ARITMETICA MODULARE (V PARTE)

<u>Teorema di Eulero</u>: $a \in \mathbb{Z}$, $N \in \mathbb{N}$, $N \geq 2$ e $MCD(a,N) = 1$.

Allora $\quad a^{\varphi(N)} \equiv 1 \mod N$

<u>Dim</u>: $\varphi(N) = |\mathbb{Z}_N^\times|$. Inoltre, poiché $MCD(a,N)=1 \Rightarrow \bar{a} \in \mathbb{Z}_N^\times$

Quindi abbiamo una funzione
$$f: \mathbb{Z}_N^\times \longrightarrow \mathbb{Z}_N^\times$$
$$\bar{x} \longmapsto \bar{a} \cdot \bar{x}$$

Tale funzione è <u>iniettiva</u>, infatti

se $f(\bar{x}) = f(\bar{y})$, cioè $\bar{a} \cdot \bar{x} = \bar{a} \cdot \bar{y}$, allora moltiplicando per $\bar{a}^{-1}$, si ottiene:

$$\underbrace{\bar{a}^{-1} \bar{a}}_{\bar{1} =} \cdot \bar{x} = \bar{a}^{-1} \bar{a} \cdot \bar{y} \implies \bar{x} = \bar{y}.$$

Ma essendo f funzione iniettiva tra insiemi <u>finiti</u> di uguale cardinalità $\Rightarrow f$ <u>biettiva</u>.

In altre parole $f(\mathbb{Z}_N^\times) = \mathbb{Z}_N^\times$ o ancora $\mathbb{Z}_N^\times = \{\bar{x}_1, \bar{x}_2, \dots, \bar{x}_{\varphi(N)}\} = \{\bar{a}\bar{x}_1, \bar{a}\bar{x}_2, \dots, \bar{a}\bar{x}_{\varphi(N)}\}$

Quindi $\quad \bar{x}_1 \cdot \bar{x}_2 \cdot \dots \cdot \bar{x}_{\varphi(N)} = \bar{a}\bar{x}_1 \cdot \bar{a}\bar{x}_2 \cdot \dots \cdot \bar{a}\bar{x}_{\varphi(N)} = \bar{a}^{\varphi(N)} \cdot \bar{x}_1 \cdot \bar{x}_2 \cdot \dots \bar{x}_{\varphi(N)}$

Moltiplicando per $\bar{x}_{\varphi(N)}^{-1} \dots \bar{x}_2^{-1} \bar{x}_1^{-1}$ otteniamo $\quad \bar{1} = \bar{a}^{\varphi(N)}$ cioè $a^{\varphi(N)} \equiv 1 \mod N$.

$\boxtimes$

Esempi di applicazione.

1) Calcolare il resto della divisione di 5^{864735} per 42.

$MCD(5,42)=1 \Rightarrow 5^{\varphi(42)} \equiv 1 \mod 42$ (Teorema di Eulero)

$\varphi(42)=\varphi(2\cdot 3\cdot 7)=\varphi(2)\cdot\varphi(3)\cdot\varphi(7)=1\cdot 2\cdot 6=12 \Rightarrow \underline{5^{12}\equiv 1 \mod 42}$

Svolgiamo la divisione con resto di 864735 per 12:

regole delle potenze

$$864735 = 12\cdot\underbrace{72061}_{q}+\underbrace{3}_{r} \quad \text{ma allora} \quad 5^{864735}=5^{12\cdot 72061+3}=\left(5^{12}\right)^{72061}\cdot 5^{3}$$

$$\left[\left(5^{12}\right)^{72061}\cdot 5^{3}\right]_{42}=\left[\left(5^{12}\right)^{72061}\right]_{42}\cdot\left[5^{3}\right]_{42}=\left[5^{12}\right]_{42}^{72061}\cdot\left[5^{3}\right]_{42}=\left[1\right]_{42}^{72061}\cdot\left[5^{3}\right]_{42}=\left[1\right]_{42}\cdot\left[-1\right]_{42}$$

$$=[-1]_{42}$$

$$=[41]_{42}$$

$5^{3}=125 \qquad 125=126-1=42\cdot 3-1\equiv \underline{-1} \mod 42$

Risposta: 5^{864735} diviso per 42 dà resto 41.

2) Calcolare il resto della divisione per 30 di $7^{4106}+11^{2171}$.

$MCD(7,30) = MCD(11,30) = 1$ $\qquad \varphi(30) = \varphi(2\cdot 3\cdot 5) = 1\cdot 2\cdot 4 = 8$

Per il Teorema di Eulero: $7^8 \equiv 1 \mod 30 \qquad 11^8 \equiv 1 \mod 30$

Svolgiamo la divisione con resto degli esponenti per 8.

$4106 = 8\cdot 513 + 2 \qquad 2171 = 8\cdot 271 + 3$

$[7^{4106}]_{30} = [7^8]_{30}^{513}\cdot[7^2]_{30} = [1]_{30}^{513}\cdot[49]_{30} = [19]_{30}$ $\qquad [19]_{30} + [11]_{30} = [0]_{30}$

$[11^{2171}]_{30} = [11^8]_{30}^{271}\cdot[11^3]_{30} = [1]_{30}^{271}\cdot[1331]_{30} = [11]_{30}$

$$7^{4106}+11^{2171} \equiv 19+11 \equiv 30 \equiv 0 \mod 30$$

Risposta $7^{4106}+11^{2171}$ è divisibile per 30.

3) Calcolare il resto della divisione di 6^{755} per 62.

Problema: $MCD(6,62)=2\neq 1$ Però: $6=2\cdot 3$ $6^{755}=2^{755}\cdot 3^{755}$

Intanto posso valutare $[3^{755}]_{62}$ $\varphi(62)=\varphi(2\cdot 31)=30 \Rightarrow 3^{30}\equiv 1 \mod 62$

$755 = 30\cdot 25+5$ $[3^{755}]_{62}=[3^{30}]_{62}^{25}\cdot[3^5]_{62}=[1]_{62}^{25}\cdot[243]_{62}=[-5]_{62}=[57]_{62}$

$$243 = 248-5 = 62\cdot 4 - 5 \equiv -5 \mod 62$$

Col primo fattore devo lavorare diversamente, perché $MCD(2,62)=2\neq 1 \Rightarrow$ non posso applicare il Teorema

$2^2=4$ $2^3=8$ $2^4=16$ $2^5=32$ $2^6=64=2+62\equiv 2 \mod 62$ cioè $[2^6]_{62}=[2]_{62}$

$755 = 6\cdot 125+5$ $[2^{755}]_{62}=[2^6]_{62}^{125}\cdot[2^5]_{62}=[2^{125}]_{62}\cdot[2^5]_{62}$

$125=6\cdot 20+5$ $[2^{125}]_{62}\cdot[2^5]_{62}=[2^6]_{62}^{20}\cdot[2^5]_{62}\cdot[2^5]_{62}=[2^{20}]_{62}\cdot[2^5]_{62}\cdot[2^5]_{62}=[2^{30}]_{62}$

$=[2^6]_{62}^5=[2^5]_{62}=[32]_{62}$

Ora moltiplichiamo: $[6^{755}]_{62}=[2^{755}]_{62}\cdot[3^{755}]_{62}=[32]_{62}\cdot[57]_{62}=[26]_{62}$

Risposta: il resto è 26.

Criteri di divisibilità

Sia $n \in \mathbb{N}$ la cui notazione in base 10 è $n = c_r c_{r-1} \dots c_2 c_1 c_0$

cioè $n = c_0 + c_1 \cdot 10 + c_2 \cdot 10^2 + \dots + c_r \cdot 10^r$.

Sulla base di questo, ricaviamo i criteri seguenti:

1) $2 \mid n$ se e solo se $2 \mid c_0$. Infatti $2 \mid 10^k$ per ogni $k \geq 1$ $\Rightarrow [10^k]_2 = [0]_2$ per $k \geq 1$

$$\Rightarrow [n]_2 = [c_0]_2 + [c_1]_2 \cdot \underbrace{[10]_2}_{=[0]_2} + \dots + [c_r]_2 \cdot \underbrace{[10^r]_2}_{=[0]_2} = [c_0]_2$$

2) $5 \mid n$ se e solo se $5 \mid c_0$. Infatti $5 \mid 10^k$ per ogni $k \geq 1$ ... come sopra.

3) $3 \mid n$ se e solo se $3 \mid (c_0 + c_1 + \dots + c_r)$. Infatti $[10]_3 = [1]_3 \Rightarrow [10]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$

quindi $[10^k]_3 = [1]_3 \Rightarrow [n]_3 = [c_0]_3 + [c_1]_3 \cdot \underbrace{[10]_3}_{=[1]_3} + \dots + [c_r]_3 \cdot \underbrace{[10^r]_3}_{=[1]_3} = [c_0]_3 + [c_1]_3 + \dots + [c_r]_3$

$$= [c_0 + c_1 + \dots + c_r]_3 .$$

4) $9 \mid n$ se e solo se $9 \mid (c_0 + c_1 + \dots + c_r)$. Infatti $[10]_9 = [1] \Rightarrow [10^k]_9 = [10]_9^k = [1]_9^k$

.... come sopra.

5) $11 \mid n$ se e solo se $11 \mid (c_0 - c_1 + \ldots + (-1)^r c_r)$

Infatti $[10]_{11} = [-1]_{11}$ $\quad [10^2]_{11} = [-1]^2_{11} = [1]_{11} \Rightarrow [10^k]_{11} = \begin{cases} [-1]_{11} & \text{se } k \text{ dispari} \\ [1]_{11} & \text{se } k \text{ pari} \end{cases}$

$$[n]_{11} = [c_0 + c_1 \cdot 10 + \ldots + c_r \cdot 10^r]_{11} = [c_0]_{11} + [c_1]_{11} \cdot \underbrace{[10]_{11}}_{= [-1]_{11}} + \ldots + [c_r]_{11} \cdot \underbrace{[10^r]_{11}}_{= [(-1)^r]_{11}} = [c_0] - [c_1] + \ldots + (-1)^r [c_r]$$

$$= [c_0 - c_1 + c_2 + \ldots + (-1)^r c_r]_{11}$$