III. SVEIKI NENEIGIAMI SKAIČIAI

3.1 Indukcijos aksioma

Natūraliųjų skaičių aibės sąvoka viena svarbiausių matematikoje. Nors natūralaus skaičiaus sąvoka labai sena, bet šio skaičiaus 'buveinės' sąvoka buvo suformuluota tik 19 am. pabaigoje G. Peano bei R. Dedekindo pastangomis.

Paruošiamuosius darbus jau esame atlikę ankstesniuose skyreliuose, todėl dabar iš karto ir pateiksime natūraliųjų skaičių aibės apibrėžimą.

Netuščią aibę $\mathcal{N}$ vadinsime natūraliųjų skaičių aibe, jeigu joje apibrėžtas binarinis sąryšis 'eina tiesiog po' siejantis kai kuriuos šios aibės elementus, tenkinantis savybes:

a1. Yra šioje aibėje elementas, pažymėkime jį '1', neinantis po jokio elemento;

a2. Po kiekvieno elemento eina vienas ir tik vienas elementas;

a3. Kiekvienas elementas eina ne daugiau kaip po vieno elemento;

a4. Bet kuris aibės $\mathcal{N}$ poaibis M, sutampa su aibe $\mathcal{N}$, jei:

1) $1 \in M$,

2) jei elementas $m \in M$, tai ir elementas einantis tiesiog po jo priklauso aibei M.

Šios aibės elementus vadinsime natūraliaisiais skaičiais. Naudojant šias aksiomas galime 'surėdyti', visus natūraliuosius skaičius tam tikra tvarka. Einantį tiesiog po 1 pažymėsime 2, einantį tiesiog po 2 pažymėsime 3 ir t. t., mums įprastu būdu. Pastebėsime, kad natūraliuosius skaičius galime žymėti labai įvairiai. Kiek vėliau susipažinsime ir su kitokiais skaičių užrašymo būdais. Tokiu būdu mes gauname natūraliųjų skaičių aibę nusakančius elementus. Dar daugiau, kadangi šioje aibėje apibrėžtas tvarkos sąryšis, tai šios aibės elementus galime sutvarkyti šio sąryšio atžvilgiu.

Pagindžiant matematinius teiginius labai svarbi a4. aksioma, kuri dar vadinama matematinės indukcijos aksioma. Kuo matematinė indukcija skiriasi nuo 'kitokios' indukcijos. Apskritai kalbant, indukcija yra metodas, leidžiantis remiantis daliniais teiginiais daryti išvadas apie bendrus teiginius. Bet 'sveikas protas ' sako mums, kad kažin ar atlikus tik baigtinį kokio tai proceso tikrinimą galime neabejodami tvirtinti, kad ir neribotai tęsdami šį procesą gausime tą patį rezultatą? Dar daugiau, mokslo istorijoje daug pavyzdžių, kurie patvirtina, kad ne visada galime apibendrinti rezultatus remdamiesi tik baigtine indukcija. Pvz. P. Ferma patikrinęs, jog skaičius $2^{2^n}+1$ yra pirminis, kai $n = 0, 1, 2, 3, 4$, padarė prielaidą, kad šis skaičius kai $n = 5$ taip pat pirminis. Bet jo prielaida nepasitvirtino. Žinoma, pilnosios indukcijos metodu yra gaunamos patikimos žinios, tačiau ji įmanoma tik tuo atveju, kai nagrinėjama aibė baigtinė. Tad kyla klausimas, o kuo gi geresnis matematinės indukcijos metodas? Tarkime, kad mums reikia patikrinti, jog tam tikras reiškinys teisingas begaliniam skaičiavimo, vertinimo ir t.t. žingsnių skaičiui. Jeigu parodysime, kad šis žingsnių skaičius sutampa su natūraliųjų skaičių aibe, tai mūsų teiginys bus įrodytas. Tad kaip mes elgiamės. Visų pirma sutapatinkime mūsų nagrinėjamo proceso žingsnių skaičiaus aibę su aibe M, kuri figūravo a4. aksiomoje. Visų pirma reikia patikrinti, ar pirmąjam žingsniui nagrinėjamas reiškinys tenkina keliamus reikalavimus, t.y. $1 \in M$. Tarkime, kad pradinis reikalavimas yra patenkintas, t.y $1 \in M$. Taigi, aibė M netuščia. Pasirinkime, bet kurį žingsnį $k \in M$ kuriam nagrinėjamas reiškinys tenkina reikalavimus (darome indukcinę prielaidą). Jei parodysime, kad tuos pat reikalavimus reiškinys tenkina ir sekančiame žingsnyje (po k tiesiog einantis elementas irgi priklauso

aibei M), taigi naudodamiesi a4. aksioma galime tvirtinti, kad žingsnių skaičius, kuriems nagrinėjamas reiškinys tenkina keliamus reikalavimus, sutampa su natūraliųjų skaičių aibe.

3.2* Sveikų, neneigiamų skaičių aibės elementų veiksmai

Šiame skyrelyje parodysime, kaip naudojant indukcijos aksiomą yra apibrėžiami veiksmai natūraliųjų skaičių aibėje, įrodomos veiksmų savybės bei apibrėžiamas tvarkos sąryšis.

Tegu $a \in \mathcal{N}$. Tada elementą einantį tiesiog po a žymėsime simboliu a'. Iš natūraliųjų skaičių aibės aksiomų išplaukia, kad jei $a' = b'$, tai tada ir $a = b$. Be to, jei $a \neq b$, tai ir $a' \neq b'$.

Papildykime natūraliųjų skaičių aibę vienu elementu. Pažymėkime

$$\mathcal{N}_0 = \{0\} \cup \mathcal{N} = \{0, 1, 2, \ldots\}.$$

Aibė $\mathcal{N}_0$ nuo natūraliųjų skaičių aibės skiriasi tik tuo, kad elementas, neinantis po jokio yra 0. Be to $0' = 1$. Šios aibės elementus vadinsime sveikais neneigiamais skaičiais.

Funkciją $f : \mathcal{N}_0 \times \mathcal{N}_0 \to \mathcal{N}$ *vadinsime sudėties operacija, apibrėžta natūraliųjų skaičių aibėje, jei* $\forall (a, b) \in \mathcal{N}_0^2$ *funkcija tenkina reikalavimus:*

1) $$f(a, 0) = a,$$

2) $$f(a, b') = (f(a, b))'.$$

Ateityje žymėsime: $f(a, b) = a + b$. Tuomet apibrėžime naudojamas lygybes galime perrašyti taip:

$$a + 0 = a, \text{ ir } \; a + b' = (a + b)'.$$

Natūralųjį skaičių $f(a, b)$ vadinsime skaičių a ir b suma, skaičiai a ir b vadinami dėmenimis.

1 Teorema $\forall a \in \mathcal{N}$ teisingas lygybė

$$a + 1 = a'.$$

$\ominus$

Nesunku matyti, kad remdamiesi sąryšio "eina tiesiog po " apibrėžimu bei sudėties apibrėžimu (paeiliui du kartus) gauname

$$a + 1 = a + 0' = (a + 0)' = a'.$$

$\oplus$

Sudėties savybės

Sudėties asociatyvumo savybė. Visiems $a, b, c \in \mathcal{N}_0$ teisinga lygybė:

$$(a + b) + c = a + (b + c).$$

$\ominus$

Parodysime, kad keičiant trečią dėmenį, kai $a, b \in \mathcal{N}_0$ yra bet kokie fiksuoti skaičiai, ši lygybė yra teisinga. Apibrėžkime naturaliųjų skaičių aibę:

$M = \{n \in \mathcal{N}_0$, kuriems lygybė $(a+b)+n = a+(b+n)$ teisinga$\}$

Parodykime, kad pirmasis aibės $\mathcal{N}_0$ elementas priklauso šiai aibei, t.y. teoremos formuluotėje esanti lygybė teisinga, kai $a = 0$ ir $a, b \in \mathcal{N}_0$ yra bet kokie fiksuoti skaičiai. Remdamiesi sudėties apibrėžimo 1) lygybe gauname, kad

$$(a+b)+0 = a+b = a+(b+0).$$

Matome,kad pirmąjam elementui ši lygybė yra teisinga, taigi $0 \in M$. Taigi, aibė M netuščia. Bet jei netuščia, tai pasirinkime kokį nors šios aibės elementą, tarkime k. Vadinasi šiam elementui lygybė teisinga:

$$(a+b)+k = a+(b+k),\ k \in M. \tag{1}$$

Pastaroji lygybė paprastai vadinama indukcine prielaida (žr. a4. aksioma

1). Jeigu sugebėsime parodyti, kad iš pastarosios prielaidos ir žinomų teiginių išplaukia, kad ir sekančiam po k skaičiui $k' = k+1$ ši lygybė teisinga, tai remdamiesi matematinės indukcijos aksioma a4. galėsime tvirtinti, kad nagrinėjamoji lygybė teisinga visiems $n \in \mathcal{N}_0$, kadangi $M = \mathcal{N}_0$. Taigi

$$(a+b)+k' \text{ (remdamiesi 2))} = ((a+b)+k)' \text{ (remdamiesi prielaida (1))} =$$

$$(a+(b+k))' \text{ (remdamiesi 2))} = a+(b+k)' \text{ (remdamiesi 2))} = a+(b+k').$$

Gavome, kad esant (1) prielaidai, teoremos tvirtinimas teisingas ir sekančiam žingsniui. Turime, kad jei $k \in M$, tai ir $k+1 \in M$. Vadinasi $M = \mathcal{N}_0$, kitaip tariant, lygybė teisinga visiems natūraliesiems skaičiams.

$\oplus$

Skaitytojui siūlome įrodyti šios lygybės teisingumą, kai fiksuota kuri nors kita skaičių pora.

Komutatyvumo savybė. Suma nepriklauso nuo dėmenų tarpusavio padėties, t.y. visiems $a, b \in \mathcal{N}_0$ teisinga lygybė:

$$a+b = b+a.$$

$\ominus$

Patikrinkime, ar teisinga lygybė $0+b = b+0$. Šiuo atveju

$M = \{n \in \mathcal{N}_0$, kuriems lygybė $0+n = n+0$ teisinga $\}$

Visų pirma ar ši lygybė teisinga pirmąjam neneigiamam skaičiui $b = 0$, t.y. ar $b \in M$.

Turime, kad $0+0 = 0+0$ yra akivaizdi lygybė. Taigi, aibė M netuščia. Sakykime, kad $k \in M$, (darome indukcinę prielaidą) t. y.

$$0+k = k+0.$$

Parodysime, kad ši lygybė teisinga ir sekančiam skaičiui $k' = k+1$. Turime, kad

$0 + k'$ (remiantis 2)) $= (0 + k)'$ (remiantis 1 Teorema) $(0 + k) + 1$
(remiantis indukcine prielaida) $= (k + 0) + 1$ (remiantis 1)) $= k + 1 = k' + 0$. Tad jei $k \in M$, tai ir $k' \in M$. Vadinasi, lygybė $0 + b = b + 0$ yra teisinga visiems $b \in \mathcal{N}_0$. Norint baigti šios teoremos įrodymą, mums tektų įrodyti, kad

$$1 + b = b + 1. \text{ Po to parodyti, kad } \ a + b = b + a.$$

Tikimės, tai mielai atliks skaitytojas.

$\oplus$

2 Teorema *Visiems $a \in \mathcal{N}$, $b \in \mathcal{N}_0$ teisinga nelygybė:* $a + b \neq b$.
Kitaip tariant, suma nusakoma vieninteliu būdu.

$\ominus$

Tarkime, kad a laisvai parinktas natūralusis skaičius, o aibę M sudaro tie aibės $\mathcal{N}_0$ elementai, kuriems teisinga teoremos nelygybė. Nesunku suprasti, kad $0 \in M$, kadangi remdamiesi 1) aksioma gauname, kad $a + 0 \neq 0$. Tarkime, kad $k \in M$ (toks k egzistuoja!). Taigi, remiantis padaryta prielaida $a + k \neq k$. Ar k' irgi priklauso aibei M? Jei taip, tai $M = \mathcal{N}_0$. Tikriname: $a + k' = (a + k)'$ (pagal prielaidą) $\neq k'$. Taigi gavome, kad $k' \in M$. Tada, kaip jau esame minėję, $M = \mathcal{N}_0$.

$\oplus$

Funkciją $g : \mathcal{N}_0 \to \mathcal{N}$ vadinsime daugybos operacija, apibrėžta sveikų neneigiamų skaičių aibėje, jei $\forall (a, b) \in \mathcal{N}_0^2$ funkcija g tenkina reikalavimus:

3) $$g(a, 0) = 0,$$

4) $$g(a, b') = (g(a, b)) + a.$$

Žymėsime: $g(a, b) = a \cdot b$, nors taška, jei nekils neaiškumų, paprastai praleisime. Tuomet apibrėžime naudojamas lygybes galime perrašyti taip:

$$a \cdot 0 = 0, \text{ ir } \ a \cdot b' = ab + a.$$

Natūralųjį skaičių $g(a, b)$ vadinsime skaičių a ir b sandauga, o skaičius a ir b vadinsime dauginamaisiais.

3 Teorema *Sveikų neneigiamų skaičių aibėje teisinga lygybė:*

$$a \cdot 1 = a.$$

$\ominus$

Turime, $a \cdot 1$ (remiantis sąryšiu "eina tiesiog po") $= a \cdot 0'$ (4) daugybos savybė)$= a \cdot 0 + a$ (3) daugybos savybė) $= 0 + a$ (sumos komutatyvumo savybe ir 1)) $= a$.

$\oplus$

Distributyvumo savybė sudaro prielaidas atskliausti, kai dauginame skaičių iš kitų dviejų skaičių sumos. Tačiau, norint atskliausti, mes visų pirma turime išsiaiškinti, ar nėra svarbu iš kurios pusės rašysime daugiklį prieš skliaustuose esančią sumą. Deja, to iš karto

atlikti negalime, todėl šią problemą spręsime atskirais etapais. Visų pirma parodysime, kad jei daugiklis parašytas prieš skliaustus iš kairės pusės, tai šiuo atveju atskliausti galime.

Kairioji distributyvumo savybė. Bet kokiems $a, b, c \in \mathcal{N}_0$ teisinga lygybė

$$a(b + c) = ab + ac.$$

$\ominus$

Tarkime, kad skaičiai a, b yra laisvai pasirinkti, bet fiksuoti. Parodysime, kad tuomet visiems $c \in \mathcal{N}_0$ lygybė teisinga. Tarkime, kad parinkome $a = 7, b = 45$. Tada turėtume parodyti, kad $7(45 + c) = 7 \cdot 45 + 7 \cdot c$. Žinoma, galime fiksuoti ir kitus du skaičius, tarkime a, c, o tada b būtų bet koks. Visų pirma parodysime, kad lygybė teisinga, kai $c = 0$. Taigi

$$a(b + 0) = ab = ab + 0 = ab + a \cdot 0.$$

Įrodydami paskutiniąją lygybę naudojome 1) ir 3) savybes. Taigi, kai $c = 0$, tai ši lygybė teisinga. Padarome prielaidą, kad ši lygybė teisinga kokiam nors skaičiui k, t.y.

$$a(b + k) = ab + ak,\ k \in \mathcal{N}_0.$$

Parodysime, kad ji teisinga ir sekančiam skaičiui k'. Naudodami 2), 4), indukcinę prielaidą, sudėties asociatyvumą ir 4), eilės tvarka, gauname, kad

$$a(b + k') = a(b + k)' = a(b + k) + a = (ab + ak) + a = ab + (ak + a) = ab + ak'.$$

Taigi, jei lygybė teisinga kokiam nors skaičiui k, tai ji teisinga ir sekančiam. Remdamiesi matematinės indukcijos aksioma gauname, kad ši lygybė teisinga visiems natūraliesiems skaičiams, kuriuos rašytume c vietoje.

$\oplus$

Dešinioji distributyvumo savybė. Visiems sveikiesiems neneigiamiems skaičiams teisinga lygybė:

$$(a + b) \cdot c = ac + bc.$$

Šio tvirtinimo įrodymą paliekame skaitytojui.

Daugybos komutatyvumo savybė. Sukeitus dauginamuosius vietomis sandauga nepasikeis:

$$ab = ba,\ a, b \in \mathcal{N}_0.$$

$\ominus$

Visų pirma parodysime, kad $\forall b \in \mathcal{N}_0$ teisinga lygybė:

$$0 \cdot b = b \cdot 0.$$

Akivaizdu, kad kai $b = 0$ ši lygybė yra teisinga. Tarkime, kad ši lygybė yra teisinga ir tuo atveju, kai $b = k$. Parodysime, kad ji teisinga ir sekančiam natūraliąjam skaičiui.

Remdamiesi 4), indukcine prielaida, 3) ir dešiniąja distributyvumo savybe, atitinkamai, gauname

$$0 \cdot k' = 0 \cdot k + 0 = k \cdot 0 + 0 = k \cdot 0 + 1 \cdot 0 = (k+1) \cdot 0.$$

Taigi, $0 \cdot b = b \cdot 0$. Analogiškai įrodoma ir lygybė $1 \cdot b = b \cdot 1$.

Įrodysime, kad pasirinkę $b \in \mathcal{N}_0$, bet kokiam $a \in \mathcal{N}_0$ teisinga lygybė $ab = ba$. Visų pirma parodysime, kad ši lygybė teisinga pirmąjam sveikąjam neneigiamam skaičiui $a = 0$. Bet lygybę $0 \cdot b = b \cdot 0$ jau esame įrodę. Taigi, padarę indukcinę prielaidą, kad lygybė $kb = bk$ yra teisinga kokiam nors sveikąjam neneigiamam skaičiui parodykime, kad ji teisinga ir sekančiam skaičiui k'. Remdamiesi dešiniąja distributyvumo savybe, indukcine prielaida, lygybe $1 \cdot b = b \cdot 1$, bei kairiąja distributyvumo savybe, paeiliui, gauname, kad

$$k' \cdot b = k \cdot b + 1 \cdot b = k \cdot k + b \cdot 1 = bk'.$$

Taigi, remdamiesi indukcijos aksioma galime tvirtinti, kad lygybė teisinga visiems neneigiamiems sveikiesiems skaičiams.

$\oplus$

Asociatyvumo savybė.
Bet kokiems sveikiesiems neneigiamiems skaičiams teisinga lygybė:

$$a(b \cdot c) = (a \cdot b)c$$

$\ominus$

Tarkime, kad a, b yra bet kokie, laisvai parinkti (bet fiksuoti) sveikieji neneigiami skaičiai. Parodysime, kad lygybė teisinga $\forall c \in \mathcal{N}_0$.

Kaip paprastai, visų pirma parodysime, kad ši lygybė teisinga kai $c = 0$. Remdamiesi 3) turime, kad $a(b \cdot 0) = a \cdot 0 = 0 = (ab) \cdot 0$. Matome, kad šiuo atveju lygybė teisinga. Padarome prielaidą, kad ši lygybė teisinga, kokiam tai skaičiui $c = k$. Tad turime, kad $(ab)k = a(bk)$. Parodome, kad ši lygybė teisinga ir sekančiam skaičiui. Eilės tvarka, remdamiesi 4), indukcine prielaida, kairiąja distributyvumo savybe ir 4) gauname tokias lygybes:

$$(ab)k' = (ab)k + ab = a(bk) + ab = a(bk + b) = a(bk').$$

$\oplus$

Parodysime, kad aibė $\mathcal{N}_0$ yra tiesiškai sutvarkyta. Sakysime, kad skaičius a *yra mažesnis už skaičių* b, *(žymėsime simboliu* " $<$ "*)* jeigu egzistuoja natūralusis skaičius c, toks kad teisinga lygybė:

$$a + c = b.$$

Žymėsime $a < b$. Sakysime, kad skaičius b *yra didesnis už skaičių* a, *(žymėsime simboliu* "$b > a$" jeigu skaičius a yra mažesnis už skaičių b. Taigi, šiuo atveju sąvoka "didesnis" apibrėžiama remiantis sąvokos "mažesnis." Žymėsime $b > a$.

Kitaip tariant, natūraliųjų skaičių aibėje apibrėžiame saryšį "mažiau".

4 Teorema *Sąryšis* $<$ *"yra tranzityvus ir asimetriškas, t.y. jei* $a < b \wedge b < c$, *tai* $a < c$ *ir* $a < b$, *arba* $a > b$.

$\ominus$

Visų pirma parodysime, kad sąryšis yra tranzityvus. Tarkime, kad $a < b \wedge b < c$. Tuomet remdamiesi sąryšio apibrėžimu gauname, kad egzistuoja skaičiai $k, m \in \mathcal{N}$ tokie, kad

$$b = a + k,\ c = b + m.$$

Iš pastarųjų lygybių išplaukia, kad

$$c = (a + k) + m = a + (k + m).$$

Kadangi $k + m \in \mathcal{N}_0$, tai išplaukia iš apibrėžimo, kad $a < c$.

Įrodysime, kad šis sąryšis turi asimetriškumo savybę. Tarkime priešingai, t.y. $a < b \wedge b < a$. Remdamiesi šio sąryšio tranzityvumu gauname, kad $a < a$. Iš apibrėžimo išplaukia, kad egzistuoja toks natūralusis skaičius k, kad teisinga lygybė: $a + k = a$. Bet tokia lygybė neįmanoma, jei $k \in \mathcal{N}$. Taigi, gavome prieštaravimą. Vadinasi pradinė prielaida, kad $a < b \wedge b < a$ yra klaidinga, tad belieka atvejis $a > b \vee b > a$.

$\oplus$

Galima nesunkiai parodyti, kad bet kokiai natūraliųjų skaičių porai galioja bent vienas iš sąryšių:

$$a < b,\ a > b,\ a = b.$$

5 Teorema *Tarkime, kad* $a, b \in \mathcal{N}_0$ *ir* $a < b$. *Tada visiems* $n \in \mathcal{N}_0$ $a + n < b + n$.

$\ominus$

Tarkime, kad $a < b$. Tada $\exists k \in \mathcal{N}$ toks, kad $b = a + k$. Pridėję prie abiejų lygybės pusių po tą patį skaičių n gauname.

$$b + n = (a + k) + n = a + (k + n) = a + (n + k) = (a + n) + k.$$

Iš pastarųjų lygybių išplaukia, kad $a + n < b + n$.

$\oplus$

6 Teorema *Tegu* $k, a, b \in \mathcal{N}$. *Jei* $a < b$, tai $ac < bc$.

Paskutiniąją teoremą siūlome įrodyti skaitytojui.

Sveikųjų neneigiamų skaičių a ir b *skirtumu* vadinsime natūralųjį skaičių c tokį, kad $b + c = a$, jei skaičius $c \in \mathcal{N}_0$ egzistuoja. Tokiu būdu apibrėžtą sąryšį sveikųjų neneigiamų skaičių aibėje vadinsime *atimties operacija*, kurią žymėsime

$$a - b = c.$$

Skaičius c vadinamas skirtumu, $a-$ turiniu, $b-$ atėminiu.

Iš apibrėžimo išplaukia, kad atimties operacija yra apibrėžta ne visiems natūraliesiems skaičiams.

7 Teorema *Sveikųjų neneigiamų skaičių a ir b skirtumas egzistuoja tik tada, jei skaičius b yra ne didesnis už skaičių a ($b \leq a$.) Be to jei skirtumas egzistuoja, tai jis yra vienintelis.*

$\ominus$

Tarkime, kad $a - b = c$. Remdamiesi skirtumo apibrėžimu gauname, kad $a = b + c$. Matome, kad jei $c > 0$, tai $a > b$, t.y. turinys didesnis už atėminį. Jeigu $c = 0$, tai $a = b$, taigi šiuo atveju skirtumas lygus nuliui. Iš pastarųjų samprotavimų gauname, kad turinys ne mažesnis už atėminį, kitaip tariant $a \geq b$.

Tarkime, kad yra du skaičių skirtumai, t.y.

$$a - b = c_1,\ a - b = c_2.$$

Tarkime, kad $c_2 \leq c_1$. Tada atėmę pirmąją lygybę iš antrosios gauname, kad $c_1 - c_2 = 0$. Bet tuomet $c_1 = c_2$. Iš paskutiniosios lygybės gauname teoremos įrodymą.

$\ominus$

3.3 Dalumo sąryšis sveikųjų neneigiamų skaičių aibėje. Dalumo požymiai

Sakysime, kad sveikas neneigiamas skaičius b *dalo* sveiką neneigiamą skaičių a, (žymėsime $b|a$) jeigu egzistuoja vienintelis sveikas neneigiamas skaičius k toks, kad $a = bk$. Šį sąryšį, apibrėžtą sveikųjų neneigiamų skaičių aibėje, vadinsime *dalybos operacija.* Skaičių b vadinsime skaičiaus a dalikliu, o skaičių $a-$ skaičiaus b daliniu. Skaičius k vadinamas dalmeniu.

Nesunku suprasti, kad jei sveikas neneigiamas skaičius b dalo sveiką neneigiamą skaičių a, tai $b \leq a$. Be to skaičių 0 dalo bet koks natūralusis skaičius. Antra vertus, 0 nedalo nė vieno natūraliojo skaičiaus a. Beje, laikome, kad 0 nedalo 0, kadangi šiuo atveju negalime nurodyti vienintelio $k \in \mathcal{N}_0$ tokio, kad būtų teisinga lygybė: $0 = 0k$. Taigi, dalyba iš nulio yra neapibrėžta.

Panagrinėkime dalumo savybes sveikųjų neneigiamų skaičių aibėje.

8 Teorema *Dalumo sąryšis yra*
1) refleksyvus, t.y. $a|a$
2) tranzityvus, t.y. jei $a|b$, $b|c$, tai $a|c$
3) antisimetriškas, t.y. jei $a|b$ ir $b|a$, tai $a = b$.

$\ominus$

Tai, kad dalumo sąryšis yra refleksyvus, akivaizdu.

Įrodysime, kad sąryšis yra tranzityvus. Turime, kad $b = ak$ ir $c = bl$, $k \in \mathcal{N}_0$. Iš pastarųjų lygybių išplaukia, lygybė $c = a(kl)$. Kadangi $kl \in \mathcal{N}_0$, tai gauname, kad $a|c$.

Turime, kad $a = bk$ ir $b = al$. Iš šių lygybių išplaukia, kad $kl = 1$. Bet pastaroji lygybė galima tik tuo atveju, kai $k = l = 1$. Taigi, $a = b$. Vadinasi sąryšis antisimetrinis.

Tuo baigiame teoremos įrodymą.

$\oplus$

9 Teorema *Jei skaičius c dalo skaičius a ir b, tai skaičius c dalo ir sumą $a + b$. Be to, jei $a \geq b$ tai c dalo ir skirtumą $a - b$.*

$\ominus$

Iš dalybos operacijos apibrėžimo išplaukia, kad $a = cl$ ir $a = ck$. Bet tada, $a + b = al + ck = c(l + k)$, čia $l + k \in \mathcal{N}_0$. Iš paskutiniosios lygybės išplaukia, kad $c|a + b$. Skirtumo dalumas įrodomas visiškai analogiškai.

$\oplus$

10 Teorema *Jei skaičius c dalo skirtumą $a - b$ (sumą $a + b$) ir be to dalo bent vieną iš skaičių, tarkime a, tai tada c dalo ir antrąjį skirtumo (sumos) narį b.*

11 Teorema *Jei skaičius c dalo a ir nedalo b, tai tada c nedalo ir skirtumo $a - b$ (sumos $a + b$)*

12 Teorema *Jeigu sandauga $bc|ac$, tai skaičius $b|a$.*

Šias teoremas siūlome įrodyti skaitytojui.

13 Teorema *Jei $c|a$ arba $c|b$, tai tada $c|(ab)$.*

$\ominus$

Tarkime, kad $c|a$. Tuomet $a = ck, k \in \mathcal{N}_0$. Padauginę abi šios lygybės puses iš skaičius b gauname, $ab = (ck)b = (cb)k$. Iš paskutiniosios lygybės išplaukia, kad $c|(ab)$.

$\oplus$

14 Teorema *Jeigu skaičius $k|a$, o skaičius $l|b$, tai $(kl)|(ab)$.*

$\ominus$

Turime, kad $a = kc_1$ ir $b = lc_2$. Iš šių lygybių išplaukia, kad

$$ab = (kl)(c_1c_2),\ c_1c_2 \in \mathcal{N}_0.$$

Tuo ir baigiame teoremos įrodymą.

$\oplus$

15 Teorema (Dalybos su liekana teorema.) *Bet kokiai skaičių porai $a \in \mathcal{N}_0,\ b \in \mathcal{N}$, egzistuoja vienintelė sveikų neneigiamų skaičių pora k, r tokia, kad*

$$a = kb + r,\ 0 \leq r < b. \tag{1}$$

$\ominus$

Visų pirma įsitikinsime, kad iš tiesų bet kokiai porai a, b galime nurodyti skaičių porą k, r, kad būtų teisinga (1) lygybė. Įrodydami šį sąryšį, naudosimės matematinės indukcijos metodu, skaičiaus a atžvilgiu, t.y. tarsime, kad b yra bet koks fiksuotas, laisvai pasirinktas natūralusis skaičius.

Taigi, patikrinkime ar (1) lygybė teisinga pirmąjam $\mathcal{N}_0$ elementui. Taigi, kai $a = 0$, tai $0 = b0 + 0$. Matome, kad (1) lygybė teisinga su $r = 0 < b$.

Vadinasi, pagrįstai galime daryti indukcinę prielaidą: tarkime, kad kokiam nors skaičiui $a = n$ teisinga lygybė

$$n = bk + r,\ 0 \leq r < b. \tag{2}$$

Parodysime, kad (1) lygybė teisinga ir sekančiam skaičiui $n + 1$. Pridėkime prie abiejų (2) lygybės pusių 1. Gausime

$$n + 1 = bk + (k + 1),\ 0 \leq r + 1 \leq b.$$

Jei $r+1<b$, tai iš karto gauname teoremos įrodymą, o jei $r+1=b$, tai paskutinioji lygybė tampa tokia

$$n+1=b(k+1)+0,\ 0=r<b.$$

Gavome, kad lygybė teisinga ir sekančiam natūraliąjam skaičiui. Vadinasi ši lygybė teisinga ir visiems $a\in\mathcal{N}_0$.

Įsitikinsime, kad porą a,b atitinka vienintelė pora k,r, šių porų sąlygos nurodytos teoremos formuluotėje. Tarkime priešingai, t.y. egzistuoja bent dvi skirtingos poros k,r ir k_1,r_1 atitinkančios porą a,b. Tuomet teisingos lygybės

$$a=bk+r,\ a=bk_1+r_1,\ 0\leq r,r_1<b. \tag{3}$$

Parodysime, kad $r=r_1$. Tarkime priešingai, t.y. $r>r_1$. Tada iš (3) lygybių gauname, kad

$$0<r-r_1<b \tag{4}$$

ir

$$r-r_1=b(k-k_1). \tag{5}$$

Kadangi $r-r_1>0$, tai ir $k-k_1\geq 1$. Bet tada $r-r_1\geq b$. Bet paskutinioji nelygybė prieštarauja gautąjai (4) nelygybei. Visiškai analogiškai gautume, jei nagrinėtume atvejį, kai $r<r_1$. Taigi $r=r_1$. Įrašę gautąjį rezultatą į (5) lygybę gauname, kad $b(k-k_1)=0$. Kadangi $b>0$, tai $k=k_1$.

$\oplus$

Taigi, $b|a$ tada ir tik tada, kad (1) formulėje, liekana $r=0$.

Panagrinėkime dalumo iš kai kurių skaičių požymius. Dalumo požymius nustatysime naudodamiesi standartine skaičiaus forma. Turime, kad

$$a=\overline{a_na_{n-1}\dots a_0}=a_n10^n+a_{n-1}10^{n-1}+\dots+a_110+a_010^0, \tag{6}$$

be to $10^k=(2\cdot 5)^k,\ k=0,1,\dots n$.

16 Teorema $2|a$ *tada ir tik tada, kai* a *yra lyginis.*

$\ominus$

Kadangi a lyginis natūralusis skaičius, tai jo paskutinis skaitmuo a_0 yra lyginis skaičius. Taigi, $2|a_0$ ir be to $2|10^k$. Taigi, 2 dalo visus (1) sumos dėmenis, o tuo pačiu ir sumą a.

$\oplus$

17 Teorema *Skaičius* $5|a$ *tada ir tik tada, kai* $5|a_0$

Paskutinioji teorema įrodoma analogiškai kaip ir 16 Teorema. Beje, šią teoremą galime perfrazuoti kiek kitaip. T.y. $5|a$ jeigu paskutinis skaičiaus a skaitmuo yra 0 arba 5.

18 Teorema *Skaičius* $3|a$ *tada ir tik tada, kai* 3 *dalo šio skaičiaus skaitmenų sumą.*

$\ominus$

Naudodamiesi gerai žinoma tapatybe

$$10^n - 1 = (10-1)(10^{n-1} + 10^{n-2} + \ldots + 10 + 1) =$$

$$10^n - 1 = 9(10^{n-1} + 10^{n-2} + \ldots + 10 + 1), \tag{7}$$

kai $n \geq 1$, matome, kad (7) reiškinį dalo skaičius 3. Perrašykime (6) lygybę tokiu būdu

$$a = a_n\big((10^n - 1) + 1)\big) + a_{n-1}\big((10^{n-1} - 1) + 1)\big) + \ldots$$

$$+a_2\big((10^2 - 1) + 1)\big) + a_1\big((10 - 1) + 1)\big) + a_0 =$$

$$a_n\big(10^n - 1\big) + a_{n-1}\big(10^{n-1}\big) + \ldots$$

$$+a_2\big(10^2 - 1\big) + a_1\big(10 - 1\big) +$$

$$a_n + a_{n-1} + \ldots + a_1 + a_0.$$

Remdamiesi (7) tapatybe darome išvadą, kad $3|a$ dalo tada ir tik tada, kai $3|(a_n + a_{n-1} + \ldots + a_1 + a_0)$, t.y. dalo šio skaičiaus skaitmenų sumą.

$\oplus$

Išvada *Skaičius* $9|a$ *tada ir tik tada, kai* 9 *dalo šio skaičiaus skaitmenų sumą.*

19 Teorema *Skaičius* $4|a$ *tada ir tik tada, kai skaičiaus* a *paskutiniai du skaitmenys sudaro skaičių, kurį dalo skaičius* 4.

$\ominus$

Skaičius $4|10^k$, kai $k > 2$. Taigi, skaičiaus a dalumas iš 4 priklauso nuo to ar 4 dalo likusią kanoninės formos dalį, t.y. $k = a_1 10 + a_0$. Bet paskutinysis reiškinys yra dviženklis skaičius, kuris sudarytas iš skaičiaus a paskutiniųjų skaitmenų. Tad jei $4|k$, tai $4|a$ ir atvirkščiai.

$\oplus$

Analogišku būdu (tai paliekame skaitytojui) galima įrodyti, kad *skaičių* a *dalo skaičius 25 tada ir tik tada, kai paskutiniai skaitmenys sudaro skaičių, kurį dalo skaičius 25.*

3.4 Didžiausias bendras daliklis. Euklido algoritmas

Tarkime, kad skaičiai $n_1, n_2, \ldots, n_k \in \mathcal{N}$. Šių skaičių bendru dalikliu vadinsime bet kokį skaičių, dalijantį nurodytus skaičius. Patį didžiausią iš šių daliklių vadinsime šių skaičių bendru didžiausiu dalikliu (toliau d.b.d.) ir žymėsime simboliu $(n_1, n_2, \ldots, n_k)$. Nesunku suprasti, kad bendras didžiausias daliklis egzistuoja, kadangi bendrų daliklių skaičius yra baigtinis. Jeigu teisinga lygybė:

$$(n_1, n_2, \ldots, n_k) = 1,$$

tai sakysime, kad skaičiai $n_1, \ldots, n_k$ yra tarpusavyje pirminiai. Jeigu be to ir bet kuri skaičių pora $(n_i, n_j) = 1$ $i, j = 1 \ldots k, i \neq j$, tai sakysime, kad skaičių rinkinyje skaičiai

poromis pirminiai. Aišku, kad jei skaičiai yra poromis pirminiai, tai jie ir tarpusavyje pirminiai. Tačiau atvirkščias teiginys nėra teisingas.

20 Teorema *Jeigu skaičius $b|a$, tai skaičių a ir b bendrų daliklių aibė sutampa su skaičiaus b bendrų daliklių aibe. Dar daugiau $(a, b) = b$.*

$\ominus$

Turime, kad bet koks skaičių a ir b bendras daliklis tuo pačiu yra ir skaičiaus b daliklis.

Atvirkščiai. Jeigu b yra skaičiaus a dalikis, tai bet koks skaičiaus b daliklis yra ir skaičiaus a daliklis, taigi, jis yra skaičių a ir b bendras daliklis. Darome išvadą, kad skaičių a ir b bendrų daliklių aibė sutampa su skaičiaus b daliklių aibe.

$\oplus$

21 Teorema *Jeigu*

$$a = bq + c$$

tai skaičių a ir b daliklių aibė yra lygi skaičių b ir c daliklių aibei. Be to $(a, b) = (b, c)$.

$\ominus$

Nesunku suprasti, kad skaičių a, b d.b.d. dalo ir skaičių c (kodėl?), taigi, $(a, b) = (b, c)$.

Atvirkščiai. Iš tos pat lygybės gauname, kad bet koks skaičių (b, c) bendras daliklis dalo ir skaičių a, taigi, šis daliklis yra ir skaičių a, b bendras daliklis. Vadinasi skaičių a, b ir b, c daliklių aibės sutampa. Todėl $(a, b) = (b, c)$.

Aptarsime dviejų skaičių d.b.d. ieškojimą, naudojant *Euklido algoritmą.*

Tarkime, kad turime du natūraliuosius skaičius a, b ir be to $a > b$. Tada naudodamiesi dalybos su liekana teorema gauname, kad

$$a = bq_1 + r_1, \;\; 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \;\; 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \;\; 0 < r_3 < r_2;$$

$$r_{n-2} = r_{n-1}q_n + r_n, \;\; 0 < r_n < r_{n-1};$$

$$r_{n-1} = r_nq_{n+1}.$$

Paskutinioji lygybių seka baigiasi, kai $r_{n+1} = 0$, kadangi skaičiai $b > r_1 > r_2 > \ldots$ yra neneigiami ir mažėjantys. Beje, šioje sekoje bus ne daugiau b teigiamų skaičių. Paskutinysis dalybos su liekana algoritmas vadinamas *Euklido algoritmu.*

Panagrinėkime Euklido algoritmą. Visų pirma pastebėkime, kad skaičių a, b bendri dalikliai sutampa su skaičių b, r_1 bendrais dalikliai, o pastarieji su skaičių r_1, r_2 bendrais dalikliais ir taip toliau, su skaičių r_{n-1}, r_n bendrais dalikliais, o iš paskutiniosios lygybės išplaukia, kad skaičių a, b bendrų daliklių aibė sutampa su skaičiaus r_n daliklių aibe. Be to teisingos lygybės (žr. 21 ir 20 teoremas)

$$(a,b) = (b,r_1) = \ldots = (r_{n-1}, r_n) = r_n.$$

Išvada. Skaičių a, b d.b.d. yra lygus Euklido algoritmo, paskutinei nelygiai nuliui, liekanai. T.y. $(a,b) = r_n$.

22 Teorema *Tarkime, kad $m \in \mathcal{N}$, o δ bet koks skaičių a, b bendras daliklis. Tada teisingos lygybės*

$$a)\ \ (am, bm) = (a,b)m; \quad b)\ \ \big(\frac{a}{\delta}, \frac{b}{\delta}\big) = \frac{(a,b)}{\delta}.$$

Be to,

$$\big(\frac{a}{(a,b)}, \frac{b}{(a,b)}\big) = 1.$$

$\ominus$

Įrodysime a) dalį. Pastebėsime, kad Euklido algoritme visas lygybes padauginę iš m gausime, kad lygybėse vietoje skaičių $a, b, r_1, \ldots, r_n$ yra skaičiai $am, bm, r_1m, \ldots, r_nm$, atitinkamai. Todėl $(am, bm) = r_nm$.

Įrodydami b) dalį remsimės a) dalimi. Turime

$$(a,b) = \big(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\big) = \big(\frac{a}{\delta}, \frac{b}{\delta}\big)\delta.$$

$\oplus$

23 Teorema *Jei $(a,b) = 1$, tai $(ac, b) = (c, b)$.*

$\ominus$

Pastebėsime, kad (ac, b) dalo skaičius ac ir b. Bet tada (kodėl?) $(ac, b)|b$ ir tuo pačiu $(ac, b)|(c, b)$.

Atvirkščiai. (c, b) dalo ac ir b, todėl (c, b) dalo (ac, b). Be tada skaičiai (ac, b) ir (c, b) dalo viens kitą, o tai reiškia, kad jie yra lygūs.

$\oplus$

24 Teorema *Jeigu $(a,b) = 1$ ir $ac|b$, tai $c|b$.*

$\ominus$

Kadangi $(a,b) = 1$, tai iš 22 Teoremos išplaukia, kad $(ac, b) = (c, b)$. Bet $b|ac$, tada išplaukia, kad $(ac, b) = b$. Taigi $(c, b) = b$ arba $b|(c, b)$.

$\oplus$

25 Teorema *Jei kiekvienas iš skaičių $a_1, \ldots, a_m$ yra tarpusavyje pirminis su bet kuriuo rinkinio $b_1, \ldots, b_n$ skaičiumi, tai*

$$(a_1a_2 \ldots a_m, b_1b_2 \ldots b_n) = 1.$$

$\ominus$

Remdamiesi 23 Teorema gauname, kad

$$(a_1 \dots a_m, b_k) = (a_2 \dots a_m, b_k) = \dots = (a_m, b_k) = 1.$$

Pažymėję $a = a_1 \dots a_n$ ir samprotaudami analogiškai gauname

$$(b_1 \dots b_n, a) = (b_2 \dots b_n, a) = \dots = (b_n, a) = 1.$$

$\oplus$
Tarkime, kad mums reikia rasti skaičių $a_1, a_2, \dots a_n$ b.d.d. Sudarykime tokią seką:

$$(a_1, a_2) = d_1, (d_1, a_3) = d_2, \dots, (d_{n-2}, a_n) = d_{n-1}.$$

Tada

$$(a_1, a_2, \dots, a_n) = d_{n-1}.$$

Siūlome skaitytojui pačiam įsitikinti paskutiniojo tvirtinimo teisingumu.

3.5 Mažiausias bendras kartotinis.

Tarkime, kad duotas skaičių rinkinys $a_1, \dots, a_m$. Skaičių a vadinsime duoto skaičių rinkinio bendru kartotiniu, jeigu bet koks rinkinio skaičius dalo skaičių a. Patį mažiausią iš šių kartotinių vadinsime duotojo rinkinio *mažiausiu bendru kartotiniu* ir žymėsime

$$M = [a_1, a_2, \dots, a_n].$$

Pažymėkime $M = (a, b)$.
26 Teorema *Skaičių, a, b, mažiausią bendrą kartotinį galime užrašyti tokiu būdu:*

$$[a, b] = \frac{ab}{(a, b)}. \tag{1}$$

$\ominus$
Teoremos formuluotę, naudodami ankstesnius žymėjimus, galime perrašyti taip: $M = m(ab)$.

Turime, kad $a = a_1 m, b = b_1 m$. Bet tada, $(a_1, b_1) = 1$. Tarkime, kad $M-$ koks nors skaičių a, b kartotinis. Tada egzistuoja $k \in \mathcal{N}$, kad $M = ak$. Be to M yra ir b kartotinis. Taigi,

$$\frac{ak}{b} = \frac{a_1 k}{b_1}$$

yra sveikas skaičius. Dar daugiau, $b|k$. Paskutinysis sąryšis reiškia, kad egzistuoja $k \in \mathcal{N}$ toks, kad $k = b_1 t = (b/d)t$. Taigi, turime

$$M = \frac{ab}{d}t. \tag{2}$$

Atvirkščiai. Jeigu skaičius užrašytas (1) lygybe, tai kokį beparinktume natūralųjį k, skaičius M bus a ir b kartotinis. Tad darome išvadą, kad (2) lygybė apibrėžia visus skaičių a, b kartotinius. Akivaizdu, kad mažiausią kartotinį gausime, jeigu parinksime $t = 1$. Tada iš (1) lygybės išplaukia formulė skaičių a ir b mažiausiam bendram kartotiniam rasti:

$$m = \frac{ab}{(a, b)}.$$

$\oplus$

Išvada. *Skaičių a, b bendrų kartotinių aibė sutampa su šių skaičių m.b.k. kartotinių aibe. Kartotinių aibė yra begalinė.*

Aptarsime būdą, kaip rasti daugiau negu dviejų skaičių m.b.k.

27 Teorema *Tarkime, duotas skaičių $a_1, a_2, \ldots, a_n$ rinkinys. Apskaičiuokime*

$$[a_1, a_2] = m_1, \;\; [m_1, a_3] = m_2, \;\; \ldots, \;\; [m_{n-1}, a_n] = m_n.$$

Tada skaičius m_n yra pradinio skaičių rinkinio b.m.k..

$\ominus$

Remdamiesi paskutiniąja išvada turime, kad skaičių a_1, a_2 bendri kartotiniai sutampa su skaičiaus m_1 bendru kartotiniu. Toliau, skaičių a_1, a_2, a_3 bendri kartotiniai sutampa su skaičių m_2 ir a_3 bendru kartotiniu, t.y. skaičiumi m_3 ir t.t. skaičių $a_1, a_2, \ldots a_n$ bendri kartotiniai sutampa su skaičiumi m_n. Kadangi skaičiaus m_n b.m.k. yra šis skaičius m_n, tad ir gauname, kad

$$[a_1, a_2, \ldots a_n] = m_n.$$

$\oplus$

Išvada. *Jeigu rinkinyje skaičiai yra poromis tarpusavyje pirminiai, tai šio rinkinio* b.m.k. *yra lygus šių skaičių sandaugai.* T.y., jei $(a_1, \ldots, a_n) = 1$, tai $[a_1, \ldots, a_n] = a_1 \ldots a_n$.

3.6 Pirminiai skaičiai. Pagrindinė aritmetikos teorema

Bet koks natūralusis skaičius, didesnis už 1, turi ne mažiau negu du daliklius, t.y. bent jau vienetą ir save patį.

Apibrėžimas *Natūralųjį skaičių vadinsime pirminiu, jeigu jis turi tik du daliklius. Jeigu skaičius turi daugiau negu du dalikliu, tokį skaičių vadinsime sudėtiniu.*

28 Teorema *Jei natūraliojo skaičiaus a pats mažiausias daliklis $q \neq 1$ ir $q \neq a$, tai 6is daliklis yra pirminis skaičius. Be to šis pirminis turi savybę: $q < \sqrt{a}$.*

$\ominus$

Tarkime, kad $q \neq 1$ pats mažiausias skaičiaus a daliklis. Jeigu q sudėtinis, tai egzistuoja skaičius $1 < k < q$, toks kad $k|q$. Bet tai prieštarauja pradinei prielaidai, kad q yra mažiausias daliklis. Vadinasi teisingas priešingas teiginys- q yra pirminis.

Įrodysime antrąją teoremos dalį. Turime, kad egistuoja $k \in \mathcal{N}$, toks kad $a = kq$, be to $k \geq q$. Be tada teisinga nelygybė $a \geq q^2$ arba $q \leq \sqrt{a}$.

$\oplus$

Išvada *Jei pirminis skaičius p dalo skaičių a, ir $p \neq a$, tai $p \leq \sqrt{a}$.*

29 Teorema *Pirminių skaičių aibė- begalinė.*

$\ominus$

Tarkime priešingai, t.y. pirminių skaičių aibė yra baigtinė, kurią sudaro tokie skirtingi pirminiai $p_1, p_2, \ldots, p_k$. Tada skaičiaus

$$p_1 \cdot p_2 \cdot \ldots p_k + 1 \tag{3}$$

nedalo nė vienas iš nurodytų pirminių, kadangi dalydamas šį skaičių, jis be to dalo ir sandaugą $p_1 \cdot p_2 \ldots p_k$, taigi, jis turėtų dalyti ir 1, bet taip būti negali. Taigi, prielaida buvo klaidinga. Darome išvadą, kad pirminių skaičių aibė begalinė.

$\oplus$

Aptarsime klasikinį metodą, kuriuo remiantis galime sudaryti pirmųjų, natūraliųjų skaičių sekos, pirminių aibę. Šis metodas vadinamas *Erastoteno rėčiu.*

Tarkime, duota natūraliųjų skaičių seka

$$1, 2, \ldots, N. \tag{4}$$

Aišku, kad pirmasis pirminis yra skaičius 2. Išbraukime iš (4) sekos visus skaičius, kurie yra skaičiaus 2 kartotiniai, išskyrus jį patį. Pirmasis neišbrauktas skaičius po 2, yra 3. Nesunku patikrinti, kad tai irgi pirminis skaičius. Išbraukime (1) sekoje visus skaičiaus 3 kartotinius, išskyrus 3. Sekantis neišbrauktas skaičius yra 5. Jis irgi pirminis, nes priešingu atveju jis būtų išbrauktas, kadangi jį dalytų arba 2 arba 3. Ir taip toliau.

Kuomet nurodytu būdu išbraukti visi skaičiai, kurie kartotiniai pirminiams, mažesniems už kokį nors p, tai visi neišbraukti skaičiai tarp p ir p^2 yra pirminiai. Iš tiesų, bet koks sudėtinis skaičius a, mažesnis už p^2, turi būti jau išbrauktas, kadangi jis yra kokio nors jo mažiausio pirminio kartotinis, kuriam teisinga nelygybė: $\sqrt{a} \leq p$.

Apibendrinkime aukščiau aptartą metodą.

1. *Prieš pradedant išbraukti pirminio p kartotinius, reikia pradėti nuo p^2.*

2. *Pirminių skaičių lentelė (1) sekoje bus baigta, kai tik išbrauksime visus sudėtinius skaičius, kurie yra pirminių, nedidesnių už $\sqrt{N}$, kartotiniai.*

30 Teorema *Tarkime, kad a be koks natūralus, o p pirminis, skaičiai. Tada a arba tarpusavyje pirminis su p arba $p|a$.*

$\ominus$

Skaičius $(a, p)|p$, todėl šis skaičius yra arba lygus 1 arba p. Pirmuoju atveju $(a, p) = 1$, o antruoju $p|a$.

$\oplus$

31 Teorema *Jeigu kelių skaičių sandaugą dalo pirminis skaičius p, tai bent vieną šios sandaugos daugiklį dalo p.*

Šios teoremos įrodymą paliekame skaitytojui.

32 Pagrindinė aritmetikos teorema *Bet kokį natūralųjį skaičių, didesnį už vienetą, vieninteliu būdu galima užrašyti pirminių skaičių laipsnių sandauga.*

$\ominus$

Pastebėsime, kad teiginys *vieninteliu būdu* suprantamas, kad dauginamųjų užrašymo tvarka skaidinyje, nėra svarbi.

Tarkime, kad $a \in \mathcal{N},\ a > 0$. Pažymėkime skaičiaus a mažiausią pirminį p_1. Tada $a = p_1 a_1$. Jeigu $a_1 > 1$, tai pažymėję p_2 mažiausią skaičiaus a_1 pirminį daliklį gauname, kad $a_1 = a_2 p_2$. Jeigu $a_2 > 1$, tai pažymėję p_3 mažiausią a_2 pirminį daliklį gauname, kad $a_2 = p_3 a_3$. Ir t.t. Kadangi $a > a_1 > a_2 \ldots >$ tai egzistuoja numeris n toks, kad $a_n = 1$. Tada $a_{n-1} = p_n$. Daugindami gautus kartotinius gauname, kad

$$a = p_1 p_2 \ldots p_n. \tag{5}$$

Parodykime, kad šis skaičiaus išskaidymas yra ne vienintelis. T.y. egzistuoja skaidinys kitais pirminiais. Bet tada turi būti teisinga lygybė:

$$p_1 p_2 \ldots p_n = q_1 q_2 \ldots q_m. \tag{6}$$

Paskutiniosios lygybės dešiniąją pusę dalo pirminis q_1. Bet tada ir bent vieną kairiosios lygybės pusės daugiklį dalo šis pirminis. Tarkime, kad $q_1 | p_1$. Tada $p_1 = q_1$. Dalindami abi lygybės puses iš p_1 gauname

$$p_2 \ldots p_n = q_2 \ldots q_m.$$

Ir t.t.. Sakykime, kad $m > n$. Pakartoję šį procesą n kartų gautume lygybę:

$$1 = q_{n+1} \ldots q_m.$$

Bet pastaroji lygybė galima tik tuo atveju, kai $q_{n+1} = \ldots = q_m = 1$. Taigi gauname, kad $p_1 = q_1; \ldots p_n = q_n$. Kitaip tariant, (5) lygybė užrašoma vieninteliu būdu.

$\oplus$

Pastebėsime, kad jei (5) lygybėje pasikartojančius pirminius sudaugintume, tai gautume tokią lygybę

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}. \tag{8}$$

Paskutinioji lygybė yra vadinama skaičiaus a *kanoniniu skaidiniu.*

Pastaba. Jeigu skaičius a užrašytas (8) lygybe, tai tada visus a daliklius gauname iš lygybių

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},\ 0 \le \beta_i \le \alpha_i,\ \ i = 1; \ldots, n. \tag{9}$$

Tarkime, kad duoti du skaičiai a ir b. Pastebėsime, kad nemažindami bendrumo galime pasiekti, kad abiejuose skaičių kanoniniuose skaidiniuose būtų tie patys pirminiai, žinoma, gali būti, kad kai kurie pirminiai bus su nuliniais laipsniais.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n},\ \ b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}.$$

Tokias skaičių kanonines formas vadinsime *suvienodintomis kanoninėmis formomis.*

Pažymėkime

$$\delta_i = \min(\alpha_i, \beta_i), \;\; \gamma_i = \max(\alpha_i, \beta_i); \; i = 1, \ldots, n.$$

Tarkime, kad nagrinėjamų skaičių kanoniniai skaidiniai yra žinomi. Tada teisinga tokia

33 Teorema *Skaičių d.b.d yra lygus sandaugai visų bendrų pirminių dauginamųjų, paimtų su mažiausiais laipsnio rodikliais jų kanoniniuose skaidiniuose. Skaičių mažiausio bendro kartotinio kanoninis skaidinys yra lygus sandaugai visų šių skaičių pirminių daliklių, paimtų su didžiausiais laipsnio rodikliais, sandaugai.*

$\ominus$

Teoremą įrodysime dviems skaičiams. Tarkime, kad skaičių a, b kanoninės formos yra suvienodintos.

Tada skaičius

$$d = p_1^{\delta_1} \ldots p_n^{\delta_n}$$

yra skaičių a ir b bendras daliklis. Dar daugiau, $(a, b)|d$. Tada, skaičiaus (a, b) bendro didžiausio daliklio kanoninį skaidinį galime užrašyti taip:

$$(a, b) = p_1^{\delta_1+\rho_1} \ldots p_n^{\delta_n+\rho_n}, \; \rho_i \geq 0.$$

Parodykime, kad $\rho_i = 0, \; i = 1, \ldots n.$

Tarkime priešingai, t.y. $\rho_0 > 0$. Bet tada vienas iš skaičių a arba b, kurio pirmasis daugiklis p_1 turi laipsnio rodiklį δ_1, nesidalys iš (a, b), kadangi $\delta_1 < \delta_1 + \rho_1$. Bet tai prieštarauja prielaidai, kad $(a, b)|a \wedge b$. Taigi, $\rho_1 = 0$. Analogiškai samprotaudami gausime, kad ir likę rodikliai $\rho_i = 0, \; i = 2, \ldots, n$. Taigi skaičius $d = (a, b)$.

Įrodysime antrąją teoremos dalį. Pažymėkime

$$m = p_1^{\gamma_1} \ldots p_n^{\gamma_n}.$$

Tada $a|m$, ir $b|m$. Taigi, skaičius m yra skaičių a ir b bendras kartotinis. Žinome, kad bet kokį kartotinį dalo bendras mažiausias kartotinis. Aišku, kad $[a, b]$ suvienodintos kanoninės formos laipsniai ne didesni už atitinkamų skaičiaus m pirminių laipsnius $\gamma_i, \; i = 1; \; \ldots n$. Užrašykime skaičiaus $[a, b]$ atitinkamų pirminių laipsnius šitaip: $\gamma_i - \rho_i, \ldots, \rho_i \geq_i \geq 0$. Tada

$$[a, b] = p_1^{\delta_1-\rho_1} \ldots p_n^{\delta_n-\rho_n}.$$

Kaip ir pirmoje teoremos dalyje parodysime, kad $\rho_i = 0$.

Tarkime priešingai, t.y. $\rho_1 > 0$. Bet tada a arba b nedalo skaičiaus $[a, b]$, kadangi vieno iš minėtų skaičių pirminio laipsnis, kanoniniame skaidinyje, δ_1 yra didesnis už skaičiaus $[a, b]$ pirmojo pirminio laipsnį $\delta_1 - \rho_1$. Taigi, prielaida klaidinga, vadinasi $\rho_1 = 0$.

Samprotaudami visiškai analogiškai galime parodyti, kad visi rodikliai $\rho_i = 0, \; i = 2, \ldots, n$. Tada $[a, b] = m$.

$\oplus$

Skaiytojui pateiksime dar vieną skaičių skaidymo dviem daugikliais algoritmą, kuris vadinamas *Ferma algoritmu.*

Įv: $n \geq 0-$ faktorizuojamas skaičius
Išv: n pirminis arba $n = k \cdot l$.
$r := \sqrt{n}$
for i **from** 1 **to** $\sqrt{\frac{n-3}{2}}$ **do**
$a := (r+i)^2$
$j := \sqrt{a-n}$
if$j \in \mathcal{Z}$**then**
$k := \sqrt{a} - \sqrt{j}$
$l := \sqrt{a} + \sqrt{j}$
$n := k \cdot l$
goto end
end if
end for
$n-$ pirminis

end

3.7 Multiplikatyviosos funkcijos. Liekanų klasės

Sakykime, kad $a \in \mathcal{R}$. Tada funkcija $f(a) = [a] = n$, jei $n \leq a < n+1$ yra vadinama skaičiaus a sveikąja dalimi, o funkcija $\{a\} = a - [a]-$ trupmenine skaičiaus a dalimi.

Priminsime, kad $n! = 1 \cdot 2 \cdot 3 \cdots n$.

34 Teorema *Sakykime, kad pirminis skaičius p dalo skaičių $n!$. Tada laipsnis α, su kuriuo pirminis p yra skaičiaus $n!$ skaidinyje yra toks:*

$$\alpha = [\frac{n}{p}] + [\frac{n}{p^2}] + \ldots + [\frac{n}{p^m}],$$

m yra mažiausias natūralusis skaičius, su kuriuo teisinga nelygybė $\frac{n}{p^m} < 1$.

$\ominus$

Skaičius $p|n!$, vadinasi skaičiai $2p, 3p, lp$ dalo $n!$, kai l toks, kad $lp \leq n < (l+1)p$. Aišku, kad $l = [n/p]$. Samprotaudami analogiškai nustatome, kad daugiklių, sudarančių skaičių $n!$, kartotinių p^2 yra lygus n/p^2 ir t.t. Šių skaičių suma ir bus ieškomasis pirminio skaičiaus, su kuriuo jis įeina į skaičiaus $n!$ kanoninį skaidinį laipsnis.

$\oplus$

Funkciją, apibrėžtą natūraliųjų skaičių aibėje ir įgyjančią realias reikšmes $f : \mathcal{N} \to \mathcal{R}$ vadinsime *aritmetine funkcija*. Aritmetinę funkciją f vadinsime multiplikatyvia, jeigu:

1. $\exists a \in \mathcal{N}$, kad $f(a) \neq 0$;

2. bet kokiai tarpusavyje pirminių skaičių porai $(a, b) = 1$ teisinga lygybė, $f(ab) = f(a)f(b)$.

Jei funkcija $f(a) = y$ yra multiplikatyvi, tai $f(1) = 1$. (Įrodykite!)

35 Teorema Jei funkcija $f : \mathcal{N} \to \mathcal{R}$ yra multiplikatyvi, ir skaičiaus a kanoninis skaidinys yra

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n},$$

tai

$$\sum_{d|a} f(d) = (1 + f(p_1) + f(p_1^2) + \ldots + f(p_1^{\alpha_1})) \cdot \cdots (1 + f(p_n) + f(p_n^2) + \ldots + f(p_n^{\alpha_n}).$$

$\ominus$

Panagrinėkime skaičiaus a daliklius. Prisiminkime, kad skaičiaus a visus daliklius galima užrašyti tokiu būdu:

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n},\ 0 \le \beta_i \le \alpha_i,\ \ i = 1; \ldots, n.$$

Atskliaudę dešiniąją teoremos formuluotėje pateiktos lygybės pusę ir naudodamiesi funkcijos multiplikatyvumo savybe gausime tokių daugiklių sumą:

$$f(p_1^{\beta_1}) f(p_2^{\beta_2}) \ldots f(p_n^{\beta_n}) = f(p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}),\ \ 0 \le \beta_i \le \alpha_i,\ \ i = 1; \ldots, n.$$

Susumavę gauname:

$$\sum_{0 \le \beta_1, \ldots \beta_n \le \alpha_n} f(p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta}) = \sum_{d|a} f(d).$$

$\oplus$

Sakykime, kad $n \in \mathcal{N}$. Tada natūraliųjų skaičių, neviršijančių n ir tarpusavyje pirminių su n skaičių žymėsime simboliu $\phi(n) = |1 \le m < n,\ (m, n) = 1|$. Ši funkcija yra vadinama Oilerio funkcija. Tokiu būdu apibrėžta aritmetinė funkcija yra multiplikatyvi, t.y. jei $(m, n) = 1$, tai $\phi(nm) = \phi(n)\phi(m)$. Nesunku suprasti, kad $\phi(p) = p - 1$ ir $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Remiantis Oilerio funkcijos multiplikatyvumo savybe, bei aukščiau padarytomis pastabomis gauname, kad

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k}),$$

kai

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

Sakysime, kad skaičius a lygsta skaičiui b moduliu m, žymėsime $a \equiv b \mathrm{mod} m$, jei skaičius $m|a - b$. Kitaip tariant, egzistuoja skaičius $l \in \mathcal{N}$, kad $a = b + lm$.

Skaitytojui siūlome įrodyti pateiktas lyginių savybes.

1. Jei $a \equiv b \mathrm{mod} m$ ir $b \equiv c \mathrm{mod} m$, tai $a \equiv c \mathrm{mod} m$.
2. Jei $a \equiv b \mathrm{mod} m$ ir $d \equiv c \mathrm{mod} m$, tai $a + d \equiv c + b \mathrm{mod} m$.
3. Jei $a \equiv b \mathrm{mod} m$ ir $d \equiv c \mathrm{mod} m$, tai $ad \equiv cb \mathrm{mod} m$.
4. Jei $d \in \mathcal{N}_0$, ir $a \equiv b \mathrm{mod} m$, tai $ad \equiv db \mathrm{mod} m$ arba $ad \equiv db \mathrm{mod} dm$.
5. Sakykime, kad $d|a, d|b, (d, m) = 1$. Jei $a \equiv b \mathrm{mod} m$, tai $\frac{a}{d} \equiv \frac{d}{b} \mathrm{mod} m$.

6. Sakykime, kad $d|a, d|b, d|m$. Jei $a \equiv b \mathrm{mod} m$, tai $\frac{a}{d} \equiv \frac{d}{b} \mathrm{mod} m$.

7. Sakykime, kad $d|m$. Jei $a \equiv b \mathrm{mod} m$, tai $a \equiv b \mathrm{mod} d$.

Tarkime, kad skaičiai a, b yra nemažesni negu m, ir skaičius $a \equiv b \mathrm{mod} m$. Tada, dalijant skaičių a iš m ir b iš m gausime tą pačią liekaną. Todėl, jei $a \equiv b \mathrm{mod} m$ tai sakysime, kad skaičiai a ir b priklauso tai pačiai liekanų klasei. Tarkime, kad modulis m fiksuotas. Tada naudojantis dalybos su liekana teorema galime teigti, kad dalijant natūraliuosius skaičius iš m gausime liekanas $0 \leq r \leq m-1$. Taigi, iš viso yra lygiai m skirtingų liekanų klasių.

36 Teorema Sakykime, kad $(a, m) = 1$. Jei x įgyja visas natūraliųjų skaičių intervalo $[0, m-1]$ reikšmes, tai tiesinė funkcija $f(x) = ax + b$ taip pat įgyja visas šio intervalo reikšmes, $E(f) = \{0, 1, \ldots, m-1\}$, $\forall b \in \mathcal{N}$.

$\ominus$

Pakanka parodyti, kad skirtingiems skaičiams x_1, x_2 iš nurodyto intervalo, funkcijos reikšmės $f(x_1)$ ir $f(x_2)$ priklauso skirtingoms liekanų klasėms moduliu m.

Tarkime priešingai, t.y. kad $ax_1 + b \equiv ax_2 + b \mathrm{mod} m$. Iš pastarosios lygybės gauname, kad $ax_1 \equiv ax_2 \mathrm{mod} m$. Naudodamiesi 5. savybe gauname prieštaravimą, t.y. $x_1 \equiv x_2 \mathrm{mod} m$.

$\oplus$

Sakykime, kad nagrinėjame liekanų klases moduliu m. Tada visos liekanų klasės, kurios tarpusavyje pirminės su moduliu, sudaro liekanų aibės poaibį, moduliu m, kurį vadinsime redukuota liekanų klase moduliu m. Nesunku suprasti, kad redukuotoje liekanų klasėje yra tiek elementų, kiek yra skaičių aibėje $\{0, 1, \ldots, m-1\}$, kurie tarpusavyje pirminiai su skaičiumi m. Bet jau žinome, kad šis skaičius yra lygus Oilerio funkcijos reikšmei $\phi(m)$.

Įrodysime Oilerio teoremą.

37 Teorema Tarkime, kad $m > 1$ ir $(a, m) = 1$. Tada

$$a^{\phi(m)} \equiv 1 \mathrm{mod} m.$$

$\ominus$

Tarkime, kad $x_1, \ldots, x_{\phi(m)}$ yra redukuota liekanų sistema. Tada, naudodamiesi 3 teorema gauname, kad ir skaičiai $ax_1 \equiv r_1 \mathrm{mod} m, \ldots, ax_{\phi(m)} \equiv r_{\phi(m)} \mathrm{mod} m$ sudaro redukuotą liekanų sistemą.

Naudodamiesi 3. savybe gauname, kad

$$ax_1 ax_2 \ldots ax_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \mathrm{mod} m.$$

Kadangi $x_1 \ldots x_{\phi(m)} = r_1 \ldots r_{\phi(m)}$, tai padaliję paskutiniosios modulinės lygybės abi puses iš sandaugų gausime teoremos įrodymą.

$\oplus$

Išvados

1. Tarkime, kad $m > 1$ ir $(a, m) = 1$. Tada

$$a^{p-1} \equiv 1 \mathrm{mod} m.$$

2. Tarkime, kad $m > 1$. Tada

$$a^p \equiv a \mathrm{mod} m.$$

Tarkime, kad $m > 1$ yra fiksuotas modulis. Sakysime, kad skaičius r yra atvirkštinis skaičiui q moduliu m, jei $rq \equiv 1 \mathrm{mod} m$. Remiantis 4 teorema galime tvirtinti, kad jei $(a, m) = 1$, tai elemento a atvirkštinis moduliu m yra lygus $a^{\phi(m)-1}$.

Uždaviniai

1. Naudodami matematinės indukcijos metodą įrodykite, kad

$$1) \quad 1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}$$

$$2) \quad 1 + 3 + 5 + \ldots + (2n-1) = n^2$$

$$3) \quad (1+p)^k > 1 + kp$$

$$4) \quad 2^n > n^2.$$

2. Naudodami indukcijos metodą įrodykite, kad koks bebūtų natūralusis skaičius n, teisingi dalumo sąryšiai:

$$6|14n^3 + 9n^2 + n; \quad 133|11^{n+2} + 12^{2n+1}, \quad 13|3^3 - 3^6 + 3^9 - \ldots - 3^{6n}.$$

3. Nurodykite aibės $\mathcal{N}$ poaibius A, B, kurie turi savybes:

$$A \sim B \sim \mathcal{N}, \; \mathcal{N} \setminus A \sim \mathcal{N},$$

be to aibė $\mathcal{N} \setminus B$ yra baigtinė.

4. Nustatykite kuriuos iš pateiktųjų skaičių dalo skaičiai $3, 4, 5, \quad 9, 12, 15$:

$$245862, 69512, 495315, 364212, 9875415, 4567824.$$

5. Parodykite, kad šešiaženklis skaičius *abcabc* yra dalus iš $7, 11$.

6. Naudodami Euklido algoritmą, raskite pateiktų skaičių porų d.b.d.:

$$425, 2135; \quad 12516, 9459; \quad 1224, 4224, \quad 3553, 527.$$

7. Raskite skaičių porų $1245, 545$; ir $3456, 981$ bendrus mažiausius kartotinius. Be to raskite d.b.d. $(7245, 5445, 145, 9135)$ ir m.b.k. $[7245, 5445, 145, 9135]$.

8. Raskite skaičių $16245, 591445, 243145, 972135$ kanoninius skaidinius. Remdamiesi šiais skaidiniais raskite pateiktų skaičių m.b.k. ir d.b.d..

9. Naudodami Ferma algoritmą, faktorizuokite skaičius:
2881, 135337, 236273, 438359, 2091589.

10. Įrodykite liekanų klasių 1-7 savybes.