Jäännösluokat

Erkki Nurminen

Lukujoukot ja laskutoimitukset

Olemme tottuneet laskemaan luvuilla esim. lukujoukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$. Tässä siis

$\mathbb{N}$ on luonnollisen lukujen joukko $\{0, 1, 2, 3, \dots\}$,
$\mathbb{Z}$ on kokonaislukujen joukko $\{\dots, -2, -1, 0, 1, 2, \dots\}$,
$\mathbb{Q}$ on rationaalilukujen joukko ja
$\mathbb{R}$ on reaalilukujen joukko.

Näistä $\mathbb{N}$ on ollut käytössä pisimpään ja riitti primitiiviseen laskemiseen: jos kaksi luonnollista lukua lasketaan yhteen, tulos on myös luonnollinen luku. Samoin luonnollisten lukujen kertolasku tuottaa aina luonnollisen luvun. Tällaisesta tilanteesta sanotaan, että $\mathbb{N}$ on suljettu yhteen- ja kertolaskun suhteen.

Tehtävä 1. Tutki, mitkä joukoista $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ ovat suljettuja minkäkin neljän peruslaskutoimituksen suhteen. Koska nollalla jakaminen ei ole mahdollista, tarkastellaan jakolaskun tapauksessa lukujoukosta sellaisia versioita, joista nolla on poistettu: $\mathbb{N}\backslash\{0\}$ = {1, 2, 3…}, $\mathbb{Z}\backslash\{0\}$ = {… -2, -1, 1, 2, …}, $\mathbb{Q}\backslash\{0\}$ ja $\mathbb{R}\backslash\{0\}$. Entä mitkä joukoista ovat suljettuja kuutiojuuren suhteen?

Näissä joukossa on äärettömän monta alkiota, joten on jotenkin ajatuksellisesti hyväksyttävää, että sopivalla laskutoimituksella tulos kuuluu joukkoon, olivatpa laskun luvut mitä hyvänsä joukon alkioita. Jos määriteltäisiin jokin äärellinen joukko, esim. $A = \{0, 1, 2, 3\}$, olisi samalla tavoin aika selvää, että sen alkioiden yhteen- tai kertolasku tuottaisivat usein lukuja, jotka eivät ole enää tämän joukon jäseniä, eli joukko ei enää ole näiden laskutoimitusten suhteen suljettu.

Tehtävä 2. Olisiko mahdollista löytää ehkä edellistä vielä pienempi ainakin kahden alkion joukko, joka kuitenkin olisi suljettu kertolaskun suhteen? Entä yhteenlaskun suhteen?

Seuraavassa tutustutaan äärellisiin joukkoihin, joissa laskutoimitukset määritellään hieman eri tavalla ja lopulta joudutaan kyseenalaistamaan jopa se, onko 1 + 1 väistämättä 2.

Kongruenssi

Kurssilla MAA11 on määritelty kokonaislukujen *kongruenssi* – lukuteoriassa usein käytetty käsite, joka liittyy lukujen jaollisuuteen. Kongruenssissa verrataan toisiinsa kahta lukua a ja b tilanteessa, jossa ne jaetaan luvulla n (jota kutsutaan *moduliksi*). Jos niillä tällöin on sama jakojäännös, sanotaan, että a ja b ovat *kongruentit* keskenään modulo n.

Kongruenssia merkitään symbolilla ≡ ja siis ”a on kongruentti b:n kanssa modulo n” merkitään

$$a \equiv b \pmod{n}$$

Esimerkiksi luvut 7 ja 22 ovat kongruentit modulo 5, eli $7 \equiv 22 \ (mod\ 5)$, koska molempien jakojäännös 5:llä jaettaessa on 2. Kongruenttien lukujen erotus on aina modulin monikerta, eli siis jaollinen modulilla. Esim. 22 – 7 = 15, joka on jaollinen 5:llä. Itse asiassa tämä on kongruenssin varsinainen määritelmä, mutta jakojäännösten vertailu on sen kanssa yhtäpitävä ja usein käytännössä helpompi tapa tarkastella asiaa.

Tehtävä 3. Tutki, ovatko seuraavat luvut kongruentteja keskenään:

a) Onko $72 \equiv 9 \pmod{7}$?
b) Onko $-21 \equiv 11 \pmod{8}$?
c) Onko $75 \equiv 5 \pmod{6}$?

Jakojäännöksestä r kannattaa huomata, että kun kokonaisluku jaetaan luvulla n, jakojäännös ei määritelmän mukaan voi olla suurempi tai edes yhtä suuri kuin jakaja, vaan $0 \leq r < n$. Siis esim. mahdolliset jakojäännökset modulo 5 ovat 0, 1, 2, 3 ja 4. Yleisesti jakojäännökset modulo n ovat 0, 1, 2, … $n - 1$ ja niitä on siis kaikkiaan n kappaletta.

Kongruenssi on kahden luvun välinen *relaatio*. Muita esimerkkejä relaatioista ovat vaikkapa yhtäsuuruus = sekä epäyhtälöiden relaatiot >, <, ≥ ja ≤. Myös muiden kuin lukujen välillä voi olla relaatioita, esim. suorat voivat olla keskenään yhdensuuntaiset ∥, janat yhtä pitkät tai kuviot yhdenmuotoiset ∼. Jopa henkilöiden samanpituisuus tai henkilöiden välinen sisaruus ovat relaatioita.

Osa relaatioista on ns. *ekvivalessirelaatioita*, jotka toteuttavat seuraavat kolme ehtoa. Relaatio $\simeq$ on ekvivalenssirelaatio, jos

ER1 $a \simeq a$ (refleksiivisyys)
ER2 Jos $a \simeq b$, niin $b \simeq a$ (symmetrisyys)
ER3 Jos $a \simeq b$ ja $b \simeq c$, niin $a \simeq c$ (transitiivisuus)

Esim. suorien yhdensuuntaisuus ∥ on ekvivalenssirelaatio, koska

1) $L_1 \parallel L_1$,
2) $L_1 \parallel L_2 \Rightarrow L_2 \parallel L_1$
3) $L_1 \parallel L_2$ ja $L_2 \parallel L_3 \Rightarrow L_1 \parallel L_3$

Tehtävä 4. Tutki ekvivalenssirelaation määritelmän perusteella, ovatko seuraavat ekvivalenssirelaatioita.
a) kuvioiden yhdenmuotoisuus, ∼ b) lukujen vertailu relaatiolla ≥
c) henkilöiden samannimisyys d) henkilöiden sisaruksena oleminen.

Luvut tai muut alkiot, jotka ovat keskenään ekvivalenssirelaatiossa, muodostavat ns. *ekvivalenssiluokan*, joukon, jonka alkiot määräytyvät yksikäsitteisesti tämän niiden keskinäisen samanlaisuuden perusteella. Esim. kaikki suorat, joiden kulmakerroin on 2 ovat yhdensuuntaisia keskenään ja muodostavat ekvivalenssiluokan. Yksikään niiden kanssa yhdensuuntainen suora ei jää luokan ulkopuolelle eikä luokkaan voi kuulua suora, jonka kulmakerroin ei olisi 2 – se kuuluu johonkin toiseen ekvivalenssiluokkaan.

Jäännösluokka

Kaikki luvut, jotka ovat keskenään kongruentteja modulin n suhteen ovat ekvivalenssirelaatiossa keskenään ja muodostavat siis ekvivalenssiluokan. Näitä ekvivalenssiluokkia kutsutaan *jäännösluokiksi* (mod n), joita on eri jakojäännösten mukaisesti n kappaletta. Esim. modulin 5 tapauksessa voitaisiin ajatella, että otetaan viisi kulhoa, joihin kaikki kokonaisluvut jaetaan jakojäännöksensä (mod 5) mukaan. Jokainen luku kuuluu yksikäsitteisesti tarkalleen yhteen kulhoon. Näitä kulhoja, jäännösluokkia merkitään [0], [1], [2], [3] ja [4].

Siirrytään nyt laskemaan näillä jäännösluokilla. Sen sijaan, että meillä olisi äärettömän paljon kokonaislukuja, meillä on vain esimerkiksi modulin 5 tapauksessa 5 kulhoa, jotka on merkitty numeroin nollasta neljään. Näiden jäännösluokkien (mod 5) joukkoa merkitään $\mathbb{Z}_5$:

$$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$$

Lasketaan lukujen sijasta näillä kulhoilla, mutta periaatteessa samalla tavoin kuin luvuilla. Esim.

$$[1] + [2] = [3]$$

Tulos kuuluu jäännösluokkien joukkoon, eikä laskussa synny ongelmaa. Jäännösluokkien joukko on kuitenkin äärellinen, eikä vaikkapa (mod 5) salli suurempia tuloksia kuin [4]. Tämän vuoksi esim. [2] + [4] ei voi olla [6], vaan se pitää laskea

$$[2] + [4] = [6] = [1]$$

Liian suuret tulokset palautetaan siis kongruenssin avulla oikeaan jäännösluokkaansa. Näin on saatu äärellinen joukko, joka on suljettu yhteenlaskun ja kertolaskun suhteen.

Hakasulkumerkinnät ovat työläitä ja ne jätetään usein pois. Näin voidaan tehdä, kunhan asiayhteydestä on selvää, että ei olla laskemassa luvuilla, vaan jäännösluokilla.

Tehtävä 5. Laske joukossa $\mathbb{Z}_7$ (ilman hakasulkumerkintöjä)

a) 3 + 5 b) 2 · 5 c) 5 · (3 + 4) + 4 · 6

Joukoille $\mathbb{Z}_n$ voidaan muodostaa yhteenlaskun suhteen ns. yhteenlaskutaulu, josta näkyy havainnollisesti, minkälainen rakenne joukolla on.

Tehtävä 6. Täytä joukon $\mathbb{Z}_5$ yhteenlaskutaulu:

+	0	1	2	3	4
0					
1					
2					
3					
4					

Lukujoukoissa $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ vastaluvuiksi kutsuttiin lukuja, joiden summa on 0. Samoin joukossa $\mathbb{Z}_n$ vasta-alkioiksi voidaan kutsua jäännösluokkia, joiden summa on [0].

Tehtävä 7. Mitkä alkiot joukossa $\mathbb{Z}_5$ ovat toistensa vasta-alkioita?

Kertotaulu

Vastaavasti voidaan joukolle $\mathbb{Z}_n$ kirjoittaa myös kertolaskutaulu. Tällöin on tapana jättää pois alkio 0, koska sen tulot kaikkien alkioiden kanssa olisivat kaikki nollia. Kertolaskutilanteessa tarkastellaan siis esim. joukon $\mathbb{Z}_6$ sijaan joukkoa $\mathbb{Z}_6 \setminus \{0\} = \{1, 2, 3, 4, 5\}$.

Tehtävä 8. Täytä joukon $\mathbb{Z}_6$ kertolaskutaulu.

·	1	2	3	4	5
1					
2					
3					
4					
5					

Lukujoukoissa $\mathbb{Q}$ ja $\mathbb{R}$ käänteisluvuiksi kutsuttiin lukuja, joiden tulo on 1. Samoin joukossa $\mathbb{Z}_n$ käänteisalkioiksi voidaan kutsua jäännösluokkia, joiden tulo on [1].

Tehtävä 9. Mitkä alkiot joukossa $\mathbb{Z}_6$ ovat toistensa käänteisalkioita?

Tehtävä 10. Laadi joukon $\mathbb{Z}_5 \setminus \{0\} = \{1, 2, 3, 4\}$ kertolaskutaulu ja selvitä sen alkioiden käänteisalkiot.

Tehtävä 11. Ratkaise joukossa $\mathbb{Z}_5$ yhtälö $3x + 2 = 0$.

Tulon nollasääntö

Lukujoukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$ laskettaessa yksi keskeinen periaate on tulon nollasääntö: jos tulo $ab = 0$, joko $a = 0$ tai $b = 0$. Jos jossain joukossa olisi olemassa sellainen tulo $ab = 0$, jossa kumpikaan tekijöistä a tai b ei ole = 0, kutsutaan lukuja a ja b *nollanjakajiksi*, koska tällöin olisi $a = \frac{0}{b}$ ja $b = \frac{0}{a}$.

Tehtävä 12. Miten edellisten taulukoiden perusteella tulon nollasääntö toteutuu joukoissa $\mathbb{Z}_5$ ja $\mathbb{Z}_6$? Etsi joukoista mahdolliset nollanjakajat. Mikä joukon $\mathbb{Z}_n$ ominaisuus aiheuttaisi sen (eli minkälainen modulin n pitäisi olla), että nollanjakajia ei voi esiintyä?

Tehtävä 13. Vertaile edellisten tehtävien taulukoita ($\mathbb{Z}_5$, +), ($\mathbb{Z}_5\setminus\{0\}$, ·) ja ($\mathbb{Z}_6\setminus\{0\}$, ·) Mitä rakenteellisia eroja ja yhtäläisyyksiä huomaat? Ovatko kaikki näiden taulukoiden joukot suljettuja taulukon laskutoimituksen suhteen?

Tehtävä 14. Laskemme päivittäin jäännösluokilla, vaikka sitä ei tule ajatelleeksi. Koita keksiä, missä tilanteessa on luonnollista laskea esim. 9 + 6 = 3 ja 11 + 8 = 7.

Siis jos ei lasketa luvuilla lukujoukoissa $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ ja $\mathbb{R}$, vaan jossain toisessa algebrallisessa systeemissä kuten jäännöskuokilla, meille tuttujen laskutoimitusten tulokset voivatkin olla muuta kuin niitä, joihin olemme tottuneet. Edes 1 + 1 = 2 ei ole itsestäänselvyys, vaan riippuu siitä, mitä 1 ja 2 tarkoittavat ja miten yhteenlasku niillä määritellään.

Tehtävä 15. Laske joukossa $\mathbb{Z}_2$ mitä on 1 + 1.