

Istnieją liczby całkowite x, y takie, że $ax+by=\text{NWD}(a,b)$.

Ile wynosi $(12)^{-1} \bmod 7$?

$$12=7+5 \Rightarrow 12-7=5$$

$\Downarrow$

$$7=5+2 \Rightarrow 7-5=2$$

$\Downarrow$

$$5=2 \times 2 + 1 \Rightarrow 5 - 2 \times 2 = 1$$

$$(-2) \times 7 + 3 \times (12 - 7) = 1 \Rightarrow 3 \times 12 + (-5) \times 7 = 1$$

$\Uparrow$

$$5 - 2 \times (7 - 5) = 1 \Rightarrow (-2) \times 7 + 3 \times 5 = 1$$

Zatem odwrotnością 12 modulo 7 jest 3.