Aritmetica Modulare (III parte)

Corollario: p primo. $\forall \bar{a} \in \mathbb{Z}_p$, $\bar{a} \neq \bar{0}$ $\bar{a}$ è invertibile, cioè $\exists \bar{b} \in \mathbb{Z}_p$ t.c. $\bar{a} \cdot \bar{b} = \bar{1}$.

Es: $\mathbb{Z}_{79}$ (79 è primo) $\bar{a} = \overline{22}$ $\quad MCD(79,22)=1$ $\quad \overline{22}$ è invertibile in $\mathbb{Z}_{79}$

Chi è l'inverso di $\overline{22}$? Applico l'algoritmo euclideo:

$$79 = 22 \cdot 3 + 13$$
$$22 = 13 \cdot 1 + 9$$
$$13 = 9 \cdot 1 + 4$$
$$9 = 4 \cdot 2 + 1$$

$$1 = 9 - 2 \cdot 4$$
$$4 = 13 - 1 \cdot 9$$
$$9 = 22 - 1 \cdot 13$$
$$13 = 79 - 3 \cdot 22$$

$$1 = 9 - 2 \cdot (13 - 9) = 3 \cdot 9 - 2 \cdot 13$$
$$= 3 \cdot (22 - 13) - 2 \cdot 13 = 3 \cdot 22 - 5 \cdot 13$$
$$= 3 \cdot 22 - 5 \cdot (79 - 3 \cdot 22) = 18 \cdot 22 - 5 \cdot 79$$

$$1 = \underbrace{79}_{N} \cdot (-5) + \underbrace{22}_{a} \cdot 18$$

Cioè $\quad 22 \cdot 18 = 1 + 5 \cdot 79$

ovvero $\quad 22 \cdot 18 \equiv 1 \mod 79$

ovvero $\quad \overline{22} \cdot \overline{18} = \bar{1}$ in $\mathbb{Z}_{79}$ $\quad$ cioè $\quad \overline{18} = \overline{22}^{-1}$ in $\mathbb{Z}_{79}$

Es. $\mathbb{Z}_{27}$ $\quad \bar{a} = \overline{10}$ $\quad MCD(10,27) = 1 \Rightarrow \bar{a}$ è invertibile in $\mathbb{Z}_{27}$

$10 = 2 \cdot 5$
$27 = 3^3$ $\Rightarrow MCD = 1$

Chi è l'inverso di $\overline{10}$?

$$
\begin{aligned}
27 &= 10 \cdot 2 + 7 & \qquad 1 &= 7 - 2 \cdot 3 \\
10 &= 7 \cdot 1 + 3 & \qquad 3 &= 10 - 7 \\
7 &= 3 \cdot 2 + 1 & \qquad 7 &= 27 - 2 \cdot 10
\end{aligned}
$$

$$1 = 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10$$
$$= 3 \cdot (27 - 2 \cdot 10) - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10$$

$$1 = \underbrace{27}_{N} \cdot 3 + \underbrace{10}_{a} \cdot (-8)$$

$$10 \cdot (-8) = 1 - 3 \cdot 27$$

$$10 \cdot (-8) \equiv 1 \mod 27 \Rightarrow \overline{10} \cdot \overline{-8} = \bar{1} \text{ in } \mathbb{Z}_{27}$$

$$\overline{10}^{-1} = \overline{-8} = \overline{27-8} = \overline{19}$$

rappresentano la stessa classe

Congruenze lineari

Ricordiamo: $a \equiv b \mod N$ vuol dire che $\bar{a} = \bar{b}$ in $\mathbb{Z}_N$, cioè $\exists k \in \mathbb{Z}$ t.c. $a - b = k \cdot N$

Vogliamo capire se è possibile (e come) risolvere equazioni del tipo:

$$(*) \qquad ax \equiv b \mod N \qquad (a, b, N \in \mathbb{N}) \quad x \in \mathbb{Z} \text{ è un'incognita.}$$

Osservazione: L'equazione (*) ha soluzioni se e solo se ha soluzioni l'equazione:

$$(**) \qquad ax - k \cdot N = b$$

Una soluzione di (**) è una coppia $(x, k) \in \mathbb{Z} \times \mathbb{Z}$ che soddisfa l'equazione.

Infatti: Se $\exists (x,k) \in \mathbb{Z}\times\mathbb{Z}$ t.c. $ax - kN = b \Rightarrow ax = b + kN \Rightarrow \exists x \in \mathbb{Z}$ t.c. $ax \equiv b \mod N$.

Viceversa, se $\exists x \in \mathbb{Z}$ t.c. $ax \equiv b \mod N \Rightarrow \exists k \in \mathbb{Z}$ t.c. $ax - b = k \cdot N \Rightarrow \exists (x,k) \in \mathbb{Z}\times\mathbb{Z}$ t.c. $ax - kN = b$.

Prop: L'equazione $ax \equiv b \mod N$ ha soluzioni se e solo se $MCD(a,N) \mid b$.

Esempi

1) $\underbrace{12}_{a} x \equiv \underbrace{10}_{b} \mod \underbrace{25}_{N}$ $\quad MCD(a,N) = MCD(12,25) = 1 \Rightarrow$ esistono soluzioni

Siamo in un caso fortunato, perché $\bar{a}$ è invertibile in $\mathbb{Z}_{25}$. Troviamo l'inverso.

$25 = 12 \cdot 2 + 1 \Rightarrow 1 = 25 - 2 \cdot 12 \Rightarrow 12 \cdot (-2) = 1 - 25$ cioè $\overline{12} \cdot \overline{-2} = \bar{1}$ in $\mathbb{Z}_{25}$

$\Rightarrow \overline{12}^{-1} = \overline{-2} = \overline{23}$.

Moltiplico per 23:

$23 \cdot 12\, x \equiv 10 \cdot 23 \mod 25$ $\quad$ ma $23 \cdot 12 \equiv 1 \mod 25 \Rightarrow (23 \cdot 12) \cdot x \equiv x \mod 25$

allora $x \equiv 10 \cdot 23 \mod 25$ $\quad$ ma $10 \cdot 23 = 230 = 25 \cdot 9 + 5$ $\quad 230 \equiv 5 \mod 25$

$x \equiv 5 \mod 25$

Cioè l'insieme delle soluzioni della congruenza lineare è $S = \{\ldots, -20, 5, 30, 55, \ldots\} = [5]_{25}$

Prova: $12 \cdot 5 = 60 = 25 \cdot 2 + 10 \equiv 10 \mod 25$

$12 \cdot (-20) = -240 = 25 \cdot (-10) + 10 \equiv 10 \mod 25$

2) $9x \equiv 14 \mod 24$ $\quad MCD(9,24) = 3$, ma $3 \nmid 14 \Rightarrow$ non ci sono soluzioni.

3) $10x \equiv 16 \mod 18$ $\quad MCD(10,18) = 2$, inoltre $2 \mid 16 \Rightarrow$ esistono soluzioni

$\overline{10}$ non è invertibile in $\mathbb{Z}_{18}$ (dobbiamo trovare una via alternativa)

$\exists k \in \mathbb{Z}$ t.c. $10x = 16 + k \cdot 18$, possiamo dividere per 2; equivalentemente:

$5x = 8 + k \cdot 9$

ovvero: $5x \equiv 8 \mod 9$ $\quad MCD(5,9) = 1$ possiamo risolvere questa.

$\overline{5}$ è invertibile in $\mathbb{Z}_9$: $\overline{5} \cdot \overline{2} = \overline{1}$ in $\mathbb{Z}_9$

$\overline{2} = \overline{5}^{-1}$

$\Updownarrow$

$\overline{5} \cdot \overline{x} = \overline{8}$ in $\mathbb{Z}_9$

moltiplichiamo per $\overline{2}$:

$\overline{2} \cdot \overline{5} \cdot \overline{x} = \overline{2} \cdot \overline{8}$ in $\mathbb{Z}_9$

$\overline{x} = \overline{7}$ in $\mathbb{Z}_9$ $\quad$ cioè $\quad x \equiv 7 \mod 9$ $\quad S = \{\ldots -11, -2, 7, 16, 25, \ldots\} = [7]_9$

Se vogliamo interpretare le soluzioni in $\mathbb{Z}_{18}$: $\overline{x} = \overline{7}$ oppure $\overline{x} = \overline{16}$ in $\mathbb{Z}_{18}$

cioè $\quad x \equiv 7 \vee x \equiv 16 \mod 18$

Schema riassuntivo :

$$ax \equiv b \mod N \qquad \circledast$$

- Si calcola $MCD(a, N) = d$. 1) Se $d \mid b \Rightarrow$ ci sono soluzioni
2) se $d \nmid b \Rightarrow$ non ci sono soluzioni STOP.

1.1) Se $MCD(a, N) = 1$

Basta trovare $c \in \mathbb{Z}$ t.c. $\bar{a} \cdot \bar{c} = \bar{1}$ in $\mathbb{Z}_N$ (usare l'identità di Bézout)

Moltiplicando $\circledast$ per $\bar{c}$ si ottiene la soluzione.

1.2) Se $MCD(a, N) = d > 1$

Occorre dividere $\circledast$ per d : $\frac{a}{d} x \equiv \frac{b}{d} \mod \frac{N}{d}$

Allora $MCD\left(\frac{a}{d}, \frac{N}{d}\right) = 1$ e si torna al punto precedente.