

# Lezione 15

Alessandro Ardizzoni

# Identità di Bézout

C'è una formula che lega due numeri al loro massimo comun divisore.

## Teorema (Identità di Bézout)

*Siano  $a, b \in \mathbb{Z}$ . Allora esistono  $m, n \in \mathbb{Z}$  tali che*

$$\text{MCD}(a, b) = m \cdot a + n \cdot b.$$

DIMOSTRAZIONE. Se  $b = 0$ , allora

$$\text{MCD}(a, b) = \text{MCD}(a, 0) = |a| = \pm 1 \cdot a + 0 \cdot b.$$

Se  $b \neq 0$ , guardiamo ai vari passi dell'algoritmo a ritroso e ricaviamo ogni resto in funzione dei resti che lo precedono eliminando dopo ogni passo i resti con pedice maggiore.

Esplicitamente, se i passi dell'algoritmo sono

Passo	divisione
0)	$a = q_0 b + r_0$
1)	$b = q_1 r_0 + r_1$
2)	$r_0 = q_2 r_1 + r_2$
...	
$n$ )	$r_{n-2} = q_n r_{n-1} + \boxed{r_n}$
$n+1$ )	$r_{n-1} = q_{n+1} r_n + 0$

partendo dall'ultimo resto non nullo, che è proprio  $\text{MCD}(a, b)$ , scriveremo

$$\begin{aligned}
 \text{MCD}(a, b) &= r_n \stackrel{n)}{=} r_{n-2} - q_n r_{n-1} \stackrel{n-1)}{=} r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\
 &= r_{n-2} - q_n r_{n-3} + q_n q_{n-1} r_{n-2} = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} \\
 &\stackrel{n-2)}{=} (\cdots) r_{n-4} + (\cdots) r_{n-3} = \cdots = (\cdots) a + (\cdots) b.
 \end{aligned}$$

Alla fine scompaiono tutti i resti e compaiono  $a$  e  $b$ .

## Osservazione

*I numeri  $m$  e  $n$  coinvolti nell'identità di Bézout non sono necessariamente unici. Ad esempio:  $1 \cdot \underline{3} + (-1) \cdot \underline{2} = \text{MCD}(3,2) = (-1) \cdot \underline{3} + 2 \cdot \underline{2}$ .*

Vediamo il procedimento concretamente in un esercizio.

## Esercizio

*Determinare l'identità di Bézout per i numeri 98 e 77.*

**SOLUZIONE.** Prima applichiamo l'algoritmo Euclideo:

$$0) \quad \underline{98} = 1 \cdot \underline{77} + \underline{21}$$

$$1) \quad \underline{77} = 3 \cdot \underline{21} + \underline{14}$$

$$2) \quad \underline{21} = 1 \cdot \underline{14} + \boxed{7}$$

$$3) \quad \underline{14} = 2 \cdot \underline{7} + \underline{0}.$$

dove abbiamo sottolineato dividendo, divisore e resto.  
Sappiamo che il massimo comun divisore è l'ultimo resto non nullo trovato, cioè  $\text{MCD}(98,77) = 7$ .

Ora ricaviamo a ritroso l'identità di Bézout:

$$\begin{aligned} \text{MCD}(98,77) = 7 &\stackrel{2)}{=} \underline{21} - 1 \cdot \underline{14} \stackrel{1)}{=} \underline{21} - 1 \cdot (\underline{77} - 3 \cdot \underline{21}) = \underline{21} - \underline{77} + 3 \cdot \underline{21} \\ &= 4 \cdot \underline{21} - \underline{77} \stackrel{0)}{=} 4 \cdot (\underline{98} - 1 \cdot \underline{77}) - \underline{77} = 4 \cdot \underline{98} - 4 \cdot \underline{77} - \underline{77} = 4 \cdot \underline{98} - 5 \cdot \underline{77}. \end{aligned}$$

Pertanto l'identità di Bézout è  $\text{MCD}(98,77) = 4 \cdot \underline{98} - 5 \cdot \underline{77}$ .

## Esercizio

*Determinare l'identità di Bézout per i numeri  $-98$  e  $77$ .*

SOLUZIONE. Sappiamo che  $\text{MCD}(-98, 77) = \text{MCD}(98, 77)$ . Ora, nell'esercizio precedente, abbiamo ottenuto che  $\text{MCD}(98, 77) = 4 \cdot \underline{98} - 5 \cdot \underline{77}$ . Volendo un'espressione del tipo  $\text{MCD}(-98, 77) = m \cdot (\underline{-98}) + n \cdot \underline{77}$ , ci basta allora scegliere  $m = -4$  ed  $n = -5$ .

Questo ci dice che **possiamo ricavare l'identità di Bézout a partire da quella degli stessi due numeri presi in valore assoluto.**

## Lemma (di Euclide)

$\forall a, b, c \in \mathbb{Z}$ , se  $\text{MCD}(a, b) = 1$  allora  $a \mid bc \Rightarrow a \mid c$ .

DIMOSTRAZIONE. Per l'identità di Bézout esistono  $m, n$  tali che  $1 = ma + nb$ . Moltiplicando per  $c$  otteniamo  $c = m\underline{a}c + n\underline{b}c$ . Visto che i due addendi sono divisibili per  $a$ , lo è anche la loro somma, cioè  $c$ .

# Funzione di Eulero


Due numeri naturali  $a, b$  si dicono **coprimi** se  $\text{MCD}(a, b) = 1$ .

## Definizione

Definiamo la **funzione di Eulero**

$$\varphi : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$$

ponendo


$$\varphi(n) = |\{k \in \mathbb{Z} \mid 1 \leq k \leq n \wedge \text{MCD}(k, n) = 1\}|.$$

## Osservazione

Notiamo che, se  $n \neq 1$ , nella definizione di  $\varphi(n)$  potevamo mettere equivalentemente  $1 \leq k \leq n-1$  oppure  $0 \leq k \leq n$  perché  $\text{MCD}(n, n) = n \neq 1$  e  $\text{MCD}(0, n) = n \neq 1$ .

## Esempio

Vediamo ad esempio per  $1 \leq n \leq 6$  quali sono i  $k$  con  $1 \leq k \leq n$  per cui  $\text{MCD}(k, n) = 1$ . Li evidenziamo con un riquadro.

$n$	$k$ con $1 \leq k \leq n$	$\varphi(n)$
1	<span style="border: 1px solid black;">1</span>	1
2	<span style="border: 1px solid black;">1</span> 2	1
3	<span style="border: 1px solid black;">1</span> <span style="border: 1px solid black;">2</span> 3	2
4	<span style="border: 1px solid black;">1</span> 2 <span style="border: 1px solid black;">3</span> 4	2
5	<span style="border: 1px solid black;">1</span> <span style="border: 1px solid black;">2</span> <span style="border: 1px solid black;">3</span> <span style="border: 1px solid black;">4</span> 5	4
6	<span style="border: 1px solid black;">1</span> 2 3 4 <span style="border: 1px solid black;">5</span> 6	2

## Osservazione

Se  $p$  è primo allora  $\text{MCD}(k, p) = 1$  per ogni  $k$  con  $1 \leq k \leq p-1$  e dunque  $\varphi(p) = p-1$ .

Indichiamo con  $\mathbb{Z}_n^\times$  l'insieme degli elementi invertibili nel monoide  $(\mathbb{Z}_n, \cdot)$ .

## Proposizione

Sia  $n \in \mathbb{N} \setminus \{0\}$ . Si ha che  $\mathbb{Z}_n^\times = \{\bar{k} \in \mathbb{Z}_n \mid \text{MCD}(k, n) = 1\}$ .

DIMOSTRAZIONE. ( $\subseteq$ ). Se  $\bar{k} \in \mathbb{Z}_n^\times$  allora  $\exists \bar{a} \in \mathbb{Z}_n, \bar{a}\bar{k} = \bar{1}$ . Pertanto  $n \mid 1 - ak$  e quindi esiste  $b \in \mathbb{Z}$  tale che  $1 - ak = bn$  e dunque  $ak + bn = 1$ . Allora  $\text{MCD}(k, n) \mid ak + bn = 1$  e dunque  $\text{MCD}(k, n) = 1$ .

( $\supseteq$ ). Se  $\text{MCD}(k, n) = 1$ , per l'identità di Bézout esistono  $a, b \in \mathbb{Z}$  tali che  $\text{MCD}(k, n) = ak + bn$  cioè  $1 = ak + bn$ . Modulo  $n$  questa uguaglianza diventa  $\bar{1} = \bar{a}\bar{k}$  cioè  $\bar{1} = \bar{a} \cdot \bar{k}$ . Quindi  $\bar{k} \in \mathbb{Z}_n^\times$ .

## Corollario

$$|\mathbb{Z}_n^\times| = \varphi(n).$$

DIMOSTRAZIONE. Abbiamo che

$$\begin{aligned} |\mathbb{Z}_n^\times| &= |\{\bar{k} \in \mathbb{Z}_n \mid \text{MCD}(k, n) = 1\}| \\ &= |\{\bar{k} \in \{\bar{1}, \bar{2}, \dots, \bar{n}\} \mid \text{MCD}(k, n) = 1\}| \\ &= |\{k \in \mathbb{Z} \mid 1 \leq k \leq n \wedge \text{MCD}(k, n) = 1\}| = \varphi(n). \end{aligned}$$



## Esempio

$$\mathbb{Z}_6^\times = \{\bar{k} \in \mathbb{Z}_6 \mid \text{MCD}(k, 6) = 1\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \{\bar{1}, \bar{5}\}.$$

In effetti  $\bar{1} \cdot \bar{1} = \bar{1}$  e  $\bar{5} \cdot \bar{5} = \bar{1}$  e dunque  $\bar{1}$  e  $\bar{5}$  sono inversi di sé stessi.

## Esercizio

*Stabilire se  $\bar{2}$  è invertibile in  $\mathbb{Z}_{15}$  e, nel caso, calcolarne l'inverso.*

## Soluzione

$\text{MCD}(2, 15) = 1$ . Quindi  $\bar{2}$  è invertibile. Per individuare l'inverso scriviamo l'identità di Bézout. In questo caso si vede ad occhio che  $2 \cdot (8) + 15 \cdot (-1) = 1$ . Modulo 15 questa uguaglianza diventa  $\bar{2} \cdot \bar{8} = \bar{1}$  e quindi  $(\bar{2})^{-1} = \bar{8}$ . Possiamo fare una piccola verifica per controllare l'esattezza del risultato ottenuto:  $\bar{2} \cdot \bar{8} = \overline{16} = \overline{1 + 15} = \bar{1}$ .

# Equazione diofantea lineare

Un'**equazione diofantea** è un'equazione in una o più incognite con coefficienti interi di cui si ricercano le soluzioni intere. Consideriamo il seguente caso particolare. Una **soluzione** in  $\mathbb{Z}$  dell'equazione

$$ax + by = c, \quad a, b, c \in \mathbb{Z}$$

è una coppia  $(m, n) \in \mathbb{Z} \times \mathbb{Z}$  tale che  $am + bn = c$ .

**Risolvere l'equazione in  $\mathbb{Z}$**  significa trovare tutte le sue soluzioni in  $\mathbb{Z}$ .

## Lemma (Criterio di risolubilità)

*L'equazione diofantea  $ax + by = c$  ha soluzione  $\Leftrightarrow \text{MCD}(a, b) \mid c$ .*

DIMOSTRAZIONE.  $(\Rightarrow)$ . Se  $\exists (m, n) \in \mathbb{Z} \times \mathbb{Z}$  tale che  $am + bn = c$ , allora  $\text{MCD}(a, b) \mid am + bn = c$ .

$(\Leftarrow)$ . Poniamo  $d := \text{MCD}(a, b)$ . Se  $d \mid c$  allora  $d$  divide  $a, b, c$ .

Se  $d = 0$ , allora  $a = b = c = 0$  e  $(0, 0)$  è una soluzione banale.

Vediamo cosa succede se  $d \neq 0$ .

Se  $d \neq 0$ , possiamo dividere per  $d$  ottenendo un'equazione equivalente (che ha cioè le stesse soluzioni):

$$ax + by = c \Leftrightarrow \underbrace{\frac{a}{d}}_{a'} x + \underbrace{\frac{b}{d}}_{b'} y = \underbrace{\frac{c}{d}}_{c'}.$$

Notiamo che

$$\text{MCD}(a', b') = \text{MCD}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{MCD}(a, b)}{d} = \frac{d}{d} = 1.$$

Per l'identità di Bézout, esistono  $m, n \in \mathbb{Z}$  tali che

$$a'm + b'n = \text{MCD}(a', b') = 1.$$

Moltiplicando per  $c'$  otteniamo  $a'mc' + b'nc' = c'$ . Quindi  $(mc', nc') \in \mathbb{Z} \times \mathbb{Z}$  è una soluzione dell'equazione  $a'x + b'y = c'$  e dunque anche di  $ax + by = c$  che è ad essa equivalente. □

A partire da una singola soluzione possiamo ricavare tutte le altre:

## Teorema

*Consideriamo l'equazione diofantea  $ax + by = c$  con  $a, b, c \in \mathbb{Z}$ . Se  $\text{MCD}(a, b) = 1$ , le sue soluzioni sono le coppie  $(x, y) \in \mathbb{Z} \times \mathbb{Z}$  della forma*

$$x = x_0 + kb, \quad y = y_0 - ka, \quad k \in \mathbb{Z}. \quad (1)$$

*dove  $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$  è una soluzione particolare derivante dall'identità di Bézout.*

DIMOSTRAZIONE. Dal lemma precedente, sappiamo che  $ax + by = c$  ha soluzioni perché  $\text{MCD}(a, b) = 1 \mid c$ . Tramite l'identità di Bézout possiamo quindi ricavare una soluzione particolare  $(x_0, y_0)$ .

Sostituendo, si vede subito che (1) è una soluzione:

$$a(x_0 + kb) + b(y_0 - ka) = ax_0 + \cancel{kab} + by_0 - \cancel{kab} = ax_0 + by_0 = c.$$

Vediamo che sono tutte fatte così.

Se  $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$  è una soluzione, allora  $ax_1 + by_1 = c = ax_0 + by_0$ .  
Pertanto

$$a(x_1 - x_0) = b(y_0 - y_1). \quad (2)$$

Siccome  $\text{MCD}(a, b) = 1$ , allora  $a$  e  $b$  non sono entrambi nulli (perché  $\text{MCD}(0, 0) = 0$ ): possiamo assumere  $a \neq 0$  (se  $b \neq 0$  si procede analogamente).

Poiché  $a \mid b(y_0 - y_1)$  e  $\text{MCD}(a, b) = 1$ , dal Lemma di Euclide deduciamo  $a \mid (y_0 - y_1)$ . Quindi esiste  $k \in \mathbb{Z}$  tale che  $y_0 - y_1 = ka$  cioè

$$y_1 = y_0 - ka.$$

Sostituendo in (2), otteniamo  $a(x_1 - x_0) = bka$ . Siccome  $a \neq 0$ , possiamo semplificare arrivando a  $x_1 - x_0 = bk$ . In definitiva

$$x_1 = x_0 + kb.$$



## Esercizio

Risolvere in  $\mathbb{Z}$ , se possibile, l'equazione  $12x + 39y = 15$ .

SOLUZIONE. Notiamo prima di tutto che  $\text{MCD}(12, 39) = 3 \mid 15$ . Quindi l'equazione si può risolvere. Dividiamo l'equazione per 3 ottenendo l'equazione equivalente

$$4x + 13y = 5.$$

Visto che  $\text{MCD}(4, 13) = 1$  questa equazione si può risolvere per il teorema precedente. Troviamo una soluzione particolare attraverso l'identità di Bézout  $1 = m \cdot 4 + n \cdot 13$  che possiamo ricavare con il metodo che abbiamo visto oppure ad occhio notando che  $m = -3$  e  $n = 1$  funzionano. Se moltiplichiamo entrambi i lati per 5 otteniamo  $5 = (5m) \cdot 4 + (5n) \cdot 13$  cioè

$$(-15) \cdot 4 + (5) \cdot 13 = 5.$$

Quindi una soluzione particolare di  $4x + 13y = 5$  è  $(x_0, y_0) = (-15, 5)$ . Il teorema ci dice che tutte le soluzioni sono (dove  $a = 4$  e  $b = 13$ ):

$$x = x_0 + kb = -15 + k13, \quad y = y_0 - ka = 5 - k4, \quad k \in \mathbb{Z}.$$

cioé  $x = -15 + 13k$  e  $y = 5 - 4k$  al variare di  $k \in \mathbb{Z}$ .

## Esercizio (Indovinello delle taniche e dei galloni di Die Hard)

*Abbiamo una tanica da 5 galloni, una da 3 galloni ed una fontana.*

*E' possibile riempire la prima tanica con esattamente 4 galloni?*

*NB: 1 gallone americano = 3,785411784 litri.*

## Soluzione

*Indichiamo con*

- $x$  il numero di volte in cui riempiamo la tanica da 5 galloni (da vuota),*
- $y$  il numero di volte in cui riempiamo la tanica da 3 galloni (da vuota).*

*Si tratta allora di risolvere l'equazione  $5x + 3y = 4$ . Visto che  $\text{MCD}(5, 3) = 1$ , l'equazione si può risolvere. Dobbiamo ricavare l'identità di Bézout  $1 = m \cdot 5 + n \cdot 3$ . Ad occhio si vede che  $m = -1, n = 2$  funziona. Moltiplicando per 4 otteniamo  $4 = 4m \cdot 5 + 4n \cdot 3$  e quindi una soluzione particolare è  $(x_0, y_0) = (4m, 4n) = (-4, 8)$ . Il teorema ci dice che le soluzioni possibili sono  $x = x_0 + kb, y = y_0 - ka, k \in \mathbb{Z}$  cioè*

$$x = -4 + 3k, \quad y = 8 - 5k, \quad k \in \mathbb{Z}.$$

## Esercizio

*Un contadino vuole comprare degli animali per un totale di €50. Se gli animali sono conigli e galline per un costo rispettivo di €20 e €6, quanti di ogni tipo potrà acquistarne?*

SOLUZIONE. Sia  $x$  il numero di conigli e  $y$  il numero di galline. Dobbiamo allora risolvere l'equazione  $20x + 6y = 50$ . Dato che  $\text{MCD}(20, 6) = 2 \mid 50$ , questa ha soluzioni in  $\mathbb{Z} \times \mathbb{Z}$ . Semplificando otteniamo  $10x + 3y = 25$ . Scriviamo l'identità di Bézout  $10m + 3n = 1$ . Ad occhio  $m = 1, n = -3$  funzionano. Moltiplicando per 25 otteniamo  $10(25m) + 3(25n) = 25$  e quindi una soluzione particolare è  $(x_0, y_0) = (25m, 25n) = (25, -75)$ . Le altre soluzioni sono  $x = x_0 + kb, y = y_0 - ka, k \in \mathbb{Z}$  cioè

$$x = 25 + 3k, \quad y = -75 - 10k, \quad k \in \mathbb{Z}.$$

Notiamo però che  $x$  ed  $y$  sono numeri di animali e quindi si dovrà avere  $x \geq 0 \wedge y \geq 0$  cioè  $25 + 3k \geq 0 \wedge -75 - 10k \geq 0$  cioè  $-\frac{25}{3} \leq k \leq \frac{-75}{10}$ . Dato che  $-\frac{25}{3} \approx -8,3$ ,  $\frac{-75}{10} = -7,5$  e  $k \in \mathbb{Z}$ , l'unico possibile valore di  $k$  è  $-8$ . Pertanto otteniamo  $x = 25 + 3 \cdot (-8) = 1$  e  $y = -75 - 10 \cdot (-8) = 5$ .



## Esercizio

*In quanti modi un cassiere potrà dare €300 ad un cliente utilizzando solo banconote da 20 e 50 €? Quale sarà il numero minimo di banconote che potrà utilizzare?*

**SOLUZIONE.** Indichiamo con  $x$  il numero di banconote da €20 e con  $y$  il numero di banconote da €50. Dobbiamo risolvere l'equazione  $20x + 50y = 300$ . Dato che  $\text{MCD}(20, 50) = 10 \mid 300$ , questa ha soluzioni in  $\mathbb{Z} \times \mathbb{Z}$ . Semplificando otteniamo  $2x + 5y = 30$ . L'identità di Bézout si vede ad occhio:  $2 \cdot (-2) + 5 \cdot 1 = 1$ . Moltiplicando per 30 otteniamo  $2 \cdot (-60) + 5 \cdot 30 = 30$  e da cui la soluzione particolare  $(x_0, y_0) = (-60, 30)$ . Le soluzioni possibili sono dunque  $x = x_0 + kb, y = y_0 - ka, k \in \mathbb{Z}$  cioè

$$x = -60 + 5k, \quad y = 30 - 2k, \quad k \in \mathbb{Z}.$$

Essendo  $x$  ed  $y$  dei numeri di banconote, si avrà  $x \geq 0 \wedge y \geq 0$  cioè  $-60 + 5k \geq 0 \wedge 30 - 2k \geq 0$  cioè  $\frac{60}{5} \leq k \leq \frac{30}{2}$  vale a dire  $12 \leq k \leq 15$ . Dato che  $k \in \mathbb{Z}$ , i possibili valori di  $k$  sono 12, 13, 14, 15. Le corrispondenti soluzioni sono:  $(x, y) = (0, 6), (5, 4), (10, 2), (15, 0)$ . Pertanto il cassiere potrà consegnare le banconote in 4 modi.

Il numero totale di banconote utilizzate è

$$x + y = (-60 + 5k) + (30 - 2k) = -30 + 3k$$

che assume valore minimo quando  $k$  ha il minimo valore consentito, cioè per  $k = 12$ , nel qual caso  $x + y = 6$ .

### Esercizio (per casa)

*Risolvere in  $\mathbb{Z}$ , se possibile, le equazioni*

①  $15x + 20y = 35$ .

②  $15x + 21y = 35$ .

### Esercizio (per casa)

*In quanti modi è possibile ottenere un sacchetto del peso di 117 grammi, usando biglie da 27 e 21 grammi?*

*Qual'è il minimo ed il massimo numero di biglie utilizzabili?*