ES. : CALCOLARE LE ULTIME DUE CIFRE DI

$$7^{91}.$$

SI CHIEDE DI CALCOLARE

$$\left[7^{91}\right]_{100}.$$

POICHE' $(100,7)=1$ $\Rightarrow$ TEO. DI EULERO $\Rightarrow$

$$\left[7^{\Phi(100)}\right]_{100}=\left[1\right]_{100}.$$

MA $\varphi(100) = 40 \Rightarrow [7^{40}]_{100} = [1]_{100}$. PERTANTO

$$[7^{91}]_{100} = \left([7^{40}]_{100}\right)^2 \cdot [7^{11}]_{100}$$

$$= \left([1]_{100}\right)^2 \cdot [7^{11}]_{100}$$

$$= [7^{11}]_{100}.$$

CALCOLIAMO

$$[7^{11}]_{100}$$

ABBIAMO CHE $11 = 8+2+1$. MA

$$[7^2]_{100} = [49]_{100}$$

$$[7^4]_{100} = \left([7^2]_{100}\right)^2 = \left([49]_{100}\right)^2 = [49^2]_{100} =$$

$$= [2401]_{100} = [1]_{100}$$

$$[7^8]_{100} = \left([7^4]_{100}\right)^2 = \left([1]_{100}\right)^2 = [1^2]_{100} = [1]_{100}.$$

PERTANTO

$$[7^{11}]_{100} = [7^8]_{100} \cdot [7^2]_{100} \cdot [7^1]_{100} =$$

$$= [1]_{100} \cdot [49]_{100} \cdot [7]_{100}$$

$$= [(49) \cdot 7]_{100} = [343]_{100} = [43]_{100}$$

CONCLUDENDO

$$[7^{91}]_{100} = [7^{11}]_{100} = [43]_{100}$$

QUINDI LE ULTIME DUE CIFRE DI 7^{91} SONO 43.

ES.: SIA $n \in \mathbb{P}$ E SIA

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0$$

LA SUA ESPRESSIONE DECIMALE ($0 \leq a_0, a_1, \ldots, a_k \leq 9$). DIMOSTRARE CHE

$$3 \mid n \iff 3 \mid (a_0 + a_1 + \ldots + a_k).$$

DIMOSTRIAMO CHE

$$[n]_3 = [a_0 + a_1 + \dots + a_k]_3 .$$

ABBIAMO CHE $[10]_3 = [1]_3$. QUINDI, SE $k \in \mathbb{P}$,

$$[10^k]_3 = \left([10]_3\right)^k = \left([1]_3\right)^k = [1]_3 .$$

PERTANTO

$$[n]_3 = [a_k \cdot 10^k + \dots + a_1 \cdot 10 + a_0]_3$$

$$= [a_k]_3 \cdot [10^k]_3 + \ldots + [a_1]_3 \cdot [10]_3 + [a_0]_3$$

$$= [a_k]_3 \cdot [1]_3 + \ldots + [a_1]_3 \cdot [1]_3 + [a_0]_3$$

$$= [a_k + \ldots + a_1 + a_0]_3 .$$

ES.: SIA $n \in \mathbb{P}$, $n \geq 3$. DIMOSTRARE CHE $\Phi(n)$ È PARI.

(PER ES., $\Phi(3)=2$, $\Phi(4)=2$, $\Phi(5)=4$, $\Phi(6)=2$, ETC...)

ABBIAMO CHE

$$\Phi(n) = \left| \{ 1 \leq i \leq n-1 : (i,n)=1 \} \right|$$

MA, SE $1 \leq i \leq n-1$, ALLORA

$$(i, n) = 1 \iff (n-i, n) = 1 \qquad (*)$$

INFATTI, SIA $(i, n) = 1$. PER ASSURDO, SIA $(n-i, n) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid (n-i, n) \Rightarrow p \mid (n-i)$ E

$p \mid n \Rightarrow p \mid (n-(n-i)) \Rightarrow p \mid i \Rightarrow p \mid i$ E

$p \mid n \Rightarrow$ ASSURDO. QUINDI $(n-i, n) = 1$.

VICEVERSA. SIA $(n-i, n)=1$. PER ASSURDO, SIA $(i, n) \geq 2 \Rightarrow \exists\, p \in \mathbb{P}$, p PRIMO, TALE CHE $p \mid i$ E $p \mid n \Rightarrow p \mid (n-i) \Rightarrow$ ASSURDO.

QUESTO DIMOSTRA (*).

PERTANTO

$$\Phi(n) = \left| \left\{ 1 \leq i \leq \left\lfloor \frac{n}{2} \right\rfloor : (i, n) = 1 \right\} \right| +$$

$$+ \left| \left\{ \lceil \tfrac{n}{2} \rceil \le i \le n-1 : (i,n) = 1 \right\} \right|$$

DOVE

$$\lfloor x \rfloor \stackrel{def}{=} \max \{ i \in \mathbb{P} : i \le x \}$$

E

$$\lceil x \rceil \stackrel{def}{=} \min \{ j \in \mathbb{P} : j \ge x \}.$$

$\left(\text{PER ES.}, \lfloor \tfrac{5}{2} \rfloor = 2, \lceil \tfrac{5}{2} \rceil = 3 \right)$. MA

$$\left| \left\{ 1 \le i \le \left\lfloor \frac{m}{2} \right\rfloor : (i, m) = 1 \right\} \right| =$$

$$\left| \left\{ \left\lceil \frac{m}{2} \right\rceil \le j \le m-1 : (m, j) = 1 \right\} \right|$$

PER $(*)$ $\Rightarrow$ $\varphi(m)$ È PARI.