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

Sono coprimi? Si

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

$51 \equiv 3 \bmod 16$

$51 \bmod 16$

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

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

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

$\rightarrow$ l'inverso è questo per verificare che è giusto facciamo

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

Pg 134 n 1

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

$9^{100} \bmod 8$

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

n 2

$15^{80} \bmod 16$

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

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

$15^0 \bmod 16 = 1$

n 3

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

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

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

$17 \cdot 17 \bmod 19 \equiv -2 \cdot (-2) \equiv \underbrace{4}_{\text{risultato finale}} \bmod 19$

a)

$11^{57} \bmod 23$

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

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

$\equiv (11^{3})^{4} \cdot 11 \bmod 23 \equiv (-3)^{4} \cdot 11 \bmod 23 \equiv 81 \cdot 11 \bmod 23$

$11^{3} \bmod 23 \equiv \underbrace{121}_{121 \bmod 23} \cdot 11 \equiv 6 \cdot 11 \bmod 23 \equiv 66 \bmod 23 \equiv -3 \bmod 23$

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

Inverso di 63 mod 10

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

$63 \equiv 3 \bmod 10$

63 mod 10

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

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

4) Inverso di 72 mod 5

$72 \equiv x \bmod 5$

$\varphi(5) = 5-1 = 4$

$72 \equiv 2 \bmod 5$

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

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

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

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

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

7)

$29^{101} \bmod 31$ $\quad\quad\quad\quad \varphi(31) = 31 - 1 = 30$

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

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

$-32 \cdot -32 \cdot -2 \bmod 31$

$-1 \quad -1 \quad -2 \bmod 31$

$-2 \bmod 31 \equiv 29 \bmod 31$

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

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

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

$1 (-1)(-1) \equiv 1 \bmod 31$

5) inverso di 83 mod 10

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

$83 \equiv 3 \bmod 10$ $\qquad 3 \cdot 7 \bmod 10 = 1 \bmod 10$

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

6) inverso di 97 mod 11

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

$97 \equiv 9 \bmod 11$

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

$9 - 11$

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

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

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

$9 \cdot 5 = 45 \equiv 1 \bmod 11$

Inverso di 100 mod 23

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

$100 \equiv 8 \bmod 23$

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

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

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

$\equiv 25 \bmod 23 \equiv 2 \bmod 23$

$\equiv 72 \bmod 23 \equiv 3 \bmod 23$

$\underbrace{3 \cdot 8 \bmod 23 \equiv 1 \bmod 23}$

↳ questa è la verifica