______14______

Equazioni diofantee

Un'equazione diofantea di primo grado è nella forma

$$ax + by = c, \tag{1}$$

con tutti i coefficienti interi, ossia $a, b, c \in \mathbb{Z}$. Sul piano cartesiano l'equazione (1) rappresenta una retta qualunque. Una soluzione per l'equazione diofantea è una coppia di valori entrambi *interi*, $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

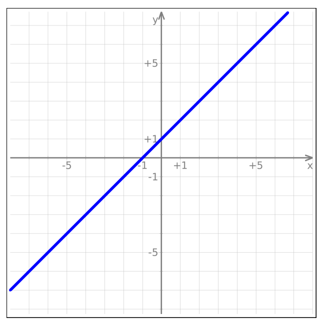

Figura 1: La retta $x - y = -1$. Si può notare come ad esempio $(-1, 0)$ e $(0, 1)$ siano soluzioni intere.

Proposizione. *L'equazione (1) ammette soluzione intera* $\iff$ *il Massimo Comune Divisore d di a e b divide c, $MCD(a, b) = d|c$.*

Dimostrazione. Parte 1, " $\Rightarrow$ *".*
Sia $(\bar{x}, \bar{y})$ una soluzione intera e sia $d = MCD(a, b)$. Per definizione di massimo comune divisore, d divide sia a che b e in particolare divide ogni combinazione lineare di a e b, compresa $a\bar{x} + b\bar{y}$; ma questa è proprio uguale a c, quindi d divide c. □

La seconda parte della dimostrazione è quella veramente utile che fornisce un metodo costruttivo per trovare le soluzioni:

Dimostrazione. Parte 2, " $\Leftarrow$ *"*
d, Massimo Comune Divisore fra a e b, divide c, quindi esiste un numero intero h tale che $dh = c$.
Poiché è sempre possibile scrivere il Massimo Comune Divisore fra due numeri come combinazione lineare di quei due numeri (*Identità di Bezout*), esistono α e β tali che

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

Allora

$$c = dh = (\alpha a + \beta b)\, h = \alpha h a + \beta h b.$$

L'ultima uguaglianza fornisce una soluzione,

$$(\bar{x}, \bar{y}) = (\alpha h, \beta h)\,.$$

□

La soluzione non è unica, ne esistono infinite che si ottengono aggiungendo a $(\bar{x}, \bar{y})$ una soluzione dell'equazione omogenea associata a (1), ossia

$$ax + by = 0,$$

che ha per soluzioni, per ogni $t \in \mathbb{Z}$,

$$\left(-\frac{b}{d}t, \frac{a}{d}t\right) \in \mathbb{Z}^2$$

Per concludere Data un'equazione diofantea nella forma

$$ax + by = c,$$

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

di cui cerchiamo soluzione intera

$$(\bar{x}, \bar{y}) \in \mathbb{Z}^2,$$

possiamo controllare se il Massimo Comune Denominatore di a e b, indicato con d, divide c, ossia se

$$c = hd.$$

Se è vero, possiamo calcolare l'identità di Bezout (esistono vari algoritmi semplici per farlo)

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

e scrivere tutte le soluzioni del problema nella forma

$$(\bar{x}, \bar{y}) = \left(\alpha h - \frac{b}{d}t, \beta h + \frac{a}{d}t\right).$$

con t qualunque numero intero.

Un esempio Prendiamo l'equazione

$$3x + 2y = 2,$$

$$a = 3,\ b = 2,\ c = 2;$$

calcoliamo il Massimo Comune Divisore

$$d = MCD(a, b) = MCD(3, 2) = 1;$$

il coefficiente c è multiplo di d, infatti

$$\boldsymbol{c} = \boldsymbol{d} \cdot h \Rightarrow \mathbf{2} = \mathbf{1} \cdot 2 \Rightarrow h = 2;$$

si può scrivere quindi d come combinazione lineare di a e b (identità di Bezout),

$$\boldsymbol{d} = \alpha \boldsymbol{a} + \beta \boldsymbol{b} \Rightarrow \mathbf{1} = (1) \cdot \mathbf{3} + (-1) \cdot \mathbf{2} \Rightarrow \begin{array}{c} \alpha = 1 \\ \beta = -1 \end{array}.$$

In conclusione la soluzione si può scrivere come

$$(\bar{x}, \bar{y}) = \left(\alpha h - \frac{b}{d}t, \beta h + \frac{a}{d}t\right) = (2 - 2t, -2 + 3t)\,;$$

quindi $(2, -2)$ è una soluzione ($t = 0$), ma lo è anche $(0, 1)$ (quando $t = 1$), o $(4, -5)$ (quando $t = -1$)...

Ora in teoria sei in grado di risolvere l'enigma delle noci di cocco! Ti riporto l'equazione qui sotto:

$$4^5 N = 5^6 F + 5^6 - 4^6.$$

La soluzione è al numero **9**.