Tod. Kirja s. 59

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

6.2 a) $71 \equiv 3 \pmod 4$, koska $71-3 = 68 = 17\cdot 4$

$\big[\; 71 = 17\cdot 4 + 3$

$3 = 0\cdot 4 + 3 \;\big]$

b) $48 \equiv -1 \pmod 7$, koska $48-(-1) = 49 = 7\cdot 7$

c) $72 \equiv 0 \pmod{12}$, koska $72-0 = 72 = 6\cdot 12$ $\quad 5^{2} 47$

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

$\Rightarrow$ jakojäännös: $\underline{0}$ (ts. on jaollinen luvulla 4)

$\big[\, (*)\ 9 \equiv 1 \pmod 4$ ja $5 \equiv 1 \pmod 4 \,\big]$

b) $9^{25} - 3^{13} \overset{(*)}{\equiv} 1^{25} - (-1)^{13} = 1-(-1) = 1+1 = 2 \pmod 4$

(tai: $\equiv$)

$\big[\, (*)\ 9 \equiv 1 \pmod 4,\quad 3 \equiv -1 \pmod 4 \,\big]$

koska 2 ei ole jaollinen luvulla 4, ei alkuperäinen luku ole jaollinen luvulla 4 (vaan jakojäännös = 2)

Huom. $\left.\begin{array}{l} 2^5 = 32 \\ 2^2 = 4 \end{array}\right\} \Rightarrow 32 \not\equiv 4 \pmod 3$ vaikka $5 \equiv 2 \pmod 3$

Siis potenssissa eksponenttia ei saa korvata sen kanssa kongruentilla luvulla mod m.

6.9 $2^{2100} = (2^3)^{700} = 8^{700} \overset{(*)}{\equiv} 1^{700} = 1 \pmod 7$

$\Rightarrow$ jakojäännös: 1

$\big[\, (*)\ 8 \equiv 1 \pmod 7 \,\big]$

Esim. $5623467 = 5\cdot 10^6 + 6\cdot 10^5 + 2\cdot 10^4 + 3\cdot 10^3 + 4\cdot 10^2 + 6\cdot 10 + 7$

$\overset{(*)}{\equiv} 5\cdot 1^6 + 6\cdot 1^5 + 2\cdot 1^4 + 3\cdot 1^3 + 4\cdot 1^2 + 6\cdot 1 + 7$

$= 5+6+2+3+4+6+7 = 33 \equiv 0 \pmod 3$

$\big[\, (*)\ 10 \equiv 1 \pmod 3 \,\big]$

Yleisesti: Kokonaisluku on jaollinen luvulla 3 $\Leftrightarrow$ numeroiden summa on jaollinen luvulla 3.