

Lucas-sorozat modulo n

A Fazekas Mihály Gimnázium idei matematika táborában hangzott el a következő feladat:

Legyen L_k a Lucas-sorozat k . tagja ($L_0 = 2, L_1 = 1, L_{n+1} = L_n + L_{n-1}$). Legyen n szép szám ha $n \mid L_n$.

Lehet-e egy szép számnak 3-nál nagyobb prímosztója?

A feladat megoldása maga nem túl bonyolult ha "megsejtjük", hogy $1926 = 2 \cdot 3^2 \cdot 107$ szép szám, annál rögzőbb út vezet a szám megtalálásáig. A cikk során megkísérlünk bemutatni - a Lucas-sorozat modulo n vett meghatározására - néhány módszert, amelyek hasonlóan definiált rekurzív sorozatoknál is hasznosak lehetnek. Ezen kívül bemutatunk néhány szép tételt a feladattal kapcsolatban, mint például, hogy $2 \cdot 3^k$ mindig szép szám vagy, hogy nincs páratlan szép szám.

Ismerkedjünk meg a Lucas-sorozattal! A Lucas-sorozat Fibonacci-típusú¹ sorozat, hiszen minden eleme az előző kettő összege. A Lucas-sorozat első néhány tagja:

n	0	1	2	3	4	5	6	7	8	9	10
L_n	2	1	3	4	7	11	18	29	47	76	123
F_n	0	1	1	2	3	5	8	13	21	34	55

A Lucas-sorozat alá felírtuk a Fibonacci-sorozatot is. A táblázatból két dolgot máris leolvashatunk: $L_n = F_{n+1} + F_{n-1}$ és megtaláltuk az első szép számot is: $6 \mid L_6 = 18$.

A Fibonacci-sorozatnál igen gyakran elmondják, hogy F_n és F_{n+1} relatív prímek. Ez a Lucas-sorozatra is igaz, a bizonyítás ugyanígy megy. Tegyük fel, hogy $d > 1$ -re, hogy $d \mid L_n$ és $d \mid L_{n+1}$. Ekkor $d \mid L_{n+1} - L_n = L_{n-1}$, azaz $d \mid L_n$ és $d \mid L_{n-1}$, és ugyanígy $d \mid L_{n-2}, \dots, d \mid L_1$, ami nem lehetséges, mert $d > 1$.

Kós Géza és Énekes Béla cikkéből (2000. évi 9. szám) azt is tudjuk, hogy egy Fibonacci-típusú sorozat n . tagja felírható $aq_1^n + bq_2^n$ alakban, ahol a, b a sorozatra jellemző számpár, $q_1 = \frac{1+\sqrt{5}}{2}, q_2 = \frac{1-\sqrt{5}}{2}$.

Esetünkben

$$L_0 = aq_1^0 + b \cdot q_2^0 = a + b = 2$$

$$L_1 = aq_1 + bq_2 = \frac{a+b}{2} + (a-b)\frac{\sqrt{5}}{2} = 1$$

Ebből $a = b = 1$ adódik, így

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

vagyis $L_n = q_1^n + q_2^n$, ahol $q_1 + q_2 = 1, q_1 q_2 = -1$. Ismerkedjünk meg egy kicsit a problémával! Próbáljunk ki néhány prímet, nézzük meg, melyek lehetnek szép szám osztói!

Nézzük meg milyen n -re lesz L_n a 2 többszöröse.

n	0	1	2	3	4	5	6	7
$L_n \bmod 2$	2	0	1	0	1	1	0	1

¹Fibonacci-típusú sorozatokról lásd Énekes Béla és Kós Géza cikkét a 2000. évi 9. és 2001. évi 1. számban.

Tehát $2 \mid L_n$ akkor és csak akkor ha $3 \mid n$.

Most nézzük a Lucas-sorozat 3-as maradékát.

$$\begin{array}{cccccccc|cc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ L_n \bmod 3 & 2 & 1 & 0 & 1 & 1 & 2 & 0 & 2 & 2 & 1 \end{array}$$

Itt 8 hosszú periódus van, és $3 \mid L_n$, ha $n = 4k + 2$, ahol k egész.

Az előző két eredményt egybevetve azt kapjuk, hogy szép számot nem oszthat a 4. Tegyük fel ugyanis, hogy m szép szám és $4 \mid m$. Ekkor $m \mid L_m$ miatt $4 \mid L_m$ (így $2 \mid L_m$), ami azt jelenti, hogy $3 \mid m$. Ekkor $3 \mid m$ és $m \mid L_m$ -ből kapjuk, hogy $3 \mid L_m$, így $m = 4k + 2$, ahol k egész, de ez ellentmond annak, hogy m osztható 4-gyel. A 4 tehát valóban nem oszthat szép számot.

Most nézzük meg a Lucas-sorozat 5-ös maradékát:

$$\begin{array}{cccc|cc} n & 0 & 1 & 2 & 3 & 4 & 5 \\ L_n \bmod 5 & 2 & 1 & 3 & 4 & 2 & 1 \end{array}$$

Tehát $5 \nmid L_n$, így persze 5 nem oszthat szép számot.

Vizsgáljuk a 7-es maradékokat:

$$\begin{array}{cccccccccccccccc|cc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ L_n \bmod 7 & 2 & 1 & 3 & 4 & 0 & 4 & 4 & 1 & 5 & 6 & 4 & 3 & 0 & 3 & 3 & 6 & 2 & 1 \end{array}$$

Tehát a 7-es maradék esetén 16 hosszú periódus van, és $7 \mid L_n$, ha $n = 8k + 4$. Ez azt jelenti, hogy ha 7 oszt egy m szép számot, akkor $7 \mid L_m$, így $4 \mid m$, ami nem lehetséges, amint azt már bebizonyítottuk.

Vizsgáljuk meg a Lucas-sorozat 11-es maradékát.

$$\begin{array}{cccccccccccc|cc} n & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ L_n \bmod 11 & 2 & 1 & 3 & 4 & 7 & 0 & 7 & 7 & 3 & 10 & 2 & 1 \end{array}$$

Tehát itt 10 hosszú periódus van, és $11 \mid L_n$ pontosan akkor, ha $n = 10k + 5$. Így ha 11 oszt egy m szép számot, akkor $5 \mid m$, ami nem lehetséges, amint azt már bebizonyítottuk.

Tehát 4, 5, 7, 11 nem oszthatnak szép számot, ugyanakkor nagyon hasznos volt a fenti vizsgálat, rengeteg sejtésünk lehet. Első és talán legtriviálisabb, hogy a Lucas-sorozat periódikus mod p . Érdekes az is, hogy a p -vel osztható helyek $2t \cdot k + t = (2k + 1)t$ alakúak ($4k + 2, 8k + 4, 10k + 5$). Nem szembetűnő, de észre lehet venni, hogy $p \mid (L_p - 1)$. Térjünk rá most ezek bizonyítására.

Vizsgáljuk először csak a 0 maradék periódikusságát. Megmutatjuk, hogy ha $k \mid L_n$ és $k \mid L_{n+d}$, akkor $k \mid L_{n+2d}$, sőt ha $n \geq d$ akkor $k \mid L_{n-d}$. Nézzük a sorozatot, legyen $L_{n+1} \equiv x \pmod{k}$.

m	$n - d$	\dots	$n - 3$	$n - 2$	$n - 1$	n	$n + 1$	$n + 2$	$n + 3$	\dots	$n + d$
$L_m \bmod k$	$(-1)^{d-1} F_d x$	\dots	$2x$	$-x$	x	0	x	x	$2x$	\dots	$F_d x$

Láthatjuk, hogy ha $L_{n+1} \equiv x \pmod{k}$, akkor

$$L_{n+s} \equiv F_s x \pmod{k} \quad \text{és} \quad L_{n-s} \equiv (-1)^{s-1} F_s x \pmod{k},$$

ahol F_s az s . Fibonacci-szám. Vegyük észre, hogy $(x, k) = 1$, máskülönben L_n és L_{n+1} -nek volna 1-nél nagyobb közös osztója, amiről pedig láttuk, hogy nem lehetséges.

Így, ha $k \mid L_{n+d}$, azaz $k \mid F_d \cdot x$, akkor $k \mid F_d$. Ebből már következik, hogy $k \mid L_{n+2d}$, mert ha $L_{n+d+1} \equiv y \pmod{k}$, akkor $k \mid L_{n+d}$ miatt $L_{(n+d)+d} \equiv F_d \cdot y \equiv 0 \pmod{k}$. Tehát ha $k \mid L_n$ és $k \mid L_{n+d}$, akkor $k \mid L_{n+2d}$. Hasonlóan adódik, hogy ekkor $k \mid L_{n-d}$ és teljes indukcióval kapjuk, hogy $k \mid L_{n+a \cdot d}$ és $k \mid L_{n-b \cdot d}$.

Most térjünk rá a másik állítás bizonyítására, nevezetesen, hogy a k -val osztható Lucas-számok valamilyen megfelelő t -vel $(2s+1)t$ alakú helyeken vannak. Tulajdonképpen csak annyit kell bizonyítani, hogy valamilyen t -re L_t és L_{3t} osztható k -val, mert akkor az előző tétel szerint $L_{5t}, L_{7t}, \dots, L_{(2s+1)t}$ is osztható k -val. Nagyon lendít a dolgokon az az észrevétel, hogy

$$L_{3t} = q_1^{3t} + q_2^{3t} = (q_1^t + q_2^t)^3 - 3q_1^t q_2^t (q_1^t + q_2^t) = L_t^3 - 3(-1)^t L_t,$$

hiszen $L_n = q_1^n + q_2^n$, ahol $q_1 + q_2 = 1$, $q_1 q_2 = -1$, mint azt a Lucas-sorozat megismerésénél láttuk. Így ha $k \mid L_t$, akkor $k \mid L_{3t}$.

Legyen ezután t a legkisebb pozitív szám, amelyre $k \mid L_t$. Ekkor $k \mid L_{3t}$ és így $k \mid L_{2t \cdot s + t}$. Másrészt $k > 2$ esetén k nem osztja L_{2t} számot, mert

$$L_{2t} = q_1^{2t} + q_2^{2t} = (q_1^t + q_2^t)^2 - 2q_1^t q_2^t = L_t^2 - 2(-1)^t.$$

Tegyük fel, hogy van olyan v , amelyre $k \mid L_v$ és v nem $(2s+1)t$ alakú. Ekkor van olyan s , amelyre $d = |2ts + t - v| \leq t$. Ha itt egyenlőség áll, akkor $v = 2at$. Mivel L_{2at} és $L_{(2a+1)t}$ is osztható k -val, így L_{2t} is, ami nem lehet $k > 2$ esetén. Ha nem áll fenn egyenlőség, akkor L_v és $L_{v \pm d}$ is osztható k -val, így L_{v-md} is, azaz $L_{(v \bmod d)}$ is, de mivel $d < t$, így $v \bmod d$ vagy 0- ekkor $k \mid L_d < L_t$ - vagy $0 < v \bmod d < t$, ekkor $k \mid L_{(v \bmod d)} < L_t$, ami ellentmond annak, hogy t a legkisebb szám, amelyre $k \mid L_t$. Tehát ha $k \mid L_n$, akkor $n = (2s+1)t$.

Még egy dolgot bizonyíthatunk abból, hogy $L_{3n} = L_n^3 - 3(-1)^n L_n$. Legyen m 3-mal osztható szép szám, vagyis $m \mid L_m$ és $m = 3m_1$, ekkor $L_m = 3m_1 \cdot h$.

$$L_{3m} = L_m^3 - 3(-1)^m L_m = (3m_1 \cdot h)^3 - 3(-1)^m 3m_1 h = 9m_1 (3m_1^2 h^3 - (-1)^m h)$$

vagyis $9m_1 \mid L_{9m_1}$. Vagyis ha m 3-mal osztható szép szám, akkor $3m$ is az. Mivel $6 \mid L_6 = 18$ és 6 osztható 3-mal, így 18 is szép szám. Teljes indukcióval bizonyítható, hogy $2 \cdot 3^k$ is szép szám, ahol k pozitív egész. Mivel $2 \cdot 3^k \mid L_{2 \cdot 3^k}$, így a fentiek alapján $2 \cdot 3^k \mid L_{2 \cdot 3^k (2s+1)}$.

Tehát azt már tudjuk, hogy a k -val osztható Lucas-számok a $t(2s+1)$ alakú helyeken vannak, de magáról a t -ről nem tudunk semmit. Ezen segít ha bebizonyítjuk a harmadik megsejtett állítást, mely szerint minden p prímre $p \mid (L_p - 1)$. Elsőre nem tűnik könnyűnek ennek bizonyítása, de a binomiális tétel segít:

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots + \binom{n}{1} a b^{n-1} + b^n.$$

Ebből a Lucas-sorozat n . tagja:

$$L_n = \left(\frac{1+\sqrt{5}}{2} \right)^n + \left(\frac{1-\sqrt{5}}{2} \right)^n = \frac{1}{2^n} 2 \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} 5^k.$$

Ha $0 < k < p$ akkor $\binom{p}{k}$ osztható p -vel, mert $\frac{p!}{k!(p-k)!} = \binom{p}{k}$ számlálója osztható p -vel, nevezője pedig nem. Másrészt a Fermat-tételből $p > 2$ esetén $2^{p-1} \equiv 1 \pmod{p}$.

Tehát minden p páratlan prímmre:

$$L_p \equiv 2^{p-1} L_p = \sum_{k=0}^{\lfloor \frac{p}{2} \rfloor} \binom{p}{2k} 5^k \equiv \binom{p}{0} 5^0 \equiv 1 \pmod{p}.$$

Az állítás $p = 2$ -re is igaz, hiszen $L_2 = 3 \equiv 1 \pmod{2}$.

Ne álljunk meg azonban itt, ezzel a módszerrel meghatározható L_{p+1} maradéka is p -vel osztva. Használjuk fel, hogy $\binom{p+1}{k} = \binom{p}{k} + \binom{p}{k-1}$. Ekkor $p \neq 5$ esetén

$$\begin{aligned} 2L_{p+1} \equiv 2^p L_{p+1} &= \sum_{k=0}^{(p+1)/2} \binom{p+1}{2k} 5^k = \binom{p+1}{0} 5^0 + \sum_{k=1}^{(p+1)/2} \left(\binom{p}{2k} + \binom{p}{2k-1} \right) 5^k \equiv \\ &\equiv \binom{p+1}{0} 5^0 + \binom{p}{p} 5^{(p+1)/2} = 1 + 5^{(p+1)/2} \pmod{p}. \end{aligned}$$

Mivel $5^{p-1} \equiv 1 \pmod{p}$, így $5^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Megjegyezzük bizonyítás nélkül², hogy $5^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, ha $p = 5k \pm 1$ és $5^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, ha $p = 5k \pm 2$.

Tehát két eset van.

1. eset: $p = 5k \pm 1$. Ekkor $2L_{p+1} \equiv 1 + 5 = 6 \pmod{p}$, ezért $L_{p+1} \equiv 3 \pmod{p}$. Így $L_{p-1} = L_{p+1} - L_p \equiv 3 - 1 = 2 \pmod{p}$. Tehát

$$L_n \pmod{p} \begin{array}{cccc|ccc} n & 0 & 1 & \dots & p-1 & p & p+1 \\ & 2 & 1 & \dots & 2 & 1 & 3 \end{array}$$

Itt tehát $(p-1)$ hosszú periódus van. (Persze nem biztos, hogy ez a legkisebb periódus.)

2. eset: $p = 5k \pm 2$. Ekkor $2L_{p+1} \equiv 1 - 5 = -4 \pmod{p}$, így $L_{p+1} \equiv -2 \pmod{p}$. Ebben az esetben $L_{p+2} = L_{p+1} + L_p \equiv -2 + 1 = -1 \pmod{p}$. Tehát

$$L_n \pmod{p} \begin{array}{cccc|ccc|cc} n & 0 & 1 & \dots & p & p+1 & p+2 & \dots & 2p+2 & 2p+3 \\ & 2 & 1 & \dots & 1 & -2 & -1 & \dots & 2 & 1 \end{array}$$

Azaz $L_k \equiv -L_{k+(p+1)} \equiv L_{k+2(p+1)} \pmod{p}$ vagyis ebben az esetben $2(p+1)$ hosszú periódus van.

Ezek az eredmények egybevágóak korábbi megfigyeléseinkkel, melyek szerint $p = 3$ esetén 8 hosszú, $p = 7$ esetén 16 hosszú, $p = 11$ esetén 10 hosszú periódus van.

Legyen t a legkisebb pozitív szám, amelyre $p \mid L_t$, ekkor $p \mid L_{t+p-1}$ vagy $p \mid -L_{t+p+1}$, azaz $p \mid L_{t+p+1}$. Így $2t \mid p-1$ vagy $2t \mid p+1$. Vagyis $t \leq \frac{p-1}{2} < \frac{p+1}{2}$ vagy $t \leq \frac{p+1}{2}$, mindenképpen $t \leq \frac{p+1}{2} < p$. Tegyük fel ezután, hogy m páratlan szép szám, azaz $m \mid L_m$. Legyen q a legkisebb prímosztója m -nek, ekkor $q \mid m$ és $m \mid L_m$ -ből kapjuk, hogy $q \mid L_m$, ezért van olyan legkisebb t , melyre $q \mid L_t$. A korábbiakból tudjuk, hogy $m = (2s+1)t$ alakú, és mivel q páratlan prím, ezért $t < q$. Ha r a legkisebb prímosztója t -nek, akkor $r \mid t$ és

²Azok részére akik ismeri a kvadratikus maradékokra vonatkozó tételeket: $5^{\frac{p-1}{2}} \equiv \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1 \pmod{5}$ ha $p = 5k \pm 1$. Ha pedig $p = 5k \pm 2$, akkor $\left(\frac{p}{5}\right) = -1$.

$t \mid m$ -ből $r \mid m$, és $r \leq t < q$, ami lehetetlen, mert q az m legkisebb prímosztója. Tehát nem létezik páratlan szép szám³.

Ha olyan szép számot keresünk, amelynek van $p > 3$ prímosztója, akkor figyelniük kell arra, hogy az a legkisebb t , amelyre $p \mid L_t$ szintén osztója a szép számnak. Könnyen adódik a gondolat, hogy t legyen $2 \cdot 3^k$ alakú, mert ezeket már jól ismerjük. Nem elég azonban, hogy $2 \cdot 3^l \mid \frac{p+1}{2}$ vagy $\frac{p-1}{2}$, meg kell mutatnunk, hogy p valóban osztója $L_{2 \cdot 3^k}$ -nak. 5 a legegyszerűbb példa olyan prímre, amely a sorozat egyetlen elemét sem osztja. Tehát találni kell olyan (s, p) párokat, melyekre $p \mid L_s$.

Legyen $p = 5k \pm 1$, erre láttuk, hogy

$$\begin{array}{cccccccccc} n & 0 & 1 & 2 & 3 & \dots & p-4 & p-3 & p-2 & p-1 & p \\ L_n \bmod p & 2 & 1 & 3 & 4 & \dots & -4 & 3 & -1 & 2 & 1 \end{array}$$

Tehát $L_{p-(2a+1)} \equiv L_{2a}$ és $L_{p-2a} \equiv -L_{2a-1} \pmod{p}$. Ha $p = 4a - 1$, akkor $L_{2a-1} \equiv -L_{2a-1} \pmod{p}$, vagyis $L_{2a-1} \equiv 0 \pmod{p}$. Tehát ha $p = 5k \pm 1$ és egyben $4a - 1$ alakú akkor $p \mid L_{\frac{p-1}{2}}$ (pl.: $11 \mid L_5$).

Legyen $p = 5k \pm 2$, erre láttuk, hogy

$$\begin{array}{cccccccccc} n & 0 & 1 & 2 & 3 & \dots & p-2 & p-1 & p & p+1 & p+2 \\ L_n \bmod p & 2 & 1 & 3 & 4 & \dots & 4 & -3 & 1 & -2 & -1 \end{array}$$

Tehát $L_{p+1-2a} \equiv -L_{2a}$ és $L_{p-2a} \equiv L_{2a+1} \pmod{p}$. Ha $p = 4a - 1$, akkor $L_{2a} \equiv -L_{2a} \pmod{p}$, azaz $L_{2a} \equiv 0 \pmod{p}$.

Ez azt jelenti, hogy ha $p = 5k \pm 2$ és ugyanakkor $4a - 1$ alakú prím, akkor $p \mid L_{\frac{p+1}{2}}$ (pl.: $23 \mid L_{12} = 322$).

Legyen $2 \cdot 3^l = \frac{p+1}{2}$ vagy $2 \cdot 3^l = \frac{p-1}{2}$, ahol p egy $4a - 1$ alakú prímszám. Ez utóbbi egyenletnek nincs megoldása, mert a bal oldal páros, a jobb oldal páratlan.

Tehát $2 \cdot 3^l = \frac{p+1}{2}$, ahol $p = 5k \pm 2$ alakú prím. $3^4 \equiv 1 \pmod{5}$ miatt csak azt kell megvizsgálni, hogy $4 \cdot 3^l - 1$ milyen maradékot ad 5-tel osztva, ha $l = 0, 1, 2, 3$. A p akkor lesz $5k \pm 2$ alakú ha $l = 4s$ vagy $l = 4s + 3$, de $l = 4s$ esetén $4 \cdot 3^{4s} - 1 = (2 \cdot 3^{2s} + 1)(2 \cdot 3^{2s} - 1)$, ami nem prím, ha $s \geq 1$.

Maradnak a $p = 4 \cdot 3^{4s+3} - 1$ alakú prímekek. Azt állítjuk, hogy ekkor $m = 2 \cdot 3^{4s+3} \cdot p$ szép szám. Láttuk ugyanis, hogy $2 \cdot 3^k \mid L_{2 \cdot 3^k(2a+1)}$, ugyanakkor $p = 4 \cdot 3^{4s+3} - 1$ egyszerre $4a - 1$ és $5k + 2$ alakú prím, és $m = \frac{p+1}{2}(2b+1)$, így $p \mid L_{\frac{p+1}{2}(2b+1)}$. Tehát L_m -et osztja $2 \cdot 3^{4s+3}$ és $4 \cdot 3^{4s+3} - 1$, így $m \mid L_m$. Tehát m valóban szép szám.

Mivel $4 \cdot 3^3 - 1 = 107$ prím, ezért $54 \cdot 107 = 5778$ szép szám. Már $1926 = \frac{5778}{3}$ is szép szám, mert $107 \mid L_{18} = 5778$. Szintén prím $4 \cdot 3^7 - 1 = 8747$, így 38259378 is szép szám. Sőt $4 \cdot 3^{15} - 1 = 57395627$ is prím, így 1647129028059378 is szép szám.

³Már eddigiekben is azt a konvenciót követtük, hogy az 1 nem szép szám, noha ezt nem mondtuk ki sehol. A fenti bizonyítás triviálisan bukik meg $m = 1$ -re: nincs (legkisebb) prímosztója.

Kiegészítés⁴

Mutatunk egy egyszerű konstukciót szép számok "generálására", ennek lényegét az alábbi állításban foglaltuk össze:

Ha m szép szám, akkor L_m is szép szám!

Tulajdonképpen ezt már eddig is megsejthettük volna, mikor láttuk, hogy $L_6 = 18$ illetve $L_{18} = 5778$ is szép szám.

Valójában ezt az állítást majdnem beláttuk. Láttuk, hogy $L_k \mid L_{(2n+1)k}$, valóban a legkisebb s szám, amelyre $L_k \mid L_s$ az éppen $s = k$ így az L_k -val osztható helyek a $2s \cdot t + s = 2k \cdot t + k = (2t + 1)k$ alakúak. Tegyük fel, hogy m szép szám, azaz $m \mid L_m$, és tegyük fel továbbá, hogy a hányadosuk páratlan szám, ekkor az előzőek szerint $L_m \mid L_{L_m}$, vagyis L_m szép szám. Mindössze azt kell belátni, hogy ha m szép szám, akkor $\frac{L_m}{m}$ páratlan. Azt láttuk a cikk során, hogy m szép szám nem lehet 4-gyel osztható és később azt is láttuk, hogy nem lehet páratlan, vagyis egy szép szám mindig $4k + 2$ alakú. Másrészt ha m páros és szép szám, akkor L_m is páros. L_n paritását vizsgálva láttuk, hogy ez csak úgy lehet, ha m 3-mal is osztható. Tehát egy szép szám mindig osztható 6-tal. Most vizsgáljuk meg az L_n sorozat 4-es maradékát:

$$\begin{array}{cccccccc|cc} n & & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ L_n \text{ mod } 4 & 4 & 2 & 1 & 3 & 0 & 3 & 3 & 2 & 1 \end{array}$$

Látjuk, hogy ekkor 6-hosszú periódus van és ha $6 \mid n$ akkor $L_n \equiv 2 \pmod{4}$. Tehát ha m szép szám akkor L_m $4k + 2$ alakú, ebből pedig következik, hogy $\frac{L_m}{m}$ páratlan. Ebből pedig mint láttuk következik, hogy L_m is szép szám.

Ez szép számok egy érdekes sorozatára ad konstrukciót: 6 szép szám, így L_6 is, így L_{L_6} is, így $L_{L_{L_6}}$ is, $L_{L_{L_{L_6}}}$ is...

⁴Ez a rész nem volt benne az eredeti cikkben.