24. Euleri teoreem ja Fermat' väike teoreem

Olgu antud täisarv $n \geqslant 2$. Vaatleme kõiki arve hulgast $\{1, 2, \ldots, n\}$, mis on arvuga n ühistegurita. Selliste arvude hulka tähistatakse $\mathbb{Z}_n^*$; niisiis näiteks $\mathbb{Z}_5^* = \{1,2,3,4\}$ ja $\mathbb{Z}_{10}^* = \{1,3,7,9\}$.

Hulkadel $\mathbb{Z}_n^*$ on üks väga huvitav omadus. Kui võtame suvalise $x \in \mathbb{Z}_n^*$, korrutame ta läbi hulga $\mathbb{Z}_n^*$ kõigi elementidega (sealhulgas iseendaga!) ja leiame korrutiste jäägid jagamisel n-ga, saame uuesti kätte kõik hulga $\mathbb{Z}_n^*$ elemendid, igaühe ühe korra.

Näiteks valides $7 \in \mathbb{Z}_{10}^*$, leiame

$$\begin{aligned} 7 \cdot 1 &\equiv 7 \bmod 10, \\ 7 \cdot 3 &\equiv 1 \bmod 10, \\ 7 \cdot 7 &\equiv 9 \bmod 10, \\ 7 \cdot 9 &\equiv 3 \bmod 10. \end{aligned}$$

Harjutus 24.1 Vali veel mõni täisarv $n \geqslant 2$ ja $x \in \mathbb{Z}_n^*$ ning kontrolli ülaltoodud omaduse kehtivust.

Tõestame, et see omadus kehtib ka üldiselt. Olgu meil siis antud täisarv $n \geqslant 2$ ja hulgas $\mathbb{Z}_n^*$ mingi fikseeritud element x.

Valime samast hulgast veel ühe elemendi y (võib olla $y = x$) ning kontrollime kõigepealt, et $x \cdot y \bmod n \in \mathbb{Z}_n^*$. Kuna $x, y \in \mathbb{Z}_n^*$, siis on nad mõlemad n-iga ühistegurita. Järelikult on n-iga ühistegurita ka arv $x \cdot y$. Arvu $x \cdot y \bmod n$ definitsiooni järgi kehtib võrdus

$$x \cdot y \bmod n = x \cdot y - t \cdot n$$

mingi täisarvu t korral. Kui arvul $x \cdot y \bmod n$ oleks n-iga ühine tegur d, peaks see tegur jagama ka summat

$$x \cdot y \bmod n + t \cdot n = x \cdot y;$$

vastuolu, sest $x \cdot y$ on n-iga ühistegurita. Muuhulgas $x \cdot y \not\vdots n$, seega $x \cdot y \bmod n \neq 0$. Kokkuvõttes olemegi näidanud, et $x \cdot y \bmod n \in \mathbb{Z}_n^*$.

Näitame nüüd, et kui $y_1 \neq y_2$, siis ka $x \cdot y_1 \bmod n \neq x \cdot y_2 \bmod n$. Oletame vastuväiteliselt, et $x \cdot y_1 \equiv x \cdot y_2 \bmod n$. Järelikult $x \cdot (y_1 - y_2) \equiv 0 \bmod n$ ehk $x \cdot (y_1 - y_2) \vdots n$. Kuna

x on n-iga ühistegurita, järeldub siit $y_1 \equiv y_2 \bmod n$. Kuna aga y_1 ja y_2 on mõlemad hulgast $\mathbb{Z}_n^*$, saame $y_1 = y_2$; vastuolu.

Niisiis on kõik korrutised $x \cdot y_i \bmod n$ (kus y_i võtab kõik väärtused hulgast $\mathbb{Z}_n^*$) erinevad. Kuna $\mathbb{Z}_n^*$ on lõplik hulk, on kõik tema elemendid muuhulgas saavutatavad kujul $x \cdot y_i \bmod n$.

Olgu $\mathbb{Z}_n^* = \{y_1, y_2, \ldots, y_k\}$. Siis oleme näidanud, et suvalise fikseeritud $x \in \mathbb{Z}_n^*$ korral kehtib

$$\{x \cdot y_1 \bmod n, x \cdot y_2 \bmod n, \ldots, x \cdot y_k \bmod n\} = \{y_1, y_2, \ldots, y_k\}\,.$$

Tuletame meelde, et elementide järjestus pole hulga puhul oluline. Teisest küljest ei sõltu ka korrutise väärtus tegurite järjekorrast, niisiis saame tuletada järgmised seosed:

$$\begin{aligned} x \cdot y_1 \cdot x \cdot y_2 \cdot \ldots \cdot x \cdot y_k &\equiv y_1 \cdot y_2 \cdot \ldots \cdot y_k \bmod n\,, \\ x^k \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_k &\equiv y_1 \cdot y_2 \cdot \ldots \cdot y_k \bmod n\,, \\ (x^k - 1) \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_k &\equiv 0 \bmod n\,, \end{aligned}$$

järelikult $(x^k - 1) \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_k \vdots n$. Kuna arvud $y_1, y_2, \ldots, y_k$ on kõik n-iga ühistegurita, peab järelikult kehtima ka seos $x^k - 1 \vdots n$ ehk $x^k \equiv 1 \bmod n$, kus k on hulga $\mathbb{Z}_n^*$ elementide arv.

Kuna arvul $|\mathbb{Z}_n^*|$ on arvuteoorias tähtis roll, on selle jaoks kasutusele võetud eraldi tähis $\varphi(n)$. Funktsiooni φ tuntakse ka *Euleri funktsiooni*[1] nime all.

Kokkuvõtteks oleme tõestanud järgmise teoreemi.

Teoreem 24.1 (Euleri teoreem) Olgu antud täisarv $n \geqslant 2$ ja temaga ühistegurita arv x. Siis kehtib seos

$$x^{\varphi(n)} \equiv 1 \bmod n\,.$$

▪ **Näide 24.1** Eelpool nägime, et $\varphi(10) = 4$. Kontrollime Euleri teoreemi kehtivust hulga $\mathbb{Z}_{10}^*$ kõigi elementide jaoks:

$$\begin{aligned} 1^4 &= 1 \equiv 1 \bmod 10\,, \\ 3^4 &= 81 \equiv 1 \bmod 10\,, \\ 7^4 &= 2401 \equiv 1 \bmod 10\,, \\ 9^4 &= 6561 \equiv 1 \bmod 10\,. \end{aligned}$$

▪

Ülesanne 24.1 (Lõppvoor 2000, 11. klass) Leia kõik algarvud, mille kuues aste ei anna 504-ga jagades jäägiks 1.

Lahendus. Vastus: 2, 3 ja 7.

Avaldades arvu 504 algtegurite korrutisena leiame, et $504 = 7 \times 8 \times 9$. See tähendab, et arvude 2, 3 ja 7 kuuenda astme jääk jagamisel 504-ga peab samuti jaguma vastavalt 2-e, 3-e ja 7-ga. Niisiis ei saa see jääk neil juhtudel olla 1.

Kõigi teiste algarvude p puhul saame kasutada Euleri teoreemi. Paneme tähele, et $\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ ja $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$, järelikult $\varphi(7) = 6$ ja $\varphi(9) = 6$. Kuna

[1] Leonhard Euler oli 18. sajandi šveitsi matemaatik, füüsik, astronoom ja insener, kes on pannud aluse paljudele tänapäevase matemaatika harudele.

$p \notin \{2,3,7\}$, saame Euleri teoreemi põhjal

$$p^6 \equiv 1 \bmod 7 \text{ ja}$$
$$p^6 \equiv 1 \bmod 9$$

ehk $p^6 - 1 \vdots 7$ ja $p^6 - 1 \vdots 9$. Aga $n = 8$ jaoks $\mathbb{Z}_8^* = \{1,3,5,7\}$, millest järeldub $\varphi(8) = 4$ ja eelpooltooduga analoogiliselt saame, et $p^4 - 1 \vdots 8$. See pole päris see, mis vaja, sest vaja oleks $p^6 - 1 \vdots 8$. Mida teha?

Siinkohal tuleb appi vana ja lihtne tulemus, mille järgi iga paaritu arvu ruudu jääk jagamisel 8-ga on 1. Tõepoolest, tõstes paaritu arvu $2m+1$ ruutu, saame

$$(2m+1)^2 = 4m^2 + 4m + 1 = 4m(m+1) + 1\,.$$

Kuna arvudest m ja $m+1$ on üks paaris, jagub $4m(m+1)$ 8-ga, mida oligi tarvis. Et p on paaritu algarv siis on ka tema kuup paaritu ja

$$p^6 = (p^3)^2 \equiv 1 \bmod 8\,,$$

millest saamegi $p^6 - 1 \vdots 8$. Kokkuvõttes jagub $p^6 - 1$ nii 7, 8 kui ka 9-ga, järelikult jagub ta ka nende korrutise ehk 504-ga.

Euleri teoreemi tähtsa erijuhu saame, kui n ise on algarv. Siis $\mathbb{Z}_n^* = \{1,2,\ldots,n-1\}$ ja järelikult $\varphi(n) = n-1$. Niisiis kehtib ka järgmine tulemus, mida nimetatakse Fermat' väikeseks teoreemiks.[2]

Teoreem 24.2 Olgu p algarv ja a mingi täisarv, mis ei jagu p-ga. Sel juhul kehtib seos

$$a^{p-1} \equiv 1 \bmod p\,.$$

Fermat' väikest teoreemi kasutatakse sageli ka veidi teises sõnastuses.

Teoreem 24.3 Kui p on algarv, siis suvalise täisarvu a korral kehtib seos

$$a^p \equiv a \bmod p\,.$$

Tõestus. Kui $a \vdots p$, siis $a \equiv 0 \bmod p$ ja $a^p \equiv 0 \bmod p$, järelikult teoreem sel juhul kehtib.

Kui $a \not\vdots p$, siis saame kasutada teoreemi 24.2, mille alusel $a^{p-1} \equiv 1 \bmod p$. Korrutades selle ekvivalentsi mõlemaid pooli a-ga, saame, et tõestatav väide kehtib ka sellel juhul. □

Teoreemi 24.3 veel ühe tõestuse leiab lugeja jaotisest 24.1.

Euleri teoreem ja Fermat' väike teoreem aitavad meil arvutada suurte arvude suurte astmete jääke. Me juba teame, et $a^b \bmod n$ arvutamiseks tohime me a asendada jäägiga, mis tekib tema jagamisel n-ga (ja seda suvalise positiivse mooduli n korral). Euleri teoreem ütleb meile, et kui a ja n on ühistegurita, tohime me lisaks b asendada jäägiga, mis tekib tema jagamisel $\varphi(n)$-iga. Tõepoolest, paneme tähele, et teoreem 24.1 lubab meil $a^{\varphi(n)}$ asendada arvuga $1 = a^0$, st vähendada astendajat $\varphi(n)$ võrra. Seda operatsiooni võime a^b puhul teha mitu korda, kuni alles jääb ainult b jääk jagamisel $\varphi(n)$-iga.

Kui n on algarv, siis Fermat' väikese teoreemi 24.3 alusel pole isegi vaja kontrollida, et a ja n oleksid ühistegurita, ja astendajat tohib $\varphi(n) = n-1$ järgi taandada igal juhul.

[2] Pierre de Fermat [ferma:] oli 17. sajandi prantsuse matemaatik.

Ülesanne 24.2 (Piirkonnavoor 1993, 10. klass) Tõesta, et $101^{100}-1$ jagub arvuga 24.

Lahendus. 24 on küll kordarv, aga 101 on temaga ühistegurita, niisiis saame rakendada Euleri teoreemi. Selleks tuleb leida $\varphi(24)$. Kuna $24 = 2^3 \cdot 3$, peame hulgast $\{1,2,\ldots,24\}$ jätma välja kõik 2-e ja 3-ga jaguvad elemendid. Saame $\mathbb{Z}_{24}^* = \{1,5,7,11,13,17,19,23\}$, järelikult $\varphi(24) = 8$ ja me tohime astendajat taandada mooduli 8 järgi. Kuna $101 \equiv 5 \bmod 24$ ja $100 \equiv 4 \bmod 8$, saame

$$101^{100} \equiv 5^4 = 625 \equiv 1 \bmod 24\,,$$

millest järeldubki, et $101^{100} - 1 \vdots 24$.

Ülesanded

Ülesanne 24.3 (Talvine lahtine võistlus 2020, vanem rühm) Olgu a täisarv. Tõesta, et $a^{2020} + 10a^{1010} + 1001$ ei ole algarv.

Ülesanne 24.4 (Lõppvoor 2019, 11. klass) Mari kirjutas tahvlile algarvu, mis on suurem kui 10^{17}, aga väiksem kui $10^{17} + 10$. Leia Mari kirjutatud arv.

Ülesanne 24.5 (Lõppvoor 2021, 11. klass) Tõesta, et arv $2021^{2020} + 5$ jagub arvuga 63.

Ülesanne 24.6 (Lõppvoor 2005, 11. klass) Kas leidub selline täisarv $n > 1$, et arv

$$2^{2^n-1} - 7$$

ei ole ühegi täisarvu ruut?

Lahendused

24.3 Proovime leida algarvu, millega ülesande avaldis kindlasti jagub. Paneme tähele, et $1001 = 7 \cdot 11 \cdot 13$. Ülesande avaldises jaguvad muutuja a astmed 10-ga; see tähelepanek viib Fermat' väikesele teoreemile mõeldes ideele proovida jaguvust 11-ga.

Näitame, et ülesande avaldis jagub tõepoolest alati 11-ga. Kuna tema väärtus on iga täisarvu a korral vähemalt 1001, ei saa ta seega olla algarv.

Kui $a \vdots 11$, on tõestatav väide ilmne, sest $1001 \vdots 11$. Kui aga a ei jagu 11-ga, saame teoreemist 24.2, et $a^{10} \equiv 1 \bmod 11$. Järelikult ka $a^{2020} = (a^{10})^{202} \equiv 1 \bmod 11$ ja samuti $a^{1010} = (a^{10})^{101} \equiv 1 \bmod 11$. Kokkuvõttes saame

$$a^{2020} + 10a^{1010} + 1001 \equiv 1 + 10 \cdot 1 + 1001 \equiv 0 \bmod 11\,.$$

24.4 Paarisnumbriga ja 5-ga lõppevad arvud ei saa olla algarvud, seega tuleb läbi vaadata arvud $10^{17}+1$, $10^{17}+3$, $10^{17}+7$ ja $10^{17}+9$.

Arv $10^{17}+1$ rahuldab 11-ga jagumise tunnust ja on järelikult kordarv.

Arvu $10^{17}+7$ jaoks saame Fermat' väikesest teoreemist $10^{17} \equiv 10 \bmod 17$, seega $10^{17} + 7 \equiv 10 + 7 \equiv 0 \bmod 17$.

Arv $10^{17}+9$ ei rahulda 2-ga, 3-ga ega 5-ga jagumise tunnust. 7-ga jaguvust uurides saame, et $10^{17} + 9 \equiv 3^{17} + 2 \bmod 7$. Fermat' väikesest teoreemist teame, et

$3^6 \equiv 1 \bmod 7$, järelikult ka $3^{12} \equiv 1 \bmod 7$ ja

$$3^{17} + 2 \equiv 3^{12} \cdot 3^5 + 2 \equiv 3^5 + 2 = 245 \equiv 0 \bmod 7\,.$$

Järelikult saab algarv olla ainult $10^{17} + 3$.

Arvutiülesanne 24.1 Kontrolli arvuti abil, et $10^{17}+3$ on algarv. Kui paremat kohta ei leia, siis võid minna aadressile https://www.wolframalpha.com/ ja tippida küsimuse

```
Is 10^17+3 a prime number?
```

24.5 Me peame näitama, et $2021^{2020} + 5$ jagub 7-ga ja 9-ga. Kuna $2021 \equiv 5 \bmod 7$, $2020 \equiv 4 \bmod 6$, $2021 \equiv 5 \bmod 9$ ja $2020 \equiv 4 \bmod 8$, siis saame Fermat' väikese teoreemi abil

$$2021^{2020} + 5 \equiv 5^4 + 5 = 630 \equiv 0 \bmod 7$$

ja

$$2021^{2020} + 5 \equiv 5^4 + 5 = 630 \equiv 0 \bmod 9\,,$$

mida oligi tarvis.

Seda ülesannet saab lahendada ka Euleri teoreemiga. Teoreemi 24.1 tähistes võime võtta $x = 2021$ ja $n = 63$; kuna $2021 = 43 \cdot 47$ ja $63 = 3^2 \cdot 7$, siis on x ja n ühistegurita. Teoreemi rakendamiseks on vaja leida $\varphi(63)$, st 63-ga ühistegurita arvude arv hulgas $\{1, 2, \ldots, 63\}$.

Selleks võime kasutada otsest loendamist. Algtegurit 3 omab hulgas $\{1, 2, \ldots, 63\}$ täpselt $\frac{1}{3}$ osa ehk 21 arvu, algtegurit 7 aga $\frac{1}{7}$ osa ehk 9 arvu. Lisaks tuleb arvestada, et nii 3-e kui 7-ga jagub vaadeldavast hulgast 3 arvu, niisiis saame kokkuvõttes $\varphi(63) = 63 - 21 - 9 + 3 = 36$.

Niisiis võime jäägiga 63 astendades taandada astendatava modulo 63, astendaja aga modulo 36. Kuna $2021 \equiv 5 \bmod 63$ ja $2020 \equiv 4 \bmod 36$, saamegi vajaliku

$$2021^{2020} + 5 \equiv 5^4 + 5 = 630 \equiv 0 \bmod 63\,.$$

Euleri φ-funktsiooni arvutamiseks saab anda ka üldise valemi, vt jaotist 24.2.

24.6 Vastus: jah.

Tegemist on teise võimaliku lahendusega ülesandele 18.20. Näitame, et $2^{2^7-1} - 7 = 2^{127} - 7$ jagub arvuga 11, aga mitte arvuga 121.

Fermat' väikese teoreemi põhjal teame, et $2^{10} \equiv 1 \bmod 11$, seega

$$2^{127} - 7 = (2^{10})^{12} \cdot 2^7 - 7 \equiv 1^{12} \cdot 128 - 7 = 121 \equiv 0 \bmod 11\,.$$

Mooduli 121 järgi saame kasutada Euleri teoreemi. Hulgas $\{1, 2, \ldots, 121\}$ on arvuga 11 ühistegurita täpselt $121 - 11 = 110$ elementi, seega Euleri teoreemi põhjal $2^{110} \equiv 1 \bmod 121$. Nüüd võime lihtsustada

$$2^{127} - 7 = 2^{110} \cdot 2^{17} - 7 \equiv 1 \cdot 2^{17} - 7 \bmod 121\,.$$

Kuna $2^7 = 128 \equiv 7 \bmod 121$, saame edasi

$$2^{17} - 7 = (2^7)^2 \cdot 2^3 - 7 \equiv 7^2 \cdot 2^3 - 7 = 49 \cdot 8 - 7 = 385 \equiv 22 \bmod 121\,.$$

Kokkuvõttes jagub $2^{2^7-1} - 7 = 2^{127} - 7$ arvuga 11, aga mitte arvuga 121, niisiis ei saa ta olla täisruut.

24.1 Fermat' väikese teoreemi kombinatoorne tõestus

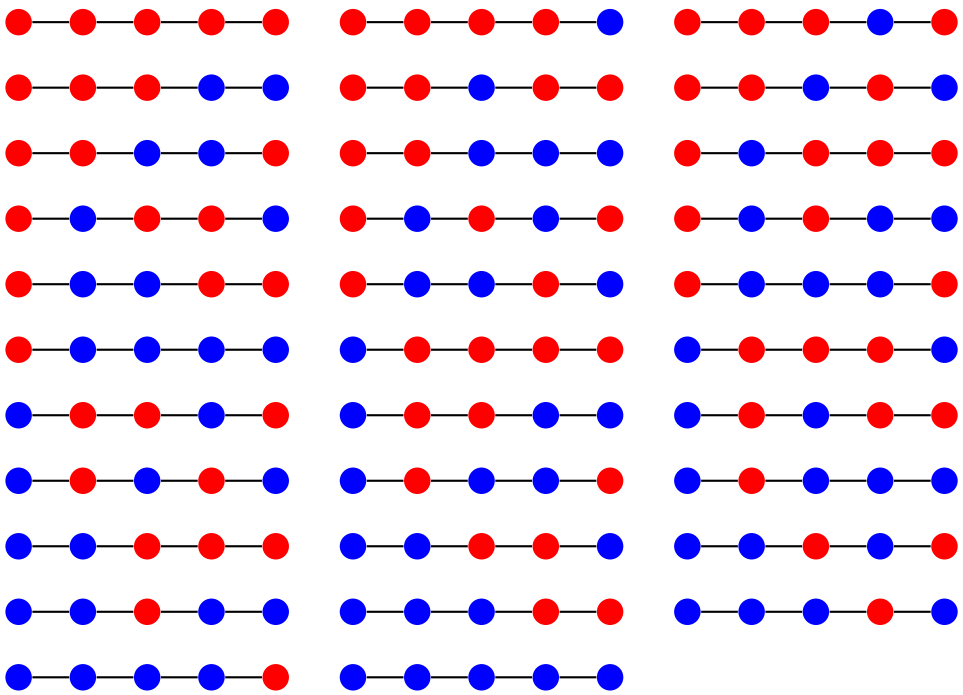
Selles jaotises anname Fermat' väikesele teoreemile (vt teoreem 24.3) veel ühe ilusa ja õpetliku tõestuse.

Teoreem 24.4 Kui p on algarv, siis suvalise täisarvu a korral kehtib seos

$$a^p \equiv a \bmod p\,.$$

Tõestus. Paneme tähele, et väites veendumiseks piisab a kohal vaadelda ainult kõiki algarvuga p jagamisel tekkivaid (mittenegatiivseid!) jääke $0,1,2,\ldots,p-1$. Lisaks on teoreemi väide $a=0$ ja $a=1$ puhul triviaalselt tõene, niisiis võime vaadelda ainult juhtu $a \geqslant 2$.

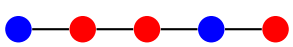
Anname Fermat' väikesele teoreemile tõestuse kaelakeede loendamise abil. Olgu meil a erinevat värvi helmeid, millest moodustame kette pikkusega p. Erinevaid võimalikke ketimustreid on siis kokku a^p. Joonisel 24.1 on näitena toodud kõikvõimalikud 5-lülilised ketid, mida saab moodustada kahte värvi helmestest (st $a=2$ ja $p=5$).



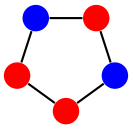
Joonis 24.1

Paneme tähele, et täpselt a nendest kettidest koosnevad ainult ühevärvilistest helmestest. Seega a^p-a ketis on vähemalt kahte värvi helmeid. Teoreem on tõestatud, kui me näitame, et $a^p-a \vdots p$. Selleks jagame kõik mitmevärvilised ketid p kaupa gruppidesse nii, et iga kett kuulub täpselt ühte gruppi ja ühtegi ketti ei jää üle.

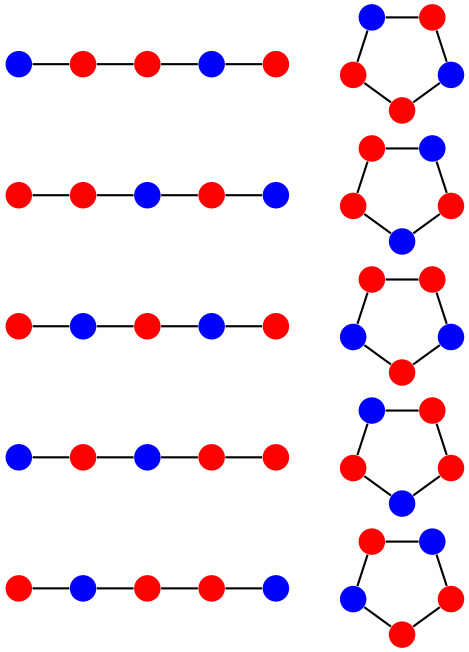
Teeme kõigist kettidest kaelakeed, ühendades omavahel nende vabad otsad. Näiteks ketist



saab kee



Ühte ja samasse gruppi võtame ketid, milledest tehtud keesid saab muuta samasugusteks pööramise abil (aga keed peegeldada st ümber keerata ei tohi!). Meie näite puhul kuuluvad ühte gruppi näiteks joonisel 24.2 kujutatud ketid ja neile vastavad keed.



Joonis 24.2

On selge, et igas grupis on vähemalt 1 ja ülimalt p ketti. Meie eesmärk on tõestada, et iga grupis on täpselt p ketti.

Oletame vastuväiteliselt, et leidub grupp, milles on vähem kui p ketti. See tähendab, et mingile selle grupi ketile vastavat keed pöörates jõuame me algsega võrreldes samasse seisu tagasi vähem kui p pöördega. Olgu q vähim pöörete arv, mis tuleb teha, et see kee algsega võrreldes samasugusesse seisu tagasi jõuaks. Siis kehtib $p > q$. Kuna kees on vähemalt kahte värvi helmeid, siis peab kehtima ka võrratus $q \geqslant 2$.

Pöörame nüüd keed järjest k korda q positsiooni kaupa kuni hetkeni, mil oleme teinud vähemalt täispöörde. Kuna iga pööre q positsiooni kaupa jätab kee seisu samaks, on meil ka lõpuks algsega sama seis. Et p on algarv, ei saa kehtida võrdus $k \cdot q = p$. Järelikult peame me olema keed pööranud rohkem kui täispöörde võrra, st $k \cdot q > p$.

Olgu $r = p - k \cdot q$ nende positsioonide arv, mille võrra me oleme täispööret ületanud. Ühest küljest on selge, et $r < q$, sest enne viimast pööret q positsiooni võrra polnud täispööre veel täis. Teisest küljest aga annaks pööre algseisust r positsiooni võrra meile algsega sama seisu. See aga on vastuolu q valikuga, sest q oli vähim niisuguste omadustega positiivne arv. □

24.2 Euleri φ-funktsiooni arvutamine

Siinses jaotises tuletame üldise valemi Euleri φ-funktsiooni arvutamiseks. Selleks sõnastame ja tõestame kaks teoreemi.

Teoreem 24.5 Kui p on algarv ja k positiivne täisarv, siis

$$\varphi(p^k) = p^k - p^{k-1}.$$

Tõestus. Hulgas $\{1,2,\ldots,p^k\}$ on p^k arvu. Nende seast jagub p-ga iga p-s arv, niisiis on vaadeldavad hulgas p-ga jaguvaid elemente kokku $\frac{1}{p}\cdot p^k = p^{k-1}$ tükki. Kuna p on algarv, on p-ga ühistegurita parajasti kõik need arvud, mis temaga ei jagu. Järelikult $\varphi(p^k) = |\mathbb{Z}^*_{p_k}| = p^k - p^{k-1}$. □

Teoreem 24.6 Kui m ja n on ühistegurita positiivsed täisarvud, siis

$$\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n).$$

Tõestus. Definitsiooni järgi on $\varphi(m\cdot n)$ selliste arvude arv hulgas $\{1,2,\ldots,m\cdot n\}$, mis on ühistegurita arvuga $m\cdot n$. Paneme tähele, et SÜT$(a, m\cdot n) = 1$ parajasti siis, kui SÜT$(a,m) = 1$ ja SÜT$(a,n) = 1$.

Kirjutame kõik arvud $1,2,\ldots,m\cdot n$ järjest veergude kaupa tabelisse mõõtmetega $m\times n$:

$$\begin{array}{cccccc}
1 & m+1 & 2m+1 & 3m+1 & \ldots & (n-1)m+1\\
2 & m+2 & 2m+2 & 3m+2 & \ldots & (n-1)m+2\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
k & m+k & 2m+k & 3m+k & \ldots & (n-1)m+k\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
m & 2m & 3m & 4m & \ldots & nm
\end{array}$$

Vaatleme rida järjekorranumbriga k. On kaks võimalust: kas SÜT$(k,m) = d > 1$ või SÜT$(k,m) = 1$.

Esimesel juhul jagab d kõiki k. rea elemente (sest nad on kujul $\ell\cdot m + k$). Niisiis pole ükski neist ühistegurita arvuga m ega järelikult ka arvuga $m\cdot n$.

Teisel juhul SÜT$(k,m) = 1$ on kõik k. rea elemendid ühistegurita arvuga m. Tõepoolest, kui arvudel $\ell\cdot m + k$ ka m leiduks ühine tegur $e > 1$, peaks see tegur jagama ka arvu $(\ell\cdot m + k) - \ell\cdot m = k$; vastuolu.

Jääb üle leida, mitu arvu tabeli k. reas on ühistegutita arvuga n.

Väidame, et vaadeldava k. rea n arvu annavad n-ga jagades kõikvõimalikud erinevad jäägid. Kuna võimalikke jääke ongi kokku n tükki, piisab tõestada, et k. rea arvude jäägid jagamisel n-ga on erinevad. Oletame vastuväiteliselt, et leiduvad $\ell_1 \neq \ell_2 \in \{0,1,\ldots,n-1\}$ nii, et

$$\begin{aligned}
\ell_1\cdot m + k &\equiv \ell_2\cdot m + k \bmod n,\\
(\ell_1\cdot m + k) - (\ell_2\cdot m + k) &\vdots n,\\
(\ell_1 - \ell_2)\cdot m &\vdots n.
\end{aligned}$$

Kuna m ja n on eelduse järgi ühistegurita, järeldub siit $\ell_1 - \ell_2 \vdots n$; vastuolu eeldustega $\ell_1, \ell_2 \in \{0,1,\ldots,n-1\}$ ja $\ell_1 \neq \ell_2$.

Jääb veel tähele panna, et arvud n ja a on ühistegurita parajasti siis, kui ühistegurita on n ja a mod n (sest a mod n saab esitada kujul $a - \ell \cdot m$ mingi täisarvu ℓ korral). Niisiis on vaadeldavas k. reas n-ga ühistegurita arve täpselt $\varphi(n)$ tükki. Kuna ridu, mille jaoks SÜT$(k,m) = 1$, on omakorda täpselt $\varphi(m)$ tükki, olemegi näidanud, et arvude $\{1,2,\ldots,m\cdot n\}$ seas on $\varphi(m)\cdot\varphi(n)$ arvu, mis on ühistegurita arvuga $m\cdot n$. □

▪ **Näide 24.2** $m = 4$ ja $n = 15$ korral näeb teoreemi 24.6 tabel välja järgmine (punasega on märgitud arvud, mis on ühistegurita arvuga $4\cdot 15 = 60$):

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57
2	6	10	14	18	22	26	30	34	38	42	46	50	54	58
3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60

▪

Teoreemid 24.5 ja 24.6 võimaldavad Euleri φ-funktsiooni arvutada argumendi kanoonilise esituse kaudu. Nii näiteks saame ülesandes 24.5 leida

$$\varphi(63) = \varphi(7^1\cdot 3^2) = \varphi(7^1)\cdot\varphi(3^2) = (7^1-7^0)\cdot(3^2-3^1) = 6\cdot 6 = 36\,.$$

Üldisemalt saame induktsiooniga erinevate algtegurite arvu s järgi tõestada järgmise reegli:

Kui arv n on antud oma kanoonilise esitusega $n = p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_s^{a_s}$, siis

$$\varphi(n) = (p_1^{a_1} - p_1^{a_1-1})\cdot(p_2^{a_2} - p_2^{a_2-1})\cdot\ldots\cdot(p_s^{a_s} - p_s^{a_s-1})\,.$$

IV Geomeetria