

20. Aritmeetika põhiteoreem. Jagajad

Teoreem 20.1 (Aritmeetika põhiteoreem) Iga naturaalarv $n \geq 2$ esitub algarvude korrutisena. See esitus on algtegurite järjekorra täpsusega ühene.

Tõestus. Näitame kõigepealt, et iga naturaalarv $n \geq 2$ esitub algarvude korrutisena. Selleks kasutame tugevat matemaatilist induktsiooni. Baasjuhul $n = 2$ on väide ilmne, sest 2 on ise algarv. Sammu tegemiseks eeldame, et väide on tõestatud arvude $2, 3, \dots, k$ jaoks, ja näitame, et see kehtib ka $n = k + 1$ korral.

Kui n on algarv, siis on väide jälle triviaalselt tõene. Kui aga n on kordarv, siis peab ta esituma kujul $n = a \cdot b$, kus $1 < a, b < n$ ehk $2 \leq a, b \leq k$. Nüüd saame aga a ja b jaoks rakendada induktsiooni eeldust ning leida nende esitused algarvude korrutisena. Olgu need esitused vastavalt $a = p_1 \cdot p_2 \cdot \dots \cdot p_s$ ja $b = q_1 \cdot q_2 \cdot \dots \cdot q_t$. Siis

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_s \cdot q_1 \cdot q_2 \cdot \dots \cdot q_t,$$

mis annabki arvu n esituse algarvude korrutisena.

Näitame nüüd, et kõigi naturaalarvude esitus algtegurite korrutisena on ühene (kui mitte arvestada võimalikku tegurite ümberjärjestamist). Oletame vastuväiteliselt, et see väide ei kehti ja olgu k vähim niisugune arv, millel leidub kaks erinevat esitust algtegurite korrutisena. (Selline arv k leidub tänu languse printsiibile, vt jaotist 2.) Vastuolu saavutamiseks konstrueerime arvust k rangelt väiksema naturaalarvu, millel on sama omadus.

Olgu arvu k esitused algtegurite korrutisena vastavalt

$$k = p_1 \cdot p_2 \cdot \dots \cdot p_s \quad \text{ja} \quad k = q_1 \cdot q_2 \cdot \dots \cdot q_t.$$

Olgu p_1 vähim kummaski esituses esinevatest algarvudest (kui vähim algtegur on mõni q_i , vahetame need kaks esitust omavahel ära).

Kõigepealt näeme, et p_1 ei esine teguritekslahutuses $q_1 \cdot q_2 \cdot \dots \cdot q_t$. Tõepoolest, kui näiteks $p_1 = q_1$, oleks arvul $\frac{k}{p_1}$ kaks erinevat esitust algtegurite korrutisena $p_2 \cdot \dots \cdot p_s$ ja $q_2 \cdot \dots \cdot q_t$. Saame vastuolu, sest $\frac{k}{p_1} < k$.

Järelikult $p_1 < q_1$. Vaatleme nüüd arvu

$$\ell = (q_1 - p_1) \cdot q_2 \cdot \dots \cdot q_t.$$

Kuna $p_1 > 0$, siis ilmselt kehtib $\ell < k$. Positiivne tegur $q_1 - p_1$ võib ise olla kordarv, aga tema tegurite hulgas ei saa olla algarvu p_1 , sest kui $q_1 - p_1 : p_1$, siis ka $q_1 : p_1$. Saame vastuolu, sest p_1 ja q_1 on mõlemad algarvud, aga $p_1 \neq q_1$.

Teisest küljest aga

$$\begin{aligned}\ell &= (q_1 - p_1) \cdot q_2 \cdot \dots \cdot q_t = q_1 \cdot q_2 \cdot \dots \cdot q_t - p_1 \cdot q_2 \cdot \dots \cdot q_t = \\ &= k - p_1 \cdot q_2 \cdot \dots \cdot q_t = p_1 \cdot p_2 \cdot \dots \cdot p_s - p_1 \cdot q_2 \cdot \dots \cdot q_t = \\ &= p_1 \cdot (p_2 \cdot \dots \cdot p_s - q_2 \cdot \dots \cdot q_t).\end{aligned}$$

Niisiis leidub arvul ℓ kaks erinevat teguriteklahutust – üks, milles ei leidu algtegurit p_1 ja teine, milles see algtegur esineb. Kuna $\ell < k$, oleme saanud vastuolu arvu k valikuga. \square

Toodud tõestuse võib leida ka Elts Abeli ja Raili Vildi õpikust [3]. Veidi teistsuguse konstruktsiooni annab Reimo Palmi koostatud õpik [12], mida huvitatud lugejal samuti uurida soovitan.

Aritmeetika põhiteoreem ütleb, et igal naturaalarvul $n \geq 2$ leidub ühene *kanooniline esitus* algtegurite astmete korrutisena

$$p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s},$$

kus p_1, p_2, \dots, p_s on erinevad algarvud mingis kindlas (nt kasvavas) järjekorras ja astendajad a_i on positiivsed täisarvud.

Matemaatikavõistlustel läheb sageli vaja naturaalarvu arvu jagajate arvu. Seda võimaldab leida järgmine teoreem.

Teoreem 20.2 Olgu naturaalarvu n kanooniline esitus $p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$. Siis tema positiivsete jagajate arv on

$$(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_s + 1).$$

Tõestus. Arvu n kõik positiivsed jagajad esituvad parajasti kujul

$$p_1^{b_1} \cdot p_2^{b_2} \cdot \dots \cdot p_s^{b_s},$$

kus $0 \leq b_i \leq a_i$ ($i = 1, 2, \dots, s$). Muuhulgas näiteks valik $b_1 = b_2 = \dots = b_s = 0$ annab jagaja 1 ning valik $b_i = a_i$ iga $i = 1, 2, \dots, s$ jaoks annab jagaja n .

Iga astendaja b_i valikuks on $a_i + 1$ võimalust ja iga astendajatekomplekti valik annab arvu n erineva jagaja. Kõiki astendajatekomplekti valiku võimalusi (ja järelikult erinevaid positiivseid jagajaid) on seega täpselt $(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_s + 1)$. \square

■ **Näide 20.1** Arvu $72 = 2^3 3^2$ kõik $(3 + 1) \cdot (2 + 1) = 12$ positiivset jagajat on

$$\begin{array}{cccc} 2^0 3^0 = 1 & 2^1 3^0 = 2 & 2^2 3^0 = 4 & 2^3 3^0 = 8 \\ 2^0 3^1 = 3 & 2^1 3^1 = 6 & 2^2 3^1 = 12 & 2^3 3^1 = 24 \\ 2^0 3^2 = 9 & 2^1 3^2 = 18 & 2^2 3^2 = 36 & 2^3 3^2 = 72 \end{array}$$

■

Ülesanne 20.1 (Sügisene lahtine võistlus 2016, noorem rühm) Kas leidub selline positiivne täisarv n , millel on täpselt 9 positiivset tegurit ja mille kõik tegurid saab paigutada 3×3 tabelina nii, et igas reas, igas veerus ja kummalgi diagonaalil olevate

arvude korrutis oleks sama?

Lahendus. Teoreemi 20.2 põhjal peame tegurite arvu 9 esitama korrutisena $(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_s + 1)$. Selleks on kaks võimalust: $9 = 8 + 1$ ja $9 = (2 + 1) \cdot (2 + 1)$. Niisiis saavad lahendiks olla ainult arvud kujul p^8 ja $p^2 q^2$ mingite algarvude p ja q ($p \neq q$) jaoks. Mõlemad võimalused annavad lahendi. Näiteks arvu $n = p^2 q^2$ tegurid saab tabelisse paigutada nii:

$p^2 q^1$	$p^0 q^0$	$p^1 q^2$
$p^0 q^2$	$p^1 q^1$	$p^2 q^0$
$p^1 q^0$	$p^2 q^2$	$p^0 q^1$

Seline paigutus annab iga rea, veeru ja diagonaali elementide korrutiseks $p^3 q^3$. Arvu p^8 jagajate paigutamise 3×3 tabelisse jätame lugeja ülesandeks.

Naturaalarvu esitust kanoonilisel kujul saab üldistada kõigile nullist erinevatele täisarvudele, kui vaadelda ka arvu märki. Kui lisaks lubada astendajatel võtta negatiivseid väärtusi, saame kõigi nullist erinevate ratsionaalarvude kanoonilise esituse algarvude astmete korrutisena.¹

Ülesanne 20.2 (Piirkonnavoor 2017, 10. klass) Leia kõik täisarvude paarid (x, y) , mille korral

$$324^{x+y} = 2^{x-y} \cdot 3^{x-3} \cdot 4^{y-4}.$$

Lahendus. Vastus: ainus lahend on $(-29, 21)$.

Kuna $324 = 2^2 3^4$, saame ratsionaalarvu kanoonilise esituse ühesusest 2-e ja 3-e astendajate jaoks vastavalt võrrandid

$$\begin{aligned} 2(x+y) &= x-y+2(y-4) = x+y-8, \\ 4(x+y) &= x-3. \end{aligned}$$

Esimesest võrrandist saame $x+y = -8$ ning seda võrdust teise võrrandisse asendades $-32 = x-3$ ehk $x = -29$. Et $x+y = -8$, järeldub siit ka $y = 21$.

Ülesanded

Ülesanne 20.3 (Piirkonnavoor 1999, 11. klass) Antud on arvupaarid $(1, 1999)$, $(2, 1998)$, $(3, 1997)$, \dots , $(1998, 2)$, $(1999, 1)$. Mitmes paaris jagub esimene arv teisega?

Ülesanne 20.4 (Lõppvvoor 1998, 12. klass) Leia kõik algarvud kujul $10101\dots 01$.

Ülesanne 20.5 (Lõppvvoor 2002, 12. klass) Kas arv, mis koosneb ainult numbritest 2 ja 0, võib olla mingi positiivse täisarvu k -s aste, kus $k \geq 2$?

Ülesanne 20.6 (Lõppvvoor 1994, 10. klass) Leia vähim naturaalarv, millel on täpselt 100 erinevat naturaalarvulist jagajat (arvu jagajateks loeme ka selle arvu enda ja arvu 1).

¹Mõlemal juhul on lisaks erandid 1 ja -1 ; nende esitamiseks peame lubama olukorda, kus kõigi algarvude astendajad on 0-d. Ega sellest midagi hullu ei juhtugi, lihtsalt esituse ühesust tuleb sel juhul hoolikamalt käsitleda.

Ülesanne 20.7 (Lõppvoor 2003, 10. klass) Leia avaldise $\frac{m^2 + n^2}{mn}$, kus m ja n on täisarvud, kõik võimalikud täisarvulised väärtused.

Ülesanne 20.8 (Lõppvoor 2012, 11. klass) Professor P uuris oma viimases teadustöös teatava omadusega naturaalarve. On teada, et alati, kui mingil naturaalarvul x on see omadus, on arvu x kõigil kordsetel samuti see omadus.

Olgu a_1, \dots, a_n sellised positiivsed täisarvud, mille kõigil ühest suurematel teguritel on professori P uuritud omadus. Kas võib kindlalt väita, et siis ka korrutise $a_1 \cdot \dots \cdot a_n$ kõigil ühest suurematel teguritel on see omadus?

Ülesanne 20.9 (Lõppvoor 2009, 11. klass) Positiivne täisarv n on selline, et nii $n - 1$ kui ka $n + 1$ on algarvud, kusjuures $n > 18$. Tõesta, et arv n jagub vähemalt 8 erineva positiivse täisarvuga.

Ülesanne 20.10 (Lõppvoor 2005, 11. klass) Täisarvud a, b ja n on sellised, et arv $a + b$ jagub arvuga n ning arv $a^2 + b^2$ jagub arvuga n^2 . Tõesta, et arv $a^m + b^m$ jagub arvuga n^m suvalise positiivse täisarvu m korral.

Ülesanne 20.11 (Piirkonnavor 1993, 12. klass) Tähistagu $d(n)$ naturaalarvu n kõigi positiivsete jagajate arvu. Leia piirväärtus $\lim_{n \rightarrow \infty} \frac{d(n)}{n}$.

Lahendused

20.3 Vastus: 19.

Ülesande arvupaarid on kujul $(2000 - n, n)$, kus $n = 1, 2, \dots, 1999$. Tingimus $2000 - n : n$ tähendab, et leidub täisarv $m \geq 1$, mille korral $2000 - n = mn$ ehk $2000 = (m + 1)n$. Niisiis sobivad parajasti sellised m väärtused, mille korral $m + 1$ on arvu 2000 jagaja, kusjuures $m + 1 \geq 2$.

Arvu 2000 kanooniline esitus algtegurite astmete korrutisena on $2^4 \cdot 5^3$, järelikult on tal teoreemi 20.2 põhjal $(4 + 1) \cdot (3 + 1) = 20$ positiivset jagajat. Neist üks on 1, seega rahuldab ülesande tingimusi 19 väärtust.

20.4 Vastus: 101 on ainus nõutud kujul algarv.

Tekstis pole küll üheselt mõistetavalt öeldud, kas arv 1 vastab ülesande tingimustele, aga isegi kui vastab, siis pole tegemist algarvuga. 101 jällegi on algarv.

Kui ülesande arvus on k numbrit 1, avaldub ta kujul

$$1 + 100^1 + 100^2 + \dots + 100^{k-1}.$$

Selles avaldises tunneme ära geomeetrilise rea summa, mistõttu saame tema väärtuseks

$$\frac{100^k - 1}{100 - 1} = \frac{(10^2)^k - 1}{99} = \frac{(10^k)^2 - 1}{99} = \frac{(10^k - 1)(10^k + 1)}{99}.$$

Kuna tegemist on täisarvuga, peavad algtegurid 3, 3 ja 11 esinema kusagil arvude $10^k - 1$ ja $10^k + 1$ kanoonilistes esitustes.

Kui $k \geq 3$, kehtivad võrratused $10^k - 1 > 99$ ja $10^k + 1 > 99$. Seega kuidas iganes ka ei jaguneks algtegurid 3, 3 ja 11 tegurite $10^k - 1$ ja $10^k + 1$ kanooniliste esituste

vahel, jääb pärast taandamist mõlemast tegurist järele 1-st suurem arv. Järelikult peab uuritav arv olema kordarv.

20.5 Vastus: ei.

Olgu m ja n sellised positiivsed täisarvud, et $m^k = n$, ning vaatleme nende kanoonilisi esitusi algarvude astmete korrutisena. Kui

$$m = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot \dots, \quad \text{siis} \quad n = 2^{ka_1} \cdot 3^{ka_2} \cdot 5^{ka_3} \cdot \dots$$

Väidame, et kui n koosneb ainult numbritest 2 ja 5, siis peab algarvu 2 aste tema kanoonilises esituses olema täpselt 1 võrra suurem kui algarvu 5 aste. Olgu arvu n lõpus ℓ nulli. Arv n esitub siis kujul

$$2 \dots \underbrace{200 \dots 0}_{\ell} = 2 \dots 2 \cdot 10^{\ell} = 1 \dots 1 \cdot 2 \cdot 10^{\ell}.$$

Näeme, et algarvude 2 ja 5 astendajad kanoonilises esituses on vastavalt $\ell + 1$ ja ℓ . See aga on vastuolu, sest teisest küljest peaksid need astendajad olema ka_1 ja ka_3 mingi täisarvu $k \geq 2$ jaoks, mis on võimatu.

20.6 Teoreemi 20.2 põhjal peame tegurite arvu 100 esitama korrutisena $(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_s + 1)$. Selleks on üheksa võimalust:

$$\begin{aligned} &99 + 1, (49 + 1) \cdot (1 + 1), (24 + 1) \cdot (3 + 1), (24 + 1) \cdot (1 + 1) \cdot (1 + 1), \\ &(19 + 1) \cdot (4 + 1), (9 + 1) \cdot (9 + 1), (9 + 1) \cdot (4 + 1) \cdot (1 + 1), \\ &(4 + 1) \cdot (4 + 1) \cdot (3 + 1), (4 + 1) \cdot (4 + 1) \cdot (1 + 1) \cdot (1 + 1). \end{aligned}$$

Korrutisele $(a_1 + 1) \cdot (a_2 + 1) \cdot \dots \cdot (a_s + 1)$ (kus $a_1 \geq a_2 \geq \dots \geq a_s$) vastav kanooniline esitus $p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_s^{a_s}$ on minimaalne, kui $p_1 = 2, p_2 = 3, p_3 = 5$ jne on esimesed algarvud kasvavas järjekorras. Niisiis on vastusekandidaatideks

$$2^9 9, 2^{49} 3^1, 2^{24} 3^3, 2^{24} 3^1 5^1, 2^{19} 3^4, 2^9 3^9, 2^9 3^4 5^1, 2^4 3^4 5^3, 2^4 3^4 5^1 7^1.$$

Nende seast osutub kõige väiksemaks $2^4 3^4 5^1 7^1 = 45360$.

20.7 Vastus: 2 ja -2 .

Näitame, et kui $\frac{m^2 + n^2}{mn}$ on täisarv, peavad kõigi algarvude astmed arvude m ja n kanoonilistes esitustes olema samad.

Oletame vastuväiteliselt, et leidub algarv p , mille astendajad arvude m ja n kanoonilistes esitustes on vastavalt a ja b , kusjuures olgu üldisust kitsendamata $a > b$. Siis $mn \div p^{a+b}$ ja $m^2 \div p^{2a} \div p^{a+b}$, aga $n^2 \not\div p^{a+b}$. Järelikult ei saa $\frac{m^2 + n^2}{mn}$ olla täisarv; vastuolu.

Järelikult on ainult kaks võimalust, kas $m = n$ või $m = -n$. Need võimalused annavad avaldise $\frac{m^2 + n^2}{mn}$ väärtusteks vastavalt 2 ja -2 .

20.8 Vastus: jah, võib küll.

Vaatleme korrutise $a_1 \cdot \dots \cdot a_n$ suvalist ühest suuremat tegurit m . Arv m ei pruugi ise olla ühegi arvu a_i jagajaks, sest tema algtegurid võivad pärineda erinevatest arvudest a_i . Küll aga saame aritmeetika põhiteoreemi alusel väita, et arvu m iga algtegur p peab jagama mõnda arvudest a_i . Siis aga on uuritav omadus nii algarvul p kui ka selle algarvu kordsel m .

20.9 Kolmest järjestikusest arvust vähemalt üks jagub 2-ga ja vähemalt üks 3-ga. Kuna $n - 1$ ja $n + 1$ on vähemalt kahekohalised algarvud, peab n jaguma nii 2-ga kui 3-ga. Kui n -il on veel mõni 3-st suurem algtegur, on tal vähemalt kolm algtegurit ja seega vähemalt $(1 + 1) \cdot (1 + 1) \cdot (1 + 1) = 8$ positiivset jagajat.

Jääb üle vaadelda juhtu, kui 2 ja 3 on arvu n ainsad algtegurid. Kui vähemalt ühe aste arvu n teguritekslahutuses on 3, on arvul n jälle vähemalt $(3 + 1) \cdot (1 + 1) = 8$ positiivset jagajat. Kui $n = 2^2 3^2$, siis on tal $(2 + 1) \cdot (2 + 1) = 9 > 8$ positiivset jagajat. Arvud $2^1 3^1$, $2^1 3^2$ ja $2^2 3^1$ aga ei sobi, sest ükski neist pole suurem kui 18.

20.10 Näitame, et ülesande tingimustest järelneb $a : n$ ja $b : n$.

Kuna $(a + b)^2 : n^2$ ja $a^2 + b^2 : n^2$, saame, et n^2 -ga peab jaguma ka nende vahe $(a + b)^2 - (a^2 + b^2) = 2ab$.

Olgu p suvaline algarv, mis esineb arvu n kanoonilises esituses algarvude korrutisena, ning olgu k tema aste selle esituses. Kuna $2ab : n^2$, peab p aste arvu $2ab$ kanoonilises esituses olema vähemalt $2k$ ning arvu ab kanoonilises esituses vähemalt $2k - 1$. Järelikult on p aste kas a või b kanoonilises esituses vähemalt k . Kuna aga $a + b : n : p^k$, peab p aste nii a kui b kanoonilises esituses olema vähemalt k .

Kuivõrd see arutelu kehtib kõigi algarvude p korral, saame järeldada, et $a : n$ ja $b : n$. Järelikult ka $a^m : n^m$, $b^m : n^m$ ja $a^m + b^m : n^m$.

20.11 Arvu n positiivsed tegurid saab jagada paaridesse, mille elementide korrutis on n (välja arvatud juhul kui n on täisruut, aga see ei muuda edasist lahendust). Kuna paari väiksem element ei ületa \sqrt{n} , on teguripaare kokku ülimalt \sqrt{n} ja järelikult $d(n) \leq 2\sqrt{n}$. Siit saame omakorda, et $\frac{d(n)}{n} \leq \frac{2}{\sqrt{n}}$, millest tuleneb $\lim_{n \rightarrow \infty} \frac{d(n)}{n} = 0$.