6. Kongruenssi

Määr. a ja b ovat **kongruentit modulo m**, merk. $a \equiv b \pmod m$
$\Leftrightarrow a - b = km$, $a, b, k, m \in \mathbb{Z}$, $m > 1$

Esim. $5 \equiv 11 \pmod 3$ koska $5 - 11 = -6 = -2 \cdot 3$
Toisaalta $5 = 1 \cdot 3 + 2$ ← sama jäännös
$11 = 3 \cdot 3 + 2$ ←
$5 \not\equiv 11 \pmod 4$ koska $5 - 11 = -6$ ei ole jaollinen 4:llä
Toisaalta $5 = 1 \cdot 4 + 1$ ← eri jäännös
$11 = 2 \cdot 4 + 3$ ←

Yleisesti $a \equiv b \pmod m \Leftrightarrow$ luvuilla a ja b on sama jäännös luvulla m jaettaessa

Lause Olkoon $a \equiv b$ ja $c \equiv d \pmod m$. Tällöin
$a + c \equiv b + d \pmod m$
$a \cdot c \equiv b \cdot d \pmod m$
$a^k \equiv b^k \pmod m$

Tod. $a \equiv b \pmod m \Leftrightarrow a - b = km$
$c \equiv d \pmod m \Leftrightarrow c - d = tm$
Tällöin $(a + c) - (b + d) = (a - b) + (c - d)$
$= km + tm$
$= m \underbrace{(k + t)}_{\in \mathbb{Z}} \Rightarrow a + c \equiv b + d \pmod m$

Siis: Kun tutkitaan jäännöstä luvulla m jaettaessa, summassa ja tulossa saa luvun ja potenssissa kantaluvun korvata sen kanssa kongruentilla luvulla (mod m).

6.2 a) $71 \equiv 3 \pmod 4 \Leftrightarrow 71 - 3 = 68 = 4 \cdot 17$ ✓ on jaollinen 4:llä
b) $48 \equiv -1 \pmod 7 \Leftrightarrow 48 - (-1) = 49 = 7 \cdot 7$ ✓ — " — 7:llä
c) $72 \equiv 0 \pmod{12} \Leftrightarrow 72 - 0 = 72 = 6 \cdot 12$ ✓ — " — 12:lla

6.8 a) $9^{24} - 5^{12} \overset{*}{\equiv} 1^{24} - 1^{12} = 1 - 1 = 0 \pmod 4 \Rightarrow$ jäännös : 0

[* $9 \equiv 1 \pmod 4$, $5 \equiv 1 \pmod 4$]

b) $9^{25} - 3^{13} \equiv 1^{25} - (-1)^{13} = 1 - (-1) = 2 \pmod 4$
$\Rightarrow$ ei ole jaollinen 4:llä (vaan jäännös on 2)