

6.22 Väite $16 \cdot 7^{2n} - 28 \cdot 3^{2n+3}$ on jaollinen luvulla 5 aina kun $n \in \mathbb{Z}_+$

Tod. $16 \cdot 7^{2n} - 28 \cdot 3^{2n+3} = 16 \cdot (7^2)^n - 28 \cdot 3^{2n} \cdot 3^3$ ($= \{1, 2, 3, \dots\}$)
 $= 16 \cdot 49^n - 28 \cdot (3^2)^n \cdot 27$
 $\stackrel{(*)}{=} 1 \cdot (-1)^n - 3 \cdot (-1)^n \cdot 2$
 $= (-1)^n - 6(-1)^n$
 $\stackrel{(*)}{=} (-1)^n - 1 \cdot (-1)^n$
 $= (-1)^n - (-1)^n$
 $= 0 \pmod{5}$

$\Rightarrow$ väite m.o.t.

$(*) \begin{cases} 16 \equiv 1, 49 \equiv -1, 28 \equiv 3, \\ 3^2 \equiv -1, 27 \equiv 2, 6 \equiv 1 \\ \pmod{5} \end{cases}$

6.12 Väite $M^5 - M$ on jaollinen luvulla 5 aina kun $M \in \mathbb{Z}$

Tod. I M on jollakin seuraavista muodoista:

1° $M = 5k : M^5 - M = (5k)^5 - 5k = 5^5 k^5 - 5k = 5(5^4 k^5 - k)$
 $\in \mathbb{Z}$ on jaollinen 5:llä

2° $M = 5k+1 : M^5 - M = (5k+1)^5 - (5k+1)$
 $= \dots 5 \cdot (\dots) \pmod{5}$
 $\in \mathbb{Z}$

5° $M = 5k+4 : M^5 - M = \dots = 5(\dots) \pmod{5}$
 $\in \mathbb{Z}$

1° - 5° $\Rightarrow$ väite

II M on jollakin seuraavista muodoista

1° $M \equiv 0 \pmod{5} : M^5 - M \equiv 0^5 - 0 \equiv 0 \pmod{5}$

2° $M \equiv 1 \pmod{5} : M^5 - M \equiv 1^5 - 1 = 1 - 1 = 0 \pmod{5}$

3° $M \equiv 2 \pmod{5} : M^5 - M \equiv 2^5 - 2 = 32 - 2 = 30 \equiv 0 \pmod{5}$

4° $M \equiv 3 \pmod{5} : M^5 - M \equiv 3^5 - 3 = 243 - 3 = 240 \equiv 0 \pmod{5}$

5° $M \equiv 4 \pmod{5} : M^5 - M \equiv 4^5 - 4 = 1024 - 4 = 1020 \equiv 0 \pmod{5}$

1° - 5° $\Rightarrow$ väite

III $M^5 - M = M(M^4 - 1) = M((M^2)^2 - 1^2)$
 $= M \underset{\uparrow 2}{(M^2 - 1)} \underset{\uparrow 2}{(M^2 + 1)} = M(M-1)(M+1)(M^2+1)$
 $\equiv M(M-1)(M+1) \underset{\leftarrow 2^2}{(M^2 - 4)} \pmod{5}$
 $= \underbrace{M(M-1)(M+1)(M-2)(M+2)}_{5 \text{ perättäistä kokonaislukua}}$