VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
TIKIMYBIŲ TEORIJOS IR SKAIČIŲ TEORIJOS KATEDRA

Ugnė Kolosovaitė

PIRMINIŲ SKAIČIŲ YRA BE GALO DAUG: ĮRODYMŲ APŽVALGA

THERE ARE INFINITELY MANY PRIME NUMBERS: REVIEW OF PROOFS

Bakalauro baigiamasis darbas

Leidžiu ginti .....

Darbo vadovas prof. Artūras Dubickas

Vilnius 2022

Turinys

Santrauka

Šiame darbe apžvelgiau keletą įrodymų, teigiančių, kad pirminių skaičių yra be galo daug. Pradėjau nuo pirmojo išlikusio šio teiginio įrodymo. Jį aprašė matematikas Euklidas, teigdamas, kad pirminių skaičių yra daugiau, nei galima rasti bet kuriame baigtiniame sąraše. Jo įrodymas naudojant prieštaros metodą iki dabar yra laikomas pačiu paprasčiausiu. Kitas žymus matematikas Oileris savo darbe *„Variae observationes circa series infinitas“* pristato net keletą teoremų, įrodinėjančių pirminių skaičių begalybę. Šiame darbe pasirinkau apžvelgti vieną iš jų. Be viso to, kiti matematikai tai įrodinėjo naudodami Ferma skaičius ir logaritmus.

Be viso to, pristačiau ir kitas pirminius skaičius nagrinėjančias sritis, tokias kaip Merseno skaičius ir apžvelgiau keletą algoritmų, sukurtų testuoti, ar skaičius yra pirminis ar ne (vienas iš algoritmų būtent ir naudojasi Merseno skaičiais). Šie algoritmai remiasi teorija apžvelgta šiame darbe.

Summary

In this work I have reviewed several proofs stating that there are infinitely many primes. I started with the very first known proof by Euklid, which is still considered to be the simplest. Mathematician proves it by using contradiction method and his original statement is that there are more prime numbers than you can find in any finite list. Other famous mathematician Euler in his work *"Variae observationes circa series infinitas"* presents not only one, but several proofs of the infinitude of primes, out of which one was reviewed in this thesis. Other mathematicians proved it by using Fermat numbers and even logarithms.

Aside from the direct proofs of the infinitude of primes I also have presented Mersenne numbers and even presented several tests used to check if the number is prime or not (one of which is based on the Mersenne prime numbers). These tests also use the theory presented in this work.

Įvadas

Pirmieji išlikę įrašai apie pirminių skaičių ir jų savybių studijavimą yra kilę iš graikų matematikų. Euklido traktate „Elementai“ yra įrodinėjama, kad pirminių skaičių yra be galo daug, fundamentalioji aritmetikos teorema, be to, rodo, kaip sukonstruoti tobulą skaičių iš Merseno pirminių skaičių.

Šio darbo tikslas yra apibrėžti ir pateikti pagrindines teoremas, įrodančias pirminių skaičių begalybę ir apžvelgti keletą pirminių skaičių testavimo algoritmų.

Pirmame šio darbo skyriuje apibrėšiu pagrindines sąvokas ir teoremas, o antrame pristatysiu Merseno ir tobuluosius skaičius bei Lucas - Lehmer ir AKS pirminių skaičių testus.

1 skyrius

Pagrindinės sąvokos ir teoremos

1.1 Pagrindiniai apibrėžimai ir žymėjimai

1 apibrėžimas. *Pirminis skaičius* - tai natūralusis skaičius, didesnis už 1, neturintis jokių kitų daliklių, apart 1 ir savęs paties.

2 apibrėžimas. *Harmoninė eilutė* - eilutė, kurios forma yra $\sum_{k=1}^{\infty} \frac{1}{k}$.

3 apibrėžimas. *Eilutės konvergavimas* - eilutė konverguoja, jei egzistuoja toks l, kad bet kokiam $\epsilon > 0$, egzistuoja toks sveikasis skaičius N, kad kiekvienam $n \geqslant N$,

$$|S_n - l| < \epsilon.$$

4 apibrėžimas. *Didžiausias bendras daliklis* - tai didžiausias sveikasis skaičius, dalantis du arba daugiau skaičių be liekanos.

5 apibrėžimas. Tarkime, kad f yra aritmetinė funkcija. f vadinama *multiplikatyvia*, jei

$$f(mn) = f(m)f(n),$$

kur $(m, n) = 1$.

6 apibrėžimas. *Oilerio funkcija* skaičiuoja natūraliųjų skaičių m kiekį, kurie yra mažesni už $n \in \mathbb{N}$ ir su juo tarpusavyje pirminiai:

$$\phi(m) = \sum_{m \leqslant n, (m,n)=1} 1.$$

7 apibrėžimas. *Teiloro eilutė* realiasias arba kompleksines reikšmes įgyjančios funkcijos $f(x)$, kuri yra diferencijuojama begalę kartų kažkokiam skaičiui $a, a \in \mathbb{R}$, yra laipsninė eilutė

$$f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + ...,$$

kur $n!$ yra skaičiaus n faktorialas. Šią eilutę taip pat galima užrašyti kaip

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n,$$

kur $f^{(n)}(a)$ yra $n-oji$ funcijos f išvestinė taške a.

8 apibrėžimas. *Rymano zeta funkcija* apibrėžta kaip

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + ... = \sum_{k=1}^{\infty} \frac{1}{k^s}.$$

Funkcija yra baigtinė visoms $s \in \mathbb{R}$ reikšmėms, išskyrus $s = 1$.

9 teorema. ***Fundamentalioji aritmetikos teorema.*** *Kiekvienas sudėtinis skaičius gali būti vieninteliu būdu išskaidytas pirminiais dauginamaisiais.*

Įrodymas: Tarkime priešingai, kad egzistuoja toks sudėtinis skaičius, kurio negalima išskaidyti pirminiais dauginamaisiais. Pažymėkime mažiausią tokį skaičių n. Kadangi jis yra sudėtinis, tai jį galima užrašyti kaip dviejų skaičių sandauga: $n = a \cdot b$, kur $a, b, < n$. Gauname prieštarą pirminei prielaidai, kad n yra mažiausias skaičius, kurio negalima išskaidyti pirminiais dauginamaisiais, nes a ir b - galima taip išskaidyti, iš ko išplaukia, kad n irgi yra išreiškiamas pirminiais dauginamaisiais.

Dabar įrodysime, kad išskaidyti galima tik vieninteliu būdu. Pažymėkime $s \in \mathbb{N}, s > 1$ mažiausią skaičių, kuris gali būti išskaidytas dviem skirtingais būdais pirminiais dauginamaisiais: $s = p_1 \cdot p_2 \cdots p_m$ ir $s = q_1 \cdot q_2 \cdots q_n$. Tada, p_1 dalija arba q_1, arba $q_2 \cdot q_3 \cdots q_n$. Kadangi $q_1 < s$ ir $q_2 \cdot q_3 \cdots q_n < s$, tai kiekvieno jų faktorizacija yra unikali, nes, pagal prielaidą, s yra mažiausias skaičius, su keliomis faktorizacijomis. Iš to galime teigti, kad p_1 yra lygus kažkokiam q_j. Vis dėlto, išprastinę p_1 ir q_j, gausime skaičių, mažesnį už s ir gauname prieštarą.

10 lema. *Jei $p|m$ ir $p|n$, tai $p|(am + bn)$ kiekvienam $a, b, p \in \mathbb{Z}$. Be to, jei p dalija m ir p dalija n, tai p dalija kiekvieną tiesinę kombinaciją iš m ir n.*

Įrodymas: Pažymėkime $n = pc$ ir $m = pd$. Tada $p|(am + bn)$, kur a, b, c, d, n, m, $p \in \mathbb{Z}$:

$$am + bn = a \cdot pd + b \cdot pc = p(ad + bc).$$

Kadangi $(ad + bc) \in \mathbb{Z}$, tai $p|(am + bn)$. Kitos tiesinės kombinacijos įrodomos analogiškai.

1.2 Euklido teorema

Pirmasis žmogus, įrodęs, kad pirminių skaičių yra be galo daug, buvo graikų matematikas Euklidas (300 B.C.). Jo įrodymas prieštaros būdu iki šiol išlieka paprasčiausias ir plačiausiai naudojamas.

11 teorema. *[11] Pirminių skaičių yra daugiau, negu galima rasti bet kokiame užrašytame baigtiniame sąraše.*

Įrodymas: Tarkime, kad $p_1 = 2 < p_2 = 3 < \cdots < p_k$ kur p_k - visi egzistuojantys pirminiai skaičiai. Pažymėkime $n = p_1 \cdot p_2 \cdots p_k + 1$. Skaičius n negali būti pirminis, nes, pagal mūsų žymėjimą, jis yra didesnis, nei visų pirminių skaičių sandauga. Kadangi jau išsiaiškinome, kad n nėra pirminis skaičius, tai galime daryti išvadą, kad jis yra dalus iš kažkokio pirminio skaičiaus.Vis dėlto, tokiu atveju, tas pirminis skaičius, dalijantis n, negali būti nei vienas iš dauginamųjų p_k, nes tada jis turėtų dalyti ir $p_1 \cdot p_2 \cdots p_k + 1$, ir $p_1 \cdot p_2 \cdots p_k$, t.y. turėtų dalyti ir $n - p_1 \cdot p_2 \cdots p_k = 1$, tačiau joks pirminis skaičius nedalo 1. Taigi, iš to išplaukia, kad pirminių skaičių yra be galo daug.

1.3 Oilerio teorema

Oileris buvo XVIII a. Šveicarų matematikas ir fizikas. Jis, savo darbe *„Variae observationes circa series infinitas“* , išleistame 1744 metais, pateikia keletą atsakymų, į klausimą „Kiek iš viso yra pirminių skaičių?“ .

Nagrinėkime 7 teoremą iš *„Variae observationes circa series infinitas“* [5]:

12 teorema. *Sandauga, tęsiama iki begalybės trupmenoje*

$$\frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot \ldots}{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot \ldots},$$

kur skaitiklyje yra dauginami pirminiai skaičiai, o vardiklyje daugikliai yra vienetu mažesni nei skaitiklyje, yra lygi begalinės eilutės sumai

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \ldots$$

ir jos abi yra lygios begalybei.

Įrodymas: Pažymėkime

$$x = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \dots$$

Tada

$$\frac{1}{2}x = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \dots$$

Iš to gauname, kad

$$\frac{1}{2}x = 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots$$

Pastebime, kad neliko nei vieno lyginio skaičiaus dešinės lygybės pusės trupmenų vardikliuose. Dabar, norėdami pašalinti skaičiaus 3 kartotinius vardikliuose, abi lygybės puses padalijame iš 3 ir gauname

$$\frac{1}{2} \cdot \frac{1}{3}x = \frac{1}{3} + \frac{1}{9} + \frac{1}{15} + \frac{1}{21} + \dots$$

Atimdami dar kartą, pašaliname likusias trupmenas, kurių vardikliai dalijasi iš 3:

$$\frac{1}{2} \cdot \frac{2}{3}x = 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \dots$$

Dar kartelį pakartoję tą patį procesą, pašaliname likusias trupmenas, kurių vardikliai yra 5 kartotiniai:

$$\frac{1 \cdot 2}{2 \cdot 3} \cdot \frac{1}{5}x = \frac{1}{5} + \frac{1}{25} + \frac{1}{35} + \dots$$

ir atėmus lieka

$$\frac{1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5}x = 1 + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \dots$$

Kartojant šį procesą, kiekvieną kartą pašaliname trupmenas su pirminiu skaičiumi vardiklyje bei visus to skaičiaus kartotinius. Galiausiai viskas dešinėje lygybės pusėje bus panaikinta, išskyrus 1:

$$\frac{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 11 \cdot \dots}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 21 \cdot \dots}x = 1.$$

Kadangi x pasižymėjome kaip harmoninės eilutės sumą, tai galime teigti, jog jos riba yra lygi ∞, o kad lygybė būtų teisinga, riba trupmenos

$$\frac{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12 \cdot 16 \cdot 18 \cdot 11 \cdot \dots}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 21 \cdot \dots}$$

turi būti $\frac{1}{\infty}$, o tai pasiekiame, tik kai yra begalinis skaičius pirminių skaičių.

1.4 Hermito teorema

XIX a. Prancūzų matematikas taip pat įrodinėjo pirminių skaičių begalybę. Jis teigė, jog bet kokiam teigiamam sveikajam skaičiui, įmanoma rasti už jį didesnį pirminį skaičių.

13 teorema. *[9]Tegul $n > 1, n \in \mathbb{Z}$ ir p yra skaičiaus $n! + 1$ pirminis daliklis. Tada $p > n$, iš ko išplaukia, kad pirminių skaičių yra be galo daug.*

Įrodymas: Jei $p \leqslant n$, tada p dalija $n!$. Be to, pagal pirminius duomenis turime, kad p taip pat dalija ir $n! + 1$. Galime teigti, kad p dalija ir $n! + 1 - n!$. Gauname, kad p dalija 1, o tai negali būti tiesa. Taigi, $p > n$.

1.5 Goldbacho teorema

Maždaug 2000 metų po Euklido įrodymo, kad pirminių skaičių yra be galo daug, vokiečių matematikas Kristianas Goldbachas pateikė kitokį šio teiginio įrodymą, naudojant Ferma skaičius. Iš pradžių apibrėžkime, kas tai yra ir įrodykime keletą jų savybių, naudojamų Goldbacho teoremos įrodyme. Remsimės [6].

14 apibrėžimas. *Ferma skaičius* - teigiamas sveikasis skaičius, kurio forma yra

$$F_n = 2^{2^n} + 1,$$

kur $n \in \mathbb{N}$.

15 lema. *Jei n nėra neigiamas sveikasis skaičius, tai $F_{n+1} - 2 = F_n F_{n-1} \cdots F_1 F_0$.*

Įrodymas: Įrodysime naudodami matematinę indukciją. Pažymėkime $P(n)$:

$$F_{n+1} - 2 = F_n F_{n-1} \cdots F_1 F_0,$$

kiekvienam $n \in \mathbb{N}$.

Iš pradžių parodysime, kad $P(0)$ yra tiesa:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3.$$

Be to,

$$F_{0+1} - 2 = (2^{2^1} + 1) - 2 = 5 - 2 = 3.$$

Taigi, $F_{0+1} - 2 = F_0$, todėl $P(0)$ yra tiesa.

Tarkime, kad $P(k)$, tai yra $F_{k+1}-2 = F_kF_{k-1}\cdots F_1F_0$ taip pat yra teisinga, kur $k \in \mathbb{N}$.

Įrodysime, kad $P(k+1)$, tai yra $F_{(k+1)+1}-2 = F_{k+1}F_kF_{k-1}\cdots F_1F_0$ taip pat yra teisinga. Tada:

$$\begin{aligned}
F_{k+1}(F_kF_{k-1}\cdots F_1F_0) &= F_{k+1}(F_{k+1}-2)\\
&= (2^{2^{k+1}}+1)(2^{2^{k+1}}+1-2)\\
&= (2^{2^{k+1}}+1)(2^{2^{k+1}}-1)\\
&= (2^{2^{k+1}})^2-1 = 2^2(2^{k+1})-1\\
&= 2^{2^{k+2}}-1\\
&= (2^{2^{k+2}}+1)-2\\
&= F_{k+2}-2\\
&= F_{(k+1)+1}-2.
\end{aligned}$$

Taigi, $P(k+1)$ irgi yra teisinga. Kadangi $P(1)$, $P(k)$ ir $P(k+1)$ yra tiesa, kai $k \in \mathbb{N}$, tai, pagal matematinę indukciją, $P(n)$ irgi yra tiesa, kai $n \in \mathbb{N}$. Įrodėme, kad $F_{n+1}-2 = F_nF_{n-1}\cdots F_1F_0$.

16 lema. *Jei $n \in \mathbb{N}$, tai $dbd(F_{n+1}, F_nF_{n-1}\cdots F_1F_0) = 1$.*

Įrodymas: Pažymėkime $d = dbd(F_{n+1}, F_nF_{n-1}\cdots F_1F_0), n \in \mathbb{N}$. Akivaizdu, kad $d > 0$. Įrodysime, kad $d = 1$. Pagal didžiausio bendro daliklio apibrėžimą, $d|F_{n+1}$ ir $d|(F_nF_{n-1}\cdots F_1F_0)$. Galime teigti, kad $F_{n+1}-2 = F_nF_{n-1}\cdots F_1F_0$. Taigi, gauname, kad $d|(F_{n+1}-2)$. Be to, d dalija visas tiesines kombinacijas skaičių F_{n+1} ir $F_{n+1}-2$. Tai yra, $d|(F_{n+1}-(F_{n+1}-2))$, iš ko išplaukia, kad $d|2$. Taigi, $d = 1$ arba $d = 2$. Kadangi Ferma skaičiai yra nelyginiai, $2 \nmid F_{n+1}$ ir $2 \nmid F_nF_{n-1}\cdots F_1F_0$, kiekvienam n. Taigi, $d \neq 2 \Rightarrow d = 1$. Įrodėme, kad Jei $n \in \mathbb{N}$, tai $dbd(F_{n+1}, F_nF_{n-1}\cdots F_1F_0) = 1$.

17 teorema. *Pirminių skaičių yra be galo daug.*

Įrodymas: Pažymėkime $F_n = 2^{2n}+1$ kiekvienam $n \in \mathbb{N}$. Taip pat yra žinoma, kad Ferma skaičių yra be galo daug. Žinome, kad $dbd(F_{n+1}, F_nF_{n-1}\cdots F_1F_0) = 1$, taigi, F_{n+1} ir $F_nF_{n-1}\cdots F_1F_0$ yra tarpusavyje pirminiai, t.y. juos išskaidžius pirminiais dauginamaisiais, jie neturės jokio bendro dauginamojo. Vadinasi, $dbd(F_i, F_j) = 1$, kai $i \neq j$. Pagal Fundamentaliąją aritmetikos teoremą, kiekvienas F_n turi pirminį daugiklį p_n. Be to, kadangi $dbd(F_i, F_j) = 1, i \neq j$, tai $p_n \nmid F_j, j \neq n$. Kadangi tai

galioja kiekvienam n ir Ferma skaičių yra be galo daug, mes darome išvadą, kad kiekvienas Ferma skaičius sugeneruos naują pirminį skaičių $\Rightarrow$ pirminių skaičių yra be galo daug.

1.6 Dirichlė teorema

Kitas vokiečių matematikas, nagrinėjęs skaičių teoriją ir pirminius skaičius XIX a. yra Petras Dirichlė.

18 apibrėžimas. *Dirichlė charakteris* χ - tai funkcija nuo $\mathbb{N}$ iki $\mathbb{C}$, kuriai galioja sąlygos:

- Egzistuoja toks teigiamas sveikasis skaičius k, kad $\chi(n) = \chi(n+k)$, kiekvienam n.
- Jei $dbd(n,k) > 1$, tai $\chi(n) = 0$.
- Jei $dbd(n,k) = 1$, tai $\chi(n) \neq 0$.
- $\chi(mn) = \chi(m)\chi(n)$, kiekvienam $m, n \in \mathbb{Z}$.

Jei χ yra pagrindinis charakteris $\chi_0 \mod k$, tai, iškėlę Rymano zeta funkciją, gauname:

$$L(s, \chi_0) = \zeta(s) \prod_{p|k} (1 - p^{-s}).$$

19 apibrėžimas. *Oilerio funkcija* - jei f yra multiplikatyvi, tai

$$D_f(s) = \prod_p (1 + \sum_{n=1}^{\infty} f(p^n) p^{-ns},$$

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}.$$

20 apibrėžimas. Jei χ yra multiplikatyvi, tai *Dirichlė L - funkciją* galima išreikšti per Oilerio funkciją:

$$L(s, \chi) = \prod_p (1 - \chi(p) p^{-s} - 1.$$

21 teorema. *[14]Egzistuoja begalinis skaičius pirminių skaičių* $p \equiv l \mod k$*, kur* l *ir* k *yra tarpusavyje pirminiai.*

Įrodymas: Paprastumo dėlei pažymėkime ${P_k}^l$ aibę pirminių skaičių, kuriems galioja lygybė $p \equiv l \mod k$. Įrodysime, kad aibė ${P_k}^l$ yra begalinė, o l ir k - tarpusavyje pirminiai.

Iš pradžių išsireiškiame Dirichlė L - funkciją per Oilerio funkciją:

$$L(s,\chi) = \prod_p (1-\chi(p)p^{-s})^{-1}.$$

Naudodami Teiloro eilutę funkcijai $\log \frac{1}{1-t}$, gauname

$$\log \frac{1}{1-\chi(p)p^{-s}} = \chi(p)p^{-s} + O((\chi(p)p^{-s})^2).$$

Logaritmuojant abi lygybės puses gauname

$$\log L(s,\chi) = \sum_p \chi(p)p^{-s} + \sum_p (\chi(p)p^{-s})^2.$$

Pastebime, kad $\sum_p (\chi(p)p^{-s})^2 = \sum_p \chi(p)^2 p^{-2s}$ konverguoja. Iš to išplaukia, kad

$$\log L(s,\chi) = \sum_p \chi(p)p^{-s} + O(1).$$

Žinome, kad $\chi \in \mathbb{S}^1$, kur $\chi(n)^{-1} = \overline{\chi(n)}$ (jei $z \in \mathbb{S}^1$, tai $z\overline{z} = 1$). Tada $\sum_{\chi \mod k} \overline{\chi}(l)\chi(p)$ neišnyksta tada ir tik tada, kai $p \in \mathbb{P}_k^l$.

$$\begin{gathered}
\varphi(k)^{-1} \textstyle\sum_{\chi \mod k} \overline{\chi}(l) \log L(s,\chi) = \\
= \varphi(k)^{-1} \textstyle\sum_{\chi \mod k} \overline{\chi}(l)(\sum_p \chi(p)p^{-s} + O(1)) = \\
= \varphi(k)^{-1} \textstyle\sum_{\chi \mod k} \overline{\chi}(l) \sum_p \chi(p)p^{-s} + \varphi(k)^{-1} \sum_{\chi \mod k} \overline{\chi}(l)O(1) = \\
= \textstyle\sum_{p \in \mathbb{P}_k^l} p^{-s} + O(1).
\end{gathered}$$

Jei χ yra pagrindinis charakteris χ_0, tai iš L-funkcijos iškeliame Rymano zeta funkciją:

$$L(s,\chi_0) = \zeta(s) \prod_{p|k} (1-p^{-s}),$$

kur

$$\zeta(s) = \sum_1^\infty n^{-s} = \int_1^\infty t^{-s}\,dt + O(1) = (s-1)^{-1} + O(1).$$

Iš to gauname:

$$\begin{gathered}
\varphi(k)^{-1}\overline{\chi_0}(l) \log L(s,\chi_0) = \varphi(k)^{-1} \log L(s,\chi) = \\
= \varphi(k)^{-1} \log(s-1)^{-1} + O(1).
\end{gathered}$$

Dabar telieka įrodyti, kad likusi sumos dalis yra apibrėžta, t.y. baigtinė, kad įrodytume, jog eilutė $\sum_{p \in \mathbb{P}_k^l} p^{-s}$ diverguoja, kai $s \to 1^+$.

Žinome, kad $\lim_{s\to 1^+} L(s,\chi)$ egzistuoja ir nenyksta. Taigi, $\lim_{s\to 1^+} \log L(s,\chi)$ yra baigtinis ne pagrindiniams charakteriams, t.y. kai $s \to 1^+$,

$$\sum_{p\in\mathbb{P}_k^l} p^{-s} = \varphi(k)^{-1}\log(s-1)^{-1} + O(1).$$

Eilutė $\sum_{p\in\mathbb{P}_k^l} p^{-s}$ diverguoja, kai $s \to 1^+$. Iš to išplaukia, kad egzistuoja be galo daug pirminių skaičių, kurių forma yra $p \equiv l \mod k$.

2 skyrius

Merseno skaičiai bei pirminių skaičių testavimo algoritmai

2.1 Merseno skaičiai

22 apibrėžimas. *Merseno skaičius* - toks pirminis skaičius, kurio forma $2^p - 1$, kai p - pirminis skaičius.

Iki 1536 buvo manoma, kad formulė $2^p - 1$ generavo vien pirminius skaičius, tačiau H. Regius pastebėjo, kad $2^{11} - 1 = 2047 = 23 \cdot 89$ - sudėtinis skaičius. Po to daugelis garsių matematikų, tokių kaip Pietro Cataldi, Pierre Fermat ir Leonhard Euler aiškinosi, kokie pirminiai skaičiai generuoja Merseno skaičių. Prancūzų matematikas Marin Mersenne savo knygos *„Cogitata Physica-Mathematica“* (1644) įvade teigė, jog skaičiai $2^p - 1$ yra pirminiai, kai

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257,$$

o visi kiti teigiami skaičiai $p < 257$, yra sudėtiniai.

Buvo akivaizdu, kad Marin Mersenne visų skaičių patikrinti negalėjo, tačiau niekas negalėjo įrodyti, kad daugiau tokių skaičių nėra intervale $[2; 257)$, ar kad įvardyti yra teisingi, todėl skaičius ir buvo pavadintas šio matematiko vardu. Tik po daugiau nei 100 metų Leonhard Euler patvirtino, kad kai $p = 31$, skaičius $2^{31} - 1$ tikrai yra pirminis. Dar po 126 metų prancūzų matematikas Eduoard Lucas patvirtino, kad $2^{127} - 1$ taip pat yra pirminis skaičius, o po dar 7 metų rusų matematikas Ivan Pervušin atrado, jog skaičius $2^{61} - 1$ taip pat yra pirminis, nors Marin Mersenne

jį savo sąraše praleido. 1900 metais Powers atrado, jog į sąrašą taip pat neįtraukti pirminiai skaičiai $2^{89}-1$ ir $2^{107}-1$. Galiausiai, 1947 sąrašas buvo patikrintas ir pataisytas intervalui $[2;258]$:

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

Šiuo metu didžiausias žinomas Merseno skaičius yra $2^{82589933}-1$ [3].

2.2 Tobulieji skaičiai

23 apibrėžimas. Sveikasis skaičius $n > 1$ yra vadinamas *tobuluoju*, jei jis yra lygus jo daliklių sumai (neįskaitant daliklio n).

Pavyzdžiui:

$$6 = 2 \cdot 3 = 1 + 2 + 3,$$

$$28 = 2^2 \cdot 7 = 1 + 2 + 4 + 7 + 14, ...$$

Be to, tarp tobulųjų ir Merseno skaičių egzistuoja sąsaja:

Pavyzdžiui:

$$6 = 2 \cdot (2^2 - 1),$$

$$28 = 2^2 \cdot (2^3 - 1),$$

$$496 = 2^4 \cdot (2^5 - 1), ...$$

Pastebime, kad $2^2-1, 2^3-1, 2^5-1$ yra Merseno skaičiai.

24 apibrėžimas. Kiekvienam sveikajam skaičiui $n > 0$, žymėsime $\sigma(n) =$ suma teigiamų skaičiaus n daliklių ir $\sigma(p^k) = \frac{p^{k+1}-1}{p-1}$

25 teorema. *[8]Jei $2^p - 1$ yra Merseno skaičius, tai $2^{p-1} \cdot (2^p - 1)$ yra tobulasis skaičius.*

Įrodymas:

Imkime p - tokį pirminį skaičių, kad $q = 2^p - 1$ taipogi yra pirminis bei $2^{p-1}(2^p - 1) = 2^{p-1}q$.Tada skaičiaus 2^{p-1} dalikliai yra $1, 2, 4, 8, 16, \ldots, 2^{p-1}$, o kiti skaičiaus $2^{p-1}q$ dalikliai yra $q, 2q, 4q, 8q, 16q, \ldots, 2^{p-2}q$. Iš pradžių sudedame 2^{p-1} daliklius:

$$1 + 2 + 4 + 8 + 6 + \cdots + 2^{p-1} = \frac{2^p - 1}{2 - 1} = 2^p - 1 = q.$$

Tada sudedame kitus $2^{p-1}q$ daliklius:

$$q + 2q + 4q + \cdots + 2^{p-2}q = q(2^0 + 2^1 + 2^2 + \cdots + 2^{p-2} = q\frac{2^{p-1} - 1}{2 - 1} = q(2^{p-1} - 1).$$

Visus $2^{p-1}q$ daliklius randame sudedant abiejų, t.y. 2^{p-1} ir kitus $2^{p-1}q$ daliklius:

$$1 + 2 + 4 + 8 + 16 + \cdots + 2^{p-1} + q + 2q + 4q + 8q + 16q + \cdots + 2^{p-2}q =$$
$$= q + q(2^{p-1} - 1) = q + q(2^{p-1}) - q = 2^{p-1}q = 2^{p-1}(2^p - 1).$$

Taigi, gavome, kad jeigu $q = 2^p - 1$ yra pirminis skaičius, tai $2^{p-1}(2^p - 1)$ yra tobulasis skaičius.

2.3 Lucas - Lehmer pirminių skaičių testas

Šis testas buvo sukurtas Lucas'o ir supaprastintas Lehmerio. Testo įrodymą savo straipsnyje pateikė J. W. Bruce [2].

Iš pradžių apibrėšime seką S_n, kur $S_1 = 4$, $S_n = S_{n-1}^2 - 2$.

26 teorema. *Pažymėkime p - pirminis skaičius. Tada $M_p = 2^p - 1$ yra pirminis tada, jei M_p dalija S_{p-1}.*

Tolimesniam įrodymui apibrėžiame $\omega = 2 + \sqrt{3}, \overline{\omega} = 2 - \sqrt{3}$. Be to, $\omega\overline{\omega} = 1$. Taigi, pagal indukciją išplaukia, kad $S_m = \omega^{2^{m-1}} + \overline{\omega}^{2^{m-1}}$.

Jeigu M_p dalija S_{p-1}, tai $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} \equiv 0 \mod M_p$.

Pažymėkime $\omega^{2^{p-2}} + \overline{\omega}^{2^{p-2}} = RM_p, R \in \mathbb{Z}$. Padauginame šią lygybę iš $\omega^{2^{p-2}}$:

$$\omega^{2^{p-1}} = RM_p\omega^{2^{p-2}} - 1,$$

pakeliame abi puses kvadratu

$$\omega^{2^p} = (RM_p\omega^{2^{p-2}} - 1)^2.$$

Tarkime, kad M_p - sudėtinis skaičius, q - pirminis daliklis, $q^2 \leqslant M_p$. Tolimesniam įrodymui reikalinga keletas lemų:

27 lema. *Pažymėkime X - aibe dvinarių operacijų, kurios yra asociatyvios ir turi tapatumą. Tada aibė X^* iš atvirkštinių aibės X elementų suformuoja grupę.*

Įrodymas: X^* yra ne tuščia aibė, nes $1 \in X^*$. Telieka parodyti, kad aibė X^* yra uždara dvinariose operacijose. Jei x_1 ir x_2 turi atvirkštinę formą x_1^{-1} ir x_2^{-1}, tai x_1x_2 turi atvirkštinę formą $x_2^{-1}x_1^{-1}$.

28 lema. *Jei G - baigtinė grupė, tai elemento eilė yra ne didesnė nei grupės eilė. Jei $x \in G$ ir $x^r = 1$, tai x eilė dalija r.*

Tęsiame teoremos įrodymą: Pažymėkime Z_q aibe sveikųjų skaičių moduliu q. Be to, apibrėžkime aibę $X := \{a + b\sqrt{3} : a, b, \in Z_q\}$. Aibėje X galime apibrėžti dvi dvinares operacijas: sudėtį ir daugybą. Daugybos atveju, pasirenkame elementus iš $Z[\sqrt{3}]$ ir atliekame aibėje X veiksmus $(a_1 + b_1\sqrt{3})(a_2 + b_2\sqrt{3})$ kaip $(a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3}$ ir sumažinam koeficientus moduliu q. Sudėties atveju gauname Abelio (komutatyvią) grupę, o daugybos atveju gauname asociatyvią dvinarę operaciją su tapatumu lygiu 1. Pažymėkime X^* - atvirkštinių aibės X elementų aibę, atsižvelgiant į daugybą. Gauname, kad X^* yra grupė, o bet kokio aibės X^* elemento eilė yra ne didesnė už $q^2 - 1$, nes X^* aibėje yra bent vienas elementas, kuris neturi atvirkštinės formos, pavyzdžiui 0.

Tarkime, kad $\omega = 2+\sqrt{3}$ priklauso aibei X. Kadangi q dalija M_p, tai $RM_p\omega^{2^{p-2}} = 0$, kai yra aibės X elementas. Taigi,

$$\omega^{2^{p-1}} = RM_p\omega^{2^{p-2}} - 1 = -1$$

ir

$$\omega^{2^p} = (RM_p\omega^{2^{p-2}} - 1)^2 = 1$$

aibėje X. Iš to išplaukia, kad ω priklauso aibei X^* ir jos eilė yra 2^p. ω eilė dalija 2^p, tačiau ji negali būti mažesnė nei 2^p . Taigi, $2^p \leqslant q^2 - 1$. Kadangi $q^2 - 1 \leqslant M_p - 1 = 2^p - 2$, gauname prieštarą.

Šį testą „Python“ programavimo kalboje galima užrašyti taip:

```
import math

# function to generate lucas lehmer series
def lucas_lehmer_series(p):
    ll_seq = [4]
    if p>2:
        for i in range(1, (p-2)+1):
            n_i = ((ll_seq[i-1]) ** 2 - 2) % ((2 ** p) - 1)
            ll_seq.append(n_i)
    return ll_seq

# function to find whether number 'p' is prime or not
def is_prime(number):
    if number <= 1 or (number > 2 and number % 2 == 0):
        return False

    for factor in range(2, int(math.sqrt(number))+1):
        if number%factor == 0:
            return False
    return True

# primality test of mersenne number using above generated series
def ll_prime(p):
    if lucas_lehmer_series(p)[-1] == 0:
        return True
    return False
```

2.1 pav.: Lucas - Lehmer testas [12]

2.4 AKS pirminių skaičių testas

AKS pirminių skaičių testas, kurį sukūrė ir aprašė Manindra Agrawal, Neeraj Kayal ir Nitin Saxena savo straipsnyje „PRIMES is in P“ [1] 2002 metais. Jų algoritmas buvo pirmasis, kuris gali nustatyti, ar skaičius yra pirminis, ar sudėtinis, nesiremdamas matematiniais spėjimais, tokiais kaip Rymano hipotezė.

Kaip teigia pačios autorės, jų testas remiasi generalizuota Mažąja Ferma teorema.

29 teorema. ***Mažoji Ferma Teorema*** *[4]. Tarkime, kad p - pirminis skaičius, kuris nedalija sveikojo skaičiaus a. Tada*

$$a^{p-1} \equiv 1 \mod (p)$$

Įrodymas: Iš pradžių išrašome $(p-1)$ teigiamų daugiklių skaičiaus a:

$$a, 2a, 3a, \ldots, (p-1)a.$$

Tarkime, kad ra ir sa yra lygūs moduliu p, todėl juos galime užrašyti kaip $r = s \mod (p)$. Taigi, visi $(p-1)$ daugikliai skaičiaus a yra skirtingi ir nelygūs nuliui. Tai reiškia, kad jie turi atitikti $1, 2, 3, \ldots (p-1)$ kuria nors tvarka. Sudauginame tuos atitikmenis ir gauname

$$a(2a)(3a)\ldots((p-1)a) \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \mod (p)$$

ir tai yra lygu

$$a^{p-1}(p-1)! \equiv (p-1)! \mod (p).$$

Padalijame abi puses iš $(p-1)!$ ir gauname:

$$a^{p-1} \equiv 1 \mod (p).$$

30 lema. *[1]Tegul $a \in \mathbb{Z}, n \in \mathbb{N}, n \geqslant 2, (a,n) = 1$. Skaičius n yra pirminis tada ir tik tada, kai*

$$(X+a)^n = X^n + a \mod (n)$$

Įrodymas: Kiekvienam $0 < i < n$ skaičiaus x^i koeficientas polinome $((X+a)^n - (X^n + a))$ yra lygus $\binom{n}{i}a^{n-i}$.

Tarkime, kad n - pirminis skaičius. Tada $\binom{n}{i}a^{n-i} = 0 \mod n$, iš ko išplaukia, kad visi koeficientai yra lygūs nuliui.

Tarkime, kad n - sudėtinis. Pasižymėkime q - pirminį skaičiaus n daugiklį ir tarkime, kad $g^k || n$ (q^k dalija n, tačiau pakėlus q kitu laipsniu - nedalija). Tada q^k nedalija $\binom{n}{q}$ ir yra tarpusavyje pirminis su a^{n-q} iš ko išplaukia, kad X^q koeficientas nėra lygus nuliui $\mod n$. Taigi, $((X+a)^n - (X^n + a))$ nėra lygus nuliui virš $\mathbb{Z}_n$, čia $\mathbb{Z}_n$ žymi skaičių moduliu n žiedą.

Remiantis šia lema, sukurtas testas patikrinti, ar skaičius yra pirminis: įvedant skaičių n ir pasirenkant a, tikrinama, ar lygybė $(X+a)^n = X^n + a \mod (n)$ yra teisinga. Vis dėlto, tai užtrunka, nes reikia apskačiuoti n koeficientų vien kairėje pusėje. Jų skaičiui sumažinti, reiktų abi lygybės puses apskaičiuoti moduliu polinomo $X^r - 1$ kokiam nors pakankamai mažam r, t.y. patikrinti, ar teisinga lygybė

$$(X+a)^n = X^n + a \mod (X^r - 1, n).$$

Akivaizdu, kad su visais pirminiais skaičiais n ir visomis a ir r reikšmėmis lygybė galioja, tačiau ji galioja net ir su kai kuriais sudėtiniais skaičiais n ir tinkamomis a ir r reikšmėmis. Vis dėlto, parodžius, kad jei tinkamai pasirinkus reikšmę r lygybė $(X+a)^n = X^n + a \mod (X^r - 1, n)$ yra teisinga keletoms a reikšmių, tai n turi būti pirminis skaičius pakeltas laipsniu. Skaičius a ir tinkamas r yra ribojami polinomo $\log(n)$ iš ko išplaukia, kad gaunamas deterministinis polinominis laiko algoritmas pirminių skaičių testavimui.

Input: integer $n > 1$.
1. If $(n = a^b$ for $a \in \mathcal{N}$ and $b > 1)$, output COMPOSITE.
2. Find the smallest r such that $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leq r$, output COMPOSITE.
4. If $n \leq r$, output PRIME.[1]
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$, output COMPOSITE;
6. Output PRIME.

2.2 pav.: Pirminių skaičių testavimo algoritmas

Čia $\phi(r)$ - Oilerio funkcija.

2.5 Išvados

Taigi, kaip matome iš aprašyto darbo, pirminiai skaičiai dar nėra visiškai ištyrinėti, nors pirmieji įrašai apie juos ir yra 300 metų prieš Kristų. Skirtinguose amžiuose yra padaryti skirtingi atradimai apie šiuos skaičius, o, pavyzdžiui, viskas, ką mes dabar žinome apie Merseno skaičius, yra ne vieno ir net ne tame pačiame šimtmetyje gyenusio matematiko tyrinėjimo rezultatas, kaip ir teiginys, kad pirminių skaičių yra be galo daug. Šiame darbe pateikiau keletą visiškai skirtingų to paties teiginio įrodymų, tad turbūt nelieka abejonės, kad pirminių skaičių tikrai neįmanoma visų išrašyti. Vis dėlto, yra sukurtas ne vienas algoritmas, tikrinantis, ar skaičius yra pirminis ar ne.

Literatūra

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, *Department of Computer Science Engineering, Indian Institute of Technology Kanpur, Kanpur-208016, INDIA,* 2004, 783 - 784.

[2] J. W. Bruce, A Really Trivial Proof of the Lucas - Lehmer Test, *The American Mathematical Monthly, Vol. 100, No. 4* 1993, 370 - 371.

[3] C.K. Caldwell, Mersenne Primes: History, Theorems and Lists, 2021, <https://primes.utm.edu/mersenne/>

[4] C.K. Caldwell, Proof of Fermat's Little Theorem, 2021, <https://primes.utm.edu/notes/proofs/FermatsLittleTheorem.html>

[5] L. Euler, Variae observationes circa series infinitas, 172-174, 1744.

[6] L. Harrison, From Euclid to Present: A Collection of Proofs regarding the Infinitude of Primes, 4-7, 2013.

[7] B. Ikenaga, Divisor Functions, 2019, <https://sites.millersville.edu/bikenaga/number-theory/divisor-functions/divisor-functions.html>

[8] A. Garcia, On Perfect Numbers, *Saint Mary's College of California, Department of Mathematics and Computer Science,* 2016, 3-4.

[9] K. McNulty, Six Proofs that there are Infinitely Many Primes, 2020, <https://www.cantorsparadise.com/six-proofs-that-there-are-infinitely-many-primes-33037bc2c54e>

[10] V. Shoup, A Computational Introduction to Number Theory and Algebra, *Cambridge University Press*, 2009, 24-25.

[11] R. Meštrović, Euclid's theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.-2017), 1, 3-5, 2018.

[12] H. Sharma, Mersenne Primes using Lucas Lehmer Primality Test in Python, 2019, <https://medium.com/@cehimanshusharma94/mersenne-primes-using-lucas-lehmer-primality-test-in-python-80b2ca792911>

[13] J.B. Snell, Multiplicative and additive arithmetic functions and formal power series, *University of Texas at El Paso,* 2021, 6.

[14] Z. Wang, Elementary Proof of Dirichlet Theorem, 2-13.