

$$a^p \equiv a \pmod{p} \quad \forall a \in \mathbb{Z}, \quad p \text{ primo}$$

Dim.

Se $a \geq 0$, usiamo il p. di induzione:

$$0^p = 0 \quad 0 \equiv 0 \quad \boxed{\text{ok}}$$

Supp. che $a^p \equiv a \pmod{p}$ e dimostriamo per $a+1$

$$(a+1)^p \equiv a^p + 1^p \equiv a+1 \quad \boxed{\text{ok}}$$

ip. $\nearrow$ induttiva

$$\forall a < 0, \quad 0^p \equiv (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p - a \Rightarrow$$

$$a^p \equiv a \pmod{p}$$

$$p = 31 \quad 2^{31} \equiv 2 \pmod{31}$$

$$8^{31} \equiv 8 \pmod{31}$$

$$\text{Se } (a, p) = 1 \Rightarrow a^p \equiv a \pmod{p} \Rightarrow \boxed{a^{p-1} \equiv 1 \pmod{p}}$$

$$a = 8, p = 7 \quad 8^6 \equiv 1 \pmod{7}$$

PROBLEMA Dimostrare che $\forall n \in \mathbb{N}$

$$K_n = 2n^{17} + 2n^{15} + 3n^3 + 3n$$

è divisibile per 5.

$$n \equiv 0 \quad K_n \equiv 0 \pmod{5}$$

$$n \equiv 1, 2, 3, 4 \Rightarrow (n, 5) = 1 \quad n^4 \equiv 1 \pmod{5}$$

$$2n^{17} + 2n^{15} + 3n^3 + 3n \equiv 2n + 2n^3 + 3n^3 + 3n = 5n + 5n^3 \equiv 0 \pmod{5}$$

$$n^{17} = n^{16} \cdot n = \underbrace{(n^4)^4}_2 \cdot n \equiv n \quad n^{15} = n^{12} \cdot n^3 = \underbrace{(n^4)^3}_2 \cdot n^3 \equiv n^3$$

FUNZIONE DI EULERO

$n > 0$ intero; si chiama f. di Eulero di n la funzione che ad n associa il numero di interi $1 \leq x < n$ coprimi con n e si indica con il simbolo $\boxed{\varphi(n)}$

$$n = 20 \quad \varphi(20) = 8 \quad \underline{1, 3, 7, 9, 11, 13, 17, 19}$$

φ è una funzione moltiplicativa.

$$\varphi(rs) = \varphi(r) \cdot \varphi(s) \quad (\varphi, 1) = 1$$

$$n = p_1^{h_1} \cdot p_2^{h_2} \cdot \dots \cdot p_e^{h_e} \quad (p_i, p_j) = 1$$

$$\varphi(n) = \varphi(p_1^{h_1}) \cdot \varphi(p_2^{h_2}) \cdot \dots \cdot \varphi(p_e^{h_e})$$

Calcoliamo φ su potenze di primi:

$$\varphi(p^h) = p^h - (\dots)$$

gli interi $\leq p^h$ che non sono primi con p^h : $\underline{k \cdot p}$

$k=1$ p ; $k=2$ $2p$...

$$1 \leq k \leq p^{h-1}$$

$$\varphi(p^h) = p^h - p^{h-1} = p^h \cdot \left(1 - \frac{1}{p}\right)$$

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{h_1}) \cdots \varphi(p_t^{h_t}) = p_1^{h_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdot p_2^{h_2} \cdot \left(1 - \frac{1}{p_2}\right) \cdots p_t^{h_t} \cdot \left(1 - \frac{1}{p_t}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_t}\right) \end{aligned}$$

$$n = 72 = 2^3 \cdot 3^2$$

$$\varphi(72) = 72 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{2}{3} = 24$$

TEOREMA DI EULERO Se n è intero positivo, $a \in \mathbb{Z}$, $(a, n) = 1$

allora

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$$n = p \quad \varphi(p) = p - 1$$

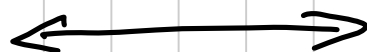
Calcolare le ultime due cifre di 3^{950} .

$$3^{950} \equiv ? \pmod{100}$$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$$

$$3^{40} \equiv 1 \pmod{100}$$

$$3^{950} = 3^{40 \cdot 23} \cdot 3^{30} \equiv 3^{30} = (3^5)^6 \equiv 43^6 = (43^3)^2 \equiv 49$$



EQUAZIONE DI FANTIA

$$\underline{x^2 + y^2 = 4m + 3} \quad (*)$$

Se (x_0, y_0, m_0) è una soluzione intera di $(*)$, allora

$$x_0^2 + y_0^2 = 4m_0 + 3$$

e quindi $x_0^2 + y_0^2 \equiv 4m_0 + 3 \pmod{m}$

$$\underline{x^2 + y^2 = 4m + 3}$$

RESIDUI QUADRATICI modulo m

$m = 3$	RESTI	0	1	2
x^2	x^2	0	1	1

I. risolvere quadratiche modulo 3 sono 0, 1

$$m \in \mathbb{Z}$$

	0	1	2	3
x^2	0	1	0	1

$$x^2 + y^2 = 4m + 3 \pmod{4}$$

$$x^2 + y^2 \equiv 3 \pmod{4} \quad \text{FALSA}$$

$\underbrace{}_{0, 1, 2}$

$\Rightarrow x^2 + y^2 = 4m + 3$ è impossibile in $\mathbb{Z}$.