

# Inverso di e (mod f)

---

Ricordando che

$a \bmod m =$  resto divisione

$a \equiv b \bmod m$  significa  $a \bmod m = b \bmod m$

$de \equiv 1 \bmod (p-1) (q-1)$

$de \equiv 1 \bmod \varphi(n)$

$de \equiv 1 \bmod f$

$de \bmod f = 1 \bmod f$

**$de \bmod f = 1$**

Conosco il numero **e**, conosco il numero **f** e so che sono coprimi.

C'è un numero **d** tale che il **resto** della divisione **(d \* e) / f** è **1**?

Per esempio prendiamo come numeri **e = 5** ed **f = 7**.

I due numeri sono coprimi perché il massimo comune divisore tra 5 e 7 è 1.

A questo punto arriva la domanda:

**C'è un numero d tale che il resto della divisione (d \* 5) / 7 è 1?**

La risposta è **si**, e il numero **d** che cerchiamo è **3**.

Infatti **3 x 5 = 15**, e il **resto della divisione 3\*5/7 è 1**.

Cioè **3\*5 mod 7 = 1**

Un modo sintetico per dire che "il resto della divisione **(d \* e) / f** è **1**" è il seguente:

"**d è l'inverso di e (mod f)**" o "**d è l'inverso (mod f) di e**".

Di seguito alcuni esempi:

- l'inverso (mod 7) di 5 è 3 perché  $3 \times 5 = 15$  e  $15 \bmod 7 = 1$
- l'inverso (mod 7) di 3 è 5 perché  $3 \times 5 = 15$  e  $15 \bmod 7 = 1$
- l'inverso (mod 7) di 6 è 6 perché  $6 \times 6 = 36$  e  $36 \bmod 7 = 1$
- l'inverso (mod 43) di 11 è 4 perché  $11 \times 4 = 44$  e  $44 \bmod 43 = 1$

l'inverso (mod 12) di 3 NON c'è perché il massimo comune divisore tra 12 e 3 è diverso da 1