KISS PÉTER

A LUCAS SZÁMOK PRIMOSZTÓIRÓL*

Abstract: **(On prime divisors of Lucas numbers)** Let R be a non-degenerate Lucas sequence defined by $R_n=A.R_{n-1}+B.R_{n-2}$ $(n>1)$, where $R_0=0$, $R_1=1$ and A, B are fixed integers.
Donate by r(p) the rank of the apparition of a prime p in the sequence, that is $p \mid R_{r(p)}$ but $p \nmid R_m$ for $0<m<r(p)$. It is known that if p is a prime with (p,B)=1, then r(p) exists, (i.e. there are terms divisible by p) and $r(p) \mid \left[p-(D/p)\right]$, where (D/p) is the Legendre-symbol and $D=A^2+4B$. In an earlier paper we proved that $\left[p-(D/p)\right]/r(p)$ is undbounded if p tends to infinity. Now we show: (i) for almost all primes p we have $\left[p-(D/p)\right]/r(p) > q\left[r(p)\right]$, where q(x) is a non decreasing arithmetical function with

$$q(n)/\log n \longrightarrow 0 \text{ if } n \longrightarrow \infty ;$$

(ii) for any δ with $0<\delta<1$ the set of primes p for which $\left[p-(D/p)\right]/r(p) > \delta.\log p$ $\left[\text{or } r(p) < p/(\delta.\log p)\right]$ has positive density in the set of all primes; (iii) the set of integers n, for which each primitive prime divisor of R_n is is greater than $\delta.n.\log n$ (where $0<\delta<1$), has positive density (p is a primitive prime divisor of R_n if r(p)=n).

---

* A kutatást (részben) az Országos Tudományos Kutatási Alap 273. sz. pályázata támogatta.

Legyenek A és B rögzített zérustól különböző egész számok. Definiáljunk egy $R=\{R_n\}_{n=0}^{\infty}$ sorozatot az $R_0=0$, $R_1=1$ kezdő elemekkel és az

$$R_n = A\,R_{n-1}+B\,R_{n-2} \quad (n > 1)$$

rekurzív formulával. Az R sorozatot A, B paraméterekkel megadott Lucas sorozatnak, tagjait pedig Lucas számoknak nevezzük. Jelöljük a sorozat

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

definiáló polinomjának gyökeit α ill. β -val. Ha $D=A^2+4B\neq 0$ és α / β nem egységgyök, akkor a sorozatot nemdegeneráltnak nevezzük.

A továbbiakban feltesszük, hogy R nem degenerált sorozat, mert belátható, hogy a degenerált sorozatok leírhatók mértani, illetve bizonyos értelemben periodikus sorozatok segítségével. A Lucas sorozat A=B=1 speciális esetét Fibonacci sorozatnak nevezzük.

A Lucas, illetve a Fibonacci sorozatnak igen sok elemi tulajdonságát ismerjük, manapság is sokan foglalkoznak ezekkel a sorozatokkal. Néhány tulajdonságot, melyekre a későbbiek során szükségünk lesz, felsorolunk, a bizonyítások és további elemi tulajdonásgok megtalálhatók például D.H.Lehmer (1930) cikkében.

Ismert, hogy ha p egy primszám $p \nmid B$ feltétellel, akkor a sorozatban van p-vel osztható tag. Ezek közül a legkisebb indexű tag indexét r(p)-vel jelöljük és p előfordulási rendjének nevezzük.

Tehát $p \mid R_{r(p)}$, de $p \nmid R_i$, ha $0 < i < r(p)$.

Ha p egy primszám és valamely n esetén $p \mid R_n$, de $p \nmid R_m$ ha $0 < m < n$, akkor p-t az R_n tag egy primitív primosztójának nevezzük. Így p primitív primosztója az $R_{r(p)}$ tagnak.

$r(p)$ meghatározása általában igen nehéz. Azt azonban tudjuk, hogy ha $p \nmid BD$ akkor $r(p) \mid \left(p-(D/p)\right)$, ahol $D=A^2+4B$ és (D/p) a Legendre-szimbólum; továbbá $r(p)=p$ ha $p \mid D$. Ezek alapján felvetődik a kérdés, vajon

$$g(p) = \frac{p-(D/p)}{r(p)}$$

milyen egész értékeket vehet fel? D. JARDEN (1958) bizonyította, hogy a Fibonacci sorozat esetén $g(p)$ függvény nem korlátos, vagyis tetszés szerinti nagy számnál nagyobb értékeket is felvesz. Ezt az eredményt Bui Minh Phong-gal közösen (P.KISS and B.M.PHONG, 1978) kiterjesztettük tetszésszerinti nem degenerált Lucas sorozatra. Megmutattuk, hogy $g(p)$ nem korlátos függvény, továbbá hogy minden elég nagy p primre

$$g(p) < c\,\frac{p}{\log p},$$

ahol c egy A és B-től függő konstans. Nyitott maradt viszont az a probléma, hogy véges vagy végtelen azon primek száma, melyekre $g(p)=1$, azaz $r(p)=p-(D/p)$? Vagy felvesz-e $g(p)$ gyakran viszonylag kis értékeket?

A következőkben megmutatjuk, hogy $g(p)$ "majdnem minden" primre "nagy". Bebizonyítjuk, hogy ha p az R_n tag primitív primosztója, akkor $g(p)$ nagyságrendje "általában" nagyobb, mint $\log n$. A következő tételt bizonyítjuk.

<u>1. TÉTEL.</u> Legyen R egy nem degenerált Lucas sorozat és legyen $q(x)$ egy pozitív értékű nem csökkenő számelméleti függvény, melyre

$$\lim_{n\to\infty} \frac{q(n)}{\log n} = 0.$$

Jelöljük R(n)-nel

$$Q_n = R_1 . R_2 . . . R_n$$

különböző primosztóinak számát és jelölje H(n) a Q_n azon p primosztóinak számát, melyekre

$$\frac{p-(D/p)}{r(p)} > q\left[r(p)\right].$$

Ekkor

$$\lim_{n \to \infty} \frac{H(n)}{R(n)} = 1 .$$

Megjegyezzük, hogy a tételben szereplő Q_n nem zérus. Ugyanis a Lucas sorozat tagjait, mint ismert, $R_n = (\alpha^n - \beta^n)/(\alpha-\beta)$ alakban is megadhatjuk, amiből következik, hogy nem-degenerált sorozat esetén $R_n \neq 0$ ha $n > 0$.

Tételünkből, illetve annak bizonyításából néhány következmény adódik.

1. KÖVETKEZMÉNY. Legyen R egy nem degenerált Lucas sorozat és legyen q egy tetszőleges rögzített pozitív valós szám. Ekkor $g(p) > q$ majdnem minden p primre.

2. KÖVETKEZMÉNY. Legyen R egy nem degenerált Lucas sorozat és δ egy rögzített valós szám $0 < \delta < 1$ feltétellel. Legyenek Q_n és R(n) a tételben definiált természetes számok, továbbá jelöljük S(n)-nel, illetve T(n)-nel Q_n azon primosztóinak számát, melyekre

$$\frac{p-(D/p)}{r(p)} > \delta \log p$$

illetve

$$r(p) < \frac{1}{\delta} \cdot \frac{p}{\log p} .$$

Ekkor

(1) $$\liminf \frac{S(n)}{R(n)} = 1 - \delta$$

és

(2) $$\liminf \frac{T(n)}{R(n)} = 1 - \delta .$$

Az 1. Tétel és a következmények bizonyításában alkalmazott módszer arra is használható, hogy következtethessünk a Lucas számok primitív primosztóinak nagyságára.

A Lucas számok, illetve általában a lineáris rekurzív sorozatok tagjainak legnagyobb primosztóival és ezek becslésével már többen foglalkoztak, többek között MAHLER (1934); SCHINZEL (1967) és STEWART (1982). A Lucas számokra vonatkozó legjobb eredményt eddig SHOREY és STEWART (1981) érték el. A következőket bizonyították: Jelöljük $\omega(n)$-nel az n természetes szám különböző primosztóinak számát és vezessük be a $q(n)=2^{\omega(n)}$ jelölést. Legyen P_n az R_n Lucas szám legnagyobb primosztója. Ekkor minden $0 < k < 1/\log 2$ feltételt kielégítő k valós és minden olyan n (>3) természetes szám esetén, melynek legfeljebb k.log log n különböző primtényezője van,

$$P_n > c\,(\varphi(n).\log n)/q(n) ,$$

ahol c egy A, B és k-tól függő, effektív kiszámítható konstans és φ az Euler-féle függvény. Továbbá "majdnem minden" n természetes szám esetén

$$P_n > n\,(\log n)^2/f(n) \log\log n ,$$

ahol f(x) egy olyan tetszőleges valós értékű függvény, melyre $f(n) \longrightarrow \infty$ ha $n \longrightarrow \infty$.

Az alábbiakban a Lucas számok primitív primosztóira a következő tételt bizonyítjuk.

2. TÉTEL. Legyen δ egy tetszőleges, $0 < \delta < 1$ feltételt kielégítő valós szám és jelöljük V(n)-nel az R sorozat $R_1, R_2, \ldots, R_n$ tagjai között azoknak az R_i tagoknak a számát, melyeknek minden p primitív primosztójára

$$p \geq \delta \, i \log i .$$

Ekkor

$$\liminf \frac{V(n)}{n} \geq 1-\delta .$$

Megjegyezzük, hogy a 2. Tétel a Lucas számok primitív primosztóira gyengébb alsó korlátot ad, mint Stewart idézett eredménye. Stewart azonban csak a legnagyobb primosztókra adott alsó becslést, a mi eredményünk viszont minden primitív primosztóra vonatkozik.

Rátérünk az eredmények bizonyítására.

1. TÉTEL BIZONYÍTÁSA. Használva a tétel jelöléseit, legyen p a Q_n egy primosztója. Így nyilván $r(p) \leq n$. Ha

$$\frac{p-(D/p)}{r(p)} \leq q(r(p)) , \tag{3}$$

akkor

$$p \leq r(p).q(r(p))+(D/p) \leq n.q(n)+1 .$$

Ezért a primszámtételből következik, hogy Q_n azon primosztóinak száma, melyekre (3) fennáll, kisebb mint

$$(1+\varepsilon)\frac{n.q(n)}{\log(n.q(n))} = \Pi(n) , \tag{4}$$

ahol $\varepsilon \longrightarrow 0$, ha $n \longrightarrow \infty$. Ebből következik, hogy

$$H(n) > R(n) - \bar{H}(n),$$

ezért csak azt kell bizonyítani, hogy

$$\lim_{n \to \infty} \frac{\bar{H}(n)}{R(n)} = 0 . \tag{5}$$

STEWART (1977) bizonyította, hogy létezik egy n_0 pozitív konstans úgy, hogy minden $n \geq n_0$ és nem degenerált Lucas sorozat esetén az R_n tagnak van primitív primosztója.

Ezért $R(n) > n-n_0$, ha n elég nagy és így (4) alapján

$$\frac{\bar{H}(n)}{R(n)} < \frac{2.n.q(n)}{(\log n+\log q(n))(n-n_0)} < 3.\frac{q(n)}{\log n},$$

amiből q(n) definiciója miatt (5) következik. Az előzőek alapján ebből már következik a tétel állítása.

A KÖVETKEZMÉNYEK BIZONYÍTÁSA. Az 1. Következmény nyilvánvaló, mivel a q(x)=q konstans függvény kielégíti az 1. Tétel feltételeit. Ezért csak a 2. Következményt kell bizonyítani.

Legyen n elég nagy $(>n_0)$. Ha Q_n egy p primosztójára

$$\frac{p-(D/p)}{r(p)} \leq \delta \log p ,$$

akkor $r(p) \leq n$ miatt

$$p \leq \delta.n.\log p + 1$$

és

$$\frac{p}{\log p} \leq \delta.n + \frac{1}{\log p}$$

következik. Ez azonban csak akkor teljesül, ha

$$p \leqq (\delta+\varepsilon)n.\log n \;,$$

ahol ε tetszőlegesen kicsi, ha p vagy r(p), illetve n elég nagy. Ezek alapján, az 1. Tétel bizonyításában használt gondolatmenethez hasonlóan

$$S(n) \geqq R(n) - (\delta+\varepsilon').n$$

illetve

$$\frac{S(n)}{R(n)} \geqq 1 - \delta - \varepsilon'$$

adódik, ahol ε' tetszőlegesen kicsi, ha n elég nagy. Ebből (1) már következik és (2) hasonlóan bizonyítható.

<u>2. TÉTEL BIZONYÍTÁSA.</u> Ha az R sorozat valamely R_i tagjának van olyan p primitív primosztója, melyre

$$p \leqq \delta \; i \; \log \; i \;,$$

akkor erre nyilván

$$p \leqq \delta \; n \; \log \; n$$

is teljesül. Ezen primek száma azonban a primszámtétel alapján nyilván kisebb mint $(\delta+\varepsilon).n$, ahol ε tetszőlegesen kicsi, ha n elég nagy. Így

$$V(n) > n - (\delta + \varepsilon).n \;,$$

amiből már következik az állítás.

FELHASZNÁLT IRODALOM

D. JARDEN, Recurring sequences, Riveon Lematematika, Jerusalem, Israel, 1958.

P. KISS and B.M.PHONG, On a function concerning second order recurrences, Ann. Univ. Sci. Budapest Eötvös 21, 1978, 119-122.

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

K. MAHLER, Eine arithmetische Eigenschaft der rekurrierenden Reihen, Mathematica (Leiden) 3, 1934-35, 153-156.

A. SCHINZEL, On two theorems of Gelfond and some of their applications, Acta Arith. 13, 1967, 177-236.

T.N. SHOREY and C.L. STEWART, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, II, J. London Math. Soc. (2) 23, 1981, 17-23.

C.L. STEWART, On divisors of terms of linear recurence sequences, J. reine angew. Math. 333, 1982, 12-31.

C.L. STEWART, Primitive divisor of Lucas and Lehmer numbers, Trascendence Theory: advances and applications, (ed. A. Baker and D. Masser), Acad. Press, London, 1977.