

$\varphi(n)$ = quanti valori ci sono in \mathbb{Z}_n^*

$$\mathbb{Z}_n^* = \left\{ x \leq n ; \text{MCD}(x, n) = 1 \right\}$$

definizione:

QUANTI SONO
I VALORI PRIMI
CON N
(senza divisore comune)

$(\varphi = F_n)$

TEOREMA:

$$\varphi(n) = n^k - n^{k-1} \quad \text{se } \begin{cases} n = p_1^{e_1} \cdots p_m^{e_m} \\ k \geq 1 \end{cases}$$

$$\text{es} \quad \varphi(12) = \varphi(3 \cdot 4) \quad \text{① fattorizzazione: term. n. primi}$$

$$\begin{aligned} &= \varphi(3) \cdot \varphi(4) \quad \text{② SPLIT} \\ &= (3^1 - 3^0)(4^2 - 4^1) \quad \text{③ TEOREMA} \\ &= (3-1)(4-2) \quad \text{④ RISULTATO} \\ &= 2 \cdot 2 = 4 \end{aligned}$$

D.M.	$\varphi(12) = \left\{ x \leq 12 ; \text{MCD}(x, 12) = 1 \right\}$
	$= \{1, 5, 7, 11\} = 4 \text{ valori} \therefore \varphi(12) = 4$

es.

$$\begin{aligned} \varphi(300000000000) &= \varphi(3) \cdot \varphi(10^{10}) = \varphi(3) \cdot \varphi(2^{10}) \cdot \varphi(5^{10}) = (3-1) \cdot (2^{10}-2^0) \cdot (5^{10}-5^0) = \\ &= 2 \cdot 2^9 (2-1) \cdot 5^9 (5-1) = 2 \cdot 2^9 \cdot 5^9 \cdot 4 = 8 \cdot (2 \cdot 5)^9 = 8 \cdot 10^9 \end{aligned}$$

TEOREMA EULERO:

$$\forall A \in \mathbb{Z}_n^* \quad [A]_n^{\varphi(n)} = [1]_n$$

$$\varphi(10) = 4$$

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

$$[1]_{10}^4 = [1]_{10}$$

$$[3]_{10}^4 = [1]_{10}$$

$$[7]_{10}^4 = [1]_{10}$$

$$[9]_{10}^4 = [1]_{10}$$

INVERSA CON EULERO:

$$[A]_n^{-1} = [A]_n^{\varphi(n)-1}$$

$$\text{dim. } A^1 \cdot A^{\varphi(n)-1} = A^{\varphi(n)} = 1$$

es
inversa di $[3]_{19}$: $\varphi(19) = 18$: $[3]^{18-1}_{19} = [3]^{17}_{19} = [13]_{19}$

SEMPLIFICAZIONE ESPOENTE:

se l'esponente è maggiore di $\varphi(n)$ è riducibile

$$\begin{cases} A^x & x = \varphi(n) \quad A_n^x = 1_n \\ A^x & x > \varphi(n) \quad A_n^x = A_n^r \end{cases}$$

$$[A]_n^x = [A]_n^r \quad \left(r \text{ il resto di } \frac{x}{\varphi(n)} \right)$$

dim

$$A^{1000} : 1000 = q\varphi(n) + r \rightarrow A^{q\varphi(n)+r} = (A^{\varphi(n)})^q \cdot A^r = (1)^q \cdot A^r = A^r$$

es

$[7]_{100}$	$m = 100$
• $\varphi(100) = 40$	
• $r = \frac{100}{40} = 2$	
• $[7]^r_{100} = [7]^{10}_{100} = [49]_{100}$	

- ORDINE DI a : $\min(t)$ tc $a^t = [1]_n$ per $t \geq 1$

COROLLARIO: $\forall a \in \mathbb{Z}_n^*$ l'ordine di a è un divisore di $\varphi(n)$

$$t = \text{ordine di } a \quad A^{\varphi(n)} = [1]_n \quad \text{allora} \quad t \leq \varphi(n) \quad (\text{e } n \text{ è un numero da } 1 \text{ a } \varphi(n))$$

es.

$$\mathbb{Z}_{15}^* = \left\{ [1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15} \right\}$$

$$\varphi(15) = \dots = 8$$

DIVISORI DI 8: 1, 2, 4, 8 - esponenti per le quattro ordini

$$\begin{aligned} & [1]_{15}^1 \\ & [2]_{15}^4 \\ & [4]_{15}^2 \\ & [7]_{15}^2 \\ & [8]_{15}^4 \\ & [11]_{15}^2 \\ & [13]_{15}^4 \\ & [14]_{15}^2 \end{aligned}$$

esponenti necessari a dare resto 1 ($[1]_{15}$)

$$\begin{aligned} & [\dots]^2 = [n] \\ & [\dots]^4 = [n]^2 = \dots \end{aligned}$$

o via a tentativi così oppure

$$[A]_n^x : \text{ se } A^x - 1 \text{ è divisibile per } n \text{ ho trovato } x$$

(perché x tra i divisori di $\varphi(n)$)

$$[\dots]_{13} \quad 13 \text{ è primo} \quad \varphi(13) = 12$$

$$\mathbb{Z}_n^* = \left\{ \text{tutti i numeri da } 1 \text{ a } \varphi(n) \right\}$$

LOGARITMO DISCRETO

il logaritmo discreto di B in base A
 è l'insieme degli interi k t.c. $A^k = B$ $(A, B \in \text{ORDINE})$

$$a^{-t} = (a^{-1})^t$$

$$\begin{array}{l} a^n \cdot a^m = a^{n+m} \\ (a^n)^m = a^{n \cdot m} \end{array}$$

$$\text{es } [3]_7^4 = \left([3]_7^{-1} \right)^4 = \left([5]_7^{-1} \right)^4 = [2]_7$$

$$\log_A([x]_n) : \text{s.t. } a^k = [x]_n$$

$$\text{es } [3]_{100}^k = [7]_{100} \quad k = 20$$

log discreto = $K \in \emptyset$ tutti i suoi risultati
 REGOLE: k è ordine concordanza

$$\text{es } [3]_{11}^k = [4]_{11}$$

1) Il suo ordine è k

$$[3]_{11}^1 = \dots$$

$$[3]_{11}^2 = \dots$$

$$[3]_{11}^3 = \dots$$

$$[3]_{11}^4 = [4]_{11}$$

$$[3]_{11}^5 = [1]_{11}$$

trovato lo stesso risultato dell'equazione iniziale ha trovato k

$$\text{ordine} = 5$$

$$K = 4$$

$$K = 4 + 5\lambda$$

$$\begin{array}{c} \text{ex:} \\ (K = 5 | 4) \\ \text{ordine} \end{array}$$

arrivato a 1
 ha trovato l'ordine

$$\bullet A \stackrel{x}{=} B$$

$$\bullet \varphi(n) = \text{ORDINE MASSIMO} : \text{prova ogni } x \text{ fino a } \varphi(n)$$

$$\textcircled{1} \quad [A]_n^x = [B]_n$$

$$\textcircled{2} \quad \text{PROVA TUTTE LE } x \text{ FINCHE' non trova } [A]_n^x = [1]_n$$

$$\textcircled{3} \quad X = \dots + \dots K$$

$$x: [A]_n^x = [B]_n \quad x: [A]_n^x = [1]$$

es logaritmo discreto

$$\begin{aligned}
 [10]_{13}^k &= [9]_{13} \cdot [5]_{13}^k \\
 [10]_{13}^k \cdot [5]_{13}^{-k} &= [9]_{13} \\
 ([5]_{13}^{-1})^k &= ([8]_{13})^k \\
 [10]_{13}^k \cdot [8]_{13}^k &= [9]_{13} \\
 [2]_{13}^k &= [9]_{13} \quad \xrightarrow[\text{ordine } 92]{\text{L'ordine } 92} k \equiv_{92} 8 \\
 (\text{ordine divisorio del } 9_{13} \text{ che dà } [7]_n) \\
 (K = \dots)
 \end{aligned}$$

Esercizi

Esercizio 29

$$7 \cdot 10^k \equiv_{11} 8 \cdot 9^k.$$

$$[7]_{11} \cdot [-1]_{11}^k = [8]_{11} \cdot [9]_{11}^k$$

Moltiplicando entrambi i membri per $[8]_{11}^{-1} = [7]_{11}$ otteniamo

$$[7]_{11} \cdot [7]_{11} \cdot [-1]_{11}^k = [9]_{11}^k,$$

da cui

$$[5]_{11} \cdot [-1]_{11}^k = [9]_{11}^k.$$

Moltiplicando entrambi i membri per $[-1]_{11}^{-k}$ otteniamo

$$[5]_{11} = [9]_{11}^k \cdot [-1]_{11}^{-k} = [9]_{11}^k \cdot (-1)_{11}^{-1} = [9]_{11}^k \cdot [1]_{11} = ([9]_{11} \cdot [-1]_{11})^k = [-9]_{11}^k = [2]_{11}^k.$$

Dobbiamo quindi risolvere il problema

$$[2]_{11}^k = [5]_{11}.$$

Abbiamo:

$$[2]_{11}^2 = [4]_{11}, \quad [2]_{11}^3 = [8]_{11}, \quad [2]_{11}^4 = [5]_{11}, \quad [2]_{11}^5 = [10]_{11}.$$

Abbiamo allora che $[2]_{11}^4 = [5]_{11}$ e che l'ordine di $[2]_{11}$ è 10 (deve essere un divisore di $\varphi(11) = 10$ e abbiamo appena visto che non è ne 2 ne 5). La soluzione del problema (27) è quindi $k \equiv_{10} 4$.

Esercizio 30

$$\begin{cases} 6^{2n} \equiv_{13} 3 \\ 5n + 3 \equiv_{16} 0. \end{cases}$$

Soluzione. Per risolvere il sistema dobbiamo portare ognuna delle due equazioni nella forma $n \equiv_a x$ per poi applicare il teorema cinese del resto. Dato che $[6^{2n}]_{13} = [6^2]^n_{13} = [10]^n_{13}$, la prima equazione diventa

$$[10]^n_{13} = [3]_{13}.$$

Abbiamo:

$$[10]^2_{13} = [9]_{13}, \quad [10]^3_{13} = [12]_{13}, \quad [10]^4_{13} = [3]_{13}, \quad [10]^5_{13} = [4]_{13}, \quad [10]^6_{13} = [1]_{13}.$$

La soluzione è quindi $n \equiv_6 4$.

La seconda equazione del sistema si può riscrivere come

$$[5]_{16} \cdot [n]_{16} = [-3]_{16}.$$

Dato che $[5]_{16}^{-1} = [13]_{16}$, moltiplicando entrambi i termini per $[13]_{16}$ otteniamo

$$[n]_{16} = [13]_{16} \cdot [-3]_{16} = [-39]_{16} = [9]_{16}.$$

La seconda equazione

ha quindi come soluzione $n \equiv_{16} 9$

$$\begin{cases} n \equiv_6 4 \\ n \equiv_{16} 9. \end{cases}$$

Questo sistema però non è risolubile in quanto $\text{MCD}(6, 16) = 2$ non divide $4 - 9 = -5$. Possiamo concludere allora che il sistema iniziale non ammette nessuna soluzione intera. \square

es

$$\begin{cases} 2^{103n} \equiv_{11} 4 \\ 2^n \equiv_{17} 3^n \end{cases}$$

$$\textcircled{1} \left([2]_{11}^{103} \right)^n = [4]_{11}$$

$$\downarrow \text{ semplificazione: } 9(11) = 10 \quad 103 \bmod 10 = 3 \\ [2]_{11}^{3n} = [4]_{11}$$

$$[8]_{11}^n = [4]_{11} \quad \begin{matrix} k \equiv 4 \\ \text{d.o. } 10 \end{matrix}$$

$$\begin{cases} \text{mcd}(10, 16) = 2 \\ \text{lcm}(10, 16) = 80 \end{cases} \quad n \equiv_{80} 64 \\ 10^{k+4} = 10^k$$

$$K \equiv_{40} 0$$

$$\begin{cases} n \equiv_{10} 4 \\ n \equiv_{16} 0 \end{cases}$$

AUTO PREPARAZIONE:

• TROVARE \mathbb{Z}_n^* : $\varphi(16) = 8$

④ $d : \{\text{divisori di } n\}$

② $\forall x \in (0 < x < n) \neq d$

$$\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

conviene che $\frac{x}{d} \neq 1$ $\forall d$

• RESTO CON
CALCOLATRICE :

$$\frac{A}{B} : \quad ① A : B = \underline{\underline{x}}, \underline{\underline{y}}$$

$$② x \cdot B = n$$

$$③ A - n = \text{resto}$$