Inverso di 51 modulo $\varphi(10) = \varphi(2 \cdot 5) = (2-1)(5-1) = 4$

Sono coprimi? Si

$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$

$51 \equiv 3 \mod 16$

51 mod 16

$3^{8-1} \mod 16 \equiv 3^7 \mod 16 = 3^3 \cdot 3^3 \cdot 3 \mod 16 \equiv$

$27 \cdot 27 \cdot 3 \mod 16 \rightarrow 11 \cdot 11 \cdot 3 \mod 16 \rightarrow 11 \cdot 33 \mod 16$

$\rightarrow 11 \cdot 1 \mod 16 \equiv 11 \mod 16$

l'inverso è questo per verificare che è giusto facciamo

$51 \cdot 11 \equiv 1 \mod 16$

Pg 134 n 1

$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$

$9^{100} \mod 8$

$9^{100 \mod 4} \mod 8 \equiv 9^0 \mod 8 \rightarrow 1$

n 2

$15^{80} \mod 16$

$\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$

$15^{80 \mod 8} \mod 16$

$15^0 \mod 16 = 1$

n 3

$13^{40} \mod 19 = ?$ $\quad \varphi(19) = 19-1 = 18$

$13^{40 \mod 18} \mod 19$

$13^{4} \mod 19 \equiv (-6)^4 \mod 19 \equiv (-6)^2 \cdot (-6)^2 \mod 19 \equiv 36 \cdot 36 \mod 19$

$17 \cdot 17 \mod 19 \equiv -2 \cdot (-2) \equiv 4 \mod 19$

↳ risultato finale

a)

$11^{57} \mod 23$

$\varphi(23) = 23-1 = 22$

$11^{57 \mod 22} \mod 23 \equiv 11^{13} \mod 23 \equiv (11)^{12} \cdot 11 \mod 23 \equiv$

$\equiv (11^3)^4 \cdot 11 \mod 23 \equiv (-3)^4 \cdot 11 \mod 23 \equiv 81 \cdot 11 \mod 23$

$11^3 \mod 23 \equiv 121 \cdot 11 \equiv 6 \cdot 11 \mod 23 \equiv 66 \mod 23 \equiv -3 \mod 23$

↳ $121 \mod 23$

$\equiv 12 \cdot 11 \mod 23 \equiv 132 \mod 23 \equiv 17 \mod 23$

Inverso di $63 \mod 10$

$\varphi(10) = \varphi(2 \cdot 5) = (2-1) \cdot (5-1) = 1 \cdot 4 = 4$

$63 \equiv 3 \mod 10$

$63 \mod 10$

$3^{4-1} \mod 10 \equiv 3^{3} \mod 10 \equiv 27 \mod 10 \equiv 7 \mod 10$

$3 \cdot 7 \mod 10 \equiv 1 \mod 10$

4) Inverso di $72 \mod 5$

$72 \equiv x \mod 5$ $\qquad \varphi(5) = 5-1 = 4$

$72 \equiv 2 \mod 5$

$2^{4-1} \mod 5 \equiv 2^{3} \mod 5 \equiv 8 \mod 5 \equiv 3 \mod 5$

$2 \cdot 3 \equiv 6 \mod 5$

5) $7^{50} \mod 11$

$\varphi(11) = 11 - 1 = 10$

$7^{50 \mod 10} \mod 11 \equiv 7^{0} \mod 11 \equiv 1 \mod 11$

7)

$29^{101} \mod 31$ $\qquad \varphi(31) = 31 - 1 = 30$

$29^{101 \mod 30} \mod 31 \equiv 29^{11} \mod 31 \equiv (-2)^{11} \mod 31 \equiv$

$\equiv (-2)^5 \cdot (-2)^5 \cdot (-2) \mod 31$

$-32 \cdot -32 \cdot -2 \mod 31$

$-1 \quad -1 \quad -2 \mod 31$

$-2 \mod 31 \equiv 29 \mod 31$

6) $40^{60} \cdot 60^{40} \mod 31$ $\qquad \varphi(31) = 31 - 1 = 30$

$40^{60 \mod 30} \cdot 60^{40 \mod 30} \mod 31 \equiv 40^{0} \cdot 60^{10} \mod 31 \equiv 60^{10} \mod 31$

$\equiv (-2)^5 \cdot (-2)^5 \mod 31 \equiv 1 \cdot (-32)(-32) \mod 31$

$1 \; (-1)(-1) \equiv 1 \mod 31$

5) inverso di 83 mod 10

$\varphi(10) = (5-1)(2-1) = 4 \cdot 1 = 4$

$83 \equiv 3 \mod 10$

$3 \cdot 7 \mod 10 \equiv 1 \mod 10$

$3^{4-1} \mod 10 \equiv 27 \mod 10 \equiv 7 \mod 10$

6) Inverso di $97 \mod 11$

$\varphi(11) \equiv 11 - 1 \equiv 10$

$97 \equiv 9 \mod 11$

$9^{10-1} \mod 11 \equiv 9^9 \mod 11 \equiv 9^8 \cdot 9^1 \mod 11 \equiv (-2)^8 \cdot 9^1 \mod 11$

$9 \cdot 11$

$(-2)^4 (-2)^4 \cdot 9^1 \mod 11$

$16 \cdot 16 \cdot 9 \mod 11 \equiv 5 \cdot 5 \cdot 9 \mod 11 \equiv 25 \cdot 9 \mod 11$

$\equiv 3 \cdot 9 \mod 11 \equiv 27 \mod 11 \equiv 5 \mod 11$

$9 \cdot 5 \mod 45 \equiv 1 \mod 45$

Inverso di $100 \mod 23$

$\varphi(23) = 23 - 1 = 22$

$100 \equiv 8 \mod 23$

$8^{22-1} \mod 23 \equiv 8^{21} \mod 23 \equiv 8^{20} \cdot 8^1 \mod 23$

$\equiv (8^4)^5 \cdot 8^1 \mod 23 \equiv 32 \cdot 8 \mod 23 \equiv 9 \cdot 8 \mod 23 \equiv$

$8^4 \mod 23 \equiv 8^2 \cdot 8^2 \mod 23 \equiv 64 \cdot 64 \mod 23 \equiv -5 \cdot -5 \mod 23$

$\equiv 25 \mod 23 \equiv 2 \mod 23$

$\equiv 72 \mod 23 \equiv 3 \mod 23$

$3 \cdot 8 \mod 23 \equiv 1 \mod 23$

↳ queste è lo verifica