

Rekurzív sorozatok egymást követő tagjainak legnagyobb közös osztóiról

Szikszai Márton

II. Alkalmazott Matematikus MSc

Debreceni Egyetem, Természettudományi és Technológiai Kar

Témavezető: Dr. Hajdu Lajos

Debreceni Egyetem

Debreceni Egyetem, 2013

A publikáció/prezentáció/poster elkészítését a TÁMOP-4.2.2/B-10/1-2010-0024 számú projekt támogatta.

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg.



SZÉCHENYI TERV

*Ezúton is szeretném megköszönni Dr. Hajdu Lajosnak
hosszú, kitartó munkáját és építő tanácsait,
melyekkel segítette a dolgozat elkészülését.*

Tartalomjegyzék

1. Bevezetés	4
2. Pillai sorozatok	8
2.1. Pillai problémája és egy általánosítás	8
2.2. Pillai- és T -Pillai sorozatok	9
3. Lineáris rekurzív sorozatok	11
3.1. Lucas és Lehmer sorozatok	11
3.2. Asszociált Lucas és Lehmer sorozatok	14
3.3. Általános oszthatósági sorozatok	15
3.4. Bizonyítások	16
3.4.1. Lucas és Lehmer sorozatok	16
3.4.2. Asszociált Lucas és Lehmer sorozatok	22
3.4.3. Általános oszthatósági sorozatok	25
4. Elliptikus oszthatósági sorozatok	27
4.1. Új eredmények	27
4.2. Bizonyítások	29
5. Hivatkozások	31

1. Bevezetés

Pillai [30] a következő problémát vetette fel. Igaz-e, hogy bármely $k \geq 2$ egymást követő egész szám között van olyan, amely az összes többivel relatív prím? Vezessünk be két jelölést. Legyen g az a legkisebb szám, hogy létezik ennyi darab egymást követő egész, melyek egyike sem relatív prím az összes többivel; legyen továbbá G az a minimális K érték, hogy minden $k \geq K$ esetén található ez utóbbi tulajdonságú k egymást követő egész szám. Pillai [30] megmutatta, hogy g létezik és $g = 17$ teljesül. Eredményét később Brauer [8] egészítette ki, - egyben teljességgel megválaszolva az eredeti kérdést - igazolva, hogy G is létezik és $G = g = 17$ áll fenn.

Pillai kérdésének később több általánosítása is született. Mi itt a teljesség igénye nélkül csupán néhány fontos és érdekes irányt említünk meg. Az első Caro [11] nevéhez fűződik, aki olyan szám létezését vizsgálta k egymást követő egész között, melynek közös osztója az összes többivel nem nagyobb, mint egy rögzített $d \geq 1$ egész szám. Caro [11] bevezetve a megfelelően módosított $g(d)$ és $G(d)$ mennyiségeket, megmutatta, hogy azok minden d esetén léteznek, továbbá korlátokat is adott nagyságukra a $\pi(x)$ függvény segítségével.

Egymást követő egészek legnagyobb közös osztóit vizsgálta Hajdu és Saradha [16] is. Legyen T egészek egy tetszőleges halmaza. Abban az esetben, amikor T véges vagy speciális, ún. S -egészek részhalmaza, Hajdu és Saradha [16] igazolták, hogy a korábbiakhoz hasonló módon definiált $g(T)$ és $G(T)$ mennyiségek - pontos definíciókért most és később is lásd a többi fejezetet - léteznek és explicit felső korlátot is adtak ezek értékére.

Egy másik irányú általánosítást vizsgált Ohtomo és Tamari [29]. Egymást követő egészek helyett tekintsük egy $A = (A_n)_{n=0}^{\infty}$ számtani sorozat egymást követő tagjait. Legyen g_A az a legkisebb szám, hogy létezik a sorozatnak ennyi darab egymást követő tagja, melyek közül egyik sem relatív prím az összes többivel; továbbá G_A az a legkisebb szám, hogy bármely $k \geq G_A$ esetén létezik k darab egymást követő tagja a sorozatnak ez utóbbi tulajdonsággal. Ohtomo és Tamari megmutatta, hogy G_A mindig létezik, ha $A = (A_n)_{n=0}^{\infty}$ számtani sorozat.

Ebben a dolgozatban több, az előbbiekhöz szorosan kapcsolódó problémát tekintünk. Legyen most $A = (A_n)_{n=0}^{\infty}$ egy tetszőleges egészekből álló sorozat, g_A és G_A pedig az előző bekezdésben definiált mennyiség. Egy sorozatot Pillai sorozatnak fogunk nevezni, ha G_A létezik. Vizsgálni fogjuk többek között, hogy a Lucas vagy Lehmer sorozatok,

illetve asszociált sorozataik mikor Pillai sorozatok.

A Lucas és Lehmer sorozatok irodalma rendkívül gazdag, különféle oszthatósági tulajdonságaikat több szerző több szemszögből is vizsgálta. Mi itt a teljesség igénye nélkül csak néhányat említünk meg az érdekes és fontos irányok közül.

Az egyik legjelentősebb probléma a Lucas és Lehmer sorozatok tagjainak primitív prímosztóival kapcsolatos. Több részleges eredmény után Bilu, Hanrot és Voutier [6] teljességgel megválaszolta a kérdést.

Többen vizsgálták, hogy egy lineáris rekurzív sorozat egy tagját mikor osztja annak indexe. A pontos részletekért lásd Győry és Smyth [15], Smyth [40] és Alba González et al. [1] publikációt és az ott található hivatkozásokat.

Egy másik kérdés az ún. oszthatósági sorozatok karakterizációja. Pontosabban fogalmazva adjuk meg az összes olyan $u = (u_n)_{n=0}^\infty$ sorozatot, melyekre $i \mid j$ esetén $u_i \mid u_j$ teljesül. Ezen sorozatok teljes jellemzése megtalálható Bézivin, Pethő és van der Poorten [5] cikkében, de megemlíjtük még Győry és Pethő [14], Schinzel [32], illetve Horák és Skula [20] fontos idevágó eredményeit is.

Vizsgálták azt is, hogy egy lineáris rekurzív sorozat egymást követő tagjainak szorzata lehet-e teljes hatvány. Az eredmények részletezése helyett Shorey és Tijdeman [34] könyvét, továbbá Luca és Shorey [24, 25, 26], illetve Brindza, Liptay és Szalay [9] cikkeit ajánljuk az olvasó figyelmébe.

Az előzőekhez ugyan szorosan nem kapcsolódó, de hasonlóan sokat vizsgált probléma a rekurzív sorozatok tagjainak multiplicitása. Pontosabban az, hogy egy rögzített elem hányszor fordul elő a sorozatban. Másodrendű esetben Kubota [21, 22], Beukers [4], továbbá Brindza, Pintér és Schmidt [10] eredményeit, míg magasabb rendű lineáris rekurziók esetén Allen [2], illetve Amoroso és Viada [3] munkáit említjük.

Foglalkozunk továbbá asszociált Lucas és Lehmer sorozatokkal is. A kapcsolódó fontosabb eredmények helyett csupán [28]-ra és az ott található hivatkozásokra utalunk.

Legyen u egy Lucas sorozat. A dolgozatban megmutatjuk, hogy néhány degenerált esettől eltekintve minden Lucas sorozat Pillai sorozat, továbbá minden sorozatra megadjuk g_u és G_u pontos értékeit is. Hasonló eredményt mondunk ki Lehmer sorozatokra is. Megemlíjtük, hogy a tételeink bizonyítása közben választ adunk Beukers [4] egy kérdésére is a nem degenerált Lucas sorozatok 1 és -1 elemeinek multiplicitásait illetően. Érdekes módon kiderül, hogy Pillai sorozatnak lenni "ritka" tulajdonság, legalábbis abban az

értelemben, hogy már az ún. asszociált Lucas- és Lehmer sorozatok sem mindig azok.

Speciális esetként mind a Fibonacci, mind a Lucas számok sorozatával kapcsolatosan kimondunk egy-egy tételt. Igazoljuk, hogy bármely $k \leq 24$ egymást követő Fibonacci számot tekintve mindig található ezek között olyat, mely az összes többivel relatív prím, ugyanakkor van olyan 25 darab egymást követő Fibonacci szám, hogy ez utóbbi nem teljesül. Megmutatjuk azt is, hogy melyik az első 25 ilyen Fibonacci szám. Igazoljuk továbbá, hogy bár a Lucas számok L sorozata nem Pillai sorozat, viszont g_L létezik és $g_L = 171$ teljesül.

Bizonyítunk egy általános tételt is. Legyen S prímek egy véges halmaza, T pedig olyan egészeké, melyeknek nincs S -en kívüli prímosztója. Az u tetszőleges rendű lineáris oszthatósági sorozat egymást követő tagjainak közös osztói helyett azok S -mentes részét tekintve, felső korlátot adunk a $g_u(T)$ és $G_u(T)$ értékeire.

A dolgozatban nem csak lineáris, hanem más típusú rekurzív sorozatokat is vizsgálunk: név szerint az elliptikus oszthatósági sorozatokat. Az elliptikus oszthatósági sorozatok irodalma szintén igen gazdag. Már maga a definíció is megannyi különféle változattal rendelkezik. Mivel ebben a fejezetben pontos fogalmakat nem közlünk, így a részletesebb eredmények helyett csak néhány vizsgált problémát említünk meg.

Elsőként Ward [42, 43] foglalkozott részletesen ezen sorozatok tulajdonságaival. Azóta több szerző több érdekes eredményt ért el különféle irányokban.

Az egyik sokat vizsgált kérdés a sorozatok alapvető oszthatósági tulajdonságaival kapcsolatos. Többek között Everest, McLaren és Ward [13], illetve Silverman [36, 37] cikkeit említjük meg az ott található utalásokkal egyetemben.

Egy másik probléma az elliptikus oszthatósági sorozatok tagjainak növekedése. Itt Silverman [35] publikációját és az ott látható hivatkozásokat ajánljuk az olvasó figyelmébe.

Többen vizsgálták azt is, hogy egy elliptikus oszthatósági sorozat mely tagjainak van primitív prímosztója. Kapcsolódó eredmények részletezése helyett most csupán Everest, McLaren és Ward [13] munkájára és az ebben található irodalomjegyzékre szorítkozunk.

Meg fogjuk mutatni, hogy minden B elliptikus oszthatósági sorozat Pillai sorozat. Bizonyítunk továbbá egy általánosabb tételt a T -Pillai tulajdonsággal kapcsolatban. Mindemellett néhány konkrét elliptikus oszthatósági sorozat esetén megadjuk a g_B és G_B mennyiségek pontos értékeit is.

Bizonyításaink során, mind a lineáris rekurzív sorozatok, mind az elliptikus oszt-

hatósági sorozatok esetében a sorozatok alapvető oszthatósági tulajdonságait kihasználva visszavezetjük a problémát egy azzal ekvivalensre az egymást követő egészek körében. Tulajdonképpen a sorozat egymást követő tagjai helyett, az egymást követő indexeket fogjuk tekinteni. Itt Lucas [27], Lehmer [23], McDaniel [28], továbbá Everest, McLaren és Ward [13] eredményeire támaszkodunk.

Ezekén túl, lineáris rekurziók vizsgálatánál szükségünk lesz Bilu, Hanrot és Voutier [6] Lucas és Lehmer sorozatok primitív prímosztóiról szóló és Beukers [4] Lucas sorozatok elemeinek multiplicitásával kapcsolatos tételére, illetve Schlickewei és Schmidt [33] mély, ún. polinomiális exponenciális diofantikus egyenletekre vonatkozó, az altér tételen alapuló eredményét használjuk. Az elliptikus oszthatósági sorozatok esetében Silverman [35] elliptikus oszthatósági sorozatok tagjainak növekedésére és primitív prímosztóira vonatkozó tételeit alkalmazzuk.

Bizonyos esetekben egy, a sorozattól függő T halmaz mellett vagyunk kíváncsiak a $g(T)$ és $G(T)$ függvények értékére vagy azok egy felső korlátjára. Itt a fő segítséget Hajdu és Saradha [16] $G(T)$ értékét egy általános esetben korlátozó eredménye, és egy idevágó, ún. prímlefedő algoritmusa jelenti.

Végül megemlítjük, hogy eredményeinket a [17, 18, 19] publikációk tartalmazzák.

2. Pillai sorozatok

Ebben a fejezetben a későbbi tárgyalás során használt terminológia és jelölésrendszer egy részét építjük ki. Elsőként az előző fejezetben már említett Pillai-féle kérdésről és egy általánosításáról ejtünk szót, bevezetve a g és G , illetve a $g(T)$ és $G(T)$ mennyiségeket - ez utóbbiak előtt a technikai jellegű T -relatív prím fogalmat ismertetjük. A második részben a vizsgálódásaink tényleges tárgyát képező Pillai- és T -Pillai sorozatokkal foglalkozunk. Végig fel fogjuk tenni, hogy $k, k_0, K \geq 2$ egész számok.

2.1. Pillai problémája és egy általánosítás

Legyen $g = k_0$ az a legkisebb szám, melyre létezik k_0 egymást követő egész úgy, hogy ezek közül egyik sem relatív prím az összes többivel. Pillai [30] megmutatta, hogy $g = 17$. Legyen továbbá $G = K$ az a minimális érték, hogy minden $k \geq K$ esetén létezik k olyan egymást követő egész melyek közül egyik sem relatív prím az összes többivel. Brauer [8], kiegészítve Pillai eredményét igazolta, hogy $G = g = 17$. Most bemutatjuk, hogyan lehetséges 17 olyan egymást követő egész számot találni, hogy ezek közül egyik sem relatív prím az összes többivel. Ennek keretében a későbbiek során fontos szerepet játszó prímlefedési technikát is szemléltetjük.

Tekintsük az $A_1, A_2, \dots, A_{17}$ egymást követő egész számokat. "Fedjük le" ezeket a 2, 3, 5, 7, 11, 13 prímeikkel az 1. táblázatban látható módon.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2,5,11	3	2,7	13	2, 3	5	2	3	2	7	2,3,5	11	2	3	2	5	2,3,7,13

1. táblázat. Egy prímlefedés: $k=17$ eset

A táblázat felső sorában az A_i egész szám i indexe látható, míg a második sorban a megfelelő indexű tagot osztó prímeik. A konstrukcióból könnyen leolvasható, hogy nincs olyan A_i , ami mindegyik másikkal relatív prím lenne. Megoldva az

$$\begin{aligned}
 x &\equiv 0 \pmod{2} \\
 x+1 &\equiv 0 \pmod{3} \\
 x &\equiv 0 \pmod{5} \\
 x+2 &\equiv 0 \pmod{7}
 \end{aligned}$$

$$\begin{aligned}x &\equiv 0 \pmod{11} \\x + 3 &\equiv 0 \pmod{13}\end{aligned}$$

lineáris kongruenciarendszert kapjuk, hogy $A_1 = x \equiv 27830 \pmod{30030}$, azaz

$$27830, 27831, \dots, 27846$$

olyan egymást követő egész számok, melyek közül egyik sem relatív prím az összes többivel. Természetesen rögzített k esetén nem csak egy lehetséges lefedés létezhet, továbbá már egy konstrukció is végtelen sok megfelelő tulajdonságú szám k -ast biztosít.

Mielőtt Pillai problémájának általánosítását tekintenénk, bevezetjük az ún. T -relatív prím számok fogalmát. Legyenek p, q tetszőleges egész számok, T pedig egészek egy rögzített halmaza. Azt mondjuk, hogy p és q T -relatív prímek, ha $\gcd(p, q) \in T$.

A T -relatív prím fogalmat felhasználva jutunk el Pillai kérdésének egy Hajdu és Saradha [16] által vizsgált általánosításához. Legyen T egészek egy tetszőleges halmaza és módosítsuk a g és G mennyiségeket a következő módon. Legyen $g(T) = k_0$ az a legkisebb szám, hogy létezik k_0 egymást követő egész szám, hogy azok közül egyik sem T -relatív prím az összes többivel; továbbá legyen $G(T) = K$ az a minimális érték, hogy minden $k \geq K$ esetén található előbbi tulajdonságú k egymást követő egész. Vegyük észre, hogy $T = \{1\}$ választással pontosan Pillai problémáját kapjuk.

2.1. Megjegyzés. Vegyük észre, hogy ha $1 \notin T$, akkor mindig léteznek a $g(T)$ és $G(T)$ mennyiségek, továbbá $g(T) = G(T) = 2$ teljesül (hiszen két egymást követő egész szám relatív prím egymással, így ebben az esetben nem T -relatív prímek). Ezért most és a későbbiekben is említés nélkül feltesszük, hogy $1 \in T$.

2.2. Pillai- és T -Pillai sorozatok

Ebben a részben egy más irányú általánosítást tekintünk, pontosabban a kérdéses közös osztó mellett az alaphalmazt is megváltoztatjuk. Legyen $A = (A_n)_{n=0}^{\infty}$ egy tetszőleges egészekből álló sorozat. Egymást követő egészek helyett tekintsük Pillai kérdését a sorozat egymást követő tagjai között. Legyen g_A az a legkisebb k_0 , hogy létezik a sorozatnak k_0 egymást követő tagja, melyek közül egyik sem relatív prím az összes többivel. Hasonlóan, mint az előzőekben legyen $G_A = K$ az a minimális érték, hogy minden $k \geq K$ esetén létezik olyan k egymást követő tagja a sorozatnak, melyek az utóbbi tulajdonságnak

eleget tesznek. Az $A = (A_n)_{n=0}^{\infty}$ sorozatot Pillai sorozatnak fogjuk nevezni, ha G_A létezik. Vegyük észre, hogy A szabad megválasztása miatt, tulajdonképpen a legáltalánosabb módon fogalmaztuk meg Pillai eredeti kérdését az egészek körében. Ohtomo és Tamari [29] alapvető eredménye, hogy minden számtani sorozat Pillai sorozat.

Következő lépésként a Hajdu és Saradha [16] által tekintett problémát terjesztjük ki tetszőleges egészekből álló sorozatokra. Legyen $A = (A_n)_{n=0}^{\infty}$ most is egy tetszőleges egészekből álló sorozat, T pedig egészek egy tetszőleges halmaza. Jelölje $g_A(T)$ azt a legkisebb k_0 számot, hogy létezik a sorozatnak k_0 egymást követő tagja, melyek közül egyik sem T -relatív prím az összes többivel. Analóg módon kapjuk a $G_A(T)$ mennyiséget is: legyen az a minimális K érték, hogy bármely $k \geq K$ esetén van k egymást követő egész, hogy azok közül egyik sem T -relatív prím az összes többivel. Az A sorozatot T -Pillainak fogjuk mondani, ha $G_A(T)$ létezik. A következő fejezetben megkezdjük a lineáris rekurzív sorozatok vizsgálatát.

3. Lineáris rekurzív sorozatok

Legyen $r \geq 1$ természetes szám, továbbá legyenek $u_0, u_1, \dots, u_{r-1}$ és $c_0, c_1, \dots, c_{r-1}$ egész számok, hogy $c_0 \neq 0$. Ekkor az $u = (u_n)_{n=0}^{\infty}$ sorozatot r -edrendű lineáris rekurzív sorozatnak nevezzük, ha bármely $n \geq 0$ esetén

$$u_{n+r} = c_{r-1}u_{n+r-1} + \dots + c_1u_{n+1} + c_0u_n.$$

Ebben a fejezetben megkezdjük a Pillai és T -Pillai tulajdonságok vizsgálatát lineáris rekurzív sorozatokban. Vegyük észre, hogy amennyiben $\gcd(c_0, c_1, \dots, c_{r-1}) \neq 1$, úgy minden $i > j \geq r$ esetén $\gcd(u_i, u_j) > 1$. Azaz u egy Pillai sorozat, továbbá $g_u = G_u = 2$. A későbbiekben - hogy ezt a triviális esetet ne ellenőrizzük minden sorozatra - a Pillai tulajdonsággal kapcsolatos tételekben feltesszük, hogy a sorozatok paraméterei relatív prímek. Ezt a feltételt minden esetben fel fogjuk tüntetni, hogy zavart ne okozzon.

Eredményeinket három jól elkülöníthető részre osztjuk. Elsőként a Lucas és Lehmer sorozatokat tekintjük, majd asszociált sorozataikkal folytatjuk. Végül egy általánosabb eredményt is megfogalmazunk tetszőleges rendű oszthatósági sorozatokra. A fejezet utolsó részében a bizonyításokat és a felhasznált eszközöket ismertetjük: ezt az alfejezetet terjedelme miatt újfent háromfelé tagoljuk.

3.1. Lucas és Lehmer sorozatok

Legyenek M és $N \neq 0$ egész számok. Az $u = (u_n)_{n=0}^{\infty}$ sorozatot Lucas sorozatnak nevezzük az (M, N) paraméterekkel, ha $u_0 = 0$, $u_1 = 1$ és minden $n \geq 0$ esetén

$$(1) \quad u_{n+2} = Mu_{n+1} - Nu_n.$$

Egy Lucas sorozatot nem degeneráltnak mondunk, ha az

$$x^2 - Mx + N$$

polinom α és β gyökeinek hányadosa nem egységgyök. A Lucas sorozatok fogalmát névadójuk, Lucas [27] vezette be a Fibonacci sorozatok általánosításaként, így legismertebb példaképpen a Fibonacci számok sorozata szolgál, melyet az $(M, N) = (1, -1)$ paraméterek választása esetén kapunk.

Legyenek M és N továbbra is a fenti egész számok. Az $\tilde{u} = (\tilde{u}_n)_{n=0}^\infty$ sorozatot Lehmer sorozatnak nevezzük, ha $u_0 = 0$, $u_1 = 1$ és minden $n \geq 0$ esetén

$$(2) \quad \tilde{u}_{n+2} = \begin{cases} \tilde{u}_{n+1} - N\tilde{u}_n, & \text{ha } n \text{ páros,} \\ M\tilde{u}_{n+1} - N\tilde{u}_n, & \text{ha } n \text{ páratlan.} \end{cases}$$

Egy Lehmer sorozatot nem degeneráltnak fogunk nevezni, ha az

$$x^2 - \sqrt{M}x + N$$

polinom α és β gyökeinek hányadosa nem egységgyök. A Lehmer sorozatokat - akárcsak a Lucas sorozatokat - is a névadó, Lehmer [23] vezette be, felismerve a Lucas sorozatok bizonyos oszthatósági tulajdonságait. Ugyanakkor a Lehmer sorozatok csak bizonyos értelmében nevezhetők a Lucas sorozatok általánosításainak, tekintettel arra, hogy van olyan Lucas sorozat, mely nem Lehmer. Mint ismert, a Lehmer sorozatok valójában negyedrendű rekurzív sorozatok; mi a dolgozat során a fenti definíciót fogjuk követni.

Első tételünk mutatja, hogy minden nem degenerált u Lucas sorozat Pillai sorozat, továbbá g_u és G_u konkrét értékeit is megadjuk minden sorozat esetén.

3.1. Tétel. *Legyen $u = (u_n)_{n=0}^\infty$ egy nem degenerált Lucas sorozat az (M, N) relatív prím paraméterekkel. Ekkor u Pillai sorozat, továbbá $g_u = G_u = 17$, eltekintve a 2. táblázatban látható esetektől.*

(M, N)	g_u	G_u
$(\pm 1, N), N \neq 1, 2, 3, 5$	25	25
$(M, M^2 \pm 1), M \geq 2$	43	43
$(\pm 12, 55)$	31	31
$(\pm 12, 377)$	31	31
$(\pm 1, 3)$	45	45
$(\pm 1, 5)$	49	51
$(\pm 1, 2)$	107	107

2. táblázat. A g_u és G_u értékei a kivételes Lucas sorozatokra

Az érdekesség kedvéért egy pontosabb tételt fogalmazunk meg abban az esetben, ha u a Fibonacci sorozat.

3.2. Tétel. Legyen $F = (F_n)_{n=0}^\infty$ a Fibonacci számok sorozata. Ekkor F Pillai sorozat és $g_F = G_F = 25$, továbbá az első n_0 index, hogy $F_{n_0}, \dots, F_{n_0+24}$ közül egyik sem relatív prím az összes többivel az $n_0 = 208569474$.

Következő eredményünkben a 3.1 Tételt terjesztjük ki Lehmer sorozatokra.

3.3. Tétel. Legyen $\tilde{u} = (\tilde{u}_n)_{n=0}^\infty$ egy nem degenerált Lehmer sorozat az (M, N) relatív prím paraméterekkel. Ekkor $\tilde{u}$ Pillai sorozat, továbbá $g_{\tilde{u}} = G_{\tilde{u}} = 25$, eltekintve a 3. táblázatban látható esetektől.

(M, N)	$g_{\tilde{u}}$	$G_{\tilde{u}}$
$\pm(N \pm 1, N), N \geq 3$	49	53
$\pm(2N \pm 1, N), N \geq 3$	47	47
$\pm(F_{n \pm 2}, F_n), n \geq 4$	45	45
$\pm(1, 5)$	49	51
$\pm(13, 4)$	49	51
$\pm(14, 9)$	49	51
$\pm(5, 2)$	61	69
$\pm(3, 2)$	81	81
$\pm(1, 2)$	107	107

3. táblázat. A $g_{\tilde{u}}$ és $G_{\tilde{u}}$ értékei a kivételes Lehmer sorozatokra

A Lucas és Lehmer sorozatok jellemzését a degenerált esetek kezelésével tesszük teljessé.

3.4. Tétel. Legyen $u = (u_n)_{n=0}^\infty$ egy degenerált Lucas sorozat az (M, N) relatív prím paraméterekkel. Ekkor u Pillai sorozat pontosan akkor, ha $(M, N) = (\pm 2, 1)$, amikor is $g_u = G_u = 17$.

Hasonlóan, legyen $\tilde{u} = (\tilde{u}_n)_{n=0}^\infty$ egy degenerált Lehmer sorozat az (M, N) relatív prím paraméterekkel. Ekkor $\tilde{u}$ Pillai sorozat pontosan akkor, ha $(M, N) = (\pm 4, 1)$, amikor is $g_{\tilde{u}} = G_{\tilde{u}} = 25$.

A fejezet következő részében az ún. asszociált Lucas és Lehmer sorozatokkal foglalkozunk.

3.2. Asszociált Lucas és Lehmer sorozatok

Legyenek M és $N \neq 0$ egész számok. Ekkor a $v = (v_n)_{n=0}^{\infty}$ sorozatot asszociált Lucas sorozatnak nevezzük az (M, N) paraméterekkel, ha $v_0 = 2$, $v_1 = M$ és minden $n \geq 0$ esetén

$$(3) \quad v_{n+2} = Mv_{n+1} - Nv_n.$$

Azt mondjuk, hogy a v sorozat nem degenerált, ha az

$$x^2 - Mx + N$$

polinom α és β gyökeinek hányadosa nem egységgyök. Az asszociált Lucas sorozatok legismertebb példája a Lucas számok sorozata, ami az $(M, N) = (1, -1)$ választással adódik.

Legyenek M és N továbbra is a fenti egész számok. A $\tilde{v} = (\tilde{v}_n)_{n=0}^{\infty}$ sorozatot asszociált Lehmer sorozatnak nevezzük, ha $\tilde{v}_0 = 2$, $\tilde{v}_1 = 1$ és minden $n \geq 0$ esetén

$$(4) \quad \tilde{v}_{n+2} = \begin{cases} M\tilde{v}_{n+1} - N\tilde{v}_n, & \text{ha } n \text{ páros,} \\ \tilde{v}_{n+1} - N\tilde{v}_n, & \text{ha } n \text{ páratlan.} \end{cases}$$

Egy ilyen sorozatot nem degeneráltnak fogunk mondani, ha az

$$x^2 - \sqrt{M}x + N$$

polinom α és β gyökeinek hányadosa nem egységgyök. Mint ismert, az asszociált Lehmer sorozatok - akárcsak a Lehmer sorozatok - negyedrendű rekurzív sorozatok.

Első eredményünkéből kiderül, hogy Pillai sorozatnak lenni "ritka" tulajdonság, legalábbis abban az értelemben, hogy már az asszociált Lucas és Lehmer sorozatok sem mindig azok.

3.5. Tétel. *Legyen $\hat{v} = (\hat{v}_n)_{n=0}^{\infty}$ egy nem degenerált asszociált Lucas vagy Lehmer sorozat az (M, N) relatív prím paraméterekkel. Ekkor $\hat{v}$ Pillai sorozat pontosan akkor, ha M páros és N páratlan.*

Következő tételünk a Lucas számok sorozatáról ad pontosabb információt: bár a Lucas számok L sorozata nem Pillai, de g_L létezik és ennek értékét meg is adjuk.

3.6. Tétel. *Legyen $L = (L_n)_{n=0}^{\infty}$ a Lucas számok sorozata. Ekkor L nem Pillai sorozat, de g_L létezik és $g_L = 171$ teljesül.*

Az asszociált Lucas sorozatokra megfogalmazunk egy általánosabb, a T -Pillai tulajdonsággal kapcsolatos eredményt is.

3.7. Tétel. *Legyen $v = (v_n)_{n=0}^{\infty}$ egy nem degenerált asszociált Lucas sorozat az (M, N) relatív prím paraméterekkel, T pedig egészek egy tetszőleges halmaza. Ekkor v pontosan akkor T -Pillai sorozat, ha $2 \notin T$.*

3.8. Megjegyzés. *Könnyen látható, hogy asszociált Lehmer sorozatok esetére a előző tétel állítása nem igaz.*

Az asszociált sorozatokkal kapcsolatos utolsó eredményünk a degenerált sorozatokat jellemzi a Pillai tulajdonság szempontjából.

3.9. Tétel. *Legyen $v = (v_n)_{n=0}^{\infty}$ egy degenerált asszociált Lucas sorozat az (M, N) relatív prím paraméterekkel. Ekkor v Pillai sorozat pontosan akkor, ha $(M, N) = (\pm 2, 1)$ vagy $(0, \pm 1)$ és itt mindkét esetben $g_v = G_v = 2$.*

Hasonlóan, legyen $\tilde{v} = (\tilde{v}_n)_{n=0}^{\infty}$ egy degenerált asszociált Lehmer sorozat az (M, N) relatív prím paraméterekkel. Ekkor $\tilde{v}$ pontosan akkor Pillai sorozat, ha $(M, N) = (0, \pm 1)$ és itt $g_{\tilde{v}} = G_{\tilde{v}} = 171$.

A lineáris rekurzív sorozatok vizsgálatát a tetszőleges r -edrendű oszthatósági sorozatokkal zárjuk le. A következő részben egy általános eredményt ismertetünk a T -Pillai tulajdonságról.

3.3. Általános oszthatósági sorozatok

Legyen $u = (u_n)_{n=0}^{\infty}$ egy r -edrendű lineáris rekurzív sorozat. Azt mondjuk, hogy u nem degenerált, ha az

$$x^r - c_{r-1}x^{r-1} - \cdots - c_1x - c_0$$

polinom különböző $\alpha_1, \dots, \alpha_t$ gyökeinek páronként vett hányadosai sohasem egységgyökök. Az u sorozatot oszthatósági sorozatnak fogjuk nevezni, amennyiben minden $i \mid j$ esetén $u_i \mid u_j$ teljesül.

Kiderül, hogy minden nem degenerált u oszthatósági sorozat T -Pillai sorozat, ha T ún. S -egészek egy részhalmaza, továbbá korlátot is adunk $G_u(T)$ értékére vonatkozóan. Általános eredményünk a következő.

3.10. Tétel. *Legyen S prímek egy tetszőleges véges halmaza, T pedig olyan egészek egy tetszőleges halmaza, hogy azoknak nincsen prímosztója S -en kívül. Legyen $u = (u_n)_{n=0}^\infty$ egy nem degenerált r -edrendű oszthatósági sorozat. Ha $r = 1$, akkor tegyük még fel, hogy u_1 -nek van S -en kívüli prímosztója. Ekkor u T -Pillai sorozat, továbbá*

$$g_u(T) \leq G_u(T) \leq C(s, r)$$

teljesül, ahol $|S| = s$ és

$$C(s, r) = \begin{cases} 2, & \text{ha } r = 1, \\ 20(s + 30) \log(s + 30), & \text{ha } r = 2, \\ r^{2^{8(s+r)}}, & \text{ha } r \geq 3. \end{cases}$$

3.4. Bizonyítások

A fejezet zárásaként a tételek bizonyításait és a háttérükben álló eredményeket ismertetjük. A könnyebb áttekinthetőség érdekében ezen a ponton további három részre tagoljuk a tárgyalást.

3.4.1. Lucas és Lehmer sorozatok

Az első lemma a Lucas és Lehmer sorozatok egy alapvető oszthatósági tulajdonságát mutatja.

3.11. Lemma. *Legyen $\hat{u} = (\hat{u}_n)_{n=0}^\infty$ egy Lucas vagy Lehmer sorozat. Ekkor minden $i, j \geq 0$ esetén*

$$\gcd(\hat{u}_i, \hat{u}_j) = \hat{u}_{\gcd(i, j)}.$$

Bizonyítás. Lásd [27] és [23]. ■

A következő eredmény pontos információt ad a Lucas és Lehmer sorozatokban az $|\hat{u}_n| = 1$ egyenlet összes n megoldásáról. Bár az állítás egyszerűen következik Beukers [4], illetve Bilu, Hanrot és Voutier [6] ismert mély eredményeiből, mi mégis különálló

tételként kezeljük, hiszen a ± 1 elemek multiplicitásának meghatározása önmagában is érdekes probléma. Tulajdonképpen Beukers [4] egy kérdését is megválaszoljuk a nem degenerált Lucas sorozatokban a ± 1 elemek multiplicitásait illetően.

3.12. Tétel. *Legyenek $u = (u_n)_{n=0}^\infty$, illetve $\tilde{u} = (\tilde{u}_n)_{n=0}^\infty$ nem degenerált Lucas, illetve Lehmer sorozatok az (M, N) paraméterekkel. Ekkor az $|u_n| = 1$ egyenlet egyetlen megoldása $u_1 = 1$, eltekintve a 4. táblázatbeli esetektől. Hasonlóan, az $|\tilde{u}_n| = 1$ egyenletnek csak $\tilde{u}_1 = \tilde{u}_2 = 1$ a két megoldása, eltekintve az 5. táblázatban foglalt esetektől. Az 5. táblázat harmadik sorában F_n az n -edik Fibonacci számot jelöli.*

(M, N)	Az n indexek, hogy $ u_n = 1$
$(\pm 1, N), N \neq 1, 2, 3, 5$	1, 2
$(M, M^2 \pm 1), M \geq 2$	1, 3
$(\pm 12, 55)$	1, 5
$(\pm 12, 377)$	1, 5
$(\pm 1, 3)$	1, 2, 5
$(\pm 1, 5)$	1, 2, 7
$(\pm 1, 2)$	1, 2, 3, 5, 13

4. táblázat. Nem degenerált Lucas sorozatok ± 1 elemei

(M, N)	Az n indexek, hogy $ \tilde{u}_n = 1$
$\pm(N \pm 1, N), N \geq 3$	1, 2, 3
$\pm(2N \pm 1, N), N \geq 3$	1, 2, 4
$\pm(F_{n \pm 2}, F_n), n \geq 4$	1, 2, 5
$\pm(1, 5)$	1, 2, 7
$\pm(13, 4)$	1, 2, 7
$\pm(14, 9)$	1, 2, 7
$\pm(5, 2)$	1, 2, 4, 5
$\pm(3, 2)$	1, 2, 3, 4, 7
$\pm(1, 2)$	1, 2, 3, 5, 13

5. táblázat. Nem degenerált Lehmer sorozatok ± 1 elemei

Bizonyítás. Legyen $\hat{u}$ egy nem degenerált Lucas vagy Lehmer sorozat. Bilu, Hanrot és Voutier [6] eredményét alkalmazva látható, hogy az $|\hat{u}_n| = 1$ egyenletnek nincs megoldása, ha $n > 30$. Továbbá, az [6]-ban található Table 1 és Table 2 segítségével megadható minden sorozatban az összes olyan n index, hogy $\hat{u}_n$ -nek nincs primitív prímosztója, egyben az is, hogy mely n index esetén lesz $|\hat{u}_n| = 1$. Például, ha $\hat{u}$ egy Lucas sorozat és meg akarjuk oldani az $|\hat{u}_n| = 1$ egyenletet, akkor Table 1 mutatja, hogy egyrészt $\alpha = \pm \frac{1+\sqrt{-7}}{2}$, másrészt $\beta = \frac{1-\sqrt{-7}}{2}$. Így $M = \pm 1$ és $N = 2$ adódik.

Néhány "kisebb" n esetén a már említett táblázatok nem adnak információt, így további számolásra van szükség. Ezt is egy példán keresztül szemléltetjük. Tegyük fel, hogy $\hat{u}$ továbbra is egy Lucas sorozat és $|\hat{u}_3| = 1$. Mivel $\hat{u}_0 = 0$ és $\hat{u}_1 = 1$, az (1) reláció értelmében $\hat{u}_3 = M^2 - N$. Ebből $|\hat{u}_3| = 1$ miatt adódik, hogy M tetszőleges és $N = M^2 \pm 1$. Ugyanakkor $M \neq 0$, hiszen $\hat{u}$ nem degenerált. Egy teljesen hasonló gondolatmenet működik a Lehmer sorozatok esetében is.

A Lucas sorozatok esetében a számolások egyszerűsödnek Beukers [4] egy eredményének alkalmazásával, ahol Theorem 4 explicit módon megadja az összes olyan sorozatot, melyben több mint két ± 1 elem van. Megjegyezzük, hogy Beukers [4] degeneráltnak nevez minden olyan Lucas sorozatot, ahol α és β egész számok, azonban egyszerűen ellenőrizhető, hogy ezekben a sorozatokban legfeljebb két ± 1 elem található, amennyiben az α/β hányados nem egységgyök.

A fent részletezett eljárás segítségével nyerjük a 4. és 5. táblázatokat. ■

A sorozatok tulajdonságaival kapcsolatos eredmények után Hajdu és Saradha [16] egy tételét mondjuk, ki ami általános esetben explicit korlátot ad a $G(T)$ értékére.

3.13. Lemma. *Legyen T pozitív egészek tetszőleges véges halmaza, továbbá jelölje $T(x)$ az x -nél nem nagyobb T -beli elemek halmazát. Tegyük fel, hogy*

$$|T(x)| \leq \frac{x}{10 \log x}$$

teljesül minden $x \geq x_1$ esetén. Ekkor

$$G(T) \leq \max(425, 2x_1 + 1).$$

Bizonyítás. Lásd [16] Theorem 2.1. ■

Szükségünk lesz rá, hogy több konkrét T halmaz esetében is meghatározzuk a $g(T)$ és $G(T)$ pontos értékét. Ezt minden esetben Hajdu és Saradha [16] egy algoritmusával tesszük meg.

3.14. Lemma. *A 6. táblázat első oszlopában látható T halmazok esetén a $g(T)$ és $G(T)$ mennyiségek pontos értékeit a második és harmadik oszlopok tartalmazzák.*

T	$g(T)$	$G(T)$
$\{1\}$	17	17
$\{1, 2\}$	25	25
$\{1, 3\}$	43	43
$\{1, 5\}$	31	31
$\{1, 2, 3\}$	49	53
$\{1, 2, 4\}$	47	47
$\{1, 2, 5\}$	45	45
$\{1, 2, 7\}$	49	51
$\{1, 2, 3, 5\}$	81	81
$\{1, 2, 4, 5\}$	61	69
$\{1, 2, 3, 4, 6\}$	79	79
$\{1, 2, 3, 4, 7\}$	81	81
$\{1, 2, 3, 5, 13\}$	107	107

6. táblázat. A $g(T)$ és $G(T)$ értékei bizonyos T halmazokra

Bizonyítás. A $T = \{1\}$ eset Pillai [30] és Brauer [8] klasszikus eredménye. A $T = \{1, 2\}$, illetve $T = \{1, 2, 3\}$ halmazok esetét Hajdu és Saradha [16] adta meg. Minden más esetben a [16]-ban használt algoritmust követjük. Mivel az eljárás teljes részletezése túlságosan sok előkészületet igényelne, így csak a módszer fő lépéseit ismertetjük egy példán keresztül, pontos magyarázatért [16]-ot ajánljuk az olvasó figyelmébe.

Legyen $T = \{1, 2, 5\}$. [16]-ot követve, valamely k egymást követő egész között pontosan akkor nincs az összes többivel T -relatív prím, ha a $K := \{1, \dots, k\}$ halmaz "lefedhető" az $L := \{p : p \text{ prím}, p \neq 2, 5, p < k\} \cup \{4, 10, 25\}$ halmazzal. Pontosabban, akkor és csakis akkor, ha létezik egy $f : L \rightarrow K$ függvény az alábbi tulajdonságokkal:

- minden $l \in L$ esetén $f(l) \leq l$,
- $2 \mid f(10) - f(4)$ és $5 \mid f(10) - f(25)$,

- minden $i \in K$ esetén létezik olyan $i \neq j \in K$ és $l \in L$, hogy $i \equiv j \equiv f(l) \pmod{l}$.

Tegyük fel, hogy van egy ilyen f függvényünk. Ekkor a kínai maradéktételt alkalmazva találhatunk olyan $S_k := \{n+1, \dots, n+k\}$ egymást követő egészekből álló halmazt, hogy minden $l \in L$ és $i \in K$ esetén $l \mid i - f(l)$ pontosan akkor, ha $l \mid n+i$. Azaz találhatunk minden $n+i \in S_k$ esetén olyan $n+j \in S_k$ egész számot, hogy $\gcd(n+i, n+j) \in L$, így $\notin T$. Ily módon $n+i$ és $n+j$ nem T -relatív prímek.

Tehát, mivel $g(T) \geq g(\{1\}) = 17$, így $k_0 = 17$ -től kezdve minden k esetén vizsgáljuk, hogy létezik-e ilyen f függvény. Pontosabban, le kell fednünk vagy igazolnunk kell, hogy lehetetlen lefednünk a $K = \{1, \dots, k\}$ halmazt a fenti értelemben. Ehhez a [16]-ban található algoritmust használjuk. Kiderül, hogy $g(T) = 45$. Vegyük észre, hogy $|T| = 3$ miatt a 3.13 Lemma értelmében $G(T) \leq 425$. Meg kell tehát vizsgálnunk minden lehetséges lefedést $45 < k < 425$ esetén. Minél nagyobb k értéke, az algoritmus annál lassabb és lassabb lesz, így a [16]-ban látható heurisztikát is igénybe kell vegyük, ami tulajdonképpen egy lefedés "továbbgördítését" jelenti a következő k értékre. Végül kiderül, hogy minden egyes k esetén meg tudjuk adni a lefedéseket, így $G(T) = 45$ adódik, azaz az állítást egy részesetben beláttuk. Hasonló módon eljárva kapjuk a többi T halmazra is a $g(T)$, $G(T)$ értékeit. ■

Az ismertetett eszközökkel felvértezve nekiláthatunk a Lucas és Lemher sorozatokkal kapcsolatos tételek bizonyításainak.

A 3.1 Tétel bizonyítása. Legyen $u = (u_n)_{n=0}^\infty$ egy nem degenerált Lucas sorozat az (M, N) relatív prím paraméterekkel. A 3.11 Lemma alapján, tekintve a sorozat k darab egymást követő $u_{n+1}, \dots, u_{n+k}$ tagjait, ezek egyike, mondjuk u_{n+i} relatív prím az összes többi u_{n+j} -vel pontosan akkor, ha $\gcd(u_{n+i}, u_{n+j}) = u_{\gcd(n+i, n+j)} = \pm 1$. Legyen

$$T = \{n : |u_n| = 1\}.$$

A fenti észrevételeket figyelembe véve u pontosan akkor Pillai sorozat, ha $\mathbb{N}$ T -Pillai sorozat és ekkor $g_u = g(T)$, illetve $g_u = G(T)$ teljesül. Innen a 3.12 Tétel és a 3.14 Lemma, illetve az ott található táblázatok felhasználásával adódik a tétel. ■

A 3.2 Tétel bizonyítása. Az $F = (F_n)_{n=0}^\infty$ Fibonacci sorozat egyben Lucas sorozat is az $(M, N) = (1, -1)$ választással, ezért F Pillai sorozat a 3.1 Tétel miatt. Mivel csakis $F_1 = F_2 = 1$, ezért $g_F = G_F = 25$. Felhasználva a 3.14 Lemma bizonyításában bemutatott módszert a $T = \{1, 2\}$ esetre kapjuk, hogy az $F_{n_0}, \dots, F_{n_0+24}$ egymást követő Fibonacci

számok közül egyik sem relatív prím az összes többivel pontosan akkor, ha vagy

$$\begin{aligned} 3 \mid n_0, \quad 4 \mid n_0 + 2, \quad 5 \mid n_0 + 3, \quad 7 \mid n_0 + 4, \quad 11 \mid n_0 + 5, \\ 13 \mid n_0 + 7, \quad 17 \mid n_0, \quad 19 \mid n_0, \quad 23 \mid n_0 + 1 \end{aligned}$$

vagy

$$\begin{aligned} 3 \mid n_0, \quad 4 \mid n_0 + 2, \quad 5 \mid n_0 + 1, \quad 7 \mid n_0 + 6, \quad 11 \mid n_0 + 8, \\ 13 \mid n_0 + 4, \quad 17 \mid n_0 + 7, \quad 19 \mid n_0 + 5, \quad 23 \mid n_0. \end{aligned}$$

Innen a kínai maradéktételt alkalmazva kapjuk, hogy $n_0 = 208569474$ a legkisebb ilyen index. ■

A 3.3 Tétel bizonyítása. Nyilvánvaló módon a 3.1 Tétel bizonyításában látott gondolatmenet egy az egyben felhasználható a Lehmer sorozatok esetére is. Így újból a 3.12 Tételt és a 3.14 Lemmát, illetve az ott található táblázatokat felhasználva kapjuk az eredményt. ■

A 3.4 Tétel bizonyítása. Legyen $\hat{u} = (\hat{u})_{n=0}^{\infty}$ egy degenerált Lucas vagy Lehmer sorozat az (M, N) relatív paraméterekkel. A bizonyítás Lucas és Lehmer sorozatok esetében is ugyanazt a vonalat követi, így feltesszük, hogy $\hat{u}$ Lucas sorozat. Feltétel szerint az $x^2 - Mx + N$ polinom α és β gyökeinek hányadosa egységgyök. Könnyen ellenőrizhető, hogy α/β egy racionális vagy másodfokú algebrai egész szám, így α/β az alábbiak egyike:

$$\pm 1, \quad \pm i, \quad \pm \epsilon, \quad \pm \epsilon^2,$$

ahol $\epsilon = \frac{1+i\sqrt{3}}{2}$. Csak egy esetet részletezünk, a többinél hasonlóan járunk el. Tegyük fel, hogy $\alpha/\beta = -\epsilon$. Ekkor $M = (1 - \epsilon)\beta$ és $N = -\epsilon\beta^2$, azaz $M^2 = N$. Mivel M és N relatív prím egész számok, így csakis $(M, N) = (1, 1)$ állhat fenn, ugyanis $(M, N) = (-1, 1)$ esetén $\alpha/\beta \neq -\epsilon$. Ekkor a sorozat $0, 1, 1, 0, -1, -1, 0, 1, \dots$, alakú, így nem Pillai sorozat.

Ezt a gondolatmenetet követve kapjuk, hogy a degenerált Lucas sorozatok (M, N) paraméterei a következők lehetnek:

$$(M, N) = (0, \pm 1), (\pm 1, 1), (\pm 2, 1).$$

Hasonlóan Lehmer sorozatok esetében:

$$(M, N) = \pm(0, 1), \pm(1, 1), \pm(2, 1), \pm(3, 1), \pm(4, 1).$$

Ezeket a sorozatokat egyesével megvizsgálva kapjuk az állítást mind Lucas, mind Lehmer sorozatokra. ■

3.4.2. Asszociált Lucas és Lehmer sorozatok

Az asszociált Lucas és Lehmer sorozatok alapvető oszthatósági tulajdonságát mondja ki McDaniel [28] alábbi tétele.

3.15. Lemma. *Legyen $\hat{v} = (\hat{v}_n)_{n=0}^\infty$ egy asszociált Lucas vagy Lehmer sorozat. Legyen továbbá $m = 2^i m'$ és $n = 2^j n'$, ahol m', n' páratlan természetes számok. Ekkor*

$$\gcd(\hat{v}_m, \hat{v}_n) = \begin{cases} 1 \text{ vagy } 2, & \text{ha } i \neq j, \\ \hat{v}_{\gcd(m,n)}, & \text{ha } i = j. \end{cases}$$

Bizonyítás. Az állítás Main Theorem (ii) része [28]-ban. ■

Szükségünk lesz egy másik eredményre is. Hasonlóan a Lucas és Lehmer sorozatokhoz, kíváncsiak vagyunk az asszociált Lucas és Lehmer sorozatok ± 1 elemeinek multiplicitására. Itt Allen [2] egy eredményét használjuk.

3.16. Lemma. *Legyen u egy nem degenerált r -edrendű lineáris rekurzív sorozat. Ekkor az $|u_n| = 1$ egyenletnek csak véges sok n megoldása létezik.*

Bizonyítás. Lásd a Corollary 1.3.-at és az (1.11) észrevételt [2]-ben. ■

Az utolsó eszköz, amit használni fogunk a páratlan számok sorozatában adja meg a g és G értékét. Ez Hajdu és Saradha [16] egy tétele.

3.17. Lemma. *A páratlan számok A sorozata Pillai sorozat, és $g_A = G_A = 86$ is teljesül. Továbbá bármely $i \in \{0, 1, \dots, 86\}$ esetén van olyan $t \in \mathbb{N}$, hogy a $2t+1, 2t+3, \dots, 2t+171$ 86 darab egymást követő páratlan szám közül egyik sem relatív prím az összes többivel, és $\nu_2(2t+i) > \nu_2(2t+j)$ teljesül minden $i \neq j \in \{0, 1, \dots, 86\}$ esetén.*

Bizonyítás. Az, hogy A Pillai sorozat, adódik a [29] Theorem 1 állításából. Az állítás többi része a [16]-beli Theorem 2.8 és 2.10, illetve a bizonyításaikban szereplő konstrukciók következménye.

Most már minden adott, hogy az első tételt bebizonyítsuk.

A 3.5 Tétel bizonyítása. Legyen $\hat{v} = (\hat{v}_n)_{n=0}^\infty$ egy nem degenerált asszociált Lucas vagy Lehmer sorozat az (M, N) relatív prím paraméterekkel és tekintsük a sorozat egymást követő $\hat{v}_{n+1}, \dots, \hat{v}_{n+k}$ tagjait. A bizonyítást M és N paritásai alapján három esetre bontjuk.

1. eset: M páratlan, N páros. Legyen $i \in \{1, \dots, k\}$ olyan, hogy $\nu_2(n+i) > \nu_2(n+j)$ bármely $i \neq j \in \{1, \dots, k\}$ esetén, ahol $\nu_2(q)$ jelöli a 2 kitevőjét q prímfaktorizációjában. Nyilván mindig létezik ilyen i . A (3) és (4) relációkat figyelembe véve $\hat{v}$ minden tagja páratlan. Ekkor a 3.15 Lemma miatt $\gcd(\hat{v}_{n+i}, \hat{v}_{n+j}) = 1$, tehát $\hat{v}$ nem Pillai sorozat.

2. eset: M páratlan, N páratlan. Legyen $k = 2^\alpha$ valamilyen $\alpha > 0$ esetén. Ekkor léteznek olyan $i, j \in \{1, \dots, k\}$ számok, hogy $\nu_2(n+i) > \nu_2(n+j) > \nu_2(n+l)$ minden $l \in \{1, \dots, k\} \setminus \{i, j\}$ esetén. Vegyük észre, hogy a definiáló (3) és (4) relációk miatt a sorozat minden harmadik eleme páros. Azonban $\hat{v}_{n+i}$ és $\hat{v}_{n+j}$ egyszerre nem lehet páros, így a 3.15 Lemmát alkalmazva vagy $\gcd(\hat{v}_{n+i}, \hat{v}_{n+l}) = 1$ minden $i \neq l \in \{1, \dots, k\}$ esetén vagy $\gcd(\hat{v}_{n+j}, \hat{v}_{n+l}) = 1$ minden $j \neq l \in \{1, \dots, k\}$ esetén. Tehát $\hat{v}$ sem Pillai sorozat.

3. eset: M páros, N páratlan. Ha $\hat{v}$ asszociált Lucas sorozat, akkor (3) miatt a sorozat minden tagja páros, így $\hat{v}$ Pillai sorozat.

Legyen most $\hat{v}$ asszociált Lehmer sorozat. Ekkor (4) miatt a sorozat minden $\hat{v}_n$ tagjának paritása megegyezik n paritásával. A 3.15 Lemma szerint páratlan i, j indexekre $\gcd(\hat{v}_i, \hat{v}_j) = \hat{v}_{\gcd(i,j)}$. A $\hat{v}$ Pillai sorozat pontosan akkor, ha valamilyen k értéktől kezdve létezik olyan n , hogy minden páratlan $i \in \{n+1, \dots, n+k\}$ esetén létezik olyan $j \neq i \in \{n+1, \dots, n+k\}$ index, hogy $\gcd(\hat{v}_i, \hat{v}_j) \neq 1$. Legyen

$$T = \{t : |\hat{v}_t| = 1\}.$$

A 3.16 Lemma miatt T véges halmaz. Legyen most

$$T' = \{t \cdot 2^\alpha : t \in T, \alpha \geq 0\}.$$

Összegezve az eddigieket és [16] Theorem 2.10 alapján $\hat{v}$ Pillai sorozat csakis akkor, ha $\mathbb{N}$ T' -Pillai. Tekintve a 3.13 Lemmában definiált $T(x)$ függvényt, láthatjuk, hogy $T'(x) \leq |T| \log_2 x$, azaz $G(T')$ létezik, így igazoltuk az állítást. ■

A 3.6 Tétel bizonyítása. Legyen $L = (L_n)_{n=0}^\infty$ a Lucas számok sorozata. Mivel $M = 1$ és $N = -1$ páratlan relatív prím paraméterek, így a 3.5 Tétel miatt L nem Pillai sorozat. Az állítás második felét két lépésben bizonyítjuk. Először konstruktív módon megmutatjuk, hogy $g_L \leq 171$. Tekintsünk 86 egymást követő páratlan indexű $L_{n+1}, L_{n+3}, \dots, L_{n+171}$ Lucas számot. Mivel $|L_n| = 1$ csak $n = 1$ esetén teljesül, ezért a 3.17 Lemmát alkalmazva kapjuk, hogy valamilyen alkalmasan választott n mellett minden $i \in \{1, 3, \dots, 171\}$ esetén létezik olyan $i \neq j \in \{1, 3, \dots, 171\}$, melyekre $\gcd(L_{n+i}, L_{n+j}) \neq 1$. Vegyük észre, hogy

$3 \mid n + 84$, $3 \mid n + 86$ és $3 \mid n + 88$ közül mindig pontosan egy teljesül. Csak egy esetben adjuk meg az összes részletet, a másik kettőben azonos gondolatmenetet követünk. A ?? Lemma alapján feltehető, hogy $3 \mid n + 88$ és $\nu_2(n + 88) > \nu_2(n + j)$ minden $88 \neq j \in I := \{2, 4, \dots, 170\}$ esetén. Így minden $i \in I$ esetén létezik olyan $i \neq j \in I$, hogy $\nu_2(n + i) = \nu_2(n + j)$, azaz $\gcd(L_{n+i}, L_{n+j}) \geq 2$. Mivel L_{t+88} páros, így nem lehet relatív prím az összes többivel. Tehát $g_L \leq 171$.

Második lépésként tegyük fel, hogy $g_L \leq 170$. Ekkor van olyan $n \geq 0$, hogy az $L_{n+1}, \dots, L_{n+g_L}$ számok között egyik sem relatív prím az összes többivel. Tekintsük közöttük a páratlan indexű elemeket. Ekkor a 3.15 Lemma miatt ezekre is igaz, hogy egyik sem relatív prím az összes többivel. Ez ellentmond a 3.17 Lemma állításának. ■

A 3.7 Tétel bizonyítása. Legyen $v = (v_n)_{n=0}^\infty$ egy nem degenerált asszociált Lucas sorozat az (M, N) relatív prím paraméterekkel, T egészek egy tetszőleges halmaza és tekintsük a sorozat egymást követő $v_{n+1}, \dots, v_{n+k}$ tagjait. Az M és N paraméterek paritásai alapján két részre bontjuk az állítást.

1.eset: M páratlan, N páros vagy páratlan. A 3.5 Tétel miatt v nem Pillai sorozat, így nem lehet T -Pillai sem.

2.eset: M páros, N páratlan. Létezik olyan $i \in \{1, \dots, k\}$, hogy $\nu_2(n + i) > \nu_2(n + j)$ minden $i \neq j \in \{1, \dots, k\}$ esetén. Mivel v minden tagja páros a (3) reláció miatt, ezért a 3.15 Lemma alapján $\gcd(v_{n+i}, v_{n+j}) = 2$. Ha $2 \notin T$, akkor v nem T -Pillai sorozat, hiszen v_{n+i} minden másik taghoz T -relatív prím. Ellenkező esetben, mikor $2 \in T$, akkor pedig v T -Pillai sorozat, ugyanis $\gcd(\hat{v}_{n+i}, \hat{v}_{n+j}) = 2$ minden $i \neq j \in \{1, \dots, k\}$ esetén. ■

A 3.8 Tétel bizonyítása. Legyen $\hat{v} = (\hat{v}_n)_{n=0}^\infty$ egy degenerált Lucas vagy Lehmer sorozat az (M, N) relatív prím paraméterekkel. Mivel a bizonyítás asszociált Lucas és Lehmer sorozatok esetén is ugyanúgy történik, ezért most feltesszük, hogy $\hat{v}$ Lehmer sorozat. (Megjegyezzük, hogy a degenerált Lucas és Lehmer sorozatokra vonatkozó tétel bizonyításában Lucas sorozatot választottunk. Jelen esetben a Lehmer sorozatokkal kapcsolatos állítás numerikus érdekessége miatt az utóbbi mellett döntünk.) A degeneráltsági feltétel értelmében az $x^2 - \sqrt{M}x + N$ polinom α és β gyökeinek α/β hányadosa egységgyök. Ellenőrizhető továbbá, hogy α/β racionális vagy másodfokú algebrai egész, így a következők egyike:

$$\pm 1, \quad \pm i, \quad \pm \epsilon, \quad \pm \epsilon^2,$$

ahol $\epsilon = \frac{1+i\sqrt{3}}{2}$ továbbra is. Újból csak egy esetet vizsgálunk meg, az összes többire az igazolás hasonlóan történik. Tegyük fel, hogy $\alpha/\beta = \pm i$. Ekkor a 3.4 Tétel bizonyításában látott számolással (Viéte-formulák és relatív prím feltétel alkalmazásával) kapjuk, hogy $(M, N) = (0, 1)$. Ekkor a sorozatunk $2, 1, -2, -3, 2, 5, -2, -7, 2, 9, 2, -11, 2, \dots$ alakot ölt. Vegyük észre, hogy minden páros indexű tag ± 2 . Legyen

$$T = \{2^\alpha : \alpha \geq 0\}.$$

Vegyük a sorozat k egymást követő $\hat{v}_{n+1}, \dots, \hat{v}_{n+1k}$ tagját. Mivel a sorozat páros indexű tagjainak legnagyobb közös osztója pontosan 2, így $\hat{v}$ sorozat Pillai pontosan akkor, ha minden páratlan $i \in \{1, \dots, k\}$ esetén van olyan páratlan $i \neq j \in \{1, \dots, k\}$, hogy $\gcd(\hat{v}_{n+i}, \hat{v}_{n+j}) = v_{\gcd(n+i, n+j)} \neq 1$. Ez a 3.17 Lemma miatt pontosan akkor igaz, ha van legalább 86 egymást követő páratlan indexű tag. Azaz $g_{\hat{v}} = G_{\hat{v}} = 171$. ■

3.4.3. Általános oszthatósági sorozatok

A 3.10 Tétel bizonyításához szükségünk lesz egy végeességi tételre a nem degenerált $r \geq 2$ rendű lineáris rekurzív sorozatokban található S -egészek számát illetően, azaz olyan tagok számának végeességére, melyeknek nincs egy rögzített S prímhalmaz elemein kívül prímosztója. Ez következik Schlickewei és Schmidt [33] alábbi mély, polinomiális exponenciális egyenletek megoldásainak számára vonatkozó tételéből.

3.18. Lemma. *Legyen $r \geq 2$, $u = (u_n)_{n=0}^\infty$ pedig egy nem degenerált r -edrendű lineáris rekurzív sorozat, továbbá $p_1, \dots, p_s$ különböző prímek. Ekkor az*

$$u_n = p_1^{z_1} \dots p_s^{z_s}$$

egyenletnek legfeljebb $r^{2^{7(s+r)}}$ megoldása van, ha $n, z_1, \dots, z_s$ nemnegatív egészek.

Bizonyítás. Ismert tény, hogy a sorozat n -edik tagja felírható

$$u_n = \sum_{i=1}^t P_i(n) \alpha_i^n$$

alakban, ahol $\alpha_1, \dots, \alpha_t$ a sorozat karakterisztikus polinomjának különböző gyökei, $P_i(n)$ pedig az α_i multiplicitásával egyező fokú, $\mathbb{Q}(\alpha_1, \dots, \alpha_t)$ -beli együtthatójú polinomok. Ekkor a fenti egyenlet

$$\sum_{i=1}^t P_i(n) \alpha_i^n - p_1^{z_1} \dots p_s^{z_s} = 0$$

alakba írható. Így a [33] Theorem 1 tétele miatt a [33] Theorem 2.1 bizonyításához hasonló számolással adódik az állítás. ■

A lemma segítségével most már igazolni tudjuk az általános tételünket.

A 3.9 Tétel bizonyítása. Legyen $S = \{p_1, \dots, p_s\}$ prímek egy tetszőleges véges halmaza, T pedig olyan egészek egy tetszőleges halmaza, hogy azoknak nincsen prímosztója S -en kívül. Legyen továbbá $u = (u_n)_{n=0}^\infty$ egy nem degenerált r -edrendű oszthatósági sorozat.

Tegyük fel először, hogy $r = 1$ és u_1 -nek van S -en kívüli prímosztója. Ekkor minden $i \geq 1$ esetén $u_1 \mid \gcd(u_i, u_j)$ (hiszen u oszthatósági sorozat), azaz $\gcd(u_i, u_j) \notin T$. Így u T -Pillai sorozat és $g_u(T) = G_u(T) = 2$.

Legyen most $r \geq 2$ és

$$H := \{n : u_n \in T\}.$$

Legyen először $r = 2$. Ekkor Győry és Pethő [14] egy eredményéből kapjuk, hogy u egy Lucas sorozat konstansszorosa. Legyen $u = tU$, ahol U egy Lucas sorozat, t pedig nem nulla egész szám. Vegyük észre, hogy ha U T -Pillai sorozat, akkor u is az és $g_u(T) \leq g_U(T)$, illetve $G_u(T) \leq G_U(T)$ teljesül. Az általánosság megszorítása nélkül feltehető, hogy $t = 1$, azaz u egy Lucas sorozat. Ekkor Bilu, Hanrot és Voutier [6] egy tétele miatt minden $n > 30$ esetén u_n -nek van primitív prímosztója, továbbá a $p_1, \dots, p_s$ prímek mindegyike legfeljebb egy elemnek lehet primitív prímosztója. Így kapjuk, hogy $|H| \leq s + 30$. Alkalmazva a 3.13 Lemmát adódik, hogy $g(H)$ és $G(H)$ létezik, továbbá egyszerű számolás eredményeként

$$G(H) \leq 20(s + 30) \log(s + 30).$$

Legyen $k = g(H)$ vagy $k \geq G(H)$. Ekkor létezik egy $n \geq 1$ egész szám, hogy $n+1, \dots, n+k$ közül egyik sem H -relatív prím az összes többivel. Azaz, minden $i \in \{1, \dots, k\}$ esetén létezik olyan $i \neq j \in \{1, \dots, k\}$, hogy $\gcd(n+i, n+j) = d \in H$. Figyelembe véve u oszthatósági tulajdonságát és H definícióját, $\gcd(u_{n+i}, u_{n+j}) = u_d \in T$ adódik. Tehát az is teljesül, hogy $u_n, \dots, u_{n+k-1}$ közül egyik sem T -relatív prím az összes többivel és így

$$g_u(T) \leq g(H) \text{ és } G_u(T) \leq G(H).$$

Azaz $r = 2$ esetre az állítás igaz.

Legyen most $r \geq 3$. A 3.18 Lemma miatt $|H| \leq r^{2^{7(s+r)}}$ teljesül. Ettől a ponttól a bizonyítás menete megegyezik az $r = 2$ esetével és egyszerű számolással adódik a tétel helyessége. ■

4. Elliptikus oszthatósági sorozatok

Ebben a fejezetben más típusú rekurzív sorozatok, az ún. elliptikus oszthatósági sorozatok kerülnek górcső alá. A fogalom elliptikus görbék segítségével való megadása után az új eredmények közül elsőként egy tételt fogalmazunk meg arra vonatkozóan, hogy minden elliptikus oszthatósági sorozat Pillai, majd egy másikat is, miszerint a sokkal általánosabb T -Pillai sorozat tulajdonságot is kielégítik. Végül kiszámítjuk a g és G mennyiségek pontos értékeit néhány, Silverman és Stephens [38] által adott konkrét sorozat esetében. A fejezet végén a bizonyítások találhatók azokkal a klasszikusnak számító eredményekkel együtt, melyekre támaszkodni fogunk - ez egyben betekintést enged az elliptikus oszthatósági sorozatok irodalmának egy kicsiny szeletébe is.

4.1. Új eredmények

Az elliptikus oszthatósági sorozatok bevezetéséhez szükségünk van néhány, elliptikus görbékkel kapcsolatos fogalomra (Weierstrass-alak, racionális pont, torziós pont). Mivel ezek a terület alapvető fogalmai közé tartoznak, így itt most nem adjuk meg őket, csupán a [12] és a [39] hivatkozásokat említjük meg. Legyen E egy Weierstrass alakban adott elliptikus görbe $\mathbb{Q}$ felett. Legyen $P = (x(P), y(P))$ egy olyan racionális pont, amely nem torziópont. Minden $n \neq 0$ egész szám esetén legyen $x(nP)$ az A_n/B_n alakban adott, ahol $A_n \in \mathbb{Z}$, $B_n \in \mathbb{N}$ és $\gcd(A_n, B_n) = 1$. Ekkor a $B = B(E, P) = (B_n)_{n=1}^{\infty}$ sorozatot elliptikus oszthatósági sorozatnak nevezzük. Ez a megadás tulajdonképpen Ward [42] elliptikus oszthatósági sorozat definíciójának bizonyos nem degenerált eseteit tartalmazza. Megjegyezzük, hogy mint az jól ismert, B_n teljes négyzet, így B_n helyett többször is a $\pm(\sqrt{B_n})_{n=0}^{\infty}$ sorozatokat tekintik. Ugyanakkor vizsgálataink szempontjából nem szükséges, mivel a mi szempontunkból csak B_n prímosztói fontosak, azok hatványai tulajdonképpen lényegtelenek. Végül megjegyezzük, hogy az elliptikus oszthatósági sorozatok nemlineáris rekurzió segítségével is megadhatóak.

Ebben a szakaszban az új eredményeinket fogalmazzuk meg. Fő tételünk az alábbi.

4.1. Tétel. *Minden $B = B(E, P) = (B_n)_{n=0}^{\infty}$ elliptikus oszthatósági sorozat Pillai sorozat, továbbá $G_B \leq C_2(E, P)$, ahol $C_2(E, P)$ egy csakis E -től és P -től függő explicit módon megadható konstans.*

Következő tételünk egy általánosabb esettel foglalkozik. Kiderül, hogy minden $B = B(E, P) = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozat T -Pillai sorozat, amennyiben T elemeinek egy véges prímhalmazból kerülnek ki a prímosztói.

4.2. Tétel. *Legyen S prímszámok egy tetszőleges véges halmaza, $|S| = s$, továbbá legyen T olyan egészek tetszőleges halmaza, melyeknek nincs S -en kívüli prímosztója. Ekkor minden $B = B(E, P) = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozat T -Pillai sorozat, továbbá $G_B(T) \leq C_3(E, P)$, ahol $C_3(E, P, s)$ egy csakis E -től, P -től és s -től függő explicit módon megadható konstans.*

4.3. Megjegyzés. *Megjegyezzük, hogy ennek az eredménynek a 4.1 Tétel azonnali következménye. Ugyanakkor a 4.1 Tétel könnyebb érthetősége és egyszerűbb eszközöket igénylő bizonyítása miatt mégis külön tételeként kezeljük őket.*

Utolsó eredményünk numerikus természetű. Néhány Silverman és Stephens [38] által adott konkrét elliptikus görbéhez tartozó $B = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozat esetén megadjuk a g_B és G_B mennyiségek pontos értékeit. Ezek a sorozatok nem lesznek mások, mint az Example 2-5 példák [38]-ban. Megjegyezzük, hogy további két példát is megadtak a szerzők [38]-ban, de míg az Example 1 és Example 2 egybeesik, addig az Example 6 egy degenerált esetet tartalmaz, így azzal jelen keretek között nem foglalkozunk.

4.4. Tétel. *Az 7. Táblázat első és második oszlopában látható E elliptikus görbékhez és P pontokhoz tartozó $B = B(E, P) = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozatokhoz tartozó g_B és G_B pontos értékeit a 7. táblázat harmadik és negyedik oszlopai tartalmazzák.*

E	$P = (x(P), y(P))$	g_B	G_B
$y^2 + y = x^3 - x$	(0,0)	79	79
$y^2 + y = x^3 + x^2$	(0,0)	81	81
$y^2 + xy = x^3 - x^2 - x + 1$	(1,0)	47	47
$y^2 + xy = x^3 - 3x + 1$	(1,0)	81	81

7. táblázat. A g_B és G_B értékei néhány elliptikus oszthatósági sorozatra

4.2. Bizonyítások

A következőkben az elliptikus oszthatósági sorozatokkal kapcsolatos néhány fontosabb ismert eredményt mutatunk be. Az első Everest, McLaren és Ward [13] nevéhez fűződik és az elliptikus oszthatósági sorozatok egy alapvető tulajdonságát mondja ki.

4.5. Lemma. *Minden $B = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozat erős oszthatósági sorozat, azaz bármely $i, j \in \mathbb{N}$ esetén*

$$\gcd(B_i, B_j) = B_{\gcd(i,j)}.$$

Bizonyítás. Lásd a Lemma 12 [13]-ban. ■

Silverman [35] alapvető eredménye, hogy minden elliptikus oszthatósági sorozatra igaz az alábbi növekedési tulajdonság.

4.6. Lemma. *Legyen $B = B(E, P) = (B_n)_{n=0}^\infty$ egy elliptikus oszthatósági sorozat. Ekkor léteznek olyan pozitív, csakis E -től és P -től függő explicit módon megadható $N_1(E, P)$ és $C_1(E, P)$ konstansok, hogy bármely $n \geq N_1(E, P)$ esetén*

$$\log B_n \geq C_1(E, P)n^2.$$

Bizonyítás. A [35]-beli Lemma 8 egyszerű következménye. ■

Végül Silverman [35] egy másik nagyon fontos eredményét említjük meg, pontosabban az elliptikus oszthatósági sorozatok tagjainak primitív prímosztóiról mondunk ki egy állítást.

4.7. Lemma. *Legyen $B = B(E, P) = (B_n)_{n=0}^\infty$ egy elliptikus oszthatósági sorozat. Ekkor létezik olyan pozitív, csakis E -től és P -től függő explicit módon megadható $N_2(E, P)$ konstans, hogy bármely $n \geq N_2(E, P)$ esetén a sorozat B_n tagjának van primitív prímosztója.*

Bizonyítás. A [35]-beli Lemma 9 azonnali következménye az állítás. ■

Most már minden szükséges ismerettel rendelkezünk ahhoz, hogy eredményeink igazolásához hozzáláthassunk.

A 4.1. Tétel bizonyítása. Legyen $B = B(E, P) = (B_n)_{n=0}^\infty$ egy elliptikus oszthatósági sorozat és legyen

$$T = \{n : B_n = 1\}.$$

Tekintsük a sorozat k darab egymást követő $B_{t+1}, B_{t+2}, \dots, B_{t+k}$ tagját. A 4.5 Lemma miatt

$$\gcd(B_{n+i}, B_{n+j}) = B_{\gcd(n+i, n+j)}.$$

Vegyük észre, hogy az erős oszthatósági tulajdonság miatt $\gcd(B_{n+i}, B_{n+j}) = 1$ pontosan akkor, ha $\gcd(n+i, n+j) \in T$. Más szavakkal, a sorozat két tagja pontosan akkor relatív prím egymással, ha indexeik T -relatív prímek. A 4.6 Lemmából következik, hogy $|T| \leq C_1(E, P)$, így a 3.13 Lemma értelmében $\mathbb{N}$ ekkor T -Pillai sorozat. Ebből következik, hogy B Pillai sorozat, továbbá $g(T) = g_B$ és $G(T) = G_B$ teljesül. Mivel T véges, így a 3.13 Lemmából $G(T) \leq C_2(E, P)$ következik, amiből a tétel azonnal adódik. ■

A 4.2. Tétel bizonyítása. Legyen S prímszámok egy tetszőleges véges halmaza, hogy $|S| = s$ és T olyan egészek tetszőleges halmaza, melyeknek nincs S -en kívüli prímosztója. Legyen továbbá $B = B(E, P) = (B_n)_{n=0}^\infty$ elliptikus oszthatósági sorozat. Legyen

$$T' = \{n : B_n \in T\}.$$

A 4.7 Lemma miatt létezik egy pozitív, csakis E -től és P -től függő $N_2(E, P)$ konstans, hogy minden $n \geq N_2(E, P)$ esetén B_n -nek van primitív prímosztója. Ebből adódik, hogy $|T'| \leq C_4(E, P, s)$. Így a 3.13 Lemma miatt $\mathbb{N}$ T' -Pillai sorozat, továbbá $G(T') \leq C_2(E, P, s)$ valamely csakis E -től, P -től és s -től függő explicit módon megadható $C_2(E, P, s)$ konstanssal. Az erős oszthatósági tulajdonságot a 4.1 Tétel bizonyításában látott módon felhasználva kapjuk, hogy B ekkor T -Pillai sorozat és $G_B(T) = G(T')$. Ezzel a bizonyítás véget ért. ■

A 4.3 Tétel bizonyítása. Bármely a 7. táblázatban látható (E, P) párra legyen a hozzájuk tartozó elliptikus oszthatósági sorozat $B = B(E, P)$. Legyen minden B esetén

$$T_B = \{n : B_n = 1\}.$$

A Magma [7] matematikai programcsomag használatával - egyszerű számolás segítségével - az összes egész pontot megtalálhatjuk az E elliptikus görbéken és kapjuk, hogy a T_B halmazok pontosan a 8. táblázatban látható halmazok. Felidézve a 4.1 Tétel bizonyítását láthatjuk, hogy B Pillai sorozat, továbbá $g_B = g(T_B)$ és $G_B = G(T)$. Innen a 3.14 Lemma használatával kapjuk a g_B és G_B mennyiségek értékeit. Ezzel a bizonyítás befejeződött. ■

E	$P = (x(P), y(P))$	T_B
$y^2 + y = x^3 - x$	(0,0)	$\{1, 2, 3, 4, 6\}$
$y^2 + y = x^3 + x^2$	(0,0)	$\{1, 2, 3, 4, 7\}$
$y^2 + xy = x^3 - x^2 - x + 1$	(1,0)	$\{1, 2, 4\}$
$y^2 + xy = x^3 - 3x + 1$	(1,0)	$\{1, 2, 3, 5\}$

8. táblázat. A T_B halmazok néhány elliptikus oszthatósági sorozatra

Hivatkozások

- [1] **J. J. Alba González, F. Luca and L. E. Shparlinski**, *On numbers n dividing the n th term of a linear recurrence*, Proc. Edinb. Math. Soc. **55** (2012) 271-289.
- [2] **P. B. Allen**, *Multiplicities of linear recurrence sequences*, Master thesis, University of Waterloo, 2006.
- [3] **F. Amoroso and E. Viada**, *On the zeros of linear recurrence sequences*, Acta Arith. **147** (2011) 387-396.
- [4] **F. Beukers**, *The multiplicity of binary recurrences*, Compos. Math. **40** (1980), 251-267
- [5] **J. P. Bézivin, A. Pethő and A. J. van der Poorten**, *A full characterization of divisibility sequences*, Amer. J. Math. **112** (1990) 985-1001.
- [6] **Y. Bilu, G. Hanrot and P. M. Voutier**, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001) 75-122.
- [7] **W. Bosma, J. Cannon, and C. Playoust**, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235–265.
- [8] **A. T. Brauer**, *On a property of k consecutive integers*, Bull. Amer. Math. Soc. **47** (1941) 328-331.
- [9] **B. Brindza, K. Liptai and L. Szalay**, *On products of the terms of linear recurrences*, Proc. of Number Theory Conf., Eger 1996, 1998, 101-106.

- [10] **B. Brindza, Á. Pintér and W. M. Schmidt**, *Multiplicities of binary recurrences*, Canad. Math. Bull. **44** (2001) 19-21.
- [11] **Y. Caro**, *On a division property of consecutive integers*, Israel J. Math. **33** (1979) 32-36.
- [12] **J. W. S. Cassels**, *Lectures on Elliptic Curves*, London Math. Soc. Stud. Texts **24** (Cambridge University Press, Cambridge, 1991).
- [13] **G. Everest, G. McLaren and T. Ward**, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006) 71-89.
- [14] **K. Győry and A. Pethő**, *On second order linear divisibility sequences over algebraic number fields*, Publ. Math. Debrecen **39** (1991) 171-179.
- [15] **K. Győry and C. Smyth**, *The divisibility of $a^n - b^n$ by powers of n* , Integers **10** (2010) 319-334
- [16] **L. Hajdu and N. Saradha**, *On a problem of Pillai and its generalizations*, Acta Arith. **144** (2010) 323-347.
- [17] **L. Hajdu and M. Szikszai**, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory **132** (2012) 3056-3069.
- [18] **L. Hajdu and M. Szikszai**, *On common factors within a series of consecutive terms of an elliptic divisibility sequence*, Arch. der Math, közlésre benyújtva.
- [19] **L. Hajdu and M. Szikszai**, *On the GCD-s of k consecutive terms of associated Lucas and Lehmer sequences*, előkészületben.
- [20] **P. Horák and L. Skula**, *A characterisation of the second-order strong divisibility sequences*, Fibonacci Quarterly, Vol. **23** (1985) 126-132.
- [21] **K. K. Kubota**, *On a conjecture of Morgan Ward, I*, Acta Arith. **33** (1977) 11-28.
- [22] **K. K. Kubota**, *On a conjecture of Morgan Ward, II*, Acta Arith. **33** (1977) 29-48.
- [23] **D. H. Lehmer**, *An extended theory of Lucas' functions*, Ann. of Math. **31** (1930) 419-448.

- [24] **F. Luca and T. N. Shorey**, *Diophantine equations with products of consecutive terms in Lucas sequences*, J. Number Theory **114** (2005) 541-560.
- [25] **F. Luca and T. N. Shorey**, *Diophantine equations with products of consecutive terms in Lucas sequences, II*, Acta Arith. **133** (2008) 53-71.
- [26] **F. Luca and T. N. Shorey**, *Products of members of Lucas sequences with indices in an interval being a power*, J. Number Theory **129** (2009) 303-315.
- [27] **E. Lucas**, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878) 184-240., 289-321.
- [28] **W. L. McDaniel**, *The G.C.D. in Lucas sequences and Lehmer number sequences*, Fibonacci Quartl. **29** (1991) 24-29.
- [29] **M. Ohtomo and F. Tamari**, *On relative prime number in a sequence of positive integers*, J. Statist. Plann. Inference **106** (2002) 509-515.
- [30] **S. S. Pillai**, *On M consecutive integers - I*, Proc. Indian Acad. Sci., Section A **11** (1940) 6-12.
- [31] **J. Reynolds** *Perfect powers in elliptic divisibility sequences*, J. Number Theory **132** (2012) 998-1015.
- [32] **A. Schinzel**, *Second order strong divisibility sequences in an algebraic number field*, Arch. Math. **23** (1987) 181-186.
- [33] **H.-P. Schlickewei and W. M. Schmidt**, *The number of solutions of polynomial-exponential equations*, Compos. Math. **120** (2000) 193-225.
- [34] **T. N. Shorey and R. Tijdeman**, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge 1986.
- [35] **J. H. Silverman**, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1998) 226-237.
- [36] **J. H. Silverman**, *Common divisors of elliptic divisibility sequences over function fields*, Manuscripta Math. **114** (2004) 432-446.

- [37] **J. H. Silverman**, *p-adic properties of division polynomials and elliptic divisibility sequences*, Math. Ann. **332** (2005) 443-471.
- [38] **J. H. Silverman and N. Stephens**, *The sign of an elliptic divisibility sequences*, Journal of Ramanujan Math. Soc. **21** (2006) 1-17.
- [39] **J. H. Silverman and J. Tate**, *Rational Points on Elliptic Curves*, Undergrad. Texts Math. (Springer-Verlag, New York, 1992).
- [40] **C. Smyth**, *The terms in Lucas sequences divisible by their indices*, J. Integer Seq. **13** (2010), Article 10.2.4.
- [41] **C. S. Swart**, *Elliptic divisibility sequences*, Ph.D. thesis, (Royal Holloway (University of London) 2003).
- [42] **M. Ward**, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948) 31-74.
- [43] **M. Ward**, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. **15** (1948) 941-946.