INVERSO DI $51 \bmod 16$ $\quad 16 = 2^4$

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

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

$$51 \equiv 3 \bmod 16$$

$$3^{8-1} \bmod 16 \equiv 3^7 \bmod 16 \equiv 3^3 \cdot 3^3 \cdot 3^1 \equiv 27 \cdot 27 \cdot 3 \bmod 16 \longrightarrow$$

$$\longrightarrow 11 \cdot \underbrace{11 \cdot 3} \bmod 16$$

$$11 \cdot 33 \bmod 16$$

$$11 \cdot 1 \bmod 16$$

$$11 \bmod 16 \equiv 11 \bmod 16$$

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

$$3 \cdot 11 \equiv \longrightarrow 33 \equiv 1 \bmod 16$$

questo 3 è il resto di $51 \bmod 16$

PAG 134 n° 1 (RIS: 1)

$9^{100} \mod 8$ $\quad \varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$

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

2) (RIS: 1)

$15^{80} \mod 16$

$15 \equiv -1 \mod 16$ → POSSO ANCHE LASCIARE 15

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

$-1^{80 \mod 8} \mod 16$ → $-1^0 \mod 16 \equiv 1$

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

$15^0 \mod 16 \equiv 1$

3) (R15: 4)

$13^{40} \mod 19$

$\varphi(19) = 19 - 1 = 18$

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

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

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

4)

$11^{57} \mod 23$

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

$11^{57 \mod 22} \mod 23$

PRIMA FA ALLA 3 e IL 4 LO FA DOPO

$11^{13} \mod 23 \equiv 11^{12} \cdot 11^{1} \mod 23 \equiv (11^{3})^{4} \cdot 11^{1} \mod 23$ —0

→ $11^{3} = 121 \cdot 11 \equiv 6 \cdot 11 \mod 23 \equiv 66 \mod 23 \equiv -3 \mod 23$ —D

→ $(-3)^{4} \cdot 11 \mod 23 \equiv 81 \cdot 11 \mod 23 \equiv 12 \cdot 11 \mod 23 \equiv$

$132 \mod 23 \equiv 17 \mod 23$

INVERSO DI $63 \mod 10$

$63 \equiv 3 \mod 10$ $\quad \varphi(10) = 4$

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

$3 \cdot 7 = 21 \equiv 1 \mod 10$

INVERSO di $72 \bmod 5$

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

$72 \equiv 2 \bmod 5$ $\qquad 2^{4-1} \bmod 5 \equiv 2^3 \bmod 5 = 8 \bmod 5 \equiv 3 \bmod 5$

$2 \cdot 3 = 6 \equiv 1 \bmod 5$

5) $7^{50} \bmod 11$ CALCOLO DEL MODULO

$\varphi(11) = 10$

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

6)

$40^{60} \cdot 60^{40} \bmod 31$ $\qquad \varphi(31) = 30$

$40^{60 \bmod 30} \cdot 60^{40 \bmod 30}$

$40^0 \cdot 60^{10} \bmod 31 = 1 \cdot (-2)^5 \cdot (-2)^5 = 1 \cdot \underset{\downarrow -1}{-32} \cdot \underset{\downarrow -1}{-32} \bmod 31$

$1 \bmod 31$

INVERSO DI 83 mod 10

$\varphi(10) = 4$

$83 \equiv 3 \bmod 10$

$3 \cdot 7 \equiv 21 \equiv 1 \bmod 10$

$4-1$

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

INVERSO DI 97 mod 11

$\varphi(11) = 10$

$97 \equiv 9 \bmod 11$

$9^{10-1} \bmod 11 \equiv 9^8 \cdot 9^1 \bmod 11 \equiv (-2^8) \cdot 9^1 \equiv -2^4 \cdot -2^4 \cdot 9^1 \bmod 11$

Se il numero (9) è minore del modulo (11) lì sottrazione (-2) è continua (anziché fare la congruenza)

$16 \cdot 16 \cdot 9 \bmod 11$

$5 \cdot 5 \cdot 9 \bmod 11$

$25 \cdot 9$

$3 \cdot 9 \bmod 11$

$27 \equiv 5 \bmod 11$

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

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