, ami g-re másodfokú egyenlet. Legyen a diszkriminánsa s^2.

Ekkor

$$s^2 = h^2 + 4(h^2 - r) = 5h^2 - 4r$$

illetve

$$s^2 - 5h^2 = -4r \ . \tag{8}$$

A tételben szereplő $\{R_k\}$ sorozat esetén $A = B = 1$ és $D = A^2 + 4B = 5$, ezért (6) miatt

$$G_k^2 - 5R_k^2 = (-1)^k 4r$$

minden $k \geq 1$ egész esetén. $s = G_{2m+1}$ és $h = R_{2m+1}$ választással, ahol $m \geq 0$ egész, (8) teljesül és (7) alapján, (5) felhasználásával

$$g = \frac{h+s}{2} = \frac{R_{2m+1} + R_{2m+2} + R_{2m}}{2} = R_{2m+2}$$

mert $g > 0$. Ekkor azonban

$$n = g^2 - h^2 = (R_{2m+2})^2 - (R_{2m+1})^2 = (R_{2m+2} - R_{2m+1})(R_{2m+2} + R_{2m+1}) =$$
$$= R_{2m}R_{2m+3} = N_m \quad (m \geq 0) .$$

Ha N_m egész és r nem osztja N_m-et, akkor a 2. lemma miatt n nem triviális választás, és ezzel a tételt igazoltuk.

2. Tétel bizonyítása: A (2) egyenlet diszkriminánsa

$$D_2 = n^2 + 4(n+r)(n+2r) = (2(n+r))^2 + (n+2r)^2 .$$

Racionális gyökök esetén, és csak akkor D_2 négyzetszám, $D_2 = t^2$, ahol t egy pozitív egész. Ezért $[2(n+r), n+2r, t]$ pitagoraszi számhármas. Reprezentáljuk $[2gh, g^2 - h^2, g^2 + h^2]$ alakban. Ebből hasonlóan az előzőhöz, azt kapjuk, hogy

$$n = R_{2m}R_{2m+1} - r = T_m - r \quad (m \geq 1)$$

esetén ha T_m egész és r nem osztója T_m-nek, akkor a (2) egyenletnek racionálisak a gyökei és n nem triviális választás.

Megjegyzés: Ha az 1. tétel bizonyításában $[2gh, g^2 - h^2, g^2 + h^2]$, illetve a 2. tétel bizonyításában $[g^2 - h^2, 2gh, g^2 + h^2]$ reprezentációt tekintjük, nem kapunk újabb n-eket.

3. Tétel bizonyítása: A (3) egyenlet diszkriminánsa

$$D_3 = (n+r)^2 + 4n(n+2r) = 5(n+r)^2 - 4r^2 .$$

Racionális gyökök esetén, és csak akkor D_3 négyzetszám, $D_3 = t^2$, ahol t egy pozitív egész és

(9) $$t^2 - 5(n+r)^2 = -4r^2 \ .$$

A tétel feltételei és (6) miatt

$$(G_{2m+1})^2 - 5(R_{2m+1})^2 = -4r^2 \ (m \geq 0) \ .$$

Ezért $n = R_{2m+1} - r$ esetén, ha r nem osztója R_{2m+1}-nek, (3) gyökei racionálisak és n nem triviális választás.

Megjegyzés: A 3. tétel feltételei nem minden $r > 1$ egész esetén teljesíthetők. Például $r = 2$ esetén (9) miatt

$$t^2 - 5(n+2)^2 = -16.$$

Ez csak páros n esetén állhat fenn, így racionális gyökök esetén n csak triviális választás lehet. Ennek következménye, hogy

$$x^2 - 5y^2 = -16 \ .$$

összes egész megoldása

$$(x, y) = (\pm 2L_{2m+1}, \pm 2F_{2m+1}),$$

illetve

$$x^2 - 5y^2 = 16$$

összes egész megoldása

$$(x, y) = (\pm 2L_{2m}, \pm F_{2m})$$

ahol F_k, illetve L_k a k-adik Fibonacci, illetve Lucas szám és $m \geq 0$ egész.

Másrészt ha $r = 11$, akkor $R_0 = 3$ és $R_1 = 13$, vagy $R_0 = 7$, és $R_1 = 17$ esetén teljesülnek a tétel feltételei.

Megjegyzés: A cikk leadása után (Fifth International Conference on Fibonacci Numbers and Their Applications, St. Andrews, 1992. július 22—24, konferencián elhangzott előadás nyomán) tudomásunkra jutott, hogy C. Long, G. L.

Cohen, T. Langtry és A. G. Shannon a jelen cikkben leírtakkal hasonló eredményekre jutottak.

IRODALOM

[1] D. Jarden, Recurring sequences, Riveon Lematematika, Jerusalem (Israel), 1958.

[2] M. K. Mahanthappa. Arithmetic sequences and Fibonacci quadratics. Fibonacci Quarterly 29 (1991), 343—346.

LIPTAI KÁLMÁN

PELL EGYENLETEK MEGOLDÁSA LINEÁRIS REKURZÍV SOROZATOK SEGÍTSÉGÉVEL

Abstract: *(On solution of Pell equation by the help of linear recurrences)* In the paper we investigate Pell equation, $x^2 - Dy^2 = N$, where N is positive integer and D is positive, not a perfect square integer. We prove that if Pell equation has a solution, then (G_n, H_n) pairs determine the all solutions, where $G(2u_0, 1, G_0, G_1)$ and $H(2u_0, 1, H_0, H_1)$ linear recurrences. The number of recurrences is finite.

Legyenek A, B, G_0, G_1 rögzített egész számok, melyekre $AB \neq 0$ és G_0, G_1 nem mindkettője zérus. Az egész számok $G_0, G_1, G_2, \ldots$ végtelen sorozatát, ahol

$$G_n = AG_{n-1} - BG_{n-2}, \quad \text{ha} \quad n > 1,$$

másodrendű rekurzív sorozatnak nevezzük és G-vel, illetve $G(A, B, G_0, G_1)$-el jelöljük. A következőkben hasonlóan definiáljuk és jelöljük a különböző adatokkal megadott másodrendű lineáris rekurzív sorozatokat.

Egy $G(A, B, G_0, G_1)$ sorozat asszociált sorozatának nevezzük azt a $H_0 = 2G_1 - AG_0$ és $H_1 = AG_1 - BG_0$.

Az általános G sorozat három speciális esete az $F = F(1,-1,0,1)$ Fibonacci sorozat, az $L = L(1,-1,2,1)$ Lucas sorozat, mely a Fibonacci sorozat asszociált sorozata, és a $P = P(2,-1,0,1)$ Pell sorozat.

Rögzített nem teljes négyzet pozitív egész D mellett az $x^2 - Dy^2 = N$ alakú Pell egyenletek és a másodrendű lineáris rekurzív sorozatok között több kapcsolat ismert. Néhány jellemző eredményt felsorolunk.

V. E. Hoggatt [5] bizonyította, hogy az $x^2 - 5y^2 = \pm 4$ egyenlet egyedüli megoldásai $x = \pm L_n$, $y = \pm F_n$ $(n = 0,1,2,...)$, ahol L_n, illetve F_n a Lucas, illetve Fibonacci sorozat n-edik tagja.

E. M. Cohn [3], I. Adler [1], [2] és V. Thébault [11] az $x^2 - 2y^2 = \pm 1$ egyenlet és a másodrendű rekurzív sorozatok, illetve a Pell sorozat között találtak hasonló kapcsolatot.

M. J. de Leon [8] bizonyította, hogy ha x_0, y_0 egy megoldása $x^2 - 2y^2 = N$ egyenletnek, akkor azon (x_n, y_n) számpárok is megoldásai, melyre

$$x_n + y_n = (x_0 + y_0)P_{2^n+1} + y_0 P_{2^n}$$

és

$$y_n = (x_0 + y_0)P_{2^n} + y_0 P_{2^n-1},$$

ahol P_i a Pell sorozat i-edik tagja.

Kiss Péter és Várnai Ferenc [6] bizonyította, hogy az $x^2 - 2y^2 = N$ egyenlet összes megoldása megadható véges számú $P(2,-1,P_0,P_1)$ sorozat elemeiből alkotott számpárokkal: $(x,y) = \left(\pm\left(P_{2^n} + P_{2^n+1}\right), \pm P_{2^n+1}\right)$.

Ezen tétel általánosítását bizonyította Kiss Péter [7], mely szerint, ha rögzített $a>0$ egész szám esetén az $x^2-(a^2+1)y^2=N$ egyenletnek létezik megoldása, akkor az összes megoldást véges számú $G(2a,-1,G_0,G_1)$ sorozat tagjaiból képzet

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

párok szolgáltatják, ahol $N>0$ esetén

$$0\le G_1<2a\sqrt{N}\ ,$$

$N<0$ esetén pedig

$$0<G_1<\left(2a^2+1\right)\sqrt{\frac{-N}{\left(a^2+1\right)}}\ .$$

Az idézett cikkben Kis Péter V. E. Hoggatt [5] fentebb idézett eredményét is általánosítja, azaz ha $x^2-(a^2-4)y^2=4N$ egyenletnek van x,y egész megoldása, akkor az összes megoldást véges számú $G(a,1,G_0,G_1)$ sorozat segítségével képzett $(x,y)=\left(\pm H_{2^n},\pm G_{2^n}\right)$ számpárok szolgáltatják, ahol H a G asszociált sorozat és $N>0$ esetén $0<G_1<\sqrt{N}$, $N<0$ esetén

$$0\ne G_1<a\sqrt{\frac{-N}{a^2-4}}\ .$$

T. Nagell [9] megmutatta, hogy tetszőleges Pell egyenletnek véges számú megoldása van.

A következőkben megmutatjuk, hogy a Pell egyenletek megoldásai tetszőleges D esetén (ha az egyenlet megoldható) másodrendű rekurzív sorozatokra vezethetők vissza, és az egyenlet összes megoldását véges számú másodrendű rekurzív sorozat tagjaiból képzett párok szolgáltatják.

A továbbiakban felhasználjuk azt a jól ismert tényt, hogy az $x^2 - Dy^2 = 1$ egyenletnek végtelen sok megoldása van, ha $D > 0$ és nem teljes négyzet. A megoldások között alapmegoldásnak nevezzük a triviális $(x,y) = (1,0)$ megoldástól különböző legkisebb pozitív (x,y) megoldást. A következő tételt bizonyítjuk:

Tétel. Legyenek N és D egész számok, $N \neq 0$ és D nem teljes négyzet pozitív egész feltétellel. Legyen $(u_0 v_0)$ az

(1) $$x^2 - Dy^2 = 1$$

egyenlet alapmegoldása. Ha az

(2) $$x^2 - Dy^2 = N$$

egyenletnek van x_0, y_0 pozitív egész megoldása, akkor az összes megoldást véges számú $G(2u_0, 1, G_0, G_1)$ és $H(2u_0, 1, H_0, H_1)$ sorozat segítségével képzett $(x,y) = (G_n, H_n)$ számpárok szolgáltatják. Továbbá ezen H sorozatokra $N > 0$ esetén $0 \leq H_0 < v_0\sqrt{N}$ és $N < 0$ esetén $0 < H_0 < \sqrt{\frac{-Nu_0^2}{D}}$.

Megjegyzés. (1.) N. Ginatempo [4] eredménye alapján a H_0-ra tett feltétel kizárólagos N és D függvényeként is kifejezhető. A tétel szerint az $x^2 - Dy^2 = 1$ egyenletnek, ahol D nem négyzetszám, van olyan nem triviális megoldása, amely kielégíti az $x < (q+1)E$ és $y < E$ egyenlőtlenségeket, ahol $E = 2(q+1)\left(\frac{2}{3}q + 1\right)^{2q}$ és $q = \left[\sqrt{D}\right]$.

(2.) Kiss Péter említett eredménye tételünkből adódik. Legyen ugyanis $D=a^2+1$, akkor $u_0=2a^2+1, v_0=2a$ és a tételünk szerint az

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

egyenletnek a megoldásai olyan a $G(2u_o,1,G_0,G_1)$ és $H(2u_0,1,H_0,H_1)$ sorozat tagjaiból képzett $(x,y)=(G_i,H_i)$ számpárok alkotják, ahol

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

és

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

Bizonyítás. Tegyük fel, hogy (2) megoldható és (x_0,y_0) egy megoldás. Ismert, hogy ha

(3) $$x_n+\sqrt{D}y_n=(x_0+\sqrt{D}y_0)(u_0+\sqrt{D}v_0)^n\quad (n=0,1,2,\ldots),$$

akkor (x_n,y_n) számpár is megoldása a (2) egyenletnek. (Lásd például Niven–Zuckerman: Bevezetés a számelméletbe, 153. oldal [10].) Ekkor

(4) $$x_n-\sqrt{D}y_n=(x_0-\sqrt{D}y_0)(u_0-\sqrt{D}v_0)^n\quad (n=0,1,2,\ldots)$$

is fennáll. A (3) és (4) egyenletek segítségével x_n és y_n meghatározható:

(5) $$x_n=\frac{x_0+\sqrt{D}y_0}{2}\alpha^n+\frac{x_0-\sqrt{D}y_0}{2}\beta^n$$

(6) $$y_n=\frac{x_0+\sqrt{D}y_0}{2\sqrt{D}}\alpha^n-\frac{x_0-\sqrt{D}y_0}{2\sqrt{D}}\beta^n$$

ahol $\alpha = u_0 + \sqrt{D}v_0$ és $\beta = u_0 - \sqrt{D}v_0$. Jól ismert, hogy ha $G = G(A,B,G_0,G_1)$ egy másodrendű rekurzív sorozat és α és β a sorozat

(7) $$f(x) = x^2 - Ax + B$$

karakterisztikus polinomjának két gyökét jelöli, akkor a G sorozat tagjai

(8) $$G_n = \frac{b\alpha^n - c\beta^n}{\alpha - \beta} \quad (n = 1,2,\ldots)$$

alakban is megadhatók, ahol $b = G_1 - G_0\beta$ $c = G_1 - G_0\alpha$. Azaz x_n és y_n tekinthető egy $X(A,B,x_0,x_1)$ és $Y(A,B,y_0,y_1)$ másodrendű rekurzív sorozat n-edik elemének.

α és β ismeretében az A és B konstansok meghatározhatók. Az $\alpha\beta = B$ és $\alpha + \beta = A$ egyenletekből $B = 1$ és $A = 2u_0$ következik, mert esetünkben

$$\alpha\beta = (u_0 + \sqrt{D}v_0)(u_0 - \sqrt{D}v_0) = {u_0}^2 - D{v_0}^2 = 1$$

és

$$\alpha + \beta = 2u_0 .$$

Az (5) és (6) egyenlet segítségével x_1, y_1 meghatározható:

(9) $$x_1 = x_0u_0 + Dy_0v_0$$

és

(10) $$y_1 = x_0v_0 + y_0u_0$$

adódik.

Ekkor az X és Y másodrendű rekurzív sorozatok egyértelműen meg vannak határozva.

Az

$$x_{n+1} = Ax_n - Bx_{n-1} = 2u_0x_n - x_{n-1}$$

és

$$y_{n+1} = Ay_n - By_{n-1} = 2u_0y_n - y_{n-1}$$

rekurziós összefüggésekből x_{n-1}, y_{n-1} is meghatározható a

(11) $$Bx_{n-1} = Ax_n - x_{n+1},$$

azaz $x_{n-1} = 2u_0x_n - x_{n+1}$ és

(12) $$By_{n-1} = Ay_n - y_{n+1},$$

azaz $y_{n-1} = 2u_0y_n - y_{n+1}$ egyenletek segítségével, azaz a sorozat i -edik és $(i+1)$-edik elemének ismeretéből az $(i-1)$-edik elem is meghatározható. Tekintsük a $G(2u_0, 1, G_0, G_1)$ és $H(2u_0, 1, H_0, H_1)$ másodrendű rekurzív sorozatokat, ahol $G_i = x_0$, $G_{i+1} = x_1$, $H_i = y_0$, $H_{i+1} = y_1$ valamely i index esetén. Nyilvánvaló, hogy ezen G, illetve H sorozatok indexeléstől eltekintve azonosak az X, illetve Y sorozatokkal és a (G_{i+k}, H_{i+k}) $(k = 0,1,2...)$ számpárok kielégítik a (2) egyenletet. Megmutatjuk, hogy a (G_{i-1}, H_{i-1}) számpárok is kielégíti a (2) egyenlet, amiből következik, hogy a (G_{i+k}, H_{i+k}) $(k = 0,-1,-2...)$ számpárok is megoldásai (2)-nek, melyek $B = 1$ miatt szintén egészek. A

$$G_{i-1}^2 - DH_{i-1}^2 = N$$

egyenlőség, $A = 2u_0$, $B = 1$, valamint (10), (11) alapján adódó

$$G_{i-1} = 2u_0x_o - x_1 \quad \text{és} \quad H_{i-1} = 2u_0y_o - y_1$$

összefüggések felhasználásával adódik, ugyanis

$$(2u_0x_0 - x_1)^2 - D(2u_0y_0 - y_1)^2 =$$
$$= 4u_0^2(x_0^2 - Dy_0^2) + x_1^2 - Dy_1^2 + 4u_0(Dy_0y_1 - x_0x_1) =$$
$$= 4u_0^2N + N + 4u_0(Dy_0y_1 - x_0x_1) = N,$$

mivel (9) és (10) miatt

$$Dy_0y_1 - x_0x_1 = Dy_0(y_0u_0 + x_0v_0) - x_0(x_0u_0 + Dy_0v_0) =$$
$$= -u_0(x_0^2 - Dy_0^2) = -u_0N.$$

Ezután megmutatjuk, hogy ha H_i nem esik a tételben szereplő intervallumok egyikébe sem, akkor $G_{i-1} \geq 0$ és $H_{i-1} \geq 0$ teljesül. Nézzük meg mi a feltétele a

$$G_{i-1} = 2u_0G_i - G_{i+1} \geq 0$$

egyenlőség fennállásának. Ez (9) alapján

$$2u_0G_i - G_iu_0 - DH_iv_0 = G_iu_0 - DH_iv_0 = \sqrt{N + DH_i^2}u_o - DH_iv_0 \geq 0$$

alakban is írható, mivel $G_i^2 - DH_i^2 = N$. Ezzel ekvivalens állítás, hogy

$$\left(N + DH_i^2\right)u_0^2 \geq D^2H_i^2v_0^2$$

azaz $u_0^2 - Dv_0^2 = 1$ miatt

$$DH_i^2 \geq -Nu_0^2$$

ami $N > 0$ esetben triviálisan teljesül, az $N < 0$ esetben pedig a H_i-re tett feltétel miatt igaz. Hasonlóan (10) alapján

$$H_{i-1} = 2u_0H_i - H_{i+1} = 2u_0H_i - H_iu_0 - G_iv_0 = H_iu_0 - G_iv_0 =$$
$$= u_0H_i - v_0\sqrt{H_i^2D + N} \geq 0$$

teljesül, ha

$$H_i^2\left(u_0^2 - Dv_0^2\right) \geq v_0^2N$$

vagyis ha

$$H_i^2 \geq v_0^2N.$$

Ez pedig igaz, ha $N < 0$, vagy ha $N > 0$ és $H_i > v_0\sqrt{N}$. A következő lépésben belátjuk, hogy $H_{i-1} < H_i$ és $G_{i-1} < G_i$, ha $N < 0$ és $H_i \geq \sqrt{\frac{-Nu_0^2}{D}}$ vagy ha $N > 0$ és $H_i \geq v_0\sqrt{N}$.

Mivel (10) és (12) alapján

$$H_{i-1} = 2u_0H_i - H_{i+1} = 2u_0H_i - H_iu_0 - G_iv_0 = H_iu_0 - G_iv_0,$$

továbbá

$$G_i^2 - DH_i^2 = N$$

miatt

$$G_i = \sqrt{N + DH_i^2} \ ,$$

ezért azt kell megvizsgálnunk, hogy milyen feltételek mellett teljesül a

$$H_i u_0 - v_0 \sqrt{N + DH_i^2} < H_i$$

egyenlőtlenség. Ez azonban

$$H_i^2 (u_0 - 1)^2 < N v_0^2 + DH_i^2 v_0^2$$

azaz $u_0^2 - Dv_0^2 = 1$ miatt

(13) $$H_i^2 (2 - 2u_0) < N v_0^2$$

egyenlőtlenséggel ekvivalens, ami $N > 0$ esetén nyilván mindig teljesül. $N < 0$ esetén (13) alapján $H_{i-1} < H_i$, ha

$$H_i > \sqrt{\frac{-N v_0^2}{2(u_0 - 1)}} \ .$$

Ez pedig igaz, ha

$$H_i > \sqrt{\frac{-N u_0^2}{D}},$$

mert $u_0 > 1$ miatt

$$\frac{v_0^2}{2(u_0 - 1)} = \frac{u_0^2 - 1}{2D(u_0 - 1)} = \frac{u_0 + 1}{2D} < \frac{u_0^2}{D}.$$

Ezzel állításunk H_{i-1}-re vonatkozó részét bebizonyítottuk. Tekintsük most a $G_{i-1} < G_i$ egyenlőtlenséget. (9) és (11) alapján

$$G_{i-1} = 2u_0 G_i - G_i u_0 - DH_i v_0 = G_i u_0 - Dv_0 H_i,$$

ezért $G_{i-1} < G_i$ ekvivalens az $G_i u_0 - Dv_0 H_i < G_i$ egyenlőtlenséggel, továbbá

$$G_i^2 - DH_i^2 = N$$

miatt

$$G_i = \sqrt{N + DH_i^2} \quad .$$

Meg kell vizsgálnunk, hogy milyen feltételek mellett teljesül az

$$u_0\sqrt{N + DH_i^2} - Dv_0H_i < \sqrt{N + DH_i^2}$$

egyenlőség. Ez azonban

$$(u_0 - 1)\sqrt{N + DH_i^2} < Dv_0H_i$$

$$(u_0 - 1)^2\left(N + DH_i^2\right) < D^2v_0^2H_i^2$$

azaz $u_0^2 - Dv_0^2 = 1$ miatt

$$N(u_0 - 1)^2 < D(u_0^2 - 1)H_i^2 - (u_0 - 1)^2 DH_i^2$$

illetve

$$N(u_0 - 1)^2 < 2DH_i^2(u_0 - 1)$$

és

(14) $$N(u_0 - 1) < 2DH_i^2$$

egyenlőtlenséggel ekvivalens. $N < 0$ esetben nyilvánvalóan teljesül. $N > 0$ esetén (14) alapján $G_{i-1} < G_i$, ha

$$H_i > \sqrt{\frac{N(u_0 - 1)}{2D}} \quad .$$

Ez pedig igaz, ha

$$H_i > v_0\sqrt{N},$$

mert $u_0 > 1$ miatt

$$\frac{u_0 - 1}{2D} < \frac{(u_0 - 1)^2}{D} = v_0^2 \quad .$$

Ezzel állítsunk G_i-re vonatkozó részét is bizonyítottuk. Ezek szerint előállítható az (x, y) megoldások (G_i, H_i), (G_{i-1}, H_{i-1}), (H_{i-2}, H_{i-2})... sorozata úgy, hogy valamely k-ra

$H_i > H_{i-1} > \ldots > H_{i-k} \geq 0$ és $G_i > G_{i-1} > \cdots > G_{i-k} \geq 0$

továbbá H_{i-k} a tételben adott intervallumok valamelyikébe esik. Ezért $i = k$ választással kapott G és H sorozatok meghatározzák a (2) egyenlet egy megoldás sorozatát. Ezen sorozatok száma nyilvánvalóan véges a kezdőértékre adott korlátok miatt, hiszen A, B rögzítettek.

IRODALOM

[1] I. Adler, Three diophantine equations I., Fibonacci Quart., 6 (1968), 360–369, 371.

[2] Adler, Three diophantine equations I., Fibonacci Quart., 7 (1969), 181–193.

[3] E. M. Cohn, Complette diophantine solution of the Pythagorean triple $(a, b = a+1, c)$, 437 and 448.

[4] N. Ginatempo, Il metodo dei tentativi per la risoluzione della equazione di Pell-Fermat, Istituto di Matematica dell'Universita di Messina, Pubblicazione No.1., (1969).

[5] V. E. Hoggatt, Some more Fibonacci diphantine equations, Fibonacci Quart., 9 (1971) 437 and 448.

[6] P. Kiss and F. Várnai, On generalized Pell numbers, Math. Sem. Not. (Kobe Univ. Japan), 6 (1978), 259–267.

[7] P. Kiss P., Pell egyenletek megoldása lineáris rekurzív sorozatok segítségével, Acta Acad. Paed. Agrienses, 17 (1984), 813–824.

[8] M. J. de Leon, Pell's equation and Pell number triples, Fibonacci Quart., 14 (1976), 456–460.

[9] T. Nagell, An elementary method for the determination of lattice points on a hyperbola, Norsk Mat. Tidsskr, 26, 60–65, (1944).
[10] Niven-Zuckerman: Bevezetés a számelméletbe, Műszaki Könyvkiadó, (1978).
[11] V. Thébault, Sur les suites de Pell, Mathesis, 65 (1956), 390–395.

ZAY BÉLA

EGY REKURZÍV SOROZATRÓL*

Abstract: (On a recursive sequence). Let k and t be fixed positive integers. Define a sequence $G_{k,t}(n)$, $n = 0,1,2,\ldots$, by

$$G_{k,t}(n) = \begin{cases} n & \text{if } n = 0,1,\ldots,t-1 \\ n - G_{k,t}^{(k)}(n-t) & \text{if } n \geq t \end{cases}$$

where

$$G_{k,t}^{(1)}(n-t) = G_{k,t}(n-t)$$

and

$$G_{k,t}^{(j)}(n-t) = G_{k,t}\left(G_{k,t}^{(j-1)}(n-t)\right)$$

for $j > 1$. In this paper we investigate the properties of the sequence $G_{k,t}$. Among others we show that the terms of our sequence can be determined by the terms of the sequence $G_{k,1}$ and prove a connection between the sequence $G_{k,t}$ and the Zeckendorf representation of natural numbers.

Legyenek k és t rögzített pozitív egészek, és definiáljunk egy $G_{k,t}(n)$, $n = 0,1,2,\ldots$, sorozatot a következőképpen:

---

* Az OTKA 1641. sz. pályázat támogatásával készült.

(1) $G_{k,t}(n) = \begin{cases} n, & \text{ha } n = 0,1,\ldots,t-1, \\ n - G_{k,t}^{(k)}(n-t), & \text{ha } n \geq t, \end{cases}$

ahol $G_{k,t}^{(1)}(n-t) = G_{k,t}(n-t)$ és $G_{k,t}^{(j)}(n-t) = G_{k,t}\left(G_{k,t}^{(j-1)}(n-t)\right)$, ha $j > 1$.

A $k = 2$, $t = 1$ speciális esettel V. Granville és J. P. Rasson [2] foglalkoztak, és bebizonyították, hogy:

(2) $G_{2,1}(n) = \left[(n+1) \cdot \frac{\sqrt{5}-1}{2} \right]$ $\qquad n = 0,1,2,\ldots,$

(Itt, és a továbbiakban is [ ] az "egészrész" függvényt jelenti.)

Az alábbiakban az általános $G_{k,t}$ sorozat tulajdonságait vizsgáljuk. Megmutatjuk a sorozat néhány tulajdonságát (1–4. Lemma), bebizonyítjuk, hogy az általános sorozat visszavezethető a $t = 1$ speciális esetre (1. Tétel), továbbá a természetes számok úgynevezett Zeckendorf reprezentációjával kapcsolatban bizonyítunk egy tételt (2. Tétel).

1. Tétel:

$$G_{k,t}(n) = \begin{cases} t \cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right), & \text{ha } G_{k,1}\left(\left[\frac{n}{t}\right]\right) = G_{k,1}\left(\left[\frac{n}{t}+1\right]\right), \\ t \cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right) + n - t \cdot \left[\frac{n}{t}\right], & \text{különben.} \end{cases}$$

A (2) és a tétel alapján, a $G_{2,t}$ sorozatra a következő adódik:

1. Következmény:

$$G_{2,t}(n) = \begin{cases} t \cdot \left[\left[\frac{n}{t}+1\right] \cdot \frac{\sqrt{5}-1}{2}\right], & \text{ha } \left[\left[\frac{n}{t}+1\right] \cdot \frac{\sqrt{5}-1}{2}\right] = \left[\left[\frac{n}{t}+2\right] \cdot \frac{\sqrt{5}-1}{2}\right], \\ t \cdot \left[\left[\frac{n}{t}+1\right] \cdot \frac{\sqrt{5}-1}{2}\right] + n - t\left[\frac{n}{t}\right], & \text{különben.} \end{cases}$$

Az 1. Tételből adódik a következő eredmény is.

2. Következmény: Ha n_1, n_2, m pozitív egészek, n_1, $n_2, n_2 \geq m^2$, és $n_1 \equiv n_2 \pmod{m}$ akkor:

$$G_{k,t_1}(n_1) - G_{k,t_2}(n_2) = \frac{n_1 - n_2}{m} \cdot G_{k,1}(m)$$

ahol $t_i = \left[\frac{n_i}{m}\right]$, $i = 1,2$-re.

A (2) alapján megmutatjuk a $G_{2,1}$ sorozatnak és a Fibonacci számoknak egy kapcsolatát. Ismert, hogy minden n természetes szám egyértelműen állítható elő $n = \sum_{i=1}^{r} F(n_i)$ alakban, ahol $n_1 < n_2 < \ldots < n_r$ természetes számok $n_{i+1} - n_i \geq 2$ feltétellel, és $F(n)$ az $F(0) = 0$, $F(1) = 1$, $F(n) = F(n-1) + F(n-2)$, (ha $n > 1$) feltételekkel definiált Fibonacci sorozat (lásd például [1]). A következő tételt bizonyítjuk:

2. Tétel: Tetszőleges n pozitív egész esetén,

ha $n = \sum_{i=1}^{r} F(n_i)$, ahol $n_1, n_2 \ldots n_r$ pozitív egészek, $n_1 > 1$

és $n_{i+1} - n_i \geq 2$ minden $i = 1,2,\ldots,r-1$-re

akkor

$$G_{2,1}\left(\sum_{i=1}^{r} F(n_i + 1)\right) = n$$

Megjegyzések:

1. A (2)-höz hasonló egyenlőség $k > 2$ esetén általában nem igaz. Tegyük fel ugyanis, hogy van olyan s_k egész szám és α_k valós szám, hogy $G_{k,1}(n) = \left[(n + s_k) \cdot \alpha_k\right]$. Ekkor

$$\lim_{n\to\infty} \frac{G_{k,1}(n)}{n} = \alpha_k.$$

De ha létezik $\lim_{n\to\infty} \frac{G_{k,1}(n)}{n} = \alpha_k$, akkor a definícióból adódó

$$\frac{G_{k,1}(n)}{n} = 1 - \frac{G_{k,1}^{(k)}(n-1)}{G_{k,1}^{(k-1)}(n-1)} \cdot \frac{G_{k,1}^{(k-1)}(n-1)}{G_{k,1}^{(k-2)}(n-1)} \cdot \ldots$$
$$\frac{G_{k,1}^{(2)}(n-1)}{G_{k,1}(n-1)} \cdot \frac{G_{k,1}(n-1)}{n-1} \cdot \frac{n-1}{n}$$

egyenlőségből következnek, hogy α_k az $x^k + x - 1 = 0$ egyenlet pozitív valós gyöke. Numerikus számolással azonban igazolható, hogy például $k = 3$ esetén nincs a feltételeknek eleget tevő s_3 konstans. Ugyanis ekkor $\alpha_3 \sim 0{,}682328$ és

$[(2+1)\cdot\alpha_3] = 2 > 1 = G_{3,1}(2)$-ből $s_3 < 1$ következne, viszont

$[(18+1)\cdot\alpha_3] = 12 < 13 = G_{3,1}(18)$-ból $s_3 > 1$ adódna.

2. Az előzőekben említett határérték viszont létezik.

[3]-ban Kiss Péterrel közösen bizonyítottuk, hogy

$$\lim_{n\to\infty} \frac{G_{k,1}(n)}{n} = \alpha_k,$$

ahol α_k az $x^k + x - 1 = 0$ egyenlet pozitív valós gyöke.

3. Könnyen bizonyítható, hogy a $G_{k,1}(n)$ sorozatban legfeljebb két egyenlő szomszédos tag van, ilyen pár viszont végtelen sok.

Az 1. Tétel bizonyítását 4 segédtétel segítségével végezzük el, s először ezeket bizonyítjuk.

1. Lemma: $G_{k,t}(n)$ definiálva van minden n természetes számra.

Bizonyítás: Elegendő belátni, hogy $0 \le G_{k,t}(n) \le n$ minden n természetes számra. Ezt teljes indukcióval bizonyítjuk.

$n = 0, 1, \ldots, t-1$-re $G_{k,t}(n)$ definíciója miatt nyilvánvalóan igaz az állítás, de $n = t$ esetén is igaz, mert (1) alapján $G_{k,t}(t) = t$. Legyen $n > t$ és tegyük fel, hogy minden $0 \le i \le n$ feltételt kielégítő i -re.

(3) $0 \le G_{k,t}(i) \le i$..

Ekkor $1 \le n+1-t \le n$ és így $i = n+1-t$-re (3)-ból

$$0 \le G_{k,t}(n+1-t) \le n+1-t$$

következik, de ekkor

$$G_{k,t}^{(2)}(n+1-t) = G_{k,t}\left(G_{k,t}(n+1-t)\right) \le G_{k,t}(n+1-t)$$

és folytatva az eljárást, a

$$(4) \qquad \begin{aligned} &0 \le G_{k,t}^{k}(n+1-t) \le G_{k,t}^{k-1}(n+1-t) \le \\ &\ldots \le G_{k,t}(n+1-t) \le n+1-t \le n \end{aligned}$$

egyenlőtlenség adódik. Így

$$1 \le n+1-G_{k,t}^{(k)}(n+1-t) \le n+1$$

azaz az (1) alapján

$$1 \le G_{k,t}(n+1) \le n+1,$$

amiből már következik az állítás.

2. Lemma: Legyenek n és t pozitív egész számok és $1 \le t \le n$.

Tegyük fel, hogy minden $1 \le i < n$. feltételt kielégítő i -re

(5') $G_{k,t}(i+1) = G_{k,t}(i)$

vagy

(5") $G_{k,t}(i+1) = G_{k,t}(i)+1.$

Ekkor minden j pozitív egész számra

(6') $G_{k,t}^{(j)}(n+1-t) = G_{k,t}^{(j)}(n-t)$

vagy

(6") $G_{k,t}^{(j)}(n+1-t) = G_{k,t}^{(j)}(n-t)+1$

teljesül.

Bizonyítás: j-re vonatkozó teljes indukcióval bizonyítjuk az állítást.

$j=1$-re a (6') az (5')-ből, a (6") az (5")-ből adódik $i=n-t$ helyettesítéssel.

Tegyük fel, hogy $j=r$-re (6') vagy (6")!

Ha $G_{k,t}^{(r)}(n+1-t) = G_{k,t}^{(r)}(n-t)$, akkor

$$G_{k,t}^{(r+1)}(n+1-t) = G_{k,t}\left(G_{k,t}^{(r)}(n+1-t)\right) =$$
$$= G_{k,t}\left(G_{k,t}^{(r)}(n-t)\right) = G_{k,t}^{(r+1)}(n-t).$$

Ha pedig $G_{k,t}^{(r)}(n+1-t) = G_{k,t}^{(r)}(n-t)+1$, akkor a

(7) $G_{k,t}^{(r+1)}(n+1-t) = G_{k,t}\left(G_{k,t}^{(r)}(n+1-t)\right) = G_{k,t}\left(G_{k,t}^{(r)}(n-t)+1\right)$

egyenlőség teljesül.

Az 1. Lemma bizonyításából

$0 \le G_{k,t}^{(r)}(n-t) \le n-t$ adódik,

ezért $i = G_{k,t}^{(r)}(n-t)$-re, az (5'), illetve (5") feltételekből

$$G_{k,t}\left(G_{k,t}^{(r)}(n-t)+1\right) = G_{k,t}\left(G_{k,t}^{(r)}(n-t)\right) = G_{k,t}^{(r+1)}(n-t)$$

vagy

$$G_{k,t}\left(G_{k,t}^{(r)}(n-t)+1\right) = G_{k,t}\left(G_{k,t}^{(r)}(n-t)\right)+1 = G_{k,t}^{(r+1)}(n-t)+1$$

adódik. Összevetve ezeket a (7) egyenlőséggel, azt kapjuk, hogy

$$G_{k,t}^{r+1}(n+1-t) = G_{k,t}^{r+1}(n-t)$$

vagy

$$G_{k,t}^{r+1}(n+1-t) = G_{k,t}^{r+1}(n-t)+1,$$

ami a teljes indukció gondolatmenete miatt bizonyítja az állítást.

3. Lemma: A $G_{k,t}(n)$ sorozat növekvő és szomszédos tagjainak a különbsége 0 vagy 1, azaz

(8') $G_{k,t}(n+1) = G_{k,t}(n)$

vagy

(8") $G_{k,t}(n+1) = G_{k,t}(n)+1$

minden $n \geq 0$ esetén.

Bizonyítás: Ismét teljes indukcióval bizonyítunk.

$n = 0,1,\ldots,t-1$ esetén az (1) definíció szerint:

$$G_{k,t}(n) = n,$$

így $n = 0,1,\ldots,t-2$re a (8") teljesül.

Szintén az (1) alapján $G_{k,t}(t) = t - G_{k,t}^{(k)}(0) = t$ és

$$G_{k,t}(t+1) = t+1-G_{k,t}^{(k)}(1) = t,$$

tehát $n = t-1$-re (8"), $n = t$-re pedig (8') áll fenn.

Legyen $n > t$ és tegyük fel, hogy minden i természetes számra, amelyre $0 \leq i < n$, teljesül a 3. Lemma állítása, azaz

$$G_{k,t}(i+1) = G_{k,t}(i),$$

illetve

$$G_{k,t}(i+1) = G_{k,t}(i)+1$$

egyike fennáll. Így teljesülnek a 2. Lemma feltételei.

Alkalmazzuk $j = k$-ra a 2. Lemmát! Ha

$G_{k,t}^{(k)}(n+1-t) = G_{k,t}^{(k)}(n-t)$ teljesül, akkor (1) alapján

$$G_{k,t}(n+1) = n+1-G_{k,t}^{(k)}(n+1-t) =$$
$$n+1-G_{k,t}^{(k)}(n-t) = G_{k,t}(n)+1$$

adódik. Ha pedig

$$G_{k,t}^{(k)}(n+1-t) = G_{k,t}^{(k)}(n-t)+1,$$

akkor

$$G_{k,t}(n+1) = n+1-G_{k,t}^{(k)}(n+1-t) =$$
$$= n+1-G_{k,t}^{(k)}(n-t) = G_{k,t}(n)+1 =$$
$$= n-G_{k,t}^{(k)}(n-t) = G_{k,t}(n).$$

4. Lemma: Minden $n \geq 0$ egész szám esetén

(9) $\quad G_{k,t}(n \cdot t) = t \cdot G_{k,1}(n).$

Bizonyítás: $n = 0$-ra nyilván igaz, hiszen $G_{k,t}(0 \cdot t) = 0 = t \cdot G_{k,1}(0)$

Tegyük fel, hogy minden $0 \leq m \leq n$-re teljesük (9), azaz

(9') $\quad G_{k,t}(m \cdot t) = t \cdot G_{k,1}(m).$

Mint ahogyan az 1. Lemma bizonyításában is láttuk:

$$0 \leq G_{k,1}^{(j)}(n) \leq n \qquad (j = 1,2,\ldots,k)$$

Így $m = G_{k,1}^{(j)}(n)$-re is teljesül a (9') egyenlőség, amit rendre $j = k-1, k-2, \ldots m\,2,1$-re alkalmazva:

$$t \cdot G_{k,1}^{(k)}(n) = t \cdot G_{k,1}\left(G_{k,1}^{(k-1)}(n)\right) = G_{k,1}\left(t \cdot G_{k,1}^{(k-1)}(n)\right) =$$
$$= G_{k,t}\left(t \cdot \left(G_{k,1}^{(k-2)}(n)\right)\right) = G_{k,t}^{2}\left(t \cdot G_{k,1}^{(k-2)}(n)\right) =$$
$$= \cdots = G_{k,t}^{(k-1)}\left(t \cdot G_{k,1}(n)\right) = G_{k,1}^{(k)}(n \cdot t)$$

adódik, amiből pedig (1) miatt

$$G_{k,t}((n+1)\cdot t) = (n+1)\cdot t - G_{k,t}^{(k)}((n+1)\cdot t - t) = (n+1)\cdot t - G_{k,t}^{(k)}(n \cdot t) =$$
$$= (n+1)\cdot t - t \cdot G_{k,1}^{(k)}(n) = t \cdot \left(n+1-G_{k,1}^{(k)}(n)\right) = t \cdot G_{k,1}(n+1)$$

következik, s ezzel a lemmát igazoltuk.

Az 1. Tétel bizonyítása: Tegyük fel először, hogy egy n természetes szám esetén

$$G_{k,1}\left(\left[\frac{n}{t}\right]\right) = G_{k,1}\left(\left[\frac{n}{t}+1\right]\right).$$

Ekkor a 4. Lemma alapján

(10)

$$G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t\right) = t\cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right) = t\cdot G_{k,1}\left(\left[\frac{n}{t}+1\right]\right) = G_{k,t}\left(\left[\frac{n}{t}+1\right]\cdot t\right).$$

Mivel $\left[\frac{n}{t}\right]\cdot t \le \frac{n}{t}\cdot t < \left[\frac{n}{t}+1\right]\cdot t$, és a 3. Lemma szerint $G_{k,t}(n)$ monoton növekvő, ezért

(11) $$G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t\right) \le G_{k,t}(n) \le G_{k,t}\left(\left[\frac{n}{t}+1\right]\cdot t\right)$$

A (11) egyenlőtlenséget (10) egyenlettel összevetve

$$G_{k,t}(n) = t\cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right)$$

adódik, ami az állítást első felét igazolja.

Ha

$$G_{k,1}\left(\left[\frac{n}{t}\right]\right) \neq G_{k,1}\left(\left[\frac{n}{t}+1\right]\right) = G_{k,1}\left(\left[\frac{n}{t}\right]+1\right)$$

akkor a 3. és 4. Lemmák alapján

$$G_{k,t}\left(\left(\left[\frac{n}{t}\right]+1\right)\cdot t\right) = t\cdot G_{k,1}\left(\left[\frac{n}{t}\right]+1\right) =$$

$$= \left(G_{k,1}\left(\left[\frac{n}{t}\right]\right)+1\right) = t\cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right)+t =$$

$$= G_{k,t}\left(t\cdot\left[\frac{n}{t}\right]\right)+t.$$

Tehát teljesül a

$$t = G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t + t\right) - G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t\right)$$

egyenlőség. Ez a 3. Lemma alapján azt jelenti, hogy minden olyan m természetes számra, melyre

$$\left[\frac{n}{t}\right]\cdot t \le m < m+1 \le \left[\frac{n}{t}\right]\cdot t + t,$$
$$G_{k,t}(m+1) - G_{k,t}(m) = 1$$

azaz

(12) $$G_{k,t}(m) - G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t\right) = m - \left[\frac{n}{t}\right]\cdot t.$$

a (12)-ből $m = n$-re, felhasználva a 4. Lemmát

$$G_{k,t}(n) = G_{k,t}\left(\left[\frac{n}{t}\right]\cdot t\right) + n - \left[\frac{n}{t}\right]\cdot t = t\cdot G_{k,1}\left(\left[\frac{n}{t}\right]\right) + n - \left[\frac{n}{t}\right]\cdot t$$

adódik, ami az állítás második részét igazolja.

Az 1. Következmény a (2) alapján triviálisan következik az 1. Tételből, ezért csak a 2. Következményt bizonyítjuk

A 2. Következmény bizonyítása:

$n_1 \equiv n_2 \pmod m$ miatt $n_i = m\cdot t_i + r$ $i = 1,2$-re, ahol r természetes szám és $0 \le r < m$.

$$n_i \ge m^2 \text{ miatt } t_i \ge m, \text{ így} \left[\frac{r}{t_i}\right] = 0.$$

Az 1. Tételből $t = t_i = \left[\frac{n_i}{m}\right]$, $n = n_i$, s így

$\left[\frac{n}{t}\right] = \left[\frac{n_i}{t_i}\right] = m + \left[\frac{r}{t_i}\right] = m$ helyettesítésekkel kapjuk a

$$G_{k,t_i}(n_i) = \begin{cases} t_i \cdot G_{k,1}(m) & \text{ha } G_{k,1}(m) = G_{k,1}(m+1) \\ t_i \cdot G_{k,1}(m) + r & \text{különben} \end{cases}$$

egyenlőséget, ami $i = 1$-re és $i = 2$-re alkalmazva, majd a kapott kifejezéseket egymásból kivonva, adódik az állítás, figyelembe véve, hogy $t_1 - t_2 = \frac{n_1 - n_2}{m}$.

A 2. Tétel bizonyítása:

A bizonyításban felhasználjuk a Fibonacci számok jól ismert

$$F(n) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

előállítását (lásd pl. [4]). Legyen n egy természetes szám és ennek

$$n = \sum_{i=1}^{r} F(n_i)$$

a 2. Tétel feltételeit kielégítő előállítása.

Mivel $n_{i+1} - n \geq 2$, $i = 1,2,\ldots,r-1$ és $n_1 \geq 2$, ezért $n_i \geq 2i > 2i - 1$, így

$$-1 < \frac{1-\sqrt{5}}{2} < 0$$

miatt

$$\left(\frac{1-\sqrt{5}}{2}\right)^{2i-1} < \left(\frac{1-\sqrt{5}}{2}\right)^{n_i} \leq \left(\frac{1-\sqrt{5}}{2}\right)^{2i},$$

ahonnan

$$\sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{2i-1} < \sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{n_i} \leq \sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{2i}$$

következik. Ebből a geometriai sorozat összegképletét és az $\left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{3-\sqrt{5}}{2}$ egyenlőséget alkalmazva,

$$\left(\frac{3-\sqrt{5}}{2}\right)^r - 1 < \sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{n_i} \leqq \frac{3-\sqrt{5}}{1-\sqrt{5}}\cdot\left(\left(\frac{3-\sqrt{5}}{2}\right)^r - 1\right)$$

adódik.

Innen pedig a

$$0 < \frac{\sqrt{5}-1}{2}\cdot\left(\frac{3-\sqrt{5}}{2}\right)^r < \frac{\sqrt{5}-1}{2}\left(1+\sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{n_i}\right) \leqq$$

$$\leqq \left(\frac{3-\sqrt{5}}{1-\sqrt{5}}\cdot\left(\left(\frac{3-\sqrt{5}}{2}\right)^r - 1\right) + 1\right)\cdot\frac{\sqrt{5}-1}{2} =$$

$$= \frac{3-\sqrt{5}}{2} - \left(\frac{3-\sqrt{5}}{2}\right)^{r+1} + \frac{\sqrt{5}-1}{2} < \frac{3-\sqrt{5}}{2} + \frac{\sqrt{5}-1}{2} = 1$$

egyenlőtlenség következik.

Tehát

$$(13) \qquad 0 < \frac{\sqrt{5}-1}{2}\cdot\left(1+\sum_{i=1}^{r}\left(\frac{1-\sqrt{5}}{2}\right)^{n_i}\right) < 1.$$

Alkalmazzuk a $G_{2,1}(n)$ sorozatot (2)-beli előállítását az $n = \sum_{i=1}^{r} F(n_i)$ helyettesítéssel, és használjuk a Fibonacci számok explicit előállítását! Ekkor

$$G_{2,1}\left(\sum_{i=1}^{r} F(n_i+1)\right) = \left[\frac{\sqrt{5}-1}{2}\cdot\left(1+\sum_{i=1}^{r} F(n_i+1)\right)\right] =$$

$$= \left[\frac{\sqrt{5}-1}{2} + \frac{\sqrt{5}-1}{2}\cdot\sum_{i=1}^{r}\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n_i+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n_i+1}\right)\right]$$

$$= \sum_{i=1}^{r} F(n_i) + \left[\frac{\sqrt{5}-1}{2} + \sum_{i=1}^{r}\frac{1}{\sqrt{5}}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^{n_i} + \sum_{i=1}^{r}\frac{1}{\sqrt{5}}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^{n_i+2}\right] =$$

$$= \sum_{i=1}^{r} F(n_i) + \left[\frac{\sqrt{5}-1}{2} \cdot \left(1 + \sum_{i=1}^{r} \left(\frac{1-\sqrt{5}}{2} \right)^{n_i} \right) \right].$$

A kifejezés utolsó tagja (13) miatt nulla, s ezzel az állítást igazoltuk.

IRODALOM

[1] J. L. Browin, Zeckendorf's theorem and some applications, Fibonacci Quart., 2 (1964), 163–168.

[2] V. Granville and J.P.Rasson, A strange recursive relation, J. Number Theory, 30(1988) 238–241.

[3] P. Kiss and B. Zay, On a generalization of a recurrence sequence, Fibonacci Quart., 30(1992), 103–109.

[4] Rényi A., Napló az információelméletről. Gondolat Kiadó, Budapest, 1976. 136–163.

ZAY BÉLA

A FIBONACCI SZÓSOROZATOK EGY ÁLTALÁNOSÍTÁSA*

Abstract: (A generalization of the Fibonacci word-sequences). In [3] J. C. Turner introduced the Fibonacci word-sequences and used for the investigation of binary sequences. Such a sequence is, e.g. The word-sequence F(0,10)= 0; 10; 010; 10010; 01010010; ... where the n^{th} word $(m>2)$ is constructed by writing the $(n-1)^{th}$ word after the $(n-2)^{th}$ one and the initial words are 0 and 10. In this squence the position of the n^{th} one determine the n^{th} Wythoff pair which was investigated by J. G. Turner [4]. Also a Fibonacci word-sequence is the so colled "papal sequence" which was investigated by P. M. Higgins [1] who has given several algoritms for the construction of this sequence. In this paper we investigate the generalization of these word-sequences.

* A dolgozat az OTKA 1641 sz. pályázat támogatásával készült.

J. C. Turner [3]-ban bináris sorozatokkal és úgynevezett Fibonacci szósorozatokkal foglalkozott. Fibonacci szósorozatnak nevezte és $F(w_1,w_2)$-vel jelölte azt a szósorozatot, melynek első két eleme w_1,w_2, az $n(n>2)$-edik elemét pedig az $n-2$-edik és $n-1$-edik elemének egymás mellé írásával képezzük. Ilyen sorozat a P. M. Higgins [1] által vizsgált

F(J,P= J) P JP PJP JPPJP ...

"pápa sorozat" is, vagy a [3]-ban is megemlített

F(0,10)= 0 10 010 10010 01010010 ..

sorozat, melyben a 0-ák sorszáma rendre

1, 3, 4, 6, 8, 9, 11, 12, 14, 16, 17, 19, ...,

s ez azonos az $\{a_n\}=\{[n\alpha]\}_{n=1}^{\infty}$ sorozattal $\left(\alpha=\frac{1}{2}\left(1+\sqrt{5}\right)\right)$, az 1-ek sorszáma pedig rendre

2, 5, 7, 10, 13, 15, 18, 20, ...,

ami azonos a $\{b_n\}=\{[n\alpha^2]\}_{n=1}^{\infty}$ sorozattal. Az (a_n,b_n) rendezett elempár (lásd például [21]-ben) éppen az n-edik Wythoff párral azonos, aminek további előállításairól olvashatunk [4]-ben.

A következőkben a Fibonacci szósorozatok egy általánosításával foglalkozunk.

Legyenek s és k rögzített pozitív egészek, $X=\{x_1,x_2,\ldots,x_s\}$ az $x_1,x_2,\ldots,x_s$ betűk halmaza! Jelöljük $W(X)$-el az X-beli betűkből, ezek egymás mellé írásával képezett, összes szó halmazát, és $\overline{w}=(w_1,w_2,\ldots,w_k)$-sal a $W(X)$ k-szoros Descartes szorzatának, $W^k(X)$-nek egy tetszőleges elemét!

Legyen $f_i(\overline{w})$ a $W^k(x)$-et $W(X)$-be képező leképezés és minden $\overline{w} \in W^k(X)$-re

(1) $f_i(\overline{w}) = f_i(w_1, w_2, \ldots, w_k) = w_{j_{1,i}}, w_{j_{2,i}}, \ldots, w_{j_{p_i,i}}$

ahol minden $i(1 \le i \le k)$-re p_i rögzített pozitív egész, és $1 \le j_{m,i} \le k$ minden $m(1 \le m \le p_i)$ és minden $i(1 \le i \le k)$ egész számra! Tehát $f_i(\overline{w}\ )$ valamely k dimenziós $\overline{w}$ vektor esetén a $j_{1,i}$-edik, $j_{2,i}$-edik ..., $j_{p_i,i}$-edik koordináták egymás mellé írásával előállított szó.

Legyenek továbbá minden $i(1 \le i \le k)$-re n pozitív egészre a $P_{n,i}(\overline{w})$ és $P_n(\overline{w})$ olyan $W^k(x)$-et $W(X)$-be képező leképezések, melyeket

(2) $$P_{n,i}(\overline{w}) = \begin{cases} w_1 & \text{ha } n = 1 \\ f_i(P_{n-1,1}(\overline{w}), (P_{n-1,2}(\overline{w}), \ldots, (P_{n-1,k}(\overline{w})), & \text{ha } n > 1 \end{cases}$$

és

(3) $$P_n(\overline{w}) = P_{n,1}(\overline{w}) P_{n,2}(\overline{w}) \ldots P_{n,k}(\overline{w})$$

definiálva, minden $\overline{w} \in W^k(X)$-re!

A következőket fogjuk bizonyítani:

1. Tétel: Minden t, n pozitív egészre és $i(1 \le i \le k)$-re

(4) $$P_{n-1+t,i}(\overline{w}) = P_{n,i}\left(P_{t,i}(\overline{w}), P_{t,2}(\overline{w}), \ldots, P_{t,k}(\overline{w})\right)$$

és

(5) $$P_{n-1+t}(\overline{w}) = P_n\left(P_{t,1}(\overline{w}), P_{t,2}(\overline{w}), \ldots, P_{t,k}(\overline{w})\right).$$

2. Tétel: Ha $h(\overline{w})$ a $W^k(x)$-nek a $W(X)$-be való olyan leképezése, amit minden $\overline{w} \in W^k(X)$-re a

(6) $$h(\overline{w}) = h(w_1, w_2, \ldots, w_k) = w_{i_1}, w_{i_2}, \ldots, i_r \le k)$$

képlet definiál, ahol $r,i_1,i_2,\ldots,i_r$ rögzített egész számok, és $H=\{H_n(\overline{w})\}_{n=1}^{\infty}$ olyan, a $W^k(x)$ halmazt $W(X)$-be képező leképzések sorozata, amelyet

$$(7)\qquad H_n(\overline{w})=\begin{cases}h(\overline{w}) & \text{ha } n=1\\ H_{n-1}\big(f_1(\overline{w}),f_2(\overline{w}),\ldots,f_k(\overline{w})\big), & \text{ha } n>1\end{cases}$$

definiál, akkor minden n pozitív egészre

$$H_n(\overline{w})=h\big(P_{n,1}(\overline{w}),P_{n,2}(\overline{w}),\ldots,P_{n,k}(\overline{w})\big)=$$

$$=P_{n,i_1}(\overline{w}\ ),P_{n,i_2}(\overline{w}\ ),\ldots,P_{n,i_r}(\overline{w}\ )P_{n,i_1}(\overline{w}),P_{n,i_2}(\overline{w}),\ldots,P_{n,i_r}(\overline{w}).$$

Megjegyezzük, hogy a H definíciója szerint a $\overline{w}=(w_1,w_2,\ldots w_k)$ vektor $H_n(\overline{w})$ képe az a szó, amely a $H_{n-1}(\overline{w})$ szóból úgy állítható elő, hogy w_1 helyett mindenhová $f_1(\overline{w})$-t, w_2 helyett $f_2(\overline{w})$, ..., w_k helyett pedig mindenhová $f_k(\overline{w})$-t írunk.

A H sorozat a $\{P_{n,i}(\overline{w})\}_{n=1}^{\infty}$ és $\{P_n(\overline{w})\}_{n=1}^{\infty}$ sorozatok közös általánosítása, hiszen (2)-ből és (7)-ből következően, ha $h(\overline{w})=w_i$ minden $\overline{w}\in W^k(X)$-re, akkor $H=\{P_{n,i}(\overline{w})\}_{n=1}^{\infty}$, ha pedig $h(\overline{w})=w_1,w_2,\ldots,w_k$, minden $\overline{w}\in W^k(X)$-re, akkor (3)-ból és (7)-ből adódik, hogy $H=\{P_{n,i}(\overline{w})\}_{n=1}^{\infty}$.

Bizonyos speciális esetekben vizsgálni fogjuk a rögzített $w_1=v_1$, $w_2=v_2,\ldots,w_k=v_k$, szavak (azaz $\overline{w}=\overline{v}=(v_1,v_2,\ldots,v_k)$) és (7) által meghatározott H szósorozatban a különböző betűk és szavak eloszlását, ezért bevezetjük a következő jelöléseket: Ha v^I a $v_1,v_2,\ldots,v_k$ szavakból konkatenációval (egymás mellé írással) készített szó, akkor minden $i(1\le i\le k)$-re $L_i(v^I)$ jelentse azt, hogy v_i hányszor fordul elő

v^I-ben, $D_m(v^I)$ pedig azt, hogy x_m betű hányszor fordul elő v^I-ben $(1 \le m \le s)$! A v^I "szóhosszát" $\left(a \sum_{i=1}^{k} L_i(v^I)$ összeget$\right)$ jelölje $L(v^I)$, a v^I "betűhosszát" $\left(a \sum_{i=1}^{o} L_i(v^I)$ összeget$\right)$ pedig $D(v^I)$!

A bevezetett fogalmakra a következő érvényes:

3. Tétel: Az $L_j(H) = \{L_j(H_n(\overline{v}))\}_{n=1}^{\infty}$, $D_m(H) = \{D_m(H_n(\overline{v}))\}_{n=1}^{\infty}, L(H) = \{L(H_n(\overline{v}))\}_{n=1}^{\infty}$ és közös $F_k(x)$ karakterisztikus polinommal rendelkező lineáris rekurzív sorozatok, ahol

$$(8)\quad F_k(x) = \det(c_{i,j}),\ c_{i,j} = \begin{cases} -L_i(f_j(\overline{v})), & ha 1 \le 1 \ne j \le k \\ x - L_i(f_j(\overline{v})), & ha 1 \le 1 = j \le k \end{cases}$$

A továbbiakban az $f_i(\overline{w})$, $1 \le s \le k$, leképezéseket speciálisan a

$$(9)\quad f_i(\overline{w}) = \begin{cases} w_k, & ha \quad i = 1 \\ w_1 w_2 \ldots w_{i-1} w_k, & ha \quad 2 \le i \le k \end{cases}$$

képlettel definiáljuk.

Legyen $w_1, w_2, \ldots, w_n$ tetszőleges szósorozat és $B_1, B_2, \ldots, B_n, \ldots$, $B_1^I, B_2^I, \ldots, B_n^I$ ... olyan leképzések, melyekre

$$B_1(w_1) = w_1 \ , \ B_1^I = \emptyset \quad (\text{"üres" szó})$$

és $i \le 1$ esetén, ha

$$B_i(w_1, w_2, \ldots, w_i) = w_{j_1} w_{j_2} \ldots w_{j_{z^{i-1}-1}} w_1$$

és

$$B_i^I(w_2,w_3,\ldots,w_i) = w_{j_1}w_{j_2}\ldots w_{j_{2i-1-1}}$$

akkor legyen

(10) $B_{i+1}(w_1,w_2,\ldots,w_{i+1}) = B_i^I(w_2,w_3,\ldots,w_i)B_i(w_2,w_3,\ldots,w_{i+1})w_1!$

A definícióból az $i=2$ és $i=3$ esetben például

$$B_2(w_1,w_2) = B_1^I B_1(w_2)w_1 = w_2w_1$$

és

$$B_3(w_1,w_2,w_3) = B_1^I(w_2)B_2(w_2,w_3)w_1 = w_2w_3w_2w_1$$

adódik.

A $P_{n,1}$ és B_i leképzések között a következő összefüggések állnak fenn:

4. Tétel: Minden $i(1 \le i \le k)$-re, $n(n \ge i+1)$-re és tetszőleges $\overline{v} \in W^k(X)$-re, teljesül a

(11) $P_{n,1}(\overline{v}) = B_i\big(P_{n-1,k}(\overline{v}), P_{n-2,k}(\overline{v}),\ldots,P_{n-i,k}(\overline{v})\big)$

egyenlőség.

5. Tétel: A $P_{n,i}(\overline{v}) = B_i\big(P_{n-1,k}(\overline{v}), P_{n-2,k}(\overline{v}),\ldots,P_{n-i,k}(\overline{v})\big)$ szóban, tetszőleges $\overline{v} \in W^k(X)$ esetén, $j(1 \le j \le i)$-re a $P_{n-j,k}(\overline{v})$ szó pontosan $\binom{i-1}{j-1}$-szer fordul elő.

Megjegyezzük, hogy (2)-ből és (9)-ből következik, hogy minden n pozitív egészre

$$P_n(\overline{v}) = P_{n,1}(\overline{v})P_{n,2}(\overline{v})\ldots P_{n,k}(\overline{v}) = f_k\big(P_{n,1}(\overline{v}),\ldots,P_{n,k}(\overline{v})\big) = P_{n+1,k}(\overline{v}),$$

így a (11)-ből adódóan

$$P_n(\overline{v}) = B_k\big(P_{n-1}(\overline{v}), P_{n-2}(\overline{v}),\ldots,P_{n-k}(\overline{v})\big)$$

is teljesül minden $n \ge k+1$-re. Továbbá a $k=2$ speciális esetben a (11)-ből a $B_1(w_1) = w_1$ és egyenlőségek felhasználásával a

$$P_{n,2}(\overline{v}) = B_2\big(P_{n-1,2}(\overline{v}), P_{n-2,2}(\overline{v})\big) = P_{n-2,2}(\overline{v})P_{n-1,2}(\overline{v})$$
$$P_{n,1}(\overline{v}) = B_1\big(P_{n-1,2}(\overline{v})\big) = P_{n-1,2}(\overline{v})$$

összefüggések következnek, ami azt jelenti, hogy a $\{P_{n,2}(\overline{v})\}_{n=1}^{\infty}$, $\{P_{n,1}(\overline{v})\}_{n=1}^{\infty}$ és $\{P_n(\overline{v})\}_{n=1}^{\infty}$ sorozatok Fibonacci szósorozatok, és

$$\{P_{n,1}(v_1,v_2)\}_{n=1}^{\infty} = F\big(P_{1,1}(v_1,v_2), P_{2,1}(v_1,v_2)\big) = F(v_1,v_2)$$
$$\{P_{n,2}(v_1,v_2)\}_{n=1}^{\infty} = F\big(P_{1,2}(v_1,v_2), P_{2,2}(v_1,v_2)\big) = F(v_2,v_1v_2)$$
$$\{P_n(v_1,v_2)\}_{n=1}^{\infty} = \{P_{n+1,2}(v_1,v_2)\}_{n=1}^{\infty} = \tag{12}$$
$$= F\big(P_{2,2}(v_1,v_2)P_{3,2}(v_1,v_2)\big) = F(v_1v_2, v_2v_1v_2).$$

1. Tétel bizonyítása: $n = 1$-re (2)-ből következik (4).

Tegyük fel, hogy $n = m-1$-re, ahol $m > 1$, teljesül (4)! Ekkor a (2)-őt felhasználva

$$P_{m,i}\big(P_{t,1}(\overline{w}),\ldots,P_{t,k}(\overline{w})\big) =$$
$$= f_i\big(P_{m-1,1}\big(P_{t,1}(\overline{w}),\ldots,P_{t,k}(\overline{w})\big),\ldots,P_{m-1,k}\big(P_{t,1}(\overline{w}),\ldots,P_{t,k}(\overline{w})\big)\big) =$$
$$= f_i\big(P_{m-2+t,1}(\overline{w}),\ldots,P_{m-2+t,k}(\overline{w})\big) = P_{m-1+t,i}(\overline{w})$$

adódik minden $i(1 \le i \le k)$ és $t \ge 1$-re. Ezzel (4)-et igazoltuk, amiből (3) alapján (5) is következik.

A 2. Tétel bizonyítása: $n = 1$-re (2)-ből, (6)-ból és (7)-ből következik az állítás. Tegyük fel, hogy $n = m$ pozitív egészre és minden $\overline{w} \in W^k(X)$-re

$$H_m(\overline{w}) = P_{m,i_1}(\overline{w})\ldots P_{m,i_r}(\overline{w})$$

teljesül! Ezt az egyenlőséget és a (7)-et felhasználva

$$H_{m+1}(\overline{w}) = H_m\big(f_1(\overline{w}), f_2(\overline{w}),\ldots,f_k(\overline{w})\big) =$$

$$= P_{m,i_1}(f_1(\overline{w}),\ldots,f_k(\overline{w}))\ldots P_{m,i_r}(f_1(\overline{w}),\ldots,f_k(\overline{w}))$$

adódik, amiből előbb az

$$f_i(\overline{w}) = P_{2,j}(\overline{w}) \quad , \quad (1 \le i \le k)$$

egyenlőtlenségeket, majd $n=m$, $t=2$-re (4)-et alkalmazva

$$H_{m+1}(\overline{w}) = P_{m,i_1}\left(P_{2,1}(\overline{w}),\ldots,P_{2,k}(\overline{w})\right)\ldots P_{m,i_t}\left(P_{2,1}(\overline{w}),\ldots,P_{2,k}(\overline{w})\right) =$$
$$= P_{m+1,i_1}(\overline{w})P_{m+1,i_2}(\overline{w})\ldots P_{m+1,i_r}(\overline{w}) =$$
$$= h\left(P_{m+1,1}(\overline{w}),P_{m+1,2}(\overline{w}),\ldots,P_{m+1,k}(\overline{w}).\right)$$

Ezzel az állítást igazoltuk.

A 3. Tétel bizonyítása: A H, $L_j(H)$, $D_m(H)$, $L(H)$ és $D(H)$ sorozatok definícióiból közvetlenül adódik, hogy

(13)

$$L_j(H_n(\overline{v}\ )) = \begin{cases} L_j(h(\overline{v})), & \text{ha} \quad n=1, 1 \le j \le k \\ \sum_{i=1}^{k} L_j(f_i(\overline{v}))\cdot L_i(H_{n-1}(\overline{v}), & \text{ha} \quad n>1, 1 \le j \le k \end{cases}$$

(14) $$D_m(H_n(\overline{v})) = \sum_{j=1}^{k} D_m(\overline{v}_j)\cdot L_j(H_n(\overline{v})), \text{ ha } n \ge 1, \ 1 \le m \le s$$

(15) $$L(H_n(\overline{v})) = \sum_{j=1}^{k} L_j(H_n(\overline{v})), \qquad \text{ha } n \ge 1,$$

(16) $$D(H_n(\overline{v})) = \sum_{m=1}^{k} D_m(H_n(\overline{v})), \qquad \text{ha } n \ge 1.$$

Ha alkalmazzuk az [5]-ben igazolt tételt a (13) lineáris rekurzív rendszerre, akkor azt kapjuk, hogy $L_j(H)$ rekurzív sorozat minden $j(1 \le j \le k)$-re, és karakterisztikus polinomja a (8)-ban definiált $F_k(x)$. Az $F_k(x)$ közös karakterisztikus polinommal rendelkező lineáris rekurzív sorozatok összege, illetve egész számszorosa is tekinthető $F_k(x)$ karakterisztikus polinommal rendelkező lineáris rekurzív sorozatnak, ezért

(14)-ből, (15)-ből és (16)-ból a $D_m(H)$, $L(H)$ és $D(H)$ sorozatokra is következik az állítás.

A 4. Tétel bizonyítása: A (2), (9) és B_1 definíciója alapján minden $n \geq 2$-re

$$P_{n,1}(\overline{v}) = f_1\left(P_{n-1,1}(\overline{v}), P_{n-1,2}(\overline{v}), \ldots, P_{n-1,k}(\overline{v})\right) =$$
$$= P_{n-1,k}(\overline{v}) = B_1\left(P_{n-1,k}(\overline{v})\right),$$

tehát $i = 1$-re igazoltuk az állítást.

Ha valamely $i(1 \leq i \leq k)$-re és minden $n \geq i+2$ teljesül a (11), akkor

$$P_{n-1,i}(\overline{v}) = B_i\left(P_{n-2,k}(\overline{v}), P_{n-3,k}(\overline{v}), \ldots, P_{n-i-1,k}(\overline{v})\right)$$

és
$$B_i\left(P_{n-1,k}(\overline{v}), P_{n-2,k}(\overline{v}), \ldots, P_{n-i,k}(\overline{v})\right) = P_{n,i}(\overline{v}) =$$
$$= f_i\left(P_{n-1,1}(\overline{v}), P_{n-1,2}(\overline{v}), \ldots, P_{n-1,k}(\overline{v})\right) =$$
$$= P_{n-1,1}(\overline{v}) \ldots P_{n-1,i-1}(\overline{v}) P_{n-1,k}(\overline{v}) =$$
$$= B_i^I\left(P_{n-2,k}(\overline{v}), P_{n-3,k}(\overline{v}), \ldots, P_{n-i,k}(\overline{v})\right) P_{n-1,k}(\overline{v}),$$

így a (10)-et is felhasználva a (9) alapján

$$P_{n,i+1}(\overline{v}) = f_{i+1}\left(P_{n-1,1}(\overline{v}), P_{n-1,2}(\overline{v}), \ldots, P_{n-1,k}(\overline{v})\right) =$$
$$= P_{n-1,1}(\overline{v}) \ldots P_{n-1,i-1}(\overline{v}) P_{n-1,i}(\overline{v}) P_{n-1,k}(\overline{v}) =$$
$$= B_i^I\left(P_{n-2,k}(\overline{v}), \ldots, P_{n-i,k}(\overline{v})\right) B_i\left(P_{n-2,k}(\overline{v}), \ldots, P_{n-i-1,k}(\overline{v})\right) P_{n-1,k}(\overline{v}) =$$
$$= B_{i+1}\left(P_{n-1,k}(\overline{v}), P_{n-2,k}(\overline{v}), \ldots, P_{n-i-1,k}(\overline{v})\right),$$

és ezzel a tételt igazoltuk.

Az 5. Tétel bizonyítása: $i = 1$-re $B_1(w_1) = w_1$-ből, $i = 2$-re $B_1(w_1, w_2) = w_2 w_1$-ből adódik az állítás.

Tegyük fel a továbbiakban, hogy valamely $i(2 \leq i < k)$-re teljesül a tétel, s ezt felhasználva igazoljuk $i+1$-re is! A 4. Tételből adódó

$P_{n,i+1}(\bar{v}) =$

$= B_i'\left(P_{n-2,k}(\bar{v}),\ldots,P_{n-i,k}(\bar{v})\right)B_i\left(P_{n-2,k}(\bar{v}),\ldots,P_{n-i-1,k}(\bar{v})\right)P_{n-1,k}(\bar{v})$

egyenlőségből így az indukciós feltétel miatt, minden $j(1 < j < i+1)$-re következik, hogy a $P_{n,i+1}(\bar{v})$ előállításában a $P_{n-j,k}(\bar{v})$

$$\binom{i-1}{j-2} + \binom{i-1}{j-1} = \binom{(i+1)-1}{j-1}\text{-szer}$$

fordul elő. Teljes indukcióval könnyen belátható, hogy $P_{n,i+1}(\bar{v})$

előállításában a legnagyobb indexű $\left(P_{n-i-1,k}(\bar{v})\right)$ szó pontosan egyszer fordul elő, így az

$$\binom{(i+1)-1}{1-1} = 1 = \binom{(i+1)-1}{(i+1)-1}$$

egyenlőséget is felhasználva, minden $j(1 \le j \le i+1)$-re azt kaptuk, hogy a $\left(P_{n,i+1}(\bar{v})\right)$ előállításában a $\left(P_{n-j,k}(\bar{v})\right)$ pontosan $\binom{(i+1)-1}{1-1}$-szer fordul elő, s ezzel az állítást igazoltuk.

IRODALOM

[1] P. M. Higgins, The Naming of Popes and a Fibonacci Sequence in Two Noncommuting Indeterminates, The Fibonacci Quarterly 25.1 (1987), 57—61.

[2] V. E. Hoggatt and M. Bicknell-Hohnson, Additiv Partition of the Positive Integers and Generalized Fibonacci Representations, The Fibonacci Quarterly 22.1 (1984), 2—21.

[3] J. C. Turner, Fibonacci Word Patterns and Bianry Sequences, The Fibonacci Quarterly, 26.3 (1988), 233—246.
[4] J. C. Turner, The Alpha and the Omega of the Wythoff Pairs, The Fibonacci Quarterly, 27.1 (1989), 76—86.
[5] B. Zay, Solutions of Linear Recursive Systems, Publ. Math. Debrecen 40. (1992), 127—134.

PHAM VAN CHUNG

EGY KLASSZIKUS PROBLÉMA ÁLTALÁNOSÍTÁSA II.

Abstract: (A generalization of a classical problem II.). In the present paper we solve a generation of a classical problem. The problem was dawn first up in the "Annales de Math." ([8], p. 220.). Since that time this problem, i.e. the solution of the congruence $x^2 \equiv x \pmod{m^k}$, was investigated by several authors, the first solution of it was given by M. Tédenant [8] in 1814. Our purpose is to generalize this problem by solving the congruence $x^n \equiv ax^s \pmod{m^k}$, where n,a,s,m and k are given natural numbers. We give the number and the explicite form of the solutions; and show some properties of them in some special cases. For example, in the case $(n-1, \varphi(m)) = 1$ we solve the congruence $x^n \equiv x \pmod{m^k}$ and give some properties of this.

1814-ben az „Annales de Math." c. folyóirat azt a problémát vetette fel, hogy „Melyek azok a természetes számok, amelyeknek négyzete ugyanarra a k-jegyű számra végződik, mint

az eredeti szám?". Ezt M. Tédenant [8] oldotta meg és igazolta, hogy két nem triviális megoldásának összege $10^k + 1$. Azóta többen foglalkoztak ilyen, illetve hasonló problémával (lásd L. E. Dickson [4]). Ez a probléma az

$$x^2 \equiv x \pmod{m^k}$$

kongruencia pozitív megoldásának keresését jelenti. [10]-ben foglalkoztunk egy általánosabb problémával, nevezetesen megoldottuk az $x^2 \equiv ax \pmod{m^k}$ kongruenciát; megadtuk a megoldások számát és a megoldások explicit alakját, valamint egy eljárást a kongruencia numerikus megoldására.

A probléma még a következőképpen általánosítható: „Melyek azok a természetes számok az m-alapú számrendszerben, amelyeknek az n-edik hatványa ugyanarra a k-jegyű számra végződik, mint az eredeti szám s-edik hatványának a-szorosa?", azaz keressük az

$$x^n \equiv ax^s \pmod{10^k}$$

kongruencia pozitív egész megoldásait.

A kongruencia speciális eseteivel sokan foglalkoztak, különösen az $m = 10$ esettel. Egy általános eredményt C. P. Popovici [7] adott meg, mégpedig az $x^n \equiv x \pmod{m^k}$ kongruencia megoldásainak explicit alakjával. Általános m esetén az $x^n \equiv x \pmod{m^k}$ kongruenciával P. Kiss [5] foglalkozott. Megadta a kongruencia megoldásainak számát és a megoldások explicit alakját.

Többen foglalkoztak a kongruenciánk $x^n \equiv x \pmod{n}$ speciális esetével a pszeudoprimszámokkal kapcsolatban. (Például R. D. Carmichael [2], A. Korselt [6], M. R. Chapson [3] és P. Bachmann [1].)

Ebben a II. cikkben explicit alakban megadjuk a

$$x^n \equiv ax^s \pmod{m^k}$$

kongruencia nem túl nagy abszolút értékű megoldásait, valamint a megoldások számát. Megmutatjuk, hogy az $s = 1$ esetben elegendő az $n \leq \varphi(m^k)$ esetet, továbbá az $a = 1$ és $(n-1, \varphi(m)) = 1$ együttes fennállása esetén az $n = 2$ esetet megoldani. Ezután vizsgáljuk a megoldásokat általában.

Mielőtt rátérünk az

(1) $$x^n \equiv ax^s \pmod{m}$$

kongruencia megoldására, néhány speciális esettel foglalkozunk.

1. Tétel: Ha $(a,m) = 1$ és $n = k\varphi(m) + r$ (φ az Euler-függvény) és $0 < r \leq \varphi(m)$, akkor a következő két kongruencia ekvivalens

(2) $$x^n \equiv ax \pmod{m}$$

(3) $$x^r \equiv ax \pmod{m}.$$

Bizonyítás: Megmutatjuk, hogy az első kongruencia megoldásai kielégítik a másodikat és viszont.

Legyen x_0 egy megoldása a (2) kongruenciának, továbbá $(x_0, m) = d$. Ezek alapján léteznek x_1 és m_1 egészek, melyekre $x_0 = dx_1$, $m = dm_1$ és $(x_1, m_1) = 1$. Ezeket (2)-be helyettesítve és d-vel osztva

$$x_1^n d^{n-1} \equiv ax_1 \pmod{m_1}.$$

De $(x_1, m_1) = 1$ miatt mindkét oldalát x_1-gyel osztva kapjuk, hogy

$$(x_1 d)^{n-1} \equiv a \pmod{m_1}.$$

Ez csak úgy állhat fenn, ha $(x_1 d, m_1) = 1$, mivel $(a,m) = 1$.

Mivel $(d,m_1)=1$ folytán $\varphi(m)=\varphi(d)\cdot\varphi(m_1)$, így a bal oldal tovább alakítható, felhasználva az Euler-Fermat tételt:

$$(x_1d)^{n-1}=(x_1d)^{k\varphi(d)\cdot\varphi(m_1)}(x_1d)^{r-1}\equiv(x_1d)^{r-1}(\text{mod } m_1).$$

Tehát a fenti kongruencia a következőre redukálódik:

$$(x_1d)^{r-1}\equiv a \pmod{m_1}.$$

Itt d-vel szorozva mindkét oldalt és a modulust is, majd x_1-gyel szorozva a két oldalt és , ill. m_1d helyébe visszaírva x_0-t, ill. m-et, az

$$x_0^r\equiv ax_0 \pmod{m}$$

kongruenciát kapjuk, mivel igazoltuk a tételt az egyik irányban.

Ha x_0 megoldása a (3) kongruenciának, akkor az előzőekhez hasonlóan látható be, hogy megoldása a (2)-nek is.

Ezután bebizonyítjuk a következő tételt, amely bizonyos esetekben egyszerűsítheti a számításokat.

2. Tétel: Ha $(n-1,\varphi(m))=1$, akkor az

(4) $$x^n\equiv x \pmod{m}$$

és az

(5) $$x^2\equiv x \pmod{m}$$

kongruencia ekvivalens.

Bizonyítás: Tegyük fel, hogy x_0 megoldása a (4) kongruenciának. Mivel $(n-1,\varphi(m))=1$, léteznek olyan v és u természetes számok, amelyekre

(6) $$v\cdot(n-1)=u\cdot\varphi(m)+1.$$

Mint az előző tétel bizonyításában, ha $(x_0,m)=d$ és a felhasznált jelöléseket tartva (4) átalakítható

(7) $$(x_1d)^{n-1}\equiv 1 \pmod{m_1}$$

alakra, ahol $(x_1 d)^{v(n-1)} \equiv 1 \pmod{m_1}$

(6)-ot a (7)-be helyettesítve

$$1 \equiv (x_1 d)^{v(n-1)} \equiv (x_1 d)^{u\cdot\varphi(m)+1} \equiv \left[(x_1 d)^{\varphi(m)}\right]^u \cdot x_1 d \equiv x_1 d \pmod{m},$$

mert $(x_1 d, m_1) = 1$ miatt $\varphi(m) = \varphi(m_1 d) = \varphi(d)\cdot\varphi(m_1)$, amiből $(x_1 d)^{\varphi(m)} \equiv 1 \pmod{m_1}$. Tehát $x_1 d \equiv 1 \pmod{m_1}$. Ezt d-vel végigszorozva, azután mind a két oldalt x_1-gyel szorozva és $x_1 d$ helyére x_0-t visszaírva $x_0^2 \equiv x_0 \pmod{m}$ adódik, amivel a tétel első részét bebizonyítottuk.

Viszont, ha x_0 megoldása az (5)-nek, akkor ez kielégíti a (4)-et is. Ugyanis $x_0^2 \equiv x_0 \pmod{m}$ miatt $n \geq 2$ esetén

$$x_0^n \equiv x_0^{n-2} \cdot x_0^2 \equiv x_0^{n-2} x_0 = x_0^{n-1} \equiv \cdots \equiv x_0 \pmod{m}.$$

Megjegyzés:

1. Tetszőleges a-ra az $(n-1, \varphi(m)) = 1$ feltétel teljesülése esetén nem mindig ekvivalensek az $x^n \equiv ax \pmod{m}$ és $x^2 \equiv ax \pmod{m}$ kongruenciák. Például $a = 3$, $n = 4$ és $m = 10$ esetén $x^4 \equiv 3x \pmod{10}$ és $x^2 \equiv 3x \pmod{10}$ nem ekvivalensek. Hiszen $x \equiv 8 \pmod{10}$ megoldása a második kongruenciának, de nem elégíti ki az $x^4 \equiv 3x \pmod{10}$ kongruenciát.

2. Ebből a tételből következik, hogy az $(n-1, \varphi(m)) = 1$ esetén minden $x^2 \equiv x \pmod{m}$ kongruenciára vonatkozó tétel érvényesül az $x^n \equiv x \pmod{m}$ kongruenciára is. Ezért igaz például a következő:

3. Tétel: Ha $(n-1, \varphi(m)) = 1$ és $m = P_1^{k_1} \cdots P_s^{k_s}$, akkor az

$$x^n \equiv x \pmod{m}$$

kongruenciának

(i) összes megoldása $u^{\varphi(v)} \pmod{m}$ alakú, ahol $uv = m$ és $(u,v) = 1$;

(ii) 2^s inkongruens megoldása van;

(iii) az inkongruens megoldások összege 2^{s-1}-gyel kongruens mod m.

Bizonyítás: A 2. Tétel miatt elegendő csak az $x^2 \equiv x \pmod{m}$ kongruenciát megoldani. A továbbiakban u és v mindig olyan számokat jelentsen, amelyekre $u \cdot v = m$ és $(u,v) = 1$.

(i) Könnyű belátni, hogy $x \equiv u^{\varphi(v)} \pmod{uv}$ megoldása az $x^2 \equiv x \pmod{m}$ kongruenciának. Még azt kell igazolni, hogy minden megoldás $u^{\varphi(v)}$ alakban írható (mod m). Valóban ha x_0 kielégíti az $x^2 \equiv x \pmod{m}$ kongruenciát, akkor $u = (x_0, m)$ jelöléssel vannak y_0 és v egészek, amelyekre

$$x = uy_0 \quad \text{és} \quad m = u \cdot v, \quad \text{ahol } (y_0, v) = 1.$$

Ezeket az $x^2 \equiv x \pmod{m}$ kongruenciába behelyettesítve az

$$(uy_0)^2 \equiv uy_0 \pmod{u \cdot v}$$

kongruenciához jutunk, amiből $(y_0, v) = 1$ miatt

$$uy_0 \equiv 1 \pmod{v}.$$

Innen $(u,v) = 1$, továbbá $y_0 \equiv u^{\varphi(v)-1} \pmod{v}$. Tehát

$$x_0 \equiv u^{\varphi(v)} \pmod{uv}$$

alakú, amit kívántunk.

(ii) A bizonyítás a [10]-ben lévő 4. Tételhez hasonló,

(iii) A tétel (i) állítása alapján $m = uv$, $(u,v) = 1$ felírással, ha $x_1 \equiv u^{\varphi(v)} \pmod{m}$ egy megoldás, akkor $x_2 \equiv v^{\varphi(u)} \pmod{m}$ egy másik megoldás. Mivel $(u,v) = 1$, így

$$u^{\varphi(v)} + v^{\varphi(u)} \equiv 1 \pmod{u \cdot v}.$$

(ii) miatt 2^{s-1} ilyen megoldáspár van, ezért a megoldásokra

$$\sum x_1 \equiv \sum_{1}^{2^{s-1}} 1 = 2^{s-1} \pmod{m}.$$

Most rátérünk az általános esetre.

Oldjuk meg a

(8) $$x^n \equiv a \cdot x^s \pmod{m};\ (a,m) = 1$$

kongruenciát. Megmutatjuk, hogy elég csak az $n > s$ esetre szorítkozni. Ha ugyanis $(a,m) = 1$, akkor (8) mindkét oldalát $a^{\varphi(m)-1}$-gyel beszorozva

$$a^{\varphi(m)-1} \cdot x^n \equiv a^{\varphi(m)} \cdot x^s \pmod{m}$$

Innen $(a,m) = 1$ miatt $a^{\varphi(m)} \equiv 1 \pmod{m}$. Ezért (8) alakja

$$x^s \equiv a' \cdot x^n \pmod{m}, \text{ ahol } a' = a^{\varphi(m)-1}$$

lesz, amelyet kívántunk. A megmaradt $n = s$ esetén a megoldás triviális.

Tehát a továbbiakban legyen $n > s$ és $m = P_0^{k_0} \cdot P_1^{k_1} \cdots P_r^{k_r}$ $(P_0 = 2)$. A (8) kongruencia ekvivalens a

$$x^n \equiv ax^s \pmod{2^{k_0}}$$

$$x^n \equiv ax^s \pmod{P_i^{k_i}} \qquad i = 1,2,\ldots,r$$

kongruencia-rendszerrel.

Az

(9) $$x^n \equiv ax^s \pmod{P_i^{k_i}} \qquad i = 1,2,\ldots,r$$

kongruenciából

(10) $$x^s(x^{n-s} - a) \equiv 0 \pmod{P_i^{k_i}}.$$

De $(x^s, x^{n-s} - a) = (x^s, a)$ és $(m,a) = 1$ miatt x^s és $x^{n-s} - a$ közül pontosan csak az egyik osztható P_i-vel. Ezek alapján (10)-ből

(11) $$x^s \equiv 0 \pmod{P_i^{k_i}}$$

vagy

(12) $$x^{n-s} \equiv a \pmod{P_i^{k_i}}.$$

a) Tekintsük a (11) kongruenciát! Nyilván, hogy ennek megoldása

$$x \equiv P_i^{k_i} \cdot t \pmod{P_i^{k_i}}, \text{ ahol } v_i = \left[\frac{k_i + s - 1}{s}\right]$$

és $t = 1, 2, \ldots p^{k_i - v_i}$, $i = 0, 1, \cdots, r$.

b) Ezuán (12) következőképpen oldható meg. Ha $k_0 \leq 2$, ill. $P_i > 2$, akkor az $x^{n-s} \equiv a \pmod{p_k^{k_i}}$ kongruencia primitív gyökök segítségével visszavezethetők $(n-s)y_i \equiv b_i \pmod{\varphi(P_i^{k_i})}$ alakú kongruenciára, ahol y_i és b_i sorrendben indexei az x-nek és a-nak. Ezek alapján a megoldások száma

$$D_1 = \begin{cases} d = \left((n-s), \varphi(P_i^{k_i})\right), & \text{ha } d | b_i, \\ 0, & \text{különben.} \end{cases}$$

$k_0 \geq 3$ esetén legyen $c = 2$ és $c_0 = 2^{k_0 - 2}$. Ekkor az $x^{n-s} \equiv a \pmod{2^{k_0}}$ kongruenciához létezik b és b_0, hogy $a \equiv (-1)^b \cdot 5^{b_0} \pmod{2^{k_0}}$, továbbá létezik y és y_0, hogy

$$\begin{cases} (n-s)y \equiv b \pmod{c} \\ (n-s)y_0 \equiv b_0 \pmod{c_0} \end{cases}$$

$x \equiv (-1)^y \cdot 5^{y_0} \pmod{2^{k_0}}$ (lásd [9]). Ebben az esetben a megoldások száma

$$D_0 = \begin{cases} d \cdot d_0, & \text{ha } d = (n-s, c) | b \quad \text{és } d_0 = (n-s, c_0) | b_0, \\ 0, & \text{egyébként.} \end{cases}$$

ha $d = (n-s, c) | b$ egyébként.

és $d_0 = (n-s, c_0) | b_0$,

Az előző jelöléseket használva kapjuk a következő tételt:

4. Tétel: Az

$$x^n \equiv a \cdot x^s \pmod{2^{k_0} \cdot P_1^{k_1} \cdot \ldots \cdot P_r^{k_r}}, \quad (a,m) = 1$$

kongruencia inkongruens megoldásainak száma

$$M = \left(D_0 + P_0^{k_0 - \nu}\right)\left(D_1 + P_1^{k_1 - \nu_1}\right) \ldots \left(D_r + P_r^{k_r - \nu_r}\right).$$

Nézzük meg ezután a (8) kongruencia általános megoldását!

Először bizonyítás nélkül közlünk két segédtételt, amelyek Kiss Pétertől [5] származnak.

1. Segédtétel. Tetszőleges $m > 1$ és k természetes számok esetén

$$\varphi(m^k) \geq k.$$

2. Segédtétel. Legyen $M = q_0 \cdot q_1 \cdots q_r$, ahol $q_i > 1$ és $q_0, q_1, \cdots q_r$ páronként relatív prímek, továbbá $Q_i = \frac{M}{q_i}$. Ekkor

$$\sum_{j=1}^{r} Q_j^{\varphi(q_j^k)} \equiv 1 \pmod{M^k}.$$

Ezután az $x^n \equiv ax^s \pmod{m^k}$, $(a,m) = 1$ kongruencia így oldható meg: Legyen G_1 megoldása az $x^n \equiv ax^s \pmod{P_i^{k_1}}$ kongruenciának $(i = 0,1,\ldots,r)$, ahol $m^k = P_0^{t_0} \cdot P_1^{t_1} \cdots P_r^{t_r}$. A $h = (t_0, t_1, \ldots, t_r)$ (azaz $t_0, t_1, \ldots, t_r$ legnagyobb közös osztója) jelöléssel $t_i = h \cdot t_i'$, továbbá $M = 2^{t_0'} \cdot P_1^{t_1'} \cdots P_r^{t_r'}$, így $M^h = m^k$. Vezessük be a $T_j = \frac{M}{P_j^{t_j'}}$, $j = 0,1,\ldots,r$ jelölést. A fentiek alapján

$$T_i^{\varphi\left(P_i^{t_i}\right)} \cdot x \equiv G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \left(\bmod P_i^{t_i} \cdot T_i^{\varphi\left(P_i^{t_i}\right)}\right).$$

De az 1. Segédtétel miatt

$$\varphi\left(P_i^{t_i}\right) = \varphi\left[\left(P_i^{t_i}\right)^h\right] \geq h, \text{ amiből } T_i^h \mid T_i^{\varphi\left(P_i^{t_i}\right)}.$$

Így $M^h \mid P_i^{t_i} \cdot T_i^{\varphi\left(P_i^{t_i}\right)}$. Tehát

$$T_i^{\varphi\left(P_i^{t_i}\right)} \cdot x \equiv G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \pmod{M^h}.$$

Ezeket 0-tól r-ig összegezve kapjuk

$$\left(\sum_{i=1}^{r} T_i^{\varphi\left(P_i^{t_i}\right)}\right) \cdot x \equiv \sum_{i=0}^{r} G_i \cdot T_i^{\varphi\left(P_i^{t_i}\right)} \pmod{M^h}.$$

De a 2. segédtétel miatt x együtthatója 1-gyel kongruens $(\mathrm{mod}\ M^h)$. Ezzel bizonyítottuk a következő tételt:

5. Tétel. Az

$$x^n \equiv a \cdot x^s \pmod{m^k}$$

kongruenciának összes megoldása

$$x \equiv \sum_{i=0}^{r} G_i \cdot Q_i^{\varphi\left(P_i^{t_i}\right)} \pmod{m^k},$$

ahol $m^k = P_0^{t_0} \cdot P_1^{t_1} \cdots P_r^{t_r}$, G_i megoldása az $x^n \equiv a \cdot x^s \pmod{P_i^{t_i}}$, $i = 0,1,\ldots,r$ kongruenciának és $Q_i = \dfrac{M}{P_i^{t_i}}$, $M = \prod_{i=0}^{r} P_i^{t_i}$ a $t_i' = t_i / (t_0, t_1, \ldots, t_r)$ jelölés mellett.

IRODALOM

[1] P. Bachmann: Über Fermat „kleinen" Satz. Archiv. Math. und physik, 21 (1913) 185–187.

[2] R. D. Carmichael: Note on a new number theory function; Bull. of Amer. Math. Soc., 16 (1910) 232–238.

[3] M. R. Chapron: Sur one proposition erronée Korselt relative aux nombres composes m qui divisent a^n-a, Bull. Sci. Mat., 80 (1956) 81–83.

[4] L. E. Dickson: History of the theory of thenumbers I., Chelsea Publ. Co., New York, (1971) 453–456.

[5] P. Kiss. Egy binom kongruenciáról, Acta Acad. Paed. Agr.-Nova Eger, XIV (1978) 453–464.

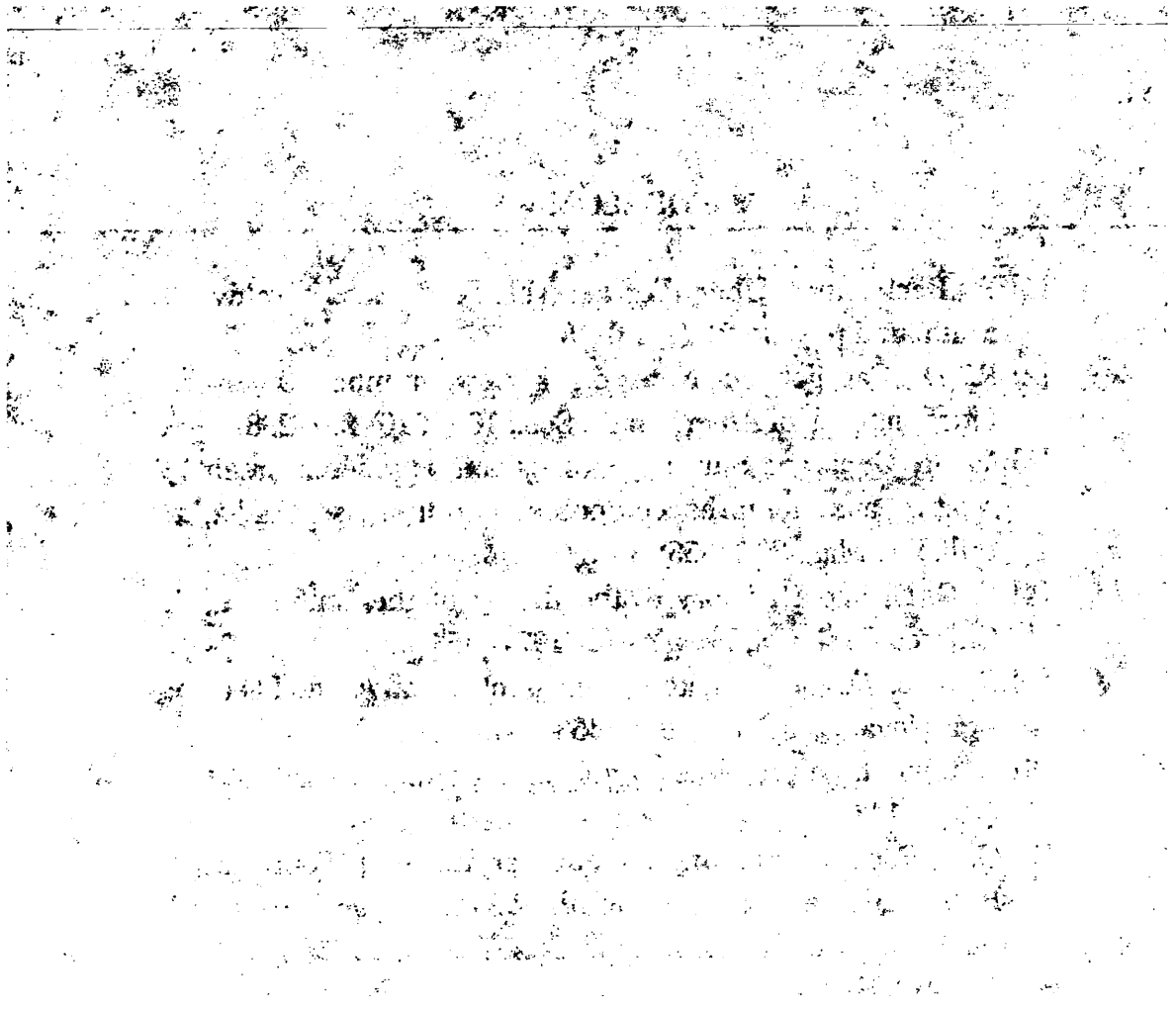
[6] A. Korselt: Le probéme chinois ..., Interm. des Math., VI (1899) 143.

[7] C. P. Popovici: Sur une équation arith. de D. Pompeiu; Bull. Math. de La Soc. Sci. Math. R.S.R., 9 (1967) 92–97.

[8] M. Tédenant: Probléme d'arith., Anales de Math., 5 (1814) 809–821.

[9] I. M. Vinogrodov: A számelmélet alapjai. Tankönyvkiadó, Budapest (1968)

[10] P. V. Chung: Egy klasszikus probléma általánosítása. Acta Acad. Pead. Agr.-Nova, Eger, XX (1991) 3–13.



JAMES P. JONES and PÉTER KISS

PROPERTIES OF THE LEAST COMMON MULTIPLE FUNCTION*

ABSTRACT: In this paper we show some properties of the function $L(x)$, the least common multiple of the natural numbers not greater than an integer x, and the function $Q(x) = x!/L(x)$.

The subject of this paper is to show the number-theoretic properties of the function $L(x) = LCM[1,2,\ldots,x]$, the least common multiple of the numbers $\leq x$. This function has a connection with the function $\Pi(x)$, the number of primes $\leq x$ and it is related to the two Chebyshev functions $\psi(x) = \ln(L(x))$ and $\theta(x)$ for which

$$\theta(x) = \sum_{p \leq x} \ln(p) \text{ and } \psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \ldots$$

* Research was supported by the Hungarian National Foundation (Grant No. 1641) for Scientific Research and the National Scienfitic and Engineering Reseurch Council of Canada.

I. The properties of the function L(x)

For any positive integer x, $L(x)$ can be written in the form

(1) $$L(x) = \prod_{p \leq x} p^{k_p}$$

Where k_p is defined for primes p by

$$p^{k_p} \leq x < p^{k_p+1}$$

and so for any prime $p \leq x$ we have

(2) $$k_p = \left[\frac{\ln(x)}{\ln(p)}\right].$$

where [ ] is the integer part function. From (1) and (2)

(3) $$\ln(L(x)) = \sum_{p \leq x} \left[\frac{\ln(x)}{\ln(p)}\right] \cdot \ln(p)$$

follows, which was shown also in [6].

In the followings we prove some other properties of $L(x)$.

LEMMA 1.1.

$$\lim_{x \to \infty} \frac{\ln(L(x))}{\theta(x)} = 1.$$

PROOF. By (3), using that $k_p = 1$ for p's with $\sqrt{x} < p \leq x$, we get

$$\ln(L(x)) = \sum_{p \leq \sqrt{x}} k_p \cdot \ln(p) + \sum_{\sqrt{x} < p \leq x} \ln(p) =$$

$$= \sum_{p \leq \sqrt{x}} \ln\left(p^{k_p - 1}\right) + \theta(x).$$

But

$$\sum_{p \leq \sqrt{x}} \ln\left(p^{k_p - 1}\right) < \sum_{p \leq \sqrt{x}} \ln(x) = \ln(x) \cdot \Pi\left(\sqrt{x}\right)$$

and

$$\frac{\ln(x).\Pi\left(\sqrt{x}\right)}{\theta(x)} \to 0 \quad \text{as} \quad x \to \infty$$

from which the lemma follows.

LEMMA 1.2. $0 \le \Pi(x)\ln(x) - \ln\left(L(x)\right) \le \theta(x)$

PROOF. From the inequality $r - 1 < [r] \leqq r$, using (3), we obtain

$$\Pi(x)\ln(x) - \theta(x) \leqq \ln\left(L(x)\right) \leqq \Pi(x)\ln(x)$$

and so the lemma is proved.

LEMMA 1.3. $\theta(x) \leqq \ln\left(L(x)\right) \leqq \Pi(x)\ln(x)$.

PROOF. $p \le x$ implies $1 \le \ln(x)/\ln(p)$. Hence from (3) we obtain

$$\theta(x) = \sum_{p \le x} \ln(p) \leqq \sum_{p \le x} \left[\frac{\ln(x)}{\ln(p)}\right] \ln(p) = \ln\left(L(x)\right).$$

The other inequality is part of Lemma 1.2.

We will need also the following result

LEMMA 1.4. $$\lim_{x \to \infty} \frac{\theta(x)}{\ln(x)\Pi(x)} = 1.$$

PROOF. We can deduce this from $\theta(x) \approx x$ plus the Prime Number Theorem (cf. e. g. in [2]). Or one can prove it from inequalities

(5) $$x\left(1 - \frac{1}{\ln(x)}\right) < \theta(x), \qquad \Pi(x) < \frac{x}{\ln(x)}\left(1 + \frac{3}{2\ln(x)}\right)$$

for $41 \le x$, which can be found in [5], since by Lemma 1.3 we have

$$1-\frac{1}{\sqrt{\ln(x)}}<\frac{\left(1-\frac{1}{\ln(x)}\right)}{\left(1+\frac{3}{2\ln(x)}\right)}=\frac{x\cdot\left(1-\frac{1}{\ln(x)}\right)}{x\cdot\left(1+\frac{3}{2\ln(x)}\right)}<\frac{\theta(x)}{\ln(x)\cdot\Pi(x)}\leqq 1.$$

The function $\Pi(x)$ can be approximated through the function $L(x)$. We will show that $\Pi(x)$ is asymptotic to $\ln(L(x))/\ln(x)$

COROLLARY 1.5.

$$\lim_{x\to\infty}\frac{\ln(L(x))}{\ln(x)\cdot\Pi(x)}=1.$$

PROOF. From Lemmas 1.3 and 1.4, we have for $x\geq 41$,

$$1-\frac{1}{\sqrt{\ln(x)}}<\frac{\theta(x)}{\ln(x)\Pi(x)}\leq\frac{\ln(L(x))}{\ln(x)\cdot\Pi(x)}\leq 1.$$

Now we can show that $\psi(x)=\ln(L(x))$ is asymptotic to x.

COROLLARY 1.6.

$$\lim_{x\to\infty}\frac{\ln(L(x))}{x}=1.$$

PROOF. Using Lemma 1.3 and the inequalities (5) we get

$$1-\frac{1}{\ln(x)}<\frac{\theta(x)}{x}\leq\frac{\ln(L(x))}{x}\leq\frac{\Pi(x)\ln(x)}{x}<1+\frac{3}{2\ln(x)}.$$

This actually shows that $\ln(L(x))=x+o\left(\frac{x}{\ln(x)}\right)$ which implies the following two corollaries.

COROLLARY 1.7. For all $\varepsilon>0$ and all sufficiently large x,

$$(e-\varepsilon)^x < L(x) < (e+\varepsilon)^x.$$

COROLLARY 1.8. (see also in [6])

$$\lim_{x\to\infty} L(x)^{\frac{1}{x}} = e.$$

LEMMA 1.9. $$\lim_{x\to\infty} \frac{\ln(x!)}{x\ln(x)} = 1.$$

PROOF. We use the following inequality, a form of Stirling's Theorem:

$$x\cdot\ln(x) - x + \frac{1}{2}\ln(x) + \frac{\ln(2\pi)}{2} < \ln(x!) \le x\cdot\ln(x) - x + \frac{1}{2}\ln(x) + 1.$$

Hence $1 - \frac{1}{\ln(x)} < \frac{\ln(x!)}{x\ln(x)} < 1$, and so $\frac{\ln(x!)}{x\ln(x)} = 1 + o\left(\frac{1}{\ln(x)}\right)$.

THEOREM 1. $$\lim_{x\to\infty} \frac{\ln(x!)}{\ln(L(x))\ln(x)} = 1.$$

PROOF. From Corollary 1.6. Lemma 1.9. we have

$$\lim_{x\to\infty} \frac{\ln(x!)}{\ln(L(x))\ln(x)} = \lim_{x\to\infty} \frac{\frac{\ln(x!)}{x\ln(x)}}{\frac{\ln(L(x))}{x}} = \frac{\lim_{x\to\infty} \frac{\ln(x!)}{x\ln(x)}}{\lim_{x\to\infty} \frac{\ln(L(x))}{x}} = \frac{1}{1} = 1.$$

Using Stirling's Formula again and Corollary 1.6 we may obtain π as a limit. Some other similar result for π was obtained in [3] and [4].

THEOREM 2.

$$\lim_{x\to\infty} \frac{x!^2\, e^{2x}}{2\ln(L(x))\cdot x^{2x}} = \pi \tag{6}$$

PFOOF. After we multiply the left side of (6) by 2 and take the log we obtain

$$2\ln x! + 2x - 2x\ln x - \ln\ln L(x) =$$
$$= 2\ln x! + 2x - 2x\ln(x) - \ln(x) - (\ln\ln L(x) - \ln x).$$

The term $\ln(\ln(L(x))) - \ln(x) \to 0$, as $x \to \infty$, by Corollary 1.6. One of the formulations of Stirling's Formula (cf. e. g. Artin [1]) says that there exists a δ, such that

$$\ln(x!) + x - x\cdot\ln(x) - \frac{1}{2}\cdot\ln(x) = \frac{1}{2}\cdot\ln(2\pi) + \frac{\delta}{12x} \qquad (0 < \delta < 1).$$

Multiply this by 2 and take the limit as $x \to \infty$, the theorem follows.

II. Quotient after $x!$ is divided by $L(x)$.

We derive some induction results about the quotient $x!/L(x)$, which is here denoted by $Q(x)$.

LEMMA 2.1. $L(x+1) = \dfrac{L(x)\cdot(x+1)}{(L(x), x+1)}$.

PROOF. Since $L(x+1) = [L(x), x+1]$.

LEMMA 2.2. $L(x+1)$ divides $L(x)\cdot(x+1)$.

PROOF. By Lemma 2.1.

LEMMA 2.3. $L(x)$ divides $x!$.

PROOF. Induction on x, using Lemm 2.2. from $L(x+1)|L(x)(x+1)$ and $L(x)|x!$, $L(x+1)|x!(x+1)$. follows.

DEFINITION 2.4. $Q(x)=\dfrac{x!}{L(x)}$.

LEMMA 2.5. $Q(x)$ is an integer and $Q(x)\,|\,x!$.

PFOOF. By Lemma 2.3.

LEMMA 2.6. $Q(x+1)=\big(Q(x)\cdot(x+1),x!\big)$.

FROOF. From Lemma 2.1. using $Q(x+1)=Q(x).\big(L(x),x+1\big)$.

LEMMA 2.7. p is a prime if and only if $L(p)=p\cdot L(p-1)$.

LEMMA 2.8. p is a prime if and only if $Q(p)=Q(p-1)$.

DEFINITION 2.9. $K(x)=\dfrac{Q(x)}{Q(x-1)}$.

LEMMA 2.10. $K(x)$ is an integer, $K(x)=(L(x-1),x)$ and $K(x)\,|\,x$.

FROOF. Use Lemma 2.6.

LEMMA 2.11. p is prime iff $K(p)=1$.

LEMMA 1.12. p is composite iff $1<K(p)$.

REFERENCES

[1] E. Artin, *Einfuhrung in die Theori der Gammafunktion,* Hamburger Mathematische Einzelschriften, Heft / 1931, Verlag B. G. Teubner, Leipzig. English translation: *The Gamma Function,* Holt Rinehart and Winston, N.Y., 1964.

[2] T. M. Apostol, *Introduction to Analytic Number Theory,* Springer-Verlag, 1976.

[3] Péter Kiss and Ferenc Mátyás, An asymptotic formula for π, Journal of Number Theory, 31 (1989), 255—259.

[4] Y. V. Matijasevic and R. K. Guy, *A new formula for* π, Amer. Math. Monthly, 93 (1986), 631—635.

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

[6] E. Trost, *Primzahlen*, Verlag Birkhauser, Basel-Stuttgart, 1953. Russian translation by N. J. Feldman and A. O. Gelfand, Moscow, Nauka, 1959.

HOFFMAN MIKLÓS

ÉRINTŐKKEL MEGADOTT PONTSOROZAT INTERPOLÁCIÓJA HARMADFOKÚ SPLINE GÖRBÉKKEL

ABSTRACT: (Interpolation of points and tangents by rational B-spilne) In this paper we provide a mentod to give a curve which goes pass to some given ponts and the tangents of the curve in these points are also given. The tool what we use is the rational B-spilne which is a well-known approximation method but also applicable to interpolate.

The main idea of the interpolation is that the given points will be the starting points of the segments of the future curve and the given tangents will be the tangents of it. These conditions yield a set of equations for the rational B-spline control points and its weights. To solve these equations we can compute the appropriate curve.

I. Bevezetés

Jelen dolgozatban egy olyan eljárást mutatunk be, amely segítségével tetszőleges számú előre megadott ponton keresztül egy görbét fektetünk oly módon, hogy a pontokban a

görbe érintője szintén előre megadott. Tesszük ezt harmadfokú racionális B-spline görbe segítségével, ami azzal az előnnyel jár, hogy a kpott görbe könnyen illeszthető más spline görbedarabokhoz, illetve lehetővé teszi az approximáció és az interpoláció ötvözését. A programok IBM-PC gépeken Turbo Pascal 5.0 nyelven íródtak, a rajzok Hewlett-Packard plotteren készültek.

II. A racionális B-spline

A B-spline, és ennek továbbfejlesztéseként a racionális B-spline a görbe- és a felületmodellezés legkedveltebb eszköze. (Itt, és ezek után a spline görbén mindig harmadfokú spline-t értünk.) Olyan előnyös tulajdonságokkal rendelkezik, mint a lokális változtathatóság vagy a C^2-folytonosság.

A B-spline tulajdonképpen approximációs feladatokra lett kitalálva, de alkalmas interpolációra is. A racionális változat annyiban különbözik az eredetitől, hogy itt az approximálandó pontokhoz még súlyokat is rendelhetünk, ami befolyásolja, hogy a görbe mennyire veszi figyelembe, mennyire közelíti az adott pontot.

Vizsgáljuk először a racionális B-spline-t mint approximáló görbét. Ha adottak a $V_i, 1 = 1,\ldots,n$ pontok (ún. kontroll pontok) és a $w_i, i = 1,\ldots,n$ súlyok, akkor az őket approximáló harmadrendű racionális B-spline görbe definíciója:

$$Q_i(u) = \frac{\sum_{r=-1}^{2} V_{i+r} w_{i+r} b_r(u)}{\sum_{r=-1}^{2} w_{i+r} b_r(u)} \qquad u \in [0,1]$$

ahol a b_r függvények az úgynevezett bázis függvények, harmadfokú polinomok:

$$b_{-1}(u) = \frac{1-3u+3u^2-u^3}{6}$$

$$b_0(u) = \frac{4-6u^2+3u^3}{6}$$

$$b_1(u) = \frac{1+3u+3u^2-3u^3}{6}$$

$$b_2(u) = \frac{u^3}{6}$$

Vegyük észre, hogy a görbe szegmensekből tevődik össze, minden szegmensen belül a paraméter befutja a [0,1] intervallumot. Ezen alapszin az interpoláció alapötlete.

III. Az interpoláció

Ha ugyanis adottak a $P_i, i = 1,\ldots,m$ interpolálandó pontok, akkor a feladatunk olyan kontroll pontokat nyerni ezekből, melyekre megrajzolva a görbét, az átmegy a P_i pontokon. E célból tegyük fel, hogy a P_i pontok a majdani görbe szegmenseinek kezdőpontjai. Ez a feltétel a következő egyenletrendszerrel írható le:

$$Q_i(0) = P_i \qquad i = 1,\ldots,m-1$$

$$Q_m(1) = P_m.$$

Az utolsó egyenlet azt fejezi ki, hogy az utolsó pont az utolsó szegmens végpontja legyen, hiszen onnan már nem indul ki új szegmens.

Azonban ha ezt az egyenletrendszert jobban megvizsgáljuk, láthatjuk, hogy az m egyenletben $2(m+2)$ ismeretlen van, a V_i pontok és a w_i súlyok. Így további meghatározó egyenletekre van szükségünk, amiket az előre adott $t_i, i = 1,\ldots,m$ érintők szolgáltatnak, ezek ugyanis a szegmen-

sek kezdőpontjaiban a görbe deriváltjával kell, hogy megegyezzenek:

$$\dot{Q}_i(0) = t_i \qquad i = 1,\ldots,m-1$$
$$\dot{Q}_m(1) = t_m.$$

Az újabb probléma az, hogy ezek az egyenletek a V_i kontroll pontokra és a w_i súlyokra mint ismeretlenekre nézve másodfokú egyenletrendszert adnak, amit csak nagyon nehezen, és hosszú idő alatt oldhatnánk meg. Ezt áthidalandó minden két P_i, P_{i+1} pont közé egy approximáló kontroll pontot előre megadunk, egységnyi súllyal. Ezt általában a két érintő, (t_i, t_{i+1}) egyeneseinek metszéspontjaként vehetjük fel, de ha ez túl messze kerülne a görbétől, azaz kis szöget zárna be a két egyenes, akkor egyszerűen a két pont, P_i, P_{i+1} felezési pontjának vesszük. Azért nem túl lényeges e pont pontos felvétele, mert később ezeket tetszés serint megváltoztathatjuk, az interpoláció elrontása nélkül. Így a tényleges egyenletek, amiket meg kell oldanunk, a következőképpen néznek ki:

$$\frac{\frac{1}{6}w_{i-1}V_{i-1} + \frac{4}{6}w_iV_i + \frac{1}{6}w_{i+1}V_{i+1}}{\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i-1}} = P_i$$

$$\frac{\left(-\frac{1}{2}w_{i-1}V_{i-1} + \frac{1}{2}w_{i+1}V_{i+1}\right)\left(\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1}\right)}{\left(\frac{1}{6}w_{i-1} + \frac{4}{6}w_i + \frac{1}{6}w_{i+1}\right)^2} -$$

$$\frac{-\left(\frac{1}{6}w_{i-1}V_{i-1}+\frac{1}{6}w_iV_i+\frac{1}{6}w_{i+1}V_{i+1}\right)\left(-\frac{1}{2}w_{i-1}+\frac{1}{2}w_{i+1}\right)}{\left(\frac{1}{6}w_{i-1}+\frac{4}{6}w_i+\frac{1}{6}w_{i+1}\right)^2}=t_i$$

Ebben a két egyenletben a V_i és a w_i ismeretlenek, a többi adat ismert, hiszen a $V_{i-1}, V_{i+1}, w_{i-1}, w_{i+1}$ adatok előre adottak. Az együtthatók a $b_i(u)$ és $\dot{b}_i(u)$ függvények $u=0$ helyen vett helyettesítési értékeiből jöttek.

Ha már most megkaptuk a keresett kontroll pontokat és a hozzájuk tartozó súlyokat, akkor az előre definiáltakkal együtt megrajzolhatjuk velük a kívánt görbét. A mellékelt ábrákon két görbe ugyanazokat a pontokat interpolálja, más-más érintőkkel.

IV. További lehetőségek

A most ismertetett eljárásnak legfőbb előnye a 'kompatibilitás', azaz mivel a végén egy közönséges spline görbét kapunk, ezt illeszthetjük más görberészekhez, függetlenül attól, hogy ezt milyen számítás végeredményeként kaptuk. Így lehetőség van például az approximáció és az interpoláció ötvözésére is úgy, hogy a végső görbe előre megadott pontokat approximál, míg másokat adott érintővel interpolál.

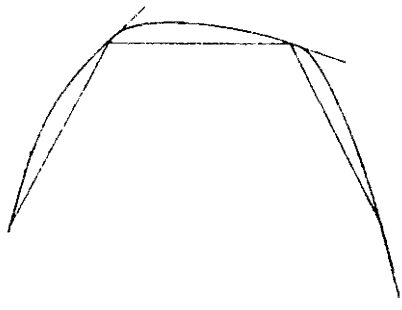


Fig. 1.

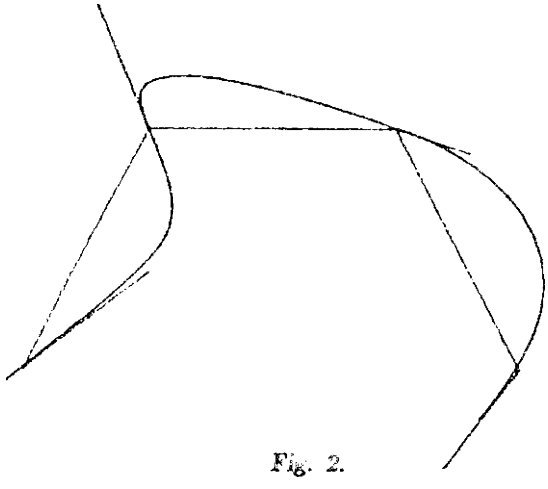


Fig. 2.

FELHASZNÁLT IRODALOM

[1] L. D. Faux and M. J. Pratt, *Computational Geometry for Design and Manufacture,* Hohn Wiley & Sons, NY, 1979.

[2] W. Tiller, *Rational B-splines for curve and surface representation,* IEEE Comp. Graph. Appl., 3(6) (1983) 91–69.

[3] M. Hoffmann, *Approximation and interpolation by B-spline at the same time,* Proc. Computergeometrie, Gaußig, Germany, 1990.

A. GRYTCZUK and J. KACIERZYNSKI

ON FACTORIZATION IN REAL QUADRATIC NUMBER FIELDS

ABSTRACT: This paper investigates uniqeness of factorization in quadratic number fields. It is proved by elementary method, that under certain conditions, the ring R_k of a field K is the ring with nonuique factorization.

1. Introduction. Using class-field theory C. S. Herz [1] proved the following result:
Let $K = Q(\sqrt{d})$ be given quadratic number field with the discriminant D which has t distinct prime divisors. Then the class group $H(K)$ of K hast $t-1$ even invariants, except the case when K is real and at least one prime $p \equiv 3 \pmod 4$ is ramified, in this case $H(K)$ has $t-2$ even invariants.
From this result we can deduce that if $h = H(K) = 1$ where $K = Q(\sqrt{d})$ and $d > 0$ then

(1.1) $d = p, 2q$

or qr where p is prime and $q \equiv r \equiv 3 \pmod 4$ are primes.

In this paper we prove by simple elementary method without using class-field theory the following.

Theorem. Let Z_s denote the set of all square-free integers and $L_d = \{d : d = p, 2q \text{ or } qr, q \equiv r \equiv 3 (\text{mod } 4)\}$
and let $K = Q(\sqrt{d})$, $d > 0$ and $d \in Z_s \setminus L_d$.
Then the ring R_K of K is the ring with nonuniqueness of factorization.
It is easy to see that from our Theorem follows also the corollary which follows from Herz's result.

Let Z_s denote the set of all squarefree positive integers and
(2.1) $L_d = \{d = p', 2q' \text{ or } q'r'; q' \equiv r' \equiv 3(\text{mod } 4), p', q', r' \text{ are primes}\}$

Then we can prove the following
Lemma 1. For every $d \in Z_s \setminus L_d$ there exist the odd primes p, q, q^* such that

(2.2) $p|d$, $q|d$ (may be $p = q$)

and

(2.3.) $\left(\frac{d}{q^*}\right) = 1$, $\left(\frac{q^*}{q}\right) = \left(\frac{-q^*}{p}\right) = -1$.

Proof. Since $d \in Z_s \setminus L_d$ thus it suffice to consider the following four cases:
1° $d = 2p$, $p \equiv 1 (\text{mod } 4)$ is a prime.

2° $d = 2^\alpha pp_1 \dots p_k$, $p \equiv 1 (\mathrm{mod}\, 4)$; $\alpha = 0$ or 1,
p and p_i are odd distinct primes.

3° $d = 2p_1 p_2 \dots p_k$, $k \geq 2$, $p_i \equiv 3 (\mathrm{mod}\, 4)$ for $i = 1,2,\dots,k$..

4° $d = p_1 p_2 \dots p_k$, $k \geq 3$, $p_i \equiv 3 (\mathrm{mod}\, 4)$ for $i = 1,2,\dots,k$.

Consider the case 1°. Let r denote the quadratic nonresidue for prime $p \equiv 1 (\mathrm{mod}\, 4)$. Hence $\left(\frac{r}{p}\right) = -1$. Suppose that m_0 is a positive integer such that

(2.4) $pm_0 + r \equiv 5 (\mathrm{mod}\, 8)$.

We note that m_0 satisfying (2.4.) exist since the number $pj + r$ for $j = 1,2,\dots,8$ gives distinct residues modulo 8. Let

(2.5) $r_m = p(8m + m_0) + r = 8pm + (pm_0 + r)$, $m = 1,2,\dots$.

From (2.4) it follows that $(8p, pm_0 + r) = 1$.
Therefore by Dirichlet's theorem we obtain from (2.5) that for some m

(2.6) $q^* = r_0$ where q^* is a prime number.

On the other hand by (2.4) it follows that $pm_0 + r = 8k + 5$ thus by (2.5) and (2.6) we obtain

(2.7) $q^* = 8t + 5$.

Since $r_m = q^* = p(8m+m_0)+r$ thus by well-known property of Legendre's symbol we have

(2.8) $$\left(\frac{q^*}{p}\right)=\left(\frac{r}{p}\right)=-1$$

By reciprocity law of Gauss in our case $q^* \equiv 5 \pmod 8$, $p = 4k+1$ we get

(2.9) $$\left(\frac{p}{q^*}\right)=-1 \quad \text{and} \quad \left(\frac{2}{q^*}\right)=-1$$

Thus by (2.9) we have

(2.10) $$\left(\frac{d}{q^*}\right)=\left(\frac{2p}{q^*}\right)=\left(\frac{2}{q^*}\right)\cdot\left(\frac{p}{q^*}\right)=+1.$$

By (2.8) and property of Legendre's symbol we have

$$\left(\frac{-q^*}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{q^*}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot\left(\frac{q^*}{p}\right)=-1$$

and the case 1° is proved.

For the proof of case 2° suppose that r, s are the residues for p and p_1 and $r_2, r_3, \ldots, r_k$ are non residues for modulo $p_2, p_3, \ldots, p_k$. Since $(p, p_i) = (p_i, p_j) = 1$ for $i \neq j$ thus by Chinese remainder theorem we obtain, that there exists positive integer u such that

(2.11) $u \equiv r \pmod p$, $u \equiv s \pmod{p_1}$, $u \equiv r_i \pmod{p_i}$; $i = 2, \ldots, k$.

Let m_0 denote the positive integer such that

(2.12) $pp_1 \dots p_k m_0 + u \equiv (\mathrm{mod}\, 8)$.

It is easy to see that such m_0 exist, because the number $pp_1 \dots p_1 j + u$ gives distinct residues (mod 8). Let

(2.13) $r_m = pp_1 \dots p_k (8m + m_0) + u = 8pp_1 \dots p_k m + (pp_1 \dots p_k m_0 + u)$ $m = 1, 2 \dots$. Since $(8pp_1 \dots p_k, pp_1 \dots p_k m_0 + u) = 1$ then by Dirichlet's Theorem we have for some m

(2.14) $q^* = r_m$ where q^* is a prime number.

It is easy to see that by (2.12) it follows that $q \overset{*}{\equiv} 1 (\mathrm{mod}\, 8)$. Therefore similarly as in the case 1° we obtain

(2.15) $$\left(\frac{q^*}{p}\right) = \left(\frac{u}{p}\right) = \left(\frac{r}{p}\right) = -1, \quad \left(\frac{q^*}{p_1}\right) = \left(\frac{u}{p_1}\right) = \left(\frac{s}{p_1}\right) = -1$$

and

(2.16) $$\left(\frac{q^*}{p_i}\right) = \left(\frac{u}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = 1 \qquad \text{for } i = 2, 3, \dots, k.$$

From (2.15), (2.16) and reciprocity law of Gauss we get

$$\left(\frac{p}{q^*}\right) = \left(\frac{p_1}{q^*}\right) = -1, \quad \left(\frac{p_i}{q^*}\right) = 1 \text{ for } i = 2, 3, \dots, k$$

and therefore we have $\left(\frac{d}{q^*}\right) = 1$, $\left(\frac{q^*}{p}\right) = -1$ and $\left(\frac{-q^*}{p}\right) = -1$.

Consider the case 3°. Let $\left(\frac{r_1}{p_1}\right)=+1$ and $\left(\frac{r_i}{p_i}\right)=-1$ for $i=2,3,\ldots,k$. Since $(p_i,p_j)=1$ for $i\neq j$ thus by Chinese remainder theorem we obtain that there exists a positive integer u such that $u\equiv r_i \pmod{p_i}$, for $i=1,2,\ldots,k$.
Similarly as in the case 2°, let m_0 denote the number statisfying $p_1\ldots p_k m_0+u\equiv 3 \pmod 8$ and let

$$r_m = 8p_1\ldots p_k m+(p_1\ldots p_k m_0+u).$$

Thus we obtain for some m, $q\doteq r_m$ and $q^*\equiv 3 \pmod 8$.
Therefore we obtain

(2.17) $\left(\frac{q^*}{p_1}\right)=\left(\frac{u}{p_1}\right)=\left(\frac{r_1}{p_1}\right)=1$ and $\left(\frac{q^*}{p_i}\right)=\left(\frac{u}{p_i}\right)=\left(\frac{r_i}{p_i}\right)=-1$

for $i=2,3,\ldots,k$. By (2.17) and reciprocity law of Gauss it follows that $\left(\frac{p_1}{q^*}\right)=-1$, $\left(\frac{p_i}{q^*}\right)=1$ for $i=2,3,\ldots,k$ and $\left(\frac{2}{q^*}\right)=-1$.

Therefore we obtain $\left(\frac{d}{q^*}\right)=1$, $\left(\frac{-q^*}{p_1}\right)=-1$, $\left(\frac{q^*}{p_2}\right)=-1$, and the case 3° is proved.
For the proof the case 4° we suppose that

$$\left(\frac{r_1}{p_1}\right)=\left(\frac{r_2}{p_2}\right)=1 \text{ and } \left(\frac{r_i}{p_i}\right)=-1 \text{ for } i=3,4,\ldots,k.$$

Since $(p_i,p_j)=1$ for $i\neq j$ thus by Chinese remainder theorem we obtain that there exists a positive integer u such

that $u \equiv r_i \pmod{p_i}$, for $i = 1,2,\ldots,k$. Let m_0 denote the number such that

$$p_1 p_2 \ldots p_k m_0 + u \equiv 3 \pmod 4$$

and

$$r_m = 4p_1 \ldots p_k m + (p_1 \ldots p_k m_0 + u),$$

$m = 1,2,\ldots$ then we have

$$(4p_1 \ldots p_k, p_1 \ldots p_k m_0 + u) = 1$$

and for some m,

$$r_m = q^* \equiv 3 \pmod 4.$$

Since $p_i \equiv 3 \pmod 4$ for $i = 1,2,\ldots,k$ thus we have

$$\left(\frac{q^*}{p_i}\right) = \left(\frac{u}{p_i}\right) = \left(\frac{r_i}{p_i}\right) = \begin{cases} 1 & \text{for } i = 1,2, \\ -1 & \text{for } i = 3,4,\ldots \end{cases}$$

By Gauss theorem we get

$$\left(\frac{p_i}{q^*}\right) = \begin{cases} -1 & \text{for } i = 1,2, \\ 1 & \text{for } i = 3,4,\ldots k. \end{cases}$$

Therefore $\left(\frac{d}{q^*}\right) = 1, \left(\frac{-q^*}{p_3}\right) = -1, \left(\frac{-q^*}{p_1}\right) = -1$

and proof the case 4° and our Lemma is finished.

Lemma 2. Let R_k denote the ring of all integers of $K = Q(\sqrt{d})$, $d > 0$. If R_k is the ring with uniqueness of factorization then the Diophantine equation

(2.18) $x^2 - dy^2 = \pm 4^\alpha p$

has a solution in positive integers x, y for every prime p such that $\left(\frac{d}{p}\right) = +1$, where

$$\alpha = \begin{cases} 0 & \text{if } d \equiv 2,3 \pmod 4 \\ 1 & \text{if } d \equiv 1 \pmod 4 \end{cases}$$

Proof. From the assumption that $\left(\frac{d}{p}\right) = +1$ it follows that there exists a positive integer x such that $x^2 \equiv d \pmod p$.
From this follows that

(2.19) $p | x^2 - d = \left(x - \sqrt{d}\right)\left(x + \sqrt{d}\right)$

Suppose that the number p is an irreducible element of R_k. Since the ring R_k is the ring with uniqueness factorization we get that the number p is also prime number in R_k.
The by (2.19) it follows that

(2.20) $p | x - \sqrt{d}$ or $p | x + \sqrt{d}$

it is impossible, because the elements $\frac{x - \sqrt{d}}{p}$ and are no elements of R_k.
Therefore we obtain

(2.21) $p = \left(\frac{x_1 + y_1\sqrt{d}}{2^\alpha}\right) \cdot \left(\frac{x_2 + y_2\sqrt{d}}{2^\alpha}\right)$

where

(2.22) $\alpha = \begin{cases} 0 & d \equiv 2,3 \pmod 4 \\ 1 & d \equiv 1 \pmod 4 \end{cases}$

and the elements $\frac{x_1 + y_1\sqrt{d}}{2^\alpha}$ and $\frac{x_2 + y_2\sqrt{d}}{2^\alpha}$ are noninvertible.

Hence by (2.21) we have

$$(2.23)\quad p^2 = N\left(\frac{x_1 + y_1\sqrt{d}}{2^\alpha}\right)\cdot N\left(\frac{x_2 + y_2\sqrt{d}}{2^\alpha}\right)$$

From (2.23) it follows that the equation

$$|x^2 - dy^2| = 4^\alpha p$$

has a solution in integers, x, y and proof of Lemma 2 is complete.

Result.

We can prove the following

Theorem. Let $K = Q(\sqrt{d})$, $d > 0$, $d \in Z_s \setminus L_d$. Then the ring R_k of K is the ring with nonuniqueness of factorization.

Proof. Suppose that for some $0 < d \in Z_s \setminus L_d$ the ring R_k is the ring with uniqueness of factorization. By Lemma 1 it follows that there are odd primes p, q, q^* such that $p|d$, $q|d$ and

$$(3.1.)\quad \left(\frac{d}{q^*}\right) = 1 \quad , \quad \left(\frac{q^*}{p}\right) = -1 \quad , \quad \left(\frac{-q^*}{p}\right) = -1$$

From (3.1) and Lemma 2 it follows that the equation

$$(3.2)\quad |x^2 - dy^2| = 4^\alpha q^*$$

has a solution in integers x, y. From (3.2) we have

$$(3.3)\quad x^2 - dy^2 = 4^\alpha q^* \qquad \text{or} \qquad x^2 - dy^2 = -4^\alpha q^*.$$

From (3.3) it follows that for $p|d$ and $q|d$ we have

$$(3.4.)\quad \left(\frac{4^\alpha q^*}{p}\right) = 1 \quad \text{or} \quad \left(\frac{-4^\alpha q^*}{q}\right) = 1.$$

But on the other hand from (3.1) we obtain

$$\left(\frac{4^{\alpha}q^{*}}{p}\right)=\left(\frac{q^{*}}{p}\right)=-1 \quad \text{and} \quad \left(\frac{-4^{\alpha}q^{*}}{q}\right)=\left(\frac{-q^{*}}{q}\right)=-1$$

so contrary to (3.4). The proof is complete.

From our Theorem we get the following

Corollary. Let $K=Q(\sqrt{d})$, $d>0$. If R_k of K is the ring with uniquenes of factorization then

$d \in L_d=\{d: d=p, 2q$ or qr, $q \equiv r \equiv 3 \pmod 4$, p,q,r are primes$\}$.

REFERENCES

[1] C. S. Herz, *Construction of class fields* in: Seminar on Complex Multiplication Lectures Notes in Math. Springer-Verlag 21, 1966.

Institute of Mathematics
Departament of Algebra and Number Theory
Pedagogical University of Zielona Góra
Zielona Góra, Poland

ALEKSANDER GRELAK

ON THE EQUATION $(x^2-1)(y^2-1)=z^2$

ABSTRACT: In this paper we get an explicit form of the formulae for all solutions in integers x,y,z of the Diophantine equation

(1) $$(x^2-1)(y^2-1)=z^2.$$

The equation (1) has been consider by K. Szymiczek [2] for the case when $x=a>1$ is a fixed integer. He proved that in this case the equation (1) has infinitely many solutions in integers x,y for every fixed integer $a>1$.

Let $T_n(u)=\cos(n \arccos u)$ be well-known Tchebyshev polynomial. In 1980 R. L. Graham [1] proved that all solutions of the equation (1) in integers x,y,z are given by the following formulae:

(2) $$x=T_n(u),\quad y=T_m(u),\quad z=\frac{1}{2}\left(T_{n+m}(u)-T_{n-m}(u)\right).$$

We note that the formulae (2) are effective but not easy to practical determination of the solutions of (1).

In this paper we prove the following theorem:

Theorem:

Let $< A_1, B_1 >$ denote the least positive solution of the Pell's equation $A^2 - DB^2 = 1$. Then all solutions of the equation (1) in the integers x, y, z are given by the formulae

$$\begin{cases} x = \frac{1}{2}\left[\left(A_1 + \sqrt{D}B_1\right)^i + \left(A_1 - \sqrt{D}B_1\right)^i\right] \\ y = \frac{1}{2}\left[\left(A_1 + \sqrt{D}B_1\right)^j + \left(A_1 - \sqrt{D}B_1\right)^j\right] \\ z = \frac{1}{4}\left[\left(A_1 + \sqrt{D}B_1\right)^i - \left(A_1 - \sqrt{D}B_1\right)^i\right]\left[\left(A_1 + \sqrt{D}B_1\right)^j - \left(A_1 - \sqrt{D}B_1\right)^j\right] \end{cases}$$

where i, j are arbitrary positive integers.

In the proof of our Theorem we use of the following Lemma.

Lemma.

Let $< A_1, B_1 >$ denote the least positive solution of the Pell's equation $A^2 - DB^2 = 1$ and let $< A_i, B_i >$ denote i-th solution of this equation.

If the equation (1) has a solution in integers x, y then there exists a positive integer D such that for some i, j we have $x = A_i$ and $y = A_j$ Moreover if for every squarefree D and every i, j we take $x = A_i$ and $y = A_j$ where $< A_i, B_i >$ and $< A_j, B_j >$ are the solutions of the equation $A^2 - DB^2 = 1$ then the numbers x, y satisfy the equation (1) with uniquely determined z.

Proof.

Suppose that integers x, y, z satisfy (1). Let $(x^2 - 1, y^2 - 1) = d = Du^2$, where D denotes the squarefree kernel of d. Then we have

(3) $x^2-1=dr,\quad y^2-1=ds;\quad (r,s)=1$

By (3) it follows that

(4) $(x^2-1)(y^2-1)=d^2rs.$

From (1) and (4) we have $r=r_1^2$, $s=s_1^2$ and consequently

(5) $x^2-1=dr_1^2=D(ur_1)^2\quad,\quad y^2-1=ds_1^2=D(us_1)^2$

what proves first part of our Lemma.

Now, let $< A_i, B_i >$ and $< A_j, B_j >$ denote arbitrary solutions of the equation $A^2-DB^2=1$ with squarefree D. Then we have $A_i^2-1=DB_i^2$ and $A_j^2-1=DB_j^2$.

Hence $\left(A_1^2-1\right)\left(A_j^2-1\right)=\left(DB_iB_j\right)^2$. Putting $z=DB_iB_j$, $x=A_i$ and $y=A_j$ we get second part of our Lemma and the proof is complete.

Proof of the Theorem

By well-known formulae from the theory of Pell's equation and our Lemma it follows that

(6) $$\begin{cases} x=\frac{1}{2}\left[\left(A_1+\sqrt{D}B_1\right)^i+\left(A_1-\sqrt{D}B_1\right)^i\right] \\ y=\frac{1}{2}\left[\left(A_1+\sqrt{D}B_1\right)^j+\left(A_1-\sqrt{D}B_1\right)^j\right] \end{cases}$$

From (6) and (1) we obtain $z=DB_iB_j$ and

$$z=\frac{1}{4}\left[\left(A_1+\sqrt{D}B_1\right)^i-\left(A_1-\sqrt{D}B_1\right)^i\right]\left[\left(A_1+\sqrt{D}B_1\right)^j-\left(A_1-\sqrt{D}B_1\right)^j\right]$$

and the proof of our Theorem is complete.

Corollary.

Let $a > 1$ be an arbitrary fixed integer.

Then all solutions in integers y, z of the equation

$$(a^2 - 1)(y^2 - 1) = z^2$$

are given by the formulae

$$y = \frac{1}{2}\left[\left(A_1 + \sqrt{D}B_1\right)^i + \left(A_1 - \sqrt{D}B_1\right)^i\right]$$

$$z = \frac{1}{2}b\sqrt{D}\left(\left(A_1 + \sqrt{D}B_1\right)^i - \left(A_1 - \sqrt{D}B_1\right)^i\right)$$

where D is squarefree kernel of $a^2 - 1 = Db^2$ and $< A_1, B_1 >$ is the least positive integer solution of the Pell's equation $A^2 - DB^2 = 1$.

REFERENCE

[1] R. L. Graham, On a Diophantine equation arsing in graph theory, Eur. J. Comb. 1(1980), 107—122.

[2] K. Szymiczek, On some Diophantine equations connected with triangular numbers (in Polish), Zeszyty Naukowe WSP Katowice - Sekcja Mat. No 4(1964), 17—22.

Institute of Mathematics
Departament of Algebra and Number Theory
Pedagogical University of Zielona Góra
Zielona Góra, Poland

KRYSTYNA GRYTCZUK

EFFECTIVE INTEGRABILITY OF THE DIFFERENCTIAL EQUATION

$P_0(x)y^{(n)} + P_1(x)y^{(n-1)} + \cdots + P_n(x)y = 0$

ABSTRACT: In the paper [1] was proved that the functions $y = s_{0,i}\ u_i^{\lambda}$, $i = 1,2,\ldots,n$ are the solutions of special form of differenctial equation

(1) $P_0(x)y^{(n)} + P_1(x)y^{(n-1)} + \cdots + P_n(x)y = 0$

This result is a generalization our recently result given in [2] for the case $n = 2$.

The purpose of this paper is to give a necessary and sufficient condition for the function

(2) $y_0 = \sum_{k=1}^{n} s_{o,k}\ u_k^{\lambda}$

to be a particular solution of (1) and also to give a necessary and sufficient condition for the functions $y_k = s_{o,k}\ u_k^{\lambda}$ for $k = 1,2,\ldots,n$ to be the particular solutions of (1).

We note that Theorem B given in [1] follows easily from our results.

We prove the follwing:

Theorem 1. Let $y_0 = y_0(x)$, $s_{l,k}(x)$, $u_k(x)$ and the coefficients $P_j(x)$ of (1), where $j,l = 0,1,\ldots,n$, $k = 1,2,\ldots,n$ satisfy the conditions:

1° $s_{l,k}(x)$, $u_k(x) \in C^{(n)}(J)$, $J = (x_1, x_2) \subset \mathbf{R}$, $\lambda \in \mathbf{R}_+$.

2° $u_k(x) \neq 0$, $y_0(x) \neq 0$, $P_0(x) \neq 0$ for $x \in J$.

3° $P_j(x) \in C(J)$.

The necessary and sufficient condition for the function (2) to be a particular solution of (1) is

$$(3) \qquad \sum_{k=1}^{n}\left(\sum_{j=0}^{n} P_j(x)\, s_{n-j,k}(x)\right) u_k^{\lambda}(x) = 0$$

where

$$(4) \qquad s_{l,k}(x) = s'_{l-1,k}(x) + s_{l-1,k}(x)\frac{u'_k(x)}{u_k(x)}$$

$k = 1,2,\ldots,n$.

Theorem 2. Let the assumptions 1°—3° of the Theorem 1 be satisfied. The necessary and sufficient codition for the functions

$$(5) \qquad y_k = y_k(x) = s_{0,k}(x)\cdot u_k^{\lambda}(x), \quad k = 1,2,\ldots,n$$

to be the particular solutions of (1) is

$$(6) \qquad \sum_{j=0}^{n} P_j(x)\cdot s_{n-j,k}(x) = 0, \quad k = 1,2,\ldots,n$$

where $s_{n,k}$ (x) are as in (4).

Proof of the Theorem 1.

For the proof of necessity we suppose that the function y_0 given in (2) is a solution of (1). Then by (2) and 1°–2° we obtain

$$(7) \qquad y_0' = \left(\sum_{k=1}^{n} s_{0,k} u_n^\lambda\right)' = \sum_{k=1}^{n}\left(s_{o,k}' + \lambda \cdot s_{o,k} \cdot \frac{u_k'}{u_k}\right) u_k^\lambda$$

Let in (7)

$$(8) \qquad s_{l,k} = s_{o,k}' + \lambda \cdot s_{o,k} \cdot \frac{u_k'}{u_k}.$$

By (7) and (8) it follows that

$$(9) \qquad y_o' = \sum_{k=1}^{n} s_{1,k} \cdot u_k^\lambda.$$

In similar way from (9) and our assumptions 1°—3° we obtain

$$(10) \qquad y_o^{(l)} = \sum_{k=1}^{n} s_{l,k} \cdot u_k^\lambda$$

where

$$(11) \qquad s_{l,k} = s_{l-1,k}' + \lambda \cdot s_{l-1,k} \cdot \frac{u_k'}{u_k} \quad ; \quad l,k = 1,2,\ldots,n.$$

From (10) and (11) get

$$P_0 y_0^{(n)} + P_1 y_0^{(n-1)} + \cdots + P_n y_0 = P_0\left(\sum_{k=1}^{n} s_{n,k} u_k^\lambda\right) +$$

$$(12) \qquad + P_1\left(\sum_{k=1}^{n} s_{n-1,k} u_k^\lambda\right) + \cdots + P_n\left(\sum_{k=1}^{n} s_{o,k} u_k^\lambda\right) = 0.$$

By (12) it follows that

$$\sum_{k=1}^{n}\left(\sum_{j=0}^{n} P_j \cdot s_{n-j,k}\right) u_k^\lambda = 0$$

and the condition (3) is true.

For the proof of sufficiency we suppose that the condition (3) holds. Then we have

$$P_0(x)\left(\sum_{k=1}^{n} s_{n,k}u_k^{\lambda}\right)+P_1(x)\left(\sum_{k=1}^{n} s_{n-1,k}u_k^{\lambda}\right)+\cdots+$$

(7)

$$+P_n(x)\left(\sum_{k=1}^{n} s_{0,k}u_k^{\lambda}\right)=0.$$

Let in (7)

(8) $$y_0 = y_0(x) = \sum_{k=1}^{n} s_{0,k}(x)\cdot u_k^{\lambda}(x)$$

By (8) it follows that

(9) $$y_0^{'} = \sum_{k=1}^{n} s_{1,k}\cdot u_k^{\lambda}$$

where

$$s_{1,k} = s_{0,k}^{'} + \lambda\cdot s_{0,k}\frac{u_k^{'}}{u_k}.$$

From (9) it follows that

(10) $$y_0^{(l)} = \sum_{k=1}^{n} s_{l,k}\cdot u_k^{\lambda};\quad l=1,2,\ldots,n$$

where

$$s_{l,k} = s_{l-1,k}^{'} + \lambda\cdot s_{l-1,k}\frac{u_k^{'}}{u_k}.$$

Substituting (8) and (10) to (7) we obtain

$$P_0y_0^{(n)} + P_1y_0^{(n-1)} + \ldots + P_ny_0 = 0$$

so the function y_0 is a solution of (1) and the proof is complete.

Proof of the Theorem 2.

For the proof of necessity suppose that the functions

(11) $$y_k = s_{0,k}\cdot u_k^{\lambda},\qquad k=1,2,\ldots,n$$

are the paricular solutions of (1).

From (11) by easy differentation we obtain

(12) $y_k^{(l)} = s_{l,k} \cdot u_k^{\lambda}, \quad l = 1,2,\ldots,n$

where

(13) $s_{l,k} = s_{l-1,k}^{\cdot} + \lambda \cdot s_{l-1,k} \cdot \dfrac{u_k^{\cdot}}{u_k}; \quad l,k = 1,2,\ldots,n.$

From our assumption for fixed $k = 1,2,\ldots,n$ we have

(14) $P_0 y_k^{(n)} + P_1 y_k^{(n-1)} + \cdots + P_n y_k = 0.$

Substituting to (14) the right hand side of (11) and (12) we get

(15) $P_0 s_{n,k} \cdot u_k^{\lambda} + P_1 s_{n-1,k} \cdot u_k^{\lambda} + \cdots + P_n s_{0,k} \cdot u_k^{\lambda} = 0.$

From (15) we have

(16) $\left(P_0 \cdot s_{n,k} + P_1 \cdot s_{n-1,k} + \cdots + P_n s_{0,k}\right) u_k^{\lambda} = 0.$

Since by 2° we have $u_k^{\lambda}(x) \neq 0$ then by (16) it follows that

$$P_0 \cdot s_{n,k} + P_1 s_{n-1,k} + \cdots + P_n s_{0,k} = 0$$

and the condition (6) is proved.

For the proof of sufficiency suppose that the conditions (6) are fulfilled. Then we have

(17) $P_0 \cdot s_{n,k} + P_1 \cdot s_{n-1,k} + \ldots + P_n \cdot s_{0,k} = 0 \quad \text{for } k = 1,2,\ldots,n.$

Substituting to (17) the right hand side of the formulae (13) we obtain

(18) $P_0\left(s_{n-1,k}^{\cdot} + \lambda \cdot s_{n-1,k} \cdot \dfrac{u_k^{\cdot}}{u_k}\right) + P_1\left(s_{n-2,k}^{\cdot} + \lambda \cdot s_{n-2,k} \cdot \dfrac{u_k^{\cdot}}{u_k}\right) + \cdots +$

$+ P_n \cdot s_{o,k} = 0.$

Now, we remark that

(19) $\left(s_{o,k} \cdot u_k^{\lambda}\right)^{\cdot} = s_{1,k} \cdot u_k^{\lambda}.$

From (19) by simple induction on l we obtain

(20) $\left(s_{o,k}\cdot u_k^{\lambda}\right)^{(l)} = s_{l,k}\cdot u_k^{\lambda}$ for $l = 1,2,\ldots,n$.

By (20) and (17) we get

(21) $p_0\left(s_{o,k}\cdot u_k^{\lambda}\right)^{(n)}\cdot u_k^{-\lambda} + P_1\left(s_{0,k}\cdot u_k^{\lambda}\right)^{(n-1)}\cdot u_k^{-\lambda}+\ldots+$
$+P_n\left(s_{0,k}\cdot u_k^{\lambda}\right)\cdot u_k^{-\lambda} = 0$

because $u_k \neq 0$ on J.

We note that

(22) $y_k = s_{0,k}\cdot u_k^{\lambda}$

and by (21) and (22) it follows that

$$P_0 y_k^{(n)} + P_1 y_k^{(n-1)} + \cdots + P_n y_n = 0$$

and for $k = 1,2,\ldots,n$.

The proof is complete.

Corollaries.

Corollary 1. Let $K = R\left[P_j\cdot s_{n-j,k}\right]$, $j = 0,1,2,\ldots,n$, $k = 1,2,\ldots,n$ denotes the ring of all polynomials of the intederminates $x_{j,k} = P_j\cdot s_{n-j,k}$ and let $u_1^{\lambda}, u_2^{\lambda},\ldots,u_n^{\lambda}$ be linearly independent over K. Then if the function

(23) $y_0 = \sum_{k=1}^{n} s_{o,k}(x)\cdot u_k^{\lambda}(x)$

is a solution of (1) then the all functions

(24) $y_k = s_{o,k}\cdot u_k^{\lambda}$ for $k = 1,2,\ldots,n$

are also the particular solutions of (1).

Proof. From the assumption of the Corollary 1 and the Theorem 1 it follows that

(25) $\sum_{k=1}^{n}\left(\sum_{j=0}^{n} P_j\cdot s_{n-j,k}\right)\cdot u_k^{\lambda} = 0.$

By (25) and the assumption that $u_1^{\lambda},\ldots u_n^{\lambda}$ are linearly independent over K we get

(26) $\sum_{j=0}^{n} P_j \cdot s_{n-j,k} = 0.$

Thus we obtain that the condition (6) of the Theorem 2 satisfied. Therefore by the Theorem 2 our Corollory 1 follows.

Corollary 2. Let the function $y_0 = \sum_{k=1}^{n} s_{0,k} \cdot u_k^{\lambda}$ be a solution of (1) and let A be the matrix of the form:

$$A = \begin{pmatrix} \sum_{k=1}^{n} S_{n,k} \cdot u_k^{\lambda} & \sum_{k=1}^{n} S_{n-1,k} \cdot u_k^{\lambda} & \cdots & \sum_{k=1}^{n} S_{0,k} \cdot u_k^{\lambda} \\ S_{n,1} & S_{n-1,1} & \cdots & S_{0,1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n,n} & S_{n-1,n} & \cdots & S_{0,n} \end{pmatrix}$$

Moreover let $D_{1,j-1}$ denote the minor of the matrix A which we obtain by deleting the first row and j column for $j = 1,2,\ldots,n+1$.

Then in the differenctial equation (1) we can take

$$P_{j-1} = (-1)^{j-1} D_{1,j-1}.$$

Proof. From the Theorem 1 we obtain

(27) $$P_0\left(\sum_{k=1}^{n} s_{n,k} \cdot u_k^{\lambda}\right) + P_1\left(\sum_{k=1}^{n} s_{n-1,k} \cdot u_k^{\lambda}\right) + \cdots + P_n\left(\sum_{k=1}^{n} s_{0,k} \cdot u_k^{\lambda}\right) = 0.$$

Since $y_0 = \sum_{k=1}^{n} s_{0,k} \cdot u_k^{\lambda} \neq 0$ on J thus by (27) we have

(28) $$P_n = -\frac{P_1\left(\sum_{k=1}^{n} s_{n,k} \cdot u_k^{\lambda}\right) + \cdots + P_{n-1}\left(\sum_{k=1}^{n} s_{0,k} \cdot u_k^{\lambda}\right)}{y_0}.$$

Put $P_{j-1} = (-1)^{j-1} D_{1,j-1}$ for $j = 1,2,\ldots,n$.

Then it suffices to prove that

(29) $P_n = (-1)^n D_{1,n}$.

For the proof of (29) note that from the form of the matrix A by Laplace's theorem we have

$$(30)\quad \det A = D_{1,0}\left(\sum_{k=1}^{n} s_{n,k}\cdot u_k^{\lambda}\right) + (-1)^1 D_{1,1}\left(\sum_{k=1}^{n} s_{n-1,k}\cdot u_k^{\lambda}\right) + \cdots + \\ + (-1)^n D_{1,n}\left(\sum_{k=1}^{n} s_{0,k}\cdot u_k^{\lambda}\right).$$

On the other hand it is easy to see that the first row of the matrix A is a linear combination of the others and therefore

(31) $\det A = 0$.

By (30) and (31) it follows that

$$(32)\quad (-1)^n D_{1,n} = -\frac{D_{1,0}\left(\sum_{k=1}^{n} s_{n,k}\cdot u_k^{\lambda}\right) + \cdots + (-1)^{n-1} D_{1,n-1}\left(\sum_{k=1}^{n} s_{1,k}\cdot u_k^{\lambda}\right)}{y_0}$$

From (32), (28) and the fact that

$P_{j-1} = (-1)^{j-1} D_{1,j-1}$ for $j = 1,2,\ldots,n$

we obtain

$(-1)^n D_{1,n} = P_n$

and the proof is complete.

REFERENCES

[1] K. Grytczuk, *Functional recurrences and differential equations*, Acta Acad. Paed. Agriensis. Tom. XX. Sectio Mat., (1991), 51—54.

[2] K. Grytczuk and A. Grytczuk, *Functional recurrences,* in: Applications of Fibonacci Numbers, (1990), 115—121, by Kluwer Academic Publishers.

Institute of Mathematics
Department of Stochastic Methods
Pedagogical University of Zielona Góra
65-069 Zielona Góra, Poland

RÓKA SÁNDOR

RAY-CHAUDHURI–WILSON TÍPUSÚ EGYENLŐTLENSÉG HÁRMAS METSZETEK ESETÉN

ABSTRACT: (On an inequality of type Ray-Chaudhuri–Wilson in the case of triple intersections) Let L be a set of a nonnegative integers and F a family of subsets of an n-element set X. Suppose that for any two distinct members $A,B \in F$ we have $|A \cap B| \in L$. Assuming in addition that F is uniform, i. e. each member of F has the same cardinality, a celebrated theorem of D. K. Ray-Chaudhuri and R. M. Wilson [3] asserts that $|F| \leq \binom{n}{s}$.

We prove a statement similar to the theorem. Let F be a family of subsets of set X having n elements. If for each $A,B,C \in F \quad A \neq B \neq C \quad |A \cap B \cap C| < t$, then $|F| \leq \frac{2}{\binom{s}{t}}\binom{n}{t}$. We give the construction of a set system for $t = 2$, close at the bound given in the theorem.

Ray-Chaudhuri–Wilson egyenlőtlenség [3] Az n-elemű X halmaz k-elemű részeinek egy családja F, és

$L=(r_1,r_2,\ldots,r_s)$, ahol az r_i számok nemnegatív egészek. Ha $\forall A,B\in F$, $A\neq B$ esetén $|A\cap B|\in L$, akkor $|F|\leq\binom{n}{s}$.

Ennek egy változata a következő tétel [5]:

Ha az n-elemű X halmaz $A_1,A_2,\ldots,A_m$ részhalmazai Sperner-rendszert alkotnak, és $|A_i\cap A_j|<s$, $1\leq i<j\leq m$ esetén, akkor $m\leq\binom{n}{s}$.

Mindkét állításból következik, hogy ha egy n-elemű X halmaznak $A_1,A_2,\ldots,A_m$ olyan k-elemű részhalmazai, hogy $|A_i\cap A_j|<s$, $1\leq i<j\leq m$, akkor $m\leq\binom{n}{s}$.

A dolgozatban ez utóbbi állításnak egy módosítását vizsgáljuk.

TÉTEL: Ha egy n-elemű X halmaznak $A_1,A_2,\ldots,A_m$ olyan 3-elemű részei, hogy $|A_i\cap A_j\cap A_k|\leq 1$, $1\leq i<j<k\leq m$, akkor $m\leq\frac{1}{3}n(n-1)$, s nagyságrendjében ez a becslés pontos.

Bizonyítás: Tekintsük az X halmaz 2-elemű részhalmazait. Egy ilyen halmaz a metszetfeltétel miatt legfeljebb két A_i-nek része. Mivel egy 3-elemű halmaznak három 2-elemű része van, így A_i-k 2-elemű részeit leszámolva az X halmaz 2-elemű részeinek mindegyikét legfeljebb kétszer kapjuk meg, tehát $3m\leq 2\binom{n}{2}$.

Lássuk be, hogy ha $m=c*n^{2-\varepsilon}$, $\varepsilon>0$, akkor az $A_1,A_2,\ldots,A_m$ halmazok még továbbiakkal bővíthetők. Egy A_i halmaznak a 3-elemű részhalmazok közül legfeljebb $3(n-3)$ db másikkal

vett metszete 2-elemű, tehát ezekből legfeljebb az egyik szerepelhet az $A_1, A_2, \ldots, A_m$ rendszerben. Valamint az kell még megfigyelni, hogy minden más 3-elemű halmaz A_i-hez képes „jó", azaz egy „jó" A_i^* halmazra $|A_i \cap A_i^* \cap A_k| \leq 1$ teljesül. Így, ha $m + m * 3(n-3) < \binom{n}{3}$, akkor van olyan 3-elemű halmaz, amely az $A_1, A_2, \ldots, A_m$ halmazok mindegyikéhez „jó", s így ezzel bővíthetjük a rendszert. Ez az egyenlőtlenség a fenti m érték esetén elegendően nagy n-re már teljesül.

Tehát valóban, nagyságrendjében pontos az $m \leq \frac{1}{3}n(n-1)$ becslés. A következőkben konstruálunk a tétel feltételeit kielégítő halmazrendszert. Az első konstrukcióban m értéke nagyságrendjében $n^{3/2}$, míg a második konstrukció közel van a megadott felsőkorláthoz, ott $m = \left[\frac{(n-1)^2}{4}\right]$.

Erdős Páltól származik a következő probléma [1]: Adott n pont a síkon (melyek között nincs három kollineáris), és minden ponthármas köré kört írunk. Mennyi a maximális száma az egységsugarú köröknek? Jelölje ezt a maximumot $f(n)$. Erdős igazolta, hogy $\frac{3*n}{2} < f(n) \leq n(n-1)$. Elekes György [2] egy szellemes konstrukcióval megmutatta, hogy $f(n) \geq c * n^{3/2}$ és megjegyzi, hogy valószínűleg nagyságrendjében ilyen a pontos korlát. Az n-pontból álló halmazt jelölje X, s azon ponthármasokat, melyek köré írt körök sugara 1 egység: $A_1, A_2, \ldots, A_m$. Ezek — mint könnyen látható — kielégítik a tétel feltételeit. Ezért mondhatjuk, hogy $f(n) \leq \frac{n(n-1)}{3}$. Sajnos a tétel és Erdős problémája közti kapcsolatból nem vonható le olyan következtetés, mely az egy-

ségkörök számára várt $c*n^{3/2}$ felső becslést kétségbe vonná. Elekes konstrukciója lehetőséget nyújt a tételben megszabott feltételeket kielégítő halmazrendszer megadására.

1. konstrukció: Tekintsük az l-elemű $H=(a_1,a_2,\ldots,a_l)$ halmaz 2-elemű részeit. Ezekből, mint elemekből álljon az X halmaz, melynek $A_1,A_2,\ldots,A_m$ részhalmazai $\{(a_r,a_s),(a_s,a_t),(a_t,a_r)\}$ alakúak. Ezekre teljesül a tételben kiszabott metszetfeltétel. $|X|=\binom{l}{2}=n$, $m=\binom{l}{3}$, tehát $m\le c*n^{3/2}$.

Az 1988-as Kürschák verseny [4] 2. feladata az általunk vizsgált halmazrendszerhez hasonlóval foglalkozik, az ott megadott konstrukció az alábbi.

2. konstrukció: Legyen $X=(1,2,3,\ldots,n)$, az $A_1,A_2,\ldots,A_m$ halmazok az $(a,b,a+b)$ alakú hármasok, ahol $1\le a<b$ és $a+b\le n$.

A tételhez hasonlóan bizonyítható: Ha egy n-elemű halmaznak $A_1,A_2,\ldots,A_m$ olyan s-elemű részei, hogy $|A_i\cap A_j\cap A_k|<t$, akkor $m\le\frac{2}{\binom{s}{t}}*\binom{n}{t}$, s nagyságrendjében ez a becslés pontos.

További vizsgálatok tárgya lehetne ilyen tulajdonságú halmazrendszer megadása, s a bevezetőben említett Ray-Chaudhuri–Wilson egyenlőtlenséggel analóg, hármas metszetekre vonatkozó állítás bizonyítása.

IRODALOM

[1] P. Erdős, *Some applications of graph theory and combinatorial methods to number theory and geometry,* Algebraic Methods in Graph Theory, Coll. Math. Soc. J. Bolyai, 25(1981), 137—148.

[2] G. Elekes, *n points in the plane can determine $n^{3/2}$ unit circles,* Combinatorica, 4(1984), 131.

[3] D. K. Ray-Chaudhuri and R. M. Wilson, *On t -designs,* Osaka J. Math., 12(1975), 737—744.

[4] Surányi János: *Az 1988. évi Kürschák József matematikai tanulóverseny feladatainak megoldása.* Középiskolai Matematikai Lapok, 1989. február, 50—60.

[5] Róka Sándor: *Ray-Chaudhuri–Vilson típusú egyenlőtlenségek.* A Bessenyei György Tanárképző Főiskola Tudományos Közleményei 12/D, 1990. 21—24.

BUI MINH PHONG
Eötvös Loránd University, Computer Center

RECURRENCE SEQUENCES AND PSEUDOPRIMES

ABSTRACT: In this paper we will present a summary of the most improtant results on recurrence sequences and pseudoprimes which we have discovered between 1974—1988.

I. RECURRENCE SEQUENCES

Let $G = G(G_0, G_1, A, B) = \{G_n\}_{n=0}^{\infty}$ be a second order linear recurrence defined by integer constans G_0, G_1, A, B and the recurrence

(1.1) $$G_n = AG_{n-1} - BG_{n-2} \qquad (n > 1),$$

where $AB \neq 0, D = A^2 - 4B \neq 0$ and $|G_0| + |G_1| \neq 0$. Let γ and δ be the roots of the characteristic polynomial $x^2 - Ax + B = 0$. The sequence $G(G_0, G_1, A, B)$ is called non-degenerate if γ / δ is not a root of unity. If $G_0 = 0$ and $G_1 = 1$, then we denote the sequence $G(0, 1, A, B)$ by $R = R(A, B)$. The sequence R is called Lucas sequence and R_n is called a Lucas number. In

the case where $A=-B=1$, the sequence $R(1,-1)$ is the Fibonacci sequence and we denote its terms by $F_0, F_1, F_2 \ldots$.

D. H. Lehmer *(Ann. Math. 31,1930,419—448)* generalized some results of Lucas on the divisibility properties of Lucas numbers to the terms of the sequence $U=U(L,M)=\{U_n\}_{n=0}^{\infty}$ which is defined by integer constants $L, M, U_0=0, U_1=1$ and the recurrence

$$U_n=\begin{cases} LU_{n-1}-MU_{n-2} & \text{for } n\not\equiv 0 \pmod 2 \\ U_{n-1}-MU_{n-2} & \text{for } n\equiv 0 \pmod 2, \end{cases} \tag{1.2}$$

where $LM\neq 0$ and $K=L-4M\neq 0$. The sequence U is called a Lehmer sequence and U_n is called a Lehmer number. We also say that the sequence $U(L,M)$ is non-degenerate if α/β is not root of unity, where α and β denote the roots of $z^2-L^{1/2}z+M=0$. It should be observed that Lucas numbers are also Lehmer numbers up to a possible multiplication by an integer factor.

I.1. *Generalized Lehmer sequences*

In [18] we define a generalized Lehmer sequence as follows:

Let H_0, H_1, L and M be integers with conditions $LM\neq 0$, $K=L-4M\neq 0$ and $|H_0|+|H_1|\neq 0$. A generalized Lehmer sequence is a sequence $H_0, H_1, \ldots H_n, \ldots$ of integer numbers satisfying a relation

(1.3) $$H_n = \begin{cases} LH_{n-1} - MH_{n-2} \text{ for } n \not\equiv 0 \pmod 2 \\ H_{n-1} - MH_{n-2} \text{ for } n \equiv 0 \pmod 2 \end{cases}.$$

We shall denote it by $H = H(H_0, H_1, L, M) = \{H_n\}_{n=0}^{\infty}$, and so $H(0,1,L,M)$ is the Lehmer sequence $U(L,M)$.

It was shown in [18] that in the case when $L = A^2$ and $M = B$ terms of sequence G defined in (1.1) are also terms of sequence H giving in (1.3) up to possible multiplication by an integer factor. Thus the sequences H are much more general sequences than the sequences G. Some authors have studied the lower and upper bound for the terms of the sequence G which is given in (1.1) with integer constants G_0, G_1, A and B. Let γ and δ be the roots of the equation $x^2 - Ax + B = 0$ with condition $|\gamma| \geqq |\delta|$. For example, K. Mahler *(J. Math. Sci. 1,1966, 12—17)* proved that if $D = A^2 - 4B < 0$ and ε is a positive constant, then there is an effectively computable constant n_0 depending only on ε such that

$$|G_n| \geqq |\gamma|^{(1-\varepsilon)n} \qquad \text{for} \qquad n > n_0.$$

From a result of T. N. Shorey and C. L. Stewart *(Math. Scand. 52,1983,24—36)* it follows that

$$|G_n| \geqq |\gamma|^{1-C_1 \log n}$$

for $n > C_2$, where C_1, C_2 are positive numbers which are effectively computable in terms of G_0, G_1, A and B. For the above constants P. Kiss *(Math. Sem. Notes (Kobe Univ.)*

7,1979,145—152) gave the explicit values, proving that $G_n \neq 0$ for $n > n_1$, where

$$n_1 = \max\left[2^{510}(\log|8B|)^{25}, 4\left(\log|G_0| + \log 4|D|^{1/2}\right)/\log 2\right],$$

furthermore if $D < 0$ and $n > n_1$, then

$$\frac{|c|}{2|D|^{1/2}}|\gamma|^n \cdot n^{-C_3} < |G_n| \leqq \frac{2|c|}{|D|^{1/2}}|\gamma|^n$$

where $c = G_1 - G_0\gamma$ and

$$C_3 = 2e200^{40}\log|8B|(1+\log\log|8B|)\log|16B|\left(G_0^2 + G_1^2\right).$$

In [18] we extended the results mentioned above to sequences $H(H_0, H_1, L, M)$, giving necessary and sufficient conditions for sequences H which have zero terms, furthermore giving lower and upper bounds for the terms. By using some results of M. Waldschmidt *(Acta Arith. 37, 1979, 257—283)* and C. L. Stewart *(Transcendence Theory, New York, 1977)* on linear forms in logarithms of algebraic numbers, we proved

Theorem 1.1. ([18], Theorem 2) *Let* $H = H(H_0, H_1, L, M)$ *be a generalized Lehmer sequence which is defined in (1.3). Let d=(L,M) and* $K = L - 4M$.

If $LK > 0$, *then* $H_n \neq 0$ *for* $n > max\ [13, min\ (|H_0|+1, |H_1|+2)]$.

If $LK < 0$, *then* $H_n \neq 0$ *for* $n > max\ (N_1, N_2)$, *where*

$$N_1 = min\left[2^{67}\log|4M|, e^{398}\right]$$

and

$$N_2 = min\left[\frac{4}{\log 2}\log|dH_0|, \frac{4}{\log 2}\log|H_1|\right].$$

Theorem 1.2. ([18], Theorem 3) *Let* $H = H(H_0, H_1, L, M)$ *be a generalized Lehmer sequence which is defined in (1.3) with the condition* $LK < 0$.

Then for $n > 2^{57}\log\left\{|4M|\left(H_o^{\,2} + H_1^{\,2}\right)\right\}$, *we have*

$$\frac{|a|}{2|LK|^{1/2}}|\alpha|^n \cdot n^{-C_0} < |H_n| < \frac{2|a|}{|K|^{1/2}}|\alpha|^n,$$

where

$$C_0 = 2^{80}\log|4M|\log\log|4M|\log\left\{|4M|\left(H_0^{\,2} + H_1^{\,2}\right)\right\},$$

$$a = H_1 - L^{1/2}H_0\beta,$$

and α, β *are roots of* $z^2 - L^{1/2}\cdot z + M = 0$.

We note that in the case $LK > 0$ Theorem 1.2 also holds.

I.2. *Prime divisors of Lehmer sequences*

Let $R = R(A, B)$ be a Lucas sequence. Assume that $(A, B) = 1$ and the sequence is non-degenerate, that is if γ and δ denote the roots of the characteristic polynomial $x^2 - Ax + B = 0$, then γ/δ is not a root of unity. It is known that in this case

$$R_n = \frac{\gamma^n - \delta^n}{\gamma - \delta} \tag{1.4}$$

for any $n \geq 0$. In the special case $(A; B = (3; 2)$ the terms of sequence R are $R_n = 2^n - 1$. For this sequence P. Erdős

(Istrael J. Math. 9, 1971, 43—48) proved that there are positive constants c and c' such that

$$\sum_{p|(2^n-1)} \frac{1}{p} < \log\log\log n + c$$

for distinct prime divisors and

$$\sum_{d|(2^n-1)} \frac{1}{d} < c' \cdot \log\log n$$

for the distinct positive divisors of the terms. Erdős note that similar results hold for the divisors of the numbers $Q^n - 1$ (Q is a positive integer), but he asked that the constants c and c' in this case depend on Q or not. In [14] with P. Kiss we extended these results for Lucas numbers, futhermore we give their improvments by showing that the constants in the inequalities do not depend on the sequence. For Lehmer sequences we proved in [10] (Chapter 4, Theorem 4.1.) the following

Theorem 1.3. ([10]) Let $U = U(L,M)$ *be the non-degenerate Lehmer sequence defined in (1.2) . Then there are positive absolute constants* c *and* c^**, which do not depend on the sequence* U*, such that*

$$\sum_{p|U_n} \frac{1}{p} < \log\log\log n + c$$

and

$$\sum_{d|U_n} \frac{1}{d} < c^* \cdot \log\log n$$

for any $n > N_0$*, where* N_0 *depends only on the sequence* $U(L,M)$.

A natural number m is called weakly composite if the reciprocal sum of its distinct prime divisors is not greater than 2, i.e.

$$\sum_{p|m} \frac{1}{p} \leq 2.$$

Proving conjecture of I. Kátai, J. Galambos *(Proc. Amer. Math. Soc. 29, 1986, 215—216)* showed that for any sufficiently large n there is a weakly composite number between n and $n+\log\log\log n$. In [10] (Chapter 4, Theorem 4.2) we proved

Theorem 1.4. ([10]) Let $U = U(L,M)$ *be a non-degenerate Lehmer sequence. For any* $n > 3$ *there is a Lehmer number* U_m *such that*

$$\sum_{p|U_m} \frac{1}{p} < C$$

and $n < m \leq n + \log\log n$, *where C is a constant depending only on* L *and* M.

We note that this result is an extension of result of P. Kiss and B. M. Phong [13] who proved a similar estimation for a non-degenerate Lucas sequence.

I.3. *Some Diophantine equations concerning recurrence sequences*

A linear recurrence $W = \{W_n\}_{n=0}^{\infty}$ of order $k(>1)$ is defined by integers $A_0, A_1, \ldots, A_{k-1}$ and by recursion

$$W_n = A_o W_{n-1} + A_1 W_{n-2} + \ldots + A_{k-1} W_{n-k} \quad (n \geq k),$$

where the initial values $W_0, W_1, \ldots, W_{k-1}$ are fixed not all zero integers and $A_{k-1} \neq 0$. Denote the distinct roots of characteristic polynomial

$$f(x) = x^k - A_0 x^{k-1} - \ldots - A_{k-1}$$

by $\alpha_0, \alpha_1, \ldots, \alpha_t$, where α_i has multiplity m_i. It is known that for $n \geq 0$

$$W_n = f_1(n)\alpha_1^n + f_2(n)\alpha_2^n + \ldots + f_t(n)\alpha_t^n,$$

where $f_i(n)$ is a polynomial of degree at most $m_i - 1$, furthermore the coefficients of $f_i(n)$ are algebraic numbers from the field $Q(\alpha_1, \ldots, \alpha_t)$. We say that the sequence W is non-degenerate if $t > 1$ *and* α_i / α_j is not a root of unity for $t \geq j > i \geq 1$.

Let $p_1, p_2, \ldots, p_r$ be primes and we denote by S the set of integers which have only these primes as prime factors.

K. Győry, P. Kiss and A. Schinzel *(Colloq. Math. 45, 1981, 75—80)* showed that if W is a non-degenerate Lucas sequence R, then

(1.5) $$W_x \in S$$

holds only for finitely many sequences W and for finitely many integers x. K. Győry *(Acta Arith. 40, 1982, 369—373)* improved this result giving explicit upper bound for x and for the constants of Lucas sequences which satisfy (1.5).

The Diophantine equation

$$W_x = sy^q \tag{1.6}$$

was also studied by several authors. T. N. Shorey and C. L. Stewart *(Math. Scand. 52, 1983, 24—36)* proved that if $y > 1$, $q > 1$ are integers and W is a non-degenerate recurrence of order k for which $m_1 = 1$ and $|\alpha_1| > |\alpha_j|$ $(j = 2,\ldots,t)$, then (1.6) implies the inequality $q < C_4$, where C_4 is an effectively computable constant in the terms of s and the parameters of sequence W. They showed that x and y are also bounded for second order recurrences. A. Pethő *(J. of Number Theory 15, 1982, 5—13)* proved similar results for second order recurrences supposing $(A_0, A_1) = 1$ and $s \in S$. For recent general results we refer to the monograph by T. N. Shorey and R. Tijdeman *(Exponential Diophantine Equations, Cambridge University Press, 1986)*, further to the references there.

The following problem remained open : if $|\alpha_1| = \ldots = |\alpha_t|$, then the equation (1.6) has finite or infinite solutions?

Let $R = R(A,B)$ be a Lucas sequence defined by integers A,B. For fixed integer $k > 0$ we put

$$T_0(k) \quad := k, \quad T_n(k) := R_{kn} / R_n \quad (\text{n=1,2,...}).$$

As it is known, $T_n(k) - s$ are integers. Let $T(k) = \{T_n(k)\}_{n=0}^{\infty}$. L. Somer *(Fibonacci Quart. 22, 1984, 98—100)* proved that the sequence $T(k)$ is a linear integeral recurrence of order k, furthermore the order k is minimal. Indeed, by using (1.4) we get

$$T_n(k) = \left(\gamma^{k-1}\right)^n + \left(\gamma^{k-2}\delta\right)^n + \ldots + \left(\delta^{k-1}\right)^n = (\alpha_1)^n + \ldots + (\alpha_k)^n,$$

where $\alpha_i = \gamma^{k-i}\delta^{i-1}$. If $D = A^2 - 4B < 0$, then $|\alpha_1| = \ldots = |\alpha_t| = |\gamma|^{k-1}$. Consequently, the investigation of the Diophantine equation $T_x = sy^q$ has meaning. In [12] we proved with I. Joó that the Diophantine equation

$$T_x(k) = sy^q$$

in integers $s \in S$, $q>2$, x, $|y|>1$ implies $\max(|s|,|y|,x,q) < C_5$, where C_5 is an effectively computable constant depending only on A, B, k and S. By using the theorem of T. N. Shorey, A. van der Poorten, R. Tijdeman and A. Schinzel *(Transcendence Theory, New York, 1977)* concerning the Thue-Mahler equation and the theorem of C. L. Stewart *(Transcendence Theory, New York, 1977)* on linear forms in logarithms of algebraic numbers, in [10] (Theorem 3.1) we improved the above result, namely we showed the following

Theorem 1.5. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence with the condition $(L,M) = 1$. Let $k > 1$ be an integer.*

Then all solutions of the Diophantine equation

$$U_{kx} / U_x = sy^q$$

in integers $s \in S$, $y \neq 0$, $q > 2$ satisfy

$$\max(x, |y|, q, |s|) < C_6$$

for $|y| > 1$ and

$$\max(x, |s|, |L|, |M|, k) < C_7$$

for the case when $|y| = 1$, $kx > 6$, $(k;x) \neq (2;4),(2;5)$, where C_6 and C_7 are effectively computable constants, C_6 depends only L, M, k and S, C_7 depends only on S.

Theorem 1.6. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence. Then the equation*

$$|U_x| = |U_y|$$

has non solutions in non-negative integers x, y with $x \neq y$ and $\max(x,y) > \min\left(e^{398}, 2^{67} \log|4M|\right)$.

I.4. *Lucas primitive roots*

Let $R = R(A,B)$ be a Lucas sequence defined by integers $R_0 = 0$, $R_1 = 1$, A, B and the recursion

$$R_{n+1} = AR_n - BR_{n-1} \quad \text{for } n > 0.$$

The sequence $R(1,-1)$ is the Fibonacci sequence F.

Let p be an odd prime with $B \not\equiv 0 \pmod{p}$ and let $e > 0$ be an integer. The positive integer $r = r(p^e)$ is called the rank of apparition of p^e in the sequence R if $R_r \equiv 0 \pmod{p^e}$ and $R_m \not\equiv 0 \pmod{p^e}$ for $0 < m < r$; furthermore $\nu = \nu(p^e)$ is called the period of the sequence R modulo p^e if it is the smallest positive integer for which $R_n \equiv 0 \pmod{p^e}$ and $R_{n+1} \equiv 1 \pmod{p^e}$. In the Fibonacci sequence, we denote the rank of apparition of p^e and period of F modulo p^e by $f(p^e)$ and $\pi(p^e)$, respectively.

Let the number R be a primitive root $\pmod{p^e}$. If $x = g$ satisfies the congruence

$$f(x) = x^2 - Ax + B \equiv 0 \pmod{p^e}, \tag{1.7}$$

then we say that R is a Lucas primitive root $\pmod{p^e}$ with parameters A and B. This is the generalization of the definition of Fibonacci primitive roots (FPR) modulo p that was given by D. Shanks for the case $A = -B = 1$ *(Fibonacci Quart., 10. 1973, 163—168, 181).*

The conditions for the existence of FPR $\pmod{p}$ and their properties were studied by several authors. For example, D. Shanks proved that if there exists a FPR $\pmod{p^e}$ then $p = 5$

or $p \equiv \pm 1 \pmod{10}$; furthermore, if $p \neq 5$ and there are FPR's $(\mathrm{mod}\ p)$ then the number of FPR's is two or one, according to whether $p \equiv 1 \pmod 4$ or $p \equiv -1 \pmod 4$. D. Shanks and L. Taylor *(Fibonacci Quart. 11. 1973, 159—160)* have shown that if g is a FPR $(\mathrm{mod}\ p)$ then $g-1$ is a FPR $(\mathrm{mod}\ p)$. M. J. DeLeon *(Fibonacci Quart. 15, 1977, 353—355)* proved that there is a FPR $(\mathrm{mod}\ p)$ if and only if $\ell(p) = p-1$. In [1] with P. Kiss we studied the connection between the rank of apparition of a prime p and the existence of FPR's $(\mathrm{mod}\ p)$. We proved that there is exactly one FPR $(\mathrm{mod}\ p)$ if and only if $f(p) = p-1$ or $p = 5$; moreover, if $p \equiv 1 \pmod{10}$ and there exitst two FPR's $(\mathrm{mod}\ p)$ or non FPR exists, then $f(p) < p-1$. M. E. Mays *(Fibonacci Quart, 20. 1982, 111)* showed that if booth $p = 60k-1$ and $q = 30k-1$ are primes then there is a FPR $(\mathrm{mod}\ p)$.

In [16] we given some connections among the rank of apparition of p^e in the Lucas sequence R, the period of R modulo p^e, and Lucas primitive roots $(\mathrm{mod}\ p^e)$; furthermore we shown necessary and sufficient conditions for the existence of Lucas primitive roots $(\mathrm{mod}\ p^e)$.

Theorem 1.7. ([16]) *Let R be Lucas sequence defined by integers $A \neq 0$ and $B = -1$, let p be an odd prime with $D = A^2 + 4 \not\equiv 0 \pmod p$, and let $e > 0$ be an integer. Then there is a Lucas primitive root* $(\mathrm{mod}\ p^e)$ *if and only if*

$$\ell(p^e) = \Phi(p^e)$$

where Φ *denotes the Euler function. There is exactly one Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if* $\psi(p^e) = \Phi(p^e)$ *and* $p \equiv -1 \,(\mathrm{mod}\, 4)$, *and there are exactly two Lucas primitive roots* $(\mathrm{mod}\, p^e)$ *if* $\psi(p^e) = \Phi(p^e)$ *and* $p \equiv 1 \,(\mathrm{mod}\, 4)$.

Theorem 1.8. ([16]) *Let* R *be Lucas sequence defined by integers* $A \neq 0$ *and* $B = -1$, *let* p *be an odd prime with* $D = A^2 + 4 \not\equiv 0 \,(\mathrm{mod}\, p)$, *and let* $e > 0$ *be an integer. Then there is exactly one Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if and only if* $r(p^e) = \Phi(p^e)$ *and* $p \equiv 1 \,(\mathrm{mod}\, 4)$, *and exactly two Lucas primitive roots* $(\mathrm{mod}\, p^e)$ *exist if and only if*

$$r(p^e) = \Phi(p^e)/2 \qquad \text{and} \qquad p \equiv 1 \,(\mathrm{mod}\, 8)$$

or

$$r(p^e) = \Phi(p^e)/4 \qquad \text{and} \qquad p \equiv 5 \,(\mathrm{mod}\, 8).$$

From these theorems, some other results follow.

Collary 1.9. *If* R, p *and* e *satisfy the conditions of Theorem 1.8 and* $r(p^e) = \Phi(p^e)$, *then* g *is a Lucas primitive root* $(\mathrm{mod}\, p^e)$ *if and only if* $x = g$ *satisfies the congruence*

$$R_n x + R_{n-1} \equiv -1 \,(\mathrm{mod}\, p^e),$$

where $n = \Phi(p^e)/2$.

Corollary 1.10. *If* R, p *and* e *satisfy the conditions of Theorem 1.8 and* g *is a Lucas primitive root* $(\mathrm{mod}\, p^e)$, *then* g-A *is a primitive root* $(\mathrm{mod}\, p^e)$.

We note that these results remain valid for Fibonacci primitive roots. In this case the following problem also remained open: Do there exist infinitely many primes p such that

$$\ell(p) = p - 1 \ ?$$

II. PSEUDOPRIMES

A problem, commonly attributed to the ancient Chinese, was to ascertain whether a natural number n must be a prime if it satisfies the congruence

$$2^n \equiv 2 \pmod{n}. \tag{2.1}$$

The question remained open until 1819, when Sarrus showed that $2^{341} \equiv 2 \pmod{341}$, yet $341=11.31$ is a composite number. In particular, a crude converse of Fermat's little theorem is false. In 1904, M. Cipolla *(Annali di Matematica 9, 1904, 139—160)* proved that there are infinitely many composite natural numbers n which satisfy the congruence (2.1).

Let $c>1$ be an integer. A composite natural n is called pseudoprime to base $c>1$ if

$$c^n \equiv c \pmod{n}. \tag{2.2}$$

If a composite natural n with $(n,c)=1$ and satisfies the congruence

$$c^{(n-1)/2} \equiv (c/n) \pmod{n}, \tag{2.3}$$

then n is called an Euler-pseudoprime to base c, where (c/n) denotes the Jacobi symbol. We simply say n is a pseudoprime (or an Euler-pseudoprime) if it is one to base 2.

The properties of pseudoprimes and their generalizations have been studied intensively, since they can be used for primality tests. For results and problems concerning pseudoprimes and their generalizations we refer to the works by A. Rotkiewicz *(Pseudoprime numbers and their generalizations, Univ. of Novi Sad, 1972),* E. Lieuwens *(Fermat pseudoprimes, Doctor thesis, Delft, 1971),* C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. *(The pseudoprimes to 25.10^9, Math. Comp. 35, 1980, 1003—1026),* further to the references there.

II. 1. *Lucas and Lehmer pseudoprimes*

Let $R = R(A,B)$ be a Lucas sequence defined by integers $R_0 = 0$, $R_1 = 1$, A and B. Let $D = A^2 - 4B \neq 0$, and we assume that the sequence R is non-degenerate. Let $S = S(A,B)$ be the sequence $G(2,A,A,B)$, that is $S_0 = 2$, $S_1 = A$ and $S_{n+1} = AS_n - BS_{n-1}$ $(n > 0)$. For odd primes n with $(n,D) = 1$, as it is well-known, we have

$$R_{n-(D/n)} \equiv 0 \pmod{n}, \tag{2.4}$$

$$R_n \equiv (D/n) \pmod{n}, \tag{2.5}$$

$$S_n \equiv S_1 \pmod{n} \tag{2.6}$$

and for odd prime n with $(n,BD) = 1$

$$(2.7)\quad \begin{cases} R_{(n-(D/n))/2} \equiv 0 & (\mathrm{mod}\, n) \text{ when } (B/n)=1 \\ S_{(n-(D/n))/2} \equiv 0 & (\mathrm{mod}\, n) \text{ when } (B/n)=-1, \end{cases}$$

where $(\ /n)$ is the Jacobi symbol. If n is composite, $(n,2D)=1$, but (2.4) still holds, then n is called a Lucas pseudoprime with parameteres A,B. Furthermore, if n is composite, $(n,2D)=1$ and satisfies the congruence (2.7), then n is called Euler-Lucas pseudoprime. It can be easily seen that in the case when $A=c+1$ and $B=c$, by using (1.4), we have $R_n=(c^n-1)/(c-1)$, and so the definitions of Lucas and Euler-Lucas pseudoprimes are generalizations of pseudoprimes and Euler pseudoprimes to base $c>1$.

We list some results which are in connection with ours. C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr. *(Math. Comp. 35, 1980, 1003—1026)* proved that for given positive integer s there is an Euler-pseudoprime which is a product of exactly s distinct primes. From results of A. J. van der Poorten and A. Rotkiewicz *(J. Austra. Math. Soc. Ser. A 29, 1980, 316—321)* it follows that there are infinitely many Euler pseudoprimes to base an integer $c>1$, which are of the form $ax+b$, where $(a,b)=1$. On the other hand, P. Erdős *(Amer. Math. Monthly 56, 1949, 623—624)* and E. Lieuwens *(Doctor thesis, Delft, 1971)* proved that for any integers c, $s>1$ there are infinitely many pseudoprimes to base c which are products of exactly s primes. This result was extended by P. Kiss, B. M. Phong and E. Lieuwens in [5] for Euler-Lucas pseudoprimes, among others, we proved that if $R=R(A,B)$ is a non-degenerate Lucas sequence with $D=A^2-4B>0$ and a,

s are positive integers, then there exist infinitely many Euler-Lucas pseudoprimes with parameters A, B which are products of exactly s primes of the form $ax+1$.

A. Rotkiewicz *(Bull. Acad. Polon. Sci. Ser. Sci. Math. Astr. Phys. 20, 1972, 349—354)* gave a proper generalization of ordinary pseudoprimes for Lehmer sequences. Let $U=U(L,M)$ be the non-degenerate Lehmer sequence defined by integers L, M and by (1.2). Let $V=V(L,M)=\{V_n\}_{n=0}^{\infty}$ be the sequence defined $V_0=2$ and by the relation

$$V_n = U_{2n}/U_n \qquad (n=1,2,\dots).$$

Similarly to the congruences (2.4)-(2.7), it is also known that for odd prime n with $(n,LK)=1$, we have

(2.8) $\quad U_{n-(LK/n)} \equiv 0 \pmod{n}$,

(2.9) $\quad U_n \equiv (K/n) \pmod{n}$

(2.10) $\quad V_n \equiv (L/n) \pmod{n}$,

and for odd prime n with $(n,LK)=1$

$$(2.11)\quad \begin{cases} U_{(n-(LK/n))/2} \equiv 0 \pmod{n} & \text{when } (LM/n)=1 \\ V_{(n-(LK/n))/2} \equiv 0 \pmod{n} & \text{when } (LM/n)=-1. \end{cases}$$

An odd composite n is called a Lehmer pseudoprime with parameters L, M if $(n,LMK)=1$ and (2.8) holds, and it is an Euler-Lehmer pseudoprime if (2.11) is true. Some results of

A. Rotkiewicz *(Math. Comp. 39, 1982, 239—247)* imply that for the non-degenerate Lehmer sequence $U(L,M)$ with $L>0$ and $K=L-4M>0$ every arithmetic progression $ax+b$, where $(a,b)=1$, contains an infinite number of Euler-Lehmer pseudoprimes with parameters L and M.

Using some theorems of A. Schinzel *(Acta Arith. 8, 1963, 213—223)* and J. Wójcik *(Acta Arith. 40, 1982, 155—174; Acta Arith. 40, 117—131)* we proved the following

Theorem 2.1. ([7]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence and let $s>1$ be an integer. Then there exists a positive integer w_0 such that for any integers a,b with condition $(a,bw_o)=1$ and for infinitely many primes p of the form $ax+b$ there exist an Euler-Lehmer pseudoprime which is the product of exactly s distinct primes and p is the least prime divisor of it.*

Theorem 2.2. ([17]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence with $LK=L(L-4M)>0$ and let a,s be positive integers. Then there are infinitely many Euler-Lehmer pseudoprimes which are products of exactly s primes of the form $ax+1$.*

A. Rotkiewicz *(Bull. Acad. Polon. Sci. Ser. Sci. Math. Astr. Phys. 21, 1972, 793—797)* showed that if $R(A,B)$ is non-degenerate Lucas sequence for which $B=1$ or $B=-1$, and a,b are relatively prime integers, then there exist infinitely many composite numbers n of the form $ax+b$ which satisfy

the congruences (2.4), (2.5) and (2.6) simultaneously. A similar result also holds for Lehmer sequences.

Theorem 2.3. ([7]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence for which $M = \pm 1$ and $LK = L(L \pm 4) > 0$. Then for any fixed positive integer s there are infinitely many Euler-Lehmer pseudoprimes n which are products of exactly s distinct primes of the form $ax+1$ and satisfy the congruences (2.8), (2.9) and (2.10) simultaneously.*

In the following we say that n is a perfect Lehmer pseudoprime with parameteres L,M if $(n, 2LMK) = 1$ and the congruences (2.8), (2.9), (2.10) hold. Improving a result of [8] concerning Lucas sequences, in [10] we showed

Theorem 2.4. ([10]) *Let $U = U(L,M)$ be a non-degenerate Lehmer sequence. Then the following three conditions are dependent:*

(i) n is a perfect Lehmer pseudoprime with parameters L,M

(ii) n is an Euler-Lehmer pseudoprime with parameters L,M

(iii) n is an Euler pseudoprime to base M.

That is, from any two ones of them, the third one follows.

II.2. *A generalized solution of A. Rotkiewicz's problem*

A. Rotkiewicz asked in his book the following question. "Let $c,k > 1$ be fixed positive integers. Do there exist infinitely

many composite integers n such that $n|(c^{n-k}-1)$?" *(Pseudoprime Numbers and Their Generalizations, Univ. of Novi Sad, 1972, problem 18)*. It is known as above that the answer is affirmative in the case $k=1$; the numbers satisfying the condition are pseudoprimes to base c. A general result was obtained by A. Makowski *(Simon Stevin 36, 1972, 71)*: For any natural number $k \geq 2$ there are infinitely many composite n such that

$$c^{n-k} \equiv 1 \pmod{n} \tag{2.12}$$

for any positive integer c with $(c,n)=1$. This result was proved earlier by D. C. Morrow *(Amer. Math. Monthly 58, 1951, 329—330)* in the case $k=3$. In this proof, Makowski showed that there are infinitely many integers n of the form $n=p.k$ (where p is a prime) such that congruence (2.12) holds for any positive integer c if $(c,n)=1$. Naturally, $(k,c)=1$ for these numbers, and so the question remained unanswered if c and k are fixed and $(k,c)>1$. In the case $(k,c)>1$, A. Rotkiewicz obtained two results: He proved that (2.12) has infinitely many solutions if $k=3$ and c is an arbitrarily fixed positive integer, or if $k=2$ and $c=2$ (see Theorem 32 in his book and *Math. Comp. 43, 1984, 271—272,* respectively).

In [9] with P. Kiss we gave a general solution of the problem, namely we proved

Theorem 2.5 ([9]) *Let* $c(<1)$ *and* k *be fixed positive integers. Then there are infinitely many composite integers* n *satisfying the congruence (2.12).*

In [17] we considered the following congruence

$$a^{n-k} \equiv b^{n-k} \pmod{n}, \tag{2.13}$$

where a,b and k are given positive integers with conditon $(a,b)=1$. Improving Theorem 2.5 we proved the following

Theorem 2.6. ([17]) *The congruence (2.13) has infinitely many composite solutions* n *if neither* (a,b,k) *is one of the following triples:*

$$\begin{aligned} &(2^u+1, 2^u-1, 3) && \text{for } u>1, \\ &(5.2^v+1, 5.2^v-1, 3) && \text{for } v>0, \\ &(c+1, c, 2); (c+3, c, 2) && \text{for } c>1. \end{aligned}$$

We note that W. L. McDaniel *(Colloq. Math. 59, 1990, 177—190)* independently proven this theorem and some generalizations of it. We obtained a similar result of Theorem 2.6 for Lehmer pseudoprimes.

Theorem 2.7. ([17]) *Let* $U=U(L,M)$ *be a non-degenerate Lehmer sequence. Then there is a positive integer* k_0 *such that for any fixed* $k>k_0$ *the congruence*

$$U_{n-k(LK/n)} \equiv 0 \qquad (\mathrm{mod}\, n)$$

has infinitely many composite solutions n. *Moreover, if* $k > 1$ *and* $(k, M) = 1$, *then there exist infinitely many composite integers* n *satisfying a congruence*

$$U_{n-k} \equiv 0 \qquad (\mathrm{mod}\, n).$$

II. 3. *Super Lucas and super Lehmer pseudoprimes*

We say that n is a super pseudoprime to base integer $c > 1$ if each divisor of it is a prime or a pseudoprime to base c. Similarly to super pseudoprimes to base c, we say that n is a super Lucas (super Lehmer) pseudoprime if each divisor of it is a prime or a Lucas (Lehmer) pseudoprime.

K. Szymiczek *(Elem. Math. 21. 1966, 59)* showed that $F_n F_{n+1}$ is a super pseudoprime to base 2 for any $n > 1$, where

$$F_n = 2^{2^n} + 1$$

is the n-th Fermat number. From the result of K. Szymiczek *(Colloq. Math. 13, 1964/65. 259—263)* it follows that there are infinitely many super pseudoprimes to base 2 which are products of exactly three primes. This result was extended by J. Fehér and P. Kiss *(Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 26, 1983. 157—159)* for super pseudoprimes to base c, where $c > 1$ is an integer with $c \not\equiv 0 (\mathrm{mod}\, 4)$. A. Rotkiewicz *(Glasgow Math. J. 9, 1968, 83—86)* has obtained another generalization of Szymiczek's result, he proved that for infinitely many primes p of the form $ax + b$, where $(a, b) = 1$,

there exist primes q and r such that pqr is a super pseudoprime to base 2. In [6] we extended the result of Rotkiewicz and the result of Fehér and Kiss mentioned above proving that form every integers $a>1$ and $c>1$ there are infinitely many triplets of distinct primes p,q and r of the for $ax+1$ such that pqr is a super pseudoprime to base c. We also showed that if the square-free kernel of the base c is congruent to ± 1 modulo *4,* then the series $\sum 1/\log n$ is divergent, where n runs through all super pseudoprimes to base c which are products of exactly three distinct primes.

P. Kiss *(Ann. Univ. Sci. Budapest. Eötvös Sect. Math. 28, 1986, 153—159)* studied the super Lucas pseudoprimes for non-degenerate Lucas sequences $R(A,B)$ and proved that R_{2p}/A is a super pseudoprime with parameters A,B for every large prime p, furthermore he showed that the series $\sum 1/\log n$, where n runs through all super Lucas pseudoprimes with parameters A and B, is divergent.

In [11], by using some result of J. Wójcik *(Acta Arith. 40, 1981/82, 155—174; 41, 1982, 117—131)* we improved above result as follows:

Theorem 2.8. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence. Then there exists a positive integer w_1 such that for infinitely many primes p of the form $ax+b$, where $(a,b)=1$ and $b\equiv 1 \pmod{(a,w_1)}$, there are primes q and r such that pqr is a super Lehmer pseudoprime with*

parameteres L,M. The constant w_1 is effectively computable in the terms of L and M.

Theorem 2.9. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence with condition $LK=L(L-4M)>0$ and let $a>1$ be an integer. Then there are infinitely many triplets of distinct primes p,q and r of the form $ax+1$ such that pqr is a super Lehmer pseudoprime with parameteres L,M.*

Theorem 2.10. ([11]) *Let $U=U(L,M)$ be a non-degenerate Lehmer sequence. Let S_1 and S_2 denote the set of all super Lehmer pseudoprimes with parameters L,M which are determined in Theorem 2.8 and Theorem 2.9, respectively. Then the series*

$$\sum_{n\in S_1}\frac{1}{\log n} \text{ and } \sum_{n\in S_2}\frac{1}{\log n}$$

are divergent.

We note that the conditions of Theorem 2.8 are satisfied for any integer $a>1$ if $b=1$ and for every pairs a,b with $(a,b,w_1)=1$. It is obvious that these results remain valid if we replace the super Lehmer pseudoprimes with super Lucas pseudoprimes. For example, from Theorem 2.10 we get.

Corollary 2.11. *For every integers $a,c>1$ the series $\sum 1/\log n$, where n runs through all super pseudoprimes to base c which are products of exactly three distrinct primes of the form $ax+1$, is divergent.*

II. 4. *The distribution of Lehmer pseudoprimes*

Let $\mathscr{A}(c,x)$ be denote the number of pseudoprimes to base c not exceeding x. In the case $c=2$ we denote $\mathscr{A}(2,x)$ by $\mathscr{A}(x)$. It is known that there exist positive constants C_1 and C_2 such that for all large x

$$C_1 \cdot \log x \leq \mathscr{A}(x) \leq x \cdot \exp\{-C_2(\log x \log\log x)^{1/2}\},$$

where the lower and the upper bound is due to D. H. Lehmer *(Amer. Math. Monthly 43, 1936, 347—354)* and P. Erdős *(Publ.Math. Debrecen. 4, 1956, 201—206)*, respectively. C. Pomerance improved these results showing that for all large x

$$\mathscr{P}(x) \geq \exp\{(\log x)^{5/14}\}$$

and

$$\mathscr{P}(x) \leq x \cdot \exp\{-\log x \log\log\log x / 2 \cdot \log x\}$$

(see Illinois J. Math. 26, 1982, 4—9 and *Math. Comp. 37, 1981, 587—593).*

Let $R = R(A,B)$ be non-degenerate Lucas sequence. Let $\mathscr{A}(R,x)$ be denote the number of all Lucas pseudoprimes with parameteres A,B not exceeding x. R. Baillie and S. S. Wagstaff, Jr. *(Math. Comp. 35. 1980, 1391—1417)* proved that there are positive constants C_3 and C_4 such that for all large x

$$\mathscr{P}(R,x) < x \cdot \exp\{-C_3(\log x \log\log x)^{1/2}\}$$

for any sequence R and

$$\mathscr{P}(R,x) > C_4 \cdot \log x$$

for sequences R for which $D = A^2 - 4B > 0$ but D is not a perfect square. This lower bound was extended by P. Kiss *(Ann. Univ. Sci. Budapest, Sect. Math. 28, 1986, 153—159)* to all non-degenerate Lucas sequences R. Very recently P. Erdős, P. Kiss and A. Sárközy *(Math. Comp. 51, 1988, 315—323)* improved the lower bound for $\mathcal{P}(R,x)$ extending Pomerance's result for Lucas pseudoprimes. They showed that there is a positive constant C_5 such that for all large x

$$\mathcal{P}(R,x) > \exp\left\{(\log x)^{C_5}\right\}$$

for any non-degenerate Lucas sequence R. In the proof of this result they showed only the existence of the constant C_5 and they noted that it would be interesting to get a reasonable numerical estimate for this constant.

By using some results of Selberg's sieve and a new idea concerning some congruences of Lehmer sequences, in [10] we extended the above result of Pomerance, Erdős, Kiss and Sárközy for Lehmer pseudoprimes, furthermore we gave a numerical value for C_5.

Theorem 2.12. ([10]) *Let $U = U(L,M)$ be a non degenerate Lehmer sequence and let $\mathcal{P}(U,x)$ denote the number of all Lehmer pseudoprimes with parameters L and M not exceeding x. Then for all large x we have*

$$\mathcal{P}(U,x) > \exp\left\{(\log x)^{1/35}\right\}$$

and

$$\mathcal{P}(U,x) < x \cdot \exp\{-\log x \cdot \log\log\log x / 2\log x\}.$$

A. Rotkiewicz *(Acta Arith. 21, 1972, 251—259)* proved the following result: If $a > 6$ is a given integer, then for all large x $\neq \{n \leq x | n$ is pseudoprime and $n \equiv 1 (\mathrm{mod}\, a)\} \geq \log x / (2 \log 2) a$.

We improved this result showing the following

Theorem 2.13. ([10]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence and let $a > 1$ be an integer with condition $(a, M) = 1$. Then there is a positive constant C_6 such that for all large x, the number of all Lehmer pseudoprimes with parameters L, M which are congruent to 1 modulo a and not exceed x is greater than*

$$\exp\{(\log x)^{C_6}\}.$$

For super Lehmer pseudoprimes we obtained the following

Theorem 2.14. ([15]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence and let Δ denote the square-free kernel of M. $\max(L, K)$, where $K = L - 4M$. If $\Delta \equiv \pm 1 (\mathrm{mod}\, 4)$, then for all large x the number of all super Lehmer pseudoprimes with parameters L, M not exceeding x is greater than*

$$(4\Delta \log |\alpha|)^{-1} \cdot \log x,$$

where α, β denote the roots of $z^2 - L^{1/2} z + M = 0$ and $|\alpha| \geq |\beta|$.

Showing a conjecture of A. Rotkiewicz, A. Makowski *(Elem. Math. 29, 1974, 13)* proved that the series $\sum 1/\log n$, where n runs through all pseudoprimes to bace c, is

divergent. In [4] we extended this result showing that the series

$$\sum \frac{1}{\log_{s-1} n}$$

is divergent, where n runs through all pseudoprimes to base c which are products of exactly s primes. Here $\log_k$ denotes the k times iterated logarithm. It was proved in [7] that

Theorem 2.15. ([7]) *Let $U = U(L, M)$ be a non degenerate Lehmer sequence. The series*

$$\sum \frac{1}{\log_{s-2} n},$$

where n runs through all Lehmer pseudoprimes which are products of exactly $s(\geq 3)$ distinct primes, is divergent.

REFERENCES

[1] P. Kiss & B. M. Phong, On the connection between the rank of apparition of a prime p in Fibonacci sequence and the Fibonacci primitive roots, Fibonacci Quart. 15 (1977), 347—349.

[2] P. Kiss & B. M. Phong, On a function concerning second order recurrences, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 21. (1978), 119—122.

[3] P. Kiss & B. M. Phong, Divisibility properties in second order recurrences, Publ. Math. Debrecen 26 (1979), 187—197.

[4] B. M. Phong, A generalization of A. Makowski's theorem on pseudoprime numbers, Tap chi Toan hoc 7 (1979), 16—19, (in Vietnamese).
[5] P. Kiss, B. M. Phong & E. Lieuwens, On Lucas pseudoprimes which are products of s primes, Fibonacci Number and Their Applications, 1986, 133—139.
[6] B. M. Phong, On super pseudoprimes which are products of three primes, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 30 (1987), 125—129.
[7] B. M. Phong, On Lucas and Lehmer pseudoprime numbers, Matematikai Lapok (1982—1986), 79—92 (in Hungarian).
[8] B. M. Phong, Connections between Lucas pseudoprimes of different types, Tudományos Közl., Eger (1987), 55—67 (in Hungarian).
[9] P. Kiss & B. M. Phong, On a problem of A. Rotkiewicz, Math. Comp. 48 (1987), 751—755.
[10] B. M. Phong, Lehmer sequences and Lehmer pseudoprimes, Ph. D. Thesis, Budapest, 1987.
[11] B. M. Phong, On super Lucas and super Lehmer pseudoprimes, Studia Math. Hungar. 23. (1988), 435—442.
[12] I. Joó & B. M. Phong, On two Diophantine equations concerning Lucas sequences, Publ. Math. Debrecen 35 (1988), 301—307.
[13] P. Kiss & B. M. Phong, Weakly composite Lucas numbers, Ann. Univ. Sci. Budapest Eötvös, Sec. Math. 31 (1988), 179—182.

[14] P. Kiss & B. M. Phong, The reciprocal sum of prime divisors of Lucas numbers, Tudományos Közl., Eger (1988), 47—54.
[15] I. Joó & B. M. Phong, On super Lehmer pseudoprimes, Studia Math. Hungar. 25 (1990), 121—124.
[16] B. M. Phong, Lucas primitive roots, Fibonacci Quart. 29 (1991), 66—71.
[17] B. M. Phong, A generalized solution of A. Rotkiewicz's problem, Matematikai Lapok, 34 (1987), 109—119.
[18] B. M. Phong, On generalized Lehmer sequences, Acta Math. Hungar., 57 /3—4 (1991), 201—211.

RIMÁN JÁNOS

SPECIÁLIS POLINOMOK IRREDUCIBILITÁSÁRÓL

ABSTRACT: (On the Irreducibhility of Special Polynomials) In this paper we generalize or improve some earlier irreducibility theorems. We prove the following theorem. *Let* $f, g \in \mathbf{Z}[x]$ *be polynomials,*

$$f(x) := \prod_{i=1}^{m} (x - a_i) \text{ and } g(x) := c_1 x + c_0,$$

where $m \geq 2$ *a is natural number,* $a_1, a_2, \ldots, a_m$ *are distinct integers,* c_0, c_1 *are nonzero integers. The polynomial* $g \circ f$ *is irreducible over the field of rational numbers* $\mathbf{Q}$ *if at least one of the inequalities*

$$|c_1| > 2^m g^2(0) + 1, \qquad \max_{1 \leq i,j \leq m} |a_i - a_j| > \lambda(g(0), m)$$

is satisfied. (The definition of $\lambda(g(0), m)$ is in the paper.)

Dolgozatunkban **R, Q, Z, N** rendre a valós, a racionális, az egész és a természetes számok halmazát, továbbá $\mathbf{Z}[x]$ az egész együtthatós polinomok gyűrűjét jelöli. Egy f polinom fokszámának jelölésére a $\deg f$ szimbólumot használjuk. Megjegyezzük még, hogy a dolgozatban a polinomokat valós

függvényeknek tekintjük, és ezért az analízisben szokásos jelöléseket alkalmazzuk.

I. Schur [7] problémafelvetése nyomán számos dolgozatban vizsgálták olyan $g \circ f$ alakú polinomok irreducibilását, ahol $g \in \mathbf{Z}[x]$ egy (szükségképpen) $\mathbf{Q}$ felett irreducibilis polinom, míg $f \in \mathbf{Z}[x]$ $l > \frac{\deg f}{2}$ számú különböző egész zérushellyel rendelkező polinom.

Győry Kálmán és a szerző a [2] dolgozatban több korábbi eredményt javított, illetve általánosított a $\deg g = 1$ esetben. Cikkünkben tovább javítjuk ezeket az eredményeket $l = \deg f$ esetén.

Vezessük be a következő jelöléseket. Legyen $m \geq 2$ természetes szám, $g(0) \neq 0$ egész szám (a szóbanforgó g polinom konstans tagja), $N := \left[\frac{m+1}{2}\right]$,

$$k := k(m) := \left(2^{1-N} \tfrac{1}{2}\left[\tfrac{m}{2}\right]\left(\tfrac{1}{2}\left[\tfrac{m}{2}\right]+1\right)\cdots\left(\tfrac{1}{2}\left[\tfrac{m}{2}\right]+N-1\right)\right)^{\frac{1}{2}},$$

továbbá

$$\lambda(g(0),m) = \begin{cases} |g(0)|+1, & ha \quad m = 2,3, \\ |g(0)|+2, & ha \quad m = 4, \\ |g(0)|, & ha \quad 5 \leq m \leq 8, \\ \frac{4(|g(0)|+2[k]-2)}{m-4}, & ha \quad 9 \leq m \leq 11, \\ \frac{|g(0)|}{2}+[k], & ha \quad m \geq 12. \end{cases}$$

Tételünk bizonyításához az alábbi *lemmákra* lesz szükségünk.

1. LEMMA. (R. J. Levit) *Legyen* $f, g \in \mathbf{Z}[x]$,

$$f(x) := \prod_{i=1}^{m}(x-a_i) \quad \textit{és} \quad g(x) := c_1 x + c_0,$$

ahol c_0, c_1 *nullától különböző egészek és az* a_i*-k különböző egész számok. Ha* $|g(0)| < k^2(m)$*, akkor* $g \circ f$ *irreducibilis* **Q** *felett.*

BIZONYÍTÁS. Az állítás közvetlenül adódik a [4]-ben szereplő 2. Tételből.

2. LEMMA. (L. Weisner) *Ha f és g az 1. Lemmában szereplő polinomok és*

$$|c_1| > 2^m g^2(0) + 1$$

vagy

$$\max_{1 \le i,j \le m} |a_i - a_j| > (3 + \lambda(m))|g(0)|,$$

ahol $\lambda(2) = \lambda(6) = 1$, $\lambda(3) = 4$, $\lambda(4) = 6$, $\lambda(5) = 3$ *és* $\lambda(m) = 0$, *ha* $m \ge 7$, *úgy* $g \circ f$ *irreducibilis* **Q** *felett, és az első egyenlőtlenségben* $g(0)$ *nagyságrendje már nem javítható.*

BIZONYÍTÁS. Lásd a [10] dolgozatot.

3. LEMMA. *Ha f és g előző lemmákban szereplő polinomok és*

$$|c_1| > 2^m g^2(0) + 1 \quad \textit{vagy} \quad \max_{1 \le i,j \le m} |a_i - a_j| > \lambda^*(g(0), m)$$

ahol

$$\lambda^*(g(0), m) = \begin{cases} |g(0)| + 1, & ha \quad m = 2, 3, \\ |g(0)| + 2, & ha \quad m = 4, \\ |g(0)|, & ha \quad 5 \le m \le 16, \\ \frac{2}{3}|g(0)| + \left(8 - \frac{m}{2}\right), & ha \quad m \ge 17, \end{cases}$$

akkor $g \circ f$ *irreducibilis* **Q** *felett.*

BIZONYÍTÁS. Lásd a [2] dolgozatban.

TÉTEL. *Legyen* $f, g \in \mathbf{Z}[x]$,

$$f(x) := \prod_{i=1}^{m} (x - a_i) \text{ és } g(x) := c_1 x + c_0,$$

ahol c_0, c_1 *nullától különböző egészek és az* a_i *különböző egész számok. Ha*

$$|c_1| > 2^m g^2(0) + 1 \quad \textit{vagy} \quad \max_{1 \le i,j \le m} |a_i - a_j| > \lambda(g(0), m),$$

akkor $g \circ f$ *irreducibilis* **Q** *felett.*

BIZONYÍTÁS. Az $m \le 8$ esetek bizonyítása megtalálható a [2] dolgozatban. (Ezzel kapcsolatban megjegyezzük, hogy a szerző doktori disszertációjában több helyen lényegesen egyszerűsítette a bizonyítást.)

Legyen $m \ge 9$. A 1. Lemma miatt elgendő a

$$\max_{1 \le i,j \le m} |a_i - a_j| > \lambda(g(0), m)$$

feltétel mellett bebizonyítanunk a tételben szereplő $g \circ f$ polinom **Q** feletti ireducibilitását.

Az általánosság megszorítása nélkül feltehetjük, hogy az a_i számok $a_1 < a_2 < \ldots < a_m$ módon vannak elrendezve, és így $\max_{1 \le i,j \le m} |a_i - a_j| = a_m - a_1$. Az állítással ellentétben tegyük fel, hogy $g \circ f = f_1 f_2$, azaz

$$(g \circ f)(x) = c_1 \prod_{i=1}^{m} (x - a_i) + c_0 = f_1(x) f_2(x)$$

minden $x \in \mathbf{R}$ esetén. Ekkor $f_1(a_i)f_2(a_i) = g(0)$ minden i-re, tehát $f_1(a_i) \mid g(0)$ és $f_2(a_i) \mid g(0)$.

Az 1. Lemma miatt azt is feltehetjük, hogy $|g(0)| \geq k^2(m)$, ahol

$$k := k(m) := \left(2^{1-N} \tfrac{1}{2}\left[\tfrac{m}{2}\right]\left(\tfrac{1}{2}\left[\tfrac{m}{2}\right]+1\right)\cdots\left(\tfrac{1}{2}\left[\tfrac{m}{2}\right]+N-1\right)\right)^{\frac{1}{2}}$$

és itt $N := \left[\dfrac{m+1}{2}\right]$. Mivel $k^2(9) = 45$ és $k^2(m+1) \geq k^2(m)$ minden m természetes számra, így a továbbiakban mindig feltesszük, hogy $|g(0)| \geq 45$.

(I) Legyen először f_1-re vagy f_2-re, például f_1-re

$$[k] \leq |f_1(a_1)|, |f_1(a_m)|.$$

Ekkor

$$|f_1(a_1)|, |f_1(a_m)| \leq \frac{|g(0)|}{[k]}$$

és a fenti egyenlőtlenségek teljesülnek f_2-re is. Ha

$$\lambda_1 < a_m - a_1 \quad | |f_1(a_m) - f_1(a_1)| \leq \frac{2|g(0)|}{[k]},$$

akkor

$$\lambda_1 := \frac{2|g(0)|}{[k]} \tag{1}$$

esetén $f_1(a_1) = f_1(a_m)$, és így $f_2(a_1) = f_2(a_m)$. Mivel minden $1 < i < m$ természetes számra $|f_1(a_i)| \leq \sqrt{|g(0)|}$ vagy $|f_2(a_i)| \leq \sqrt{|g(0)|}$,

és az $[a_1, a_m]$ intervallum, „közepén" legfeljebb $\left[\frac{m}{2} - 1\right]$ számú a_i kivételével

$$\frac{\lambda_2}{2} + \frac{\frac{m}{2}-2}{2} < \frac{a_m - a_1}{2} + \frac{m-4}{4} \leq a_m - a_i$$

vagy

$$\frac{\lambda_2}{2}+\frac{\frac{m}{2}-2}{2}<\frac{a_m-a_1}{2}+\frac{m-4}{4}\le a_i-a_1.$$

Például mindkét esetben az első lehetőséget választva

$$\frac{\lambda_2}{2}+\frac{m-4}{2}<a_m-a_i \mid |f_1(a_m)-f_1(a_i)| \le \frac{|g(0)|}{[k]}+\sqrt{|g(0)|},$$

amiből

$$\lambda_2:=\frac{2|g(0)|}{[k]}+2\sqrt{|g(0)|}-\frac{m-4}{2} \tag{2}$$

esetén $f_1(a_i)=f_1(a_m)=f_1(a_1)$, és ezért $f_2(a_i)=f_2(a_m)=f_2(a_1)$, azaz f_1 és f_2 is azonos értéket vesz fel legalább $m-\left[\frac{m}{2}-1\right]>\frac{m}{2}$ számú különböző helyen, ami például $\deg f_1 \le \frac{m}{2}$ miatt ellentmondás.

(II) Ezután tegyük fel, hogy f_1-nek és f_2-nek az a_1, a_m helyeken felvett értékei közül legalább egy abszolút értékben kisebb, mint $[k]$. Legyen például $|f_1(a_1)|<[k]$.

(i) Ha $|f_1(a_m)|\neq|g(0)|$, akkor $|f_1(a_m)|\le\frac{|g(0)|}{2}$, és így

$$\lambda_3<a_m-a_1 \mid |f_1(a_m)-f_1(a_1)|\le\frac{|g(0)|}{2}+[k],$$

amiből

$$\lambda_3:=\frac{|g(0)|}{2}+[k] \tag{3}$$

esetén $f_1(a_1)=f_1(a_m)$, és ezért $f_2(a_1)=f_2(a_m)$. Ha $\deg f_1=1$ vagy $\deg f_2=1$, akkor ez ellentmondás. Ha pedig $\deg f_1\ge 2$ és $\deg f_2\ge 2$, akkor léteznek olyan $f_1^*, f_2^* \in \mathbf{Z}[x]$ polinomok, amelyekkel

$$f_1(x)=(x-a_1)(x-a_m)f_1^*(x)+b_1$$

és

$$f_2(x)=(x-a_1)(x-a_m)f_2^*(x)+\frac{g(0)}{b_1}$$

minden x valós számra, ahol $b_1 \in \mathbf{Z}$ és $0 < b_1 < [k]$. Legyen $s := \left[\frac{m}{4} + 1\right]$. Ekkor bármely $s \le i \le m - s + 1$ esetén

$$a_m - a_1 \ge \frac{a_m - a_1}{2} \quad \text{vagy} \quad a_i - a_1 \ge \frac{a_m - a_1}{2}$$

és mindkét különbség nagyobb vagy egyenlő, mint $s-1$. Válasszuk például az első lehetőséget. Ha $|f_1(a_i)| \neq |g(0)|$ és $f_1^*(a_i) \neq 0$, akkor

$$\frac{|g(0)|}{2} + [k] - 1 \ge |f_1(a_i) - b_1| \ge |a_i - a_1||a_i - a_m| \ge (a_i - a_1)\frac{a_m - a_1}{2} \ge$$

$$\ge (s-1)\frac{a_m - a_1}{2} = \left[\frac{m}{4} + 1\right]\frac{a_m - a_1}{2} > \frac{m-4}{8}\lambda_4,$$

ami

$$\lambda_4 := \frac{4\left(|g(0)| + 2[k] - 2\right)}{m-4} \tag{4}$$

mellett nem lehetséges. Azaz $f_1^*(a_i) = 0$, és így $f_1(a_i) = b_1$, amiből $f_2^*(a_i) = 0$ és $f_2(a_i) = \frac{g(0)}{b_1}$ következik. Ha pedig $|f_1(a_i)| = |g(0)|$, akkor $f_2(a_i) = 1$, és ezért

$$\frac{\lambda_5}{2} < \frac{a_m - a_1}{2} \le a_m - a_i \;|\; |f_2(a_m) - f_2(a_i)| \le [k],$$

amiből

$$\lambda_5 := 2[k] \tag{5}$$

esetén $f_2(a_i) = f_2(a_m) = \frac{g(0)}{b_1}$, és így $f_1(a_i) = f_1(a_m) = b_1$, továbbá $f_1^*(a_i) = 0$ és $f_2^*(a_i) = 0$. Tehát f_1^*-nak és f_2^*-nak legalább $m - 2(s-1)$ számú a_i zérushelye van, és ezért f_1 és f_2 is legalább $m - 2s + 4$ különböző helyen b_1, illetve $\frac{g(0)}{b_1}$ értéket vesz fel, ami $m - 2s + 4 > \frac{m}{2}$ és például $\deg f_2 \le \frac{m}{2}$ miatt ellentmondás.

(ii) Ha $|f_1(a_m)|=|g(0)|$, akkor $|f_2(a_m)|=1$. Ismét két esetet különböztetünk meg.

Ha $2 \le |f_1(a_1)| < [k]$, akkor

$$\frac{|g(0)|}{[k]} < |f_2(a_1)| \le \frac{|g(0)|}{2},$$

és így

$$\lambda_6 < a_m - a_1 \mid |f_2(a_m) - f_2(a_1)| \le \frac{|g(0)|}{2} + 1,$$

amiből

$$\lambda_6 := \frac{|g(0)|}{2} + 1 \tag{6}$$

esetén $f_2(a_1) = f_2(a_m)$, és ez $|f_2(a_m)|=1$ miatt ellentmondás.

Ha $|f_1(a_1)|=1$, akkor $|f_2(a_1)|=|g(0)|$. Létezik legalább egy olyan a_i, amelyre

$$a_i - a_1 \ge \frac{a_m - a_1}{2} \quad \text{vagy} \quad a_m - a_i \ge \frac{a_m - a_1}{2},$$

és mindkét különbség nagyobb vagy egyenlő, mint $\left[\frac{m+1}{2}\right]-1$. Válasszuk például a második lehetőséget. Ha

$$|f_2(a_i)| \le \frac{|g(0)|}{\left[\frac{m+1}{2}\right]-2}$$

akkor

$$\frac{\lambda_7}{2} < \frac{a_m - a_1}{2} \le a_m - a_i \mid |f_2(a_m) - f_2(a_i)| \le \frac{|g(0)|}{\left[\frac{m+1}{2}\right]-2} + 1,$$

amiből

$$\lambda_7 := \frac{2|g(0)|}{\left[\frac{m+1}{2}\right]-2} + 2 \tag{7}$$

esetén $f_2(a_i) = f_2(a_m)$ és ezért $f_1(a_i) = f_1(a_m)$ következik. Ha $\deg f_2 = 1$, akkor ez ellentmondás. Ha pedig $\deg f_2 \ge 2$, akkor

létezik olyan $f_2^{**} \in \mathbf{Z}[x]$ polinom és b_2 egész szám, amelyekkel

$$f_2(x) = (x-a_m)(x-a_i)f_2^{**}(x) + b_2$$

minden $x \in \mathbf{R}$ számra, továbbá $|b_2| = 1$. Mivel $f_2^{**}(a_1) \neq 0$, így

$$|g(0)|+1 \geq |f_2(a_1) - b_2| \geq |a_m - a_1||a_1 - a_i| > \lambda_8\left(\left[\frac{m+1}{2}\right]-1\right),$$

ami

$$\lambda_8 := \frac{|g(0)|+1}{\left[\frac{m+1}{2}\right]-1} \tag{8}$$

mellet nem lehetséges. Ha a fenti a_i-re

$$|f_2(a_i)| > \frac{|g(0)|}{\left[\frac{m+1}{2}\right]-2}, \quad \text{akkor} \quad |f_1(a_i)| \leq \left[\frac{m+1}{2}\right]-3,$$

és így

$$\left[\frac{m+1}{2}\right]-1 \leq a_i - a_1 \,|\, |f_1(a_i) - f_1(a_1)| \leq \left[\frac{m+1}{2}\right]-2,$$

amiből $f_1(a_i) = f_1(a_1)$, és ezért $f_2(a_i) = f_2(a_1)$ következik. Ha $\deg f_1 = 1$, akkor ez ellentmondás. Ha $\deg f_1 \geq 2$, akkor létezik olyan $f_1^{**} \in \mathbf{Z}[x]$ polinom és b_3 egész szám, amelyekkel

$$f_1(x) = (x-a_1)(x-a_i)f_1^{**}(x) + b_3$$

minden $x \in \mathbf{R}$ számra, továbbá $|b_3| = 1$. Ekkor $|f_1(a_m)| = |g(0)|$ miatt $f_1^{**}(a_m) \neq 0$, így

$$|g(0)|+1 \geq |f_1(a_m) - b_3| \geq |a_m - a_1||a_m - a_i| > \lambda_9\left(\left[\frac{m+1}{2}\right]-1\right),$$

amiből $\lambda_9 = \lambda_8$ választással ismét ellentmondásra jutunk.

Végül legyen

$$\lambda(g(0),m) := \max_{1\leq i\leq 9}\{\lambda_i\} \quad \text{és} \quad \max_{1\leq i\leq 9}|a_1 - a_j| = a_m - a_1 > \lambda(g(0),m).$$

A $\lambda(g(0),m)$ ilyen választása mellett minden esetben ellentmondásra jutunk, tehát $g \circ f$ falóban irreducibilis $\mathbf{Q}$ felett.

Hátra van a $\lambda(g(0),m)$ értékének meghatározása. Felhasználva, hogy $m \geq 9$, $|g(0)| \geq 45$ és $[k] \geq 6$, az (1)—(8) egyenlőségekből egyszerű számolással adódik, hogy

$$\lambda(g(0),m) = \lambda_4 := \frac{4(|g(0)+2[k]-2)}{m-4}, \quad \text{ha } 9 \leq m \leq 11$$

és

$$\lambda(g(0),m) = \lambda_3 := \frac{|g(0)|}{2} + [k], \quad \text{ha } m \geq 12.$$

Ezzel a tétel bizonyítását befejeztük.

IRODALOM

[1] H. L. DORWART and O. ORE, *Criteria for the irreducibility of polynomials, Annals of Math.,* **34** (1933), 81–94.

[2] GYŐRY K. és RIMÁN J., *Schur-típusú irreducibilitási tételekről,* Matematikai Lapok, **24** (1973), 225–273.

[3] H. KLEIMAN, *Irreducibility criteria,* J. London Math. Soc., **5** (1972), 133–138.

[4] R. J. LEVIT, *Irreducibility of polinomyals with low absolute values,* Trans. Amer. Math. Soc., **132** (1968), 297–305.

[5] E. L. PETTERSON, *Einigen aus den Grössenbeziehungen der Wurzeln abgeleitete Irreduzibilitätskriterien,* Math. Annalen, **114** (1937), 79–83.

[6] G. PÓLYA, *Verschiedene Bemerkungen zur Zahlentheorie,* Jahresber. Deutsch. Math. Ver., **28** (1919), 31–40.

[7] I. SCHUR, *Aufgabe 275 und 279,* Archiv der Math. und Physik, **15** (1909).

[8] T. TATUZAWA, *Über die Irreduzibilität gewisser ganzzahliger Polynome,* Proc. Imp. Acad. Tokyo, **15** (1939), 253–254.

[9] H. TVERBERG, *On the irreducibility of polinomials taking small values,* Math. Scand., **32** (1973), 5–21.

[10] l. WEISNER, *Irreducibility of polynomials of degree n which assume the same value n times,* Bull. Amer. Math. Soc., **41** (1935), 248–252.

MÓDSZERTANI DOLGOZATOK

PELLE BÉLA

GEOMETRIAI TRANSZFORMÁCIÓK AZ ÁLTALÁNOS ISKOLÁBAN

RESÜMEE: Geometrische Transformationen in der Schule, Teil 2. Seit einiger Zeit verstärken sich die Versuche, den geometrischen Unterricht in den Prozeß der Umgestaltung und Modernisierung des mathematischen Unterreichts dadurch einzubeziehen, daß den eindeutigen (geometrischen) Abbildungen der Ebene auf sich, den Transformationen, der ihnen gebührende zentrale Platz eingeräumt wird. Dem Vorschlag liegt ein axiomensystem zugrunde, das aus dem Hilbertshen durch gewiesse Änderungen entsteht. Die Hilbertschen Kongruenzaxiome werden durch solche der Spiegelung ersetzt, durch Zusammensetzung von Spiegelungen die Bewegungen (Kongruenztransformationen) gewonnen. Mit diesen Transformationen untersucht man die Eigenschaften von Figuren der Ebene. Diese Verhandlung muß in der Grundschule gegründet werden. Der propädeutische Unterricht erarbeitet wesentliche Inhalte der Hilbertschen Axiomengruppen der Verknüpfung, Anordnung, Parallelität sowie Sachverhalte der Kungruenzlehre (gleichlange Strecken, gleichgroße Winkel, Spiegelungen an Geraden).

Im Teil 1. habe ich über die Lehrstoffe der Klassen 1–4 der Grundschule geschrieben. Im Teil 2. fasse ich die Lehrstoffe der Klassen 5–6 zusammen.

Általános megjegyzés

A geometria tárgyalásánál a sík ponthalmazához olyan transzformációkat rendelünk, amelyek a síkot önmagára képezik le. Az alakzatokat a sík ponthalmazának részhalmazaként fogjuk fel. Az alakzatok tulajdonságait a sík ponthalmazához rendelt transzformációk segítségével állítjuk össze. A tárgyalás során tehát először megismerjük az egyes transzformációkat, ezek alkalmazását feladatokon gyakoroljuk, majd az alakzatok tulajdonságait a transzformációk segítségével megvizsgáljuk.

Geometriai transzformációk az 5. osztályban

A tengelyes tükrözéssel kapcsolatos néhány fogalom gyakorlására az adott tulajdonságú pontok keresésénél nyílik alkalom. A két ponttól egyenlő távolságra lévő pontok keresésénél megállapítjuk, hogy az az AB szakasz felező merőlegese. Az eddig tanultakból azonnal következik, hogy a felezőmerőlegesre az A, B pontpár tükrös, tehát a felezőmerőleges tükörtengely.

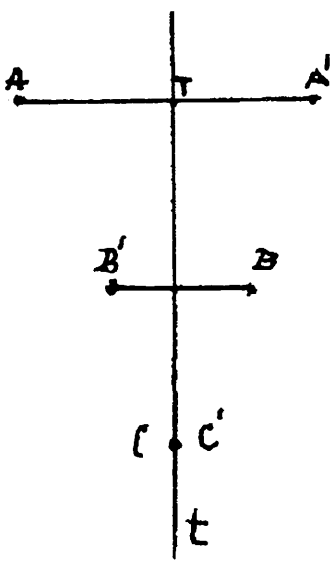
A közös pontból kiinduló két félegyenestől egyenlő távolságra lévő pontokról megállapítjuk, hogy azok a hajtásél pontjai. A hajtásél mentén összehajtva a két egyenes fedésbe

hozható. Ellenőrizhetjük, hogy a két egyenes pontjai a hajtásélre tükrözve egymásba mennek át, továbbá a hajtásél felezi a szöget. Éppen azért szögfelezőnek nevezzük. A szögfelező tehát a szög száraihoz tartozó tükörtengely.

Az 5. osztály anyagában körülbelül ezekkel tarthatjuk fenn a folyamatosságot az alsó tagozat és felső tagozat között a geometriai transzformációknál.

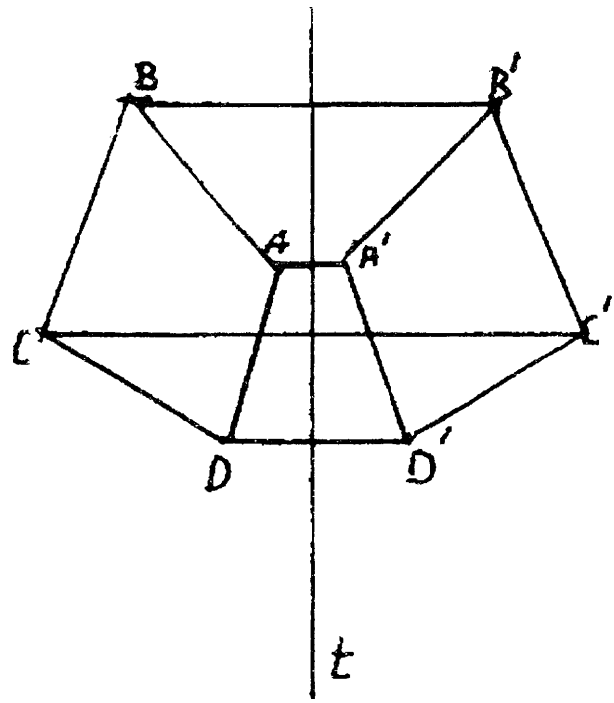
Geometriai transzformációk a 6. osztályban

Tengelyes tükrözés a síkon.



A tengelyes tükrözés egy sík pontjaihoz a sík pontjait rendeli a következő előírás szerint: Egy tetszőleges A pontból merőlegest húzunk a t tengelyre és a tengelyen lévő T metszéspontból felmérjük az AT szakaszt a másik félsíkban a merőleges egyenesre. Így kapjuk meg az A pont A' tükörképét.

Tükrözzük az $ABCD$ négyszöget a t tükörtengelyre!



Mondj igaz állításokat!

a) a pontokról és képeikről;

b) a szakaszokról és képeikről;

c) a szögekről és képeikről;

d) a szakaszokra illeszkedő egyenesekről és képeikről,

e) a tengelyek pontjairól;

f) a tengely által meghatározott félsíkokról;

g) a pontokat és képeiket összekötő egyenesekről.

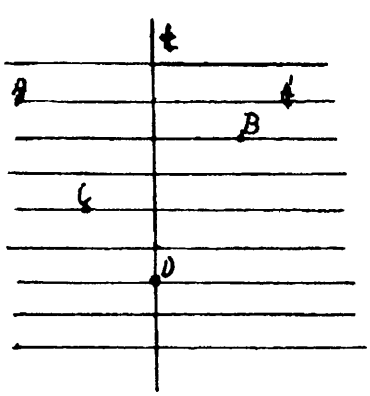
Ezek után foglaljuk össze a *tengelyes tükrözés alaptulajdonságait*!

1. A sík ponthalmazához a sík ponthalmazát rendeli.
2. A tengely pontjai fixek.
3. A félsíkokat felcseréli.
4. A pontot és képét összekötő szakasz merőleges a tengelyre, a tengely a szakaszt felezi.
5. Az eredeti és a képpontokat összekötő szakaszok párhuzamosak.
6. A tengelyes tükrözés szakasztartó és szögtartó transzformáció.
7. Alakzat és képe egybevágó.
8. Az alakzatok körüljárást megváltoztatja.

Gyakorlás

1. Négyzetrácson adott egy pont és a tükrözéssel kapott képe. Jelöld ki a tükörtengelyt!

Válaszolj!



a) A sík bármely pontjának a képét meg tudjuk ezután rajzolni?
b) A pont és képe meghatározza a tengelyes tükrözést?
c) Egy pontnak egy képe van, vagy több?

Egy pont és képe a tengelyes tükrözést egyértelműen meghatározza.

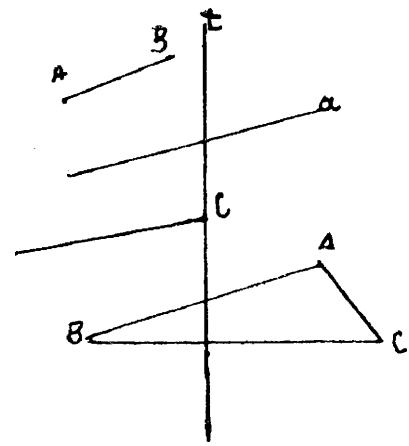
2. Adott a tengely, szerkesszük meg

a) az *AB* szakasz képét;

b) az *a* egyenes képét;

c) a *C*-ből kiinduló félegyenes képét

d) az *ABC* háromszög képét!



A tengely a tengelyes tükrözést egyértelműen meghatározza.

3. Négyzetrácson jelöljünk ki egy szakaszt! Keressünk olyan tengelyt, amelyre tükrözve a szakasz önmaga lesz a tükörképe.
Hány ilyen tengely van?

4. Rajzoljunk egy egyenest! Keressünk olyan tengelyt, amelyre tükrözve az egyenes saját magának a tükörképe lesz! Hány ilyen tengely van?
Azokat az egyeneseket, amelyeknek képe önmaga, invariáns *egyeneseknek* nevezzük.

5. Négyzetrácson jelöljünk ki két párhuzamos egyenest! Húzzunk olyan egyenest, amelyre az egyik egyenest tükrözve a másik egyenes kapjuk! Hány ilyen egyenes van?

Megoldás: a két párhuzamos egyeneshez egy tengely-egyenes van. Ezt a tengely-egyenest a két párhuzamos egyenes *középvonalának* nevezzük.

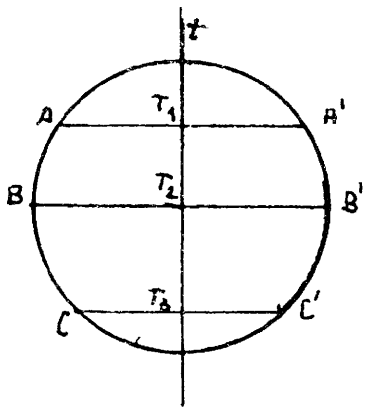
A következőkben a tengelyes szimmetrikus alakzatok tulajdonságait vizsgáljuk meg a tengelyes tükrözés segítségével.

A kör tükrös alakzat

A következő felépítésben tárgyalhatjuk:

a) Észrevétetjük, hogy a kör tükrös az átmérőre;
b) A tükrözésből megállapítjuk a húr és átmérő kapcsolatát, ezt összevetjük az 5. osztályban tanultakkal,
c) Rávezetjük a tanulókat az érintő és sugár kapcsolatára.
Ezt elvégezzük pl. a következő felépítésben.

Húzzunk meg a körben egy tetszőleges átmérőt! Hajtsuk ketté az átmérő mentén a kört! A két rész fedi egymást. Jelöljünk meg az egyik félkörön tetszőleges pontokat. A hajtogatás után jelöljük meg a másik félkörön a pontok megfelelőit. Kössük össze a megfelelő pontokat.
Mit tapasztalunk?



AA', BB', CC' merőleges az átmérőre. Mindegyik szakaszt felezi az átmérő, tehát $AT_1 = T_1A'$, $BT_2 = T_2B'$, $CT_3 = T_3C'$. A és A', B és B', C és C' szimmetrikus az átmérőre. Az egyik félkörből a másik félkört megkapjuk, ha a félkör pontjait tükrözzük az átmérőre.

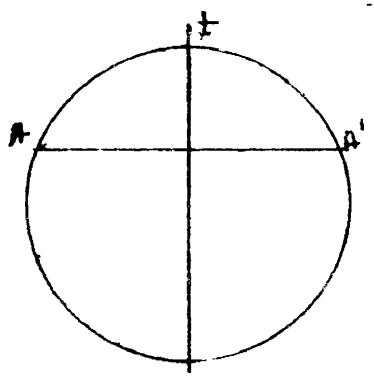
A kör átmérője a körnek tükörtengelye. A körnek minden átmérő tükörtengelye.

Rajzoljunk a körbe egy húrt! A középpontból rajzoljunk merőlegest a húrra!

Az előzőek alapján mondjunk igaz állításokat a húrra és a rá merőleges átmérőre!

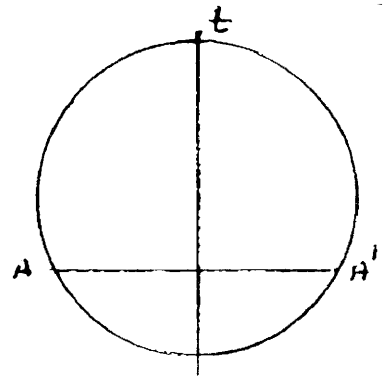
A húrra merőleges átmérő felezi a húrt. A húr felezési pontján átmenő átmérő merőleges a húrra.

A húr felezőmerőlegese átmérő.



Ellenőrizzük, igazoljuk ezeket az állításokat az 5. osztályban tanultak segítségével!

AA' egy szakasz. A szakasz két végpontjából egyenlő távolságra lévő pontok mértani helye a szakaszfelező merőleges. A középpont is ilyen tulajdonságú, tehát a húrfelező merőleges átmegy a kör középpontján.

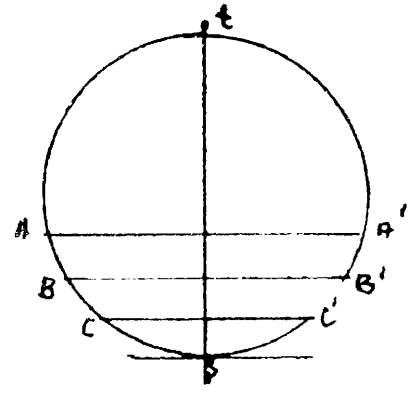


A húr közeledjen az átmérő egyik végpontja felé!

AA', BB', CC' húrok párhuzamosak, merőlegesek az átmérőre, A és A', B és B', C és C' szimmetrikus társak. Az átmérő végpontját jelöljük P-vel.

Mi lesz P szimmetrikus társa?

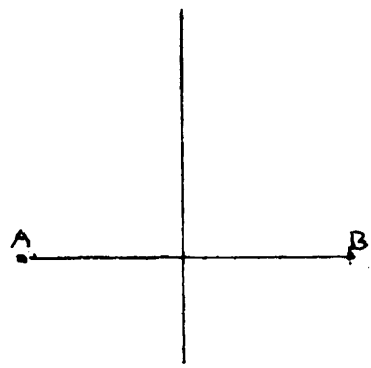
P szimmetriatársa P, P fixpont, mert a tengelyen van.



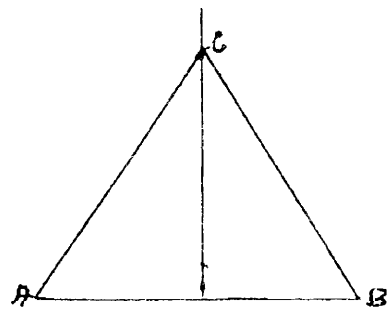
P-ben húzzunk merőlegest az átmérőre, mint tükörtengelyre. Ez a merőleges a körből P szimmetriatársát metszené ki. Mivel ez P, így a merőleges nem metszi a kört, csak egy közös pontja van a körrel. Ez a merőleges egyenes, tehát *érintő*.

Milyen tulajdonsága van az érintőnek és az átmérőnek a tükrözés alapján? Az átmérő és a végpontjában húzott érintő merőleges egymásra. Ha az átmérőnek csak az érintési ponthoz tartozó felét tekintjük, akkor az sugár.
Így: *az érintő merőleges az érintési pontba húzott sugárra.*

Tükrös háromszögek



Az eddig tanultak alapján rajzoljuk meg azt az egyenest, amelynek pontjai egyenlő távolságra vannak az A és a B pontoktól.
Milyen neveket adtunk ennek az egyenesnek? *Szakaszfelező merőleges*, amely két ponttól egyenlő távolságra lévő pontok mértani helye, két ponthoz tartozó tükörtengely.



Válasszuk ki a szakaszfelező merőleges tetszőleges C pontját és kössük össze A-val és B-vel. $AC = BC$, tehát az ABC háromszög *egyenlő szárú háromszög.*

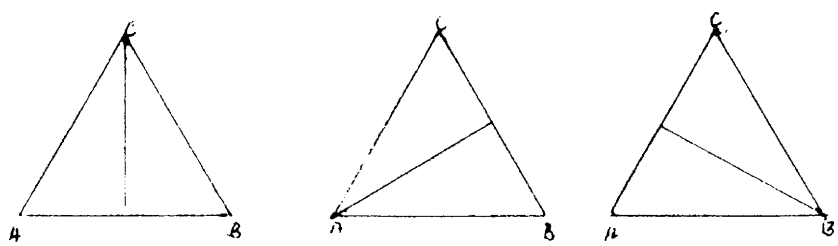
Tükrözzük az ABC háromszöget az alapfelező merőlegesre! Az A pont B-be kerül, a B pont A-ba, C pedig C-be. Így a háromszög képe önmaga.

Az egyenlő szárú háromszög tükrös az alap felezőmerőlegesére. Az alapfelező merőleges tükörtengely.

Állapítsuk meg az egyenlőszárú háromszög tulajdonságait a tükrözés alapján!

1. A CAB szög képe CBA szög, tehát az *alapon lévő szögek egyenlők*;
2. Az ACT szög képe BCT szög, tehát a *tükörtengely felezi a szárak szögét*;
3. Az egyenlő szárú háromszög tükörtengelye merőleges az alapra és azt felezi.

Az AB szakaszhoz tartozó tükörtengelyen jelöljük ki azt a pontot, amelynek A-tól és B-től a távolsága AB-vel egyenlő!



A háromszög nem csak egyenlő szárú, *hanem egyenlő* oldalú is, mert $AB = AC = BC$.

A tükrözés alapján (és az egyenlő szárú háromszögről tanultak alapján) az alapon lévő szögek egyenlők, tehát

$$CAB \sphericalangle = CBA \sphericalangle .$$

Válasszuk most BC-t alapnak. BC szakaszfelező merőleges átmegy az A csúcson, mert A egyenlő távolságra van a B és C pontoktól ($AB = AC$). Akkor a BC alapon lévő szögek is egyenlők, vagyis:

$$CAB \sphericalangle = BCA \sphericalangle .$$

Így: $CAB \sphericalangle = CAB \sphericalangle = BCA \sphericalangle$, vagyis az egyenlő oldalú háromszög szögei egyenlők.

Igazoljuk, hogy az AC oldal is lehet alapja az egyenlő oldalú háromszögnek!

Az AC szakaszhoz tartozó felezőmerőleges átmegy a B csúcson, mert a B pont egyenlő távolságra van az A és a C pontoktól: $AB = CB$. Hány tükörtengelye van az egyenlő oldalú háromszögnek? (Három.)

Foglaljuk össze az *egyenlő oldalú háromszög tulajdonságait*!

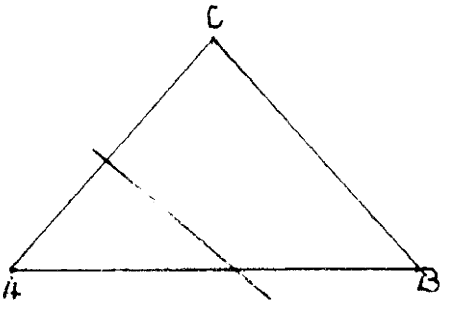
1. Minden szöge egyenlő.
2. Három tükörtengelye van.
3. A tükörtengelyek felezik a szögeket.

Méréssel válaszoljunk a következő kérdésekre!

Hány fokos az egyenlő oldalú háromszög egyik szöge? (60).

Hány fok egy háromszög belső szögeinek összege? (180).

Igazoljuk, hogy a nem egyenlő oldalú, egyenlő szárú háromszögnek nem lehet három tükörtengelye!

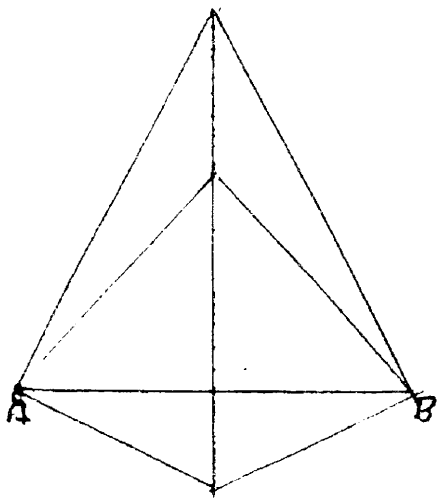


Ha $BC = AC$, de $BC \neq AB$, akkor az AC oldalhoz tartozó felezőmerőleges nem megy át a B csúcson, mert B nincs egyenlő távolságra A-tól és C-től. Hasonlóan ez igaz a BC szakaszra is.

Mi következik a bizonyításból?
Az egyenlő szárú, nem egyenlő oldalú háromszögnek 2 vagy 3 tükörtengelye nem lehet, csak 1.

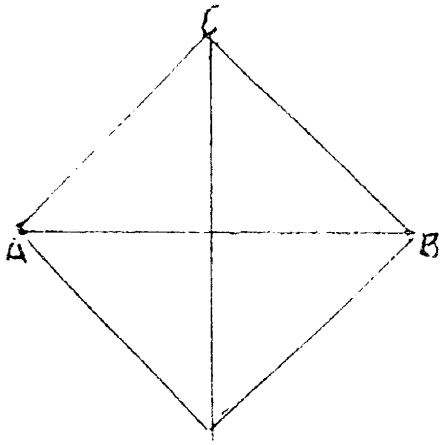
Szerkesztések a tükrös háromszög tulajdonságai alapján

1. Szerkesszünk olyan egyenlő szárú háromszöget (tükrös háromszöget), amelynek az alapja 3 cm!



Hány ilyen háromszöget tudunk szerkeszteni?
Mondjunk igaz állításokat ezekre a háromszögekre! Emeljük ki az igaz állítások közül a következőket:
– A tükörtengely felezi az egyenlő szárú háromszög alapját.
– A tükörtengely felezi az alappal szemközti szöget

2. Felezzük meg egy adott *AB* szakaszt!



Elemezzük az I. feladatot, az segít a megoldásban! Egyenlő szárú háromszögeket kell az *AB* szakaszra rajzolni. Elég kettőt megrajzolni. Ezek csúcsait összekötő egyenes lesz a tükörtengely, amely felezi az alapot.
Úgy rajzoljuk meg a két egyenlő szárú háromszöget, hogy csúcsai távolabb legyenek egymástól! Így pontosabban meg tudjuk rajzolni az egyenest.

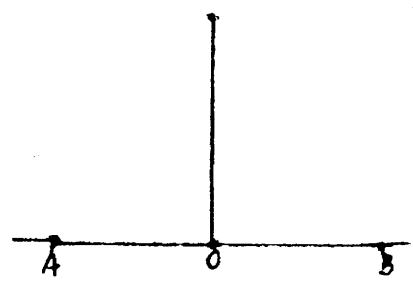
Az AB szakaszhoz megrajzolt tükörtengelyt *szakaszfelező merőlegesnek* neveztük.

3. Felezzünk meg egy szöget! Az előző ábráról olvassuk le a szerkesztést!

4. Szerkesszünk 60°-os szöget!
Keressünk a tükrös háromszögek között olyat, amelynek 60°-os szöge van! Ezt egyenlő oldalú háromszögnek neveztük. Az egyenlő oldalú háromszögnek csak egyik szögét kell megszerkeszteni.

5. Milyen szögeket tudunk szerkeszteni szögmérő felhasználása nélkül?
Ha 60°-ost tudunk szerkeszteni, akkor 300°-ost is tudunk, ugyanis a 60°-os szöghöz tartozó másik szögtartomány 300°-os, a 60°-os szögből 120°-os is szerkeszthető.
A 60°-os szög felezésével 30°-os, majd ennek a felezésével 15°-os szöget kapunk.

6. Szerkesszünk 90°-os szöget!
Egy egyenesen kijelöljük a 180°-os szög O csúcsát. A szögszárakon lévő A, B pontokból, $OA = OB$, az AB alaphoz tetszőleges körzőnyílással egyenlő szárú háromszöget szerkesztünk. A O

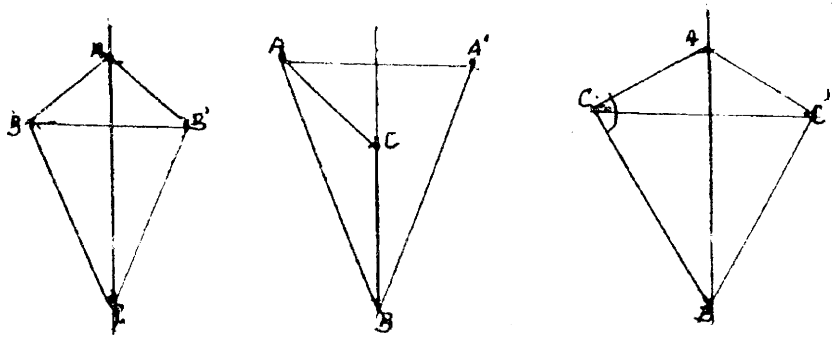


csúcsot összekötjük a metszésponttal. Ezzel a 180°-os szöget megfeleztük.

7. Szerkesszünk 45°-os szöget!
   a) Felezzük a 90°-os szöget.
   b) A 90°-os szöghöz egyenlő szárú derékszögű háromszöget szerkesztünk.

Tükrös négyszögek

Rajzoljunk fel nem egyenlő szárú hegyesszögű, tompaszögű és derékszögű háromszögeket! Tükrözzük ezeket egyik oldalukra, a derékszögűt az átfogóra. Négyszögeket kapunk.



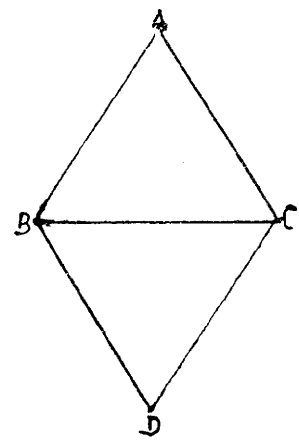
A tükörtengely a négyszögnek átlója lesz.

Az olyan négyszöget, amelynek egyik átlója tükörtengely, deltoidnak nevezzük.
A tükrözés alapján határozzuk meg a deltoid tulajdonságait!

– Két-két szomszédos oldala egyenlő.
– Két szöge egyenlő.
– A szimmetria átló felezi a két szöget.
– A szimmetria átló merőlegesen felezi a másik átlót.

Vizsgáljuk ezután azokat a deltoidokat, amelyeket egyenlő szárú háromszögekből kapunk, az alapra történő tükrözéssel! Olyan deltoidot kapunk, amelynek mindkét átlója tükörtengely.
Ezt a deltoidot *rombusznak* nevezzük.

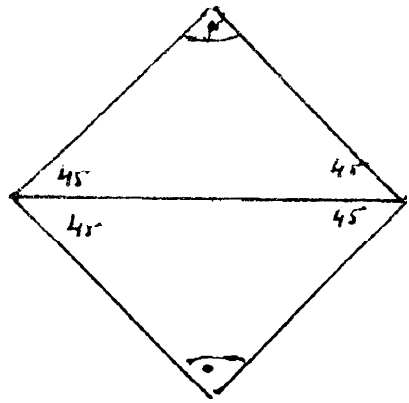
Figyeljük meg! A *BC* alaphoz a *BA* szár és a *CD* szár ugyanolyan szög alatt hajlik, tehát párhuzamosak.
Ellenőrizzük!
Ugyanazért párhuzamos a *CA* és *BD* is.



A rombusz olyan deltoid, amelynek mindkét átlója tükörtengely.
A tükrös háromszög tükrözéséből következtetünk a rombusz tulajdonságaira.
– Oldalai egyenlők.
– Szemközti oldalai párhuzamosak.
– Szemközti szögei egyenlők.
– Átlói felezik a szögeket.

– Átlói merőlegesen felezik egymást.

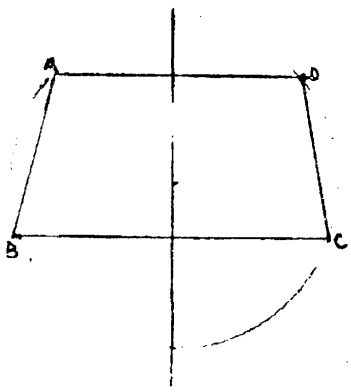
Tükrözzünk egy egyenlő szárú derékszögű háromszöget az átfogójára!
A kapott négyszög átlói itt is szimmetriatengelyek.
A négyszög tehát rombusz.



Vizsgáljuk a szögeit. Ezek derékszögek. *A derékszögű rombusz neve négyzet.* Ellenőrizd az átlók hosszát. Ezek egyenlők. További tulajdonságai megegyeznek a rombusz tulajdonságaival.
Ezután a tükrös négyszögek tulajdonságai alapján szerkesztéseket végezhetünk.

A húrtrapéz

Rajzoljunk egy kört és rajzoljunk bele két húrt, amelyek párhuzamosak. Kössük össze a két húr felezési pontját.



„A kör tükrös alakzat"-nál tanultak alapján mondjunk igaz állításokat a párhuzamos húrok felezési pontjait összekötő egyenesről.

– A párhuzamos húrok felezési pontjait összekötő egyenes átmegy a kör középpontján.

– A párhuzamos húrok felezési pontjait összekötő egyenes az átmérő egyenese.

– A párhuzamos húrok felezési pontjait összekötő egyenesre a kör tükrös.

Próbáljuk bizonyítani, hogy a párhuzamos húrok felezési pontjait összekötő egyenes átmegy a kör középpontján!

Kössük össze a húrok végpontjait! A kapott négyszög két oldala párhuzamos, tehát trapéz. Oldalai egy kör húrjai, így a trapéz neve: *húrtrapéz.* Az eddig megismert tükrös négyszögeknél a tükörtengely a négyszög csúcsain ment át. A húrtrapéznál van olyan tükörtengely, amely nem a csúcsokon meg át.

Húrtrapéz: olyan trapéz, amelynek van nem a csúcsponton átmenő tükörtengelye.

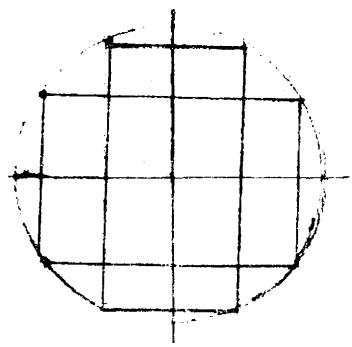
A kör tükrös tulajdonságának segítségével állítsuk össze a húrtrapéz tulajdonságait!

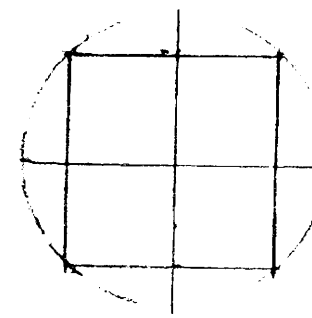
1. Oldalai egy kör húrjai.
2. Szárai egyenlőek.

3. A közös alapon lévő szögek egyenlők.

4. Átlói egyenlők és a tengelyen metszik egymást.

Kísérletezzünk! Rajzoljunk olyan húrtrapézt, amelynél az alapok egyenlő távolságra vannak a körközépponttól! Hány ilyent tudunk egy körben rajzolni? Mivel több ezeknek a tulajdonsága az előző tulajdonságoknál?





A párhuzamos alapok egyenlők. Figyeljük meg a szárakat is! Ellenőrizzük a tapasztalatokat!

Ennél a húrtrapéznál a szemközti oldalak egyenlők és párhuzamosak. Mivel *AB* és *CD* szárak párhuzamos húrok, ezek felezési pontjait összekötő egyenes átmegy a középponton, tehát tükörtengely. Ezek a szárak is lehetnek alapok, így az ezen lévő szögek is egyenlők. Ennek a húrtrapéznak minden szöge egyenlő, egy szöge 90°-os. A húrtrapéz *téglalap.*

A téglalapnak két olyan tükörtengelye van, amely nem megy át a csúcsokon, és felezi az oldalakat.

A téglalapok között lehet olyan, amelynek mind a négy oldala egyenlő.

Az ilyen téglalapot *négyzetnek* nevezzük.

A négyzetnek két csúcsponton átmenő és két nem csúcsponton átmenő, tehát négy tengelye van.
Ezek után szerkesztések végezhetők a húrtrapéz tulajdonságai alapján.

CSERVENYÁK JÁNOS

EGY KÖZÉPISKOLAI GEOMETRIAOKTATÁSI KÍSÉRLETRŐL. IV.

SUMMARY: In this paper we have summarized the syllabus material written for the 4th year of secondary school geometry.

We have demonstrated how it is possible to define the circumference of the convex plane figure, the length of the of the convex arc, the area of the plane figure, the superficies of the convex geometric solid and the volume of the convex geometric solid with the help of limit value.

E dolgozatban annak a geometriai tananyagnak az összefoglalását adjuk meg, amelyet a tanterv a IV. osztály számára írt elő, és szeretnénk azt is megmutatni, milyen módon történt ez a korábban már tanított határérték fogalomra építve.

A tananyag a kerület-, ívhossz-, terület-, a felszín-, a térfogatszámítás.

Ahhoz, hogy a fogalmak mindannyiunk számára ugyanazt jelentsék, összefoglaltuk a *térelemek kölcsönös helyzetéről* szóló ismereteket, értelmeztük azok *távolságát* és *szögét.*

I. Sokszögek, síkidomok

A. Kerület és ívhossz

Mindenekelőtt a *töröttvonalat* értelmeztük, oldalai hosszának összegeként a *töröttvonal hosszát,* s bebizonyítottuk róla, hogy az nem kisebb a kezdő és végpontja összekötő szakaszának hosszánál (teljes indukcióval).

1. *Sokszögnek* neveztük az egyszerű, síkbeli zárt töröttvonalat, amelynek három egymást követő csúcsa nem illeszkedik egy egyenesre.
Értelmeztük a konvex és a konkáv sokszögeket is.
Sokszög kerületén oldalai hosszának összegét értettük. Bebizonyítottuk, hogy konvex sokszög kerülete nagyobb az általa tartalmazott konvex sokszögek kerületénél.
Beláttuk azt is, hogy hasonló sokszögek kerületének aránya a hasonlóság arányával egyenlő.
2. *Síkidomon* a sík véges, nem kolineánis részét értettük, határán pedig síkbeli vonalat, *síkgörbét* értettünk. Miután bebizonyítottuk, hogy konvex síkidom által tartalmazott konvex sokszögek kerületének van felső határa, ezt a *síkidom kerületének* neveztük. Következett az is, hogy minden konvex síkidomnak van kerülete, egybevágó síkidomok kerülete egyen-

lő, végül hasonló síkidomok kerületének aránya a hasonlóság arányával egyenlő.

3. A kör kerületét az előbbi gondolatok alapján adtuk meg. Mivel a kör konvex és mind hasonló, kerületük létezik és kerületük aránya sugaraik arányával egyenlő.

Ha k-val a kerületüket, r-rel a sugarukat jelöljük, akkor

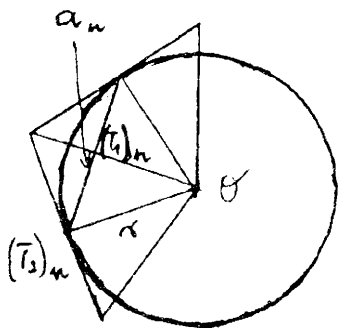
$$k_1 : k_2 : \cdots : k_n = r_1 : r_2 : \cdots r_n = 2r_1 : 2r_2 : \cdots : 2r_n .$$

Tehát a kerület és az átmérő aránya állandó (π):

$$\frac{k_n}{2r_n} = \pi, \text{ így } k = 2r\pi.$$

Az alábbi állítást szükségesnek tartottuk itt belátni, bár később a kör területének meghatározásánál volt rá csak szükség:

a körbe írt és a kör köré írt szabályos sokszögek kerülete a kör kerületéhez tart, ha a sokszög oldalszáma minden határon túl nő.



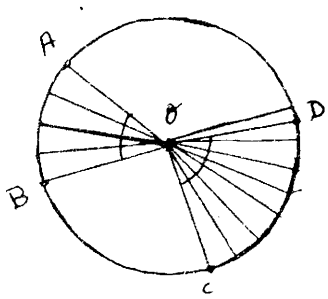
A körbe és köré n oldalú szabályos sokszöget írtunk. A beírt sokszögek kerülete a kör kerületéhez tart.

Ha $\frac{B_n}{K_n} \to 1$-hez, akkor Kn is a kör kerületéhez tart.

Mivel a két sokszög hasonló, ezért a hasonlóság arányával egyenlő a kerületek aránya.

Ezért $\frac{B_n}{K_n} = \frac{O(T_1)_n}{O(T_2)_N}$. Ez utóbbi azért tart az 1-hez, mert $O(T_2)_n = r$ és $O(T_2)_n - O(T_1)_n < (T_1)_n(T_2)_n$, valamint n minden határon túl való növelésével $a_n = 2(T_1)_n(T_2)_n \to 0$, vagyis $r - O(T_1)_n \to 0$, amiből $O(T_1)_n \to r$ adódik.

4. Egy konvex síkgörbét két pontja két konvex ívre bontja. Konvex ív hosszán, a konvex ív és a két végpont szakasza által meghatározott konvex síkidom kerületének és a két végpont szakasza hosszának különbségét értettük. Beláttuk, hogy ha egy konvex ívet bármely belső pontja két részre bont, a részek hosszának összege az eredeti ív hosszával egyenlő. Beláttuk, hogy egybevágó ívek hossza egyenlő, hasonlók hosszának aránya egyenlő a hasonlóság arányával.
5. Bebizonyítottuk, hogy egy kör ívei hosszának aránya egyenlő a hozzájuk tartozó középponti szögek arányával. (A területnél a térfogatnál a hasonló bizonyításoktól eltekintünk).



Osszuk fel az AOB szöget $n=2^m$ egyenlő részre, a kapott szöget mérjük fel az OC szártól a COD szögre ahányszor tudjuk.
Tegyük fel, hogy k-szor még ráfér, de $k+1$-szer már nem.
Ekkor

$$k\cdot\frac{AOB\sphericalangle}{n}\le COD\sphericalangle<(k+1)\cdot\frac{AOB\sphericalangle}{n}$$

Az I. osztályban bizonyítottuk, hogy egyenlő középponti szögekhez egybevágó (egyenlő) ívek tartoznak, így

$$k\cdot\frac{\overset{\frown}{AB}}{n}\le\overset{\frown}{CD}<(k+1)\cdot\frac{\overset{\frown}{AB}}{n}.$$

Osztások után

$$\frac{k}{n}\le\frac{COD\sphericalangle}{AOB\sphericalangle}<\frac{k+1}{n}\text{ és }\frac{k}{n}\le\frac{\overset{\frown}{CD}}{\overset{\frown}{AB}}<\frac{k+1}{n}$$

adódik.

Képezve az alábbi különbség abszolút értékét,

$$\left|\frac{COD}{AOB}-\frac{\overset{\frown}{CD}}{AB}\right|<\frac{1}{n},$$

mivel e két hányados a $\left[\frac{k}{n};\frac{k+1}{n}\right)$ balról zárt jobbról nyitott intervallumban van.

Mivel $\lim_{n\to\infty} \frac{1}{n} = 0$, azért ez csak úgy állhat fenn minden n-re, ha

$$\frac{COD\sphericalangle}{AOB\sphericalangle} = \frac{\overset{\frown}{CD}}{\overset{\frown}{AB}}.$$

Így ha α szöghöz i hosszúságú ív tartozik, akkor

$$i:2r\pi = \alpha:2\pi, \text{ amiből } i = r \cdot \alpha.$$

B. Terület

1. Bizonyítás nélkül elfogadtuk azt az állítást, hogy minden sokszöghöz hozzárendelhető egy pozitív valós szám, amelyet a *sokszög területének* nevezünk és amelyre fennáll az alábbi három tulajdonság:
   a) az egységnyi oldalhosszúságú négyzet területe 1;
   b) egybevágó sokszögek területe egyenlő;
   c) ha egy sokszöget két részsokszöggé bontunk, akkor a részek területének összege az eredeti sokszög területével egyenlő.

Ezen állításból két újabb következik:

egyrészt, ha egy sokszög tartalmaz egy másik sokszöget, akkor területe a tartalmazott területénél nagyobb, másrészt ha egy sokszöget véges részsokszögre bontunk a részsokszögek területének összege az eredeti sokszög területével egyenlő. (A bizonyítás gondolatmenetét persze röviden ismertettük, amiből kiderült, hogy sokszög területe azon háromszöget területének összege, amelyekre az valamilyen módon felbontható, s a háromszöghöz területként a háromszög

valamely oldalának és hozzátartozó magassága szorzatának felét rendeltük, ami egy háromszögre állandó.)

A terület egyértelműségét úgy láttuk be, hogy feltettük: létezik olyan terület (függvény) amely az előbbitől különbözik, de a három tulajdonságot teljesíti.

Belátható volt, hogy ha két téglalap egy-egy oldala egyenlő, akkor területük aránya a hozzájuk csatlakozó oldalaik arányával egyenlő. Ebből aztán beláttuk, hogy a téglalap területe két szomszédos oldalának szorzatával egyenlő. Azt is beláttuk, hogy ezen ismeretek birtokában a háromszög területére valamelyik oldala és hozzátartozó magassága szorzatának fele adódik. Így tehát minden sokszögnek van egyértelműen meghatározott területe.

Ezek után a trapéz területe: $\frac{a+c}{2} \cdot m$,

a paralelogrammáé: $a \cdot m_a$,

a deltoidé: $\frac{1}{2} e \cdot f$,

az érintősokszögé: $\frac{1}{2} k \cdot r$

ebből a háromszögé: $g \cdot s$, ahol a betűk az irodalmakban megszokott mennyiségeket jelölik. Persze teljességről itt szó sincs.

2. Mivel a síkidomok korlátos ponthalmazok, ezért vannak olyan sokszögek, amelyek a síkidomot tartalmazzák, és vannak olyan sokszögek, amelyeket a síkidom tartalmaz.

Értelmezés: Ha a síkidomot tartalmazó sokszöget területének alsó határa egyenlő a síkidom által tartalmazott sokszögek területének felső határával, akkor ezt a számot a *síkidom területének* nevezzük.

Megfogalmaztuk, hogy ha egy síkidomnak van területe, az analízis nyelvén azt jelenti, hogy létezik olyan külső (K) és olyan belső (B) sokszög, amelyekre bármilyen kicsiny $\varepsilon > 0$ esetén $t(K) - t(B) < \varepsilon$,

$$\frac{t(K)}{t(B)} < 1 + \varepsilon \text{ vagy } \frac{t(B)}{t(K)} > 1 - \varepsilon \text{ áll fenn.}$$

Beláttuk, hogy ha egybevágó síkidomok közül valamelyiknek van területe, akkor a többinek is van, s a területük egyenlő. Bizonyítás nélkül elfogadtuk, hogy ha egy síkidomot két olyan síkidomra bontunk, amelyeknek van területük, akkor van területe az eredeti síkidomnak, amelynek területe a két részsíkidom területének összegével egyenlő. Ugyanígy elfogadtuk, hogy ha egy síkidomnak és egy részének van területe, akkor van terület a másik részének is és területe, az eredeti területének és a részsíkidom területének különbségével egyenlő.

Ezek segítségével a kör területe: $r^2\pi$

(a kiszámításnál az érintősokszög kerületét használtuk fel),

a körcikké: $\frac{ri}{2}$,

a körgyűrűé: $2g\pi d$,

a körszeleté: $\frac{ri}{2} - \frac{1}{2}r^2 \sin\alpha$.

Mivel a hasonló háromszögek területének aránya a hasonlóság arányának négyzetével egyenlő, ezért az értelmezések alapján a hasonló síkidomok területének arányára is a hasonlóság arányának négyzete áll fenn.

II. Poliéderek, mértani testek

A. Poliéderek

Az olyan térrészt, amelyet véges számú sokszög határol és nem tartalmaz félegyenest, *poliédernek* nevezzük.

Néhány speciális poliéderrel foglalkoztunk. Először a *hasábfelülettel*, majd a hasábbal, köztük a *paralelepipedonnal*, a *téglatesttel*, *kockával* foglalkoztunk.

Másodszor a *gúlafelülettel*, majd a *gúlával*, és a *csonka gúlával*. A feladatok megoldásához pedig néhány sajátos síkmetszetet vizsgáltunk.

B. Mértani testek

A tér tetszőleges, nem komplanáris korlátos ponthalmazát *mértani testnek* nevezzük (ilyenek a poliéderek is).

Itt is előbb a *hengerfelületet*, a *hengert*, továbbá a *kúpfelületet*, a kúpot és a csonka kúpot értelmeztük, vizsgáltuk sajátos síkmetszeteiket is.

A gömböt mint a tér adott pontjától adott távolságra lévő pontjainak halmazát értelmeztük. Értelmeztük a *forgástes-*

ket is és az *egyenes körhengert*, az *egyenes körkúpot*, az *egyenes csonka körkúpot*, valamint a gömböt *forgástestekként* is értelmeztük.

C. Felszínszámítás

1. Poliéder *felszínén* a határoló sokszögek területének összegét értjük.

Így az egyes hasáb felszíne: $F = 2T + km$, ahol T a hasáb alaplapjának területe, k a kerülete, m pedig a hasáb magassága.

A szabályos sokszögalapú egyenes csonka gúla felszíne

$$F = T + t + \frac{k + K}{2} m_t,$$

ahol az m_t az oldallap (trapézok) magassága.

A szabályos sokszögalapú egyenes csonka gúla felszíne

$$F = T + t + \frac{k + K}{2} m_t,$$

ahol az m_t az oldallap (trapézlapok) magassága.

2. Konvex mértani test felszínén a testbe írt konvex poliéderek felszínének felső határát értjük.

A fenti összefüggések az alábbi határok meghatározásához kellenek. Az r sugarú, m magasságú egyenes körhenger térfogata a beleírt n oldalú szabályos sokszög alapú egyenes hasábok $F_n = 2t_n + k_n \cdot m$ felszínének felső határa:

$$F = 2r^2\pi + 2r\pi \cdot m.$$

Az r sugarú, o alkotójú egyenes körkúp térfogata a beleírt n oldalú szabályos sokszögalapú egyenes gúlák

$$F_n = t_n + \frac{1}{2} k_n \pi \cdot o_n \text{ f}$$

elszínének felső határa

$$F = r^2\pi + r\pi + r\pi \cdot o.$$

Az egyenes csonka kúp felszíne a beleírt n oldalú szabályos sokszög alapú csonka gúlák

$$F_n = T_n + t_n + \frac{k_n + K_n}{2} m_{tr}$$

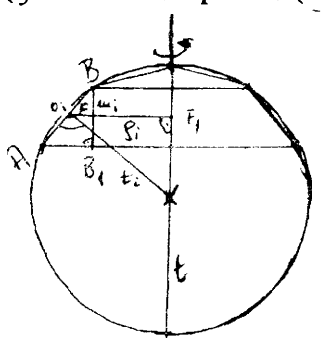
felszínének felső határa

$$F = R^2\pi + r^2\pi + (r+R)\pi \cdot o.$$

A gömb felszínének meghatározásához felhasználjuk a csonka kúp palástjának felszínét, ami

$$P = (r+R)\pi o = 2\varsigma\pi d, \text{ ahol } \varsigma = \frac{r+R}{2},$$

(ς a kiterített palást (körgyűrűcikk) középívének sugara).



Így az r sugarú gömb felszíne $F = 4r^2\pi$. Tekintsünk ugyanis az r sugarú kört és egy abba írt páros ($n = 2k$) oldalszámú szabályos sokszöget. Válasszuk ki valamely átellenes csúcspont párjának összekötő egyenesét és forgassuk meg t körül a kört és a sokszöget. A körből gömb, a sokszögből k darab csonkakúppalást (2 speciális) alakul ki.

Az $OFF_{1\Delta} \sim ABB_{1\Delta}$-höz két-két szög egyenlősége miatt. Így az i -edik palástfelszín $P_i = 2\varsigma_i \pi o_i$, az előbbi Δ-ek hasonlósága miatt ($\varsigma_i \cdot t_i = m_i : o_i$) $P_i = 2t_i \pi m_i$ alakot veszi fel.

Összegezve a palástfelszíneket,

$$P = P_1 + P_2 + \cdots\cdots + P_n$$

$$P = 2t_i\ \pi(m_1 + m_3 + \cdots\cdots + m_k) = 2t_i\ \pi 2r.$$

Ennek felső határa $n \to \infty$ esetén a gömb felszíne $F = 4r^2\pi$, hiszen $t_i \to r$.

D. Térfogatszámítás

Egy nem bizonyított tétellel kezdtük.

1. Minden poliéderhez hozzárendelhető egy pozitív valós szám, amit a poliéder térfogatának nevezünk, és ami rendelkezik az alábbi tulajdonságokkal.
   a) az egységnyi élhosszúságú kocka térfogata 1,
   b) egybevágó poliéderek térfogata egyenlő,
   c) ha egy poliédert két poliéderre bontunk, akkor a részek térfogatának összege egyenlő az eredeti poliéder térfogatával.

E tételből következik, hogy ha egy poliéder egy másik poliédert tartalmaz, akkor a térfogata nagyobb a tartalmazott poliéder térfogatánál, s az is, hogy ha egy poliédert véges sok részre osztunk, akkor a részek térfogatának összege az eredeti poliéder térfogatával egyenlő.

Persze ezek alapján hozzá is fogtunk néhány poliéder térfogatának meghatározásához.

Előbb beláttuk, hogy ha két téglatest alaplapja egybevágó, akkor térfogatuk aránya magasságuk arányával egyenlő.

A téglatest térfogatát a három egy csúcsból kiinduló élének szorzataként kaptuk. Ezután a háromszögalapú, majd a sokszögalapú egyenes hasáb térfogatát határoztuk meg. A ferde hasáb térfogata – egy az oldaléleire merőleges síkmetszet és az alaplap területe közötti $T' = T_o \cos\alpha$ kapcsolat felismerésével – mint előbb az alapterület és a magasság szorzata lett.

A gúla térfogatának felhasználásával, s a hasáb három egyenlő térfogatú háromszög alapú gúlára való bontásával a háromszög alapú gúla térfogata az alapterület és a magasság szorzatának harmadaként adódott.

A csonka gúla térfogatát egy azt gúlává egészítő újabb gúla segítségével nyertük: $V = \frac{m}{3}(T + \sqrt{Tt} + t)$ alakban.

2. A mértani testhez – annak korlátossága miatt – találhatók azt tartalmazó, és általa tartalmazott poliéderek. Ezeket külső, illetve belső poliédereknek nevezzük. Eddigi eredményeink alapján az előbbiek térfogata alulról, az utóbbiak térfogata felülről korlátos számhalmazt alkot. (Létezik alsó, illetve felső határ.)

   Ha egy mértani testet tartalmazó poliéderek térfogatának alsó határa egyenlő a mértani test által tartalmazott poliéderek térfogatának felső határával, akkor ezt a közös *határt a mértani test térfogatának* neveztük. Bár a mértani testek térfogatára is fenn állnak a poliéder térfogatára ki-

mondott tétel állításai, ezekkel nem foglalkozhattunk, segítségükkel néhány speciális mértani test térfogatának meghatározására szorítkozunk.

Az egyenes körhenger térfogata $V = r^2 \cdot \pi \cdot m$.
Írtunk a körhengerbe és köré n oldalú szabályos húrsokszög alapú hasábokat.
A beírt hasábok térfogata: $V_{bn} = t_{bn} \cdot m$,
a körülírtaké: $V_{kn} = t_{kn} \cdot m$,.
Mivel $t_{bn} \to r^2 \cdot \pi$ és $t_{bn} \to r^2 \cdot \pi$, ha $n \to \infty$, így $V_{bn} \to r^2 \cdot \pi \cdot m$ és $V_{kn} \to r^2 \cdot \pi \cdot m$, van közös határ, vagyis a henger térfogata $V = r^2 \cdot \pi \cdot m$.
Hasonló módon bizonyítottuk be, hogy az egyenes körkúp térfogata:

$$V = \frac{1}{3} \cdot r^2 \cdot \pi \cdot m,$$

míg az egyenes csonka körkúp térfogata:

$$V = \frac{m\pi}{3} \cdot (R^2 + R \cdot r + r^2).$$

A gömb térfogatát a nem bizonyított ún. Cavalieri-elv segítségével határoztuk meg. Mivel egy r sugarú félgömb és egy r sugarú és r magasságú egyenes körhengerből kivett r sugarú r magasságú körkúp után visszamaradó test teljesíti a Cavalieri elvben felsorolt feltételeket, az utóbbi $V = \frac{2}{3} \cdot r^3 \cdot \pi \cdot m$, térfogata a félgömb térfogatával egyenlő, s a gömb térfogata $V = \frac{4}{3} \cdot r^3 \pi$.

Integrálszámítással a forgástestek térfogatát is megadtuk. A konvex síkidomok kerületének — köztük a kör kerületének —, a konvex ív hosszának, köztük a körív hosszának —, a síkidom területének, a konvex mértani test felszínének és a mértani test térfogatának, az alulról, illetve felülről korlátos számhalmazok tulajdonságainak, valamint a számszorzat határértéke fogalmának felhasználásával való definiálása a közepes vagy annál jobb tanulók esetében nagyon sokat adott.
Eddig ezekről csak képletek formájában volt fogalmuk, most már némi tapasztalat és absztrakció segítségével a valóságot jobban leíró fogalmak alakultak ki a fent említettekről.

Itt persze e dolgozatban csak egy angol tagozatos osztálynak tanított geometriai tananyag vázlatát közöltem az eddig megszokottól eltérő módon.
A kísérletet sikeresnek ítélem, hiszen a gyengébbek is tudták követni úgy az anyagot, ahogyan más osztályok az ott tanítottakat. Viszont a továbbtanulók (azóta történt visszajelzésekre is alapozva) annyi többletet kaptak, amennyi könnyen segítette át őket a középiskola és a felsőoktatás matematika oktatásának feltűnő szintkülönbségén.

SASHALMINÉ KELEMEN ÉVA

A FŐISKOLAI GEOMETRIA ANYAG EGY LEHETSÉGES MEGALAPOZÁSA

II. RÉSZ

ABSTRACT: This paper continues the theme that was published in the latest issue of Acta Academiae Paedagogicae Agriensis (Vol. XX. 1991) It contains the statements that can be deduced from the axioms of the distance and symmetry, and the initiation and marka of the axial symmetry. The marks of central symmetry and the other coincidental transformations on plane will be found in the next part.

Ez a cikk az előző kötetben (Acta Academiae Paedagogicae Agriensis tom. XX.) megjelent anyag folytatása. Tartalmazza a távolság és a szimmetria (X, XI) axiómáiból levezehető állításokat; a tengelyes tükrözés bevezetését, jellemzőit. A centrális tükrözés tulajdonságai és a többi síkbeli egybevágósági transzformáció a következő részben lesz megtalálható.

4. Távolság, egybevágóság

A továbbiakban felhasználjuk a valós számok tulajdonságait. A következő axióma bevezetése után már metrikus geometriával foglalkozunk, bevezetjük ugyanis a mérték, a távolság fogalmát.

X. **Axióma:** Az $\mathcal{E}$ térhez hozzárendeljük a tér pontpárjai halmazának, $(\mathcal{E} \times \mathcal{E})$ -nek a nem negatív valós számok halmazára történő d leképezését, melyet *távolság függvénynek* nevezünk, s melyre a következők teljesülnek:

1. $d(A,B)=d(B,A)$ minden $A,B \in \mathcal{E}$ -re.
2. Tetszőleges irányított e egyenes, rá illeszkedő tetszőleges A pont és tetszőleges $c \geq 0$ valós szám estén az e egyenesen egyetlen olyan B pont létezik, amelyre $A \leq B$ és $d(A,B) = c$.
3. Ha $P \in [A,B]$, akkor $d(A,P) + d(P,B) = d(A,B)$.
4. Legyen A,P,B tetszőleges, nem egy egyenesre illeszkedő ponthármas: ezekre teljesül:
$$d(A,B) < d(A,P) + d(P,B).$$

4.1. **Értelmezés:** Két, tetszőleges A,B *pont távolságán* a $d(A,B)$-t értjük.

4.1. **Következmény:**

$(d(P,Q) = 0) \leftrightarrow (P = Q)$

A X.3. alapján, (ha $A = P, Q = B$)

$d(P,P) + d(P,Q) = d(P,Q)$, amelyből következik, hogy $d(P,P) = 0$.

Ha $P \neq Q$, akkor tegyük fel, hogy $P < Q$. A $P \leq P < Q$ viszonyból következik, hogy $d(P,Q) \neq 0$.
A $d(P,P) = d(P,Q) = 0$ teljesülése ellentmondásban lenne a X.2-vel.)

4.2. **Következmény:**

1. $(P \in [A,B]) \rightarrow (d(A,P) \leq d(A,B))$
   egyenlőség csak akkor állhat fenn, ha $P = B$.
2. Az e egyenes minden P,Q,R pontjára teljesül a
   $d(P,R) \leq d(P,Q) + (Q,R)$.
3. Az $\mathcal{L}$ sík tetszőleges, P,Q,R három pontjára:
   $d(P,R) \leq d(P,Q) + d(Q,R)$.

4.1. **Tétel:** Legyen e tetszőleges irányított egyenes és A ezen egyenes tetszőleges pontja. Az e egyenesnek pontosan egy olyan, a valós számok halmazára történő, növekvő, f leképezése létezik, amelyre igaz, hogy $f(A) = 0$, és $d(P,Q) = |f(Q) - f(P)|$ minden $P,Q \in e$-re. Ez a leképezés az e halmaz **R**-re történő kölcsönösen egyértelmű leképezése.

Bizonyítás: Az első részben megkonstruáljuk a f függvényt, a második részben igazoljuk, hogy rendelkezik a kívánt tulajdonságokkal.

1. Az f leképezésre adott feltételekből következik, hogy $d(P,A) = |f(P)|$ ($Q = A$-t tekintve). Ebből, mivel f növekvő kell legyen és $f(A) = 0$, adódik, hogy

ha $A < P$, akkor $f(P) = d(A,P)$
ha $P < A$, akkor $f(P) = -d(A,P)$.

2. Megmutatjuk, hogy ezen két egyenlőséggel adott f kielégíti a tétel feltételeit.

A X. axióma alapján:

$(P \leq A \leq Q) \rightarrow (d(P,Q) = d(P,A) + d(A,Q))$, azaz

$d(P,Q) = -f(P) + f(Q)$,

$(A \leq P \leq Q) \rightarrow (d(A,Q) = d(A,P) + d(P,Q))$, azaz

$f(Q) = f(P) + d(P,Q)$

$(P \leq Q \leq A) \rightarrow (d(P,A) = d(P,Q) + d(Q,A))$, azaz

$-f(P) = d(P,Q) - f(Q)$.

Minden olyan P,Q-ra, amelyekre $P \leq Q$, mindhárom esetben $d(P,Q) = f(Q) - f(P)$ teljesül.

Mivel $d(P,Q) \geq 0$, ebből következik, hogy $f(P) \leq f(Q)$, azaz az f leképezés növekvő. $d(P,Q) = |f(Q) - f(P)|$ is teljesül.

Kölcsönösen egyértelmű is, hiszen

$(P < Q) \rightarrow (f(Q) - f(P) = d(P,Q) \neq 0)$, azaz különböző pontok képei különbözőek. A X.2. alapján minden $c \geq 0$ esetén $(c \in R)$ létezik, olyan P,Q, hogy

$A \leq P$ és $d(A,P) = c$, ahonnan $f(P) = c$,

$Q \leq A$ és $d(Q,A) = c$, ahonnan $f(Q) = c$;

ami azt jelenti, hogy az f leképezésnél **R** minden eleme valamely e-n levő pont képe.

4.3. **Következmény**: Az előző tételből következik, hogy minden olyan egyenest, amelyen van egy kitüntetett pont, (O) az **R** halmazzal lehet azonosítani, s alkalmazni lehet rajta az **R** test tulajdonságait.

4.2. **Értelmezés:** Legyen e tetszőleges irányított egyenes, O ennek kitüntetett pontja, s f ezen egyenes fentebb leírt leképezése R-re. Az $f(P)$-t ebben az (e,O) rendszerben a P pont ***abszcisszájának*** nevezzük. Jelentése $d(O,P)$-vel vagy $-d(O,P)$-vel egyenlő, attól függően, hogy $O < P$ vagy $P < O$.
(A korábban bevezetett φ_1(P), φ_2(P) pontok abszcisszáit (az (O,e_1), (O,e_2) rendszerben) most már nevezhetjük a P pont koordinátáinak).

4.3. **Értelmezés:** A tetszőleges A,B pontpár által meghatározott **szakasz felezési pont**jának nevezzük az $[A,B]$ azon F pontját, amelyre $d(A,B) = d(F,B)$.

4.4. **Következmény:** Mivel $d = (A,B) = d(A,F) + d(F,B)$, így $d(A,B) = 2d(A,F) = 2d(F,B)$.

4.4. **Értelmezés:** Legyen φ az $\mathcal{E}$ tér olyan önmagára történő leképezése, amelyre teljesül, hogy bármely két térbeli pont távolsága egyenlő a képpontok távolságával, azaz

$$d(A,B)=d(\varphi(A),\varphi(B)) \quad /A,B\in\mathcal{E}/$$

Az φ leképezést **egybevágóságnak** (izometriának) nevezzük.

4.5. **Következmény:**
Tulajdonságok:
1. Az egybevágóság geometriai transzformáció.
Egyértelmű leképezés: ha egy A pontnak A' és A'' is képe lenne, akkor $d(A,A) = 0$ és $d(A'A'') \neq 0$ is telje-

sülne, ami nem lehetséges. Különböző pontok képei is különbözőek (távolságuk nem lehet 0).

2. Két egybevágóság szorzata is egybevágóság.
   Ha A,B képe az φ_1 leképezésnél A', B'; A', B' képe az φ_2-nél A'', B'', akkor $d(A,B) = d(A',B') = d(A'',B'')$. A valós számok tulajdonságai miatt $d(A,B) = d(A'',B'')$, így $\varphi_2 \circ \varphi_1$ is egybevágóság.
3. Az egybevágóság egyenestartó leképezés.
   Legyen A,B,C kollineáris ponthármas, s képük A',B',C'.
   (1) $d(A,B) = d(A',B')$, $d(B,C) = d(B',C')$,
   $d(A,C) = d(A',C')$.
   Teljesüljön $A < B < C$, ekkor a X.3. axióma miatt
   (2) $d(A,C) = d(A,B) + d(B,C)$.
   Ha az A',B',C' nem kollineáris:
   $d(A',C') < d(A',B') + d(B',C')$.
   Az (1) miatt $d(A,C) < d(A,B) + d(B,C)$ ami ellentmond a (2)-nek.
   Hasonlóan belátható, hogy nem kollineáris pontokat nem vihet át kollineáris pontokba.
4. Az egybevágóság az egyenesen a pontok elrendezését megtartja. Ha $A < B < C$ akkor $A' < B' < C''$ vagy $A' > B' > C'$.
   Nem lehet pl. az $A' < B' < C'$, hiszen ekkor $d(A',C') < d(A',B') + d(B'C')$, ami ellentmond a (2)-nek.

Ha B elválasztotta A-t és C-t, akkor B' is elválasztja A'-t és C'-t. A képekre teljesülhet az eredeti $A' < B' < C'$, vagy az ellentétes $A' > B' > C'$.

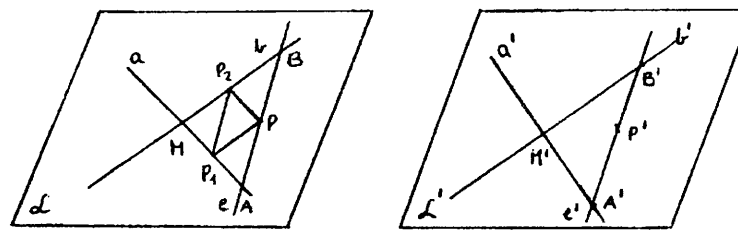
5. Az előző állítás alapján az egybevágóság félegyenest félegyenesbe visz át. Szakasz képe szakasz.

4.2. **Tétel.** Az egybevágóság két metsző egyenest metsző egyenespárba visz át úgy, hogy az egyenesek metszéspontjának képe a képegyenesek metszéspontja.

Bizonyítás: Legyen $\mathcal{L}$ tetszőleges sík; ennek tetszőleges M pontjára illeszkedik két olyan a,b síkbeli egyenes, amelynek metszéspontja M. Először azt igazoljuk, hogy az a,b egyenesek a',b' képe is metsző egyenespár, s M képe a képegyenesek M' metszéspontja. Mivel az M pont illeszkedik az a és b egyenesre is, képe, M' az egyenestartás miatt illeszkedni fog az a',b' képegyenesekre is, Mivel $a \neq b$, $a' = b'$ sem lehetséges, így M' az a',b' egyenesek metszéspontja.

4.3. **Tétel:** Az egybevágóság síktartó leképezés.

Bizonyítás: Be kell látni, hogy tetszőleges $P \in \mathcal{L}$ esetén $P' \in \mathcal{L}'$, ahol $\mathcal{L}'$ az a',b' egyenesek által meghatározott sík. (2. ábra)



2. ábra

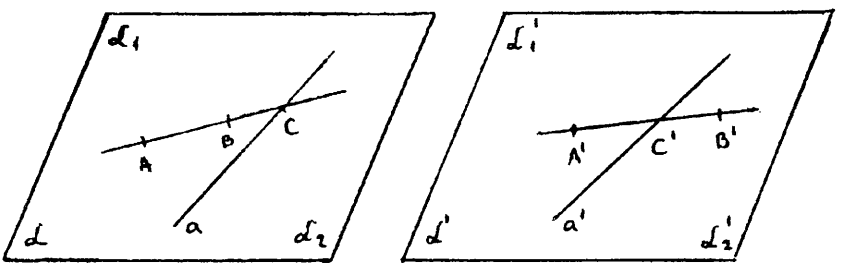
Ha $P \in \{a \cup b\}$, akkor az állítás nyilvánvaló.

Legyen $P \notin \{a \cup b\}$. Tekintsük P pontnak az a,b tengelyrendszerre vonatkozó P_1, P_2 meghatározó pontjait. A feltétel miatt $P \notin \overline{P_1, P_2}$.

Illesszünk P-re $\overline{P_1, P_2}$-vel párhuzamos e egyenest. Az 1.4. következmény miatt létezik $e \cap a = A$ és $e \cap b = B$. Az A' és B' képpontok illeszkednek az a', b' egyenesekre, így az $\mathcal{L}'$-re is. A IV. axióma alapján $\overline{A'B'} \subset \mathcal{L}'$, s az egyenestartás miatt $P' \in \overline{A'B'}$, azaz $P' \in \mathcal{L}'$.

4.6. **Következmény:** Az egybevágóság két párhuzamos egyenest két párhuzamos egyenesbe visz át.
Síkjuk képe sík, a képeknek közös pontja nem lehet.

4.7. **Következmény:** Az egybevágóság félsíkot félsíkba, félteret féltérbe visz át.
Tegyük föl, hogy az $\mathcal{L}$-ra illeszkedő a egyenes által meghatározott $\mathcal{L}_1$ félsíkbeli A,B pontokat az a' által meghatározott különböző félsíkbeli pontokba viszi át. (3. ábra)



3. ábra

Legyen $\overline{A,B} \cap a = C$. (Ha $\overline{A,B}$ egyállású a-val, akkor $\overline{A',B'}$ is egyállású a'-vel, s ekkor a következmény állítása teljesül.) Az $[A,B]$-nek ekkor a C nem belső pontja, míg az $\overline{A',B'} \cap a' = C'$ pont a 3.1. tétel miatt az $[A',B']$ belső pontja. A rendezéstartás miatt ez nem lehetséges.
A félterekre vonatkozó állítás hasonlóan igazolható.

4.8. **Következmény:** A tér önmagára történő egybevágóságainak összessége csoportot alkot.
– Két egybevágóság szorzata is egybevágóság. (4.5.2. következmény)
– Egybevágóságok szorzása asszociatív.
– Létezik neutrális elem: az identikus egybevágóság.
– Minden egybevágóságnak van inverze és az is egybevágóság.
(4.5.1. következmény).

5. Szimmetria

XI. Axióma:

Tetszőleges γ sík esetén egy és csak egy olyan egybevágóság létezik, amely az γ által meghatározott zárt féltereket egymásnak felelteti meg, s melynél teljesül, hogy a γ sík pontjai fixpontok.

5.1. **Értelmezés:** A XI. axiómában leírt leképzést γ **sík szerinti szimmetriá**nak vagy γ **síkra vonatkozó tükrözés**nek nevezzük. A γ **szimmetriasík** vagy **tükörsík.**

A leképezés jele S_γ vagy T_γ.

5.1. **Következmény:** A XI. axiómából a síkszimmetria több tulajdonsága közvetlenül adódik.

1. Egybevágóság, így teljesülnek rá annak tulajdonságai: egyenestartó, síktartó, rendezéstartó; párhuzamos, illetve metsző egyenespár képe szintén párhuzamos, illetve metsző egyenespár.
2. Csak a szimmetriasík pontjai fixpontok.
   Ha $T_\gamma(A)=A'$ és $A=A'$, akkor $A\in\gamma$, mert mindkét féltérhez csak a γ pontjai tartoznak.
3. Ha egy A pont képe A', akkor az A' képe az A pont.
   $A\in\gamma$ esetén triviális, így a továbbiakban $A\notin\gamma$.
   Legyen A' képe $\overline{A}\neq A$ pont. A és $\overline{A}$ ugyanazon γ határsíkú féltérben van, s az $[A,A']$ képe az $[A',\overline{A}]$. Létezik $[A,A']\cap\gamma=F$, ami fixpont, s így illeszkedik $[A,A']$ képére is, azaz $F\in[A',\overline{A}]$. $\overline{A'F}$-re illeszkedik az A és $\overline{A}$ is, s mivel $d(A,A')=(A'\overline{A})$, a X. axióma alapján $A=\overline{A}$.

4. Ha az A pont nem illeszkedik a γ szimmetriasíkra, és képe A', akkor az $\overline{A,A'}$ képe önmaga, de nem pontonként fix. $\overline{A,A'}$ a tükrözés invariáns egyenese. A IX. axióma miatt létezik $\overline{A,A'} \cap \gamma = F$. $d(A,F) = d(A',F')$, s így F az $[A,A']$ felezési pontja.
5. $T_\gamma \circ T_\gamma = \mathrm{I}$. A T_γ involutórikus leképezés.

5.2. **Értelmezés:** A T_γ által egymáshoz rendelt pontokat (A,A'), **tükörképek**nek nevezzük.

5.2. **Következmény:** Ha egy g egyenes és g' képe egy G pontban metszi egymást, akkor G illeszkedik a szimmetriasíkra. A g,g' metsző egyenespár képe a g', g metsző egyenespár, s a G metszéspont G' képe a képegyenesek metszéspontja, azaz $G=G'$, s így $G \in \gamma$.

5.1. **Tétel:** Ha $T_\gamma(A)=A'$, és $A \notin \gamma$, akkor a γ sík minden pontja egyenlő távolságra van A és A'-től, s a tér minden olyan pontja, amely A és A'-től egyenlő távolságra van, a γ síkra illeszkedik.

Bizonyítás: 1.) Legyen tetszőleges $P \in \gamma$.

$$d(A,P) = d(A',P') = d(A',P)$$

2. Legyen $Q \in \mathcal{E}$ és $d(A,Q) = d(A',Q)$, valamint $Q \notin \gamma$. Legyen Q a γ által meghatározott azon féltérben, mint az A'. Ekkor a IX. és XI. axióma miatt létezik $\overline{A,Q} \cap \gamma = B$. A bizonyítás első része miatt $d(A,B) = d(A',B)$; mivel az $\overline{A,A'}$-n csak az $[A,A']$ γ-ra illeszkedő F felezési pontjára teljesül a $d(A,F) = d(A',F')$, így $Q \notin \overline{A,A'}$.

A X. axióma alapján:

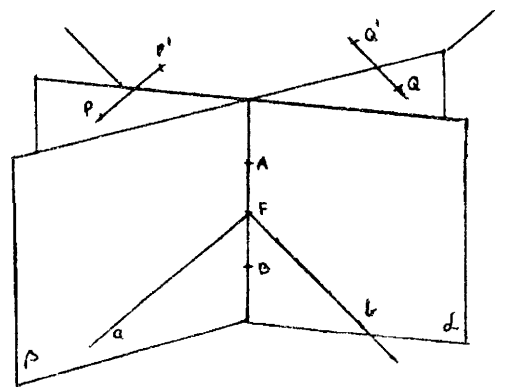
$$d(Q,A') < d(A',B) + d(B,Q).$$

Mivel $d(A',B)+d(B,Q)=d(A,B)+d(B,Q)=d(A,Q)$,

a $d(Q,A')<d(A,Q)$ ellentmond a feltételnek, így $Q\in\gamma$

5.2. **Tétel:** A tér bármely két különböző pontjához egy és csak egy szimmetriasík tartozik.

1. **A létezés bizonyítása:** Konstruktív. Legyen a két tetszőleges pont A és B. Tekintsünk egy tetszőleges, $\overline{A,B}$-re illeszkedő $\mathcal{L}$ síkot. (4. ábra)



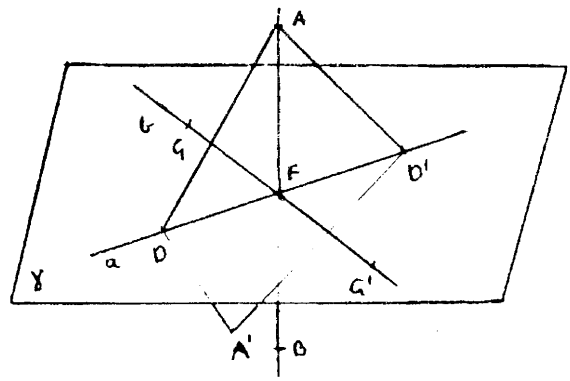
4. ábra

A XI. axióma alapján ez a sík meghatároz egy $\mathcal{L}$ szerinti szimmetriát; legyen egy megfelelő pontpár P,P', amelyekre $P\neq P'$. Az 1.3. következmény alapján az $[A,B]$ F felezési pontjára egy és csak egy $\overline{P,P'}$-vel párhuzamos a egyenes illeszkedik. (Ha $F\in\overline{P,P'}$, akkor $\overline{P,P'}=a$).

Párhuzamos egyenesek képei párhuzamosak, s mivel $\overline{P,P'}$ invariáns, $\overline{P,P'}\|a'$, ahol $T_{\mathcal{L}}(a)=a'$. F fixpont, $F\in a'$, de mivel F-re csak egy $\overline{PP'}$-vel párhuzamos egyenes illeszt-

hető, $a=a'$. Egy ℓ-tól különböző, az $\overline{A,B}$-t tartalmazó β síkot tekintve, hasonlóan az a-hoz, konstruálható egy olyan b egyenes, melyre teljesül, hogy $F \in b$ és $T_\beta(b)=b$.

Azt fogjuk bizonyítani, hogy az a,b metsző egyenesek által meghatározott γ sík a keresett tükörsík, azaz $T_\gamma(A)=B$. Tegyük fel, hogy $T_\gamma(A)=A'$ és $A' \notin \overline{A,B}$. (5. ábra)



5. ábra

Legyen $D \in a$, $D \neq F$ és $T_\ell(D)=D'$, mivel $\overline{A,B} \subset \ell$, így $d(A,D)=d(A,D')$.

A $\overline{D,D} \subset \gamma$, így az előzőek alapján $d(A,D)=d(A',D)$ és $d(A,D')=d(D'A')$.

Ezekből adódik, hogy $d(A',D')=s(A',D)$ ami azt jelenti az előző tétel miatt, hogy $A' \in \ell$.

Felvéve b egyenesen a G,G' $(G \neq F)$ β-ra szimmetrikus pontpárt, hasonlóan kimutatható, hogy

$d(A',G') = d(A',G)$, ami azt jelenti, hogy $A' \in \beta$.
Így $A' \in (\ell \cap \beta) = \overline{A,B}$.
$d(A,F) = d(F,B) = d(F,A')$; a X. axióma miatt $A' = B$.
Így az A-nak γ-ra való tükörképe B.

2. **Az egyértelműség bizonyítása:**
Ha $T_\gamma\ (A) = B$ és $T_{\gamma'}\ (A) = B$ is teljesülne, akkor az előző tétel alapján γ és γ' minden pontja egyenlő távol lenne A-tól is és B-től is, s mivel ezen pontok egy síkra illeszkednek, $\gamma = \gamma'$.

5.3. **Következmény:** Bármely, $\overline{A,B}$-re illeszkedő síkban azok a pontok, amelyek az A,B pontpártól egyenlő távolságra vannak, egy egyenesre illeszkednek, s ezen egyenes minden pontja egyenlő távolságra van az A és B pontoktól.
Ez az egyenes a tekintett sík és az A,B pontpárhoz tartozó szimmetriasík metszésvonala.

5.3. **Tétel:** A tér tetszőleges pontjából kiinduló két félegyeneshez egy és csak egy szimmetriasík tartozik.

Bizonyítás: Legyen a_1, b_1 a két félegyenes és kezdőpontjuk O. A X. axióma alapján létezik olyan $B \in b_1$ pont, melyre $d(O,B) = d(O,A)$, ahol $A \in a_1$ tetszőleges pont. Az 5.2 tétel alapján A,B pontokhoz létezik szimmetriasík. Ez a sík tartalmazza az A,B pontoktól egyenlő távolságra levő pontokat, így a O-t is.
Az $\overline{O,A}$ félegyenes képe így az $\overline{O,B}$ félegyenes.
Ha létezne a két félegyeneshez az előbbitől különböző szimmetriasík, akkor az 5.2 következmény alapján O illesz-

kedne erre a síkra is. Az A képe legyen ez utóbbi síkra történő tükrözésnél A'.

$d(O,A)=d(O,A')=d(O,B)$, de a X. axióma miatt $A'=B$, ami azt jelenti, hogy a két tükörsík megegyezik.

A következő tétel segítségével a síkra vonatkozó szimmetriából származtatjuk a tengelyes szimmetriát.

5.4. **Tétel:** Tetszőleges $\mathcal{L}$ síkhoz van olyan, azt metsző γ sík, amelyre vonatkozó tükrözés $\mathcal{L}$-t önmagára képezi le.

Bizonyítás: Tekintsük az $\mathcal{L}$ sík két tetszőleges, de különböző A,B pontját. Az 5.2 tétel alapján ezekhez egy és csak egy γ szimmetriasík tartozik, s ez illeszkedik az $[A,B]$ F felezési pontjára. Az $A\neq B$ miatt $\gamma\neq\mathcal{L}$. Így a 3.3 tétel következtében létezik $\mathcal{L}\cap\gamma=t$ metszésvonal. A γ-ra történő tükrözésnél $\overline{A,B}$ képe $\overline{B,A}$, a $t\subset\gamma$, így pontonként fix egyenes; az általuk meghatározott $\mathcal{L}$ sík képe is az $\mathcal{L}$ sík, hiszen a γ-ra való tükrözés síktartó.

5.3. **Értelmezés:** A tetszőleges $\mathcal{L}$ síkot t egyenesben metsző γ síkra vonatkozó tükrözés által az $\mathcal{L}$ síkon létrehozott leképezést, ha az $\mathcal{L}$-t önmagára képezi le, t **egyenesre vonatkozó síkbeli tengelyes szimmetriának** vagy **tengelyes tükrözés**nek nevezzük. **Jele:** S_t vagy T_t. Az egymáshoz rendelt pontok **tükörképek**, a t **tükörtengely** vagy **szimmetriatengely.**

5.4. **Következmény:** A tengelyes szimmetria származtatása alapján érvényesek a következő tulajdonságok:

1. Kölcsönösen egyértelmű leképezés. A t által meghatározott félsíkokat felcseréli, a tükörtengely pontjai és csak azok fixpontok.

2. Bármely $A,B \in \mathcal{L}$-ra $d(A,B) = d(T_t(A), T_t(B))$ – mivel egybevágóság.

3. Egyenestartó, párhuzamos egyeneseket párhuzamos, metsző egyeneseket metsző egyenesekbe visz át.

4. A rendezéstartó leképezés; félegyenes, szakasz, félsík képe félegyenes, szakasz, félsík.

5. Ha egy A pont képe A', akkor az A' képe az A. Involutórikus leképezés.

6. A sík bármely két különböző pontjához egy és csak egy szimmetriatengely tartozik.

Az 5.4 tétel és az 5.3 értelmezés alapján egy tartozik. Kettő nem tartozhat, mert ezek két szimmetriasíknak az $\mathcal{L}$ -val való metszésvonalai lennének, két ponthoz viszont két szimmetriasík nem tartozhat.

Az 5.4 tétel bizonyítása alapján $[A,B]$ F felezési pontjára: $F \in t$. t minden pontja egyenlő távol van az A és B pontoktól.

5.5. **Tétel:** A síkban tetszőleges pontból kiinduló két félegyeneshez egy és csak egy tükörtengely tartozik.

Bizonyítás: Legyen a_1, b_1 a két félegyenes, kezdőpontjuk O, síkjuk $\mathcal{L}$. Az 5.3 tétel alapján a_1, b_1-hez egyetlen γ tükörsík tartozik, s erre illeszkedik az O. Az $\mathcal{L}$ és γ sík így metszi egymást egy t egyenesben. $T_\gamma(a_1) = b_1$, t pontonként fix, $\mathcal{L}$ képe a γ-ra való tükrözénél $\mathcal{L}$, így γ az $\mathcal{L}$ síkon egy t tengelyű tükrözést létesít, amelynél $T_\gamma(a_1) = b_1$.

Több tükörtengely nem tartozhat, hiszen ha lenne még egy, akkor az értelmezés alapján ehhez is tartozna egy sík,

amely a_1 és b_1-nek szimmetriasíkja lenne, ez viszont ellentmond az 5.3 tételnek.

5.5. **Következmény**: A síkban tetszőleges pontból kiinduló két félegyeneshez tartozó tükörtengely átmegy a félegyenesek közös kezdőpontján.

5.6. **Tétel**: Legyen a és b az $\mathcal{L}$ sík két különböző egyenese. Ha $T_a(b) = b$, akkor $T_b(a) = a$ teljesül.

Bizonyítás: Az a egyenesre vonatkozó tükrözés az a által meghatározott félsíkokat felcseréli, így ha $T_a(b) = b$, akkor a és b nem lehetnek párhuzamosak, csak metszők. Mivel b-nek a-ra való tükörképe b, így tetszőleges $B \in b$, de $B \notin a$ pontot véve $T_a(B) = B'$, $B' \in b$.

Az 5.4 következmény utolsó állítása alapján az a egyenes illeszkedik a $[B,B']$ F felezési pontjára, és minden pontja egyenlő távol van a B és B'-től.

Legyen $A \in a$, de $A \neq F$. A $T_b(A) = A'$ pontnak az a-ra kell illeszkednie, ugyanis az a-ra való tükrözés miatt $d(A,B)) = d(A,B')$; b-re való tükrözés miatt $d(A,B) = d(A,B')$ és $d(A,B') = d(A',B')$, melyekből $d(A',B) = d(A',B')$, s az ilyen pontok csak az a tengelyen lehetnek.

Hasonlóan belátható, hogy ha $T_b(a) = a$, akkor $T_a(b) = b$.

5.6. **Következmény**: Egy sík bármely egyenese lehet szimmetriatengely ebben a síkban.

Tekintsük a sík tetszőleges a egyenesét, s ennek két, A és B pontját. Ezekhez egy és csak egy t szimmetriatengely tartozik. Mivel $T_t(a) = a$, az előző tétel miatt $T_a(t) = t$ is teljesül, így a is szimmetriatengelye a síknak.

5.7. **Következmény**: Az előző állítások alapján megfogalmazható a XI. axiómának megfelelő, síkra érvényes állítás:
Az $\mathcal{L}$ sík tetszőleges e egyenesét tekintve, egy és csak egy olyan egybevágóság létezik, amely az e által meghatározott zárt félsíkokat egymásnak felelteti meg, s melynél az e pontjai fixpontok.

5.4. **Értelmezés**: Ha két különböző egyenes olyan tulajdonságú, hogy egyiknek a másikra vonatkozó tükörképe önmaga, akkor a két egyenest **merőlegesnek** nevezzük. **Jele**: $a \perp b$.

5.8. **Következmény**:

1. Ez a reláció szimmetrikus és antireflexiv, ($a \perp a$ nem lehet)
2. A merőleges egyenesek metsző egyenesek. (Az 5.6 tétel bizonyításából következik.)
3. Az A,B pontokhoz tartozó szimmetriatengely merőleges $\overline{A,B}$-re. Az $\overline{A,B}$ intervariáns egyenes merőleges a tengelyre.

5.5. **Értelmezés**: Az a,b merőleges egyeneseken a közös pont által meghatározott, különböző egyenesekhez tartozó **félegyeneseket** is **merőlegeseknek** nevezzük.

5.6. **Értelmezés**: Az A,B pontpárhoz tartozó szimmetriatengelyt az $[A,B]$ **szakaszfelező merőlegesének** nevezzük.

5.7. **Értelmezés**: Adott tulajdonságú pontok összességét **mértani helynek** nevezzük.

5.7. **Tétel:** A sík azon pontjainak mértani helye, amelyek a sík két pontjától egyenlő távolságra vannak, a két pontot összekötő szakasz felezőmerőlegese.

Bizonyítás: Egyszerűen adódik az előzőekből. A szakaszfelező merőleges a két pont szimmetriatengelye, s korábban már beláttuk, hogy ennek minden pontja egyenlő távol van a két ponttól, s több ilyen pont nem létezik a síkban.

5.8. **Tétel:** Az $\mathcal{L}$ sík tetszőleges P pontjából a sík egy tetszőleges e egyenesére egy és csak egy merőleges illeszthető.

Bizonyítás:

1/ $P \notin e$: Legyen $T_e(P) = P'$. A keresett egyenes a $\overline{P,P'}$. Ha lenne még egy P-re illeszkedő merőleges, akkor az értelmezés alapján $T_e(P)$ erre is illeszkedne, ez csak úgy lehet, ha a két egyenes egybeesik.

2/ $P \in e$: A X. axióma alapján ha az e egyenes P által meghatározott egyik félegyenesén kiválasztunk egy tetszőleges A pontot, akkor létezik a másik félegyenesen pontosan egy olyan A' pont, melyre $d)P,A) = d(P,A')$. Az A,A' pontokhoz tartozó szimmetriatengely illeszkedik P-re, és merőleges e-re, jelöljük b-vel.

Ha lenne még egy P-re illeszkedő $g \perp e$ egyenes, akkor az értelmezés alapján $T_g(e) = e$ teljesül. Az A képe ennél a tükrözésnél is csak A' lehet, két ponthoz viszont csak egy szimmetriatengely tartozik, így $b = g$.

5.8. **Értelmezés:** Legyen e és P egy $\mathcal{L}$ sík egyenese, ill. pontja. A P pontból az e-re állított merőleges egyenesnek és

az e-nek a T metszéspontját a P pont e egyenesre vonatkozó **merőleges vetületének** vagy röviden **vetületnek** nevezzük. (T a merőleges talppontja.)

5.9. **Következmény:** Ha T a P pont e egyenesre vonatkozó merőleges vetülete, és P az e tetszőleges, de $A \neq T$ pontja, akkor $d(P,T) < (d(P,A)$.

Legyen $T_e(P) = P'$, $\overline{P,P'}$, a P-ből állított merőleges, és T a $[P,P']$ felezési pontja. A tetszőleges $P \in e$-re teljesül, hogy

$d(P,P') < d(P,A) + d(A,P') = 2d(P,A)$, de

$d(P,P') = 2d(P,T)$, így $d(P,T) < d(P,A)$.

5.9. **Értelmezés:** Legyen a P pont e egyenesre való merőleges vetülete T. A $d(P,T)$-t az A **pont** e **egyenestől való távolságának** nevezzük.

5.9. **Tétel:** Legyen $a \perp b$, és egy t tengelyű szimmetriánál képük a' és b'; ezekre teljesül, hogy $a' \perp b'$.

Bizonyítás: Indirekt. Tegyük föl, hogy $a' \perp b'$. Legyen $a \cap b = M$, ennek képe $a' \cap b' = M'$. Vegyünk föl az a-n egy $A \neq M$ pontot. A-nak a merőleges vetülete b-n M. A-nak A' képe illeszkedik a'-re, de merőleges vetülete b'-n egy $T' \neq M'$ pont.

Az 5.9 következmény alapján a T' eredeti pontjára, a T-re:

$D(A,T) > d(A,M)$, de $d(A,M) = d(A',M')$ és $d(A,T) = d(A',T')$, így $d(A',T') > d(A',M')$, ami ellentmond az idézett következménynek.

5.10. **Következmény:** Tükrözések sorozata merőleges egyeneseket merőleges egyenesekbe visz át.

5.10. **Tétel:** Legyen $a \perp b$. Ekkor $(a \perp c) \leftrightarrow (b \parallel c)$, ahol a, b, c $\mathcal{L}$-beli egyenesek.

Bizonyítás:

1/ Legyen $a \perp b$ és $b \parallel c$. Ekkor $a \perp c$. Az 1.4 következmény alapján létezik $a \cap c = P$. A b és c párhuzamos egyenesek képei az a-ra történő tükrözésnél a szintén párhuzamos b és c' egyenesek lesznek. $P \in c'$, így csak $c = c'$ teljesülhet, de a merőleges egyenesek értelmezése alapján így $a \perp c$.

2/ Legyen $a \perp b$ és $a \perp c$. Ekkor $b \parallel c$. Tekintsük a c egyenes tetszőleges C pontját. Az előbbi bizonyítás alapján a C-re illeszkedő, b-vel párhuzamos egyenes merőleges a-ra, s mivel csak egy ilyen merőleges létezik, ez maga a c, így $b \parallel c$.

5.11. **Következmény:** A tengelyes szimmetria invariáns egyenesei a tengely, és a rá merőleges egyenesek, ezektől különböző invariáns egyenese nincs a leképezésnek.
Az 5.4 értelmezés alapján a tengelyre merőleges egyenesek invariánsak. Ha $\overline{P, P'}$ invariáns egy t tengelyű tükrözésnél, akkor $\perp$ is a t-re, mivel a P-ből egyetlen merőleges állítható.

5.12. **Következmény:** A tengelyes szimmetria tengelytől különböző invariáns egyenesei párhuzamosak.

5.11. **Tétel:** A tengelyes tükrözést egy megfelelő (nem fix) pontpár, vagy a tengely egyértelműen meghatározza.

Bizonyítás:

1/ A pontpár felezőmerőlegese a tengely.

2/ Ha adott a tengely, akkor a tetszőleges P pont képe a P-ből a t -re állított merőlegesen van, a t által meghatározott másik félsíkban. Ha T a P $\perp$ vetülete, úgy $d(P,T)=d(P',T')$, ahol P' a képpont, s ez a X. axióma alapján egyértelműen meghatározható.

5.10. **Értelmezés:** Egy geometriai alakzatot **tengelyesen szimmetrikus**nak nevezünk, ha van olyan egyenes, amire tükrözve az alakzat önmagába megy át.

5.12. **Tétel:** Két metsző egyeneshez pontosan két tükörtengely tartozik.

Bizonyítás:

1./ Kettő tartozik. Legyen $a \cap b = O$, s az O által meghatározott félegyenesek a_1, a_2, ill. b_1, b_2. Az 5.5 tétel alapján az a_1, b_1 és a b_1, a_2 félegyenesekhez tartozik egy t_1, és egy t_2 tengely. A T_{t1} az a_2 és b_2 félegyeneseket is egymásnak felelteti meg, míg a T_{t2} az a_1 és b_2 félegyeneseket. $T_{t1} \neq T_{t2}$, hiszen a képpontok nem azonosak, így $t_1 \neq t_2$.

2./ Több nem tartozhat. Ha lenne még egy t_3, akkor $O \in T_3$, így ez a félegyenespárok valamelyikének szimmetriatengelye lenne, s így az 5.5 tétel alapján $t_1 = t_3$ vagy $t_2 = t_3$.

5.13. **Tétel:** Két metsző egyenestől egyenlő távolságra levő pontok mértani helye az egyenesek szimmetriatengelyei.

Bizonyítás:

1/ Legyen t_1, t_2 az a,b metsző egyenespár két szimmetriatengelye, s $P \in t_1$. A P-nek a-ra, ill. b-re való merőleges vetülete A, ill. B. Igazolni kell, hogy $d(P,A)=d(P,B)$. A t_1-re történő tükrözésnél a képe b, s merőleges egyenesek

képei merőleges egyenesek. Mivel P-ből b-re egyetlen merőleges állítható, így az a és $\overline{P,A}$ egyenesek A metszéspontja a képek B metszéspontjába meg át. P fixpont, így $d(A,P)=d(B,P)$. t_2-re hasonlóan belátható az állítás.

2/ Legyen P az a,b egyenesek síkjában olyan pont, amelyre teljesül, hogy az a és b-től való távolsága egyenlő, azaz $d(P,A)=d(P,B)$.

Tükrözzünk a $\overline{P,A}$ és $\overline{P,B}$ félegyenesekhez tartozó t tengelyre. A feltétel miatt A képe B, s mivel B-ben, $\overline{P,B}$-re egyetlen merőleges állítható, a képe b. t az a,b egyenespárnak is szimmetriatengelye, így $O\in t$, s P valóban a két egyeneshez tartozó szimmetriatengelyre illeszkedik.

5.14. **Tétel:** A metsző egyenesekhez tartozó szimmetriatengelyek merőlegesek egymásra.

Bizonyítás: Legyen a,b a két metsző egyenes, t_1,t_2 a két tükörtengely. Igazolni kell, hogy $T_{t1}(t_2)=(t_2)$ vagy $T_{t2}(t_1)=(t_1)$.

Tegyük fel, hogy az első állítás nem teljesül, s $T\in t_2$ képe, $T'\notin t_2$. Az előző tétel alapján $d(T,A)=d(T,B)$. A t_1-re történő tükrözésnél A képe $A'\in b$ és B képe $B'\in a$. Így $d(A,T')=d(B',T')$.

Az előző tétel szerint T' csak a két egyeneshez tartozó szimmetriatengelyeken lehet, ebben az esetben t_2-n.

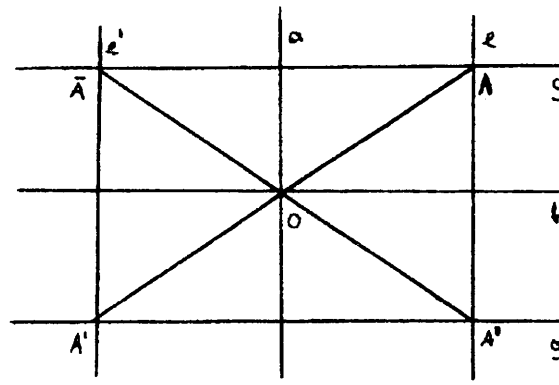
A következő tételben a centrális szimmetria értelmezését készítjük elő.

5.15. **Tétel:** Ha a,b merőleges egyenesek, akkor a két egyenesre történő tükrözések sorrendje felcserélhető. Ha egy A pontot erre a két egyenesre történő tükrözések szor-

zata A'-be visz át, akkor az A, O, A' pontok kollineárisak, ahol $O=a\cap b$.

Bizonyítás: Ha $\in\{a\cup b\}$, akkor az állítás közvetlenül adódik az előző állításokból.

Legyen $A\notin\{a\cup b\}$. (6. ábra) Jelöljük e,g-vel az A-ra illeszkedő, a, ill. b-vel párhuzamos egyeneseket.



6. ábra

A tengelyes szimmetria tulajdonságai alapján az $e\|e'$, ahol $e'=T_a(e)$, és $g\|g'$, ahol $g'=T_b(g)$. Mivel $e\|a$ és $a\perp b$, valamint $b\|g$, az 5.10 tétel miatt $e\perp b$ és $e\perp g$ teljesül. Mivel $g\|b\|g'$ és $b\perp a$, az a-ra történő tükrözésnél g és g' is invariáns egyenes ($g\perp a$, $g'\perp a$ is teljesül).

Hasonló okok miatt a b-re történő tükrözésnél e és e' is invariáns egyenes. Az 5.10 következmény alapján az egymásra merőleges e,g egyeneseket a $T_b\,o\,T_a$ és a $T_a\,o\,T_b$ szorzatleképezések is az e', g' merőleges egyenespárba viszik át. Legyen $\overline{A}=e'\cap g$, $A''-e\cap g$, $A'=e'\cap g'$.

Mindkét szorzatleképezés az A pontot az A'-be viszi át, így $T_a o T_b o = T_b o T_a$.

Az $[A,A']$ képe a b-re vonatkozó tükrözésnél az $[A'',\overline{A}]$; legyen b-vel való metszéspontjuk O_1. (O_1 létezik, mert g és g' két különböző, b határegyenesű félsíkban van).

Az $[A,A']$ képe az a-ra való tükrözésnél $[\overline{A},A'']$; a-val való metszéspontjuk legyen O_2.

$[\overline{A},A''] \cap [A,A'] = O_1 = O_2 = O$. Így A,O,A' kollineáris, s mivel a tükrözések szorzata is egybevágóság, $d(O,A) = d(O,A')$.

5.16. **Tétel:** Két különböző, a és b egyenes akkor és csak akkor merőleges, ha $T_a o T_b = T_b o T_a$.

Bizonyítás:

1/ Ha $(a \perp b) \rightarrow (T_a o T_b = T_b o T_a)$. Ez az előző tétel első állítása.

2. Ha $a \neq b$ és $T_a o T_b = T_b o T_a$, akkor $a \perp b$.

Tekintsük az a egyenesnek egy nem b-n lévő A pontját.

$T_b(T_a(A)) = T_b(A) = A'$. A feltétel alapján $T_a(T_b(A)) = A'$.

Mivel $T_b(A) = A'$, így $T_a(A') = A'$. Az a tengelyű tükrözésnél A' fixpont, így $A' \in a$. Az a egyenes tetszőleges pontjának képe a b-re történő tükrözésnél a-ra illeszkedik, így mivel $a \neq b$, az $a \perp b$ teljesül.

(A felépítés a centrális szimmetria értelmezésével folytatódik.)

IRODALOM

[1] G. Choquet, Geometria, Mir Moszkva, 1970.
[2] Dr. Hajós György: Bevezetés a geometriába. Tankönyvkiadó, Budapest, 1966.
[3] Dr. Pelle Béla: Geometria. Tankönyvkiad., Budapest, 1974.
[4] Radó Ferenc—Orbán Béla: A geometria mai szemmel. Dacia Könyvkiadó, Kolozsvár, 1981.
[5] Dr. Redling Elemér: Geometriai transzformációk. Tankönyvkiadó, Budapest, 1980.
[6] Dr. Szendrei János: Algebra és számelmélet. Tankönyvkiadó, Budapest, 1974.
[7] Vigassy Lajos: Egybevágósági transzformációk a síkban és a térben. Tankönyvkiadó, Budapest, 1979.

OROSZ GYULÁNÉ

MOTIVÁCIÓ A MATEMATIKA TANÁROK KÉPZÉSÉBEN

ABSTRACT: *(Motivation at the mathematics teachers training)* This paper is about an experiment connected with motivation and our experiences.

The structure of this paper is as follows: Introduction, some models about motivation at the mathematics teaching, conclusion about our lessons.

Igen, a matematika óra is lehet érdekes, színes, hasznos, de még több is annál: „hozzászoktathatja szemünket, hogy lássa az igazságot tisztán és világosan", ahogy Descartes olyan találóan mondta. Éppen ezért nagyon fontos feladat a matematikát tanító tanárok számára a tanulói motiváció kialakítása, tervszerű és tudatos fejlesztése. Nem könnyű feladat ez, hiszen a tanulói motivációt igen sokféle és bonyolult hatásmechanizmus alakítja.

A motivációval kapcsolatos hazai és külföldi kutatások arra utalnak, hogy e kérdéskör nagyon széles skálán mozog és egyáltalán nem könnyű az összefüggéseit feltárni.

Kozéki Béla a motivációt, mint aktív tevékenység folyamatában kialakuló, tevékenységre késztető belső feszültséget értelmezi, amely kognitív, effektív és affektív dimenziókban fejlődik [4].

(A továbbiakban tanulói motiváción a tanulási tevékenységre késztető belső feszültséget értjük.)

A. Z. Krygwska szerint „a matematikai érdeklődésterminus pontosítást és bizonyos kategorizálást igényel annak a megfigyelése alapján, ami iránt a tanulók különösen érdeklődnek" [1]. Véleménye szerint a motivációra vonatkozó kutatás kisszámú és alapvető felfogásbeli különbségeket mutat a matematika iránt érdeklődő tanulóknál és tanároknál.

M. Besuden a motiválást a matematika oktatásában a problémafölvető oktatás segítségével képzeli el. Azt állítja, hogy a matematika szisztematikus felépítése általában nem elegendő ösztönző a tanulók számára a vele való foglalkozáshoz [1].

Pólya György szerint a tanítás művészet, de később elismeri, hogy lehet elmélet tárgya is, s e művészet gyakorlását lehet és kell is tanulni. A tanítás tudományos alapelvének tekinti a „legjobban motiváltság" elvét [5].

Réthy Endréné kutatásában a tanulási motiváció hatásösszefüggéseit vizsgálja. Kísérlettel igazolja, hogy a tanulási motiváció szituációkban történő tudatos fejlesztése pozitív hatást gyakorol a tanuló órai munkájára, érdeklődésére, kitartására a feladatmegoldásban és tanulmányi teljesítményére is. Kérdőíves vizsgálattal feltárja a gyakorló tanárok motiváló tevékenységét. Szükségesnek tartja a tanulási motiváció hatékonyabb fejlesztését. Javasolja, hogy a motiváló eljárások be-

mutatása, elemzése, s a gyakorlatban való alkalmazása mikrotanítási kurzus segítségével kapjon helyet a tanárképzésben is [6].

Falus Iván vizsgálataiban rámutat a mikrotanítás szerepére, a tanítási készségek fontosságára, tekintettel a motiváció készségére is [2].

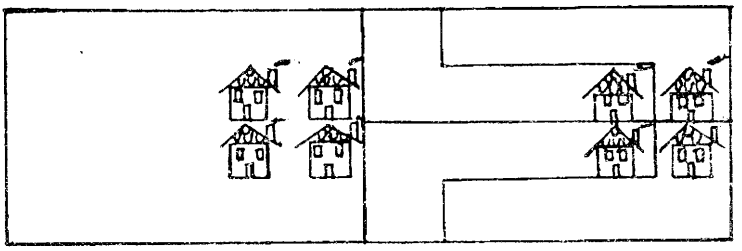
A fenti gondolatok a matematika szakos tanárképzésben a következőket jelentik. Tervszerűen és tudatosan készítsük fel hallgatóinkat arra, hogy érezzék a motiváció fontosságát a tanításban. Legyenek képesek tanítványaik érdeklődését felkelteni, megerősíteni. Röviden: tanítsuk meg őket arra, hogy motiváljanak és hogyan motiváljanak.

Ennek érdekében a matematika módszertan óráinkon motiváló tényezőkkel ismertettük meg hallgatóinkat, motiváló eljárásokat mutattunk be számukra. Az általános iskolai tananyaghoz kapcsolódó mikroóra-modelleket állítottunk össze, amelyekben a motiváció készségeit helyeztük előtérbe. A megismert motívumok egy részét a mikrotanítások során a gyakorlatban is megvizsgáltuk, elemeztük. Kísérletünkben az 1989–90-es tanévtől kezdődően a III. évfolyam hallgatói vettek részt. Dolgozatunkban konkrét feladatok kapcsán mutatjuk be modellünket. Elemzésükkel rámutatunk a motiválási lehetőségekre és röviden ismertetjük tapasztalatainkat.

1. SZEMLÉLTETŐESZKÖZ FELADATHOZ

FELADAT

Egy gondoskodó apa négy fiának egy téglalap alakú telekre házat épített, az 1. ábrán látható módon. Hogyan kell felosztani a telket, ha azt szeretné, hogy minden fia azonos alakú, egyenlő területű részt és 1–1 házat kapjon?



1. ábra

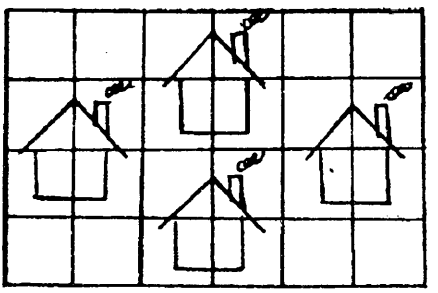
Az eszköz leírása: Tanári bemutatáshoz rajzlapból készítettük el, úgy, hogy applikálható legyen. Ehhez a nagyméretű rajzlapot használtuk és a házakat színes zsírkrétával megrajzoltuk. A gyerekek számára is készítettünk 1–1 példányt írólapra, amelyre lerajzolhatták a megoldást. A tanári eszköznél a megoldást a rajzlap hátoldalán rögzítettük.

Tapasztalatok, észrevételek:

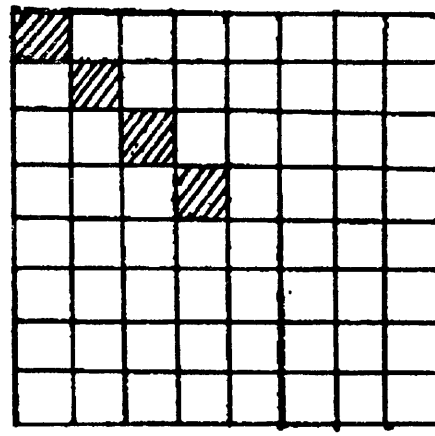
Az eszközt szemináriumi csoportjainknak bemutattuk és a problémát felvetettük. Megjegyezzük, hogy a hall-

gatók hosszabb idő alatt oldották meg, mint amire számítottunk, egy részük nem is tudta megoldani.
Mikrotanítás során az egyik III. éves hallgató 5. osztályos tanulók számára, motiváló célzattal kitűzte a feladatot. A gyerekek rendkívüli lelkesedéssel fogadták, szinte türelmetlenül várták, hogy megkapják a számukra elkészített eszközt és belemerültek a munkába. A tanulók többsége megbirkózott a feladattal és alig várta, hogy ismertesse a megoldást. Motiváló hatása meglepte a hallgatókat is, hiszen az a vártnál erősebb volt.
A tanulók aktivitásának fokozódása meggyőzte őket a szemléltetés fontosságáról.
A mikrotanításról készített videófelvételen részletesen elemeztük a tapasztalatokat.

Amikor az 1.-es ábrához tartozó probléma nehéznek bizonyult a gyerekek számára, megbeszéltük a hallgatókkal, hogy úgy segítsenek a tanulóknak, hogy a lapot hajtsák ketté és két ház esetén keressék a megoldást.



2. ábra



3. ábra

A feladat differenciálásra is alkalmas a 2. és 3. ábrával kiegészítve, amelyet előre elkészítettünk. A 3. ábrához tartozó problémát a különösen érdeklődő tanulók számára, otthoni munkára ajánlottuk.
A 2. ábrához tartozó szemléltető eszközt azoknak a tanulóknak adtuk, akik az elsőt igen rövid idő alatt megoldották.

A hallgatók feladatai:
Tervezzenek szemléltető eszközöket feladatokhoz. Írjanak különböző szövegeket olyan matematikai tartalmú problémához, amely közel áll a gyerekek érdeklődéséhez.

A szövegíráshoz néhány ötletet javasoltunk:
– A játszótéren négy hintát rögzítettek, ...

– Egy parkba négy fát ültettek, ...
– A Lutra album egy lapjára négy képet ragasztottak, ...
– Sportpályán négy tenisz-pályát építettek, ...

2. TÖBBFÉLE MEGOLDÁSI MÓD KERESÉSE

FELADAT: Határozzuk meg az x értékét, ha

$$1243^{1962} \equiv x \qquad \text{mod } (100).$$

I. Megoldási mód: (Főiskolai ismeretek felhasználásával)
Az Euler–Fermat kongruencia-tétel alapján,
mivel $(43, 100) = 1$ és $\varphi(100) = 40$
ezért $43^{40} \equiv 1 \ (100)$ és $43^{1962} \equiv 43^2 \equiv 49 \ (100)$, tehát
$x = 49$.

II. Megoldási mód: (Középiskolai ismeretek alapján)

Először megfogalmaztuk a problémát a középiskolai diák tudásszintjének megfelelően.
Mennyi a maradék, ha az 1243-nak az 1962. hatványát 100-zal osztjuk:

$1243^{1962} = (12 \cdot 100 + 43)^{1962}$, ezért a binomiális tételre hivatkozva elegendő a 43^{1962}-t vizsgálni, mivel $43^{1962} = \left[(43)^2\right]^{981} = (18 \cdot 100 + 49)^{981}$.... az eljárást folytatva kapjuk, hogy a maradék: 49.

III. Megoldási mód: (Általános iskolai tudásszintnek megfelelően)

A probléma megfogalmazása a tanuló ismereteihez:
Mi az utolsó két számjegye az 1243^{1962} hatványnak?
Számológép segítségével végeztük a számításokat.
Mivel a tízeseknél nagyobb helyiértékű számjegy nem befolyásolja az utolsó két számjegyet, ezért elegendő a 43 hatványait kiszámítani.

Hatvány:	**Utolsó két számjegy:**	
1243^1	43	1.
1243^2	49	2.
1243^3	07	3.
1243^4	01	4.
1243^5	43	5.
.	.	.
.	.	.
.	.	.

A gyerekek induktív úton felismerik, hogy a számjegyek ismétlődnek. Mivel $1962 = 4 \cdot 490 + 2$ az ismétlődő számok között a 2. adja a megoldást, azaz 49.

Tapasztalatok, észrevételek

A hallgatók szívesen oldanak meg ilyen jellegű feladatokat. Szemináriumi munkájukra kifejezetten pozitív hatást gyakorolnak. A legtöbb esetben ugyanis nem a megoldás okoz számukra nehézséget, hanem az, hogy nem tudnak olyan megoldást találni, ami igazodik az általános iskolás tanuló matematikai ismereteihez. Önmagunk számára mindezekből azt a következtetést vontuk le, hogy meg kell őket tanítanunk ilyen megoldási módszerekre.

A látszólag száraznak tűnő problémát 6. osztályos tanulók részére vetettük fel. Tudatosan motívumokat építettünk a feladatba, olyan lépésekben, amelyeket a hallgatók számára is bemutattunk.

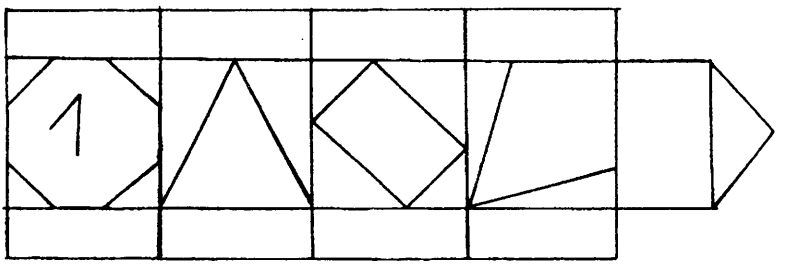
1. lépés:
Feladatot készítettünk a hatványalap meghatározására:

FELADAT:
Melyik az a négyjegyű természetes szám, amelyikről a következőt tudjuk: Balról jobbra haladva:

- Első számjegye a legkisebb pozitív természetes szám.
- Második számjegye a 34 és a 190 legnagyobb közös osztója.
- A harmadik számjegye a 2 és a 4 legkisebb közös többszöröse.
- Az utolsó számjegyét megkapjuk, ha a következő mondatból a hiányzó szót pótoljuk:

.... kívánság —televíziós műsor gyerekeknek.
MEGOLDÁS: 1243.

2. lépés
Szemléltetőeszközt készítettünk, ami segítette a feladat értelmezését. (4. ábra)

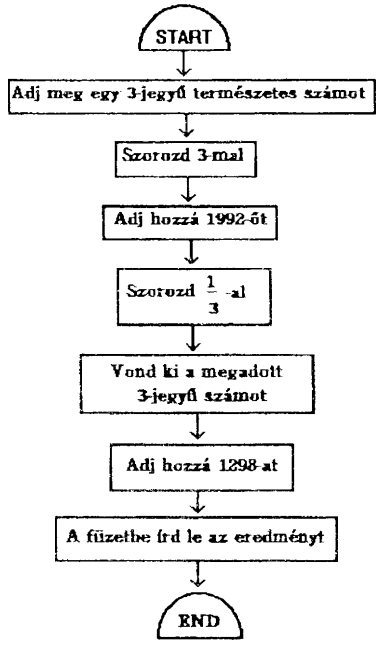


4. ábra

3. lépés
Feladatot készítettünk a hatványkitevő kiszámítására.

FELADAT:

A folyamatábra utasításai alapján végezd el a kijelölt műveleteket! (5. ábra)



5. ábra

4. lépés
Számológép segítségével a gyerekekkel ellenőriztettük számításaikat.

MEGOLDÁS: 1962.

5. lépés
A tanulók számára azt az utasítást adtuk, hogy írják fel a füzetbe azt a hatványt, amelynek alapja az 1243 kitevője pedig 1962.

Ezekkel a lépésekkel jutottunk el a probléma kitűzéséhez.

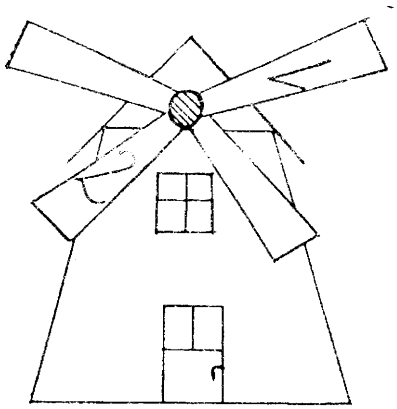
A mikrotanítások során a tanulók érdeklődéssel fogadták a feladatot. Az általunk tudatosan beépített motívumok pozitív hatást gyakoroltak a tanulók órai munkájára. Kitartóan oldották meg további feladataikat is.

A hallgatók feladatai:

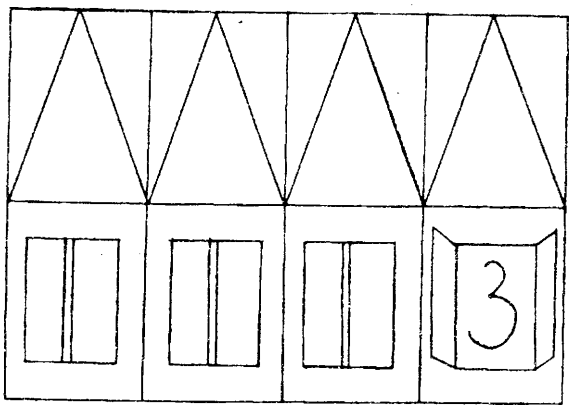
Készítsenek számelméleti feladatokat, amelyekbe motívumokat terveznek!

A hallgatók is érdekesnek találták a bemutatott modelleket és feladataikat magasabb színvonalon, igényesebben oldották meg. Figyelmet érdemelnek a hallgatók munkái, amelyek közül kettőt bemutatunk.

A hallgatók által készített szemléltetőeszközök:



6. ábra



7. ábra

A szemináriumokon a tanulmányunkban említetteken kívül több motiválási lehetőséget, modellt mutattunk meg, amelyek közül a következőket emeljük ki:

További motiváló tényezők:

1. *Versenytesztek készítése*
   A jelenlegi taneszközökben lévő tudáspróbákat ezekkel kiegészíthetjük, az ellenőrzést változatosabbá tehetjük.
2. *Keresztrejtvények*
   Alkalmasak óra elején a számolási készség fejlesztésére, nem teszik azt mechanikussá.
3. *Varázskártyák*
   A tanulók érdeklődéssel fogadják, az órákat színesítik, élményszerűvé teszik.

A felsoroltakon kívül számos terület elemezhető, amelyekkel további vizsgálatainkban szeretnénk foglalkozni.

IRODALOM

[1] Ambrus András: *Matematikadidaktikai tanulmányok.* Tankönyvkiadó, Budapest, 1989.

[2] Falus Iván: *A mikrotanítás elméleti és gyakorlati kérdései.* Tankönyvkiadó, Budapest, 1986.

[3] J. I. Ignatyev: *A találékonyság birodalmában.* Tankönyvkiadó, Budapest, 1982.

[4] Kozéki Béla: *A motiválás és motiváció összefüggéseinek pedagógiai és pszichológiai vizsgálata.* Akadémiai Kiadó, Budapest, 1980.

[5] Pólya György: *A problémamegoldás iskolája.* I.–II. kötet, Tankönyvkiadó, Budapest, 1971.

[6] Réthy Endréné: *A tanítás - tanulási folyamat motivációs lehetőségeinek elemzése.* Akadémiai Kiadó, Budapest, 1988.

[7] Takács Gábor–Takács Gáborné: *A tanulói motiváció erősítése az alapfokú matematika tanításában.* A Matematika Tanítása, 1988. 3. sz.

[8] Takács Gábor: *Szerettessük meg a matematikát.* Tanító, 1991. 10. sz.

SZILÁK ALADÁRNÉ

SZÁMÍTÁSTECHNIKA A SZAKOSÍTOTT MATEMATIKA-TANTERVŰ ÁLTALÁNOS ISKOLAI 6., 7. OSZTÁLYBAN

(Egy kísérlet tapasztalatai)

ABSTRAKTO: *(Kalkultekniko en la fakaj matematikaj studplanaj 6., 7. klasoj)* La skríbleciono la matematikaj fakaj-studplanaj „Kalkulteknika" téma 6., 7. klasaj instruajn spertojn rezumas.

Tiaj nivelaj la instruadon de kalkulteknikaj konoj konsílas, por kio en la matematikaj lernhoroj, baldaŭ ankaŭ en la mezlernejo ebla konstrui sukcese.

Hazánkban különböző kísérletek folynak a számítástechnika középiskolai oktatásával kapcsolatban. A kísérletek tapasztalatairól, eredményeiről rendszeresen olvashattunk „A Matematika Tanítása" című folyóiratban (Dr. Simonovits Miklós az „irányított vonalról", Török Turul a „szabad vonalról"). Mivel a számítástechnikai alapismereteket az általános iskolás korú gyerekekkel is meg lehet tanítani, érdemes lenne a középiskolának az itt szerzett ismeretekre

alapozva egy általánosabb értelmezésű informatikával foglalkozni. Sajnos a számítástechnika oktatása és alkalmazása – az ország összes általános iskoláját figyelembe véve – még nem jutott el odáig, hogy a megszerzett számítástechnikai ismeretekre minden középiskolába kerülő tanulónál lehetne építeni.

Számítástechnikai alapismertek tanítására az általános iskolában is többféle lehetőség van: pl. szakköri foglalkozások, fakultáció, tanóra (elsősorban matematika, technika) keretében.

A szakosított tantervű (matematika-tagozatos) osztályokban 5. osztálytól évente 10–12 órában tanítunk számítástechnikát matematika órán. A szakosított tanterv 5., 6., 7. osztályos számítástechnika-anyaga olyan alapismereteket tartalmaz, amely megtanítható a jobb képességű, általános tantervű osztályokban is a matematika tananyagba beépítve, matematikai problémák megoldásához kapcsolva. Természetesen ez több felkészülést, sok időt, új, hatékonyabb tanítási módszerek kidolgozását, eszközök használatát igényli a tanártól, de a munkaráfordítás megtérül, akár a matematika, akár a számítástechnika oldaláról nézzük. Fontos, hogy akkor kezdjük el az algoritmikus gondolkodásmód kialakítását, a számítástechnika alapjainak tanítását, amikor erre a tanulók a legfogékonyabbak, már az általános iskolában. Az alábbiakban röviden szeretnék beszámolni azokról a tapasztalatokról, amelyeket a szakosított tantervű hatodik, majd a következő évben hetedik osztályban a számítástechnika témakör tanításakor tapasztaltam az egri Tanárképző Főiskola IV. Sz. Általános Iskolájában.

Az iskolában angol-, matematika-tagozatos, illetve általános-tantervű osztályok tanulnak. Az angol-tagozatos osztályokba harmadik év elején a legjobb tanulókat válogatják. A matematika-tagozatra negyedik év végén veszik fel a tanulókat a nem angol-tagozatos osztályokból. Ezért a matematika-tagozatos osztályokba már közepes képességű gyerekek is járhatnak. Nehezíti a munkát az is, hogy elég nagy létszámú csoportokban (osztályokban) folyik a tanítás (30–33 fő).

A témakör tanításakor a tantervi követelmények (tudjanak a tanulók egyszerű algoritmusokat készíteni,. azokat a számítógép nyelvén megfogalmazni elsősorban az INPUT, LET, IF...THEN, FOR..TO...NEXT utasítások alkalmazásával) figyelembevételével számbavettem a megtanítandó ismereteket, és az ismeretekkel összefüggésben a tudásszinteket: ráismerés, megnevezés, reprodukálás, operatív alkalmazás és a megismerő alkalmazás szintjét. Az ismeretek alkalmazásának, számonkérésének megfelelő feladattípusokat a tudásszintekhez igazodva állítottam össze, miközben olyan problémákat fogalmaztam meg, melyek megoldása tanult matematikai ismeretek alkalmazását is lehetővé tette.

Így 6. osztályban pl. olyan egyszerű algoritmusokat készítettünk, amelyek segítségével terület-, térfogatszámításokat végeztünk, meghatároztuk egy (nem 0) természetes szám összes osztóját, prímszámokat kerestünk stb. 7. osztályban az előző évben elkészített algoritmusokat kiegészítettük, elmélyítettük, majd további problémák megoldásával erősítettük ismereteinket: „verbális" vagy „félig formalizált" algoritmusokat fogalmaztunk meg a legnagyobb közös osztó,

legkisebb közös többszörös meghatározására, a racionális számok tizedes tört alakjának a felírására stb. A tudásszintek figyelembevételével készült a témazáró feladatlap (A és B változatban) is mindkét évfolyamon. Az egyes feladatok különböző szinteken kérték számon a tanulók tudását, fontosságát tekintve azonban nem volt különbség az egyes feladatok között, ugyanis adott szinten minden feladat megoldása egyformán fontos. A pontozásnál is ezt vettem alapul.

A feladatok között szerepelt alternatív, feleletválasztásos, konstruktív, kiegészítéses, rendszerező, besoroló feladat. Mivel adott ismeretet 7. osztályban magasabb szinten kell tudni és alkalmazni, mint 6. osztályban, így a feladattípusok a két évfolyamon (ugyanahhoz a problémához kapcsolódva) különbözőek voltak. A magasabb évfolyamon elsősorban konstruktív, rendszerező, besoroló típusok fordultak elő a gyakorlás és a számonkérés során is.

Pl.:

– „Tudjanak a tanulók egyszerű (feltétel nélküli) folyamatábrákat készíteni" tantervi követelményt a megismerő alkalmazás szintjén hatodikban rendszerező, besoroló feladattípussal gyakoroltattam és kértem számon, míg hetedikben már konstruktív feladatokon keresztül kellett számot adni a követelményről.

– Aritmetikai kifejezés, reláció értékének meghatározása 6. osztályban feleletválasztásos feladattípussal történt, 7. osztályban konstruktív formában.

– Az ABS(X), INT(X) függvények 6. osztályban reprodukálás szintjén, feleletválasztásos feladatokon keresztül rögzí-

tődtek, 7. osztályban az operatív és a megismerő alkalmazás szintjén a konstruktív feladattípusok voltak a gyakoribbak.

A számonkéréshez készített témazáró feladatsort mindkét évfolyamon 30–30 tanuló írta meg. Az osztály átlaga hatodikban 89 % pont, hetedikben 86 % pont teljesítésű lett. Abszolút hibátlanul az alacsonyabb évfolyamon a tanulók 23 %-a, a magasabb évfolyamon a 19 %-a dolgozott. Sajnos mindenki által hibátlanul megoldott feladat egyik évfolyamon sem volt. Megnyugtató azonban az, hogy hatodikban a tanulók 90 %-a jól összeállította adott utasításszimbólumokból az egyszerű (feltétel nélküli) folyamatábrát, és 77 %-a írta meg hibátlanul a BASIC-programját. Folyamatábrát – teljesen önállóan – a 7. osztályos feladatlapon kellett készíteni. Ez már nehezebb volt, ugyanis a tanulók 52 %-a készített csak „működőképes" folyamatábrát, és 48 %-a írta meg hibátlanul a programját. Az utóbbi adatok nem tűnnek túl nagy eredménynek. Sajnos a feladatoknál a tanulók többsége matematikai hibákat vétett.

Lényegesen jobb eredmény mutatkozott az előző évhez (6. osztály) viszonyítva az alábbi ismeretekhez kapcsolódva:

- Az egész-, valós-, karakter-típusú, egyszerű változókat a tanulók 84 %-a helyesen értelmezte és alkalmazta.
- Feltételt tartalmazó folyamatábra elemzését, kiegészítését, a feladat programját az osztály 90 %-a készítette el hibátlanul.
- Hasonló eredményt értek el ciklusutasítást tartalmazó programrészlet elemzésével.
- Az abszolut érték, egész rész és a véletlen számokat előállító függvényeket tartalmazó program „futtatását" a tanulók 84 %-a jól elvégezte.

Összegezve: A gyerekek 80 %-a a hetedik osztály végére eljutott oda, hogy rendelkezik olyan számítástechnikai alapismeretekkel, amelyekre nyolcadik osztályban, majd a középiskolában eredményesen lehet építeni. A számítógépes problémamegoldás lépéseit (elemzés, algoritmus-, folyamatábrakészítés, programírás, futtatás adatokkal) a tanulók rendszerint követték, indokoltnak tartották, hogy egy-egy probléma megoldásakor a tanult lépések szerint járjanak el. A programok elkészítése, elemzése, eredményének előrelátása, majd számítógépen történő futtatása, ellenőrzése erősítette bennük azt a tényt, hogy a gép tevékenységének szervezője az ember, a gép magától nem tud semmit.

Vannak azonban megoldásra váró feladatok is: a számítógép kezelése terén nem jutott el az osztály minden tanulója olyan szintre, hogy irányítás, segítség nélkül, viszonylag gyorsan megoldotta volna egy-egy program futtatását. Harmincas létszámú osztályban ugyanis nehéz a számítógépes gyakorlatokat úgy megszervezni, hogy minden tanuló aktívan gépközelbe kerülhessen. A tanórán kívüli gyakorlásra sem lehetett a gyerekek többségénél számítani, mert nem jártak szakkörre, vagy nem volt otthon számítógépük, vagy nem is érdeklődtek különösebben a gép és a számítástechnika iránt.

E hiányosságok mellett az eredményeink a fontosabbak: a tanulókban erősödött az algoritmikus gondolkodásmód, értették az egyszerűbb feladatok logikai szerkezetét, le tudták azt jegyezni (folyamatábra formájában) és a gép nyelvére lefordítani (BASIC-program formájában).

Az előző évben még passzív ismeretek hetedik osztályban aktív tudássá váltak.

Továbbiakban feladatomnak tartanám a megszerzett számítástechnikai ismeretek alkalmazását a matematika valamely fejezetének (pl. 8. osztályában: kombinatorika, valószínűség, matematikai statisztika) a tanításakor. Ez egyrészt biztosítaná a számítástechnika eszköz-, fejlesztő-, előkészítő-jellegű alkalmazását a matematika tanításában, másrészt felszínen tartaná a számítástechnikai ismereteket is.

IRODALOM

[1] Dr. Simonovits Miklós: *TANTERV-vázlatok a Számítástechnika c. tankönyvhöz.* A Matematika Tanítása, 1987/5.

[2] Török Turul: *Matematika és számítástechnika.* A Matematika Tanítása. 1988/5.

Az Eszterházy Károly Tanárképző Főiskola
Tudományos Közleményeinek kötetei

Amerikanisztikai tanulmányok
Angol filológiai tanulmányok
Francia filológiai tanulmányok
Germanistische Studien
Szláv filológiai és metodológiai tanulmányok
Tanulmányok a biológiai tudományok köréből
Tanulmányok a filozófia köréből
Tanulmányok a fizikai tudományok köréből
Tanulmányok a földrajztudomány köréből
Tanulmányok az irodalomtudomány köréből
Tanulmányok a kémia köréből
Tanulmányok a közgazdaságtudomány köréből
Tanulmányok a magyar nyelvről
Tanulmányok a matematikai tudományok köréből
Tanulmányok a neveléstudomány és pszichológia köréből
Tanulmányok az oktatástechnológia és informatika köréből
Tanulmányok a politikatudomány köréből
Tanulmányok a számítástechnika köréből
Tanulmányok a testnevelés- és sporttudományok köréből
Tanulmányok a történelemtudomány köréből