# Lezione 06 - 13/10/2022



# Algoritmo euclideo

Notazione: Si chiama $(a, b) = \text{MCD}$ positivo di $a, b$.

Nel seguito vediamo come:

1. Calcolare algoritmicamente $(a, b)$
2. Trovare un'identità di bezout per $(a, b)$

Esempio:

- $(3522, 321)$

$$\begin{aligned} 3522 &= 321 \cdot 10 + 312 \\ 321 &= 312 \cdot 1 + 9 \\ 312 &= 9 \cdot 34 + 6 \\ 9 &= 6 \cdot 1 + \underline{3} \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

  Dove l'ultimo resto non nullo nella catena di divisioni è il risultato, in questo caso $(3522, 321) = 3$.

  Vediamo l'dentità di bezout: cerchiamo un'espressione del tipo $3 = x \cdot 321 + y \cdot 3522$

$$
\begin{aligned}
3 &= 9 - 6 \\
&= 9 - (312 - 9 \cdot 34) \\
&= 9 \cdot 35 - 312 \\
&= (321 - 312) \cdot 35 - 312 \\
&= 321 \cdot 35 - 312 \cdot 36 \\
&= 321 \cdot 35 - (3522 - 321 \cdot 10) \cdot 36 \\
&= -3522 \cdot 36 + 321 \cdot 35 + 321 \cdot 360 \\
&= -3522 \cdot 36 + 321 \cdot 395
\end{aligned}
$$

quindi abbiamo che $3 = -3522 \cdot 36 + 321 \cdot 395$.

- $(57, 23)$

$$
\begin{aligned}
57 &= 23 \cdot 2 + 11 \\
23 &= 11 \cdot 2 + \underline{1} \\
11 &= 1 \cdot 11 + 0
\end{aligned}
$$

Quindi $(57, 23) = 1$ (sono coprimi)

Vediamo l'identità di bezout: cerchiamo un'espressione del tipo $1 = x \cdot 23 + y \cdot 57$

$$
\begin{aligned}
1 &= 23 - 11 \cdot 2 \\
&= 23 - (57 - 23 \cdot 2) \cdot 2 \\
&= 23 - 57 \cdot 2 + 23 \cdot 4 \\
&= 23 \cdot 5 - 57 \cdot 2
\end{aligned}
$$

quindi abbiamo che $1 = 23 \cdot 5 - 57 \cdot 2$.

# Proposizione - Soluzioni di ax+by=c

L'equazione $(1) ax + by = c,\ a, b, c \in \mathbb{Z}$ possiede una soluzione intera

$$(x, y) \in \mathbb{Z} \text{ sse } (a, b) \mid c$$

Esempi:

- $2x + 2y = 5$ non ha soluzione intere perche $(2, 2) \nmid 5$

- $2x + 2y = 4$ ha soluzioni intere, ad esempio $x = y = 1$

Dimostrazione: supponiamo che l'equazione $(1)$ abbia soluzione $(\bar{x}, \bar{y})$. Allora vale

$$a\bar{x} + b\bar{y} = c$$

Sia $d = (a, b)$ con $d \mid a$ e $d \mid b$, quindi $d \mid a\bar{x}, d \mid b\bar{y}$, quindi $d \mid a\bar{x} + b\bar{y} = c$ come vogliamo.

Viceversa, supponiamo che $d \mid c$. Scriviamo l'**identità di bezout** per $d$:

$$d = \alpha a + \beta b$$

Poichè $d \mid c, c = hd$

$$c = hd = \underbrace{h\alpha}_{x} a + \underbrace{h\beta}_{y} b$$

# Proposizione - In Z ogni irriducibile è primo

In $\mathbb{Z}$ ogni **irriducibile** è **primo**.

Dimostrazione: Supponiamo $p$ **irriducibile** e $p \mid ab$. Dobbiamo far vedere che se $p \nmid a$ allora $p \mid b$.

Siccome $p \mid ab,\ ab = ph \Rightarrow (a, p) = 1.$

Dunque esistono $s, t \in \mathbb{Z}$ t.c. $as + tp = 1$. Moltiplico questa relazione per $b$

$$b = bas + btp = \overbrace{abs}^{p|} + \overbrace{pbt}^{p|} \Rightarrow p \mid b$$

# Teorema fondamentale dell'aritmetica

Sia $n > 1$ un intero. Allora $n$ è prodotto di un numero finito di potenze di primi:

$$n = p_1^{h_1} ... p_s^{h_s} \quad h_i > 0,\ p_i \neq p_j,\ i \neq j$$

Inoltre tale fattorizzazione è unica nel senso che se

$$n = q_1^{k_1} ... q_t^{k_t} \quad k_i > 0,\ q_i \neq q_j, i \neq j, q_i \text{ primi}$$

allora $s = t$ a meno di **rioridinamenti $p_i = q_i$ e $h_i = k_i$.**

Dimostrazione:

- **Esistenza**: per induzione su $n$, con base ovvia $n = 2$.

  Supponiamo di avere dimostrato l'esistenza della fattorizzazione per ogni intero $k,\ 2 \leq k < n$ e dimostriamola per $n$.

  Se $n$ è **primo** non c'è **nulla da dimostrare**.

  Altrimenti **non è irriducibile**, quindi può scriversi come

$$\begin{aligned} n = n_1 n_2, \quad & 2 \leq n_1 < n \\ & 2 \leq n_2 < n \end{aligned}$$

  Per induzione $n_1, n_2$ hanno fattorizzazione e quindi anche $n$ ce l'ha

$$n_1 = p_1^{a_1} ... p_s^{a_s} \ , \quad n_2 = q_1^{b_1} ... q_s^{b_s}$$
$$n = p_1^{a_1} ... p_s^{a_s} q_1^{b_1} ... q_s^{b_s} = t_1^{c_1} ... t_n^{c_n} \text{ con i } t_i \ \underline{\text{primi}}$$

  Esempio:

$$\begin{aligned} n_1 &= 2^3 \cdot 3^4 \cdot 5 \\ n_2 &= 2^3 \cdot 3 \cdot 5 \cdot 7 \\ n_1 n_2 &= 2^6 \cdot 3^5 \cdot 5^2 \cdot 7 \end{aligned}$$

- **Unicità**: Si consideri $n = p_1^{h_1} ... p_s^{h_s} \ (*)$

  Procediamo per induzione su $m = h_1 + ... + h_s$

  - Caso base: $m = 1$; la $(*)$ ci dice che $n$ è primo. **Supponiamo** che ci sia **un'altra fattorizzazione in primi**. Sia $p$

$$\begin{aligned} p = n = q_1^{k_1} ... q_t^{k_t} \\ \implies p \mid q_1^{k_1} ... q_t^{k_t} \end{aligned}$$

    Poichè $p$ è primo, $p$ **divide uno dei $q_i$**

$$p \mid q_i$$

    ma $q_i$ è primo, quindi $p = q_i$. Allora

$$p = q_1^{k_1} ... p^{k_i} ... q_t^{k_t}$$

implica

$$\begin{aligned} 1 &= q_1^{k_1} ... p^{k_i - 1} ... q_t^{k_t} \\ \implies k_1 &= ... = k_{i-1} = k_{i+1} = ... = k_t = 0 \quad k_i = 1 \end{aligned}$$

Quindi la seconda fattorizzazione è proprio $n = q_i = p$.

- Caso $m > 1$: **supponiamo** che $n$ abbia **due fattorizzazioni.**

$$(**) n = p_1^{h_1} ... p_s^{h_s} = q_1^{k_1} ... q_t^{k_t}$$

con $h_1 + ... + h_s = m_i$ come prima

$$p_1 \mid q_1^{k_1} ... q_t^{k_t}$$

quindi come prima $p_1 \mid q_i$ e quindi $p_1 = q$.

Allora $(**)$ diventa

$$\begin{aligned} p_1^{h_1} ... p_s^{h_s} &= q_1^{k_1} ... p_1^{k_i} ... q_t^{k_t} \\ p_1^{h_1 - 1} ... p_s^{h_s} &= q_1^{k_1} ... p_1^{k_i - 1} ... q_t^{k_t} \end{aligned}$$

Al primo membro la somma degli esponenti è $m - 1$. Per induzione ho l'unicità della fattorizzazione, quindi $h_i - 1 = k_i - 1$ e gli altri fattori coincidono a meno di riordinamento. Quindi la **fattorizzazione di $n$ è unica**.

> ⚠️ Si noti come nel corso della dimostrazione si sia utilizzata pesantemente l'equivalenza in $\mathbb{Z}$ tra l'essere **primo** e l'essere **irriducibile**.

## Proposizione - I numeri primi sono infiniti

Dimostrazione: supponiamo il viceversa, ovvero che $p_1 ... p_N$ sia la lista **finita** di tutti i numeri primi. Sia

$$M = p_1 \cdot ... \cdot p_N + 1$$

Osserviamo che $M$ da resto $1$ quando è diviso per ogni numero primo, quindi $M$ **non è divisibile** per nessun primo, **contro il teorema fondamentale dell'aritmetica**$\blacksquare$

# Congruenze e sistemi di congruenze

Vogliamo risolvere equazioni del tipo

$$ax = b \text{ in } \mathbb{Z}_n$$

ovvero **congruenze** del tipo

$$ax \equiv b \mod n$$

e anche sistemi del tipo

$$\begin{cases} a_1 x \equiv b_1 \mod n_1 \\ a_2 x \equiv b_2 \mod n_2 \\ ... \\ a_k x \equiv b_k \mod n_k \end{cases}$$

## Proprietà fondamentali delle congruenze

Ricordiamo che $a \equiv b \mod n$ se $n \mid b - a$

$$\begin{aligned} a &= xn + r \\ b &= yn + r \\ b - a &= (x-y)n \Rightarrow n \mid b - a \end{aligned}$$

viceversa se $n \mid b - a,\ b - a = hn$, se

$$\begin{aligned} a &= xn + r_1 \\ b &= yn + r_2 \\ b - a &= (x-y)n + r_1 - r_2 \\ &= hn \Rightarrow r_1 = r_2 \end{aligned}$$

⚠️ Il fatto che $r_1 = r_2$ segue dal fatto che $n$ divide $a - b$, quindi il resto deve essere $0$. Questo accade solo se $r_1 = r_2$.

Sia $a \equiv_n b$; allora

1. $a + c \equiv_n b + c$
2. $ac \equiv_n bc$
3. $a^i \equiv_n b^i,\ i \geq 0$
4. $ac \equiv_n bc,\ (c, n) = 1 \Rightarrow a \equiv_n b$

$$\begin{gathered} n \mid bc - ac = (b-a)c \\ (c,n) = 1 \Rightarrow \exists s, t : cs + tn = 1 \\ b - a = (b-a)cs + (b-a)tn \\ = ns + (b-a)tn \\ = n(s + (b-a)t) \end{gathered}$$

   Dunque $n \mid b - a$, ovvero $a \equiv_n b$.

5. $ac \equiv bc \mod n \Rightarrow a \equiv b \mod \dfrac{n}{(n, c)}$

⚠️ Nota: **non** è vero che $ac \equiv_n bc \Rightarrow a \equiv_n b$, ovvero non è vero che si può dividere per $c$. Esempio:

$$\begin{gathered} 3 \cdot 5 \equiv 3 \cdot 8 \mod 9 \\ 15 \equiv 24 \mod 9 \\ 6 \equiv 6 \mod 9 \checkmark \end{gathered}$$

Ma $5 \not\equiv 8 \mod 9$.

# Lemma

Sia $p$ primo e $x, y \in \mathbb{Z}$,

$$(x+y)^p = x^p + y^p \mod p$$

Dimostrazione:

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Ma $p \mid \binom{p}{k}$ se $k \neq 0, p$, quindi nella somma restano solo il primo e l'ultimo termine $\mod p$

$$(x+y)^p = \underbrace{\binom{p}{0}}_{=1} x^0 + y^{p-0} + \underbrace{\binom{p}{p}}_{=1} x^p y^{p-k} = x^p + y^p$$

# Teorema - Piccolo teorema di Fermat

Sia $a \in \mathbb{Z}$, $p$ un **numero primo**, allora

$$a^p \equiv a \mod p$$

Dimostrazione: Se $a \geq 0$, **procediamo per induzione** su $a$

- $a = 0$

  Non c'è niente da dimostrare

- $a > 0$

  Assumiamo $a^p \equiv a \mod p$ sia vero e dimostriamo che $(a+1)^p \equiv a+1 \mod p$.

  $$(a+1)^p \equiv a^p + 1^p \equiv a^p + 1 \equiv a + 1 \mod p$$

- $a < 0$

  $$0 = 0^p = (a + (-a))^p \equiv a^p + (-a)^p \equiv a^p - a \Rightarrow a^p \equiv a \mod p$$

  Nota: dato che $-a > 0$, per quanto provato nel punto precedente si ha che $(-a)^p \equiv -a$.

## Corollario

Se $(a, p) = 1$, allora $a^{p-1} \equiv 1 \mod p (*)$.

Dimostrazione: Se $(a,p)=1$, posso semplificare $a$ nella relazione $a^p \equiv a \mod p$, ottenendo $(*)$