

Debreceni Egyetem
Természettudományi Kar
Matematikai Intézet

Szakdolgozat

Rekurzív sorozatok oszthatósága

készítette:

Barta Attila
Matematika BSc szakos hallgató

témavezető:

Dr. Tengely Szabolcs
egyetemi adjunktus

Debrecen, 2016

TARTALOMJEGYZÉK

Tartalomjegyzék	i
1 Rekurzív sorozatok	2
2 Bináris rekurziók	4
2.1. A zárt formula	4
2.2. A Fibonacci sorozat zárt alakja	5
2.3. Rekurzív rend	6
2.4. A Fibonacci sorozat rekurzív rendje	13
3 Általános lineáris csoport	15
4 Sage kódok	17
Irodalomjegyzék	20

BEVEZETŐ

Szakedolgozatomban a bináris rekurziókban fellépő oszthatósági szabályokat vizsgáljuk.

Az első fejezetben általánosan definiáljuk a rekurzív sorozat fogalmát és egy példán keresztül bemutatjuk a sorozat n -edik tagjának explicit megadási módját.

A második fejezetben definiáljuk a bináris rekurziót és a továbbiakban ezeket a sorozatokat fogjuk vizsgálni mátrixos formában a bennük fellelhető periódusok szerint.

A harmadik fejezetben a csoportelmélet alapján adunk oszthatósági szabályokat.

A negyedik fejezetben a Sage programot használva, tetszőleges prímre adunk olyan sorozatokat, amelyekben különböző oszthatóságok lépnek fel.

1. REKURZÍV SOROZATOK

1.0.1. Definíció. Egy S halmaz feletti $(s_i)_{i \in \mathbb{N}} = (s_0, s_1, s_2, \dots, s_i, \dots)$ végtelen sorozatot m -edrendben rekurzívnak nevezünk, ha létezik olyan m -változós

$$F : S^m \longrightarrow S$$

függvény, mellyel tetszőleges nemnegatív egész i -re

$$s_{i+m} = F(s_i, s_{i+1}, \dots, s_{i+m-1}).$$

A következőkben egy ismertebb matematikai játékról, a Hanoi tornyairól és az ehhez kapcsolható rekurzióról lesz szó. Összesen három rúd áll rendelkezésre és a játék szabályai szerint az első rúdról az utolsóra kell átrakni a korongokat úgy, hogy minden lépésben egy korongot lehet áttenni, nagyobb korong pedig nem tehető kisebb korongra.

Mennyi a legkevesebb szükséges lépés, amivel az első rúdról a harmadik rúdra lehet juttatni a korongokat?

A megoldáshoz szükséges lépésszámot a következő rekurzió írja le:

$$t_n = 2^n - 1,$$

ahol n az átpakolni kívánt korongok száma.

Bizonyítás. A bizonyítás teljes indukcióval történik.

$n = 1$ esetben a lépések száma 1.

Tegyük fel, hogy n darab korong esetén a megoldásszám t_n .

Ekkor $t_{n+1} = 2t_n + 1$, mivel n darabot t_n lépéssel tudunk áttenni a középső rúdra és a legelső helyrerakása után szintúgy t_n lépés kell, hogy a harmadik rúdra helyezzük őket.

Jelölje T a rekurzióhoz csatolható mátrixot: $T = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$. T sajátértékei 2

és 1. Legyen $D = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. A sajátvektorokból álló mátrix: $S = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = S^{-1}$.

Ekkor $T \begin{pmatrix} t_{n-1} \\ 1 \end{pmatrix} = \begin{pmatrix} t_n \\ 1 \end{pmatrix}$.

Ezután kapjuk, hogy

$$T^{n-1} = SD^{(n-1)}S^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 2^{n-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 2^{n-1} & 2^{n-1} - 1 \\ 0 & 1 \end{pmatrix}$$

.

Így eljutunk az explicit alakhoz:

$$\begin{pmatrix} 2^{n-1} & 2^{n-1} - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2^n - 1 \\ 1 \end{pmatrix} = \begin{pmatrix} t_n \\ 1 \end{pmatrix}$$

.

□

2. BINÁRIS REKURZIÓK

A következőkben a bináris rekurziókkal fogunk részletesebben foglalkozni.

2.0.2. Definíció. Egy

$$s_i = c_1 s_{i-1} + c_2 s_{i-2} + \dots + c_m s_{i-m}$$

képlettel ellátott rekurziót m -edfokú lineáris rekurciónak nevezünk ($c_i \in \mathbb{R}$).

2.1. A zárt formula

Az $s_n = u s_{n-1} + v s_{n-2}$ rekurzió felírható a következő alakban:

$$s_n = \begin{pmatrix} u & v \end{pmatrix} \begin{pmatrix} s_{n-1} \\ s_{n-2} \end{pmatrix}.$$

Legyen az M mátrix a következő:

$$M = \begin{pmatrix} s_2 & v s_1 \\ s_1 & v s_0 \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & 0 \end{pmatrix}.$$

2.1.1. Tétel.

$$M^n = \begin{pmatrix} s_{n+1} & v s_n \\ s_n & v s_{n-1} \end{pmatrix}.$$

Bizonyítás. A bizonyítást teljes indukcióval végezzük.

Az $n = 1$ esetben M definíciójából adódik az állítás.

Tegyük fel, hogy n -re igaz. Ekkor

$$\begin{aligned} M^{n+1} &= M M^n = \begin{pmatrix} u & v \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s_{n+1} & v s_n \\ s_n & v s_{n-1} \end{pmatrix} = \\ &= \begin{pmatrix} u s_{n+1} + v s_n & u v s_n + v^2 s_{n-1} \\ s_{n+1} & v s_n \end{pmatrix} = \begin{pmatrix} s_{n+2} & v s_{n+1} \\ s_{n+1} & v s_n \end{pmatrix}. \end{aligned}$$

□

Az M mátrix karakterisztikus polinomjának gyökeit jelölje ezentúl α és β :

$$\alpha = \frac{u + \sqrt{u^2 + 4v}}{2}, \quad \beta = \frac{u - \sqrt{u^2 + 4v}}{2}.$$

Számoljuk ki az α sajátértékhez tartozó $\begin{pmatrix} X \\ Y \end{pmatrix}$ sajátvektort. Ehhez a következő lineáris egyenletrendszeret oldjuk meg:

$$\begin{pmatrix} u - \alpha & v \\ 1 & -\alpha \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} = 0,$$

ami ekvivalens az

$$(u - \alpha)X + vY = X - \alpha Y$$

egyenlettel. Ebből adódóan

$$(u - \alpha - 1)X = (-v - \alpha)Y.$$

Hasonlóan kaphatjuk a β -hoz tartozó sajátvektort.

Jelölje T a sajátvektorokból álló mátrixot és legyen $D = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$.

Ha $\alpha \neq \beta$, akkor a megfelelő sajátvektorok segítségével az M mátrix felírható a következő alakban:

$$M = TDT^{-1}.$$

Ekkor

$$M^n = (TDT^{-1})^n = TD^nT^{-1} = T \begin{pmatrix} \alpha^n & 0 \\ 0 & \beta^n \end{pmatrix} T^{-1}.$$

2.2. A Fibonacci sorozat zárt alakja

A következőkben a [2] cikket használtuk fel.

A Fibonacci sorozatot a következőképp definiáljuk:

$$F_0 = 0, \quad F_1 = 1,$$

$$F_n = F_{n-1} + F_{n-2}.$$

Ebben az esetben a rekurzió együtthatói: $u = 1$ és $v = 1$.

Ekkor a fentebb leírtak alapján:

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

A következő azonosságok teljesülnek:

$$\alpha^2 = \alpha + 1, \quad \beta^2 = \beta + 1, \quad \alpha - \beta = \sqrt{5}, \quad \alpha + \beta = 1, \quad \frac{1}{\alpha} = -\beta, \quad \frac{1}{\beta} = -\alpha.$$

Legyen M a rekurzió mátrixa. Ekkor a sajátvektorokat a következőképp számoljuk:

$$\alpha I - M = \begin{pmatrix} \alpha - 1 & -1 \\ -1 & \alpha \end{pmatrix} \longrightarrow \begin{pmatrix} \alpha & -(\alpha + 1) \\ -1 & \alpha \end{pmatrix} =$$

$$\begin{pmatrix} \alpha & -\alpha^2 \\ -1 & \alpha \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & -\alpha \\ -1 & \alpha \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & -\alpha \\ 0 & 0 \end{pmatrix}.$$

β esetben hasonlóképpen eljárva kapjuk, hogy diagonalizáláshoz a bázistranszformáció mátrixa:

$$T = \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix}.$$

Ennek a mátrixnak az inverze:

$$T^{-1} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & -\beta \\ -1 & \alpha \end{pmatrix}.$$

Ezek után már könnyen tudjuk M hatványát számolni:

$$M^n = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha^n & 0 \\ \beta^n & 0 \end{pmatrix} \begin{pmatrix} 1 & -\beta \\ -1 & \alpha \end{pmatrix}.$$

Ekkor kapjuk, hogy:

$$\begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \alpha^{n+1} - \beta^{n+1} \\ \alpha^n - \beta^n \end{pmatrix}.$$

A végén megkapjuk a zárt formulát:

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right].$$

2.3. Rekurzív rend

Az alábbiakban az $s_n = us_{n-1} + vs_{n-2}$ bináris rekurziót fogjuk vizsgálni, ahol $u, v \in \mathbb{Z}$ és $s_0 = 0, s_1 = 1$.

2.3.1. Definíció. Egy rekurzív sorozat periódusán azt a legkisebb $k > 1$ természetes számot értjük modulo m felett ($m \in \mathbb{N}$), amelyre $s_k \equiv 0 \pmod{m}$ és $s_{k+1} \equiv 1 \pmod{m}$. Jelölés: $k(m)$.

Legyen p prím. Ekkor a modulo p maradékosztályok rendszere véges testet alkot. Jele: $GF(p)$.

2.3.1. Tétel. Egy bináris rekurzió modulo p feletti periódusának felső korlátja $p^2 - 1$.

Bizonyítás. Két egymást követő tag egyértelműen meghatározza az őket követő harmadikat. Mivel két nulla nem állhat egymás mellett, ezért $p^2 - 1$ féle szomszédot állíthatunk össze. $\square$

A továbbiakban a rekurzió rendjét mátrixának sajátértékei szerint fogjuk vizsgálni a következő feltételek mellett: p prím, $u, v \in GF(p)$, $u \neq 0, v \neq 0$.

2.3.2. Tétel. Ha $\sqrt{u^2 - 4v} \in GF(p)$ és $\sqrt{u^2 - 4v} \neq 0$, akkor a rekurzió rendje osztja $(p - 1)$ -et.

Bizonyítás. A mátrix ekkor $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ alakra diagonalizálható, ahol λ_1 és λ_2 a mátrix sajátértékei. Legyen T a sajátvektorokból álló mátrix. A kis Fermat-tétel szerint λ_1^{p-1} és λ_2^{p-1} azonosan 1, így

$$\begin{pmatrix} u & v \\ 1 & 0 \end{pmatrix}^{(p-1)} = T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} T^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

$\square$

2.3.1. Példa. modulo 5 felett az $u = 1, v = 2$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: 2 és 4.

A mátrix periódusa: $p - 1 = 4$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 1 & 2 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7
s_n	0	1	1	3	5	11	21	43
$s_n \pmod{p}$	0	1	1	3	0	1	1	3

Ekkor a sorozat minden negyedik eleme osztható 5-tel. Ezen oszthatósági szabályt a periódusszám is megadja.

2.3.2. Példa. modulo 11 felett az $u = -1$, $v = 2$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 10 & 2 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: 1 és 9.

A mátrix periódusa: $\frac{p-1}{2} = 5$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 6 & 6 \end{pmatrix}, \begin{pmatrix} 10 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 9 \\ 10 & 2 \end{pmatrix}, \begin{pmatrix} 6 & 6 \\ 3 & 9 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9
s_n	0	1	-1	3	-5	11	-21	43	-85	171
$s_n \pmod{p}$	0	1	10	3	6	0	1	10	3	6

Ekkor a sorozat minden ötödik eleme osztható 11-gyel. Ezen oszthatósági szabályt a periódusszám is megadja.

2.3.1. Lemma. Egy 2×2 -es Jordan blokk k -edik hatványa $\begin{pmatrix} \lambda^k & k \cdot \lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix}$ alakú, ahol λ a mátrix sajátértéke.

Bizonyítás. A bizonyítást teljes indukcióval végezzük.

Az $n = 1$ esetben triviális az állítás.

Tegyük fel, hogy $n = k$ esetben teljesül az indukció. Ekkor $n = k + 1$ esetben $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \lambda^k & k \cdot \lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix} = \begin{pmatrix} \lambda^k \lambda & k \lambda^k + \lambda^k \\ 0 & \lambda^k \lambda \end{pmatrix} = \begin{pmatrix} \lambda^{k+1} & (k+1) \cdot \lambda^k \\ 0 & \lambda^{k+1} \end{pmatrix}$. $\square$

2.3.3. Tétel. Ha $v = \frac{-u^2}{4}$, akkor a mátrix periódusa osztja $p(p-1)$ -et.

Bizonyítás. Mivel $v = \frac{-u^2}{4}$, a diszkrimináns 0. A mátrix ekkor Jordan-féle normálalakra hozható: $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$, amely k -edik hatványa: $\begin{pmatrix} \lambda^k & k \cdot \lambda^{k-1} \\ 0 & \lambda^k \end{pmatrix}$.

Ekkor a mátrixot $(p-1)$ -edik hatványra emelve a főátlóban egyeseket kapunk. Továbbá p -edik hatványra emelve a főátlón kívüli elemeket kinullázzuk. Így

$$\begin{pmatrix} u & v \\ 1 & 0 \end{pmatrix}^{p(p-1)} = T \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} T^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

amiből következik, hogy $s_{p(p-1)-1} \equiv 0$, $s_{p(p-1)} \equiv 1 \pmod{p}$. $\square$

2.3.3. Példa. modulo 5 felett az $u = 1, v = 1$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: 3, kétszeres multiplicitással.

A mátrix periódusa: $(p-1)p = 20$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}, \\ \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \\ \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix}, \\ \begin{pmatrix} 4 & 4 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 3 & 0 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
u_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377
$u_n \pmod{p}$	0	1	1	2	3	0	3	3	1	4	0	4	4	3	2

n	15	16	17	18	19	20	21	22	23
u_n	610	987	1597	2584	4181	6765	10946	17711	28657
$u_n \pmod{p}$	0	2	2	4	1	0	1	1	2

Ekkor a sorozat minden ötödik eleme osztható 5-tel. A periódusszám valódi osztója ad oszthatósági szabályt.

2.3.4. Példa. modulo 5 felett az $u = -2, v = -1$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: 4, kétszeres multiplicitással.

A mátrix periódusa: $\frac{p-1}{2}p = 10$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 4 & 0 \end{pmatrix}, \\ \begin{pmatrix} 2 & 3 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 1 & 0 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
u_n	0	1	-2	3	-4	5	-6	7	-8	9	-10	11	-12	13
$u_n \pmod{p}$	0	1	3	3	1	0	4	2	2	4	0	1	3	3

n	14	15	16	17	18	19	20
u_n	-14	15	-16	17	-18	19	-20
$u_n \pmod{p}$	1	0	4	2	2	4	0

Ekkor a sorozat minden ötödik eleme osztható 5-tel. A periódusszám valódi osztója ad oszthatósági szabályt.

2.3.5. Példa. modulo 5 felett az $u = 2, v = -1$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: 1, kétszeres multiplicitással.

A mátrix periódusa: $p = 5$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 2 & 4 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9
u_n	0	1	2	3	4	5	6	7	8	9
$u_n \pmod{p}$	0	1	2	3	4	0	1	2	3	4

Ekkor a sorozat minden ötödik eleme osztható 5-tel. Ezen oszthatósági szabályt a periódusszám is megadja.

2.3.6. Példa. modulo 11 felett az $u = -2, v = -1$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: -1, kétszeres multiplicitással.

A mátrix periódusa: $2p = 22$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 10 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 10 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 9 & 8 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 10 & 0 \end{pmatrix}, \\ \begin{pmatrix} 2 & 3 \\ 8 & 7 \end{pmatrix}, \begin{pmatrix} 4 & 5 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 8 & 9 \end{pmatrix}, \begin{pmatrix} 8 & 9 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 8 & 7 \\ 4 & 5 \end{pmatrix}, \\ \begin{pmatrix} 5 & 4 \\ 7 & 8 \end{pmatrix}, \begin{pmatrix} 5 & 6 \\ 5 & 4 \end{pmatrix}, \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 10 & 9 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 9 & 8 \\ 3 & 4 \end{pmatrix}, \\ \begin{pmatrix} 9 & 10 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 7 & 8 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 7 & 6 \\ 5 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 9 & 10 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 7 & 6 \end{pmatrix},$$

$$\begin{pmatrix} 6 & 5 \\ 6 & 7 \end{pmatrix}, \begin{pmatrix} 6 & 7 \\ 4 & 3 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9	10	11
u_n	0	1	-2	3	-4	5	-6	7	-8	9	-10	11
$u_n \pmod{p}$	0	1	9	3	7	5	5	7	3	9	1	0

n	11	12	13	14	15	16	17	18	19	20
u_n	11	-12	13	-14	15	-16	17	-18	19	-20
$u_n \pmod{p}$	0	10	2	8	4	6	6	4	8	2

n	22	23	24	25	26
u_n	-22	23	-24	25	-26
$u_n \pmod{p}$	0	1	9	3	7

Ekkor a sorozat minden tizenegyedik eleme osztható 11-gyel. A periódusszám valódi osztója ad oszthatósági szabályt.

2.3.4. Tétel. *Ha a mátrix karakterisztikus polinomjának diszkriminánsa nem $GF(p)$ -beli elem, akkor a mátrix rendje osztja $(p^2 - 1)$ -et.*

Bizonyítás. Kibővítjük a véges testet a diszkriminánsal. Ekkor az így kapott test ekvivalens $GF(p^2)$ -tel. A mátrixot diagonalizáljuk és ekkor a kis Fermat-tétel szerint az elem rendje osztja $(p^2 - 1)$ -et. $\square$

2.3.7. Példa. modulo 5 felett az $u = 1, v = -2$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 1 & -2 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: $\lambda, 4\lambda + 1 \in \mathbb{Z}_5/(x^2 + x + 2)$.

A mátrix periódusa: $p^2 - 1 = 24$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 3 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 1 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}, \\ \begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 3 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\ \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 2 \\ 4 & 3 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \\ \begin{pmatrix} 4 & 1 \\ 2 & 2 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 4 \\ 3 & 1 \end{pmatrix}, \begin{pmatrix} 4 & 3 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \\ \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 3 \\ 1 & 2 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9	10	11
u_n	0	1	1	-1	-3	-1	5	7	-3	-17	-11	23
$u_n \pmod{p}$	0	1	1	4	2	4	0	2	2	3	4	3

n	12	13	14	15	16	17	18	19	20
u_n	45	-1	-91	-89	93	271	85	-457	-627
$u_n \pmod{p}$	0	4	4	1	3	1	0	3	3

n	21	22	23	24	25	26
u_n	287	1541	967	-2115	-4049	181
$u_n \pmod{p}$	2	1	2	0	1	1

Ekkor a sorozat minden hatodik eleme osztható 5-tel. A periódusszám valódi osztója ad oszthatósági szabályt.

2.3.8. Példa. modulo 5 felett az $u = 2, v = 1$ rekurzió.

A mátrixos alak ekkor: $\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$.

A sajátértékek: $\lambda + 3, 4\lambda + 4 \in \mathbb{Z}_5/(x^2 + x + 2)$.

A mátrix periódusa: $\frac{p^2-1}{2} = 12$.

A mátrix hatványai:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 4 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 3 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 3 \\ 3 & 0 \end{pmatrix}, \\ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 2 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 4 & 0 \end{pmatrix}.$$

n	0	1	2	3	4	5	6	7	8	9	10
u_n	0	1	2	5	12	29	70	169	408	985	2378
$u_n \pmod{p}$	0	1	2	0	2	4	0	4	3	0	3
n	11	12	13	14	15	16					
u_n	5741	13860	33461	80782	195025	470832					
$u_n \pmod{p}$	1	0	1	2	0	2					

Ekkor a sorozat minden harmadik eleme osztható 5-tel. A periódusszám valódi osztója ad oszthatósági szabályt.

2.4. A Fibonacci sorozat rekurzív rendje

A következőkben a Fibonacci sorozat oszthatóságát vizsgáljuk.

2.4.1. Tétel. $2|F_{3n}$, ahol $n \in \mathbb{N}$.

Bizonyítás. Az $n = 1$ esetben igaz: $F_3 = 2$.

Tegyük fel, hogy n -re igaz: $2|F_n$.

Ekkor $n + 1$ esetén: $F_{n+3} = F_{n+2} + F_{n+1} = F_{n+1} + F_n + F_{n+1} = 2F_{n+1} + F_n$. $\square$

2.4.2. Tétel. $3|F_{4n}$, ahol $n \in \mathbb{N}$.

Bizonyítás. Az $n = 1$ esetben igaz: $F_4 = 3$.

Tegyük fel, hogy n -re igaz: $3|F_n$.

Ekkor $n + 1$ esetén: $F_{n+4} = F_{n+3} + F_{n+2} = (F_{n+2} + F_{n+1}) + (F_{n+1} + F_n) = F_{n+1} + F_n + F_{n+1} + F_{n+1} + F_n = 3F_{n+1} + 2F_n$. $\square$

2.4.3. Tétel. $5|F_{5n}$, ahol $n \in \mathbb{N}$.

Bizonyítás. Az $n = 1$ esetben igaz: $F_5 = 5$.

Tegyük fel, hogy n -re igaz: $5|F_n$.

Ekkor $n + 1$ esetén: $F_{n+5} = F_{n+4} + F_{n+3} = (F_{n+3} + F_{n+2}) + (F_{n+2} + F_{n+1}) = (F_{n+2} + F_{n+1}) + (F_{n+1} + F_n) + (F_{n+1} + F_n) + (F_{n+1}) = 5F_{n+1} + 3F_n$. $\square$

A következőkben a Fibonacci sorozat periódusát fogjuk vizsgálni az [1] cikk alapján.

A Fibonacci periódusának felső korlátja $m^2 - 1$ modulo m felett, mert minden két egymást követő tag meghatározza az utánuk következőket, így $m^2 - 1$ féle szomszédot tudunk összeállítani, mivel két nulla nem állhat egymás mellett.

Ezentúl jelölje $U^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$ a Fibonacci mátrix n -edik hatványát és α, β a Fibonacci mátrix sajátértékeit.

Legyen $D = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ és C az ehhez tartozó sajátvektorokból álló mátrix.

Ha a sajátértékek megegyeznek, akkor D egy Jordan blokk.

2.4.1. Lemma. A periódus osztója bármely n -nek, amelyre teljesül a $D^n = E$ egyenlőség.

2.4.4. Tétel. Ha p egy páratlan prím és $p \equiv 1$ vagy $p \equiv 4 \pmod{5}$, akkor $k(p) \mid p - 1$.

Bizonyítás. A sajátvektorok ekkor különbözőek. A Fermat-tétel alapján $\alpha^{p-1} \equiv \beta^{p-1} \equiv 1 \pmod{p}$, ezért $D^n = E$. $\square$

Ha $p \equiv 2$ vagy $p \equiv 3 \pmod{5}$, akkor az U mátrix karakterisztikus polinomjának nincsenek gyökei $GF(p)$ -ben, ezért kénytelen vagyunk testet bővíteni. Legyen $F = GF_p(x)/(x^2 - x - 1)$. Ekkor F izomorf $GF(p^2)$ -tel.

2.4.2. Lemma. *Ha $p \equiv 2$ vagy $p \equiv 3 \pmod{5}$, akkor $(\sqrt{5})^p = -\sqrt{5}$.*

2.4.3. Lemma. $\alpha^{p+1} \equiv \beta^{p+1} \pmod{F}$ felett.

2.4.5. Tétel. *Ha p egy páratlan prím és $p \equiv 2$ vagy $p \equiv 3 \pmod{5}$, akkor $k(p) \mid 2(p+1)$.*

Bizonyítás. Tudjuk, hogy $\alpha\beta = -1 \pmod{p^2}$, így $\alpha^{p+1}\alpha^{p+1} = \alpha^{p+1}\beta^{p+1} = (-1)^{p+1}$. Mivel p páratlan, ezért $(-1)^{p+1} = 1$, így $\alpha^{2(p+1)} = 1$. Az előző lemma alapján tudjuk, hogy $\beta^{2(p+1)} = 1$. $\square$

3. ÁLTALÁNOS LINEÁRIS CSOPORT

Ebben a fejezetben az általános lineáris csoport rendje által fogunk eljutni a bináris rekurzív sorozatok rendjéig.

3.0.1. Definíció. Általános lineáris csoportnak nevezzük a V vektortér invertálható lineáris transzformációinak csoportját. Jele: $GL(V)$

3.0.2. Definíció. A másodrangú lineáris csoport egy véges test felett a mátrix-szorzással definiált 2×2 -es invertálható mátrixok csoportja. Jele: $GL(2, F)$.

3.0.6. Tétel. Legyen p prím. Egy $GL(2, p)$ -beli mátrix rendje legfeljebb $(p^2 - p)(p^2 - 1)$.

Bizonyítás. A mátrix első sorába $p^2 - 1$ féle elempárt választhatunk, mivel a csupa nulla sor szingularitáshoz vezetne. Ekkor a második sorba az első nem skalárszorosa szerepelhet, amiből $p^2 - p$ darab létezik. $\square$

3.0.7. Tétel. Legyen $s_n = us_{n-1} \pm s_{n-2}$ rekurzió. Ekkor bármely p prím osztja $s_{2p(p^2-1)}$ -et.

Bizonyítás. Legyen

$$G := \{A \in M_2(\mathbb{Z}_p) \mid \det(A) = \pm 1\}$$

és

$$M = \begin{pmatrix} u & \pm 1 \\ 1 & 0 \end{pmatrix}.$$

Ekkor $M \in G$ és G rendje $2p(p^2 - 1)$.

$$\begin{aligned} \text{Így} \quad \begin{pmatrix} s_{n+1+2p(p^2-1)} & s_{n+2p(p^2-1)} \\ s_{n+2p(p^2-1)} & s_{n-1+2p(p^2-1)} \end{pmatrix} &= M^{n+2p(p^2-1)} = M^n = \\ \begin{pmatrix} s_{n+1} & s_n \\ s_n & s_{n-1} \end{pmatrix} & \pmod{p}. \end{aligned} \quad \square$$

1. Következmény. Bármely p prím osztja $F_{2p(p^2-1)}$ -et, ahol F_n a Fibonacci sorozat n -edik tagja.

Bizonyítás. Az előző tétel bizonyítása alapján:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \{A \in M_2(\mathbb{Z}_p) \mid \det(A) = \pm 1\}.$$

□

3.0.3. Definíció. Az $u = 2, v = 1$ bináris rekurziót Pell sorozatnak hívjuk.

2. Következmény. Bármely p prím osztja $P_{2p(p^2-1)}$ -et, ahol P_n a Pell sorozat n -edik tagja.

3. Következmény. Bármely p prím osztja $s_{2p(p^2-1)}$ -et, ahol s_n az $u = 4, v = -1$ rekurzió n -edik tagja.

3.0.1. Példa. A fentebb leírt sorozat néhány tagja:

n	0	1	2	3	4	5	6	7	8	9	10	11
s_n	0	1	4	15	56	209	780	2911	10864	40545	151316	564719

4. SAGE KÓDOK

Ebben a fejezetben három Sage [5] programon keresztül szerkesztünk példákat a $p-1$, p^2-p és a p^2-1 osztóival megegyező periódusszámokra.

4.0.2. Példa.

```
def rek(u,v,n):
    if n==0:
        return 0
    elif n==1:
        return 1
    else:
        return u*rek(u,v,n-1)+v*rek(u,v,n-2)

@interact
def _(p=('p',7)):
    Mp=MatrixSpace(GF(p),2,2)
    L=(p-1).divisors()
    L.remove(1)
    for d in L:
        Md=[k for k in Mp if k[1,0]==1 and k[0,1]!=0 and k[1,1]==0
and (k[0,0]^2+4*k[0,1]).is_square() and (k[0,0],k[0,1])!=(0,0)
and k.multiplicative_order()==d]
        pretty_print(html('Egy mátrix, amelynek a rendje
$$s$:%\text{latex}(d)$$'))
        M1=Md.pop()
        pretty_print(M1)
        pretty_print(html('Kapcsolódó rekurzív sorozat:
$a_0=0,a_1=1,a_n=s_{n-1}+s_{n-2}.$'
%\text{latex}(M1[0,0]),\text{latex}(M1[0,1]))))
        Muj=[(k,rek(M1[0,0],M1[0,1],k)) for k in [0..2*d]]
        pretty_print(Muj)
```

4.0.3. Példa.

```
def rek(u,v,n):
    if n==0:
        return 0
    elif n==1:
        return 1
```

```

        else:
            return u*rek(u,v,n-1)+v*rek(u,v,n-2)
@interact
def _(p=('p',5)):
    Mp=MatrixSpace(GF(p),2,2)
    L=((p-1)*p).divisors()
    L.remove(1)

    for d in L:
        Md=[k for k in Mp if k[1,0]==1 and k[0,1]!=0
and k[1,1]==0 and (k[0,0]^2+4*k[0,1])==0
and (k[0,0],k[0,1])!=(0,0) and k.multiplicative_order()==d]
        if Md!=[]:
            pretty_print(html('Egy mátrix, amelynek a rendje  $s$ :
'%latex(d)))
            M1=Md.pop()
            pretty_print(M1)
            pretty_print(html('Kapcsolódó rekurzív sorozat:  $a_0=0,$ 
a_1=1,a_n=
 $s_{n-1}+s_{n-2}$ . $s$ '%(latex(M1[0,0]),latex(M1[0,1]))))
            Muj=[(k, rek(M1[0,0],M1[0,1],k)) for k in [0..2*d]]
            pretty_print(Muj)

```

4.0.4. Példa. `def rek(u,v,n):`

```

    if n==0:
        return 0
    elif n==1:
        return 1
    else:
        return u*rek(u,v,n-1)+v*rek(u,v,n-2)
@interact
def _(p=('p',5)):
    Mp=MatrixSpace(GF(p),2,2)
    L=(p^2-1).divisors()
    L.remove(1)

    for d in L:
        Md=[k for k in Mp if k[1,0]==1 and k[0,1]!=0
and k[1,1]==0 and (k[0,0]^2+4*k[0,1])!=0
and (k[0,0]^2+4*k[0,1]).is_square==false
and (k[0,0],k[0,1])!=(0,0) and k.multiplicative_order()==d]
        if Md!=[]:

```

```

        pretty_print(html('Egy mátrix, amelynek a rendje  $\$s\$$ :
'%latex(d))
        M1=Md.pop()
        pretty_print(M1)
        pretty_print(html('Kapcsolódó rekurzív sorozat:  $a_0=0,$ 
a_1=1, a_n=
        %sa_{n-1}+%sa_{n-2}.$'%(latex(M1[0,0]), latex(M1[0,1]))))
        Muj=[(k, rek(M1[0,0], M1[0,1], k)) for k in [0..2*d]]
        pretty_print(Muj)

```

Az előző kódok egyikének futási képe a következő.

p 7

Egy mátrix, amelynek a rendje 2:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Kapcsolódó rekurzív sorozat: $a_0 = 0, a_1 = 1, a_n = 0a_{n-1} + 1a_{n-2}$.

n	0	1	2	3	4
$a_n \pmod{p}$	0	1	0	1	0

Egy mátrix, amelynek a rendje 3:

$$\begin{pmatrix} 6 & 6 \\ 1 & 0 \end{pmatrix}$$

Kapcsolódó rekurzív sorozat: $a_0 = 0, a_1 = 1, a_n = 6a_{n-1} + 6a_{n-2}$.

n	0	1	2	3	4	5	6
$a_n \pmod{p}$	0	1	6	0	1	6	0

Egy mátrix, amelynek a rendje 6:

$$\begin{pmatrix} 4 & 5 \\ 1 & 0 \end{pmatrix}$$

Kapcsolódó rekurzív sorozat: $a_0 = 0, a_1 = 1, a_n = 4a_{n-1} + 5a_{n-2}$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$a_n \pmod{p}$	0	1	4	0	6	3	0	1	4	0	6	3	0

IRODALOMJEGYZÉK

- [1] Sanjai Gupta, Parousia Rockstroh, and Francis Edward Su. Splitting fields and periods of Fibonacci sequences modulo primes. *Math. Mag.*, Volume 85, Number 2, April 2012, 130-135.
- [2] <http://www.math.ucla.edu/~mwilliams/pdf/fibonacci.pdf>
- [3] Charles W. Campbell II. The Period of the Fibonacci Sequence Modulo j . *Math 399* Spring 2007
- [4] http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-spring-2005/lecture-notes/112_recur2.pdf
- [5] W. A. Stein et al., *Sage Mathematics Software (Version 7.1)*, The Sage Development Team, 2016, <http://www.sagemath.org>