Algjuurte teoreem

Algjuurte teoreem, olgugi et väitena lihtsasti mõistetav, tugineb tõestuses väga erinevat laadi faktidele. Sellisena on algjuurte teoreem sügavaim matemaatiline tulemus, mis teile arvuteooriast on räägitud. IMO ülesannetes vaevalt et nii erinevaid keerulisi fakte kombineerida tuleb; kuid mine sa tea. Igal juhul tuleb selle matemaatikatüki läbitöötamine kasuks. See näitab teed tõsise matemaatika juurde. Senised teadmised on vaid tilulilu või, nagu uhkeldavad teadlased ütlevad, triviaalsus.

Gaussi teoreem

Algjuurte teoreemi üks tugitala on nn Gaussi teoreem Euleri funktsiooni väärtuste summast üle jagajate.

Teoreem 1 (Gaussi teoreem) *Olgu n positiivne täisarv. Siis*

$$\sum_{d:d|n} \varphi(d) = n.$$

Teisi sõnu, liites Euleri funktsiooni väärtused arvu kõigil jagajatel, saame kokku antud arvu enda. Võime seda näidetel proovida. Näiteks arvul 1 on ainus jagaja 1 ja $\varphi(1) = 1$; arvul 2 on jagajad 1 ja 2 ning $\varphi(1)+\varphi(2) = 1+1 = 2$; suvalisel algarvul p on jagajad 1 ja p ning $\varphi(1) + \varphi(p) = 1 + (p-1) = p$. Kordarvudest näiteks arvu 6 jagajad on 1, 2, 3, 6 ning $\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6) = 1+1+2+2 = 6$. Järgnev tõestus kinnitab, et see seaduspära on üldkehtiv.

Tõestus. Kuna $\varphi(d) = |\{r :\ 0 \leqslant r < d,\ \gcd(d,r) = 1\}|$, siis

$$\sum_{d:d|n} \varphi(d) = |\{(d,r) :\ d \mid n,\ 0 \leqslant r < d,\ \gcd(d,r) = 1\}|.$$

Iga täisarvu r, $0 \leqslant r < d$, korral

$$\gcd(d,r) = 1 \iff \frac{n}{d} \cdot \gcd(d,r) = \frac{n}{d} \iff \gcd(n, r \cdot \frac{n}{d}) = \frac{n}{d},$$

kusjuures ka tingimuse $0 \leqslant r < d$ saab esitada kujul $0 \leqslant r \cdot \frac{n}{d} < n$. Seega

$$\sum_{d:d|n} \varphi(d) = \left|\left\{(d,r) :\ d \mid n,\ 0 \leqslant r \cdot \frac{n}{d} < n,\ \gcd(n, r \cdot \frac{n}{d}) = \frac{n}{d}\right\}\right|.$$

Kuna r esineb nüüd ainult kontekstis $r \cdot \frac{n}{d}$, võib vaadeldagi arvude r asemel nende $\frac{n}{d}$-kordseid, sest algne r on üheselt tuvastatav. Seega

$$\begin{aligned}\sum_{d:d|n} \varphi(d) &= \left|\left\{(d,s) :\ d \mid n,\ 0 \leqslant s < n,\ \frac{n}{d} \mid s,\ \gcd(n,s) = \frac{n}{d}\right\}\right| \\ &= \left|\left\{(d,s) :\ 0 \leqslant s < n,\ \gcd(n,s) = \frac{n}{d}\right\}\right|,\end{aligned}$$

kus tingimustest $d \mid n$ ja $\frac{n}{d} \mid s$ sai loobuda seetõttu, et võrduse $\gcd(n,s) = \frac{n}{d}$ korral peavad need nagunii kehtima.

Jääb üle märgata, et saadud hulgas esineb iga n-st väiksem naturaalarv s täpselt ühe paari parempoolse komponendina, sest vasakpoolne komponent d on tema poolt seosega $d = \frac{n}{\gcd(n,s)}$ üheselt määratud. Järelikult on selles hulgas paare niisama palju kui arvust n väiksemaid naturaalarve ehk

$$\sum_{d:d|n} \varphi(d) = |\{s :\ 0 \leqslant s < n\}| = n.$$

Teoreem on tõestatud. ■

Minnes tagasi enne tõestust toodud näidete juurde, algarvu p korral loendatakse jagajale $d = 1$ vastavas liidetavas parajasti arv 0, sest ainult tema suurim ühistegur p-ga on $\frac{p}{1}$ ehk p, jagajale $d = p$ vastavas liidetavas loendatakse arvud 1 kuni $p-1$, sest kõigi nende suurim ühistegur p-ga on $\frac{p}{p}$ ehk 1. Kordarvu 6 puhul on loendatavad arvud koondatud järgmisesse tabelisse.

d	$\frac{n}{d}$	Loendatavad arvud
1	6	6
2	3	3
3	2	2, 4
6	1	1, 5

Polünoomi juurte arv

Järgmisena põikame valda, millel ei näi eelnevaga ehk arvuteoreetiliste funktsioonidega mingit ühisosa olevat — polünoomide teooriasse.

Teada-tuntud Bezout' teoreem (täpsemalt, Bezout' nn väike teoreem) sätestab, et mittekonstantse polünoomi P ja tema suvalise juure a jaoks leidub tegurdus

$$P(x) = (x - a) \cdot Q(x),$$

kus

- Q on polünoom;
- Q aste (st astendaja muutuja x kõrgeima astmega liikmes) on 1 võrra väiksem kui P aste;
- muutuja kõrgeima astme kordaja polünoomis P ja polünoomis Q on sama.

Tavaliselt mõistetakse siin polünoome kas üle reaalarvude või kompleksarvude, kuid samalaadset fakti võib täheldada ka polünoomidel üle jäägiklasside. Alustame sellest, et kui P kordajad on täisarvud ja juur a on samuti täisarv, siis ka tegur Q tuleb täisarvuliste kordajatega. Kui nüüd m on positiivne täisarv, P on täisarvuliste kordajatega mittekonstantne polünoom ning a on täisarv, mis rahuldab võrdust $P(a) \equiv 0 \pmod{m}$, siis leidub Q nii, et iga täisarvu x korral

$$P(x) \equiv (x - a) \cdot Q(x) \pmod{m},$$

kus Q vastab samadele nõuetele nagu ülal.

Polünoomil üle reaalarvude või kompleksarvude on teatavasti ülimalt niimitu juurt, kui suur on tema aste. See fakt järeldub lihtsasti Bezout' teoreemist. Esitame siinkohal ka selle väite koos tõestusega. Tähistagu $\deg P$ polünoomi P astet.

Teoreem 2 (Teoreem polünoomi juurte arvust) *Olgu P selline polünoom, mis pole samaselt null. Siis P erinevate juurte arv on ülimalt $\deg P$.*

Tõestus. Teeme induktsiooni $\deg P$ järgi. Kui $\deg P = 0$, on tegu konstantse polünoomiga. Et eelduse kohaselt P pole samaselt null, on P väärtus igal kohal nullist erinev ehk juurte arv on 0 ning $0 \leqslant \deg P$. Järgnevalt olgu $\deg P > 0$ ja eeldame, et väide kehtib polünoomide jaoks, mille aste on $\deg P - 1$. Kui polünoomil P juuri pole, siis P rahuldab vajalikku tingimust, sest $0 \leqslant \deg P$. Kui polünoomil P on juur a, siis leiame Bezout' teoreemist

tegurduse $P(x) = (x - a) \cdot Q(x)$, kus $\deg Q = \deg P - 1$. Et x kõrgeima astme kordaja on polünoomis P ja polünoomis Q sama, siis Q pole samaselt null.

Olgu veel c polünoomi P suvaline muu juur. Siis $0 = P(c) = (c - a) \cdot Q(c)$, mistõttu $c - a = 0$ või $Q(c) = 0$. Kuna $c \neq a$, siis jääb üle vaid $Q(c) = 0$ ehk c on polünoomi Q juur. Kokkuvõttes, kõik polünoomi P juured peale a on polünoomi Q juured.

Induktsiooni eelduse kohaselt on polünoomil Q ülimalt $\deg Q$ juurt. Arvestades juurde ka a, on polünoomi P juurte arv kokku ülimalt $\deg Q + 1$ ehk $\deg P$. ■

Osutub, et ka see teoreem on teatud tingimustel üle kantav jäägiklassidele. Nimelt algarvulise mooduli puhul saab ülaltoodud mõttekäigu põhimõtteliselt samamoodi jäägiklasside jaoks läbi viia.

Teoreem 2 (Teoreem polünoomi juurte arvust jääkidel) *Olgu p algarv ja P täisarvuliste kordajatega polünoom, mille kordajad ei jagu kõik p-ga. Siis leidub ülimalt $\deg P$ paarikaupa mooduli p järgi mittekongruentset arvu a, mille korral $P(a) \equiv 0 \pmod{p}$.*

Tõestus. Eeldame, et muutuja kõrgeima astme kordaja polünoomis P ei jagu p-ga. See ei kitsenda üldisust, kuna kõrgemate astmete lisamisel p-ga jaguva kordajaga ei muutu P väärtused mooduli p järgi ega niisiis ka paarikaupa mittekongruentsete nullkohtade arv, polünoomi aste aga kasvab.

Teeme induktsiooni $\deg P$ järgi. Kui $\deg P = 0$, on tegu konstantse polünoomiga. Vastavalt eeldusele ei jagu P ainus kordaja p-ga, seega on tingimust $P(a) \equiv 0 \pmod{p}$ rahuldavate täisarvude a arv 0 ning $0 \leqslant \deg P$. Järgnevalt olgu $\deg P > 0$ ja eeldame, et väide kehtib polünoomide jaoks, mille aste on $\deg P - 1$. Kui $P(a) \equiv 0 \pmod{p}$ ei kehti ühegi täisarvu a jaoks, siis P rahuldab vajalikku tingimust, sest $0 \leqslant \deg P$. Kui aga $P(a) \equiv 0 \pmod{p}$ mingi täisarvu a jaoks, siis leiame Bezout' teoreemist $P(x) = (x - a) \cdot Q(x)$, kus $\deg Q = \deg P - 1$. Seejuures Q on täisarvuliste kordajatega ja x kõrgeima astme kordaja on sama p-ga mitte jaguv arv mis polünoomil P.

Olgu c mingi täisarv, mille korral $c \not\equiv a \pmod{p}$ ja $P(c) \equiv 0 \pmod{p}$. Siis $0 \equiv P(c) = (c-a) \cdot Q(c) \pmod{p}$ ehk $p \mid (c-a) \cdot Q(c)$. Et p on algarv, siis $p \mid c-a$ või $p \mid Q(c)$, aga c valikust johtuvalt just $p \mid Q(c)$ ehk $Q(c) \equiv 0 \pmod{p}$.

Induktsiooni eelduse kohaselt leidub ülimalt $\deg Q$ paarikaupa mooduli p järgi mittekongruentset täisarvu c, mille korral $Q(c) \equiv 0 \pmod{p}$. Arvestades juurde ka a, on kokku ülimalt $\deg Q + 1$ ehk $\deg P$ paarikaupa mittekongruentset täisarvu polünoomi P jaoks. ■

Algarvulisust kasutab see tõestus ainult kohas, kus korrutise $(c-a)\cdot Q(c)$ jaguvusest p-ga järeldatakse emma-kumma teguri jaguvus p-ga. See algarvude omadus osutub analoogiks elementaarse aritmeetika faktile, et korrutis võrdub nulliga ainult siis, kui mõni teguritest on null. Jäägiklasside aritmeetikas formuleerubki see algarvude omadus sarnasel kujul: kui korrutis on mooduli p järgi null, siis mõni teguritest on mooduli p järgi null.

Kordarvulise mooduli puhul need omadused ei kehti. Näiteks mooduli 6 järgi on arv $2\cdot 3$ kongruentne nulliga, kuid kumbki tegur seda pole. Selle kohta öeldakse, et 2 ja 3 on mooduli 6 järgi nn nullitegurid (samuti 4 — kõik nulliga mittekongruentsed arvud, mis pole mooduliga ühistegurita, on nullitegurid). Teoreem juurte arvust ebaõnnestub juba esimese astme puhul. Näiteks polünoomil $4x-2$ on kaks mooduli 6 järgi mittekongruentset juurt 2 ja 5, samas kui $2>\deg(4x-2)$.

Algjuurte teoreem

Kõrvalepõige polünoomide teooriasse vihjab, et algjuurte teoreemi tõestamiseks interpreteeritakse kongruentsid $x^d\equiv 1 \pmod p$ ümber tingimusena polünoomi x^d-1 nullkohtadest mooduli p järgi. Näiteks saame juurte arvu teoreemist vahetult, et kongruentsidel $x^2\equiv 1 \pmod p$ on ülimalt kaks mittekongruentset lahendit. Seda fakti on paaritute arvude jaoks lihtne muidugi ka polünoome kasutamata tõestada. Kuid juurte arvu teoreem näitab, et üldiselt on kongruentsil $x^d\equiv 1 \pmod p$ algarvulise p korral ülimalt d paarikaupa mooduli p järgi mittekongruentset lahendit.

Kuid kuidas seda täpselt kasutada? Tähistame arvu a järku mooduli m järgi $\mathrm{ord}_m\, a$ — see on siis vähim positiivne täisarv d, mille korral kongruents $a^d\equiv 1 \pmod m$ kehtib. Algjuureks mooduli m järgi nimetatakse arvu c, mille korral $\mathrm{ord}_m\, c=\varphi(m)$ ehk mille astmete $1, c, c^2, \ldots, c^{\varphi(m)-1}$ jääkidena esituvad kõik m-ga ühistegurita arvud.

Algarvu p korral $\varphi(p)=p-1$, niisiis on tegu arvudega c, mis rahuldavad tingimust $c^{p-1}\equiv 1 \pmod p$ ehk nad on polünoomi $x^{p-1}-1$ nullkohad mooduli p järgi. Kuid sellest ju ei piisa. Kõik algjuured peavad küll selle polünoomi nullkohad olema, kuid mitte kõik selle polünoomi nullkohad pole algjuured, vaja on ka astendaja minimaalsust (Fermat' teoreemi põhjal rahuldab tingimust $x^{p-1}\equiv 1 \pmod p$ tegelikult ju iga p-ga mittejaguv arv, kaasa arvatud nt 1, mille järk 1 on väiksem mistahes temaga mittekongruentse arvu järgust).

Rakendame polünoomide teooriat aga kõigile võimalikele astendajatele.

Teoreem 3 (Algjuurte teoreemi põhilemma) *Olgu p algarv. Olgu a suvaline täisarv, mis p-ga ei jagu. Siis leidub täpselt $\varphi(\mathrm{ord}_p\, a)$ paarikaupa mittekongruentset täisarvu, mille järk mooduli p järgi on $\mathrm{ord}_p\, a$.*

Tõestus. Arvu a astmed

$$1, a, a^2, \ldots, a^{\mathrm{ord}_p\, a-1} \tag{1}$$

on järgu definitsioonist tulenevalt paarikaupa mittekongruentsed mooduli p järgi. Seejuures iga i korral $(a^i)^{\mathrm{ord}_p\, a}=(a^{\mathrm{ord}_p\, a})^i\equiv 1^i=1 \pmod p$. Kui $\gcd(i, \mathrm{ord}_p\, a)=d>1$, siis $(a^i)^{\frac{\mathrm{ord}_p\, a}{d}}=(a^{\mathrm{ord}_p\, a})^{\frac{i}{d}}\equiv 1^{\frac{i}{d}}=1 \pmod p$, kusjuures $\dfrac{\mathrm{ord}_p\, a}{d}<\mathrm{ord}_p\, a$, seega sellised astmed a^i ei ole a-ga sama järku. Kui aga $\gcd(i, \mathrm{ord}_p\, a)=1$, siis iga k, $0<k<\mathrm{ord}_p\, a$ korral $ik\not\equiv 0 \pmod{\mathrm{ord}_p\, a}$, mistõttu $(a^i)^k\not\equiv 1 \pmod p$, seega sellised astmed a^i on a-ga sama järku. Selliseid on vastavalt Euleri funktsiooni definitsioonile täpselt $\varphi(\mathrm{ord}_p\, a)$ ehk oleme leidnud nimekirjas (1) täpselt $\varphi(\mathrm{ord}_p\, a)$ arvu, mille järk on $\mathrm{ord}_p\, a$.

Tingimus $(a^i)^{\mathrm{ord}_p\, a}\equiv 1 \pmod p$ tähendab teisi sõnu, et a iga aste on polünoomi $x^{\mathrm{ord}_p\, a}-1$ nullkoht mooduli p järgi. Niisiis on nimekirjas (1) parajasti $\mathrm{ord}_p\, a$ ehk täpselt polünoomi astme jagu paarikaupa mittekongruentseid nullkohti. Et p on algarv, siis need ongi kõik selle polünoomi nullkohad mooduli p järgi. Järelikult ei leidu rohkem ka arve, mille järk võrduks a järguga. ■

Tõestuse teine lõik on väga oluline. Esimene lõik läheb samamoodi läbi ka kordarvu puhul, kuid valides mingi a, ei tarvitse kõik a-ga sama järku arvud olla kongruentsed mõne a astmega. Näiteks võttes mooduli 8 korral $a=7$, on $\mathrm{ord}_8\, a=2$ ja nimekiri vaid kaheliikmeline:

$$1, 7.$$

Samas, nagu kõik hästi teavad, on mooduli 8 järgi ka $\mathrm{ord}_8\, 3=\mathrm{ord}_8\, 5=2$. Kokkuvõttes, polünoomide teooria rakendub tõestuse teises lõigus näitamaks, et algarvulise mooduli korral on kõik a-ga sama järku arvud kongruentsed mõne a astmega, ehk selliste arvude läbivaatamiseks piisab vaadata läbi arvud nimekirjas (1).

Nüüd võib lugejale korraks tunduda, et algjuurte teoreem ongi juba tõestatud, piisab vaid põhilemmas võtta järguks $p-1$. Ei veel! Põhilemma ei väida üldsegi, et mingi järguga arve on olemas. Vastupidi, ta eeldab, et mingi arv mingi järguga on antud, ja näitab, kui palju samasugust järku arve kokku on. Seega kui meie algarv p tuleks ja teataks, et temal sellist arvu a ei

leidu, mille järk on $p-1$, siis oleks põhilemma selle rünnaku vastu näiliselt kaitsetu.

Ometi tugineb algjuurte teoreemi tõestus just sellele lemmale. Pangem tähele, kuidas mittekonstruktiivseks argumenteerimiseks võetakse appi kombinatoorika koos võimsuslike kaalutlustega.

Teoreem 4 (Algjuurte teoreem) *Olgu p algarv. Siis leidub algjuur mooduli p järgi.*

Tõestus. Fermat' teoreemi põhjal $a^{p-1} \equiv 1 \pmod p$ iga p-ga ühistegurita arvu a korral. Samaväärselt, $\mathsf{ord}_p\, a$ on alati arvu $p-1$ jagaja.

Tähistagu selguse mõttes

$$\gamma_p(d) = |\{r : \ 0 < r < p, \ \mathsf{ord}_p\, r = d\}|$$

ehk $\gamma_p(d)$ on erinevate järku d jääkide arv mooduli p järgi. Põhilemma põhjal $\gamma_p(d) = 0$ või $\gamma_p(d) = \varphi(d)$.

Summeerime suurused $\gamma_p(d)$ üle arvu $p-1$ kõigi jagajate d. Et esimese lõigu põhjal saab $\gamma_p(d) > 0$ kehtida ainult $d \mid p-1$ korral, on iga p-ga ühistegurita jääk r loendatud mingis sellises $\gamma_p(d)$-s. Võttes teisalt appi Gaussi teoreemi mooduli $p-1$ jaoks, saame

$$\sum_{d:d|p-1} \gamma_p(d) = p-1 = \sum_{d:d|p-1} \varphi(d).$$

Kui nüüd oletada, et mõne d (näiteks $p-1$ enda) korral $\gamma_p(d) = 0 < \varphi(d)$, siis seisame kohe silmitsi vastuoluga.

Järelikult peab leiduma ka algjuur. ■

Otsese järeldusena saame, et algarvulise mooduli p korral on arvu $p-1$ iga jagaja d jaoks olemas parajasti $\varphi(d)$ paarikaupa mittekongruentset arvu, mille järk on d.

Vaatame näitena läbi algarvuga 7 ühistegurita jääkide järgud. Need on kõik arvu 6 jagajad. Viimases lahtrireas, järguga 6, on algjuured (3 ja 5).

Järk	Arv	Jäägid	Astmed
1	1	1	1
2	1	6	1,6
3	2	2	1,2,4
		4	1,4,2
6	2	3	1,3,2,6,4,5
		5	1,5,4,6,2,3

Järelsõna

Mitmest vallast pärinevate faktide tulevärk võib olla efektne ka teiste teoreemide tõestamisel, mida siiski saab ka elementaarse nokitsemisega alistada. Vaatleme näiteks järgmist nn Wilsoni teoreemi.

Teoreem 5 (Wilsoni teoreem) *Olgu p algarv. Siis* $(p-1)! \equiv -1 \pmod p$.

Võtame algul jälle appi polünoomid.

Tõestus. Juhul $p = 2$ on väide ilmne, mistõttu eeldame, et p on paaritu.

Polünoomi $x^{p-1} - 1$ nullkohtadeks mooduli p järgi on Fermat' teoreemi põhjal kõik p-ga ühistegurita jäägid $1, 2, \ldots, p-1$. Igaüks annab polünoomile ühe lineaarteguri, mistõttu saab esitada

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \cdot Q(x) \pmod p$$

iga x korral. Et iga lineaartegur alandab jagatispolünoomi astet 1 võrra ja algse polünoomi aste on $p-1$, on $Q(x)$ konstantne polünoom. Kõrgeima astme kordaja on tal sama mis algsel polünoomil ehk 1, mistõttu võib selle välja jätta. Viies kõik ühele poole, saame

$$x^{p-1} - 1 - (x-1)(x-2)\ldots(x-(p-1)) \equiv 0 \pmod p \qquad (2)$$

iga x korral. Samasuse (2) vasakul pool on polünoom, mille aste on väiksem kui $p-1$, kuid tal on p paarikaupa mittekongruntset nullkohta mooduli p järgi. Järelikult on tegu polünoomiga, millele teoreem juurte arvust ei rakendu ehk kus kõik kordajad jaguvad arvuga p. Muuhulgas jagub arvuga p vabaliige $-1 - (-1)^{p-1} \cdot (p-1)!$, kust järeldubki $(p-1)! \equiv -1 \pmod p$. ■

Samas on tegu hoopis elementaarse tulemusega, mida demonstreerib järgmine tõestus.

Tõestus. Iga mooduliga ühistegurita arvu a jaoks leidub kongruentsi täpsusega ühene pöördelement x, mille korral $ax \equiv 1$, kusjuures x on samuti mooduliga ühistegurita ja tema pöördelement on a. Nii jagunevad kõik mooduliga ühistegurita jäägid paaridesse, mille komponentide korrutis on 1. Kui jääk a võrduks oma pöördelemendiga, tähendaks see, et $a^2 \equiv 1$. Algarvulise mooduli p korral on aga $p \mid a^2 - 1 = (a-1)(a+1)$ võimalik ainult juhul $a \equiv 1$ või $a \equiv -1$. Seega korrutises $1 \cdot 2 \cdot \ldots \cdot (p-1)$ taanduvad kõik tegurid peale 1 ja $p-1$ oma pöördelemendiga välja. Järelejäänud arvude korrutis mooduli p järgi on -1. ■

Algjuurte teoreemile aga mina teistsugust tõestust ei tea, mis asetab selle enamikust mulle tuntud arvuteooriafaktidest kõrgemale.