Tavola n. 6.2 Potenze modulo n

L'algoritmo dei quadrati successivi

Osserva il seguente esempio: vogliamo calcolare

$$17^{31} \bmod 58$$

Scriviamo 31 in forma polinomiale in base 2

$31 = 2 \times 15 + 1 = 2 \times (2 \times 7+1)+ 1 = 2 \times (2 \times (2 \times 3+1)+1)+ 1$

$= 2 \times (2 \times (2 \times (2 \times 1+1)+1)+1)+ 1 = 2^4 + 2^3 + 2^2 + 2 + 1$

Dunque $17^{31} = 172^4 + 2^3 + 2^2 + 2 + 1$

Procediamo dividendo per 2 l'esponente, ad ogni passo:

$17^{31} = (17^{15})^2 \times 17 =$

$((17^7)^2 \times 17)^2 \times 17 =$

$(((17^3)^2 \times 17)^2 \times 17)^2 \times 17 =$

$(((17^2 \times 17)^2 \times 17)^2 \times 17)^2 \times 17 =$

Ora distribuiamo le potenze

$((17^4 \times 17^2 \times 17)^2 \times 17)^2 \times 17 =$

$(17^8 \times 17^4 \times 17^2 \times 17)^2 \times 17 =$

$17^{16} \times 17^8 \times 17^4 \times 17^2 \times 17$

Ora basta calcolare: $17^2 =$; $17^4 =$; $17^8 =$; $17^{16} =$

e farne il prodotto, ottenendo:

Osserva che gli esponenti utilizzati provengono dalla scrittura di 31 in base 2:

$$31 = 2^4 + 2^3 + 2^2 + 2 + 1 = 16 + 8 + 4 + 2 + 1$$

Prova a calcolare 3^{13} modulo 7