**Analisi indeterminata di primo grado in due variabili**

di Antonino Giambò

**1.** Nel piano, riferito ad un sistema di assi cartesiani ortogonali (Oxy), consideriamo la retta di equazione:

$$2\,x + 3\,y = 8\,.$$

La sua rappresentazione grafica (figura 1), ma anche una semplice verifica ordinaria, evidenziano che ad essa appartengono i seguenti punti, le cui coordinate sono numeri interi:

$$(4, 0),\quad (1, 2),\quad (-2, 4).$$

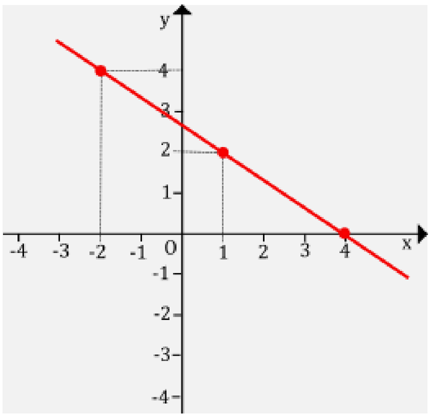


figura 1

Si pongono alcune domande:

- Esistono sulla retta altri punti le cui coordinate sono numeri interi?
- Ammesso che ne esistano altri, quanti sono complessivamente questi punti?
- Esistono formule idonee a determinare tali coordinate?

Quello di trovare le soluzioni espresse da numeri interi di un'equazione di primo grado in due variabili, come la seguente:

(1) $$a\,x + b\,y = c\,,$$

dove a, b, c sono numeri interi non nulli, e della quale l'equazione precedente è evidentemente un caso particolare, è un problema che rientra in una tipologia di problemi concernenti la cosiddetta **analisi indeterminata di primo grado**.

La risoluzione di un tale problema risale al matematico **Diofanto di Alessandria** (II-III sec. d.C.) ed è per questo che le equazioni del tipo (1) sono chiamate ***equazioni diofantee lineari*** e il loro studio rientra nella cosiddetta ***analisi diofantea***.

Diofanto ne tratta in un'opera dal titolo *Arithmetica*, che in origine doveva contenere 13 libri, ma di cui ci sono pervenuti solo i primi 6. Altri 4 libri, andati perduti nell'originale greco, sono stati ritrovati, ma in una traduzione araba, dal matematico egiziano Roshdi Rashed (n. 1936), che li ha pubblicati in francese nel 1984.

Bisogna dire che Diofanto non trova tutte le soluzioni dell'equazione (1) – considerata comunque non nella sua forma generale bensì per particolari valori dei coefficienti – ma si accontenta di trovarne una e a volte neanche intera ma razionale.

Bisogna dire inoltre che egli non fu il primo matematico ad occuparsi di quel tipo di equazioni. Erano infatti già presenti molti secoli prima nella matematica indiana. Precisamente, compaiono "equazioni diofantee" in un'opera dal titolo *Shulba Sutra*, composta in un periodo incerto collocabile tra il secolo IX e il secolo VI a.C. Se ne sarebbero occupati, tra gli altri, Baudhāyana (vissuto nel IX sec. a.C.) e Apastamba (vissuto del VII sec. a.C.).

Si tratta, tuttavia, di studi ancora parziali, sia nella matematica indiana sia in Diofanto.

In questo articolo intendo soffermarmi su uno dei metodi idonei a trovare una soluzione intera di una qualsiasi equazione diofantea lineare e a trovare le formule generali che ne forniscono tutte le soluzioni intere.

**2.** Diofanto, dunque, si accontentava di una sola soluzione e a volte neppure formata da valori interi. E riferita comunque ad un'equazione con coefficienti numerici e non letterali, e quindi a casi particolari.

Teniamo presente che il matematico alessandrino, pur disponendo di una sorta di simbolismo di sua invenzione, non disponeva però del nostro agile simbolismo algebrico.

Questo simbolismo permette a noi di studiare una generica equazione del tipo (1) e di ottenere facilmente non solo una singola soluzione razionale della stessa, ma le sue infinite *soluzioni razionali*.

Basta costatare che dalla (1), risolvendo rispetto ad y, si ottiene:

$$y = \frac{c - a\,x}{b}\,.$$

Per cui, le infinite soluzioni razionali dell'equazione sono le seguenti:

$$\left(x\,, \frac{c - a\,x}{b}\right),\ \ x \in \mathbb{Q}\,.$$

Diverso, e anche più complicato, è il problema della ricerca delle ***soluzioni intere*** dell'equazione, vale a dire le soluzioni espresse da coppie ordinate di numeri interi.

Certo, si può procedere per tentativi, che talora riescono, ma a volte sono infruttuosi e non approdano a nulla, poiché non ci sono soluzioni intere. Come accade, per esempio, con la seguente equazione, rappresentata in figura 2:

$$4\,x + 6\,y = 9\,.$$

Per quanti tentativi si facciano, sprecando naturalmente tempo ed energie, non si riesce a trovare una sua soluzione intera, proprio perché una tale soluzione non esiste.

Ma come si fa a saperlo in anticipo? Lo vedremo fra breve.

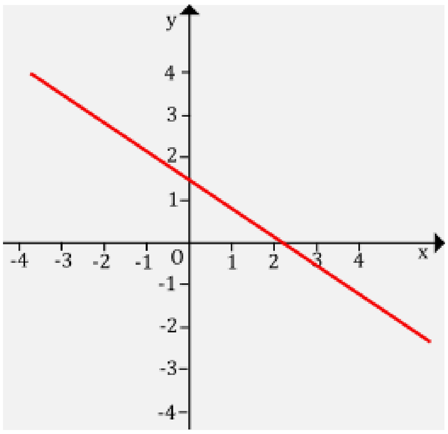


figura 2

Forse Diofanto ripiegava su una soluzione razionale proprio in situazioni come questa.

Ma, ritornando all'equazione (1), ribadiamo, come si fa a stabilire preventivamente se essa ammette una soluzione intera o se non l'ammette?

Questo né la matematica indiana né Diofanto furono in grado di farlo. Bisogna aspettare molti secoli prima che i matematici scoprissero criteri appositi. Esattamente bisogna aspettare l'opera dei matematici europei a partire dal secolo XVII e, in particolare, di Fermat [1], Eulero [2], Gauss [3], Lagrange [4].

Sembra, tuttavia, che già intorno all'anno 510 d.C. il matematico e astronomo indiano Aryabhata (476-550) abbia trovato un procedimento idoneo a risolvere l'equazione ax+by=c. Procedimento descritto nella sua opera principale, *Aryabhatiya*, che per la verità è l'unica sua opera che ci è pervenuta, ma è certo che egli ne ha scritte altre, andate perdute.

---

1 Pierre de Fermat, letterato e giurista francese, matematico per diletto, 1601-1665.
2 Leonhard Euler (italianizzato Leonardo Eulero), matematico svizzero, 1707-1783.
3 Car Friedrich Gauss, matematico tedesco, 1777-1855.
4 Giuseppe Luigi Lagrange, matematico italo-francese, 1736-1813.

Prima di occuparci di un criterio idoneo a stabilire se e quando un'equazione diofantea lineare ammette soluzioni intere, s'impone una precisazione: supporremo, senza che il problema perda di generalità, che i coefficienti a, b, c dell'equazione ax+by=c siano numeri primi fra loro. Giacché, se non lo fossero, basterebbe dividerli per il loro massimo comune divisore per ricondurci alla condizione che siano coprìmi.

CRITERIO (idoneo a stabilire se un'equazione diofantea lineare ammette soluzioni intere).

Considerata l'equazione:

$$a\,x + b\,y = c\,,$$

dove a, b, c sono numeri interi primi fra loro, condizione necessaria e sufficiente affinché ammetta una soluzione intera è che i numeri a, b siano primi far loro.

Prima di passare alla dimostrazione costatiamo che nella precedente equazione 4x+6y=9, dove a=4 e b=6, i numeri a, b non sono coprìmi ed è per questo che l'equazione non ha soluzioni intere. Per cui è inutile cercarne.

DIMOSTRAZIONE.

- Dimostriamo che *la condizione è necessaria*. Ovvero, ammesso che $(x_0, y_0)$ sia una soluzione intera dell'equazione, bisogna dimostrare che i numeri a, b sono primi fra loro.

Ragioniamo per assurdo. Se a, b non fossero coprìmi, ammetterebbero un massimo comune divisore d>1. Per cui esisterebbero due numeri interi a' e b' tali che risulti: a=a'd, b=b'd,. D'altro canto, dovendo essere $ax_0+by_0=c$, risulterebbe:

$$c = a'\,d\,x_0 + b'd\,y_0 \quad \text{ossia} \quad c = (a'\,x_0 + b'\,y_0)\,d\,.$$

Insomma, considerato che $a'\,x_0+b'\,y_0$ è certamente un numero intero, anche c sarebbe divisibile per d. Contro l'ipotesi che a, b, c siano numeri primi fra loro.

- Dimostriamo che *la condizione è sufficiente*. Ovvero, ammesso che i numeri a, b siano primi fra loro bisogna dimostrare che l'equazione ammette una soluzione intera.

Possiamo assumere che sia a>0, giacché in caso contrario basterebbe moltiplicare entrambi i membri dell'equazione per −1. Risolviamo l'equazione rispetto all'incognita x:

$$x = \frac{c - b\,y}{a}\,.$$

Attribuiamo adesso ad y gli a valori interi da 0 ad a−1. Otteniamo i seguenti a valori di x:

$$x_0 = \frac{c - b \cdot 0}{a}, \quad x_1 = \frac{c - b \cdot 1}{a}, \quad x_2 = \frac{c - b \cdot 2}{a}, \quad \dots\;, \quad x_{a.-1} = \frac{c - b \cdot (a-1)}{a}.$$

Indichiamo con $x_h$ ( $h = 0, 1, 2, \dots, a-1$ ) il generico di questi valori, ossia:

$$x_h = \frac{c - b\,h}{a}.$$

Indichiamo inoltre con $q_h$ ed $r_h$ il quoziente e il resto della divisione di c− bh per a. Si ha pertanto:

$$c - b\,h = a\,q_h + r_h \quad \text{e dunque:} \quad x_h = q_h + \frac{r_h}{a}\,.$$

Osserviamo adesso che i resti $r_h$ sono tutti diversi l'uno dagli altri. Se, infatti, ce ne fossero due uguali, mettiamo $r_m$ e $r_n$, sarebbe evidentemente:

$$x_m - x_n = q_m - q_n \quad \text{e anche:} \quad \frac{c - b\,m}{a} - \frac{c - b\,n}{a} = q_m - q_n \quad \text{da cui:} \quad \frac{b}{a}\,(n - m) = q_m - q_n.$$

Poiché il secondo membro dell'ultima uguaglianza è un numero intero, anche il primo deve esserlo. Questo, essendo a, b primi fra loro, accade solo se n − m è multiplo di a. Il che, dal momento che sia m sia n sono minori di a, può verificarsi solo se n − m=0. Ossia se $r_m$ e $r_n$ sono il medesimo resto.

I resti $r_h$ sono dunque tutti diversi fra loro. Considerato che sono in numero di a, sono esattamente i seguenti numeri, a parte l'ordine:

$$0,\; 1,\; 2,\; \dots\;,\; a-1.$$

Insomma, uno di tali resti è certamente uguale a 0. Supponiamo che sia uguale a 0 il resto $r_k$. Ricordando che c–b k=a $q_k$+$r_k$, si ha dunque;

$$c - b\,k = a\,q_k \quad \text{ossia} \quad a\,q_k + b\,k = c.$$

Questo significa che la coppia ordinata di numeri interi $(q_k, k)$ è una soluzione dell'equazione ax+by=c. [c.v.d.]

**3.** Proviamo in un caso particolare per mostrare non solo che l'equazione ammette una soluzione intera, ma anche per determinare la stessa. Sia allora l'equazione:

$$4\,x + 5\,y = 22\,,$$

nella quale evidentemente a=4, b=5.

Siccome i numeri 4 e 5 sono coprìmi, in virtù del criterio suddetto l'equazione ammette una soluzione intera. Proviamo a trovarla risolvendo l'equazione rispetto alla variabile x. Otteniamo:

$$x = \frac{22}{4} - \frac{5}{4}\,y\,.$$

Assegnando ad y i 4 valori 0, 1, 2, 3, ricaviamo i corrispondenti valori di x (tabella 1):

| y | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $x = \frac{22}{4} - \frac{5}{4}\,y$ | $\frac{22}{4}$ | $\frac{17}{4}$ | 3 | $\frac{7}{4}$ |

tabella 1

Dunque la coppia $(x{=}3, y{=}2)$ costituisce una soluzione intera dell'equazione.

Si capisce che questa modalità può andar bene se il coefficiente di x (o eventualmente, se è più comodo, quello di y) non è eccessivamente grande. In caso contrario la modalità potrebbe rivelarsi piuttosto noiosa, anche se potrebbe essere semplificata utilizzando uno strumento di calcolo automatico.

**4.** Esistono tuttavia altri metodi, non basati su tentativi, di ricerca della soluzione intera dell'equazione:

$$a\,x + b\,y = c\,,$$

dove a, b, c sono numeri coprìmi, una volta appurato ovviamente che essa ammette una tale soluzione, vale a dire dopo aver costatato che i numeri a, b sono coprìmi.

Uno di questi metodi è stato trovato da Eulero, un altro da Lagrange.

Noi ci limitiamo a descriverne uno basato sulle proprietà delle congruenze, argomento che, com'è noto, è stato creato e sviluppato da Gauss [(5)].

Ritorniamo allora sulla precedente relazione. Essa implica la seguente uguaglianza:

$$c - a\,x = b\,y\,.$$

Supponendo che y sia un numero intero, questo significa che ax e c sono numeri congrui rispetto al modulo b, ossia:

$$a\,x \equiv c \pmod{b}.$$

In particolare, ammesso che $(x_0, y_0)$ sia una soluzione intera dell'equazione – soluzione che, pur non sapendo ancora qual è, sappiamo tuttavia che esiste – si ha:

$$a\,x_0 \equiv c \pmod{b}.$$

D'altro canto, essendo a, b numeri coprìmi, in virtù del teorema di Fermat-Eulero risulta:

$$a^{\varphi(b)} \equiv 1 \pmod{b}\,,$$

dove $\varphi(b)$ indica, come si sa, il numero dei numeri minori di b e primi con esso.

Da quest'ultima relazione, ricordando una proprietà delle congruenze, segue:

$$c \cdot a \cdot a^{\varphi(b)-1} \equiv c \pmod{b}\,.$$

[5] Nelle righe seguenti si danno per acquisiti concetti in realtà già sviluppati in precedenti articoli pubblicati su questa stessa rubrica.

Dal confronto tra questa congruenza e la congruenza

$$a\,x_0 \equiv c \pmod{b},$$

segue:

$$x_0 = c \cdot a^{\varphi(b)-1}\,.$$

E quindi:

$$y_0 = \frac{c - a\,x_0}{b} = \frac{c - a \cdot c \cdot a^{\varphi(b)-1}}{b} = \frac{c}{b}\left(1 - a^{\varphi(b)}\right).$$

In definitiva, una soluzione intera dell'equazione è la seguente:

$$x_0 = c \cdot a^{\varphi(b)-1}, \qquad y_0 = \frac{c}{b}\left(1 - a^{\varphi(b)}\right).$$

Per esempio, riprendendo l'equazione $4x+5y=22$, dopo aver costatato che $a=4$, $b=5$, $c=22$ e che $\varphi(b)=\varphi(5)=4$, si ha:

$$x_0 = c \cdot a^{\varphi(b)-1} = 22 \cdot 4^3 = 1.408, \qquad y_0 = \frac{c}{b}\left(1 - a^{\varphi(b)}\right) = \frac{22}{5}\left(1 - 4^4\right) = -1.122\,.$$

Altro esempio, con riferimento all'equazione $4x+6y=26$. Siccome i suoi coefficienti non sono primi fra loro, li dividiamo per il loro massimo comune divisore, che è 2, e otteniamo l'equazione $2x+3y=13$. Osserviamo allora che $a=2$, $b=3$, $c=13$, per cui $\varphi(b)=\varphi(3)=2$. Una soluzione dell'equazione è pertanto la seguente:

$$x_0 = c \cdot a^{\varphi(b)-1} = 13 \cdot 2^1 = 26, \qquad y_0 = \frac{c}{b}\left(1 - a^{\varphi(b)}\right) = \frac{13}{3}\left(1 - 2^2\right) = -13\,.$$

**5.** Ammesso, a questo punto, di conoscere una soluzione intera dell'equazione:

$$a\,x + b\,y = c\,,$$

dove a, b, c sono numeri primi fra loro e, così pure, sono numeri primi fra loro anche i numeri a, b, siamo adesso in grado di dimostrare che l'equazione ammette infinite soluzioni intere e anche di trovare delle formule idonee ad ottenerle tutte.

Vediamo in che modo.

Sia dunque $(x_0, y_0)$ una soluzione intera dell'equazione, per cui si ha:

$$a\,x_0 + b\,y_0 = c\,.$$

Sottraendo membro a membro le due equazioni precedenti, si ha:

$$a\,(x - x_0) + b\,(y - y_0) = 0 \quad \text{o anche:} \quad a\,(x - x_0) = -b\,(y - y_0)\,.$$

Dall'ultima relazione si desume che il numero b divide $a(x - x_0)$. Per cui deve dividere almeno uno dei numeri a, $x - x_0$. Non potendo dividere a, con cui è primo, deve dividere $x - x_0$. Questo significa che esiste un intero k tale che:

$$x - x_0 = k\,b \quad \text{cioè} \quad x = x_0 + k\,b\,.$$

Di conseguenza, riprendendo la relazione $a\,(x - x_0) = -b\,(y - y_0)$, si ricava:

$$a\,k\,b = -b\,(y - y_0) \quad \text{da cui segue:} \quad y = y_0 - k\,a\,.$$

Ecco allora le formule cercate:

$$\mathbf{x = x_0 + k\,b}\,, \qquad \mathbf{y = y_0 - k\,a}\,,$$

dove k è un qualsiasi numero intero.

A conferma, possiamo verificare che effettivamente quelle trovate sono soluzioni dell'equazione. Di fatto:

$$a\,(x_0 + k\,b) + b\,(y_0 - k\,a) = a\,x_0 + b\,y_0 = c\,.$$

Questo dovrebbe assicurare che tutte le soluzioni intere dell'equazione in esame sono fornite dalle formule trovate. Se, ad ogni buon conto, si cerca una conferma di ciò, ossia che ogni soluzione intera $(\bar{x}, \bar{y})$ dell'equazione soddisfa alle formule, basta ripetere il ragionamento precedente mettendo $(\bar{x}, \bar{y})$ al posto di $(x, y)$. Si trova per l'appunto che, per un particolare valore $\bar{k}$ di k risulta:

$$\bar{x} = x_0 + \bar{k}\,b\,, \qquad \bar{y} = y_0 - \bar{k}\,a\,.$$

Per esempio, riprendendo ancora una volta l'equazione $4x+5y=22$, di cui abbiamo trovato la soluzione $(1.408, -1.122)$, tutte le sue soluzioni intere sono date dalle formule seguenti:

$$x = 1.408 + 5\,k, \qquad y = -1.122 - 4\,k\,.$$

A titolo di curiosità, si può costatare che per $k = -281$ si ritrova la soluzione $(3, 2)$ che abbiamo segnalato nell'incipit di questo articolo.

Invece per l'equazione $4x+6y=26$ bisogna riferirsi all'equazione equivalente $2x+3y=13$, della quale abbiamo trovato sopra la soluzione particolare $(26, -13)$. Di modo che tutte le soluzioni dell'equazione sono date dalle seguenti formule:

$$x = 26 + 3\,k, \qquad y = -13 - 2\,k\,.$$

Di fatto:

$$4\,x + 6\,y = 4\,(26 + 3k) + 6\,(-13 - 2k) = 4 \cdot 26 + 4 \cdot 3k - 6 \cdot 13 - 6 \cdot 2k = 26\,.$$

BIBLIOGRAFIA.

[1] Armando Chiellini – Roberto Giannarelli, *L'esame orale di matematica nei concorsi a cattedre di scuola secondarie*, Roma, Libreria Eredi Virgilio Veschi, 1962, pagg. 105-114.

[2] Richard Courant – Herbert Robbins, *Che cos'è la matematica*? Torino, Bollati Boringhieri, 2000 (II edizione), pagg. 90-92.

[3] Pierre de Fermat, *Osservazioni su Diofanto* (Nuova edizione a cura di Alberto Conte), Torino, Bollati Boringhieri, Ristampa 2017.

[4] Antonino Giambò – Roberto Giambò, *Matematica pre-universitaria, storia e didattica*, Bologna, Pitagora Editrice, 2005, pag. 143.

[5] Johan Gómez I Urgellès, *Diofanto*, Milano, RBA Italia, 2018.