Jäännösluokat

Alkupala Aiemmin on tullut sana jäännösluokka vastaan. Tarkastellaan lukujoukkoja

$$\{\ \ 3k\ \ |\ k \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$$
$$\{3k+1|\ k \in \mathbb{Z}\} = \{\dots, -5, -2, 1, 4, 7, \dots\}$$
$$\{3k+2|\ k \in \mathbb{Z}\} = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

Osoita, että jokainen kokonaisluku on täsmälleen yhdessä näistä joukoista. Miten saat selville, missä?

Vastaus: Tarkastellaan *jakojäännöstä* jaettaessa annettu luku luvulla 3, mahdolliset jakojäännökset ovat 0,1 tai 2, joten… .

Esimerkki, kellotauluaritmetiikka ja jäännösluokka modulo 12:
Tarkastellaan *kellotauluaritmetiikkaa* eli 12-tuntisen kellotaulun tuntiosoittimen noudattamaa aritmetiikkaa. Esimerkiksi $9 + 5 = 2$, koska tuntiosoittimen ollessa luvun 9 kohdalla, tulee tämä osoitin 5 tunnin kuluttua luvun 2 kohdalle.

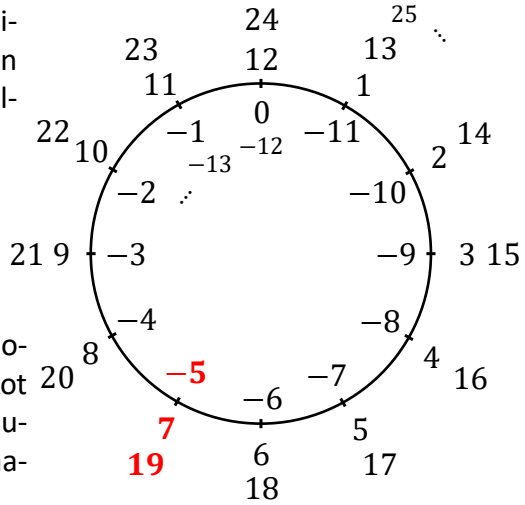
Esimerkki(jatkuu)
”Nollahetkellä” $t = 0$ kello on tasan 12, eli tasan 0 ja aikaa mitataan kokonaisina tunteina. Tällöin jos kello on sanotaan vaikka 7, niin ”nollahetkestä” on kulunut 7 tuntia, mutta yhtä hyvin ”nollahetkestä” on voinut kulua 19 tuntia tai 31 tai yleisesti $7 + 12k$ tuntia, missä $k \in \mathbb{N}$.

Myös negatiiviset k:n arvot voidaan hyväksyä , jolloin saadaan ajanhetket ennen ”nollahetkellä”, siis $k \in \mathbb{Z}$.

Kaikkina ajanhetkinä $7 + 12k$, ($k \in \mathbb{Z}$) kello on 7, joten lukema 7 vastaa joukkoa

$$\{7 + 12k|\ k \in \mathbb{Z}\}.$$

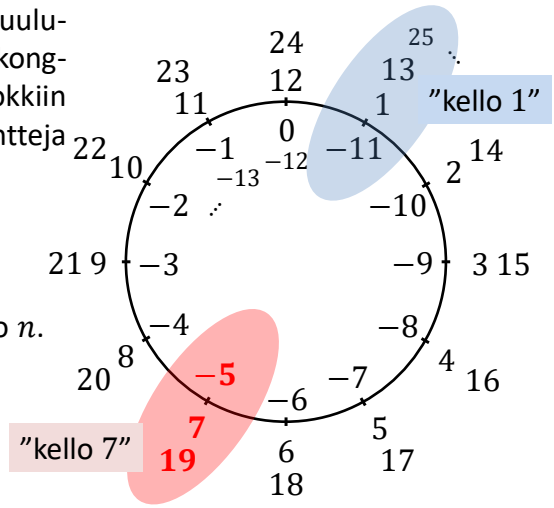
Vastaavalla tavalla voidaan muodostaa muutkin sellaiset joukot niin, että samaan joukkoon kuuluvat samaa kellonaikaa vastaavat ajanhetket.



Esimerkki(jatkuu)
Näin saatuja joukkoja:
"kello 0"$= \{12k|\ k \in \mathbb{Z}\}$, "kello 1"$= \{1 + 12k|\ k \in \mathbb{Z}\}$,
"kello 2"$= \{2 + 12k|\ k \in \mathbb{Z}\}$, "kello 3"$= \{3 + 12k|\ k \in \mathbb{Z}\}$, … ,
"kello 11"$= \{11 + 12k|\ k \in \mathbb{Z}\}$ kutsutaan *jäännösluokiksi modulo* 12.

Samaan jäännösluokkaan kuuluvat luvut ovat keskenään kongruentteja ja eri jäännösluokkiin kuuluvat luvut epäkongruentteja modulo 12.

Tarkastellaan seuraavaksi yleistä kongruenssia modulo n.



Määritelmä, jäännösluokat modulo n:
Luvun a määräämä *jäännösluokka modulo* n on luvun a kanssa kongruenttien lukujen joukko. Jäännösluokkaa merkitään hakasulkuja tai alleviivausta käyttäen, siis

$$[a]_n = \underline{a} = \{x \in \mathbb{Z}|\ x = a \pmod{n}\} = \{a + kn|\ k \in \mathbb{Z}\}.$$

Huomautus 1) Hakasulkumerkintä selkeämpi, koska siitä käy ilmi moduli n. Kirjassa lause: *Jos modulista ei ole epäselvyyttä, se voidaan jättää merkitsemättä*. MODULI lähes AINA NÄKYVIIN, se ei ole koskaan selvä! Lisäksi alleviivausmerkintä on jakaumien tarkasteluissa käytetty merkintä satunnaismuuttujalle.
2) Sanotaan, että luku a on kyseisen luokan *edustaja*. Yhtä hyvin voitaisiin edustajaksi ottaa minkä tahansa muotoa $a + kn$ olevan luvun, joten $[a]_n = [a + kn]_n$.

Esimerkki Jäännösluokat modulo 3 ovat $[0]_3 = \{\ \ 3k\ \ |\ k \in \mathbb{Z}\}$, $[1]_3 = \{3k + 1|\ k \in \mathbb{Z}\}$ ja $[2]_3 = \{3k + 2|\ k \in \mathbb{Z}\}$. Edustajiksi olisi voitu valita yhtä hyvin $[0]_3 = [-3]_3$, $[7]_3 = [1]_3$ ja $[2]_3 = [17]_3$.

Lause, jäännösluokkien modulo n ominaisuuksia:

(1) $[a]_n = [b]_n$ jos ja vain jos $a \equiv b \pmod{n}$.
Esim. $[8]_5 = [3]_5$, koska $8 \equiv 3 \pmod{5}$,
$[9]_5 \neq [2]_5$, koska $9 \not\equiv 2 \pmod{5}$.

(2) Jäännösluokat voidaan esittää muodossa

$$[0]_n, [1]_n, \dots, [n-1]_n,$$

Josta saadaan jäännösluokkien modulo n lukumääräksi n kpl. Esimerkiksi jäännösluokat modulo 5 ovat: $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$ ja $[4]_5$.

(3) Jokainen luku kuuluu täsmälleen yhteen jäännösluokkaan. Jos $a = qn + r$, $0 \leq r < n$, niin $[a]_n = [r]_n$. Tällä tavalla voidaan selvittää mihin jäännösluokkaan $[0]_n, [1]_n, \dots, [n-1]_n$ luku a kuuluu. Esimerkiksi jakolaskussa $19:5$ on jakojäännös 4. Siis $[19]_5 = [4]_5$.

Huomautus Jäännösluokkien modulo n joukkoa merkitään $\mathbb{Z}_n$, siis

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

Toisaalta $\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\cdot\mathbb{Z}}$, eli $\mathbb{Z}$ jaetaan osiin.

Jäännösluokkien laskusääntöjä

Palataan kellotauluun, jonka mukaan $9 + 5 = 2$. Kyseessä oli jäännösluokat modulo 12, joten voidaan määritellään $+$-lasku joukossa $\mathbb{Z}_{12}$

$$[9]_{12} + [5]_{12} = [2]_{12} \quad \text{eli}$$
$$\{9 + 12k \mid k \in \mathbb{Z}\} + \{5 + 12k \mid k \in \mathbb{Z}\} = \{2 + 12k \mid k \in \mathbb{Z}\}$$

Toisin sanoen; Määritellään, että niiden ajanhetkien joukon, jolloin ”kello on 9” ja niiden ajanhetkien joukon, jolloin ”kello on 5” summa on niiden ajanhetkien joukko, jolloin ”kello on 2”.
Havaitaan, ettei luokan edustajalla ole väliä. Koska $21 \equiv 9 \pmod{12}$ ja $29 \equiv 5 \pmod{12}$, niin $[21]_{12} + [29]_{12} = [2]_{12}$. Jos jäännösluokkien summa riippuisi yhteenlaskettavien edustajista, niin koko laskutoimitus olisi mieletön.

Määritelmä, jäännösluokkien modulo n yhteen- ja kertolasku:
Yhteen- ja kertolaskut joukossa $\mathbb{Z}_n$ määritellään kuten ”kellotauluaritmetiikassa”. Siis

$$[a]_n + [b]_n = [a + b]_n \quad \text{ja} \quad [a]_n \cdot [b]_n = [ab]_n .$$

Voidaan osoittaa, että näin määritellyt summa ja tulo eivät riipu valituista jäännösluokkien edustajista, joten sanotaan, että jäännösluokkien summa ja tulo ovat *hyvin määriteltyjä*.

Summan tapaus: Tarkastele jäännösluokkien $[a]_n$ ja $[b]_n$ summaa, joka edustajien $[a]_n$ ja $[b]_n$ avulla lausuttuna on $[a+b]_n$. Olkoot $[a']_n$ ja $[b']_n$ kyseisten jäännösluokkien jotkin muut edustajat, jolloin summa niiden avulla lausuttuna on $[a'+b']_n$. Nyt pitäisi osoittaa, että $[a+b]_n = [a'+b']_n$.

Esimerkki Muodosta yhteen- ja kertolaskutaulut joukossa **a)** $\mathbb{Z}_4$ ja joukossa **b)** $\mathbb{Z}_5$. HUOM! Nyt voidaan taulukossa jättää moduli n kirjoittamatta, koska se on oikeasti selvä.

a) Koska joukossa $\mathbb{Z}_4$on esimerkiksi

$$[2]_4 + [3]_4 = [5]_4 = [1]_4$$
$$[1]_4 + [3]_4 = [4]_4 = [0]_4$$
$$[0]_4 + [1]_4 = [1]_4 = [1]_4$$

niin saadaan diagonaalin suhteen symmetrinen yhteenlaskutaulukko. → Kertolaskutaulukko vastaavasti…

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

Koska joukossa $\mathbb{Z}_4$on esimerkiksi

$$[2]_4 \cdot [3]_4 = [6]_4 = [2]_4$$
$$[1]_4 \cdot [3]_4 = [3]_4 = [3]_4$$
$$[0]_4 \cdot [1]_4 = [0]_4 = [0]_4$$

Niin saadaan diagonaalin suhteen symmetrinen kertolaskutaulukko. →

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

b) Joukon $\mathbb{Z}_5$ + ja · laskutaulukot

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Esimerkki(jatkuu) Taulukoista voidaan kohtuu näppärästi etsiä yhtälöille $[x]_n + [3]_n = [1]_n$ ja $[x]_n \cdot [3]_n = [1]_n$ ratkaisut molemmissa jäännösluokissa $n = 4{,}5$. Saadaan

$[x]_4 + [3]_4 = [1]_4 \implies x = 2$ ja $[x]_4 \cdot [3]_4 = [1]_4 \implies x = 3$ sekä

$[x]_5 + [3]_5 = [1]_5 \implies x = 3$ ja $[x]_5 \cdot [3]_5 = [1]_5 \implies x = 2$.

Lause, jäännösluokkien modulo n laskusääntöjä:

Vaihdantalait: $[a]_n + [b]_n = [b]_n + [a]_n$ ja $[a]_n[b]_n = [b]_n[a]_n$.

Liitäntälait: $[a]_n + ([b]_n + [c]_n) = ([a]_n + [b]_n) + [c]_n$ ja
$[a]_n([b]_n[c]_n) = ([a]_n[b]_n)[c]_n$.

Osittelulaki: $[a]_n([b]_n + [c]_n) = [a]_n[b]_n + [a]_n[c]_n$.

Nolla yhteenlaskun neutraalialkiona: $[a]_n + [0]_n = [a]_n$.

Ykkönen kertolaskun neutraalialkiona: $[a]_n[1]_n = [a]_n$.

Vasta-alkio: Kaikilla $[a]_n \in \mathbb{Z}_n$ on olemassa sellainen $-[a]_n \in \mathbb{Z}_n$, että

$$[a]_n + (-[a]_n) = [0]_n.$$

Todistus Vaihdantalaki yhteenlaskun suhteen:

$$[a]_n + [b]_n \overset{\text{jäännösl. määr.}}{=\!=} [a+b]_n \overset{\text{vaihdanta–laki } \mathbb{Z}\text{:ssa}}{=\!=} [b+a]_n \overset{\text{jäännösl. määr.}}{=\!=} [b]_n + [a]_n$$

Muut kohdat harjoitustehtävä.

Esimerkki **a)** Määritä joukkojen $\mathbb{Z}_4$ ja $\mathbb{Z}_5$ alkioiden vasta-alkiot.
b) Mitä voidaan sanoa näiden joukkojen alkioiden käänteisalkioista, kun alkion $[a]_n$ käänteisalkio $[a]_n{}^{-1}$ määritellään yhtälöllä $[a]_n[a]_n{}^{-1} = [1]_n$?

a) Yhteenlaskutaulusta nähdään, että joukossa $\mathbb{Z}_4$ on $-[0]_4 = [0]_4$ eli nolla on itsensä vasta-alkio, $-[1]_4 = [3]_4$, $-[2]_4 = [2]_4$ eli kakkonen on myös itsensä vasta-alkio ja $-[3]_4 = [1]_4$. Vastaavasti joukossa $\mathbb{Z}_5$ on $-[0]_5 = [0]_5$, $-[1]_5 = [4]_5$, $-[2]_5 = [3]_5$, $-[3]_5 = [2]_5$ ja $-[4]_5 = [1]_5$. Jos tarkasteltaisiin muita joukkoja $\mathbb{Z}_n$, niin havaittaisiin, että aina $-[0]_n = [0]_n$.

b) Kertolaskutauluista nähdään, että joukossa $\mathbb{Z}_5$ jokaiselle nollasta eroavalla alkiolla on käänteisalkio, sillä $[1]_5{}^{-1} = [1]_5$, $[2]_5{}^{-1} = [3]_5$, $[3]_5{}^{-1} = [2]_5$ ja $[4]_5{}^{-1} = [4]_5$. Joukossa $\mathbb{Z}_4$ näin ei ole: $[1]_4{}^{-1} = [1]_4$ ja $[3]_4{}^{-1} = [3]_4$, mutta alkiolla $[2]_4$ ei ole käänteisalkiota. Yleisesti pätee tulos: Jos $n = p \in \mathbb{P}$, niin tällöin jokaisella nollasta eroavalla alkiolla on käänteisalkio. TOD. HT.