Aritmetica Modulare (IV Parte)

Osservazione: se $\bar{a}, \bar{b}$ sono invertibili in $\mathbb{Z}_N$, allora $\bar{a} \cdot \bar{b}$ è invertibile in $\mathbb{Z}_N$.

Infatti $(\bar{b}^{-1} \cdot \bar{a}^{-1}) \cdot (\bar{a} \cdot \bar{b}) = \bar{b}^{-1} \cdot \underbrace{(\bar{a}^{-1} \cdot \bar{a})}_{\bar{1}=} \cdot \bar{b} = \bar{b}^{-1} \cdot \bar{b} = \bar{1}$

Denotiamo $\mathbb{Z}_N^\times$ il sottoinsieme di $\mathbb{Z}_N$ dato dagli elementi invertibili.

Notare che $\mathbb{Z}_N^\times$ è un sottoinsieme proprio e non vuoto di $\mathbb{Z}_N$ $\left(\bar{0} \notin \mathbb{Z}_N^\times, \bar{1} \in \mathbb{Z}_N^\times \quad \forall N \geq 2\right)$

$$\emptyset \subsetneq \mathbb{Z}_N^\times \subsetneq \mathbb{Z}_N .$$

L'osservazione sopra ci dice che $\mathbb{Z}_N^\times$ è chiuso rispetto alla moltiplicazione.

<u>Def</u>: Si dice <u>funzione φ di Eulero</u> la funzione $\varphi : \mathbb{N} \setminus \{0\} \longrightarrow \mathbb{N}$ tale che:

$$\varphi(n) = \left| \{ r \in \mathbb{N} \mid 1 \leq r \leq n \wedge MCD(r,n) = 1 \} \right| .$$

In sostanza, se $n \geq 2$, $\varphi(n) = |\mathbb{Z}_n^\times|$.

<u>Es.</u>

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	....	30
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8		8

<u>oss</u>: Se n è primo, $\varphi(n) = n-1$

Quanto vale $\varphi(n)$ se $n = p^k$, con p primo?

<u>Prop</u>: Se $p \in \mathbb{N}$ è primo, $k \in \mathbb{N} - \{0\} \Rightarrow \varphi(p^k) = p^{k-1}(p-1)$

<u>dim</u>: Sia $1 \leq r \leq p^k$ e $MCD(r, p^k) \neq 1$, allora $\exists j$ $1 \leq j \leq k$ t.c. $MCD(r, p^k) = p^j$

Allora r può essere soltanto uno di questi valori:

$$\underbrace{\underbrace{1 \cdot p, 2p, 3p \ldots, p \cdot p = p^2}_{p \text{ valori}}, (p+1) \cdot p, \ldots\ldots\ldots, (p^{k-1}-1) \cdot p, p^k = p^{k-1} \cdot p}_{p^{k-1} \text{ valori}}$$ Sono tutti i multipli di p fino a p^k.

Allora gli elementi di $\{r \in \mathbb{N} \mid 1 \leq r \leq p^k, MCD(r, p^k) = 1\}$ sono $p^k - p^{k-1} = p^{k-1}(p-1)$. $\boxtimes$

Come calcolare φ in generale?

<u>Lemma</u>: Siano $m, n \in \mathbb{N} - \{0\}$ t.c. $MCD(m, n) = 1$. Allora

$$f : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \qquad [a]_{mn} \longmapsto ([a]_m, [a]_n)$$

è una biezione che preserva i prodotti {cioè $f([a] \cdot [b]) = f([a]) \cdot f([b])$}

Es. $m = 4$ $n = 3$

$[7]_{12} \mapsto ([7]_4, [7]_3) = ([3]_4, [1]_3)$

<u>dim</u>: 1) È ben definita e preserva i prodotti. (esercizio)

2) È <u>iniettiva</u>: Siano $[a]_{mn}$ e $[b]_{mn}$ tali che $f([a]) = f([b])$ ovvero $([a]_m, [a]_n) = ([b]_m, [b]_n)$

allora $\begin{cases} \exists h \in \mathbb{Z} \text{ t.c. } a - b = hm \\ \exists h' \in \mathbb{Z} \text{ t.c. } a - b = h' n \end{cases}$ quindi $hm = h'n$, ma $MCD(m, n) = 1 \Rightarrow m \mid h'$, cioè $\exists k \in \mathbb{Z}$ t.c. $h' = km$

allora $a - b = h'n = kmn \Rightarrow a \equiv b \mod mn \Rightarrow [a]_{mn} = [b]_{mn}$.

3) f è suriettiva: osserviamo che $|\mathbb{Z}_{mn}| = mn = |\mathbb{Z}_m| \cdot |\mathbb{Z}_n| = |\mathbb{Z}_m \times \mathbb{Z}_n|$
quindi f è una funzione iniettiva tra insiemi finiti di uguale cardinalità $\Rightarrow$ f è suriettiva. $\boxtimes$

Lemma: f (come sopra) si restringe a una biezione $\overline{f}: \mathbb{Z}_{mn}^\times \longrightarrow \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

dim: 1) gli invertibili in $\mathbb{Z}_m \times \mathbb{Z}_n$ sono del tipo $(\bar{a}, \bar{a}')$ dove $\bar{a} \in \mathbb{Z}_m^\times$, $\bar{a}' \in \mathbb{Z}_n^\times$ infatti
se $(\bar{a}, \bar{a}')$ è invertibile $\exists (\bar{b}, \bar{b}') \in \mathbb{Z}_m \times \mathbb{Z}_n$ t.c. $(\bar{a}, \bar{a}') \cdot (\bar{b}, \bar{b}') = (\bar{1}, \bar{1})$ cioè $\begin{cases} \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_m \\ \bar{a}' \cdot \bar{b}' = \bar{1} \text{ in } \mathbb{Z}_n \end{cases}$
Perciò $(\mathbb{Z}_m \times \mathbb{Z}_n)^\times = \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$.

2) Se $\bar{a} \in \mathbb{Z}_{mn}^\times$ allora $\exists \bar{b} \in \mathbb{Z}_{mn}^\times$ t.c. $\bar{a} \cdot \bar{b} = \bar{1}$ in $\mathbb{Z}_{mn}$, ma allora $f(\bar{a} \cdot \bar{b}) = f(\bar{1}) = (\bar{1}, \bar{1})$
Poiché f preserva i prodotti $f(\bar{a} \cdot \bar{b}) = f(\bar{a}) \cdot f(\bar{b}) = (\underset{\text{in } \mathbb{Z}_m}{\bar{a}}, \underset{\text{in } \mathbb{Z}_n}{\bar{a}}) \cdot (\bar{b}, \bar{b}) = (\bar{1}, \bar{1})$
ma allora $\begin{cases} \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_m \\ \bar{a} \cdot \bar{b} = \bar{1} \text{ in } \mathbb{Z}_n \end{cases} \Rightarrow \bar{a} \in \mathbb{Z}_m^\times$ e $\bar{a} \in \mathbb{Z}_n^\times$. (Invertibili vanno in invertibili)

Viceversa, sia $(\bar{a}, \bar{a}') \in \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, vogliamo mostrare che $f^{-1}(\bar{a}, \bar{a}')$ è invertibile
Sia $(\bar{b}, \bar{b}')$ l'inverso di $(\bar{a}, \bar{a}')$, cioè $(\bar{a}, \bar{a}')(\bar{b}, \bar{b}') = (\bar{1}, \bar{1})$.

Ora $f^{-1}(\bar{a}, \bar{a}') \cdot f^{-1}(\bar{b}, \bar{b}') = f^{-1} f\left(f^{-1}(\bar{a}, \bar{a}') \cdot f^{-1}(\bar{b}, \bar{b}')\right) = f^{-1}\left(f f^{-1}(\bar{a}, \bar{a}') \cdot f f^{-1}(\bar{b}, \bar{b}')\right) =$
$= f^{-1}\left((\bar{a}, \bar{a}') \cdot (\bar{b}, \bar{b}')\right) = f^{-1}\left((\bar{1}, \bar{1})\right) = \bar{1}$. Quindi $f^{-1}(\bar{a}, \bar{a}')$ è invertibile $\boxtimes$

Conseguenza: $\quad |\mathbb{Z}_{mn}^\times| = |\mathbb{Z}_m^\times \times \mathbb{Z}_n^\times| = |\mathbb{Z}_m^\times|\cdot|\mathbb{Z}_n^\times|$, quindi abbiamo dimostrato:

Prop: Siano $m,n \in \mathbb{N}\setminus\{0\}$ con $MCD(m,n)=1$. Allora $\varphi(mn)=\varphi(m)\cdot\varphi(n)$.

(Basta ricordare che $\varphi(n)=|\mathbb{Z}_n^\times| \quad \forall n\geq 2$)

Ora usando la fattorizzazione in prodotto di primi, possiamo calcolare $\varphi(n)$ per ogni $n\in\mathbb{N}\setminus\{0\}$.

Sia $n=p_1^{e_1}\cdot p_2^{e_2}\cdot \ldots \cdot p_r^{e_r}$. Allora $\boxed{\varphi(n)=\prod_{i=1}^{r} p_i^{e_i-1}\cdot(p_i-1)}$ φ di Eulero

(è conseguenza delle proposizioni precedenti)

Es. $n=31 \qquad \varphi(31)=30 \qquad$ (31 è primo!)

$n=49=7^2 \qquad \varphi(49)=7^{2-1}\cdot(7-1)=7\cdot 6=42$

$n=81=3^4 \qquad \varphi(81)=3^{4-1}\cdot(3-1)=3^3\cdot 2=54$

$n=120=2^3\cdot 3\cdot 5 \qquad \varphi(120)=2^{3-1}\cdot(2-1)\cdot 3^{1-1}\cdot(3-1)\cdot 5^{1-1}(5-1)=4\cdot 2\cdot 4=32$

$n=87120=2^4\cdot 3^2\cdot 5\cdot 11^2 \qquad \varphi(87120)=2^3\cdot 3\cdot 2\cdot 4\cdot 11\cdot 10=21120$

87120	$2\cdot 5$
8712	2
4356	2
2178	2
1089	3
363	3
121	11^2

Conoscere i valori di $\varphi(n)$ diventa importante grazie al seguente teorema:

Teorema (di Eulero): Sia $a \in \mathbb{Z}$, $N \geq 2$ t.c. $MCD(a, N) = 1$. Allora $a^{\varphi(N)} \equiv 1 \mod N$

Piccolo teorema di Fermat: Sia $a \in \mathbb{Z}$, p primo. Allora $a^{p-1} \equiv 1 \mod p$.

(è un caso particolare del precedente).