Benkő Miklós:

Prímszámvadászat homogén lánctörtekkel

A cikk két kétváltozós függvényt ismertet. Az egyik alkalmas prímszámok keresésére, a másik sohasem eredményez prímszámot. Bevezetésre kerül a „homogén reguláris lánctört" fogalma, számítógépes programozók számára gyakorlati útmutatóval.

Bevezetés

Lánctörtön a következő matematikai alakzatot értjük $(a, b \in N)$:

$$a_0 + \frac{b_1}{a_1 + \frac{b_2}{a_2 + \ldots}}.$$

A reguláris lánctört számlálóiban csupa 1-es szerepel $(b_1, b_2, \ldots, b_n = 1)$:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}.$$

A reguláris lánctörtet a következő formában szokás ábrázolni: $[a_0; a_1, a_2, \ldots]$. A lánctört a racionális számok esetében véges, az irracionális és transzcendens számok esetében végtelen.

1.) A Fibonacci számokat előállító generátorfüggvény általánosítása

Vegyük a következő másodfokú egyenletet: $x^2 - x - 1 = 0$. Rendezzük át: $x^2 = x + 1$, majd osszuk el mindkét oldalt x-szel:

$$x = 1 + \frac{1}{x}.$$

Ha a jobb oldali x helyébe behelyettesítjük az egész jobb oldalt, egy emeletes törtet kapunk:

$$x = 1 + \frac{1}{1 + \frac{1}{x}}.$$

A behelyettesítés a végtelenségig folytatható:

$$1 + \frac{1}{1 + \frac{1}{1 + \ldots}}.$$

Az így kapott lánctört $[1; 1, 1, 1, 1, 1, 1, 1, 1, \ldots]$ határértéke a fenti $x^2 - x - 1 = 0$ egyenlet egyik gyökével egyezik meg:

$$\frac{1+\sqrt{5}}{2}.$$

A másik gyök ennek reciproka (előjelcserével):

$$\frac{1-\sqrt{5}}{2}.$$

Ezzel a két gyökkel levezethető egy generátorfüggvény, mely n kitevő különböző értékei esetén a Fibonacci-számokat állítja elő:

$$f_1(1,n) = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}},$$

1 1 2 3 5 8 13 21 34 55 89 144 233 377 610 987 1597 2584 4181 6765 10946 17711 28657 46368 75025 121393 196418 317811 514229.

Ha módosítunk a másodfokú egyenleten: $x^2 - C \cdot x - 1 = 0$, akkor a két gyök

$$\frac{C+\sqrt{C^2+4}}{2}$$

és

$$\frac{C-\sqrt{C^2+4}}{2},$$

az ezekből alkotott generátorfüggvény:

$$f_1(C,n) = \frac{\left(\frac{C+\sqrt{C^2+4}}{2}\right)^n - \left(\frac{C-\sqrt{C^2+4}}{2}\right)^n}{\sqrt{C^2+4}}.$$

Ez a formula tartalmazza mind a négy alapműveletet (a négyzetre emelés önmagával való szorzás), valamint egy négyzetgyökös kifejezést is. Ha C és (a kitevőben szereplő n) 0-nál nagyobb természetes számok, mindig egész számokat kapunk, mert a számlálóban azok a tagok, melyek nem tartalmazzák a négyzetgyökös kifejezést, a két hatványkifejezésben azonos előjellel lépnek fel, ezért a kivonás miatt kiesnek. A maradék tagok mind tartalmazzák a négyzetgyökös kifejezést, ezért $\sqrt{C^2+4}$-gyel végig lehet osztani.

A generátorfüggvényhez tartozó lánctört $[C; C, C, C, C, C, C, C, \ldots]$ alakú:

$$C + \cfrac{1}{C + \frac{1}{C + \ldots}}$$

és „homogén reguláris lánctört” a neve (vagy egyszerűen „homogén lánctört”).

2.) Az $f_1(C, n)$ függvénynek két változója van, C és n.

Nézzük meg, hogyan viselkedik rögzített n kitevő esetén.

I. Ha $n = 1$, $f_1(C, n) = 1$, azaz konstans.

II. Ha $n = 2$, $f_1(C, n) = C$, azaz visszakapjuk C értékét.

III. Ha $n = 3$, $f_1(C, 3) = C^2 + 1$.

Ha vizsgáljuk a $C^2 + 1$ formulát, és különböző értékeket adunk C-nek, azt tapasztaljuk, hogy vegyesen kapunk összetett számokat és prímszámokat. Ha csak azokat az értékeket tüntetjük fel, melyek prímszámok, a következő táblázatot kapjuk:

1.	$C =$	2	5	Fermat-féle prímszám
2.	$C =$	4	17	Fermat-féle prímszám
3.	$C =$	6	37	
4.	$C =$	10	101	
5.	$C =$	14	197	
6.	$C =$	16	257	Fermat-féle prímszám
7.	$C =$	20	401	
8.	$C =$	24	577	
9.	$C =$	26	677	
…	…	…	…	
42.	$C =$	256	65537	Fermat-féle prímszám

Tehát ha C 2-től 256-ig változik, az előállított számok között 42 prímszám található, közöttük 4 Fermat-féle prím.

IV. Ha $n = 4$, $f_1(C, 4) = C^3 + 2 \cdot C$. Látható, hogy a polinomból C kiemelhető, ezért a függvény mindig összetett számot állít elő.

V. Ha $n = 5$, $f_1(C, 5) = C^4 + 3 \cdot C^2 + 1$, és C értéke 1-től $10\,000$-ig változik, 1148 prímszámot állít elő, melyből az első 30 a következő ($C \leq 100$):

5 29 109 701 2549 4289 10301 21169 84389 161201 281429 812701 1051649 1189189 4106701 5315329 7898909 11326589 14787869 20164589 21395249 24024701 31657501 35170829 37033309 40979201 57312469 65634301 88557509 100030001

VI. Ha $n = 6$, $f_1(C, 6) = C^5 + 4 \cdot C^3 + 3 \cdot C$, amiből C kiemelhető, tehát mindig összetett számot kapunk.

VII. Ha $n = 7$, $f_1(C, 7) = C^6 + 5 \cdot C^4 + 6 \cdot C^2 + 1$.

Ez a formula, ha C értéke 1-től 1000-ig változik, 80 prímszámot állít elő, ebből az első 23:

13 53353 283009 34539049 64802401 1297404109 10803626989 139448469889 282644809453 404840783593 783182518273 886303622569 1871173661293 3298411715689 3815918062501 6613617740029 12830433853789 29726659302913 36349118326249 45586013273893 65952322047613 88255850497093 98781981671101

Láthatjuk, hogy ha n páros szám, akkor az $f_1(C, n)$ generátorfüggvényből származó polinom osztható C-vel, tehát (ha ezt tartjuk szem előtt) csak akkor kaphatunk prímszámot, ha n páratlan. További számítógépes vizsgálatokból fogalmazódott meg az a SEJTÉS, hogy az $f_1(C, n)$ függvény csak akkor állít elő prímszámot, ha n értéke maga is prím. Ezért érdemes átugorni $n = 8, 9, 10$ értékét (a teljesség kedvéért a polinomokat közöljük):

VIII. Ha $n = 8$, $f_1(C, 8) = C^7 + 6 \cdot C^5 + 10 \cdot C^3 + 4 \cdot C$.

IX. Ha $n = 9$, $f_1(C, 9) = C^8 + 7 \cdot C^6 + 15 \cdot C^4 + 10 \cdot C^2 + 1$.

X. Ha $n = 10$, $f_1(C, 10) = C^9 + 8 \cdot C^7 + 21 \cdot C^5 + 20 \cdot C^3 + 5 \cdot C$.

Ha $n = 11$, $f_1(C, 11) = C^{10} + 9 \cdot C^8 + 28 \cdot C^6 + 35 \cdot C^4 + 15 \cdot C^2 + 1$.

Ez a polinom a számok géppel ábrázolható tartományában (18 jegyig) 19 prímszámot eredményezett a gép segítségével, a következő „C"-k esetén:

$C = 1, 2, 3, 5, 6, 8, 17, 19, 20, 23, 33, 39, 41, 43, 46, 48, 50, 51, 56.$

A fenti polinomok együtthatói nem mások, mint a *binomiális együtthatók*, melyeket a *Pascal-háromszögből* lehet kiolvasni, de nem „vízszintesen", mint a binomiális tétel alkalmazása esetén az $\binom{n}{k}$ képletet használva, hanem „ferdén", az

$$\binom{n-1-k}{k}$$

formulával. Ellenőrzésképpen, ha soronként összeadjuk az együtthatókat, eredményül Fibonacci-számokat kell kapnunk.

3.) Választhatjuk azt az utat is, hogy C-t rögzítjük és n-et változtatjuk. Az $f_1(C,n)$ fügvénnyel $C=20$ és $n=3,5,7,11$ esetén prímszámot kapunk, $n=13$-ra nem.

n	$f_1(20,n)$	
1.	1	–
2.	20	$2\times2\times5$
3.	401	–
4.	8040	$2\times2\times2\times3\times5\times67$
5.	161201	–
6.	3232060	$2\times2\times5\times13\times31\times401$
7.	64802401	–
8.	1299280080	$2\times2\times2\times2\times3\times5\times7\times7\times17\times67\times97$
9.	26050404001	$37\times401\times1755773$
10.	522307360100	$2\times2\times5\times5\times32401\times161201$
11.	10472197606001	–
12.	209966259480120	$2\times2\times2\times3\times3\times5\times11\times13\times31\times59\times67\times$ $\times83\times401$
13.	4209797387208401	$337\times5381\times2321497933$
14.	84405914003648140	$2\times2\times5\times43\times1514549\times64802401$

Megjegyzés a (fenti) táblázathoz: A 3. szám 401-gyel egyenlő, a 6., 9., 12. szám osztható vele. Az 5. szám 161201-gyel egyenlő, a 10. szám osztható vele. A 7. szám 64802401-gyel egyenlő, a 14. szám osztható vele. Csak akkor kaphatunk prímszámot, ha az n kitevő maga is prím.

4.) A lánctörtben a kivonás művelete is meg van engedve, ekkor a kiindulási egyenlet az $x^2-C\cdot x+1=0$ alakot ölti, átrendezve: $x=C-\frac{1}{x}$,

$$x=C-\frac{1}{C-\frac{1}{x}}.$$

Látható, hogy a lánctörtben sorozatos kivonás van. Így kapjuk meg a második, $f_2(C,n)$ függvényünket, mely – bár csak egy előjelben különbözik az elsőtől – egészen másként viselkedik.

$$f_2(C,n) = \frac{\left(\frac{C+\sqrt{C^2-4}}{2}\right)^n - \left(\frac{C-\sqrt{C^2-4}}{2}\right)^n}{\sqrt{C^2-4}}.$$

Ha n-et 1-től 16-ig változtatjuk, a következő polinomokat kapjuk:

$$\begin{array}{l}
1 \\
C \\
C^2 - \ 1 \\
C^3 - \ 2 \cdot C \\
C^4 - \ 3 \cdot C^2 + 1 \\
C^5 - \ 4 \cdot C^3 + 3 \cdot C \\
C^6 - \ 5 \cdot C^4 + 6 \cdot C^2 - 1 \\
C^7 - \ 6 \cdot C^5 + 10 \cdot C^3 - 4 \cdot C \\
C^8 - \ 7 \cdot C^6 + 15 \cdot C^4 - 10 \cdot C^2 + 1 \\
C^9 - \ 8 \cdot C^7 + 21 \cdot C^5 - 20 \cdot C^3 + 5 \cdot C \\
C^{10} - \ 9 \cdot C^8 + 28 \cdot C^6 - 35 \cdot C^4 + 15 \cdot C^2 - 1 \\
C^{11} - 10 \cdot C^9 + 36 \cdot C^7 - 56 \cdot C^5 + 35 \cdot C^3 - 6 \cdot C \\
C^{12} - 11 \cdot C^10 + 45 \cdot C^8 - 84 \cdot C^6 + 70 \cdot C^4 - 21 \cdot C^2 + 1 \\
C^{13} - 12 \cdot C^11 + 55 \cdot C^9 - 120 \cdot C^7 + 126 \cdot C^5 - 56 \cdot C^3 + 7 \cdot C \\
C^{14} - 13 \cdot C^12 + 66 \cdot C^10 - 165 \cdot C^8 + 210 \cdot C^6 - 126 \cdot C^4 + 28 \cdot C^2 - 1 \\
C^{15} - 14 \cdot C^13 + 78 \cdot C^11 - 220 \cdot C^9 + 330 \cdot C^7 - 252 \cdot C^5 + 84 \cdot C^3 - 8 \cdot C
\end{array}$$

Ezek a polinomok az $f_1(C,n)$ függvény polinomjaitól csak abban különböznek, hogy alternálva szerepelnek bennük kivonások és összeadások. Ugyanakkor az $f_2(C,n)$ függvény esetében ki kell kötni, hogy $C > 2$, mert (bár a polinomok nem vezetnek hibára) $C = 2$ esetén a négyzetgyökös kifejezés 0-val egyenlő, és ezzel osztani is kellene, $C = 1$ esetében pedig képzetes számokat kapnánk. Második számú SEJTÉS: az $f_2(C,n)$ formula, amennyiben C és n 2-nél nagyobb pozitív egész számok, sohasem eredményez prímszámot, csak összetett számot. Ez az állítás csak számítógéppel van ellenőrizve, a gép nem talált ellenpéldát.

5.) Az $f_2(C,n)$ függvény érdekes alkalmazása: $C = 6$ esetén a „háromszögű négyzetszámokat" állítja elő, azokat a számokat, melyeknek a négyzete egyben háromszögszám is, tehát az

$$M^2 = N \times \frac{N+1}{2}$$

egyenlet egész „M" megoldásait, például $6 \times 6 = 8 \times 9/2 = 36$.

$$M = 1 \;\; 6 \;\; 35 \;\; 204 \;\; 1189 \;\; 6930 \;\; 40391 \;\; 235416 \;\; 1372105 \;\; 7997214 \\ 46611179 \;\; 271669860 \;\; 1583407981 \;\; 9228778026$$

$$f_2(6,n) = \frac{\left(3+2\sqrt{2}\right)^n - \left(3-2\sqrt{2}\right)^n}{4\sqrt{2}}.$$

(Ezt a formulát már Leonhard Euler is ismerte.) Az $f_2(C,n)$ függvény alkalmas további sokszögszámok között fennálló egyenlőségek megkeresésére is.

6.) További gyakorlati alkalmazások

Amennyiben valaki számítógépbe szeretné programozni a fenti képleteket, két módszer közül választhat. Ha megelégszik legfeljebb 18-jegyű prímszámok előállításával, akkor az $f_1(C,n)$ formulát kell választani, amely tartalmazza mind a négy alapműveletet és egy négyzetgyökös kifejezést is (amellyel osztani is kell). Ebben az esetben szükség van lebegőpontos aritmetikára (és lebegőpontos változókra) is. Eredményül egész számokat kapunk, de ehhez irracionális számok kiszámításán keresztül vezet az út.

Amennyiben minél nagyobb („rekord") prímszámokra vadászik valaki, akkor célszerű kijelölni egy „n" hatványkitevőt, és csak az ehhez az n-hez tartozó egyetlen sort beprogramozni.

Például ha az $n = 19$-es értéket választjuk, akkor a képletünk a következő:

$$C^{18} + 17 \cdot C^{16} + 120 \cdot C^{14} + 455 \cdot C^{12} + 1001 \cdot C^{10} + 1287 \cdot C^8 \\ + 924 \cdot C^6 + 330 \cdot C^4 + 45 \cdot C^2 + 1.$$

Ez a formula csak összeadást és szorzást tartalmaz (a hatványozást szorzások sorozatára vezetjük vissza). Ha például 100 millió jegyet tartalmazó prímszámokat keresünk (amelyek megtalálásáért pénzjutalmat tűzött ki a „GIMPS project"), akkor a $C = 10^{5555555}$ értékkel célszerű indítani, és C-t egyesével növelni, léptetni. Ugyanis C mibenlétére semmiféle korlátozás nincsen, lehet páros, páratlan, prím- vagy összetett szám is.

Voltaképpen nem egyetlen prímszámképletről beszélhetünk, hanem prímszámképletek (végtelen) sorozatáról. Annyi prímszámképlet van, ahány prímszám. Minden prím „n”-hez hozzárendelhetünk egy prímszámképletet. A táblázatban felsorolt azon polinomokat, melyek sorszáma összetett szám, figyelmen kívül kell hagyni.

n	$f_1(C, n)$
3	$C^2 + 1$
5	$C^4 + 3 \cdot C^2 + 1$
7	$C^6 + 5 \cdot C^4 + 6 \cdot C^2 + 1$
11	$C^{10} + 9 \cdot C^8 + 28 \cdot C^6 + 35 \cdot C^4 + 15 \cdot C^2 + 1$
13	$C^{12} + 11 \cdot C^{10} + 45 \cdot C^8 + 84 \cdot C^6 + 70 \cdot C^4 + 21 \cdot C^2 + 1$
17	$C^{16}+15\cdot C^{14}+91\cdot C^{12}+286\cdot C^{10}+495\cdot C^8+462\cdot C^6+210\cdot C^4+36\cdot C^2+1$

Vizsgálataim során a legnagyobb prímszám $C = 64$ és $n = 47$ esetén lépett fel, ez egy 84-jegyű prímszám, melynek első 75 számjegye a következő:

122757598692418781147104210611116761516797358732284384882390533627837932878...

Abban bízom, hogy ez a képlet ($f_1(C, n)$ függvény) a legnagyobb („largest”) prímek tartományában ugyanúgy viselkedik, mint az általam vizsgált (legalacsonyabb) nagyságrendben. Azt is elképzelhetőnek tartom, hogy egyszer a prímszámrekordot is ezzel a képlettel állítják majd be.

Irodalomjegyzék

[1] Maurer I. Gyula, *Tizedes törtek és lánctörtek*, Dacia Könyvkiadó, Kolozsvár-Napoca, 1981.

[2] Gerőcs László, *A Fibonacci-sorozat általánosítása*, Tankönyvkiadó, 1988.

[3] Freud Róbert, Gyarmati Edit, *Számelmélet*, Nemzeti Tankönyvkiadó, 2000.

[4] Ian Stewart, *A matematika problémái*, Akadémiai Kiadó, 1991.

[5] Sain Márton, A Fibonacci-sorozattól lánctörtekkel az aranymetszésig. In: *A lánctörtektől a számítógépig*, Tankönyvkiadó, 1975.