BUI MINH PHONG

KAPCSOLATOK A KÜLÖNBÖZŐ TÍPUSÚ LUCAS PSZEUDOPRIM SZÁMOK KÖZÖTT

Abstract: **(Connections between Lucas pseudoprimes of different types)** We investigate the properties of four spcial types of pseudoprimes with respect to Lucas sequences: Euler Lucas pseudoprimes, complete Lucas pseudoprimes, perfect Lucas pseudoprimes, and Gauss Lucas pesudoprimes. We prove some new connections among them.

Legyen A és B két egész szám, amelyekre $D = A^2 - 4B \neq 0$. Definiáljuk az $R = R(A,B) = \left\{R_n\right\}_{n=0}^{\infty}$ és $S = S(A,B) = \left\{S_n\right\}_{n=0}^{\infty}$ Lucas sorozatokat az A,B paraméterekkel, az $R_0=0$, $R_1=1$, $S_0=2$, $S_1=A$ kezdőelemekkel és az

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

illetve

$$S_n = AS_{n-1} - BS_{n-2} \qquad (n > 1)$$

rekurzív formulákkal. Legyen α és β az

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

karakterisztikus polinom gyökei és tegyük fel, hogy az R(A,B) és S(A,B)

Lucas sorozatok nem degeneráltak, vagyis $AB \neq 0$, $(A,B)=1$ és α/β nem egységgyök. Jól ismert, hogy a sorozatok tagjainak explicit előállítása

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

illetve

$$S_n = \alpha^n + \beta^n \ .$$

Ismert, hogy ha n egy prímszám, amelyre $(n,2BD)=1$, akkor

(1) $$R_{n-(D/n)} \equiv 0 \pmod{n} \ ,$$

(2) $$R_n \equiv (D/n) \pmod{n}$$

és

(3) $$S_n \equiv S_1 = A \pmod{n} \ ,$$

ahol $D=A^2-4B$ és $(./n)$ a Jacobi szimbolum (lásd pl. LEHMER (1930)). Ha n összetett, $(n,2BD)=1$, de (1) kongruencia teljesül, akkor az n számot Lucas peszudoprimnek nevezzük az R sorozat vonatkozásában. A továbbiakban egy R(A,B) sorozat vonatkozásában az összes Lucas pszeudoprimek halmazát $P[A,B]$ -vel jelöljük. Továbbá, ha egy $n > 0$ összetett egészre $(n,2BD)=1$ és

(4) $$R_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \text{ ha } (B/n)=1$$

vagy

(5) $$S_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \text{ ha } (B/n)=-1$$

teljesül, akkor az n számot Euler Lucas pszeudoprimnek nevezzük az R sorozat vonatkozásában és ezek halmazát $EP[A,B]$ -vel jelöljük. Könnyen belátható, hogy ezek a definiciók az A=c+1 és B=c esetben az $(n,c-1)=1$

feltételt kielégítő közönséges c vonatkozású pszeudoprim, illetve Euler pszeudoprim számokat definiálják, miszerint n szám c egész szám vonatkozásában pszeudoprim, illetve Euler pszeudoprim, ha n összetett, (n,2c)=1 és

$$c^{n-1} \equiv 1 \pmod{n}$$

illetve

$$c^{\frac{n-1}{2}} = (c/n) \pmod{n}$$

kongruenciák fennállnak. A továbbiakban c vonatkozású pszeudoprimek, illetve Euler pszudoprimek halmazát $P[c]$ -, illetve $EP[c]$ -vel jelöljük.

A pszeudoprim számokkal kapcsolatos 1972-ig elért eredményekről ROTKIEWICZ (1972/a) adott jó összefoglalást, könyvében számos problémát is felvetett. Az utóbbi időben egyre több szerző foglalkozik pszeudoprim számokkal és különböző általánosításukkal, mert a primtesztek elméletében igen jól használhatók (lásd pl. BAILLIE, WAGSTAFF, Jr. (1980) és POMERANCE, SELFRIDGE, WAGSTAFF, Jr. (1980)). Jól ismert, hogy tetszőleges nem degenerált Lucas sorozatok esetén végtelen sok Lucas, illetve Euler Lucas pszeudoprim szám van (lásd pl: LIEUWENS (1971) és BAILLIE, WAGSTAFF, Jr. (1980)). Ennél többet sikerült bizonyítanunk, megmutattuk, hogy rögzített s természetes szám esetén végtelen sok Euler Lucas pszeudoprim szám létezik, mely pontosan s különböző primszám szorzata és ezek a primszámok választhatók egy számtani sorozat tagjaiból (lásd BUI MINH PHONG (megjelenés alatt) és P. KISS, BUI MINH PHONG, E. LIEUWENS (1986)).

DUPARC (1955), LIEUWENS (1971) és ROTKIEWICZ (1972/B) foglalkoztak

azokkal az n összetett számokkal, amelyek egyidejűleg kielégítik az (1), (2) és (3) kongruenciákat. Ilyen tulajdonságú összetett számokat teljes Lucas pszeudoprimeknek nevezzük és halmazukat $CP[A,B]$ -vel fogjuk jelölni. DUPARC (1955) bizonyította, hogy az (1), (2) és (3) kongruenciák lineárisan függőek (mod n), vagyis ha egy n összetett egész esetén az (1), (2) és (3) kongruenciák közül bármely kettő teljesül, akkor a harmadik kongruencia is teljesül. A Lucas pszeudoprim számok körében egyik nyitott probléma az, hogy a teljes Lucas pszeudoprim számok halmaza, vagyis $CP[A,B]$, végtelen-e? Ez a probléma nehéznek tűnik. Például abban a speciális esetben, amikor A=5 és B=6, az $n \in CP[5,6]$ állítás egyenértékű azzal, hogy n egyidejűleg kielégíti az

$$2^{n-1} \equiv 1 \pmod{n}$$

és

$$3^{n-1} \equiv 1 \pmod{n}$$

kongruenciákat. Még nem tudjuk, hogy a fenti kongruenciák teljesülnek-e végtelen sok összetett egészre (lásd ROTKIEWICZ (1972/a), 23. probléma), az azonban ismert, hogy a 25.10^9 -nél kisebb számok között 4709 darab ilyen tulajdonságú n természetes szám létezik (lásd pl. POMERANCE, SELFRIDGE, WAGSTAFF, Jr. (1980)). ROTKIEWICZ (1972/b) bizonyította, hogy ha R(A,B) nem degenerált Lucas sorozat, amelyre B=1 vagy B=-1, akkor végtelen sok teljes Lucas pszudoprim szám létezik, vagyis $CP[A,\pm 1]$ végtelen halmaz. Ezt az eredményt egy korábbi cikkben, illetve egy P.KISS és E.LIEUWENS szerzőkkel közösen írt dolgozatban megjavítottuk, bizonyítva, hogy tetszőleges $a,s > 1$ és A egészek esetén $CP[A,\pm 1]$ végtelen sok olyan Euler Lucas pszeudoprim számot tartalmaz, mely pontosan s különböző

ax+1 alakú primszám szorzata (lásd BUI MINH PHONG (megjelenés alatt) és P.KISS, BUI MINH PHONG, E.LIEUWENS (1986)).

Ebben a dolgozatban megadjuk a szükséges és elégséges feltételét annak, hogy egy természetes számra $n \in CP[A,B]$ fennálljon és kapcsolatokat mutatunk meg az $EP[A,B]$, $CP[A,B]$ és $EP[B]$ halmazok között.

Először megjegyezzük, hogy minden $n \in P[A,B]$ szám egyértelműen írható $n = n_R \cdot n_S$ alakban, ahol n_R és n_S pozitív egészek, amelyekre a következő feltételek teljesülnek:

(i) $$\left(n_R,\ n_S\right) = 1$$

(ii) $$R_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n_R}$$

és

(iii) $$S_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n_S} .$$

Valóban $n \in P[A,B]$ feltételből következik, hogy n páratlan szám és így a sorozatok explicit alakja alapján

(6) $$R_{n-(D/n)} = R_{\frac{n-(D/n)}{2}} \cdot S_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n} .$$

Mivel minden $k \geq 1$ esetén $\left(R_k, S_k\right) = 1$ vagy 2, ezért (6) miatt a fenti felbontás lehetséges és nyilvánvalóan egyértelmű.

Felhasználva ezen jelöléseket, a következőket fogjuk bizonyítani.

1. TÉTEL. Legyenek R(A,B) és S(A,B) nem degenerált Lucas sorozatok, és legyen $n = n_R \cdot n_S$ egy Lucas pszeudoprim, amelyre az (i), (ii) és (iii) feltételek teljesülnek.

n akkor és csak akkor teljes Lucas szeudoprim. szám, ha

$$(7) \qquad B^{\frac{n-1}{2}} \equiv 1 \pmod{n_R} \quad \text{és} \quad B^{\frac{n-1}{2}} \equiv -1 \pmod{n_S} .$$

2. TÉTEL. Legyenek R(A,B) és S(A,B) nem degenerál Lucas sorozatok. Ekkor az

a/ n teljes Lucas pszeudoprim $(n \in CP[A,B])$

b/ n Euler Lucas pszeudoprim $(n \in EP[A,B])$

c/ n Euler pszudoprim B vonatkozásában $(n \in EP[B])$

állítások függőek, vagyis közöttük bármely kettőből következik a harmadik. Másszóval

$$CP[A,B] \cap EP[A,B] = CP[A,B] \cap EP[B] = EP[A,B] \cap EP[B] =$$
$$= CP[A,B] \cap EP[A,B] \cap EP[B] .$$

A továbbiakban legyen

$$PP[A,B] = CP[A,B] \cap EP[A,B] \cap EP[B]$$

és nevezzük az $n \in PP[A,B]$ számokat tökéletes Lucas pszudoprimeknek.

Euler Lucas pszeudoprim számok mintájára vezessünk be egy új típusú Lucas pszeudoprim fogalmat. Mivel (4) és (5) teljesül minden primszámra és ha n primszám (n,2BD=1) feltétellel, akkor

$$B^{\frac{n-1}{2}} \equiv (B/n) \pmod{n} ,$$

ezért primek esetén (4) és (5) az

(8) $$R_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \quad \text{ha} \quad B^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

vagy

(9) $$S_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \quad \text{ha} \quad B^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

kongruenciákkal egyenértékű. Legyen n olyan összetett szám, melyre (n,2BD)=1 és

$$B^{\frac{n-1}{2}} \equiv 1 \pmod{n} \quad \text{vagy} \quad B^{\frac{n-1}{2}} \equiv -1 \pmod{n} .$$

Ekkor az n számot Gauss Lucas pszeudoprimnek nevezzük, ha (8) vagy (9) fennáll. Megyjegyezzük, hogy Euler Lucas pszeudoprim és Gauss Lucas pszeudoprim fogalmak különbözőek, vagyis nem mindig következnek egymásból. Például az A=17 és B=35 esetén $n=17.73=1241 \in EP[17,35]$, de n=1241 nem Gauss Lucas pszudoprim szám, mert

$$35^{620} \equiv 1004 \pmod{1241} .$$

A továbbiakban az összes Gauss Lucas pszeudoprimek halmazát $GP[A,B]$-vel fogjuk jelölni. Érvényesek a következő állítások.

3. TÉTEL. Legyenek R(A,B) és S(A,B) nem degenerált Lucas sorozatok. Ekkor

a/ Ha n tökéletes Lucas pszeudoprim, akkor n Gauss Lucas pszeudoprim.

b/ Ha n Gauss Lucas szeudoprim, akkor n teljes pszeudoprim.

Másszóval: $PP[A,B] \subseteq GP[A,B] \subseteq CP[A,B]$.

4. TÉTEL. Legyenek R(A,B) és S(A,B) nem degenerált Lucas sorozatok, amelyekre B=1 vagy B=-1. Továbbá legyenek $a,s > 1$ természetes számok. Ekkor végtelen sok tökéletes Lucas pszeudoprim szám létezik, mely pontosan s különböző ax+1 alakú primszám szorzata. Másszóval $PP[A,\pm 1]$ végtelen sok $n=p_1 \ldots p_s$ alakú elemet tartalmaz, ahol $p_1,\ldots,p_s$ különböző ax+1 alakú primszámok.

MEGJEGYZÉSEK. 1. A 4. Tétel állítása B=1 és B=-1 esetekben nyilvánvalóan igaz a $GP[A,\pm 1]$ és $CP[A,\pm 1]$ halmazokra is.

2. Megjegyezzük, hogy R(A,B) és S(A,B) sorozatok explicit előállítása alapján könnyen igazolhatók a következő összefüggések

$$R_n - (D/n)\, B^{\frac{n-1}{2}} = R_{\frac{n-(D/n)}{2}} \cdot S_{\frac{n+(D/n)}{2}} \qquad (10)$$

(11) $$R_n + (D/n)\, B^{\frac{n-1}{2}} = R_{\frac{n+(D/n)}{2}} \cdot S_{\frac{n-(D/n)}{2}} ,$$

amelyeket fel fogunk használni a bizonyításokban.

Most rátérünk a tételek bizonyítására.

1. TÉTEL BIZONYÍTÁSA. Legyen $n = n_R\, n_S \in P[A,B]$, amelyre az (i), (ii) és (iii) feltételek teljesülnek. Így (10) és (11) alapján

(12) $$R_n \equiv (D/n)\, B^{\frac{n-1}{2}} \pmod{n_R}$$

és

(13) $$R_n \equiv -(D/n)\, B^{\frac{n-1}{2}} \pmod{n_S}$$

következik.

Legyen n teljes Lucas pszeudoprim szám, vagyis tegyük fel, hogy n-re az (1), (2) és (3) kongruenciák teljesülnek. Így (12), (13) és (2) alapján valóban (7) következik.

Fordítva, tegyük fel, hogy (7) teljesül. Ekkor (7) és (12), valamint (7) és (13) alapján

$$R_n \equiv (D/n) \pmod{n_R} \quad \text{és} \quad R_n \equiv (D/n) \pmod{n_S} ,$$

amiből (i) alapján

$$R_n \equiv (D/n) \pmod{n} .$$

Tehát n kielégíti a (2) kongruenciát és n megválasztása miatt nyilván (1)-et is, amiből DUPARC említett eredménye alapján következik, hogy n teljes Lucas pszeudoprim szám.

2. TÉTEL BIZONYÍTÁSA. Legyen n egy teljes Lucas és emellett Euler Lucas pszeudoprim szám. Ha (B/n)=1, akkor (2), (4) és (10) alapján

$$B^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

következik. Ha pedig (B/n)=-1, akkor (2), (5) és (11) alapján

$$B^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

következik. Tehát mindkét esetben

$$B^{\frac{n-1}{2}} \equiv (B/n) \pmod{n} ,$$

vagyis n egy Euler pszeudoprim B vonatkozásában.

Most legyen n egy teljes Lucas pszeudoprim és emellett B vonatkozású Euler pszeudoprim. Ekkor BAILLIE és WAGSTAFF, Jr. (1980) egyik eredménye (Theorem 5., p. 1397) alapján n valóban Euler Lucas pszeudoprim szám.

Végül legyen n egy Euler Lucas és emellett B vonatkozású Euler pszeudoprim szám. Mivel n Euler pszeudoprim B vonatkozásában, ezér a definició szerint

$$B^{\frac{n-1}{2}} \equiv (B/n) \pmod{n} . \tag{14}$$

Így (4), (10) és (14), valamint (5), (11) és (14) alapján valóban (2) kongruencia következik. Tehát DUPARC eredménye alapján n valóban teljes Lucas pszeudoprim szám, mert (1) nyilván teljesül minden Euler Lucas

pszeudoprim esetén.

3. TÉTEL BIZONYÍTÁSA a/ Legyen n egy tökéletes Lucas pszeudoprim szám. Ekkor n Euler Lucas pszeudoprim és B vonatkozású Euler pszeudoprim szám. Így

$$R_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \quad \text{ha} \quad B^{\frac{n-1}{2}} \equiv (B/n) = 1 \pmod{n}$$

vagy

$$S_{\frac{n-(D/n)}{2}} \equiv 0 \pmod{n}, \quad \text{ha} \quad B^{\frac{n-1}{2}} \equiv (B/n) = -1 \pmod{n},$$

amiből következik, hogy n valóban Gauss Lucas pszeudoprim.

b/ Legyen n egy Gauss Lucas pszeudoprim szám, vagyis tegyük fel, hogy (8) vagy (9) teljesül. Ha (8) teljesül, akkor $n_R = n$, $n_S = 1$ és így (7) érvényes. Ha pedig (9) teljesül, akkor $n_R = 1$, $n_S = n$ és így (7) ismét fennáll. Tehát az 1. Tétel alapján n valóban teljes Lucas pszeudoprim szám.

4. TÉTEL BIZONYÍTÁSA. Kiss Péterrel és Erik Lieuwens-szel közösen bizonyítottuk, hogy ha az R(A,B) Lucas sorozat nem degenerált és $D=A^2-4B > 0$, akkor tetszőleges $a,s > 1$ természetes számok esetén végtelen sok Euler Lucas pszeudoprim szám létezik, mely pontosan s különböző ax+1 alakú primszám szorzata (lásd P.KISS, BUI MINH PHONG, E.LIEU-

WENS (1986), Theorem 1.).

Ha egy Lucas sorozatban B=1 vagy B=-1 és nem degenerált, akkor $D=A^2-4B = A^2\pm4 > 0$. Ezért $B = \pm 1$ esetén a fenti eredmény alapján végtelen sok olyan Euler Lucas pszeudoprim létezik, mely pontosan s különböző 4ax+1 alakú primszám szorzata. Nyilvánvaló, hogy ezek is Euler pszeudoprimek $B = \pm 1$ vonatkozásában. Ebből 2. Tétel alapján az állításunk már következik.

FELHASZNÁLT IRODALOM

BAILLIE R., WAGSTAFF S.S.,JR. (1980), Lucas pseudoprimes, Math.Comp., 35.,pp.1391-1417.

BUI MINH PHONG, Lucas és Lehmer pszeudoprim számokról, Matematikai Lapok, 33., 1982-1985, megjelenés alatt.

DUPARC H.J.A. (1955), On almost primes of the second order, Report Z.W. 1955-013, Math. Center, Amsterdam, pp. 1-13.

KISS P., BUI MINH PHONG, E. LIEUWENS, On Lucas pseudoprimes which are products of s primes, Fibonacci numbers and their applications, (ed. by A.N. Philippou, G.E. Bergum, A.F. Horadam), D. Reidel Publ. Comp., Dordrecht-Boston-Lancaster-Tokyo, 1986, pp. 131-139.

LEHMER D.H. (1930), An extended theory of Lucas' functions, Ann. Math., 31., pp. 419-448.

LIEUWENS E. (1971), Fermat pseudoprimes, Doctor thesis, Delft.

POMERANCE C., SELFRIDGE J.L., WAGSTAFF S.S. Jr. (1980), The pseudoprimes to 25.10^9m Math.Comp., 35., pp.1003-1026.

ROTKIEWICZ A. (1972/a), Pseudoprime numbers and their generalizations, Univ. of Novi Sad.

ROTKIEWICZ A. (1972/b), On pseudoprimes with respect to the Lucas sequences, Bull.Acad.Polon.Sci.Ser.Sci.Math.Astr.Phys., 21., pp. 793-797.