# CONGRUENZE (mod $n$)

Def. Siano $a, b \in \mathbb{Z}$, $n \in \mathbb{N}^*$. Si dice che $a$ è congruo $b$ modulo $n$ e si scrive

$$a \equiv b \pmod n$$

se $n \mid a - b$.

Per esempio: $15 \equiv 7 \pmod 2$ perché $15 - 7 = 8$ che è multiplo di 2;

$18 \equiv 12 \pmod 3$ perché $18 - 12 = 6$ è è multiplo di 3;

$18 \equiv 12 \pmod 6$ perché $18 - 12 = 6$ che è multiplo di 6.

Fissato $n \in \mathbb{N}^*$, sia $R_n \subset \mathbb{Z} \times \mathbb{Z}$ così definita

$\forall a, b \in \mathbb{Z} \quad (a, b) \in R_n \iff a \equiv b \pmod n$

Prop. $R_n$ è una relazione di equivalenza su $\mathbb{Z}$.

$R_n$ è riflessiva: $\forall a \in \mathbb{Z}$ $\quad n \mid a-a$ perché $a-a=0$ e quindi la coppia $(a,a) \in R_n$

$R_n$ è simmetrica: $\forall a,b \in \mathbb{Z}$ $\quad (a,b) \in R_n \Rightarrow (b,a) \in R_n$

$a,b \in \mathbb{Z}$

$$\underbrace{(a,b) \in R_n} \Rightarrow n \mid a-b \Rightarrow n \mid -(a-b) \Rightarrow n \mid b-a \Rightarrow \underbrace{(b,a) \in R_n}$$

$R_n$ è transitiva: $\forall a,b,c \in \mathbb{Z}$ $\big((a,b) \in R_n \wedge (b,c) \in R_n\big) \Rightarrow (a,c) \in R_n$

Siano $\underline{a,b,c \in \mathbb{Z}}$ con $\underbrace{\big((a,b) \in R_n \wedge (b,c) \in R_n\big)} \Rightarrow$

$\Rightarrow (n \mid a-b \wedge n \mid b-c) \Rightarrow n \mid a-\cancel{b}+\cancel{b}-c \Rightarrow n \mid a-c \Rightarrow$

$\Rightarrow \underbrace{(a,c) \in R_n}$.

$R_n$ è una relazione di equivalenza su $\mathbb{Z}$.

__Prop__: Sia $n \in \mathbb{N}^*$ $\quad \forall a,b,c,d \in \mathbb{Z}$

1) $\big(a \equiv b \pmod n \wedge c \equiv d \pmod n\big) \Rightarrow a+c \equiv b+d \pmod n$

2) $\big(a \equiv b \pmod n \wedge c \equiv d \pmod n\big) \Rightarrow a \cdot c \equiv b \cdot d \pmod n$

3) $\forall k \in \mathbb{N}$ $\quad a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$

__Dim__. 1) $\big(a \equiv b \pmod n \wedge c \equiv d \pmod n\big) \Rightarrow (n \mid a-b \wedge n \mid c-d)$

$\Rightarrow n \mid a-b+c-d \Rightarrow n \mid (a+c)-(b+d) \Rightarrow a+c \equiv b+d \pmod n$

2) $(a \equiv b \pmod n \wedge c \equiv d \pmod n) \Rightarrow (n \mid a-b \wedge n \mid c-d) \Rightarrow$

$\Rightarrow (n \mid (a-b)c \wedge n \mid (c-d)b) \Rightarrow n \mid ac-\cancel{bc}+\cancel{bc}-bd \Rightarrow$

$\Rightarrow n \mid ac-bd \Rightarrow ac \equiv bd \pmod n$

3) si dimostra per induzione completa su $k$. $P(k): a^k \equiv b^k \pmod n$

passo base: $P(0)$: $a \equiv b \pmod n \Rightarrow a^0 \equiv b^0 \pmod n$ perché
$a^0 = b^0 = 1$ vero

passo induttivo: $P(k)$ vera $\Rightarrow P(k+1)$ vera
$$\Big(a \equiv b \pmod{} \wedge \underbrace{a^k \equiv b^k \pmod n}_{\text{ipotesi d'induzione}}\Big) \xRightarrow{2)} a^k \cdot a \equiv b^k \cdot b \pmod n$$

$\Rightarrow a^{k+1} \equiv b^{k+1} \pmod n$ questo prova la tesi.

per la definizione ricorsiva di potenza

Ricordiamo: sia $R$ una relazione di equivalenza su un insieme $A$.

$\forall a \in A \qquad [a]_R = \{b \in A : (a,b) \in R\}$

si definisce l'insieme quoziente $A/_R = \{[a]_R : a \in A\} \subset \mathcal{P}(A)$

Teorema. Sia $n \in \mathbb{N}^*$. Allora $\mathbb{Z}/_{R_n} = \{[0]_{R_n}, [1]_{R_n}, \dots, [n-1]_{R_n}\}$.

Per brevità si indica con $\mathbb{Z}_n = \mathbb{Z}/_{R_n}$ e

con $[a]_n = [a]_{R_n}$ $\forall a \in \mathbb{Z}$.

Dim. Proviamo che le classi $[0]_n, [1]_n, \dots, [n-1]_n$ sono tutte distinte tra loro.

Fissiamo $i, j \in \{0, 1, \dots, n-1\}$ $i \neq j$, per esempio supponiamo che sia $i < j$.

$$\left.\begin{array}{l} 0 \leq i \leq n-1 \\ 0 \leq j \leq n-1 \end{array}\right\} \Rightarrow 0 < j - i \leq n-1 < n$$

$$\underbrace{0 < j - i < n}$$

Supponiamo che sia $\underbrace{[i]_n = [j]_n} \Rightarrow (i,j) \in R_n \Rightarrow i \equiv j \pmod n$

$\Rightarrow n \mid j - i \Rightarrow \exists h \in \mathbb{N}^*$ tale che $\left.\begin{array}{l} j - i = nh \geq n \\ j - 1 < n \end{array}\right|$ contraddiz.

Ora si deve provare $\forall a \in \mathbb{Z} \ \exists\, r \in \{0, \dots, n-1\}$ tale che
$$[a]_n = [r]_n.$$

Sia $a \in \mathbb{Z}$, dividendo $a$ per $n$ si ha:
$\exists!\, q, r \in \mathbb{Z}$ tali che
$$a = nq + r \qquad 0 \leq r < n$$

$$a - r = nq$$
e quindi $n \mid a - r$, cioè $a \equiv r \pmod{n}$

$\exists!\, r \in \{0, \dots, n-1\}$ tale che $a \equiv r \pmod{n}$ per cui
$$[a]_n = [r]_n \quad \text{con} \quad r \in \{0, 1, \dots, n-1\}.$$

Esempi $\mathbb{Z}_1 = \{[0]_1\}$

$\forall a, b \in \mathbb{Z} \qquad a \equiv b \pmod{1} \Leftrightarrow 1 \mid a - b$ sempre

$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$$

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

$$\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$$

Numeri in base $n$.

Teorema. Sia $n \in \mathbb{N}^*$. $n \neq 1$. $\forall a \in \mathbb{N}$ esistono e sono unici $r_h, r_{h-1}, r_{h-2}, \dots, r_2, r_1, r_0 \in \mathbb{N}$ $0 \leq r_i < n$ tali che

$$a = r_h n^h + r_{h-1} n^{h-1} + r_{h-2} n^{h-2} + \dots + r_2 n^2 + r_1 n + r_0 .$$

Dim. (cenno) si divide $a$ per $n$

$$a = q_0 n + r_0 \qquad 0 \leq r_0 < n$$

$$q_0 = q_1 n + r_1 \qquad 0 \leq r_1 < n$$

$$q_1 = q_2 n + r_2 \qquad 0 \leq r_2 < n$$

$$\vdots$$

$$q_{h-1} = \underset{\substack{\parallel \\ 0}}{q_h} n + r_h \qquad 0 \leq r_h < n$$

$$a = q_0 n + r_0 = (q_1 n + r_1) n + r_0 = q_1 n^2 + r_1 n + r_0 =$$

$$= (q_2 n + r_2) n^2 + r_1 n + r_0 = q_2 n + r_2 n^2 + r_1 n + r_0 =$$

$$\dots = r_h n^h + r_{h-1} n^{h-1} + \dots + r_1 n + r_0 .$$

Osserv. Con le stesse notazioni del teorema, si scrive: $(a)_n = r_h\, r_{h-1}\, r_{h-2} \cdots r_1\, r_0$

e questa si dice scrittura di $a$ in base $n$.

Esempi. 128 in base 5

$$\overset{a}{128} = \overset{q_0}{25}\cdot\overset{n}{5} + \overset{r_0}{3}$$

$$\overset{q_0}{25} = \overset{q_1}{5}\cdot\overset{n}{5} + \overset{r_1}{0}$$

$$\overset{q_1}{5} = \overset{q_2}{1}\cdot\overset{n}{5} + \overset{r_2}{0}$$

$$\overset{q_2}{1} = \overset{q_3}{0}\cdot\overset{n}{5} + \overset{r_3}{1}$$

$$(128)_5 = 1003$$

$$128 = 25\cdot 5 + 3 = (5\cdot 5 + 0)\cdot 5 + 3 = 5\cdot 5^2 + 0\cdot 5 + 3 =$$

$$= (1\cdot 5 + 0)\cdot 5^2 + 0\cdot 5 + 3 = 1\cdot 5^3 + 0\cdot 5^2 + 0\cdot 5 + 3 =$$

$$= (0\cdot 5 + 1)\cdot 5^3 + 0\cdot 5^2 + 0\cdot 5 + 3 = 1\cdot 5^3 + 0\cdot 5^2 + 0\cdot 5 + 3$$

124 in base 5

$$\overset{a}{124} = \overset{q_0}{24}\cdot\overset{n}{5} + \overset{r_0}{4}$$

$$\overset{q_0}{24} = \overset{q_1}{4}\cdot\overset{n}{5} + \overset{r_1}{4}$$

$$\overset{q_1}{4} = \overset{q_2}{0}\cdot\overset{n}{5} + \overset{r_2}{4}$$

$$(124)_5 = 444$$

$$(100101)_{10} = 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2 + 1 =$$

in base 2

$$= 2^5 + 2^2 + 1 = 32 + 4 + 1 = 37.$$

$(n)_n = 10$

$n = 1\cdot n + 0$

$1 = 0\cdot n + 1$

$(n+1)_n = 11$

$(2)_2 = 10$

Sommiamo in base 2

$$\begin{array}{r} 1101 \\ 1001 \\ \hline 10110 \end{array}$$

Moltiplichiamo in base 2

$$\begin{array}{r} 1001 \times \\ 11 \\ \hline 1001 \\ 1001\phantom{0} \\ \hline 11011 \end{array}$$

Criteri di divisibilità.

Lemma Sia $n \in \mathbb{N}^*$ $a, b \in \mathbb{Z}$, con $a \equiv b \pmod{n}$

Allora: $n \mid a \iff n \mid b$

Dim. ipotesi $a \equiv b \pmod n$ ovvero $n \mid a-b$

$\Rightarrow$) se $n \mid a \wedge n \mid a-b$ allora $n \mid \cancel{a}-\cancel{a}+b$ cioè $n \mid b$

$\Leftarrow$) se $n \mid b \wedge n \mid a-b$ allora $n \mid \cancel{b}+a-\cancel{b}$ cioè $n \mid a$

Sia $a \in \mathbb{N}$ $\quad a = r_h 10^h + r_{h-1} 10^{h-1} + \dots + r_1 \cdot 10 + r_0$

$(a = r_h r_{h-1} \dots r_1 r_0)$ $\qquad 1259 = 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 9$

$$a - r_0 = 10 (r_h \cdot 10^{h-1} + r_{h-1} 10^{h-2} + \dots + r_1)$$

dunque $10 \mid a - r_0$

$5 \mid a - r_0$

$2 \mid a - r_0$

Per il lemma abbiamo $10 \mid a \Leftrightarrow 10 \mid r_0 \Leftrightarrow r_0 = 0$

$5 \mid a \Leftrightarrow 5 \mid r_0 \Leftrightarrow r_0 = 5 \vee r_0 = 0$

$2 \mid a \Leftrightarrow 2 \mid r_0$

$10 \equiv 1 \pmod 9$ $\qquad 10 - 1 = 9$ multiplo di 9

$10 \equiv 1 \pmod 3$ $\qquad 10 - 1 = 9$ " " 3

$a = r_h 10^h + r_{h-1} 10^{h-1} + \dots + r_1 \cdot 10 + r_0 \equiv$

$\equiv r_h \cdot 1 + r_{h-1} \cdot 1 + \dots + r_1 \cdot 1 + r_0 \pmod 9$
$\pmod 3$

infatti:
$10^k \equiv 1 \pmod 9$ $\quad 10^k \equiv 1 \pmod 3 \quad \forall k \in \mathbb{N}$
per il Lemma

$9 \mid a \iff 9 \mid r_h + r_{h-1} + \dots + r_1 + r_0$

$3 \mid a \iff 3 \mid r_h + r_{h-1} + \dots + r_1 + r_0$.

$10 \equiv -1 \pmod{11}$ perché $10 - (-1) = 10 + 1 = 11$
multiplo di 11

$10^k \equiv (-1)^k \pmod{11}$

$10^k \equiv 1 \pmod{11}$ se $k$ è pari

$10^k \equiv -1 \pmod{11}$ se $k$ è dispari

$a = r_h 10^h + \dots + r_1 \cdot 10 + r_0 \equiv r_h (-1)^h + r_{h-1} (-1)^{h-1} + \dots - r_1 \cdot 1 + r_0$

$11 \mid a \iff 11 \mid r_h (-1)^h + r_{h-1} (-1)^{h-1} + \dots - r_1 + r_0$.

Es. $\quad 3.190.429 \quad +\cancel{3} - \cancel{1} + 9 - 0 + 4 \cancel{-2} + 9 = 22$
$\rightarrow$ multiplo di 11