KONGRUENSSIT

(Kokonaislukujen kongruenssi)

esim 1 jakoyhtälönä

a) $\frac{38}{5}$ b) $\frac{143}{5}$ c) $\frac{3}{5}$

Ratk. a) $38 = 7 \cdot 5 + \boxed{3}$

b) $143 = 28 \cdot 5 + \boxed{3}$

c) $3 = 0 \cdot 5 + \boxed{3}$

Edellisen esimerkin luvuilla 3, 38, 143 on sama jakojäännös, kun ne jaetaan viidellä. Sanotaan, että luvut 3, 38, 143 ovat **kongruentteja** keskenään.

$$a \equiv b \pmod{n} \Leftrightarrow n \mid (a-b)$$

$a, b \in \mathbb{Z}$

$n \in \mathbb{N}$

"a on kongruentti b modulo n"

esim. Ovatko lauseet tosia (T)? epätosi (E)

a) $45 \equiv 3 \pmod 7$

b) $-4 \equiv 10 \pmod 7$

c) $65 \equiv 13 \pmod 7$

Ratk. a) $45-3 = 42 = 6\cdot 7$ eli $7 \mid (45-3)$ T

b) $-4-10 = -14 = -2\cdot 7$ eli $7 \mid (-4-10)$ T

c) ... $52 = 7\cdot 7 + 3$ eli $7 \nmid (65-13)$ E

$a \equiv b \pmod m$

luvuille a ja b on sama jakojäännös, kun ne jaetaan luvulla m.

esim. Mikä on jakojäännös, kun $753 + 6^{1201}$ jaetaan seitsemällä?

Ratk.

$$
\begin{aligned}
\underbrace{753}_{\text{jakoyhtälö}} + 6^{1201} &\equiv 107\cdot 7 + 4 + 6^{1201} \\
&\equiv 4 + 6^{1201} \\
&\equiv 4 + (-1)^{1201} \\
&\equiv 4 - 1 \\
&\equiv 3 \pmod 7
\end{aligned}
$$

$753 \equiv 4 \pmod 7$

$6 \equiv -1 \pmod 7$ $(6-(-1) = 7)$

$(-1)^{1201} = -1$

V: Jakojäännös on 3.

esim. Mikä on luvun 3^{2007} viimeinen numero?

Ratk. Luvun 3^{2007} viimeinen numero saadaan laskemalla kongruenssi modulo 10.

$$
\begin{aligned}
3^{2007} &\equiv 3^{2\cdot 1003 + 1} \\
&\equiv (3^2)^{1003} \cdot 3^1 \\
&\equiv 9^{1003} \cdot 3 \\
&\equiv (-1)^{1003} \cdot 3 \\
&\equiv -1 \cdot 3 \\
&\equiv -3 \\
&\equiv 7 \pmod{10}
\end{aligned}
$$

jakoyhtälö, potenssisäännöt

$9 \equiv -1 \pmod{10}$

$(-1)^{1003} = -1$

V: Luvun viimeinen numero on 7.

esim a) $2x \equiv 3 \pmod 5$

b) $2x \equiv 3 \pmod 6$

Ratk. a) taulukoidaan

x	$2x \equiv 3 \pmod 5$
0	$2 \cdot 0 \equiv 0 \not\equiv 3 \pmod 5$
1	$2 \cdot 1 \equiv 2 \not\equiv 3 \pmod 5$
2	$2 \cdot 2 \equiv 4 \not\equiv 3 \pmod 5$
3	$2 \cdot 3 \equiv 6 \not\equiv 3 \pmod 5$
4	$2 \cdot 4 \equiv 8 \equiv 3 \pmod 5$

$4-3=1$, $\frac{1}{5} \notin \mathbb{Z}$

Huomataan, että $x = 4$ tot. yhtälön.

$x = 4 + 5n$, $n \in \mathbb{Z}$

b) ei ratk. (taulukoimalla)

esim 2 $13x + 5 \equiv 3 \pmod{25}$

⊛ ratk. Diofantoksen yht. avulla

⊛ $(13x + 5) - 3 = 25y$

syt

lin. komb.

yht. ratk.

yhtäs. ratk.

V: $x = 21 + 25n$, $n \in \mathbb{Z}$