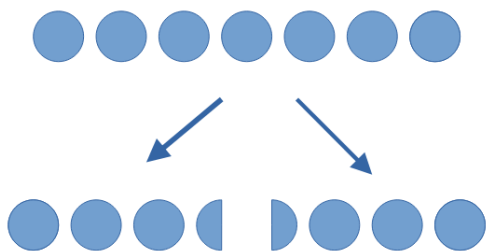


# Kongruenssi

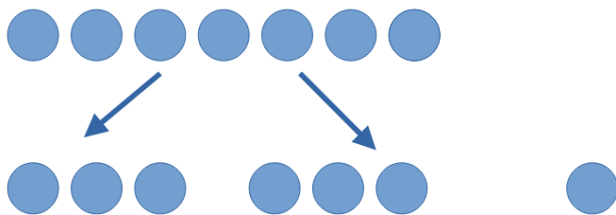
$\frac{7}{2} = 3.5$ . Visuaalisesti esitettynä:



*Kuvaselitys: Kuvassa on seitsemän palloa, ja kaksi nuolta osoittaa niistä muodostettuihin kahteen eri ryhmään. Molemmissa ryhmissä pallot jakautuvat kolmeen kokonaiseen ja yhteen puolikkaaseen palloon.*

## Entäpä jos jaettaisiin vain kokonaislukuihin?

$\frac{7}{2} = 3$  kokonaista ja 1 jää (jakojäännös)



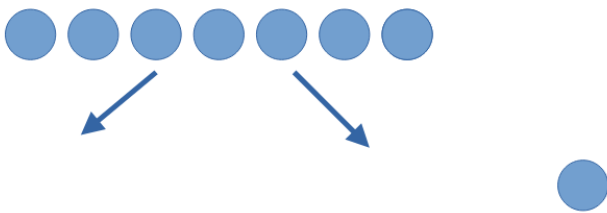
*Kuvaselitys: Kuvassa on seitsemän palloa, ja kaksi nuolta osoittaa niistä muodostettuihin kahteen eri ryhmään. Molemmissa ryhmissä pallot jakautuvat kolmeen kokonaiseen palloon. Ryhmien ulkopuolella on yksi yksittäinen pallo kuvastamassa jakojäännöstä.*

## Miten tämä voitaisiin merkitä kongruenssin avulla?

$\frac{7}{2} = 3$  kokonaista ja 1 jää. Kongruenssissa tämä olisi:

$$7 \equiv 1 \pmod{2}$$

Kongruenssissa ei tarvitse tietää, kuinka monta kokonaista lukua tulokseen sisältyy. Halutaan tietää vain mitä jaetaan, millä jaetaan, ja mikä jää jakojäännökseksi. Kongruenssi visuaalisesti esitettynä:



*Kuvaselitys: Kuvassa on seitsemän palloa, ja kaksi nuolta osoittaa niistä muodostettuihin kahteen eri ryhmään. Ryhmiä ei ole piirretty näkyviin, mikä kuvastaa kongruenssimerkinnän tapaa jättää pois tieto siitä, kuinka monta täyttä ryhmää muodostuu. Ryhmien ulkopuolella on yksi yksittäinen pallo kuvastamassa jakojäännöstä.*

## Miten kongruenssi puretaan?

$$7 \equiv 1 \pmod{2}$$

$$7 - 1 = 6$$

6 on jaollinen 2:lla

Modulo tarkoittaa jakojäännöstä, jota merkataan mod n:llä.

Lukujen kongruenssissa tarkoitetaan, että kaksi lukua antavat saman jakojäännöksen. Yllä oleva esimerkki luetaan 7 on kongruentti 1:sen kanssa. (Juuri, 2021)

## Miksi käytetään $\equiv$ , eikä $=$ ?

$=$  merkitsee numeraalista yhtäsuuruutta, missä arvot ovat merkin molemmin puolin yhtä suuria tietyssä tilanteessa tai tietyillä muuttujien arvoilla.

$\equiv$  merkitsee vahvempaa yhteyttä. Se ilmaisee numeerisen yhtäsuuruuden ja lausekkeiden identtisyuden. Lausekkeet voidaan korvata toisillaan kaikissa yhteyksissä, riippumatta muuttujien arvoista.

### Esimerkiksi:

$x = 3$  on tosi vain silloin, kun  $x$  on 3.

$2 \cdot x \equiv x + x$  on tosi aina kaikilla mahdollisilla  $x$ :n arvoilla

(Lingabites, 2023)

## Mitä hyötyä?

Jaollisuutta ja jakojäännöksiä voidaan tutkia kongruenssien avulla. Niitä hyödynnetään käytännössä esimerkiksi salasanojen muodostuksessa. (Juuri, 2021)

## Sääntöjä

$a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$  ja  $k \in \mathbb{Z}_+$

1. Kongruenttien lukujen summat ovat kongruenteja  $a + c \equiv b + d \pmod{n}$
2. Kongruenttien lukujen tulot ovat kongruenteja  $a \cdot c \equiv b \cdot d \pmod{n}$
3. Kongruenttien lukujen potenssit  $a^k \equiv b^k \pmod{n}$

## Todistaminen esimerkeillä:

1.  $7 \equiv 1 \pmod{2}$  ja  $5 \equiv 1 \pmod{2}$   
 $7 + 5 = 1 + 1 \pmod{2}$   
 $12 = 2 \pmod{2}$   
Tarkistetaan:  
 $12 - 2 = 10$

10 on jaollinen 2:lla

2.  $7 \pmod{2} \equiv 1$  ja  $5 \pmod{2} \equiv 1$

$$7 \cdot 5 = 1 \cdot 1 \pmod{2}$$

$$35 = 1 \pmod{2}$$

Tarkistetaan:

$$35 - 1 = 34$$

34 on jaollinen 2:lla

3.  $k = 3$  ja  $7^3 \pmod{2} \equiv 1^3$

$$343 = 1 \pmod{2}$$

Tarkistetaan:

$$343 - 1 = 342$$

342 on jaollinen 2:lla

(Moodi, 2023)

## Lähteet

**Lingabites.** (2023). *Mathematical symbols – equivalent sign.*

<https://lingabites.com/2023/12/22/mathematical-symbols-equivalent-sign>

**Harsunkorpi, J., Heiskanen, P., Liekas, M., Saarelainen, M.-M., & Tahvainen, J.** (2023).

*Moodi: Algoritmit ja lukuteoriaa* (1.–2. painos). Sanoma Pro Oy.

**Hähkiöniemi, M., Juhala, S., Juutinen, P., Laitinen, A., Luoma-aho, E., Raittila, T., & Tikka, T.** (2021).

*Juuri: Algoritmit ja lukuteoriaa* (1. painos). Kustannusosakeyhtiö Otava.