

Esercizi.

1. (appello di novembre 2021)

$$P(n): \sum_{i=0}^n (2i+1) = (n+1)^2 \quad n \in \mathbb{N} .$$

$$\sum_{i=0}^m 2i+1 = 1 + 3 + 5 + \dots + 2n+1 .$$

Passo base $P(0)$ è vera: $\sum_{i=0}^0 2i+1 = (0+1)^2$

$$\sum_{i=0}^0 2i+1 = 2 \cdot 0 + 1 = 1 \quad (0+1)^2 = 1$$

$P(0)$ è vera.

Passo induttivo: $P(n)$ vera $\Rightarrow P(n+1)$ vera

$$P(n) \text{ vera: } \sum_{i=0}^n (2i+1) = (n+1)^2 \quad \text{ipotesi d'induzione}$$

$$P(n+1) \text{ vera: } \sum_{i=0}^{n+1} (2i+1) = (n+1+1)^2 = (n+2)^2 \quad \text{terzi}$$

$$\sum_{i=0}^{n+1} (2i+1) = \sum_{i=0}^n (2i+1) + (2(n+1)+1) = \underset{\substack{\uparrow \\ \text{ipotesi d'induzione}}}{(n+1)^2} + (2n+2+1) =$$

$$= (n+1)^2 + 2n+3 = n^2 + 2n+1 + 2n+3 = n^2 + 4n+4 = (n+2)^2 .$$

Per il principio d'induzione completa $P(n)$ è vera $\forall n \in \mathbb{N}$.

$$2. \quad 2 \mid n^2 - n \quad \forall n \in \mathbb{N}.$$

Passo base: $P(0)$ vero: $2 \mid 0^2 - 0 \Rightarrow 2 \mid 0$ vero

Passo induttivo: $P(n)$ vero $\Rightarrow P(n+1)$ vero

$P(n)$ vero: $2 \mid n^2 - n$; ipotesi d'induzione

$P(n+1)$ vero: $2 \mid (n+1)^2 - (n+1)$ teni

$$\underline{(n+1)^2 - (n+1)} = n^2 + 2n + 1 - n - 1 = \underline{n^2 - n} + 2n$$

$(2 \mid n^2 - n$ per ipotesi d'induz. $\wedge \quad 2 \mid 2n)$ \Rightarrow

$$\Rightarrow 2 \mid \underline{n^2 - n + 2n} \Leftrightarrow 2 \mid (n+1)^2 - (n+1)$$

$$3. \quad \sum_{i=1}^n \frac{1}{i(i+1)(i+2)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} \right) \quad \forall n \in \mathbb{N}^*$$

$$\text{Passo base } P(1): \quad \sum_{i=1}^1 \frac{1}{i \cdot (i+1) \cdot (i+2)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(1+1)(1+2)} \right)$$

$$\text{stam: } \sum_{i=1}^1 \frac{1}{i(i+1)(i+2)} = \frac{1}{1 \cdot (1+1)(1+2)} = \frac{1}{1 \cdot 2 \cdot 3} = \frac{1}{6}$$

$$\text{dx: } \frac{1}{2} \left(\frac{1}{2} - \frac{1}{2 \cdot 3} \right) = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{6} \right) = \frac{1}{2} \cdot \frac{3-1}{6} = \frac{1}{2} \cdot \frac{2}{6} = \frac{1}{6}$$

Quindi $P(1)$ è vero.

Passo induuttivo: $P(n)$ vero $\Rightarrow P(n+1)$ vero

$$P(n) \text{ vero: } \sum_{i=1}^n \frac{1}{i(i+1)(i+2)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} \right) \quad \begin{matrix} \text{iotaesi} \\ \text{d'induzione} \end{matrix}$$

$$\frac{1}{p} > \frac{1}{m} \quad \text{quando } p < m$$

$$P(n+1) \text{ vero} \quad \sum_{i=1}^{n+1} \frac{1}{i(i+1)(i+2)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+2)(n+3)} \right) \quad \begin{matrix} + e s i \\ \text{+e si} \end{matrix}$$

$$\sum_{i=1}^{n+1} \frac{1}{i(i+1)(i+2)} = \sum_{i=1}^n \frac{1}{i(i+1)(i+2)} + \frac{1}{(n+1)(n+2)(n+3)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} \right) + \frac{1}{(n+1)(n+2)(n+3)} = \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} \right)$$

$\stackrel{\text{iotaesi d'induz.}}{=}$

$$= \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} \right) =$$

$$= \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} \right) =$$

$$= \frac{1}{2} \left(\frac{1}{2} + \frac{-(n+3) + 2}{(n+1)(n+2)(n+3)} \right) =$$

$$= \frac{1}{2} \left(\frac{1}{2} + \frac{-n-3+2}{(n+1)(n+2)(n+3)} \right) = \frac{1}{2} \left(\frac{1}{2} + \frac{\cancel{-(n+1)}}{\cancel{(n+1)}(n+2)(n+3)} \right) =$$

$$= \frac{1}{2} \left(\frac{1}{2} - \frac{1}{(n+2)(n+3)} \right).$$

CONGRUENZE LINEARI

Def. Siano $a, b \in \mathbb{Z}$ con $a \neq 0$. Si dice congruenza lineare l'espressione

$$(1) \quad ax \equiv b \pmod{n},$$

dove x è una incognita. Si dice soluzione di (1) un elemento $x_0 \in \mathbb{Z}$ tale che

$$ax_0 \equiv b \pmod{n}$$

ovvero tale che $n | ax_0 - b$. Se esiste x_0 soluzione di (1), allora si dice che (1) ammette soluzioni. Il caso $n=1$ non si considera perché banale.

Teorema. Siano $a, b \in \mathbb{Z}$ $a \neq 0$, $n \in \mathbb{N}^*$, $n \neq 1$.

La congruenza lineare (1) ha soluzioni se e solo se, post. $d = \text{M.C.D.}(a, n)$, risulta $d | b$.

Se inoltre x_0 è una soluzione di (1), tutte e sole le altre soluzioni sono $x_0 + h \bar{n}$, dove $\bar{n} = \frac{n}{d} \in \mathbb{N}$.

Infine ci sono esattamente d soluzioni non congruenti (mod n) e sono $x_0, x_0 + \bar{n}, \dots, x_0 + (d-1)\bar{n}$.

Dim. (1) ha soluzioni $\Leftrightarrow \exists x_0 \in \mathbb{Z}$ tale che $ax_0 \equiv b \pmod{n}$
 $\Leftrightarrow \exists x_0 \in \mathbb{Z}$ tale che $n | ax_0 - b \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z}$ tali che
 $ax_0 - b = y_0 n \Leftrightarrow \exists x_0, y_0 \in \mathbb{Z}$ tali che $ax_0 + n(-y_0) = b$
 $\Leftrightarrow \exists (x_0, y_0)$ soluzione della equazione Diofantea $ax + ny = b$
 \Leftrightarrow posto $d = \text{M.C.D.}(a, n)$ risulta $d | b$.

Se x_0 è una soluzione di (1), allora esiste $y_0 \in \mathbb{Z}$ tale che $(x_0, -y_0)$ è soluzione di $ax + ny = b$.
 Allora tutte le soluzioni sono: $(x_0 + \bar{m}h, -y_0 - \bar{a}h)$, $h \in \mathbb{Z}$ dove $\bar{a} = \frac{a}{d}$. Questi corrispondono a $x_0 + \bar{m}h$ sono tutte e sole le soluzioni di (1).
 Si tralascia la dimostrazione dell'ultima parte.

Esempio:

$$1. 155x \equiv 10 \pmod{55}$$

$$\begin{array}{rcl} 55 = 5 \cdot 11 & 155 & 5 \\ 155 = 5 \cdot 31 & 31 & 31 \\ & 1 & \end{array}$$

$d = \text{M.C.D.}(a, n) \mid b$ perché $5 \mid 10$.

Possiamo dividere per 5

$$a_1 \quad b_1 \quad n_1 \\ 31x \equiv 2 \pmod{\underline{11}}$$

$$31 = 11 \cdot 2 + 9 \Rightarrow g = 31 + 11(-2)$$

$$11 = 9 \cdot 1 + 2 \Rightarrow 2 = 11 + 9(-1)$$

$$g = 2 \cdot 4 + 1 \Rightarrow 1 = 9 + 2(-4)$$

$$2 = 2 \cdot 1 + 0$$

$$1 = 9 + 2(-4) = 9 + (11 + 9(-1))(-4) = 9 + 11 \cdot (-4) + 9 \cdot 1 = 9 \cdot 5 + 11(-4)$$

$$= (31 + 11 \cdot (-2)) \cdot 5 + 11(-4) = 31 \cdot 5 + 11(-10) + 11(-4) =$$

$$= 31 \cdot 5 + 11 \cdot (-14)$$

$$1 = 31 \cdot 5 + 11(-14) \quad \text{identità di Bezout}$$

$$\text{moltiplichiamo per } \bar{b}_1 = \frac{b_1}{d} = 2$$

$$t = 31 \cdot \underline{10} + 11(-28) =$$

Una soluzione è 10. Tutte le altre sono

$$10 + 11k \quad \text{per } k \in \mathbb{Z} \quad \bar{n}_1 = \frac{11}{1} = 11$$

Le soluz. non congrue fra loro $(\text{mod } 55)$

10 , 21 , 32 , 43 , 54

Il teorema ci assicura che le congruenze lineari
in oggetto ammette soluzioni.

$$155 = 55 \cdot 2 + 45 \Rightarrow 45 = 155 + 55(-2)$$

$$55 = 45 \cdot 1 + 10 \Rightarrow 10 = 55 + 45(-1)$$

$$45 = 10 \cdot 4 + 5 \xrightarrow{\text{H.C.D. } (155, 55)} \Rightarrow 5 = 45 + 10(-4)$$

$$10 = 5 \cdot 2 + 0$$

$$5 = 45 + 10(-4) = 45 + (55 + 45(-1))(-4) = 45 + 55(-1) + 45 \cdot 4 =$$

$$= 45 \cdot 5 + 55(-4) = (155 + 55(-2)) \cdot 5 + 55(-4) =$$

$$= 155 \cdot 5 + 55(-10) + 55 \cdot (-4) = 155 \cdot 5 + 55(-14)$$

$$5 = 155 \cdot 5 + 55(-14) \quad \text{idemthit de' Bezout}$$

$$\bar{b} = \frac{b}{d} = \frac{10}{5} = 2$$

moltiplichiamo tutto per \bar{b}

$$2 \cdot 5 = 155(10) + 55(-28)$$

$$10 = 155 \cdot 10 + 55(-28)$$

$$155 \cdot 10 - 10 = 55 \cdot 28 \quad \text{f28e71 tale che } 155 \cdot 10 - 10 = 55 \cdot 28$$

$$55 \mid 55 \cdot 10 - 10$$

$$155 \cdot 10 \equiv 10 \pmod{55}$$

$x_0 = 10$ è una soluzione di $155x \equiv 10 \pmod{55}$.

tutte le soluzioni: $10 + 11h$, $h \in \mathbb{Z}$.

ci sono 5 soluzioni non congrue tra loro $\pmod{55}$

-45	-34	-23	-19	-1
10	21	32	43	54
65	76	87	98	109
:	:	:	:	:
;	;	;	;	;

8. $144x \equiv 4 \pmod{48}$

$$144 = 12^2 = 3^2 \cdot 4^2 = 3^2 \cdot 2^4$$

$$48 = 6 \cdot 8 = 3 \cdot 2 \cdot 2^3 = 3 \cdot 2^4$$

$$\text{M.C.D.}(144, 48) = 48$$

$48 \nmid 4$ quindi

le congruenze lineare non ha soluzioni.

$$3. \quad 162x \equiv 24 \pmod{30}$$

$$\begin{array}{r|l} 162 & 2 \\ 81 & 3 \\ \hline & \end{array}$$

$$162 = 2 \cdot 3^4$$

$$30 = 2 \cdot 3 \cdot 5$$

$\text{M.C.D.}(162, 30) = \cancel{6}$ $6/2h$ e quindi ci sono soluzioni

dividendo tutto per 6: $\cancel{a_1} \quad \cancel{b_1} \quad \cancel{n_1}$
 $27x \equiv 4 \pmod{5}$

$$27 = 5 \cdot 5 + 2 \quad 2 = 27 + 5(-5)$$

$$5 = 2 \cdot 2 + 1 \quad \rightarrow \quad 1 = 5 + 2(-2)$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 5 + 2(-2) = 5 + (27 + 5(-5))(-2) = 5 + 27(-2) + 5(10) = 5 \cdot 11 + 27(-2)$$

$$1 = 27 \cdot (-2) + 5 \cdot 11 \quad \text{identità di Bezout.}$$

moltiplicate per 4:

$$4 = 27(-8) + 5 \cdot 44$$

una soluzione è $x_0 = -8$

Tutte le soluzioni $x = -8 + 5h$, $h \in \mathbb{Z}$ ($\bar{n}_1 = 5$)

Le soluzioni non congrue tra loro mod 30:
sono in numero 186:

$$-8, -3, 2, \underset{22}{\cancel{2}}, 7, 12, 17$$

non congrue $(\text{mod } 30)$

minime soluzioni
positive

SISTEMI DI CONGRUENZE LINEARI

$$a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z} \quad a_1 \neq 0, \dots, a_n \neq 0$$

$$n_1, \dots, n_n \in \mathbb{N} = \{0, 1\}$$

Un sistema di congruenze lineari è del tipo

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1} \\ a_2 x \equiv b_2 \pmod{n_2} \\ \vdots \\ a_n x \equiv b_n \pmod{n_n} \end{cases}$$

Risolvere un sistema di congruenze lineari significa
verificare se tale sistema ha soluzioni (in primis
verificare se le singole congruenze lineari hanno soluzioni)

e quindi determinare tutte le soluzioni si multiasse delle congruenze lineari componenti il sistema.

Esempio:

$$\begin{cases} 3x \equiv 4 \pmod{5} \\ 2x \equiv 4 \pmod{3} \end{cases}$$

$$3 \cdot 8 - 4 = 24 - 4 = 20 \text{ multiplo di } 5$$

$$2 \cdot 8 - 4 = 16 - 4 = 12 \text{ multiplo di } 3$$

Le congruenze componenti il sistema hanno soluzioni.

$$3x \equiv 4 \pmod{5}$$

3 è una soluzione perché

$$3 \cdot 3 - 4 = 9 - 4 = 5 \text{ multiplo di } 5.$$

$$x = 3 + 5h, \quad h \in \mathbb{Z}$$

$$2(3 + 5h) \equiv 4 \pmod{3}$$

$$6 + 10h \equiv 4 \pmod{3}$$

$$10h \equiv 4 - 6 \pmod{3}$$

$$10h \equiv -2 \pmod{3}$$

$$10h \equiv 1 \pmod{3}$$

$$\left. \begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array} \right\} \Rightarrow a + c \equiv b + d \pmod{n}$$

$$-2 \equiv 1 \pmod{3}$$

$h = 1$ è una soluzione perché $10 \cdot 1 - 1 = 9$ multiplo di 3.

$$h = 1 + 3k, \quad k \in \mathbb{Z}$$

$$x = 3 + 5k = 3 + 5(1+3k) = 3 + 5 + 15k = 8 + 15k$$

$k \in \mathbb{Z}$

Le soluzioni del sistema sono

$$x = 8 + 15k, \quad k \in \mathbb{Z}.$$

Teorema chiuso del resto.

Siano $b_1, \dots, b_n \in \mathbb{Z}$, $n_1, \dots, n_h \in \mathbb{N} - \{0, 1\}$.

Se $\text{M.C.D.}(n_i, n_j) = 1 \quad \forall i, j \in \{1, 2, \dots, h\}$ allora il sistema di congruenze lineari

$$(2) \quad \begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \vdots \\ x \equiv b_n \pmod{n_n} \end{cases}$$

ammette soluzioni. Se x_0 è una soluzione tutta e sole le soluzioni sono $x_0 + Rh$, dove $R = n_1 \cdot n_2 \cdot \dots \cdot n_h$.

Caso di dim. Si ponе

$$R_1 = \frac{R}{n_1}, \quad R_2 = \frac{R}{n_2}, \quad \dots, \quad R_h = \frac{R}{n_h}$$

Si considerano le congruenze lineari

$$R_1 x \equiv b_1 \pmod{n_1}$$

x_1 soluzione

$$R_2 x \equiv b_2 \pmod{n_2}$$

x_2 soluzione

$$R_n x \equiv b_n \pmod{m_n} \quad x_n \text{ soluzione}$$

Si vede che

$$x_0 = R_1 x_1 + R_2 x_2 + \dots + R_n x_n$$

è una soluzione del sistema di partenza (2).