Lucas-sorozat

Bevezetés. Az alábbi jegyzetben két sorozat számelméleti tulajdonságait hasonlítjuk össze: $2^n + (-1)^n$ és a $q_1^n + q_2^n$, ahol $q_1 = \frac{1+\sqrt{5}}{2}$ és $q_2 = \frac{1-\sqrt{5}}{2}$. Ezutóbbi sorozat a Lucas-sorozat és az $L_{n+1} = L_n + L_{n-1}$, $L_0 = 2$, $L_1 = 1$ rekurziót elégíti ki, míg az előbbi sorozat az $M_{n+1} = M_n + 2M_{n-1}$, $M_0 = 2$, $M_1 = 1$ rekurziót elégíti ki. Továbbiakban néhány egyszerű lemmát bizonyítunk be.

I. lemma: A Lucas-sorozat k-val osztható elemei periódikusan helyezkednek el a sorozatban.

Bizonyítás: Először egy apró megjegyzés: $(L_n, L_{n+1}) = 1$, ez nyilvánvaló, hiszen ha $d \mid L_n$ és $d \mid L_{n+1}$ akkor $d \mid L_{n+1} - L_n$ azaz $d \mid L_{n-1}$ és indukcióból következően $d \mid L_1 = 1$.

Ezután tegyük fel, hogy $k \mid L_n$ és $k \mid L_{n+d}$, megmutatjuk, hogy ekkor $k \mid L_{n+2d}$, illetve ha $n \geq d$ akkor $k \mid L_{n-d}$. Tekintsük a sorozatot, legyen $L_{n+1} \equiv x \pmod{k}$.

m	$n-d$	$\ldots$	$n-2$	$n-1$	n	$n+1$	$n+2$	$\ldots$	$n+d$
$L_m \mod k$	$(-1)^{d-1}F_d x$	$\ldots$	$-x$	x	0	x	x	$\ldots$	$F_d x \equiv 0$

Tehát ha $L_{n+1} \equiv x \pmod{k}$, akkor $L_{n+s} \equiv F_s x \pmod{k}$ és $L_{n-s} \equiv (-1)^{s-1} F_s x \pmod{k}$, ahol F_s az s. Fibonacci szám. $(x, k) = 1$, különben L_n és L_{n+1}-nek lenne 1-nél nagyobb közös osztója, ami nem lehet. Tehát $k \mid F_d$. Ebből már következik, hogy $k \mid L_{n+2d}$, mert ha $y \equiv L_{n+d+1} \pmod{k}$, akkor $k \mid L_{n+d}$ miatt $L_{(n+d)+d} \equiv F_d \cdot y \equiv 0 \pmod{k}$. Hasonlóan adódik, hogy $k \mid L_{n-d}$ és teljes indukcióval kapjuk, hogy $k \mid L_{n+ad}$ és L_{n-bd}.

Legyen $l(k)$ az a legkisebb pozitív egész, amelyre $k \mid L_{l(k)}$, ezt továbbiakban k rendjének nevezzük. Ha nem létezik akkor $l(k) = \infty$.

II. lemma: Legyen $k > 2$. Ha $k \mid L_n$ akkor $\frac{n}{l(k)}$ páratlan egész szám.

Bizonyítás: Először is vegyük észre, hogy

$$L_{3n} = q_1^{3n} + q_2^{3n} = (q_1^n + q_2^n)^3 - 3q_1^n q_2^n (q_1^n + q_2^n) = L_n^3 - 3(-1)^n L_n$$

Tehát $k \mid L_{l(k)}$-ból következik, hogy $k \mid L_{3l(k)}$ és így az előző tétel miatt $k \mid L_{(2t+1)l(k)}$. Másrészt ha $k > 2$ akkor $k \nmid L_{2l(k)}$, mert

$$L_{2n} = q_1^{2n} + q_2^{2n} = (q_1^n + q_2^n)^2 - 2q_1^n q_2^n = L_n^2 - 2(-1)^n$$

Tegyük fel, hogy van olyan v, amelyre $k \mid L_v$ és v nem $(2t+1)l(k)$ alakú. Ekkor van olyan s, melyre $0 < d = |(2s+1)l(k) - v| \leq l(k)$. Ha itt egyenlőség áll, akkor $v = 2al(k)$, így k osztja $L_{2al(k)}$-t és $L_{(2a+1)l(k)}$-t, amiből következik, hogy $k \mid L_{2l(k)}$, 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, speciálisan $L_{(v \mod d)}$-t is osztja k, de mivel $v \mod d < d < l(k)$, ezért ez nem lehet. Ezzel bebizonyítottuk a lemmát.

Megjegyzés: Ha $k = 2$ akkor $2 \mid L_n$ ha $3 \mid n$.

III. lemma: Legyen p páratlan prím. Ha $l(p)$ létezik, akkor $\frac{p-\left(\frac{p}{5}\right)}{l(p)}$ páros egész.

Bizonyítás: Tudjuk, hogy az $L_n \mod k$ sorozat periódikus, legyen a periódus $m(k)$. Ekkor a 0-k periódusa osztója $m(k)$-nek, így $2l(k) \mid m(k)$. Tehát elegendő megvizsgálni $m(p)$-t. Megmutatjuk, hogy ha $p = 5t \pm 1$ akkor $m(p) \mid p-1$, míg $p = 5t \pm 2$ esetén $m(p) \mid 2(p+1)$. Először is megmutatjuk, hogy $p \mid L_p - 1$:

$$L_p \equiv 2^{p-1}L_p = \frac{1}{2}((1+\sqrt{5})^p + (1-\sqrt{5})^p) = \sum_{k=0}^{\left[\frac{p}{2}\right]} \binom{p}{2k} 5^k \equiv \binom{p}{0}5^0 = 1 \pmod{p}$$

Most megvizsgáljuk L_{p+1} modulo p vett maradékát.

$$2L_{p+1} \equiv 2^p L_{p+1} = \sum_{k=0}^{\frac{p+1}{2}} \binom{p+1}{2k} 5^k = \sum_{k=0}^{\frac{p+1}{2}} \left(\binom{p}{2k} + \binom{p}{2k-1} \right) 5^k \equiv$$

$$\equiv \binom{p}{0}5^0 + \binom{p}{p}5^{\frac{p+1}{2}} \equiv 1 + 5\left(\frac{5}{p}\right) \pmod{p}$$

Most megvizsgáljuk a két esetet külön-külön.

1.eset. $p = 5t \pm 1$. Ekkor $2L_{p+1} \equiv 1 + 5 \pmod{p}$, azaz $L_{p+1} \equiv 3 \pmod{p}$. Mivel $L_p \equiv L_1 \pmod{p}$ és $L_{p+1} \equiv L_2 \pmod{p}$, ezért itt $p-1$ hosszú periódus van. (Persze nem biztos, hogy ez a legrövidebb periódus.)

2.eset. $p = 5t \pm 2$. Ekkor $2L_{p+1} \equiv 1 - 5 \pmod{p}$, azaz $L_{p+1} \equiv -2 \pmod{p}$. Mivel $L_p \equiv 1 \pmod{p}$, ezért $L_{p+2} \equiv -1 \pmod{p}$, így $L_{p+1} \equiv -L_0$ és $L_{p+2} \equiv -L_1 \pmod{p}$. Tehát $L_k \equiv -L_{k+p+1} \equiv L_{k+2(p+1)} \pmod{p}$ vagyis ebben az esetben $2(p+1)$ hosszú periódus van.

Tehát ha $p = 5t \pm 1$ akkor $2l(p) \mid p-1$, ami éppen a bizonyítandó állítás. Ha $p = 5t \pm 2$ akkor $2l(p) \mid 2(p+1)$, ezután már csak azt kell bizonyítani, hogy $\frac{p+1}{l(p)}$ páros, ez pedig következik abból, hogy $p \not| L_{p+1}$. Ezzel bebizonyítottuk a lemma állítását.

M1-Tétel: Ha M_n prím akkor n 0, kettőhatvány vagy prím.

Az állítás jól ismert, ha n kettőhatvány akkor a Fermat-prímeket kapjuk, ha n prím akkor a Mersenne-prímeket.

L1-Tétel: Ha L_n prím akkor n 0, kettőhatvány vagy prím.

Bizonyítás: Ha n páratlan és p egy n-nél kisebb prímosztója akkor a II. lemma alapján $L_p \mid L_n$, tehát ekkor L_n nem lehet prím. Ha n páros és $n = 2^k r$, ahol r 1-nél nagyobb páratlan szám, akkor $L_{2^k} \mid L_n$, tehát L_n ekkor sem lehet prím. Ezzel bebizonyítottuk az állítást.

M2-Tétel: Legyen p prím és q prímosztója M_p-nek, ekkor q $2pk+1$ és $8t\pm 1$ alakú.

L2-Tétel: Legyen $p>3$ prím és q prímosztója L_p-nek, ekkor q $2pk+1$ és $5t\pm 1$ alakú.

Bizonyítás: Először megmutatjuk, hogy q $5t\pm 1$ alakú. Ehhez felhasználjuk azt az azonosságot, hogy $5F_{2n+1}^2 - L_{2n+1}^2 = 4$, ahol F_{2n+1} a $2n+1$. Fibonacci-szám. Mivel $p>3$ páratlan prím, így $q>2$ és q osztója L_p-nek, ezért $\left(\frac{5}{q}\right)=1$ azaz $q=5t\pm 1$.

Mivel $q \mid L_p$, ezért $l(q) \mid p$, de $L_1=1$, így $l(q)=p$, másrészt a III. lemma alapján $l(q) \mid (q-\left(\frac{5}{q}\right))$, azaz $p \mid q-1$. Ezzel bebizonyítottuk az állítást.

M3-Tétel: Legyen q prímosztója M_{2^n}-nek, ekkor q $2^{n+1}r+1$ alakú, sőt ha $n\geq 2$ akkor $2^{n+2}r+1$ alakú.

L3-Tétel: Legyen q prímosztója L_{2^n}-nek, ekkor q $2^{n+1}r\pm 1$ alakú.

Bizonyítás: Mivel $q \mid L_{2^n}$, ezért $\frac{2^n}{l(q)}$ páratlan azaz $l(q)=2^n$. Másrészt $\frac{q-\left(\frac{5}{q}\right)}{l(q)}$ páros, így $q=2^{n+1}r+\left(\frac{5}{q}\right)$. Ezzel bebizonyítottuk az állítást.

Megjegyzés: Ennél több nem mondható, mert $L_{2^n}=2^{n+1}r-1$ alakú, ahol r páratlan, így biztosan lesz olyan prímosztója , amely nem írható fel $2^{n+2}r\pm 1$ alakban.

IV. lemma: Ha $p\equiv -1 \pmod 4$ akkor $p \mid L_m$, ahol $m=\frac{p-\left(\frac{p}{5}\right)}{2}$.

Bizonyítás: Két esetet különböztetünk meg aszerint, hogy $p=5t\pm 1$ vagy $p=5t\pm 2$ alakú.

1.eset Legyen $p=5t\pm 1$. A III. lemma bizonyításánál láttuk, hogy $L_p\equiv 1 \pmod p$ és $L_{p-1}\equiv 2 \pmod p$, ebből kapjuk, hogy $L_{p-2}\equiv -1$ és $L_{p-3}\equiv 3 \pmod p$. Teljes indukcióval kapjuk, hogy $L_{p-k}\equiv (-1)^{k+1}L_{k-1} \pmod p$. Ha $p=4a-1$ akkor azt kapjuk, hogy $L_{2a-1}\equiv -L_{2a-1} \pmod p$. Tehát ekkor $p \mid L_m$ ahol $m=\frac{p-1}{2}$.

2. eset Legyen $p=5t\pm 2$. A III. lemmánál látottak alapján $L_p\equiv 1 \pmod p$ és $L_{p+1}\equiv -2 \pmod p$, így $L_{p-1}\equiv -3$ és $L_{p-2}\equiv 4 \pmod p$ és teljes indukcióból következően $L_{p+1-k}\equiv (-1)^{k+1}L_k \pmod p$. Ha $p=4a-1$ akkor $L_{2a}\equiv -L_{2a} \pmod p$, azaz $p \mid L_m$, ahol $m=\frac{p+1}{2}$.

Tehát mindkét esetben $p \mid L_m$, ahol $m=\frac{p-\left(\frac{p}{5}\right)}{2}$.

Megjegyzés: Mivel $L_nL_{n+1}=L_{2n+1}+(-1)^n$, ezért $L_{\frac{p-1}{2}}L_{\frac{p+1}{2}}=L_p-1\equiv 0 \pmod p$, ha $p=4a-1$, de ekkor nem tudjuk, hogy p melyiket osztja a két tag közül. Az is látszik ebből, hogy ha $p=4a+1$ akkor $p \not\mid L_{\frac{p-1}{2}}L_{\frac{p+1}{2}}$.

Lucas-tétel: Ha $p\equiv -1$ (4) akkor 2^p-1 akkor és csak akkor prím ha $2^p-1 \mid L_{2^{p-1}}$.

Bizonyítás: Először tegyük fel, hogy 2^p-1 prím, megmutatjuk, hogy $2^p-1 \mid L_{2^{p-1}}$. A IV. lemma alapján $2^p-1 \mid L_m$, ahol $m = \frac{1}{2}(2^p-1-\left(\frac{2^p-1}{5}\right))$, mivel $2^p-1 \equiv -1$ (4). Másrészt $\left(\frac{2^p-1}{5}\right) = \left(\frac{2^{4k+3}-1}{5}\right) = \left(\frac{8-1}{5}\right) = -1$, vagyis $m = 2^{p-1}$. Így éppen a bizonyítandó állítást kaptuk.

Most tegyük fel, hogy $2^p-1 \mid L_{2^{p-1}}$, megmutatjuk, hogy 2^p-1 prím. Legyen q 2^p-1 legnagyobb prímosztója. Tudjuk, hogy $L_{2^{p-1}}$, minden prímosztója, így q is, $2^p r \pm 1$ alakú az L3-Tétel alapján, tehát $q \geq 2^p-1$, ami csak úgy lehet ha $q = 2^p-1$ prím. Ezzel bebizonyítottuk a tétel állítását.

LM2-Tétel: Ha n pozitív egész, melyre $n \equiv 0$ (4) vagy $n \equiv 3$ (4), akkor $3 \cdot 2^n - 1$ akkor és csak akkor prím ha $3 \cdot 2^n - 1 \mid L_{3 \cdot 2^{n-1}}$.

Bizonyítás: A bizonyítás ugyanúgy megy, mint előbb. Ha $3 \cdot 2^n - 1$ prím akkor $3 \cdot 2^n - 1 \mid L_m$, ahol $m = \frac{1}{2}(3 \cdot 2^n - 1 - \left(\frac{3 \cdot 2^n - 1}{5}\right)) = 3 \cdot 2^{n-1}$.

Ha pedig $3 \cdot 2^n - 1 \mid L_{3 \cdot 2^{n-1}}$ és q prímosztója $3 \cdot 2^n - 1$-nek, akkor $\frac{3 \cdot 2^{n-1}}{l(q)}$ páratlan, így $l(q) = 2^{n-1}$ vagy $l(q) = 3 \cdot 2^{n-1}$. Mivel $\frac{q-\left(\frac{5}{q}\right)}{l(q)}$ páros, ezért
$q = 2^n r \pm 1$. Mivel $q \mid 3 \cdot 2^n - 1$, ezért $t(2^n r \pm 1) = 3 \cdot 2^n - 1$, ahol t nem lehet se 2, se 3, mert azzal a jobb oldal nem osztható, tehát $t = 1$ vagy $t \geq 4$. Ha $t = 1$ akkor mivel a jobb oldal $4k-1$ alakú, így a bal oldalon is -1-nek kell állnia és $r = 3$ vagyis $3 \cdot 2^n - 1$ prím. Ha $t \geq 4$ akkor rendezzük át az egyenletet: $(tr-3)2^n = \pm t - 1$, de $(tr-3)2^n \geq (tr-3)4 = (4r-1)t - 12 + t \geq 12 - 12 + t > \pm t - 1$, tehát ez az eset nem lehet.

Ezzel bebizonyítottuk az állítást.

M4-Tétel: $n \mid \sum_{d|n} \mu\left(\frac{n}{d}\right) M_d$.

L4-Tétel: $n \mid \sum_{d|n} \mu\left(\frac{n}{d}\right) L_d$.

Bizonyítás: Elegendő leellenőrizni, hogy az

$$a_n = \frac{1}{n} \sum_{i=1}^{n} (-L_i) a_{n-i} \quad a_0 = 1$$

rekurzió egészeket definiál-e. Az L_n sorozat rekurziója miatt $a_1 = a_2 = -1$, $i > 2$ esetén $a_i = 0$. Ezzel bebizonyítottuk az állítást.

L5-Tétel: $L_{2n+1} \mid 2(L_{n+1}^{2n+1} - 1)$

Bizonyítás: Tekintsük a következő azonosságot: $L_{2n} L_{2n+2} = L_{2n+1}^2 + 5$, másrészt a rekurzió miatt $L_{2n} \equiv L_{2n+2} \pmod{L_{2n+1}}$, így $L_{2n+2}^2 \equiv 5$ (L_{2n+1}). Fennáll továbbá a következő azonosság: $L_{n+1}^2 = L_{2n+2} + 2(-1)^{n+1}$. Ezek alapján $L_{n+1}^{2n+1} = L_{n+1}(L_{2n+2} + 2(-1)^{n+1})^n$. Legyen $(\sqrt{5} + 2(-1)^{n+1})^k = a_k + b_k\sqrt{5}$, ekkor $a_{k+1} = 2(-1)^{n+1} a_k + 5b_k$ és $b_{k+1} = a_k + 2(-1)^{n+1} b_k$. Ekkor $(L_{2n+2} + 2(-1)^{n+1})^k \equiv a_k + b_k L_{2n+2} \pmod{L_{2n+1}}$, hiszen ugyanaz a rekurzió teljesül rájuk, mivel $L_{2n+2}^2 \equiv 5 \pmod{L_{2n+1}}$.

Mivel $(\sqrt{5}+2(-1)^{n+1}) = \left(\frac{\sqrt{5}+(-1)^{n+1}}{2}\right)^3$, ezért $a_k = (-1)^{(n+1)k}\frac{L_{3k}}{2}$, míg $b_k = (-1)^{(n+1)(k+1)}\frac{F_{3k}}{2}$. Tehát

$$2L_{n+1}^{2n+1} \equiv L_{n+1}(L_{3n} + (-1)^{n+1}F_{3n}L_{2n+2}) \pmod{L_{2n+1}}$$

A továbbiakban felhasználjuk a következő azonosságokat: $F_{3n} = \frac{1}{5}(L_{3n} + 2L_{3n-1})$, továbbá $L_mL_n = L_{m+n}+(-1)^nL_{m-n}$, így $L_{3n} \equiv (-1)^nL_{n+2} \pmod{L_{2n+1}}$ és $L_{3n-1} \equiv (-1)^{n+1}L_{n+3} \pmod{L_{2n+1}}$. Fel fogjuk használni továbbá, hogy $L_{2n+2} \equiv L_{2n+3} \pmod{L_{2n+1}}$ és $L_{2n+4} \equiv 2L_{2n+2} \pmod{L_{2n+1}}$ és a már megismert $L_{2n+2}^2 \equiv 5 \pmod{L_{2n+1}}$ kongruenciát.

Az első azonosság alapján:

$$10L_{n+1}^{2n+1} \equiv 5L_{n+1}L_{3n} + (-1)^{n+1}L_{n+1}L_{3n}L_{2n+2} + 2(-1)^{n+1}L_{n+1}L_{3n-1}L_{2n+2} \pmod{L_{2n+1}}$$

A második azonosságot ebbe beírva kapjuk, hogy

$$10L_{n+1}^{2n+1} \equiv 5L_{n+1}(-1)^nL_{n+2}+(-1)^{n+1}L_{n+1}(-1)^nL_{n+2}L_{2n+2}+2(-1)^{n+1}L_{n+1}(-1)^{n-1}L_{n+3}L_{2n+2}$$

Megint az $L_mL_n = L_{m+n} + (-1)^nL_{m-n}$ azonosságot használjuk.

$$10L_{n+1}^{2n+1} \equiv 5(-1)^n(L_{2n+3}+(-1)^{n+1})-(L_{2n+3}+(-1)^{n+1})L_{2n+2}+2(L_{2n+4}+3(-1)^{n+1})L_{2n+2}$$

Most használjuk fel az utolsó kongruenciákat.

$$10L_{n+1}^{2n+1} \equiv -5+5(-1)^nL_{2n+2}-L_{2n+2}^2+(-1)^nL_{2n+2}+4L_{2n+2}^2+6(-1)^{n+1}L_{2n+2} \equiv 10 \pmod{L_{2n+1}}$$

Mivel $(5, L_{2n+1}) = 1$, ezért $L_{2n+1} \mid 2(L_{n+1}^{2n+1} - 1)$. Ezzel bebizonyítottuk az állítást.

Megjegyzés: Ha $3 \nmid 2n+1$ akkor $(L_{2n+1}, 2) = 1$, így $L_{2n+1} \mid L_{n+1}^{2n+1} - 1$.