Dénes Tamás matematikus-kriptográfus
www.titoktan.hu e-mail: **tdenest@freemail.hu**

Prímszámok a Fibonacci sorozatban

A továbbiakban Fibonacci sorozaton az alapsorozatot (*u_n=1,1,2,3,5,...*), Fibonacci számon az alapsorozat valamely elemét értjük. N.N.Vorobjev [1]-ben bizonyította az u_n-re vonatkozó alábbi tételt:

(1) $$u_{n+k} = u_{n-1}u_k + u_n u_{k+1} \qquad \textit{(n, k természetes számok)}$$

Az (1) összefüggésből következnek az alábbi (2), (3), (4) összefüggések:

(2) $$\forall n \rangle 2 \Rightarrow u_{2n} = u_{n-1}u_n + u_n u_{n+1} = u_n(u_{n-1} + u_{n+1}) \quad \Rightarrow$$
$$\Rightarrow \quad u_n(u_{n-1} + u_{n+1}) = u_n(u_{n-1} + u_{n-1} + u_n) = u_n^2 + 2u_n u_{n-1} = (u_n + u_{n-1})^2 - u_{n-1}^2 \quad \Rightarrow$$
$$\Rightarrow \quad u_{2n} = u_{n+1}^2 - u_{n-1}^2 = (u_{n+1} + u_{n-1})(u_{n+1} - u_{n-1})$$

Példa: *n=4*, $u_3 = 2,\ u_5 = 5,\ u_8 = 21 \rightarrow 5^2 - 2^2 = (5+2)(5-2) = 21$

A (2) levezetés szerint tehát, ***a Fibonacci sorozat minden (kettőnél nagyobb) páros indexű eleme összetett szám.***

(3) $$u_{2n+1} = u_{n+(n+1)} \xrightarrow{(1)} u_{2n+1} = u_{n-1}u_{n+1} + u_n u_{n+2} = u_{n-1}u_{n+1} + u_n(u_n + u_{n+1}) =$$
$$= u_{n-1}u_{n+1} + u_n^2 + u_n u_{n+1} = u_{n+1}(u_{n-1} + u_n) + u_n^2 \quad \Rightarrow \quad u_{2n+1} = u_{n+1}^2 + u_n^2$$

Példa: *n=4*, $u_4 = 3,\quad u_5 = 5,\quad u_9 = 34 \quad \rightarrow \quad 5^2 + 3^2 = 34$

(4) $$u_{2n-1} = u_{n+(n-1)} \xrightarrow{(1)} u_{n-1}u_{n-1} + u_n u_n = u_{n-1}^2 + u_n^2 \quad \Rightarrow u_{2n-1} = u_{n-1}^2 + u_n^2$$

Példa: *n=4*, $u_3 = 2,\quad u_4 = 3,\quad u_7 = 13 \quad \rightarrow \quad 2^2 + 3^2 = 13$

1. Tétel

Ha u_n a Fibonacci sorozat n-ik eleme, akkor u_{kn} osztható u_n-nel ($k= 1,2,3,...$).

Bizonyítás (teljes indukció):

A tétel $k=1$ esetén triviális, $k=2$ esetén érvényes a (2) összefüggés, azaz a tétel igaz.

Tegyük fel, hogy k-ig minden természetes számra igaz a tétel, azaz

(5) $$u_{kn} = c \cdot u_n \qquad (k>2,\ c \text{ természetes szám})$$

Vizsgáljuk a $k+1$ esetet:

(6) $$\begin{aligned} u_{(k+1)n} &= u_{kn+n} = u_{kn-1} \cdot u_n + u_{kn} \cdot u_{n+1} = \\ &= u_{kn-1} \cdot u_n + c \cdot u_n \cdot u_{n+1} = u_n (u_{kn-1} + c \cdot u_{n+1}) \end{aligned}$$

Q.E.D.

Következmény

A Fibonacci sorozat minden u_{6k} eleme osztható $u_6=8$-al.

Példa: $u_{11} = 89 \quad u_{22} = 89 \cdot 199 \quad u_{33} = 2 \cdot 89 \cdot 19801$

$u_{22} = 89 \cdot 199 \quad u_{44} = 3 \cdot 43 \cdot 89 \cdot 199 \cdot 307 \quad u_{66} = 2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$

$u_{33} = 2 \cdot 89 \cdot 19801 \quad u_{66} = 2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$

Az 1. tétel általánosításaként adódik ***a Fibonacci sorozat összetett elemeire*** *vonatkozó szükséges és elegendő egzisztencia tétel:*

2. Tétel

Legyen az n index prímfelbontása $n=p_1 p_2 \ldots p_k$. **u_q akkor és csak akkor osztója u_n-nek, ha $q \in \{p_1, p_2, ..., p_n\}$.**

A bizonyítás szükségessége és elegendősége egyaránt az 1. tételből következik.

Következmény:

A 2. tétel jelöléseit használva kapjuk, hogy u_n osztható $lkkt(u_{p_1}, u_{p_2}, ..., u_{p_k})$-vel[1] .

----- . -----

[1] *lkkt* = a legkisebb közös többszörös jelölése. Ezzel analóg tétel található [2]-ben a legnagyobb közös osztóra.

Példa: n=42 = $2\cdot 3\cdot 7$ ekkor $n_1=2 \quad n_2=3 \quad n_3=7 \quad n_4=6 \quad n_5=14 \quad n_6=21$

$u_2=1 \quad u_3=2 \quad u_7=13 \quad u_6=2^3 \quad u_{14}=13\cdot 29 \quad u_{21}=2\cdot 13\cdot 421$

$lkkt\,(1,2,13,2^3,13\cdot 29,2\cdot 13\cdot 421)=2^3\cdot 13\cdot 29\cdot 421 \;=\; \dfrac{u_{42}}{211}$

Lásd az 1. táblázatot!

3. Tétel

Ha u_n prímszám, akkor n is prímszám.

Bizonyítás:

Ha u_n prímszám, akkor csak két osztója van $u_1=1$ és u_n, ekkor a 2. tétel miatt n összes osztója *1* és *n*, azaz n prímszám.

Q.E.D.

A 3. tétel megfordítása csak az alábbi megszorítással érvényes (lásd 4. tétel).

4. Tétel

Ha n prímszám, akkor u_n vagy prímszám, vagy nincs olyan 2-nél nagyobb prímtényezője, amelyik Fibonacci szám.

Bizonyítás:

Tegyük fel, hogy n prímszám és $u_n=k\cdot u_i$ $(i\langle n)$, ekkor a 2. tétel értelmében n *i*-nek többszöröse, ami ellentmondás. Tehát u_n prímtényezői között nincs Fibonacci szám, kivéve, ha prímszám és az egyetlen prímtényezője önmaga.

Q.E.D.

5. Tétel

Ha $n=6k\pm 1$ (*k=1,2,3,...*) alakú, akkor u_n is az, azaz

(7) $$n=6k\pm 1 \quad\Rightarrow\quad u_n\equiv \pm 1 \bmod 6$$

Bizonyítás (teljes indukció):

k=1 esetén $u_5=5,\quad u_7=13$ tehát a tétel állítása teljesül.

Tegyük fel, hogy *k*-ra teljesül a tétel. Vizsgáljuk *k+1*-re a *6(k+1)+1* esetet:

(8) $$u_{6(k+1)+1}=u_{6k+1+6}\xrightarrow{(1)} u_{6k}u_6+u_{6k+1}u_7=(u_{6k+1}-u_{6k-1})u_6+u_{6k+1}u_7=$$
$$=u_{6k+1}(u_6+u_7)-u_{6k-1}u_6=u_{6k+1}u_8-u_{6k-1}u_6=21\cdot u_{6k+1}-8\cdot u_{6k-1}$$

Az indukciós feltétel szerint $u_{6k\pm1} \equiv \pm1 \mod 6$, tehát a (8) levezetés eredményeként kapott kifejezés *mod 6* maradékait az alábbi táblázat foglalja össze:

$21\cdot$	$u_{6k+1}-$	$8\cdot$	u_{6k-1}	$\mod 6$
3	+1	2	−1	+1

Most vizsgáljuk meg a 6(*k+1)-1* esetet:

(9) $$u_{6(k+1)-1} = u_{6k+1+4} \xrightarrow{(1)} u_{6k}u_4 + u_{6k+1}u_5 = (u_{6k+1} - u_{6k-1})u_4 + u_{6k+1}u_5 =$$
$$= u_{6k+1}(u_4 + u_5) - u_{6k-1}u_4 = u_{6k+1}u_6 - u_{6k-1}u_4 = 8\cdot u_{6k+1} - 3\cdot u_{6k-1}$$

Az indukciós feltétel szerint $u_{6k\pm1} \equiv \pm1 \mod 6$, tehát a (9) levezetés eredményeként kapott kifejezés *mod 6* maradékát az alábbi táblázat foglalja össze:

$8\cdot$	$u_{6k+1}-$	$3\cdot$	u_{6k-1}	$\mod 6$
2	+1	3	−1	−1

Q.E.D.

Ha az 5. tételt összevetjük a prímszámokra vonatkozó [3]–ban bizonyított 1. tétellel, mely szerint minden prímszám *6k-1*, vagy *6k+1* alakú, akkor az alábbi 6. tételhez jutunk:

6. Tétel

Ha n prímszám, akkor u_n $6k\pm1$ alakú.

----- . -----

Ha a 6.tételt a [3]–ban bizonyított 2. tétellel (Komplementer Prímszita tétel) vetjük össze, akkor a következő 7.tételhez jutunk:

7. Tétel

Ha n prímszám és u_n nem prím, valamint r az u_n prímtényezőinek száma, akkor

(10) $$u_n = \prod_{i=1}^{r}(6k_i \pm 1)$$

----- . -----

Figyelembe véve a fenti 4. tételt adódik, hogy a (10)-ben szereplő $6k_i \pm 1$ prímtényezők egyike sem Fibonacci szám.

Példák: n=19, u_{19}= 4181=(6· 6+1)(19· 6-1)= 37· 113
n=31, u_{31}= 1346269=(93· 6-1)(403· 6-1)= 557· 2417

További példák e dolgozat végén közölt 1. táblázatban találhatók.

NYITOTT PROBLÉMA: Van-e a Fibonacci sorozatnak végtelen sok prímszám eleme?

References

[1] Vorobjev, N.N.: Fibonacci Numbers
Pergamon Press, New York, 1961.

[2] Verner E. Hoggatt: Fibonacci and Lucas Numbers
Houghton Mifflin Company, Boston, 1969.

[3] Dénes Tamás: http://www.titoktan.hu/_raktar/_e_vilagi_gondolatok/KomplementerPrimszita.pdf

1. Táblázat *A Fibonacci sorozat 1-73. elemei és ezek prímfelbontása*

i	u_i	u_i **prímfelbontása**	***i***	u_i	u_i **prímfelbontása**
1	*1*		38	*39.088.169*	37x113x9349
2	*1*		39	*63.245.986*	2x233x135721
prím 3	*2*	prím	40	*102.334.155*	3x5x7x11x41x2161
4	*3*	prím	prím 41	*165.580.141*	2789x59369
prím 5	*5*	prím (6k-1)	42	*267.914.296*	$2^3 \cdot 13 \cdot 29 \cdot 211 \cdot 421$
6	*8*	2^3	prím 43	*433.494.437*	prím (6k-1)
prím 7	*13*	prím (6k+1)	44	*701.408.733*	3x43x89x199x307
8	*21*	3x7	45	*1.134.903.170*	2x5x17x61x109441
9	*34*	2x17	46	*1.836.311.903*	139x461x28657
10	*55*	5x11	prím 47	*2.971.215.073*	prím (6k+1)
prím 11	*89*	prím (6k-1)	48	*4.807.526.976*	$2^6 \cdot 3^2 \cdot 7 \cdot 23 \cdot 47 \cdot 1103$
12	*144*	$2^4 \cdot 3^2 = 12^2$	49	*7.778.742.049*	13x97x6168709
prím 13	*233*	prím (6k-1)	50	*12.586.269.025*	$5^2 \cdot 11 \cdot 101 \cdot 151 \cdot 3001$
14	*377*	13x29	51	*20.365.011.074*	2x1597x6376021
15	*610*	2x5x61	52	*32.951.280.099*	3x233x521x90481
16	*987*	3x7x47	prím 53	*53.316.291.173*	953x55945741
prím 17	*1.597*	prím (6k+1)	54	*86.267.571.272*	$2^3 \cdot 17 \cdot 19 \cdot 53 \cdot 109 \cdot 5779$
18	*2.584*	$2^3 \cdot 17 \cdot 19$	55	*139.583.862.445*	5x89x661x474541
prím 19	*4.181*	37x113	56	*225.851.433.717*	$3 \cdot 7^2 \cdot 13 \cdot 29 \cdot 281 \cdot 14503$
20	*6.765*	3x5x11x41	57	*365.435.296.162*	2x37x113x797x54833
21	*10.946*	2x13x421	58	*591.286.729.879*	59x19489x514229
22	*17.711*	89x199	prím 59	*956.722.026.041*	353x2710260697
prím 23	*28.657*	prím (6k+1)	60	*1.548.008.755.920*	$2^4 \cdot 3^2 \cdot 5 \cdot 11 \cdot 31 \cdot 41 \cdot 61 \cdot 2521$
24	*46.368*	$2^5 \cdot 3^2 \cdot 7 \cdot 23$	prím 61	*2.504.730.781.961*	4513x555003497
25	*75.025*	$5^2 \cdot 3001$	62	*4.052.739.537.881*	557x2417x3010349
26	*121.393*	233x521	63	*6.557.470.319.842*	2x13x17x421x35239681
27	*196.418*	2x17x53x109	64	*10.610.209.857.723*	3x7x47x1087x2207x4481
28	*317.811*	3x13x29x281	65	*17.167.680.177.565*	5x233x14736206161
prím 29	*514.229*	prím (6k-1)	66	*27.777.890.035.288*	$2^3 \cdot 89 \cdot 199 \cdot 9901 \cdot 19801$
30	*832.040*	$2^3 \cdot 5 \cdot 11 \cdot 31 \cdot 61$	prím 67	*44.945.570.212.853*	269x116849x1429913
prím 31	*1.346.269*	557x2417	68	*72.723.460.248.141*	3x67x1597x3571x63443
32	*2.178.309*	3x7x47x2207	69	*117.669.030.460.994*	2x137x829x18077x28657
33	*3.524.578*	2x89x19801	70	*190.392.490.709.135*	5x11x13x29x71x911x141961
34	*5.702.887*	1597x3571	prím 71	*308.061.521.170.129*	6673x46165371073
35	*9.227.465*	5x13x141961	72	*498.454.011.879.264*	$2^5 \cdot 3^3 \cdot 7 \cdot 17 \cdot 19 \cdot 23 \cdot 107 \cdot 103681$
36	*14.930.352*	$2^4 \cdot 3^3 \cdot 17 \cdot 19 \cdot 107$	prím 73	*806.515.533.049.393*	9375829x86020717
prím 37	*24.157.817*	73x149x2221			