Calcolare $145^{145} \bmod 13$

$$145^{145 \bmod \phi(13)} \equiv 145^{145 \bmod 12} \equiv 145 \bmod 13 \equiv 2$$

Verificare che $11^{13} \bmod 17 = 17^{13} \bmod 11$

$$11^{13} \bmod 17 = [(11 \bmod 17) \cdot ((11^2)^6 \bmod 17)] \bmod 17 =$$
$$= \{11 \cdot [(121 \bmod 17)^6 \bmod 17]\} \bmod 17 =$$
$$= \{11 \cdot [2^6 \bmod 17]\} \bmod 17 = \{11 \cdot 13\} \bmod 17 = 7$$

$$17^{13} \bmod 11 = 17^{13 \bmod \phi(11)} \bmod 11 = 17^3 \bmod 11 = (17 \bmod 11)^3 \bmod 11 =$$
$$= 6^3 \bmod 11 = [(6 \bmod 11) \cdot (6^2 \bmod 11)] \bmod 11 = (6 \cdot 3) \bmod 11 = 7$$

INVERSO MOD. DI 11 mod 7

$$(n \bmod m)^{\phi(m)-1} \bmod m$$

$$(11 \bmod 7)^5 \bmod 7 = 4^5 \bmod 7 = [(4^2 \bmod 7) \cdot (4^2 \bmod 7) \cdot (4 \bmod 7)] \bmod 7 = 2$$

INVERSO MOD. DI 30 mod 11

$$(30 \bmod 11)^{\phi(11)-1} \bmod 11 = 8^9 \bmod 11 = [(8 \bmod 11) \cdot (64^4 \bmod 11)] \bmod 11$$
$$= [8 \cdot (64 \bmod 11)^4 \bmod 11] \bmod 11 =$$
$$= [8 \cdot (9^4 \bmod 11)] \bmod 11 = [8 \cdot (9^2 \bmod 11)^2 \bmod 11] \bmod 11$$
$$= 7$$

VERIFICO:

$(7 \cdot 30) \bmod 11 = 1 \bmod 11$

$1 = 1$

$9^{100} \bmod 8$ $= 9^{100 \bmod \phi(8)} \bmod 8 = 9^{100 \bmod 4} \bmod 8 = 9^0 \bmod 8 = 1 \bmod 8 = 1$

$15^{80} \bmod 16$ $= 15^{80 \bmod \phi(16)} \bmod 16 = 15^{80 \bmod 8} \bmod 16 = 1$

$13^{40} \bmod 19$ $= 13^{40 \bmod \phi(19)} \bmod 19 = 13^{40 \bmod 18} \bmod 19 = 13^4 \bmod 19 =$
$= [(13^2 \bmod 19)(13^2 \bmod 18)] \bmod 19 = 17^2 \bmod 19 =$
$= (-2)^2 \bmod 19 = 4 \bmod 19 = 4$

$11^{57} \bmod 23$ $= 11^{57 \bmod \phi(23)} \bmod 23 = 11^{57 \bmod 22} \bmod 23 = 11^{13} \bmod 23 =$
$= [(11 \bmod 23) \cdot (121^6 \bmod 23)] \bmod 23 =$
$= \{11 \cdot [(121 \bmod 23)^6 \bmod 23]\} \bmod 23 =$
$= \{11 \cdot [6^6 \bmod 23]\} \bmod 23 =$
$= \{11 \cdot [(36 \bmod 23)^3 \bmod 23]\} \bmod 23 =$
$= \{11 \cdot [13^3 \bmod 23]\} \bmod 23 =$
$= \{11 \cdot [(169 \bmod 23) \cdot 13]\} \bmod 23 \} \bmod 23 =$
$= \{11 \cdot [104 \bmod 23]\} \bmod 23 = (11 \cdot 12) \bmod 23 = 132 \bmod 23 = 17$

$7^{50} \bmod 11$ $= 7^{50 \bmod \phi(11)} \bmod 11 = 7^0 \bmod 11 = 1$

$40^{60} \cdot 60^{40} \bmod 31$ $= [(40^{60} \bmod 31) \cdot (60^{40} \bmod 31)] \bmod 31 = (60^{40} \bmod 31) \bmod 31$
$\cdot 40^{60} \bmod 31 = 40^{60 \bmod \phi(31)} \bmod 31 = 1$
$\cdot 60^{40} \bmod 31 = 60^{40 \bmod \phi(31)} \bmod 31 = 60^{10} \bmod 31 =$
$= (60 \bmod 31)^{10} \bmod 31 = 29^{10} \bmod 31 = [(29^2 \bmod 31)^5 \bmod 31] =$
$= (841 \bmod 31)^5 \bmod 31 = 4^5 \bmod 31 = [(4 \bmod 31)(4^4 \bmod 31)] \bmod 31$
$= \{4 \cdot [((4^3 \bmod 31) \cdot (4 \bmod 31)) \bmod 31]\} \bmod 31 = \{4 \cdot 8\} \bmod 31 = 1$
$= 1 \bmod 31 = 1$

$29^{101} \bmod 31$

$$= 29^{101 \bmod \phi(31)} \bmod 31 = 29^{101 \bmod 30} \bmod 31 = 29^{11} \bmod 31 =$$
$$= [(29 \bmod 31) \cdot (29^{10} \bmod 31)] \bmod 31 = [29 \cdot (29^{10} \bmod 31)] \bmod 31$$
$$= \{29 \cdot [(29^2 \bmod 31)^5 \bmod 31]\} \bmod 31 = \{29 \cdot [4^5 \bmod 31]\} \bmod 31 =$$
$$= \{29 \cdot [((4^3 \bmod 31)(4^2 \bmod 31)) \bmod 31]\} \bmod 31 = \{29 \cdot 1\} \bmod 31 = 29$$

$$(n \bmod m)^{\phi(m)-1} \bmod m$$

Inverso di 49 modulo 23

$$(49 \bmod 23)^{\phi(23)-1} \bmod 23 = 3^{21} \bmod 23 = (3^3 \bmod 23)^7 \bmod 23 =$$
$$= 4^7 \bmod 23 = [(4^3 \bmod 23)(4^4 \bmod 23)] \bmod 23 =$$
$$= \{18 \cdot [((4^3 \bmod 23)(4 \bmod 23)) \bmod 23]\} \bmod 23 =$$
$$= \{18 \cdot [(18 \cdot 4) \bmod 23]\} \bmod 23 = \{18 \cdot 3\} \bmod 23 =$$
$$= 8$$

Inverso di 51 modulo 16

$$(51 \bmod 16)^{\phi(16)-1} \bmod 16 = 3^7 \bmod 16 = [(3^3 \bmod 16)(3^3 \bmod 16)(3 \bmod 16)] \bmod 16 =$$
$$= (11 \cdot 11 \cdot 3) \bmod 16 = (11^2 \cdot 3) \bmod 16 =$$
$$= [(11^2 \bmod 16)(3 \bmod 16)] \bmod 16 = 27 \bmod 16 = 11$$

Inverso di 63 modulo 10

$$(63 \bmod 10)^{\phi(10)-1} \bmod 10 = 3^3 \bmod 10 = 27 \bmod 10 = 7$$

Inverso di 72 modulo 5

$$(72 \bmod 5)^{\phi(5)-1} \bmod 5 = 2^3 \bmod 5 = 3$$

Inverso di 83 modulo 10

$$(83 \bmod 10)^{\phi(10)-1} \bmod 10 = 3^3 \bmod 10 = 7$$

Inverso di 97 modulo 11

$$(97 \bmod 11)^{\phi(11)-1} \bmod 11 = 9^9 \bmod 11 = [(9^2 \bmod 11)(9^7 \bmod 11)] \bmod 11 =$$
$$= \{4 \cdot [(9^2 \bmod 11)(9^2 \bmod 11) \cdot (9^2 \bmod 11)(9 \bmod 11)] \bmod 11\} \bmod 11 =$$
$$= \{4 \cdot (4 \cdot 4 \cdot 4 \cdot 9) \bmod 11\} \bmod 11 =$$
$$= \{4 \cdot (4^3 \cdot 9) \bmod 11\} \bmod 11 =$$
$$= \{4 \cdot [(4^3 \bmod 11)(9 \bmod 11)] \bmod 11\} \bmod 11 =$$
$$= \{4 \cdot (81 \bmod 11)\} \bmod 11 = (4 \cdot 4) \bmod 11 = 5$$

Inverso di 100 modulo 23

$$(100 \bmod 23)^{\phi(23)-1} \bmod 23 = 8^{21} \bmod 23 = (8^3 \bmod 23)^7 \bmod 23 = 6^7 \bmod 23 =$$
($6^7 = 6^3 \cdot 6^3 \cdot 6$)
$$= [(486 \bmod 23)] \bmod 23 = 3 \bmod 23 = 3$$