Kongruenssi

Hannu Lehto
Lahden Lyseon lukio

Kongruenssi

Määritelmä. Olkoon $a, b, m \in \mathbb{Z}$ ja $m \geq 1$. Luku a on kongruentti luvun b kanssa modulo m, jos m jakaa $(a-b)$:n. Toisin sanoen

$$\boxed{a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)}.$$

Määritelmän perusteella on $a \equiv b \pmod{m} \Leftrightarrow a = b + qm$. **Esimerkkejä.**
$35 \equiv 11 \pmod{24}$, koska $24 \mid (35-11)$.
$98 \not\equiv 4 \pmod{24}$, koska $24 \nmid (98-4)$.
$6 \equiv -15 \pmod{7}$, koska $7 \mid (6-(-15))$

$$\begin{aligned} 43 \equiv x \pmod{7} &\Leftrightarrow 7 \mid (43-x) \\ &\Leftrightarrow 43 - x = k \cdot 7 \, (k \in \mathbb{Z}) \\ &\Leftrightarrow x = 43 - k \cdot 7 \\ &\Leftrightarrow x = \ldots, 50, 43, 36, \ldots, 8, 1, -6, -13, \ldots \end{aligned}$$

Siis kaikki ne luvut, joiden jakojäännös 7:llä jaettaessa on sama kuin luvun 43 jakojäännös eli 1.

Kongruenssi ja jakojäännös

Lause. $a \equiv b \pmod{m}$, jos ja vain jos jakolaskuilla $\frac{a}{m}$ ja $\frac{b}{m}$ on sama jakojäännös.

Todistus.
'$\Rightarrow$'

'$\Leftarrow$'

■

Kongruenssin ominaisuuksia

Refleksiivisyys: $a \equiv a \pmod{m}$
Symmetrisyys: Jos $a \equiv b \pmod{m}$, niin $b \equiv a \pmod{m}$
Transitiivisuus: Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $a \equiv c \pmod{m}$

Transitiivisuuden todistus.
Koska $m \mid (a-b)$ ja $m \mid (b-c)$, niin $a - b = pm$ ja $b - c = qm$.
Nyt on $a - c = pm + b + qm - b = m(p+q)$, joten $m \mid (a-c)$ ja näin $a \equiv c \pmod{m}$.■

Kongruenssin laskusäännöt

Olkoon $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$ ja $k \in \mathbb{Z}$. Silloin

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $ac \equiv bd \pmod{m}$
4. $a + k \equiv b + k \pmod{m}$
5. $ka \equiv kb \pmod{m}$
6. $a^n \equiv b^n \pmod{m}, \quad (n \in \mathbb{N})$
7. $p(a) \equiv p(b) \pmod{m}$ kaikilla kokonaiskertoimisilla polynomeilla p

Kohtien 1, 2 ja 3 perusteella kongruensseja voidaan laskea yhteen, vähentää ja kertoa puolittain. Kohtien 4 ja 5 mukaan kongruenssiin voidaan lisätä puolittain mielivaltainen luku ja kongruenssi voidaan kertoa millä tahansa luvulla. Lisäksi kohdan 6 mukaan kongruenssi voidaan korottaa puolittain potenssiin.

5 / 10

Kongruenssin laskusäännöt

Jos $syt(k, m) = 1$, niin

$$ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$$

6 / 10

Esimerkkejä

1. Mikä on pienin luonnollinen luku, jonka kanssa 3^{21} on kongruentti modulo 4? Toisin sanoen mikä on jakolaskun $3^{21} : 4$ jakojäännös?

$$\begin{aligned} 3 &\equiv -1 \pmod{4} \\ 3^{21} &\equiv (-1)^{21} \pmod{4} \\ 3^{21} &\equiv -1 \pmod{4} \\ 3^{21} &\equiv 3 \pmod{4} \end{aligned}$$

Täten jakojäännös on 3.

7 / 10

Esimerkkejä

2. Osoita, että $7^n - 4^n$ on jaollinen luvulla 3, kun $n \in \mathbb{Z}_+$. Toisin sanoen, osoita, että jakolaskun $(7^n - 4^n) : 3$ jakojäännös on nolla.

$$\begin{aligned} 7 &\equiv 1 \pmod{3} \\ 7^n &\equiv 1^n \pmod{3} \\ 7^n &\equiv 1 \pmod{3} \end{aligned}$$

$$\begin{aligned} 4 &\equiv 1 \pmod{3} \\ 4^n &\equiv 1^n \pmod{3} \\ 4^n &\equiv 1 \pmod{3} \end{aligned}$$

Täten $7^n - 4^n \equiv 1 - 1 \equiv 0 \pmod{3}$, joten $7^n - 4^n$ on jaollinen luvulla 3.

8 / 10

Lineaarinen kongruenssi — ratkaisutapa 1

Lineaarinen kongruenssi on muotoa $ax \equiv b \pmod{m}$. Sen ratkaisu voidaan palauttaa Diofantoksen yhtälön ratkaisemiseksi.

$$\begin{aligned} ax \equiv b \pmod{m} &\Leftrightarrow m \mid (ax - b) \\ &\Leftrightarrow ax - b = my \\ &\Leftrightarrow ax - my = b. \end{aligned}$$

Tekemällä muuttujan vaihto $y = -y$, saadaan

$$\boxed{ax \equiv b \pmod{m} \Leftrightarrow ax + my = b}$$

Täten kongruenssilla $ax \equiv b \pmod{m}$ on ratkaisu, joss $syt(a, m) \mid b$.

Esimerkki. Ratkaise $9x \equiv 2 \pmod{7}$.
On siis ratkaistava yhtälö $9x + 7y = 2$. Ratkaisut ovat $x = -6 + 7t$, $t \in \mathbb{Z}$ [a]

9 / 10

[a] Yhtälö on ratkaistu aikaisemmin.

Lineaarinen kongruenssi — ratkaisutapa 2

Jos lineaarisessa kongruenssissa $ax \equiv b \pmod{m}$ moduli m on pieni, voidaan kokeilemalla etsiä yksittäisratkaisut ja niiden avulla kirjoittaa yleinen ratkaisu.

Esimerkki. Ratkaise $9x \equiv 2 \pmod{7}$.

Yksittäisratkaisuehdokkaat ovat 0, 1, 2, 3, 4, 5, 6.
Kokeilemalla todetaan, että $9 \cdot 1 \equiv 2 \pmod{7}$. Muut ehdokkaat eivät toteuta kongruenssia.
Täten ratkaisu on $x = 1 + 7t,\ t \in \mathbb{Z}$.

Jos mikään ehdokas ei ole ratkaisu, kongruenssilla ei ole ratkaisua.
Jokainen ehdokas on testattava!

10 / 10

Esimerkki

Kongruenssin $4x \equiv 2 \pmod{6}$ yksittäisratkaisuehdokkaat ovat 0, 1, 2, 3, 4, 5. Näistä $x = 2$ ja $x = 5$ toteuttavat kongruenssin, koska $6 \mid (4 \cdot 2 - 2)$ ja $6 \mid (4 \cdot 5 - 2)$. Muut ehdokkaat eivät toteuta kongruenssia.

Ratkaisu on siis $x = 2 + 6t$ tai $x = 5 + 6t$, eli yhdistettynä $x = 2 + 3t$, $t \in \mathbb{Z}$.

note 1 of slide 10