

Atli Harðarson

Fibonacci tölur mod a

Inngangur

Í því sem hér fer á eftir verður f_n notað til að tákna tölu númer n í fibonacci talnaröðinni: 1, 1, 2, 3, 5, 8, 13, 21, 34 ...

Tölurnar verða númeraðar frá 1 og upp úr (ekki frá 0 eins og stundum er gert) svo $f_1 = 1$, $f_2 = 1$ og ef $n > 2$ þá er $f_n = f_{n-2} + f_{n-1}$.

Rithátturinn $a|b$ verður notaður til að tákna að talan a gangi upp í tölunni b.

Rithátturinn $x \equiv y \pmod{a}$ verður notaður til að tákna að x og y tilheyri sama leifaflokki mod a, þ.e. að $a|(x-y)$. Gert er ráð fyrir að lesandi sé kunnugur reiknireglum um leifaflokka.

Mengi náttúrulegra talna verður táknað með \mathbf{N} og þá er átt við heilu tölurnar frá 1 og upp úr, þ.e.a.s. hér telst $0 \notin \mathbf{N}$.

Taflan á næstu blaðsíðu sýnir fibonacci tölurnar f_1 til f_{60} (í 2. dálki) og þar fyrir aftan eru talnarunurnar $f_n \pmod{a}$ fyrir $1 \leq n \leq 60$ og $2 \leq a \leq 22$. Þetta eru lægstu jákvæðu tölurnar í leifaflokkum fibonacci talnanna mod a. Í 7. línu, dálkinum fyrir $a=5$ er t.d. lægsta jákvæða talan, i, sem um gildir $i \equiv f_7 \pmod{5}$ og almennt gildir að í línu n, dálki a er lægsta jákvæða tala, i, sem um gildir $i \equiv f_n \pmod{a}$.

Hér verður tala númer n í rununni $f_n \pmod{a}$ kölluð a_n . Hægt er að reikna a_n á sama hátt og fibonacci tölurnar því $a_1 = 1$, $a_2 = 1$ og ef $n > 2$ þá er $a_n = (a_{n-2} + a_{n-1}) \pmod{a}$.

Þegar taflan er skoðuð kemur í ljós að dálkarnir fyrir $f_n \pmod{a}$ eru **lotubundnir**. Þetta er dregið fram með því að innramma og skyggja fyrstu lotu hvers dálks. Annað sem veur athygli er að í hverjum dálki kemur talan **0** fyrir **með jöfnu millibili**. Þetta er dregið fram með því að feitiletra öll 0 og skyggja reitinn sem það fyrsta er í. Það þriðja sem veur athygli er að **bilið milli núlla er afar mislangt** og ekki virðist nein einföld regla á hve langt það er og sömuleiðis eru loturnar mislangar en **fjöldi núlla í hverri lotu er þó alltaf 1, 2 eða 4**.

Í því sem hér fer á eftir verða sannaðar nokkrar setningar um þessar lotur, lengd þeirra og fjölda núlla í þeim.

n	fibonacci tala nr. n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	0	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4	3	1	0	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
5	5	1	2	1	0	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
6	8	0	2	0	3	2	1	0	8	8	8	8	8	8	8	8	8	8	8	8	8	8
7	13	1	1	1	3	1	6	5	4	3	2	1	0	13	13	13	13	13	13	13	13	13
8	21	1	0	1	1	3	0	5	3	1	10	9	8	7	6	5	4	3	2	1	0	21
9	34	0	1	2	4	4	6	2	7	4	1	10	8	6	4	2	0	16	15	14	13	12
10	55	1	1	3	0	1	6	7	1	5	0	7	3	13	10	7	4	1	17	15	13	11
11	89	1	2	1	4	5	5	1	8	9	1	5	11	5	14	9	4	17	13	9	5	1
12	144	0	0	0	4	0	4	0	0	4	1	0	1	4	9	0	8	0	11	4	18	12
13	233	1	2	1	3	5	2	1	8	3	2	5	12	9	8	9	12	17	5	13	2	13
14	377	1	2	1	2	5	6	1	8	7	3	5	0	13	2	9	3	17	16	17	20	3
15	610	0	1	2	0	4	1	2	7	0	5	10	12	8	10	2	15	16	2	10	1	16
16	987	1	0	3	2	3	0	3	6	7	8	3	12	7	12	11	1	15	18	7	0	19
17	1.597	1	1	1	2	1	1	5	4	7	2	1	11	1	7	13	16	13	1	17	1	13
18	2.584	0	1	0	4	4	1	0	1	4	10	4	10	8	4	8	0	10	0	4	1	10
19	4.181	1	2	1	1	5	2	5	5	1	1	5	8	9	11	5	16	5	1	1	2	1
20	6.765	1	0	1	0	3	3	5	6	5	0	9	5	3	0	13	16	15	1	5	3	11
21	10.946	0	2	2	1	2	5	2	2	6	1	2	0	12	11	2	15	2	2	6	5	12
22	17.711	1	2	3	1	5	1	7	8	1	1	11	5	1	11	15	14	17	3	11	8	1
23	28.657	1	1	1	2	1	6	1	1	7	2	1	5	13	7	1	12	1	5	17	13	13
24	46.368	0	0	0	3	0	0	0	0	8	3	0	10	0	3	0	9	0	8	8	0	14
25	75.025	1	1	1	0	1	6	1	1	5	5	1	2	13	10	1	4	1	13	5	13	5
26	121.393	1	1	1	3	1	6	1	1	3	8	1	12	13	13	1	13	1	2	13	13	19
27	196.418	0	2	2	3	2	5	2	2	8	2	2	1	12	8	2	0	2	15	18	5	2
28	317.811	1	0	3	1	3	4	3	3	1	10	3	0	11	6	3	13	3	17	11	18	21
29	514.229	1	2	1	4	5	2	5	5	9	1	5	1	9	14	5	13	5	13	9	2	1
30	832.040	0	2	0	0	2	6	0	8	0	0	8	1	6	5	8	9	8	11	0	20	0
31	1.346.269	1	1	1	4	1	1	5	4	9	1	1	2	1	4	13	5	13	5	9	1	1
32	2.178.309	1	0	1	4	3	0	5	3	9	1	9	3	7	9	5	14	3	16	9	0	1
33	3.524.578	0	1	2	3	4	1	2	7	8	2	10	5	8	13	2	2	16	2	18	1	2
34	5.702.887	1	1	3	2	1	1	7	1	7	3	7	8	1	7	7	16	1	18	7	1	3
35	9.227.465	1	2	1	0	5	2	1	8	5	5	5	0	9	5	9	1	17	1	5	2	5
36	14.930.352	0	0	0	2	0	3	0	0	2	8	0	8	10	12	0	0	0	0	12	3	8
37	24.157.817	1	2	1	2	5	5	1	8	7	2	5	8	5	2	9	1	17	1	17	5	13
38	39.088.169	1	2	1	4	5	1	1	8	9	10	5	3	1	14	9	1	17	1	9	8	21
39	63.245.986	0	1	2	1	4	6	2	7	6	1	10	11	6	1	2	2	16	2	6	13	12
40	102.334.155	1	0	3	0	3	0	3	6	5	0	3	1	7	0	11	3	15	3	15	0	11
41	165.580.141	1	1	1	1	1	6	5	4	1	1	1	12	13	1	13	5	13	5	1	13	1
42	267.914.296	0	1	0	1	4	6	0	1	6	1	4	0	6	1	8	8	10	8	16	13	12
43	433.494.437	1	2	1	2	5	5	5	5	7	2	5	12	5	2	5	13	5	13	17	5	13
44	701.408.733	1	0	1	3	3	4	5	6	3	3	9	12	11	3	13	4	15	2	13	18	3
45	1.134.903.170	0	2	2	0	2	2	2	2	0	5	2	11	2	5	2	0	2	15	10	2	16
46	1.836.311.903	1	2	3	3	5	6	7	8	3	8	11	10	13	8	15	4	17	17	3	20	19
47	2.971.215.073	1	1	1	3	1	1	1	1	3	2	1	8	1	13	1	4	1	13	13	1	13
48	4.807.526.976	0	0	0	1	0	0	0	0	6	10	0	5	0	6	0	8	0	11	16	0	10
49	7.778.742.049	1	1	1	4	1	1	1	1	9	1	1	0	1	4	1	12	1	5	9	1	1
50	12.586.269.025	1	1	1	0	1	1	1	1	5	0	1	5	1	10	1	3	1	16	5	1	11
51	20.365.011.074	0	2	2	4	2	2	2	2	4	1	2	5	2	14	2	15	2	2	14	2	12
52	32.951.280.099	1	0	3	4	3	3	3	3	9	1	3	10	3	9	3	1	3	18	19	3	1
53	53.316.291.173	1	2	1	3	5	5	5	5	3	2	5	2	5	8	5	16	5	1	13	5	13
54	86.267.571.272	0	2	0	2	2	1	0	8	2	3	8	12	8	2	8	0	8	0	12	8	14
55	139.583.862.445	1	1	1	0	1	6	5	4	5	5	1	1	13	10	13	16	13	1	5	13	5
56	225.851.433.717	1	0	1	2	3	0	5	3	7	8	9	0	7	12	5	16	3	1	17	0	19
57	365.435.296.162	0	1	2	2	4	6	2	7	2	2	10	1	6	7	2	15	16	2	2	13	2
58	591.286.729.879	1	1	3	4	1	6	7	1	9	10	7	1	13	4	7	14	1	3	19	13	21
59	956.722.026.041	1	2	1	1	5	5	1	8	1	1	5	2	5	11	9	12	17	5	1	5	1
60	1.548.008.755.920	0	0	0	0	0	4	0	0	0	0	0	3	4	0	0	9	0	8	0	18	0
Fyrsta 0 er í línu		3	4	6	5	12	8	6	12	15	10	12	7	24	20	12	9	12	18	30	8	30
Lengd lotu er		3	8	6	20	24	16	12	24	60	10	24	28	48	40	24	36	24	18	60	16	30

Setning 1 Um allar tölur $a \in \mathbf{N}$, $a > 1$ gildir að talnarunan $f_n \pmod a$ er lotubundin og ef lengd lotunnar er táknuð með $L(a)$ gildir $L(a) \leq a^2$.

Sönnun Hver tala í rununni ákvarðast af næstu tveim á undan svo ef talnatvennd endurtekur sig þannig að fyrir einhverja tölu $k \in \mathbf{N}$ gildi $a_n = a_{n+k}$ og $a_{n+1} = a_{n+1+k}$ þá er $a_{n+2} = a_{n+2+k}$ o.s.frv. svo fyrir allar tölur $m \in \mathbf{Z}$ er $a_{n+m} = a_{n+m+k}$ svo fremi $n + m > 0$.

Ástæðan fyrir því að þetta gildir um allar tölur $m \in \mathbf{Z}$, en ekki bara um náttúrulegar tölur, er sú að talnapar ákvarðar ekki aðeins það sem á eftir kemur heldur líka það sem er á undan því $a_{n-1} = (a_{n+1} - a_n) \pmod a$. Það er því ekki um það að ræða að runa sé aðeins lotubundin frá einhverri tölu a_j , $j > 1$.

Nú eru tölurnar í rununni $f_n \pmod a$ allar á bilinu frá 0 upp í $a - 1$, semsagt a mismunandi tölur svo tvær tölur í röð geta verið á a^2 mismunandi vegu. Ef ritaðar eru meira en a^2 talnatvenndir hljóta því einhverjar tvær að vera eins. Fyrsta talnatvenndin samanstendur af tölunum a_1 og a_2 , sú næsta af a_2 og a_3 o.s.frv. Þegar komnar eru $a^2 + 1$ tölur eru tvenndirnar því orðnar a^2 og þá er ekki hægt að fjölga tölum án þess að talnatvennd endurtaki sig og þar með er komin fram lota í rununni. ■

Setning 2 Um allar tölur $a \in \mathbf{N}$, $a > 1$ gildir að talnarunan $f_n \pmod a$ inniheldur töluna 0.

Sönnun Sérhver runa hefst á tölunum 1, 1 og er (skv. setningu 1) lotubundin þannig að talnaparið 1, 1, kemur fyrir aftur. Talan 0 hlýtur því að koma fyrir, því ef talan á undan 1, 1 eru kölluð a_k þá standa í töð tölurnar $a_k, 1, 1$, þar sem $a_k + 1 \equiv 1 \pmod a \Rightarrow a_k \equiv 0 \pmod a \Rightarrow a_k = 0$. ■

Þar sem $a_k = 0$ þá og því aðeins að $a|f_k$ leiðir beint af setningu 2 að fyrir sérhverja tölu $a \in \mathbf{N}$ er til einhver fibonacci tala f_k þ.a. $a|f_k$.

Hjálparsetning Ef $a_k = 0$ og $a_{k-1} = i$ þá gildir um allar tölur $m \in \mathbf{N}$ að $a_{k+m} \equiv i \cdot a_m$.

Sönnun Þetta er hægt að sanna með þrepun, svona:

Setningin gildir fyrir $m = 1$ því $a_{k+1} \equiv a_k + a_{k-1} \equiv 0 + i \equiv i \cdot a_1$ (þar sem $a_1 = 1$). Hún gildir líka fyrir $m = 2$ því $a_{k+2} \equiv a_{k+1} + a_k \equiv i + 0 \equiv i \cdot a_2$ (þar sem $a_2 = 1$).

Ef setningin gildir fyrir allar tölur frá 1 til m (þar sem $m > 1$) þá gildir hún fyrir $m + 1$ því $a_{k+m+1} \equiv a_{k+m} + a_{k+m-1} \equiv i \cdot a_m + i \cdot a_{m-1} \equiv i \cdot (a_m + a_{m-1}) \equiv i \cdot a_{m+1}$. ■

Setning 3 Um allar tölur $a \in \mathbf{N}$, $a > 1$ gildir að ef talan 0 kemur fyrir í línu k í talnarununni $f_n \pmod a$ þá kemur 0 fyrir í línu $n \cdot k$ fyrir öll $n \in \mathbf{N}$.

Sönnun Alls staðar þar sem 0 kemur fyrir er talan á undan því sama tala og næstu tvær á eftir, því á eftir a_i , 0 kemur $a_i + 0 = a_i$ og þar á eftir $0 + a_i = a_i$.

Nú notum við hjálparsetninguna til að sanna, með þrepun, að ef $a_k \equiv 0$ þá gildir um allar tölur $n \in \mathbf{N}$ að $a_{nk} \equiv 0$. Setjum k inn fyrir

m í $a_{k+m} \equiv i \cdot a_m$. Þá fæst $a_{k+k} \equiv i \cdot a_k \equiv i \cdot 0 \equiv 0$. Hér með er sýnt að ef $a_k \equiv 0$ þá er $a_{2k} \equiv 0$. Næst er sýnt fram á að ef $a_{nk} \equiv 0$ þá er $a_{(n+1)k} \equiv 0$ svona: $a_{(n+1)k} \equiv a_{nk+k} \equiv i \cdot a_{nk} \equiv i \cdot 0 \equiv 0$.

Af þessu leiðir að ef núll kemur fyrir í línu k þá kemur annað núll í línu $2k$ það þriðja í línu $3k$ o.s.frv. ■

Af setningu 3 leiðir beint:

Setning 4 Fyrir sérhverja tölu $a \in \mathbf{N}$ er til tala $k \in \mathbf{N}$ þannig að um allar tölur $n \in \mathbf{N}$ gildi $a|f_{nk}$.

Sönnun Samkvæmt setningu 3 er til tala $k \in \mathbf{N}$ þannig að um allar tölur $n \in \mathbf{N}$ gildi $a_{nk} \equiv 0 \pmod{a}$. Þetta jafngildir því að $f_{nk} \pmod{a} = 0$ eða með öðru orðalagi að $a|f_{nk}$. ■

Önnur athyglisverð afleiðing af setningu 3 er:

Setning 5 Um allar náttúrulegar tölur i og j gildir að ef $i|j$ þá $f_i|f_j$.

Sönnun Setjum $a = f_i$, þá er $a_i = 0$ (því þá er $f_i \pmod{a} = f_i \pmod{f_i} = 0$).

Ef $i|j$ þá er til $n \in \mathbf{N}$ þ.a. $j = n \cdot i$ og fyrst $a_i = 0$ leiðir af þessu og setningu 3 að $a_j = 0$ sem þýðir að $a|f_j$. Fyrst $a = f_i$ jafngildir $a|f_j$ því að $f_i|f_j$. ■

Af setningu 5 má leiða:

Setning 6 Ef $j > 4$ og f_j er prímtala þá er j prímtala.

Sönnun Ef j er samsett tala og $j > 4$ þá er til náttúruleg tala $i > 2$ sem er þáttur í j . Þar sem $i|j$ leiðir af setningu 5 að $f_i|f_j$ og þar sem $f_i > 1$ ef $i > 2$ leiðir af þessu að f_j er ekki prímtala. ■

Vert er að árétta að þetta gildir ekki ef $j \leq 4$ því $f_4 = 3$ svo f_4 er prímtala þótt 4 sé það ekki. Einnig er vert að nefna að leiðingin gengur aðeins í aðra áttina og það gildir ekki almennt og yfirleitt að f_j sé prímtala ef j prímtala. T.d. er 19 prímtala en $f_{19} = 4181$ er það ekki því $4181 = 37 \cdot 113$.

Nú er komið að því að segja eitthvað um lotulengd runu á forminu $f_n \pmod{a}$.

Hjálparsetning Ef $a_k \equiv 0$ þá er $a_{k+2} \equiv -a_{k-2}$.

Sönnun Almennt gildir að $a_k \equiv a_{k-1} + a_{k-2}$ og þar sem $a_k \equiv 0$ og $a_{k-1} \equiv a_{k+2}$ jafngildir þetta því að $0 \equiv a_{k+2} + a_{k-2}$ sem jafngildir því að $a_{k+2} \equiv -a_{k-2}$. ■

Setning 7 Fyrir sérhvert $a \in \mathbf{N}$, $a > 1$ gildir að talan 0 kemur fyrir 1 sinni eða 2 sinnum eða 4 sinnum í lotu rununnar $f_n \pmod{a}$.

Sönnun Ef k er lægsta tala þ.a. $a_k \equiv 0$ þá er tvennt til:

- i. Það getur verið að $a_{k-1} \equiv 1$ og þá endar lotan á a_k og inniheldur því aðeins eitt núll.
- ii. Það getur verið að $a_{k-1} \not\equiv 1$ og þá er $a_{k+1} \equiv a_{k-1}$ og $a_{k+2} \equiv -a_{k-2}$ (samkvæmt hjálparsetningunni sem sönnuð var hér að framan). Þar sem $a_{k-1} \equiv f_{k-1}$ og $-a_{k-2} \equiv -f_{k-2}$ leiðir af þessu að $a_{k+3} \equiv a_{k+1} + a_{k+2} \equiv a_{k-1} + (-a_{k-2}) \equiv f_{k-1} + (-f_{k-2}) \equiv f_{k-3}$ og

$$a_{k+4} \equiv a_{k+2} + a_{k+3} \equiv -a_{k-2} + f_{k-3} \equiv -f_{k-2} + f_{k-3} \equiv -f_{k-4}$$

og þannig gengur þetta áfram að $a_{k+m} \equiv (-1)^{m-1} \cdot f_{k-m}$. (Taflan til hægri sýnir hvernig þetta lítur út fyrir $a = 5$ og $a = 7$.)

Þegar fibonacci tölugildin koma svona í öfugri röð og önnur hver með mínus fyrir framan hljóta a_{2k-2} og a_{2k-1} báðar að hafa tölugildið 1 og önnur að vera -1. Nú er enn tvennt til.

- ii. a) a_{2k-1} getur verið 1 og þá endar lotan á tölu a_{2k} (sem er að sjálfsögðu 0 sbr. setningu 3) og þá hefur lotan 2 núll. (Þetta gerist t.d. þegar $a = 7$ sbr. aftasta dálkinn í töflunni til hægri.)

- ii. b) a_{2k-1} getur verið -1 og þá er $a_{2k+1} \equiv a_{2k+2} \equiv -1$ og þá gildir (sbr. hjálparsetningu á undan setningu 3) um allar tölurnar neðan við a_{2k} að $a_{2k+m} \equiv -1 \cdot a_m$, svo fyrst $a_{2k-1} \equiv -1$ er $a_{4k-1} \equiv 1$ og lotan endar á a_{4k} og hefur þá 4 núll. (Þetta gerist t.d. þegar $a = 5$ sbr. næstaftasta dálkinn í töflunni til hægri.)

Útilokað er að lota innihaldi 3 núll því eins og sýnt hefur verið fram á hefst ný lota eftir fjórða núll ef hún hefur meira en tvö núll og ef lota hefur meira en tvö núll þá getur ný ekki byrjað bæði við þriðja og fjórða núll. ■

Af rökfærslunni í þessari sönnun er ljóst að ef fyrsta núll í runu er í línu k þá er það næsta í línu númer $2k$ og ekki getur verið neitt núll þar á milli. Við getum því staðhæft sterkari fullyrðingu en setningu 3

Setning 8 Ef fyrsta núll í talnaruninni $f_n \bmod a$ er í línu númer k þá gildir um öll $n \in \mathbb{N}$ að n -ta núllið er í línu númer $n \cdot k$.

*

Auðvelt er að ákvarða $L(a)$, þ.e. lengd lotu í talnaruninni $f_n \bmod a$, þegar búið er að skrifa rununa niður að fyrsta núlli. Ef fyrsta núll er í línu k þá er $L(a) = k$ ef $a_{k-1} \equiv 1$, annars er $L(a) = 2k$ ef k er slétt tala og $L(a) = 4k$ ef k er oddatala.

Reynum nú að átta okkur á hvenær 0 kemur fyrst fyrir í talnarunu af þessari gerð?

Ég skilgreini **einþátta tölu** sem tölu á forminu p^n þar sem p er prímtala og $n \in \mathbb{N}$. Þetta eru semsagt prímtölurnar og heil veldi af þeim. **Einþættir** samsettrar tölu eru hæstu einþátta tölur sem ganga upp í hana. Þannig eru 16 og 5 t.d. einþættir tölunnar 80. Þótt 4 sé einþátta tala telst hún ekki til einþátta tölunnar 80 því til er hærra veldi af 2, nefnilega 16, sem gengur upp í 80.

Fallið $N(a)$ skilgreini ég svo að það sé lægsta tala $k \in \mathbb{N}$ sem um gildir að $f_k \bmod a = 0$. Útkoma fallsins segir hvar 0 kemur fyrst fyrir í rununni $f_n \bmod a$.

n	f_n	$f_n \bmod 5$	$f_n \bmod 7$
1	1	$1 \equiv 1$	$1 \equiv 1$
2	1	$1 \equiv 1$	$1 \equiv 1$
3	2	$2 \equiv 2$	$2 \equiv 2$
4	3	$3 \equiv 3$	$3 \equiv 3$
5	5	$0 \equiv 0$	$5 \equiv 5$
6	8	$3 \equiv 3$	$1 \equiv 8$
7	13	$3 \equiv -2$	$6 \equiv 13$
8	21	$1 \equiv 1$	$0 \equiv 0$
9	34	$4 \equiv -1$	$6 \equiv 13$
10	55	$0 \equiv 0$	$6 \equiv -8$
11	89	$4 \equiv -1$	$5 \equiv 5$
12	144	$4 \equiv -1$	$4 \equiv -3$
13	233	$3 \equiv -2$	$2 \equiv 2$
14	377	$2 \equiv -3$	$6 \equiv -1$
15	610	$0 \equiv 0$	$1 \equiv 1$
16	987	$2 \equiv -3$	$0 \equiv 0$
17	1.597	$2 \equiv 2$	
18	2.584	$4 \equiv -1$	
19	4.181	$1 \equiv 1$	
20	6.765	$0 \equiv 0$	

Setning 9 Ef einþættir tölunnar a eru e_1, e_2, \dots, e_n þá er $N(a)$ lægsta sameiginlegt margfeldi talnanna $N(e_1), N(e_2), \dots, N(e_n)$.

Sönnun Þar sem a gengur upp í $f_{N(a)}$ ganga allir þættir a upp í $f_{N(a)}$ svo um sérhvern einþátt e_i gildir að $f_{N(a)} \bmod e_i = 0$ og þar sem núll koma (skv. setningu 8) fyrir með jöfnu millibili í öllum runum á forminu $f_n \bmod e_i$ hlýtur $N(a)$ að vera sameiginlegt margfeldi talnanna $N(e_1), N(e_2), \dots, N(e_n)$.

Notum k til að tákna lægsta sameiginlega margfeldi talnanna $N(e_1), N(e_2), \dots, N(e_n)$. Allir einþættir a eru þá þættir í f_k og a gengur upp í f_k fyrst allir einþættir hennar gera það svo k er þá lægsta tala sem um gildir að $f_k \bmod a = 0$. ■

Setning 10 Ef $a_i | a_j$ þá $N(a_i) | N(a_j)$.

Sönnun Ef $a_i | a_j$ þá gildir um allar tölur $n \in \mathbf{N}$ að ef $f_n \bmod a_j = 0$ þá er $f_n \bmod a_i = 0$. Núllin eru (skv. setningu 8) með jöfnu millibili í báðum röðum. Ef fyrsta núllið í röðinni $f_n \bmod a_j$ er tala númer k í þeirri röð hlýtur k því að vera heilt margfeldi af $N(a_i)$ sem jafngildir því að $N(a_i) | N(a_j)$. ■

Þær setningar sem sannaðar hafa verið duga til að finna lotulengd runu á forminu $f_n \bmod a$ ef a er samsett tala og vitað er um staðsetningu fyrsta núlls í öllum runum á forminu $f_n \bmod e_i$ þar sem e_i eru einþættir tölunnar a .

Mér hefur ekki tekist að finna neina reglu á því hvenær núll kemur fyrst fyrir í runu, $f_n \bmod a$, þegar a er prímtala. En mér finnst eftirfarandi tilgáta um einþátta tölur sennileg.

Tilgáta Ef a er á forminu p^n þar sem p er prímtala, $p > 2$ og $n \in \mathbf{N}$ þá er $N(a) = p^{(n-1)} \cdot N(p)$.

Mér hefur ekki tekist að sanna þess tilgátu en prófanir fyrir nokkrar lágar tölur benda til að það sé þess virði að hugleiða hana.

Eftirfarandi tafla sýnir $N(a)$ fyrir einþátta tölur sem eru 1. til 6. veldi af prímtölunum 3, 5, 7, 11, 13, 17, 19, 23, 29, 31. Talan 110 í 4. línu, 2. dálki táknar að $N(11^2) = N(121) = 110$, þ.e. í rununni $f_n \bmod 121$ komi fyrsta núllið í 110. sæti.

Eins og sést verða þetta fljótt ansi háar tölur. Þannig er fyrsta fibonacci talan sem 31^6 gengur upp í númer 858.874.530.

Allar tölur í töflunni koma heim við þá tilgátu að $N(p^n) = p^{(n-1)} \cdot N(p)$. Prófun á nokkrum öðrum einþátta tölum sem valdar af handahófi og allar voru lægri en 10^9 dugði ekki til að hrekja tilgátuna.

p	$N(p)$	$N(p^2)$	$N(p^3)$	$N(p^4)$	$N(p^5)$	$N(p^6)$
3	4	12	36	108	324	972
5	5	25	125	625	3.125	15.625
7	8	56	392	2.744	19.208	134.456
11	10	110	1.210	13.310	146.410	1.610.510
13	7	91	1.183	15.379	199.927	2.599.051
17	9	153	2.601	44.217	751.689	12.778.713
19	18	342	6.498	123.462	2.345.778	44.569.782
23	24	552	12.696	292.008	6.716.184	154.472.232
29	14	406	11.774	341.446	9.901.934	287.156.086
31	30	930	28.830	893.730	27.705.630	858.874.530