

Resto di una divisione e MOD

Il resto di una divisione è ciò che rimane dopo aver sottratto il più grande multiplo del divisore che è minore o uguale al dividendo.

Nel caso della divisione $659 \div 661$:

- Il **divisore** è **661**, e il **dividendo** è **659**.
- Poiché **659** è minore di **661**, il più grande multiplo di **661** che è minore o uguale a **659** è **0**.
- Quindi, sottraendo 0 da 659, otteniamo 659.

In termini matematici, possiamo esprimere la divisione come:

$$659 = 661 \times 0 + 659$$

Pertanto, il resto della divisione è 659 e significa che non è divisibile .

Quando si dice che il resto di una divisione è diverso da zero, significa che il numero non è divisibile dal divisore.

Nel caso di $659 \div 661$:

- **Resto:** 659
- **Divisore:** 661

Poiché il resto è **659** (diverso da zero), ciò indica che **659** non è divisibile per **661**. In altre parole, non puoi dividere **659** in parti uguali di **661** senza avere una parte restante.

Quindi, **659** non è un multiplo di **661**, e quindi non è divisibile.

Immagina di avere una torta che desideri dividere tra un certo numero di persone. Ecco un esempio per chiarire il concetto di divisibilità e resto usando la torta come metafora.

Scenario:

Hai **8 fette di torta** e vuoi dividerle tra **3 persone**.

Calcolo:

1. **Divisione:**

- Ogni persona può ricevere **2 fette** di torta.
- Dopo aver dato **2 fette** a ciascuna delle **3 persone**, hai usato $3 \times 2 = 6$ fette.

2. Fette rimaste:

- Totale fette: **8**
- Fette date: **6**
- **Fette rimaste:** $8 - 6 = 2$

Interpretazione:

- **Ogni persona riceve:** 2 fette
- **Fette rimaste:** 2
- **Resto:** 2 (perché $8 \div 3 = 2$ con un resto di **2**)

Conclusione:

- **Divisibilità:** Non puoi dividere le 2 fette rimaste tra le 3 persone senza tagliarle ulteriormente, quindi **non sono divisibili in modo equo**.
- **Resto:** Le 2 fette sono ciò che rimane dopo la divisione e indicano che **8** non è divisibile esattamente per **3**.

Questo esempio mostra come una quantità può essere divisa, e quando non è completamente divisibile, rimane un resto.

Rimanendo in tema di RSA e modulo segue che $8 \text{ MOD } 6 = 2$