Jaksolliset desimaaliesitykset algebrallisesta näkökulmasta

Jaska Poranen
Tampereen yliopisto, Kasvatustieteiden yksikkö
Jaska.Poranen@uta.fi

Pentti Haukkanen
Tampereen yliopisto, Informaatiotieteiden yksikkö
Pentti.Haukkanen@uta.fi

Johdanto

Rationaaliluvun $\frac{a}{b}$ muuntaminen kokonaisluvuksi, desimaaliluvuksi tai päättymättömäksi jaksolliseksi desimaalikehitelmäksi on tuttua puuhaa koulussa. Esimerkiksi

(i) $\frac{10}{5} = 2$

(ii) $\frac{3}{5} = 0{,}6 \qquad \frac{3}{40} = 0{,}075$

(iii) $\frac{4}{9} = 0{,}444\cdots = 0{,}\overline{4} \qquad \frac{1}{7} = 0{,}142857142857\cdots = 0{,}\overline{142857}$

(iv) $\frac{1}{6} = 0{,}1666\ldots \qquad \frac{7}{30} = 0{,}2333\ldots$ (esijaksollisia, ts. jakso ei ala heti).

Tyypin (iii) murtoluvun muuntaminen päättymättömäksi jaksolliseksi desimaalikehitelmäksi on varsin mitättömältä, mekaaniselta, tylsältä ja pieneltä näyttävä ilmiö koulumatematiikassa. Silti jo siihenkin vaikuttaa kätkeytyvän liki loputtomasti kohtalaisen kiehtovia piirteitä. Opettajalle olisi hyväksi kaikilla kouluasteilla ylläpitää omaa tutkijanmieltään ja uteliaisuuttaan. Tällä jos millään on tärkeä siirtovaikutus hänen oppilaisiinsa. Oma sovelluksemme on vain yksi mahdollisuus monista koulumatematiikan ilmiöistä, joissa opettaja yhdessä oppilaidensa kanssa voi ikään kuin raapaista pintaa vähän syvemmältä. Nykypäivän opettajalla on oltava myös kokonaiskuvaa siitä, mitä ja miten eri kouluasteilla opiskellaan, olkoonpa hän sitten itse esimerkiksi ala- tai yläkoulun tai lukion opettaja. Esittämämme sovelluksen avulla hän voi osaltaan tehdä elävää ajatuksellista tai konkreettista vaellusta pitkin opetussuunnitelmien aikajanaa alakoulusta lukioon.

Tarkastelemme tyyppiä (iii) tiukan matemaattisesti yliopistotason luku- ja ryhmäteoriaa käyttäen. Löydämme sieltä yhteyksiä mm. kongruenssiin, alkuluokkaryhmään, Eulerin funktioon, ryhmien aliryhmiin, sivuluokkiin, syklisiin ryhmiin,

alkion kertalukuun ja Lagrangen lauseeseen. Ensin kuitenkin luomme tarkastelustamme havainnollis-konkreettisen kuvan ja esitämme asiaan liittyviä alustavia tehtäväideoita eri kouluasteille, joita opettajat voivat edelleen kehittää.

Sovelluksemme konkretisointia

Tyyppiä (iii) luonnehtii se, että desimaalimuoto on silloin päättymätön ja jaksollinen sekä se, että jakso alkaa heti pilkun jälkeen. Yleisesti teemme nyt ensinnäkin luonnolliset oletukset, että $1 \leq a < b$ ja että kyse on supistetusta muodosta (ts. $\mathrm{syt}(a, b) = 1$); lisäksi varsinainen tätä tyyppiä koskeva oletus on siinä, että $\mathrm{syt}(b, 10) = 1$. Nämä oletukset ovat seuraavassa aina ilman erillismainintaa voimassa.

Esimerkki 1. Jakolaskulle $\frac{1}{7}$ saadaan jakokulmassa esitys $0{,}142857142\ldots$ Jakokulmamenettelyn taustalla on jakoyhtälö, lukuteorian perustyökalu. Ensin kirjoitetaan $1 = 7 \cdot 0 + 1$ ja näin saadaan osamäärän ensimmäinen termi 0 (osamäärän kokonaisosa). Ensimmäinen jakojäännös 1 on 10 kymmenesosaa, niinpä kirjoitetaan $10 = 7 \cdot 1 + 3$ ja saadaan osamäärän seuraava termi 1 (kymmenesosat) ja toinen jakojäännös 3. Se on 30 sadasosaa, joten kirjoitetaan $30 = 7 \cdot 4 + 2$. Näin osamäärässä on sadasosia 4. Kolmas jakojäännös 2 (sadatta osaa) antaa nyt 20 tuhannetta osaa, joten kirjoitetaan $20 = 7 \cdot 2 + 6$ jne. Jakojäännökset ovat 1, 3, 2, 6, 4, 5 (tässä järjestyksessä) – ja sitten uudestaan alkaen 1:llä. Koska jakojäännös voi olla vain 1, 2, 3, 4, 5 tai 6 (se ei voi olla nyt 0, silloinhan jako päättyisi), tulee jakoprosessiin pakosti toistoa eli jaksollisuutta. Nyt saavutetaan ”teoreettinen maksimipituus” $7 - 1$ ja jakso rakentuu numeroista 1, 4, 2, 8, 5, 7, tässä järjestyksessä. Jakokulmamenettely on täysin deterministinen prosessi, kun ensimmäinen jakojäännös on selvillä. Havainnollis-konkreettinen tulkinta – ainakin jossain määrin – jaolle $\frac{1}{7}$ saadaan kuvittelemalla vaikkapa metrin mittaisen pitsan jakamista seitsemälle sisarukselle. Kukin sisaruksista saa yhden kymmenesosan, neljä sadatta osaa, kaksi tuhannetta osaa jne. Toisaalta jako ei ”matemaattisessa maailmassa” koskaan pääty. Jos sisarukset syövät osuutensa aina sen mukaan kuin sen saavat, voivat he syödä pitsaansa loputtomiin, annokset tosin pienenevät pienenemistään. Jos he odottavat jaon päättymistä, he saattavat kuolla nälkään.

Jakoyhtälöstä seuraa helposti, että yleisesti luvun $\frac{a}{b}$ desimaalikehitelmän (perus)jakson pituus on aina enimmillään $b - 1$, koska mahdolliset jakojäännökset b:llä jaettaessa ovat $1, 2, \ldots, b - 1$. Siis vaikkapa jaossa $\frac{1}{7}$ saadaan maksimaalinen jaksonpituus eli $7 - 1$; jaossa $\frac{4}{9} = 0{,}444\ldots$ jäädään puolestaan maksimipituudesta kauaksi. Jakokulmamenettelyn tietyt ulkoiset piirteet ovat artikkelin kirjoittajien elinaikana muuttuneet moneen kertaan, mutta jakoyhtälö ei ole muuttunut, eikä se tule muuttumaan.

Jaksonpituuksien tarkastelu avaa kiintoisia näkymiä. Esimerkiksi kun $a = 1$ ja $b = 21$, saadaan $1/21 = 0{,}047619\,047619\ldots$ eli jaksonpituuden ”teoreettista maksimia” $21 - 1$ ei saavuteta, vaan jaksonpituus $\lambda = 6$. Luku 21 ei ole alkuluku, mutta

luku 7 on. Voisiko ero siis johtua tästä? Ei ainakaan yksinomaan, sillä onhan vaikkapa luku 11 alkuluku, mutta $1 : 11 = 0{,}0909\ldots$ eli jaksonpituus λ on vain kaksi. Myöhemmin tulemme sitovasti osoittamaan muun muassa sen, että tyypin (iii) $\frac{a}{b}$ desimaaliesityksen jakson pituus λ on aina Eulerin funktion arvon $\phi(b)$ tekijä, ts. $\lambda \mid \phi(b)$.

Eulerin funktio $\phi(b)$ ilmaisee lukujen $1 \leq k \leq b$ määrän, joille $\text{syt}(k, b) = 1$. Siis esimerkiksi $\phi(7) = 6$ ja $\phi(21) = 12$. Pienten lukujen b kohdalla on Eulerin funktion arvo helposti määritettävissä kirjoittamalla ensin luvut $1, 2, \ldots, b$ näkyviin ja poistamalla tästä luettelosta kaikki luvut k, joille $\text{syt}(k, b) > 1$. Sitten lasketaan vain näin jäljelle jääneiden lukujen määrä. Tulemme esittämään myös kaavan, jonka avulla Eulerin funktion arvo on määritettävissä. Jos koulussa on käytettävissä jokin symbolisen laskennan ohjelmisto, niin sellaisesta löytyy suoraan funktion arvon laskeva komento. Erinomainen ohjelmisto on myös *Wolfram Alpha*, jota voi käyttää suoraan selaimella.

Luku $\phi(21) = 12$ on myös alkuluokkien määrä modulo 21; vastaavasti luku 6 on alkuluokkien määrä modulo 7. Yleisesti alkuluokat $\mathbb{Z}_m^\times$ muodostavat ryhmän kertolaskulla $\odot$ modulo m. Siis esimerkiksi luvut $\mathbb{Z}_{21}^\times = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$ muodostavat ryhmän modulo 21 laskutoimituksella $\odot$. Joukko $\mathbb{Z}_{21}^\times$ on sama kuin kaikkien mahdollisten jaettavien joukko tilanteessa $\frac{a}{21}$.

Tehdään kokeeksi jakokulmassa jakoa $1 : 21$. Ensimmäinen jakojäännös on silloin jaettava 1, seuraava 10, sitten 16, 13, 4 ja 19, kunnes alkaa toisto; huomataan, että jakojäännöksetkin kuuluvat joukkoon $\mathbb{Z}_{21}^\times$. Saamme desimaalikehitelmän $0{,}047619\ldots$, missä siis jakson pituus $\lambda = 6$ ja itse jakso rakentuu numeroista 0, 4, 7, 6, 1 ja 9. Jakojäännökset muodostavat aliryhmän H ryhmälle $G = (\mathbb{Z}_{21}^\times, \odot)$, ts. joukon $\mathbb{Z}_{21}^\times$ osajoukko H on itse ryhmä operaatiolla $\odot$.

Tehdään esimerkkiimme liittyen taulukko, josta äärellisten ryhmien aliryhmäkriteerin perusteella voimme helposti todeta, että H todella on G:n aliryhmä. Vaikkapa tapauksessa $13 \odot 19$ tehdään ensin tavallinen kertolasku $13 \cdot 19 = 247$. Sitten määritetään luvun 247 jakojäännös modulo 21. Se on 16, onhan nimittäin $247 = 21 \cdot 11 + 16$.

Taulukko 1. $(H, \odot)$ on ryhmän $(\mathbb{Z}_{21}^\times, \odot)$ aliryhmä, kun H on jaon $1 : 21$ jakojäännösten joukko.

$\odot \pmod{21}$	1	4	10	13	16	19
1	1	4	10	13	16	19
4	4	16	19	10	1	13
10	10	19	16	4	13	1
13	13	10	4	1	19	16
16	16	1	13	19	4	10
19	19	13	1	16	10	4

Lagrangen lauseen mukaan pätee yleisesti, että jos H on äärellisen ryhmän G aliryhmä, niin H:n kertaluku on G:n kertaluvun tekijä – ja tämähän toteutuu esimerkissämme: $6 \mid 12$.

Jakokulmamenettelyssä jakojäännös määrää jakoyhtälön mukaisesti aina yksikäsitteisesti desimaalikehitelmän jakson numeron, samoin seuraavan jakojäännöksen. Voimme havainnollistaa tätä vaikkapa seuraavasti.

Taulukko 2. Aliryhmäjakojäännökset jakolaskussa $1 : 21$ ja niiden määräämät jakson desimaalit.

Aliryhmäjakojäännös	1	10	16	13	4	19
Jakson desimaali	0	4	7	6	1	9

On näin ollen selvää, että jos jakolaskussa $a : 21$ jaettavaksi valitaan vuorotellen aliryhmämme muut luvut 4, 10, 13, 16 ja 19, niin saatavan desimaalikehitelmän on toistettava syklisesti kehitelmä $\frac{1}{21} = 0{,}047619\ldots$

Valitaan esimerkiksi $a = 13$. Silloin $\frac{13}{21} = 0{,}619047\ldots$ Jakso alkaa siis ensimmäisen jakojäännöksen 13 määräämällä numerolla 6, mikä määrää puolestaan seuraavan jakojäännöksen 4 jne. Havainnollis-konkreettisesti taulukko 2 voitaisiin liimata sylinterin kiertäväksi nauhaksi, josta ilmiötä olisi helppo seurata ja hallita.

Tehdään sitten jakokulmassa vastaavasti jako $2 : 21$, missä siis jaettava 2 ei kuulu yllä esiteltyyn aliryhmään H (mutta on muuten mahdollinen esitettyjen oletusten valossa). Nyt jakojäännökset ovat 2, 20, 11, 5, 8 ja 17 ja nekin kuuluvat joukkoon $\mathbb{Z}_{21}^{\times}$. Ne muodostavat myös vasemman (oikean) sivuluokan modulo H. Jakolasku $2{:}21$ johtaa desimaalikehitelmään $0{,}095238\ldots$ Jakson pituus on taas 6. Sivuluokan generoi esimerkiksi $2 \in G$:

$$\begin{aligned} 2 \odot H &= \{\, 2 \odot H \colon h \in H \,\} \\ &= \{2 \odot 1, 2 \odot 4, 2 \odot 10, 2 \odot 12, 2 \odot 16, 2 \odot 19\} \\ &= \{2, 8, 20, 5, 11, 17\}. \end{aligned}$$

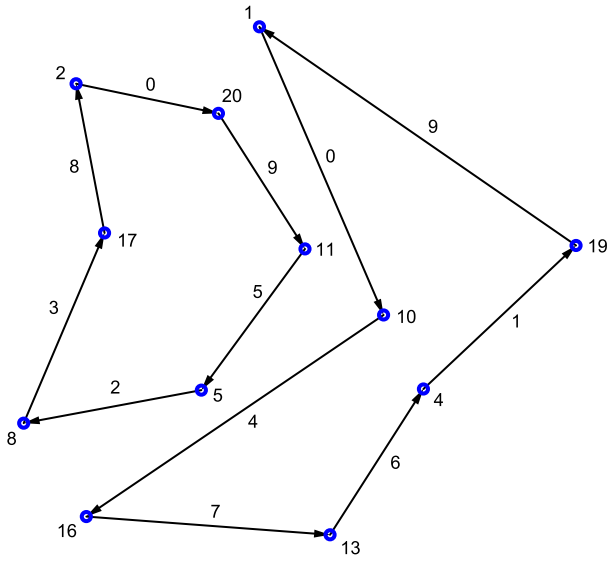
Taulukko 3. Sivuluokkajakojäännökset jakolaskussa $2 : 21$ ja niiden määräämät jakson desimaalit.

Sivuluokan $2 \odot H$ jakojäännökset	2	20	11	5	8	17
Jakson desimaali	0	9	5	2	3	8

Jos jaettavalle a annetaan vuorotellen arvot 20, 11, 5, 8 ja 17, niin saatavan desimaalikehitelmän on oltava jälleen syklinen toisto kehitelmälle $0{,}095238\ldots$

Sivuluokassa $2 \odot H$ on tietysti sama määrä elementtejä kuin aliryhmässä (ja sivuluokassa) $H = 1 \odot H$. Yhdessä nämä sivuluokat $H = 1 \odot H$ ja $2 \odot H$ antavat joukon $\mathbb{Z}_{21}^{\times}$ osituksen.

Tässä siis näemme, että kaikkien mahdollisten jakojäännösten joukko jaossa $a : 21$ on $1 \odot H \cup 2 \odot H = \mathbb{Z}_{21}^{\times}$, jonka alkioiden määrä $\phi(21) = 2 \cdot 6 = 2 \cdot \lambda$, ts. $\lambda \mid \phi(21)$. Taulukkojen 2 ja 3 avulla on myös kaikille mahdollisille jaoille $a : 21$ saatu kompakti esitys. On tietysti olemassa paljon muitakin havainnollistusmahdollisuuksia esitettyjen taulukkojen lisäksi. Seuraavassa vielä ”graafiteoreettinen” kuva ilmiöstä.



Kuva 1. *Jakolasku* a:21 *esitettynä suunnattuina graafeina. Solmut esittävät kaikkia mahdollisia jaettavia* a*; nuolia seuraten ja niitä lukemalla nähdään jaon* a:21 *jakso.*

Jos yllä (Kuva 1) lähdetään esimerkiksi solmusta 4 (eli jaosta $4 : 21$) päädytään nuolia seuraten jaksoon 190476, ts. $4 : 21 = 0{,}190476\ldots$

Jaksonpituudesta λ voidaan yleisesti tietää vielä enemmänkin kuin se, että $\lambda \mid \phi(b)$. Onhan nimittäin $\lambda = \mathrm{ord}_b(10)$, kuten myöhemmin tullaan osoittamaan. Palataan vielä tapaukseen $b = 21$. Luvun 10 kertaluku modulo 21 saadaan selville suoraviivaisesti tutkimalla luvun 10 potenssien 10^1, 10^2 jne. jakojäännöksiä jaettaessa luvulla 21. Kun jakojäännös $= 1$, on kertaluku löytynyt. Etsitään se: $10 = 21 \cdot 0 + 10$; $10^2 = 100 = 21 \cdot 4 + 16$; $10^3 = 21 \cdot 47 + 13$; $10^4 = 21 \cdot 476 + 4$; $10^5 = 21 \cdot 4761 + 19$; $10^6 = 21 \cdot 47619 + 1$. Etsitty kertaluku on siis 6 ja se on yhtä suuri kuin jaksonpituus λ. (Oikeasti kertaluku on helpompi etsiä kongruenssilla, mutta tässä sitä ei esitetä.)

On ilmeistä, että yleisesti jaksonpituuden λ maksimin $b - 1$ saavuttamiseksi on jakajan b välttämättä oltava alkuluku. Onhan nimittäin $\phi(b) = b - 1$, jos b on alkuluku. Jos b on yhdistetty luku (kuten vaikkapa $21 = 3 \cdot 7$), on vastaavasti ilmeistä, että $\phi(b) < b-1$ eli jaksonpituuden ”teoreettista maksimia” ei tällöin voida saavuttaa. Se, että b olisi alkuluku, ei ole kuitenkaan riittävä ehto jaksonpituuden maksimin saavuttamiseksi, kuten jo näimme.

Tehtäväideoita kouluun

Vuosiluokat 1–5

Valtakunnallisen opetussuunnitelman perusteiden (Opetushallitus 2004) mukaan koulujärjestelmässämme ovat kymmenjärjestelmä ja jakolasku esillä jo vuosiluokilla 1–2. Vuosiluokilla 3–5 käsitellään jaollisuutta jo yleisemmin sekä muun muassa murtolukujen ja desimaalilukujen välistä yhteyttä. Tällöin esitellään myös negatiiviset kokonaisluvut, joten ainakin opettajalla voisivat käsitteet ryhmä, aliryhmä ja sivuluokka käväistä tuolloin mielessä. Esimerkiksi viidellä jaolliset kokonaisluvut $5k$, kun k käy läpi kaikki kokonaisluvut, antaisivat aliryhmän ja yhden sivuluokan

kokonaislukujen ryhmälle (joka on varustettu yhteenlaskutoimituksella ja joka ei tietenkään ole äärellinen). Vastaavasti muodot $5k+1$, $5k+2$, $5k+3$ ja $5k+4$ antaisivat neljä muuta oikeata sivuluokkaa. Yhdessä ne jakaisivat kokonaisluvut viiteen erilliseen luokkaan.

Näin näyttäisi siltä, ettei ole mitään periaatteellisia esteitä tarkastella jo vuosiluokilla 1–5 monia sovelluksemme kannalta olennaisia seikkoja. Jaollisuuden yhteydessä ei ole lainkaan omituista puhua myös kahden positiivisen kokonaisluvun suurimmasta yhteisestä tekijästä (eli suurimmasta yhteisestä jakajasta). Tällöin myös tarkastelemamme ilmiön perusoletukset voisivat olla helposti esitettävissä. Yhtenä oppimistavoitteena vuosiluokilla 3–5 mainitaan, että oppilas "oppii tutkien ja havainnoiden muodostamaan matemaattisia käsitteitä ja käsitejärjestelmiä". Esimerkiksi Eulerin funktion $\phi(b)$ idean keksiminen on aivan ulottuvilla, jos ryhdytään järjestelmällisemmin tutkimaan ja havainnoimaan jakoja $a : b$. Kiinnitetään aina b ja rajoitutaan (mikä loppujen lopuksi ei ole oleellinen rajoitus) kokonaislukuvälille $1 \leq a < b$ siten, että $\text{syt}(a, b) = 1$, ja kysytään, montako kelvollista jaettavaa a löytyy. Tässä havaintomateriaalissa on syytä b:n olla vuoroin alkuluku, vuoroin yhdistetty, vaikka näitä käsitteitä ei pakosti vuosiluokilla 1–5 ole käsiteltykään.

Jakokulman käyttö miellettäneen vuosiluokilla 1–5 useimmiten kiintoisaksi ja tehokkaaksi työvälineeksi. Tämän artikkelin aiheen kannalta olisi hyvä, jos oppilaat uurastaisivat esimerkiksi jaot 1/7, 2/7, 3/7, 4/7, 5/7 ja 6/7 huomaten tulosten syklisyyden. Vastaavasti he voisivat ahkeroida vaikkapa jaot $1/13, 2/13, \ldots, 12/13$ ja huomata, että tilanne on silloin hieman mutkikkaampi. Nämä tarkastelut voisi koota ja havainnollistaa taulukoiden 2 ja 3 tai graafien tapaan. Havainnollisuutta voisi vielä lisätä käyttämällä sopivasti värejä.

Jaksollisuuden yleisempi idea ei sekään ole mitenkään hankalaa näillä vuosiluokilla. Esimerkiksi viikonpäivien toistuminen on kaikille tuttua. Opettaja voisi pistää oppilaansa kartoittamaan tuttuja toistuvia ilmiöitä. Päättymättömien jaksollisten desimaalikehitelmien luonne on epäilemättä monin tavoin vaativa, joten opettaja joutuu käyttämään myös mielikuvitustaan käsitellessään niitä näillä vuosiluokilla. Murtolukujen muuntamista desimaalimuotoihin perustellaan tyypillisesti siten, että tällöin laskeminen helpottuu – palautuuhan se silloin tietyllä tavalla laskemiseen kokonaisluvuilla Mutta tällainen perustelu tuskin vakuuttaa, jos muunnos tuottaa päättymättömän desimaalikehitelmän.

Vuosiluokat 6–9

Opetussuunnitelman perusteiden mukaan (Opetushallitus 2004) vuosiluokilla 6–9 on esimerkiksi pohjustettava todistamista perustelluilla arvauksilla ja kokeiluilla sekä vääräksi osoittamisella. Lukujen ja laskutoimitusten aihealueelta käsitellään muun muassa rationaali- ja reaalilukuja, vasta- ja käänteislukua, luvun jakamista alkutekijöihin, murtolukujen supistamista sekä desimaaliluvun esittämistä murtolukuna.

Sovellukseemme liittyviä tehtäväideoita voisivat olla esimerkiksi seuraavat.

1. Kiinnitetään b siten, että $\text{syt}(b, 10) = 1$. Selvitetään $\phi(b)$ (Eulerin funktiosta ei tarvitse puhua mitään; voidaan puhua esim. kaikkien mahdollisten supistettujen muotojen a/b määristä, kun $1 \leq a < b$). Tarkastellaan sitten jakolaskujen

$a : b$ tuotoksia (myös ilman laskimia) laskemalla ensin $1 : b$. Jos saadun desimaalikehitelmän jakson pituus $\lambda = \phi(b)$, niin testataan, että myös muilla jaettavan a valinnoilla jakolaskun $a : b$ tuotos on syklinen toisto jakolaskun $1 : b$ tuloksesta. Laaditaan tuloksista taulukko. Jos sitten $\lambda < \phi(b)$, niin jakamalla $\phi(b)$ luvulla λ saadaan selville sivuluokkien määrä alkuluokkien ryhmässä $\mathbb{Z}_b^\times$. Valitaan kustakin sivuluokasta yksi edustaja a' ja tehdään jako $a' : b$. Laaditaan taulukot, graafit tai muut havainnollistukset kompaktin kokonaisesityksen esityksen saamiseksi kaikille jaoille $a : b$.

2. Ideoitava jokin oma sovellus tyypin (iii) kehitelmistä.

3. Selvitettävä, miksi kehitelmän $a : b$ jakson pituus ei riipu a:sta.

4. Osoitettava, että b on alkuluku ei takaa jakson maksimipituutta $b - 1$.

5. Etsittävä väliltä $2 \ldots 100$ sellaiset alkuluvut b, jotka tuottavat maksimipituisen jakson. (Maksimijakso tulee esim. alkuluvuilla $b = 7, 17, 19, 23, \ldots$; mutta ei tule esim. luvuilla 3, 11, 13, 31 ja 37 (jaksojen pituudet näissä 1, 2, 6, 15, 3)).

6. Voiko maksimijakso esiintyä, kun b on yhdistetty luku? Tutki ja perustele!

Lukio

Sekä pitkän että lyhyen matematiikan opetussuunnitelmien perusteiden yleisissä tavoitteissa kannustetaan kokeilevaan, keksivään ja tutkivaan toimintaan (Opetushallitus 2003). Tavallisesti ainakin pitkän matematiikan ensimmäisessä kurssissa tehdään kertaava ja täydentävä katsaus eri lukualueisiin. Esimerkiksi kirjasta Kangasaho ym. (2004, 20–21) löytyy sovelluksemme kannalta mielenkiintoisia tehtäviä.

Pitkän matematiikan syventävässä kurssissa Lukuteoria ja logiikka (ks. myös esim. Merikoski ym. 1996) käsitellään muun muassa jaollisuutta, jakoyhtälöä, kongruenssia ja aritmetiikan peruslausetta. Eulerin funktio $\phi(b)$ voitaisiin esitellä tällä kurssilla ihan kunnolla (esimerkkikirjassamme näin menetelläänkin) – ja yksi motiivi sille voisi olla juuri sovelluksemme. Siihen liittyviä pikkutehtäviä voisivat olla esimerkiksi kaavojen keksimiset tapauksissa $\phi(p)$, $\phi(p^k)$, $\phi(p \cdot q)$, kun p ja q ovat eri alkulukuja, $\phi(m \cdot n)$, kun $\mathrm{syt}(m, n) = 1$ jne. Hieman suurempi tehtävä voisi olla sen osoittaminen, että $\phi(b)$ on parillinen, kun $b > 2$. Sivumennen sanottuna uusi kurssi Lukuteoria, logiikka ja *algebra* voisi olla myös hyödyllinen.

Kongruenssiopissa voitaisiin tutkia alkuluokkien modulo b summaa ja osoittaa, että se on luvun $\phi(b)$ monikerta. Täällä voitaisiin myös luontevasti valaista alkuluokkien modulo b algebrallista rakennetta multiplikatiivisena ryhmänä (vaikka ryhmäkäsitettä ei sinänsä esitettäisikään). Kokeellisen työskentelyn osuus olisi koko ajan varsin huomionarvoista.

Mahdollisesti hieman laajempia tutkimus- ja pohdintatehtäviä voisivat olla esimerkiksi seuraavat.

1. Havaitse kokeellisesti, että muodoilla

$$\frac{1}{99\ldots9} \qquad \text{ja} \qquad \frac{1}{11\ldots1}$$

voit tuottaa halutun pitkiä jaksoja. Miksi?

2. Jos halutaan jakson pituudeksi vaikkapa 7, niin tarkastellaan lukua $10^7 - 1 = 9999999$. Haetaan sen alkutekijäesitys (esimerkiksi *Wolfram Alphalla*): $9999999 = 3^2 \cdot 239 \cdot 4649$ ja edelleen sen kaikki positiiviset tekijät 1, 3, 9, 239, 717, 2151, 4649, 13947, 41841, 1111111, 3333333 ja 9999999. Luvuksi b eivät nyt kelpaa kolme ensimmäistä tekijää, mutta muut kelpaavat.

Miten voitaisiin tuottaa systemaattisesti kokonaislukuja b siten, että niiden käänteislukujen $\frac{1}{b}$ desimaaliesitykset olisivat tyyppiä (iii) ja joissa jakson pituus olisi halutun suuruinen?

3. Yllä havaittiin, että esimerkiksi $1:717$ tuottaa kehitelmän, missä jakson pituus on $= 7$. Itse kehitelmä on $0{,}0013947\ldots$ Koska $\phi(717) = 476$ ja $476:7 = 68$, on ryhmässä $\mathbb{Z}_{717}^{\times}$ 7-alkioisia sivuluokkia 68 jakoon $a:717$ liittyen. On siis olemassa tarkalleen 476 lukua a siten, että $1 \leq a < 717$ ja että desimaalikehitelmän $a:717$ jakson pituus on 7. Nämä kehitelmät jakautuvat 68 erilliseen "sykliseen luokkaan". Jakokulmamenettelyllä saadaan selville nämä luokat määräävä aliryhmä $H = 1 \odot H = \{1, 10, 100, 283, 679, 337, 502\}$. $\mathrm{Syt}(2, 717) = 1$ ja $2 \notin H$, joten saamme vaikkapa luvun 2 avulla sivuluokan $2 \odot H = \{2 \odot 1, 2 \odot 10, 2 \odot 100, 2 \odot 283, 2 \odot 679, 2 \odot 337, 2 \odot 502\} = \{2, 20, 200, 566, 641, 674, 287\}$ modulo 717. Nyt esimerkiksi $674:717 = 0{,}9400278\ldots$ ja $287:717 = 0{,}4002789\ldots$ Ideoi sopivassa ohjelmointiympäristössä (esim. *Maplen* tms. avulla) muut sivuluokat tuottava ohjelma.

4. Voitko kehittää uuden metodin päättymättömän jaksollisen desimaalikehitelmän (ilman esijaksoa) muuntamiseksi murtolukumuotoon? ("Vanhat metodit": geometrinen sarja ja "kertomismenettely" luvulla 10^{λ}.)

5. $\phi(21) = 12$, $\phi(21^2) = 252 = 21 \cdot 12$, $\phi(21^3) = 5292 = 21 \cdot 252 = 21^2 \cdot 12$, $\phi(21^4) = 111132 = 21^3 \cdot \phi(21)$ jne. Selvitä mitä säännönmukaisuutta tyypin (iii) mielessä jaksojen pituudet ja sivuluokkien määrät noudattavat tapauksissa $b = 21^2, 21^3, 21^4$ jne. Ohje: Tarkastele tapauksia $\frac{1}{21^2}$, $\frac{1}{21^3}$ jne.

6. Tee mahdollisimman kattava esitys lukiomatematiikan jaksollisuuteen liittyvistä teemoista.

7. Jakokulmamenettely kokonaisluvuille ja jakoyhtälö.

8. Irrationaaliluvun käsite? Miten voit konstruoida loputtomasti irrationaalilukuja jo yhdestä ainoasta rationaaliluvun päättymättömästä jaksollisesta desimaalikehitelmästä, esimerkiksi kehitelmästä $1:21 = 0{,}047619\ldots$

9. Villimpiä ideoita? Selvitä Hedy Lamarrin ja George Antheilin "frequency-hoppingin" perusidea. Voisiko jaksollisten desimaalikehitelmien teorialla olla jotain samantyyppisiä sovelluksia?

Algebran ja lukuteorian esitietoja

Esitämme vain ne tiedot algebrasta ja lukuteoriasta, jotka tarvitaan tässä artikkelissa. Esitys ei siten ole tarkoitettu muuten kattavaksi. Lisää tietoa algebrasta ja lukuteoriasta saa esimerkiksi kirjoista Malik ym. 1997 ja Rosen 2011.

Ryhmistä

Olkoon G epätyhjä joukko ja $\star$ siinä määritelty laskutoimitus (ts. $\star$ on kuvaus $G \times G \to G$). Pari $(G, \star)$ on *puoliryhmä*, jos $(a \star b) \star c = a \star (b \star c)$ aina, kun $a, b, c \in G$ (ts. laskutoimitus $\star$ on assosiatiivinen eli liitännäinen). Puoliryhmä on *monoidi*, jos on olemassa sellainen alkio $e \in G$ (ns. neutraalialkio), että $a \star e = e \star a = a$ aina, kun $a \in G$. Jos monoidissa jokaista alkiota $a \in G$ kohti on olemassa sellainen alkio $a^{-1} \in G$ (ns. käänteisalkio), että $a \star a^{-1} = a^{-1} \star a = e$, on kyseessä *ryhmä*. Ryhmää kutsutaan *Abelin ryhmäksi*, jos $a \star b = b \star a$ aina, kun $a, b \in G$ (ts. laskutoimitus $\star$ on kommutatiivinen eli vaihdannainen).

Pari $(H, \star)$ on ryhmän $(G, \star)$ *aliryhmä*, jos H on joukon G epätyhjä osajoukko ja $(H, \star)$ on ryhmä. Aliryhmäkriteeri äärellisille ryhmille sanoo, että jos $(G, \star)$ on äärellinen ryhmä ja H on joukon G epätyhjä osajoukko, niin $(H, \star)$ on ryhmän $(G, \star)$ aliryhmä, jos ja vain jos

$$\forall a, b \in H : a \star b \in H$$

ts. jos ja vain jos laskutoimitus $\star$ on sulkeutuva joukossa H. Lagrangen lause taas sanoo, että jos $(G, \star)$ on äärellinen ryhmä ja $(H, \star)$ sen aliryhmä, niin

$$|H| \,\Big|\, |G|$$

ts. joukon H alkioitten lukumäärä on joukon G alkioitten lukumäärän tekijä.

Olkoon $(G, \star)$ ryhmä ja $a \in G$. Merkitään alkion a potenssien joukkoa symbolilla $\langle a \rangle$, ts.

$$\langle a \rangle = \{\, a^k \mid k \in \mathbb{Z} \,\}.$$

Silloin $(\langle a \rangle, \star)$ on ryhmän $(G, \star)$ suppein aliryhmä, joka sisältää alkion a. Joukon $\langle a \rangle$ alkioiden lukumäärää sanotaan alkion a *kertaluvuksi* ryhmässä G. Alkion a kertaluvusta käytetään merkintää $\mathrm{ord}(a)$. Ryhmä $(G, \star)$ on *syklinen*, jos on olemassa sellainen $a \in G$, että $G = \langle a \rangle$. Alkiota a sanotaan syklisen ryhmän *generaattoriksi*.

Olkoon $(G, \star)$ ryhmä ja $(H, \star)$ sen aliryhmä. Silloin alkion $a \in G$ määräämä *vasen sivuluokka* modulo H on

$$a \star H = \{\, a \star h \mid h \in H \,\}.$$

Kaikki vasemmat sivuluokat saadaan, kun a käy läpi joukon G. Kun e on ryhmän neutraalialkio, niin $e \star H = H$. Yleisesti, $a \star H = H$, kun $a \in H$. Edelleen, $a \in a \star H$, kun $a \in G$. Vasemmat sivuluokat ovat ekvivalenssiluokkia, joten ne muodostavat joukon G osituksen, ts. kaksi vasenta sivuluokkaa ovat joko samat tai erilliset ja kaikkien vasenten sivuluokkien yhdiste on joukko G. Lisäksi $a \star H = b \star H \Leftrightarrow a \in b \star H \Leftrightarrow b \in a \star H$.

Alkion $a \in G$ määräämä *oikea sivuluokka* modulo H on vastaavasti

$$H \star a = \{\, h \star a \mid h \in H \,\}.$$

Jos G on Abelin ryhmä, niin $a \star H = H \star a$ aina, kun $a \in G$. Jos G ei ole Abelin ryhmä, niin yleensä $a \star H \neq H \star a$. Jokaisella sivuluokalla (sekä vasemmalla että oikealla) modulo H on sama kardinaaliluku. Erikoisesti jos H on äärellinen, niin sivuluokkien modulo H alkioiden lukumäärät ovat samat. Jos G on äärellinen, niin sekä vasempien että oikeiden sivuluokkien modulo H lukumäärä on kumpikin $|G| \,/\, |H|$.

Kongruenssista

Olkoon m kokonaisluku (≥ 2). Silloin sanotaan, että luku a on *kongruentti* luvun b kanssa *modulo* m, jos luku $a-b$ on jaollinen luvulla m ts. jos $m \mid (a-b)$. Tällöin merkitään $a \equiv b \pmod{m}$. Siis $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen $k \in \mathbb{Z}$, että $a = b + mk$.

Relaatio $\equiv \pmod{m}$ on ekvivalenssirelaatio joukossa $\mathbb{Z}$. Sen ekvivalenssiluokkia sanotaan *jäännösluokiksi* modulo m. Luvun a määräämää ekvivalenssiluokkaa merkitään symbolilla $[a]$. Lukua a sanotaan luokan $[a]$ *edustajaksi*. Kaikkien jäännösluokkien joukkoa modulo m merkitään symbolilla $\mathbb{Z}_m$. Siis

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}.$$

Jakoyhtälön mukaan jokaista lukua $a \in \mathbb{Z}$ kohti on olemassa yksikäsitteiset luvut q ja r, jotka toteuttavat ehdon $a = mq + r$, missä $0 \leq r < m$. Lukua q kutsutaan *osamääräksi*, ja lukua r kutsutaan *jäännökseksi* modulo m. Selvästi

$$[a] = [r]$$

ja yleisemmin

$$[a] = [b] \Leftrightarrow a \equiv b \pmod{m}.$$

Näin ollen luokan $[a]$ edustaja a voidaan korvata millä tahansa luvun a kanssa kongruentilla luvulla modulo m, esimerkiksi luvun a jäännöksellä r modulo m.

Yhteenlasku joukossa $\mathbb{Z}_m$ määritellään niin, että

$$[a] \oplus [b] = [a+b],$$

kun $[a]$, $[b] \in \mathbb{Z}_m$. Tätä yhteenlaskua kutsutaan usein yhteenlaskuksi modulo m. Pari $(\mathbb{Z}_m, \oplus)$ on Abelin ryhmä. Emme kuitenkaan tässä artikkelissa tarvitse yhteenlaskua modulo m vaan kertolaskua modulo m, jonka esittelemme seuraavaksi.

Kertolasku joukossa $\mathbb{Z}_m$ määritellään kaavalla

$$[a] \odot [b] = [ab],$$

missä $[a]$, $[b] \in \mathbb{Z}_m$. Yhtälön oikealla puolella hakasulkujen sisällä tulo ab on tavallinen kokonaislukujen tulo. Vasemman puolen tulo on määriteltävänä oleva kertolasku joukossa $\mathbb{Z}_m$ eli kertolasku modulo m. Pari $(\mathbb{Z}_m, \odot)$ on kommutatiivinen monoidi. Alkiolla $[a]$ on käänteisalkio monoidissa $(\mathbb{Z}_m, \odot)$, jos ja vain jos $(a, m) = 1$, missä $(a, m) = \mathrm{syt}(a, m)$, lukujen a ja m suurin yhteinen tekijä. Merkitään

$$\mathbb{Z}_m^\times = \{\, [a] \in \mathbb{Z}_m \mid (a, m) = 1 \,\}.$$

Joukon $\mathbb{Z}_m^\times$ alkioita sanotaan *alkuluokiksi* modulo m. Ne ovat siis monoidin $(\mathbb{Z}_m, \odot)$ kääntyvät alkiot. Nyt pari $(\mathbb{Z}_m^\times, \odot)$ on Abelin ryhmä, ns. *alkuluokkaryhmä* modulo m tai multiplikatiivinen ryhmä modulo m.

Eulerin funktio ϕ määritellään kaavalla

$$\phi(m) = |\{\, a : 1 \leq a \leq m,\ (a, m) = 1 \,\}|, \quad m \in \mathbb{Z}^+,$$

ts. $\phi(m)$ on joukon $\mathbb{Z}_m^\times$ alkioiden lukumäärä. Funktio ϕ toteuttaa muun muassa kaavan

$$\phi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right),$$

missä p käy läpi kaikki ne alkuluvut, jotka jakavat luvun m. Erityisesti $\phi(p^k) = p^k - p^{k-1}$, kun p on alkuluku ja $k \in \mathbb{Z}^+$.

Olkoot a ja m (> 1) yhteistekijättömät, ts. olkoon $(a, m) = 1$. Silloin Eulerin lauseen mukaan $a^{\phi(m)} \equiv 1 \pmod{m}$. Näin ollen on olemassa ainakin yksi sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Luvun a *kertaluku modulo* m on pienin näistä luvuista x. Merkitään $x = \mathrm{ord}_m(a)$. Algebrallisesti sanottuna $\mathrm{ord}_m(a)$ on alkion a kertaluku multiplikatiivisessa ryhmässä $\mathbb{Z}_m^\times$ modulo m. Lagrangen lauseen mukaan $\mathrm{ord}_m(a)$ jakaa luvun $\phi(m)$. Yleisemmin, jos $i, j \geq 0$, niin

$$a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{\mathrm{ord}_m(a)}.$$

Etsitään esimerkiksi $\mathrm{ord}_7(2)$. Selvästi

$$2^1 \equiv 2 \pmod{7},\ 2^2 \equiv 4 \pmod{7},\ 2^3 \equiv 1 \pmod{7},$$

joten $\mathrm{ord}_7(2) = 3$. Toisaalta $\phi(m) = \phi(7) = 6$.

Joukko $\{n_1, n_2, \ldots, n_{\phi(m)}\}$ on *supistettu jäännössysteemi* modulo m, jos $(n_i, m) = 1$, kun $i = 1, 2, \ldots, \phi(m)$, ja $n_i \not\equiv n_j \pmod{m}$, kun $i \neq j$. Esimerkiksi joukot $\{\, n \mid 0 \leq n \leq m-1,\ (n, m) = 1 \,\}$ ja $\{\, n \mid 1 \leq n \leq m,\ (n, m) = 1 \,\}$ ovat supistettuja jäännössysteemejä modulo m. Supistetun jäännössysteemin modulo m käsite on analoginen käsitteen alkuluokkaryhmä modulo m kanssa.

Desimaaliesitysten teoriaa

Jokainen reaaliluku $x \in (0, 1)$ voidaan kirjoittaa yksikäsitteisesti muodossa

$$x = \sum_{n=1}^{\infty} q_n 10^{-n} = 0, q_1 q_2 \ldots, \tag{1}$$

missä luvut q_n ovat kokonaislukuja väliltä $[0, 9]$ kuitenkin niin, että jokaista positiivista kokonaislukua N kohti on olemassa sellainen kokonaisluku $n > N$, että $q_n \neq 9$. Viimeisin ehto takaa, että esimerkiksi luvun $1/2$ esitys on yksikäsitteinen $0, 5$, koska esitys $0, 4999\ldots$ ei ole nyt sallittu. Esitystä (1) sanotaan luvun x *desimaaliesitykseksi*.

Desimaaliesitys on *päättyvä*, jos on olemassa sellainen luku n_0, että $q_n = 0$ aina, kun $n > n_0$. Reaaliluvun $x \in (0, 1)$ desimaaliesitys on päättyvä, jos ja vain jos $x \in \mathbb{Q}$ ja x voidaan kirjoittaa muodossa

$$x = \frac{a}{b}, \quad 1 \leq a < b,\ (a, b) = 1, \tag{2}$$

missä luvun b alkutekijät ovat 2 tai 5. (Luku b siis kuuluu lukujen 2 ja 5 generoimaan monoidin $(\mathbb{Z}, \cdot)$ alimonoidiin.) Tällöin $x = 0, q_1 q_2 \ldots q_{n_0}$. Esimerkiksi $7/50 = 0, 14$.

Desimaaliesitys on *jaksollinen*, jos on olemassa sellaiset luvut n_0 ($\geq$ 0) ja λ ($\geq$ 1), että $q_{n+\lambda} = q_n$ aina, kun $n > n_0$. Tällöin kirjoitamme $x = 0, q_1 q_2 \ldots q_{n_0}\overline{q_{n_0+1}q_{n_0+2}\ldots q_{n_0+\lambda}}$. Silloin $q_1 q_2 \ldots q_{n_0}$ on *esijakso* ja $q_{n_0+1}q_{n_0+2}\ldots q_{n_0+\lambda}$ on *jakso*, jonka *pituus* on λ. Reaaliluvun $x \in (0,1)$ desimaaliesitys on jaksollinen, jos ja vain jos $x \in \mathbb{Q}$ ja x ei ole muotoa (2). Esijakson pituus riippuu luvusta $(b, 10)$ ja sitä ei ole lainkaan, kun $(b, 10) = 1$. Esimerkiksi $1/6 = 0, 1\overline{6}$ ja $1/7 = 0, \overline{142857}$. Luvun $1/6 = 0, 1\overline{6}$ esijakson ja jakson pituus on kumpikin 1, ja luvun $1/7 = 0, \overline{142857}$ esijakson pituus on 0 ja jakson pituus on 6. (Huomaa, että jos desimaaliesityksessä on λ merkin pituinen jakso, on siinä tietenkin aina $t\lambda$ merkin pituinen jakso, kun $t \in \mathbb{Z}^+$. Tässä artikkelissa puhutaan kuitenkin koko ajan pienimmistä jaksoista.)

Reaaliluku $x \in (0,1)$ on rationaalinen, jos ja vain jos sen desimaaliesitys on päättyvä tai jaksollinen. Esimerkiksi luku $0, 1010010001000010\ldots$ on irrationaalinen. Siinä ykkösten välissä olevien nollien lukumäärä lisääntyy koko ajan yhdellä eikä esitys näin ollen ole jaksollinen.

Tässä artikkelissa käsittelemme rationaalilukuja

$$x = \frac{a}{b}, \quad 1 \leq a < b,\ (a,b) = 1,$$

missä $(b, 10) = 1$ ts. missä $2 \nmid b$ ja $5 \nmid b$. Silloin luvun x desimaaliesitys on jaksollinen ja esijaksoa ei ole lainkaan. Luvun x desimaaliesityksen $x = 0, q_1 q_2 \ldots$ saamme jakokulmalaskulla. Tarkastelemme aluksi jakokulmalaskua $1/b$, missä $(b, 10) = 1$. Osamäärien jono on silloin $q_0, q_1, q_2, \ldots$, missä $q_0 = 0$. Jakojäännösten jonolle käytämme merkintää $r_0, r_1, r_2, \ldots$ Jakojäännökset r_n toteuttavat rekursion

$$\begin{aligned} 10r_n &= bq_{n+1} + r_{n+1}, \quad n = 0, 1, \ldots \\ r_0 &= 1. \end{aligned} \tag{3}$$

Esimerkiksi kun lasketaan $1/7$, saadaan

$$\begin{aligned} 1 &= 7 \cdot 0 + 1 \quad \text{eli} \quad 1 = 7 \cdot q_0 + r_0, \\ 10 \cdot 1 &= 7 \cdot 1 + 3 \quad \text{eli} \quad 10r_0 = 7 \cdot q_1 + r_1, \\ 10 \cdot 3 &= 7 \cdot 4 + 2 \quad \text{eli} \quad 10r_1 = 7 \cdot q_2 + r_2, \\ 10 \cdot 2 &= 7 \cdot 2 + 6 \quad \text{eli} \quad 10r_2 = 7 \cdot q_3 + r_3, \\ 10 \cdot 6 &= 7 \cdot 8 + 4 \quad \text{eli} \quad 10r_3 = 7 \cdot q_4 + r_4, \end{aligned}$$

jne.

Kaavan (3) perusteella

$$\begin{aligned} 10r_n &\equiv r_{n+1} \pmod{b}, \quad n = 0, 1, \ldots \\ r_0 &= 1, \end{aligned}$$

josta saadaan, että

$$r_n \equiv 10^n \pmod{b}, \quad n = 0, 1, \ldots$$

Olkoon $\ell = \mathrm{ord}_b(10)$, ts. ℓ on pienin sellainen kokonaisluku $x > 0$, että

$$10^x \equiv 1 \pmod{b}.$$

Näin ollen jakojäännokset ovat kongruentteja lukujen

$$1, 10, 10^2, \ldots, 10^{\ell-1}, 1, 10, \ldots$$

kanssa modulo b. Merkitään vastaavien jäännösluokkien modulo b joukkoa kirjaimella L, ts.

$$L = \{[1], [10], [10^2], \ldots, [10^{\ell-1}]\}.$$

Silloin L on joukon $\mathbb{Z}_b^\times$ epätyhjä osajoukko, sillä $(b, 10^n) = 1$, kun $n = 0, 1, \ldots, \ell-1$. Edelleen

$$[10^i] \odot [10^j] = [10^{i+j}] = [10^n] \in L,$$

missä n on luvun $i + j$ jäännös modulo ℓ ja siis $n < \ell$. Täten kertolasku $\odot$ on sulkeutuva joukossa L. Näin ollen äärellisten ryhmien aliryhmäkriteerin nojalla $(L, \odot)$ on ryhmän $(\mathbb{Z}_b^\times, \odot)$ aliryhmä. Itse asiassa $L = \langle 10 \rangle$ eli alkion 10 generoima ryhmän $(\mathbb{Z}_b^\times, \odot)$ syklinen aliryhmä. Lagrangen lauseen perusteella $\ell \mid \phi(b)$, missä $\ell = |L|$ ja $\phi(b) = \left|\mathbb{Z}_b^\times\right|$.

Ryhmän $(\mathbb{Z}_b^\times, \odot)$ sivuluokat modulo L ovat muotoa

$$[a] \odot L = \{[a], [10a], [10^2a], \ldots, [10^{\ell-1}a]\},$$

missä $(a, b) = 1$. Kyseessä ovat jakojäännökset jakolaskussa

$$\frac{a}{b}, \quad 1 \leq a < b, \ (a, b) = 1,$$

missä $(b, 10) = 1$. Tarkemmin sanottuna jakojäännökset ovat kongruentteja lukujen

$$a, 10a, 10^2a, \ldots, 10^{\ell-1}a, a, 10a, \ldots$$

kanssa modulo b tässä järjestyksessä. Itse asiassa jakolaskun a/b jakojäännökset r_n toteuttavat rekursion

$$\begin{aligned} 10r_n &= bq_{n+1} + r_{n+1}, \quad n = 0, 1, \ldots \\ r_0 &= a, \end{aligned}$$

josta saadaan

$$\begin{aligned} 10r_n &\equiv r_{n+1} \pmod{b}, \quad n = 0, 1, \ldots \\ r_0 &= a \end{aligned}$$

ja edelleen

$$r_n \equiv 10^n a \pmod{b}, \quad n = 0, 1, \ldots$$

Todistetaan seuraavaksi, että luku ℓ on myös luvun a/b desimaaliesityksen jakson pituus. Jakojäännösten jonon jakson pituus on $\ell = \mathrm{ord}_b(10)$. Siis desimaaliesityksen jakson pituus $\lambda \leq \ell$. Todistetaan, että $\lambda = \ell$. Todistuksen idea on kirjasta (Rosen 2011). Merkitään $a/b = 0, \overline{q_1 q_2 \ldots q_\lambda}$. Siis

$$\begin{aligned} \frac{a}{b} &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right) + \left(\frac{q_1}{10^{\lambda+1}} + \frac{q_2}{10^{\lambda+2}} + \cdots + \frac{q_\lambda}{10^{2\lambda}}\right) + \cdots \\ &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right)\left(1 + \frac{1}{10^\lambda} + \frac{1}{10^{2\lambda}} + \cdots\right) \\ &= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \cdots + \frac{q_\lambda}{10^\lambda}\right)\left(\frac{10^\lambda}{10^\lambda - 1}\right) \\ &= \frac{q_1 10^{\lambda-1} + q_2 10^{\lambda-2} + \cdots + q_\lambda}{10^\lambda - 1}. \end{aligned}$$

Näin ollen $b \mid (10^\lambda - 1)$ eli $10^\lambda \equiv 1 \pmod{b}$. Täten luvun kertaluvun modulo b määritelmän nojalla $\lambda \geq \operatorname{ord}_b(10) = \ell$. Siis $\lambda \geq \ell$ ja $\lambda \leq \ell$, joten $\lambda = \ell = \operatorname{ord}_b(10)$.

Huomattakoon, että $\operatorname{ord}_b(10) \mid \phi(b)$. Siis jakson pituus $\operatorname{ord}_b(10)$ on Eulerin funktion arvon $\phi(b)$ tekijä. Lisäksi jakson pituus on sama $\operatorname{ord}_b(10)$ kaikilla luvuilla a/b, missä $(a, b) = 1$ ja $(b, 10) = 1$.

Sivuluokat muodostavat joukon $\mathbb{Z}_b^\times$ osituksen ja sivuluokkien lukumäärä on $\phi(b)/\operatorname{ord}_b(10)$. Tarkastellaan samaan sivuluokkaan kuuluvien lukujen desimaaliesityksiä. Oletetaan, että $[a]$ ja $[a']$ kuuluvat samaan sivuluokkaan $[a] \odot L$ (mutta ovat erisuuret). Silloin lukujen a/b ja a'/b jakojäännökset ovat samat ja samassa järjestyksessä mutta alkavat eri kohdasta ja täten desimaaliesitysten numerot ovat yhtä lailla samat ja samassa järjestyksessä mutta alkavat eri kohdasta. Esitetään asia tarkemmin. Olkoon luvun a/b desimaaliesitys $a/b = 0, \overline{q_1 q_2 \ldots q_\lambda}$, ja olkoon $[a'] \in [a] \odot L$ ja $1 \leq a' < b$. Silloin on olemassa sellainen yksikäsitteinen $i = 0, 1, \ldots, \lambda - 1$, että $a' \equiv 10^i a \pmod{b}$. Silloin luvun a'/b jakokulmalaskun jakojäännökset ovat kongruentteja modulo b lukujen $10^i a$, $10^{i+1}a, \ldots, 10^{\lambda-1}a$, a, $10a, \ldots, 10^{i-1}a, \ldots$ kanssa tässä järjestyksessä. Näin ollen luvun a'/b desimaaliesitys on $a'/b = 0, \overline{q_{i+1} \ldots q_\lambda q_1 q_2 \ldots q_i}$. Esimerkiksi olkoon $a = 1$ ja $b = 7$. Silloin $a/b = 1/7 = 0, \overline{142857}$, missä $[1] \odot L = L = \{[1], [10], \ldots, [10^5]\} = \mathbb{Z}_7^\times$ ja $\lambda = \phi(7) = 6$. Olkoon sitten $a' = 3$. Silloin $[3] \in L$ ja $3 \equiv 10^1 \pmod{7}$, joten $i = 1$ ja siis $a'/b = 3/7 = 0, \overline{q_2 \ldots q_6 q_1} = 0, \overline{428571}$.

Lähteet

Kangasaho, Jukka, Mäkinen, Jukka, Oikkonen, Juha, Paasonen, Johannes, Salmela, Maija, Tahvanainen, Jorma 2004. *Pitkä matematiikka. Funktiot ja yhtälöt.* WSOY.

Malik, D. S., Mordeson, John N., Sen, M. K. 1997. *Fundamentals of Abstract Algebra.* McGraw-Hill.

Merikoski, Jorma, Väänänen, Keijo, Laurinolli, Teuvo 1996. *Matematiikan Taito 11. Lukuteoria ja logiikka.* Weilin+Göös.

Opetushallitus 2003. Lukion opetussuunnitelman perusteet 2003: http://www.oph.fi/download/47345_lukion_opetussuunnitelman_perusteet_2003.pdf.

Opetushallitus 2004. Perusopetuksen opetussuunnitelman perusteet 2004: http://www02.oph.fi/ops/perusopetus/pops_web.pdf.

Rosen, Kenneth H. 2011. *Elementary Number Theory and Its Applications*, 6th ed. Pearson.