Equazioni diofantee

Alberto Abbondandolo

Forte dei Marmi, 17 Ottobre 2006

Un'equazione diofantea è un'equazione algebrica a coefficienti *interi* in una o più indeterminate di cui si cercano soluzioni *intere*.

1 Equazioni diofantee di primo grado

Consideriamo l'equazione

$$132\,x + 51\,y = 7. \tag{1}$$

Sappiamo che il luogo dei punti di coordinate x e y descritto da questa equazione è una retta. Questa equazione possiede soluzioni x, y intere? In altre parole, sulla retta di cui sopra esistono punti che abbiano entrambe le coordinate intere?

No. Infatti tanto 132 quanto 51 sono divisibili per 3, quindi il membro sinistro dell'equazione è divisibile per 3, per ogni valiore intero di x e y. Invece a destra troviamo 7, che non è divisibile per 3.

Più in generale, consideriamo l'equazione diofantea

$$ax + by = c, \tag{2}$$

con a, b, c numeri interi. Un'equazione di questa forma si dice di *primo grado*. Se questa equazione possiede soluzioni, ogni numero d che divida[1] sia a che b deve dividere anche c. In particolare, questo deve valere per il più grande tra i divisori comuni di a e b, cioè per il loro *massimo comun divisore*, che si indica generalmente con (a, b). Abbiamo quindi scoperto che *affinché l'equazione (2) abbia soluzione, è necessario che c sia un multiplo di (a, b).*

Modifichiamo l'equazione (1) affinché possa avere soluzioni. Consideriamo ad esempio

$$132\,x + 51\,y = 6. \tag{3}$$

Dato che $(132, 51) = 3$ e 6 è un multiplo di 3, questa equazione può avere soluzioni. Per vedere se effettivamente ne ha, è utile il seguente:

Teorema di Bézout. *Se a, b sono interi e (a, b) è il loro massimo comun divisore, allora esistono interi h, k tali che*

$$ha + kb = (a, b).$$

Il Teorema di Bézout ci assicura che esistono interi h, k tali che

$$132\,h + 51\,k = 3,$$

e moltiplicando questa equazione per 2 troviamo che $x = 2h$ e $y = 2k$ costituiscono una soluzione di (3). Il problema si riduce quindi a dimostrare il teorema di Bézout, con una dimostrazione *costruttiva* che ci fornisca un metodo per calcolare h e k. Tale dimostrazione si basa sull'*Algoritmo di Euclide*, che andiamo a descivere.

[1] Si dice che un numero d divide a se a è un multiplo intero di d, in formula $a = qd$ con q intero.

L'Algoritmo di Euclide. L'algoritmo di Euclide è una procedura algebrica che, dati due interi positivi a, b, determina il loro massimo comun divisore (a, b). Si basa sulla divisione con resto di numeri interi. Vediamo come funziona questo algoritmo nel caso che ci interessa, cioè per gli interi $a = 132$ e $b = 51$. Iniziamo con lo scrivere la divisione con resto del più grande tra i due per il più piccolo: il 51 nel 132 ci sta 2 volte e resta 30, in formula:

$$132 = 2 \cdot 51 + 30.$$

Nel caso generale (supponendo a maggiore di b), avremmo scritto

$$a = q \cdot b + r,$$

dove q è il quoziente della divisione, ed r il resto, ossia un intero compreso tra 0 e $b - 1$. L'identità appena scritta mostra che se un intero d divide sia a che b, deve dividere anche r (infatti $r = a - q \cdot b$). Analogamente, se un intero d divide sia b che r, deve dividere anche a. Quindi un numero è divisore comune di a e b se e solamente se è divisore comune di b e r. Applicando questo ragionamento al più grande dei edivisori comuni, deduciamo che $(a, b) = (b, r)$, quindi ci siamo ricondotti a trovare il massimo comun divisore tra b ed r, operazione più semplice, visto che si tratta di due numeri più piccoli dei precedenti. Inoltre l'argomento si può iterare, con b, r al posto di a, b.

Nel nostro caso, abbiamo che $(132, 51) = (51, 30)$, e ripetendo la divisione con resto con questi nuovi numeri troviamo,

$$51 = 1 \cdot 30 + 21,$$

e proseguendo alla stessa maniera

$$30 = 1 \cdot 21 + 9,$$

quindi

$$21 = 2 \cdot 9 + 3,$$

fino a

$$9 = 3 \cdot 3.$$

Quando si trova una divisione senza resto l'algoritmo è concluso. Si noti che nelle divisioni successive i resti diminuiscono, quindi prima o poi deve comparire il resto 0. Dalle considerazioni fatte sopra sappiamo che

$$(132, 51) = (51, 30) = (30, 21) = (21, 9) = (9, 3) = (3, 0) = 3,$$

quindi il massimo comun divisore tra 132 e 51 è 3, ossia l'ultimo resto non nullo generato dall'algoritmo di Euclide. Il massimo comun divisore di 132 e 51 si può ovviamente trovare anche fattorizzando i due numeri. Nel caso di numeri molto grandi però la fattorizzazione è molto difficile (sostanzialmente bisogna provare a dividere il numero da fattorizzare per tutti i numeri primi minori della sua radice quadrata), mentre l'algoritmo di Euclide è piuttosto veloce. Chi ha una minima esperienza di programmazione non avrà difficoltà a scrivere un programma che prenda come input due interi, applichi loro l'algoritmo di Euclide, e produca come output il loro massimo comun divisore.

Qua l'algoritmo di Euclide ci interessa non tanto come modo per determinare il massimo comun divisore, ma perchè rileggendo i suoi passaggi al contrario è possibile risalire agli interi h e k del Teorema di Bézout. Riscriviamo di seguito i passaggi dell'algoritmo, tralasciando l'ultimo:

$$\begin{array}{rll} (E1) & 132 & = 2 \cdot 51 + 30 \\ (E2) & 51 & = 1 \cdot 30 + 21 \\ (E3) & 30 & = 1 \cdot 21 + 9 \\ (E4) & 21 & = 2 \cdot 9 + 3. \end{array}$$

Il nostro scopo è scrivere 3 come *combinazione intera di 132 e 51* ossia come somma dei numeri 132 e 51 moltiplicati per oopurtuni coefficienti interi. Dalla quarta equazione possiamo scrivere 3 come combinazione intera di 21 e 9. Della terza possiavo ricavare 9 come combinazione intera di 30 e 21. Mettendo assieme queste due cose, troviamo 3 come combinazione intera di 30 e 21. Proseguendo allo stesso modo, otterremo 3 come combinzione intera di 51 e 30 (dalla seconda equazione), ed infine di 132 e 51 (dalla prima equazione), che è quello a cui vogliamo arrivare. Vediamo i passaggi (sopra ad alcune delle uguaglianze è indicata la riga dell'algoritmo di Euclide utilizzata, negli altri passaggi si è solamente raccolto a fattore comune):

$$\begin{aligned} 3 &\overset{(E4)}{=} 21 - 2 \cdot 9 \overset{(E3)}{=} 21 - 2 \cdot (30 - 21) = -2 \cdot 30 + 3 \cdot 21 \overset{(E2)}{=} -2 \cdot 30 + 3 \cdot (51 - 30) \\ &= 3 \cdot 51 - 5 \cdot 30 \overset{(E1)}{=} 3 \cdot 51 - 5 \cdot (132 - 2 \cdot 51) = -5 \cdot 132 + 13 \cdot 51. \end{aligned}$$

In conclusione,

$$3 = -5 \cdot 132 + 13 \cdot 51, \tag{4}$$

quindi in questo caso i coefficienti di Bézout sono $h = -5$ e $k = 13$. Con un po' di esperienza matematica, i passaggi che abbiamo visto in questo caso particolare possono essere trasformati in una dimostrazione del Teorema di Bézout.

Soluzione generale. Moltiplicando per 2 l'uguaglianza (4) fornita dal Teorema di Bézout, troviamo che

$$\bar{x} = -10, \quad \bar{y} = 26$$

è una soluzione dell'equazione (3). Vogliamo adesso capire se ve ne sono altre, ed in questo caso determinarle. Se facciamo la sostituzione

$$x = \bar{x} + x' = -10 + x', \quad y = \bar{y} + y' = 26 + y',$$

il primo membro dell'equazione (3) diventa

$$132x + 51y = 132(\bar{x} + x') + 51(\bar{y} + y') = 132\bar{x} + 51\bar{y} + 132x' + 51y' = 6 + 132x' + 51y',$$

dove abbiamo usato il fatto che $\bar{x}, \bar{y}$ è una soluzione. Questa espressione deve essere uguale a 6, quindi troviamo che le nuove incognite x', y' devono risolvere l'equazione

$$132\,x' + 51\,y' = 0.$$

Il fatto che a destra ci sia lo zero rende semplice determinare le soluzioni intere di questa equazione. Infatti possiamo ricavare la y' in funzione della x' come

$$y' = -\frac{132}{51}x' = -\frac{44}{17}x',$$

dove abbiamo ridotto la frazione in modo da avere numeratore e denominatore primi tra loro. Il fatto che 44 e 17 siano primi tra loro implica che y' è un intero se e solamente se x' è un multiplo di 17 (questo è l'unico modo per semplificare il denominatore). Quindi $x' = 17n$, dove n è un intero arbitrario, da cui ricaviamo $y' = -44n$. Concludiamo che le soluzioni di (3) sono esattamente le coppie x, y della forma

$$x = -10 + 17n, \quad y = 26 - 44n,$$

al variare di n fra tutti gli interi. Geometricamente, si tratta dei punti sulla retta di equazione $132x+51y = 6$ ottenuti partendo dal punto $(-10, 26)$ e facendo n passi di lunghezza 17 verso destra (rispettivamente, verso sinistra) ed n passi di lunghezza 44 verso il basso (rispettivamente, verso l'alto).

Riassumiamo quel che abbiamo imparato sulle equazioni diofantee di primo grado. L'equazione diofantea di primo grado

$$ax + by = c, \tag{5}$$

con a, b, c interi, possiede soluzioni se e solamente se c è un multiplo di (a, b). In questo caso, posto $c = (a, b) \cdot q$, si usa l'algoritmo di Euclide per trovare le soluzioni h, k di

$$ha + kb = (a, b),$$

e si ha che $\bar{x} = qh$, $\bar{y} = qk$ è una soluzione particolare di (5). Tutte le soluzioni sono date dalla formula

$$x = \bar{x} + \frac{b}{(a,b)}n, \quad y = \bar{y} - \frac{a}{(a,b)}n,$$

al variare di n tra tutti gli interi.

Esercizio 1 *Risolvere, se è possibile, le seguenti equazioni diofantee*

$$3x + 6y = 22, \quad 7x + 11y = 13, \quad 3x - 4y = 29, \quad 11x + 12y = 58,$$
$$153x - 34y = 51, \quad 3x + 12y - 9z = 5, \quad 3x + 12y - 9z = 15, \quad x + 2y + 3z = 4.$$

2 Equazioni diofantee di secondo grado

Eliminazione di una incognita. Consideriamo l'equazione diofantea

$$3x^2 + xy - 2x + 5y + 7 = 0. \tag{6}$$

Si tratta di un'equazione di secondo grado, ma di tipo particolare, in quanto l'incognita y compare soltanto al primo grado. Quindi possiamo ricavare la y in funzione della x mediante una formula che non faccia comparire radici (come accadrebbe se l'equazione fosse di secondo grado in y). Raccogliendo si ha

$$(x+5)y = -3x^2 + 2x - 7,$$

da cui

$$y = -\frac{3x^2 - 2x + 7}{x+5}. \tag{7}$$

Per avere il membro destro in una forma più maneggevole, eseguiamo la divisione con resto del polinomio al numeratore per quello al denominatore

$$\begin{array}{ccc|c}
3x^2 & -2x & +7 & \underline{x+5} \\
-3x^2 & -15x & & 3x-17 \\
 & -17x & +7 & \\
 & 17x & +85 & \\
 & & 92 &
\end{array}$$

quindi

$$3x^2 - 2x + 7 = (3x-17)(x+5) + 92.$$

Dalla (7) ricaviamo quindi

$$y = -\frac{(3x-17)(x+5)+92}{x+5} = -\frac{(3x-17)(x+5)}{x+5} - \frac{92}{x+5} = -3x + 17 - \frac{92}{x+5},$$

ossia

$$y = -3x + 17 - \frac{92}{x+5}. \tag{8}$$

Dato che x è un intero, l'espressione sopra fornisce un valore intero per y se e solamente se $x+5$ divide 92. Determiniamo tutti i divisori di 92. Dato che $92 = 2 \cdot 2 \cdot 23$, i divisori di 92 sono

$$\pm 1, \ \pm 2, \ \pm 23, \ \pm 4, \ \pm 46, \ \pm 92.$$

Perciò $x+5$ deve assumere uno dei 12 valori elencati sopra, da cui x deve assumere uno dei 12 valori seguenti

$$-6, \ -4 \ -7, \ -3, \ -28, \ 18, \ -9, \ -1, \ -51, \ 41, \ -97, \ 87.$$

Possiamo infine ricavare la y dalla (8) e concludere che l'equazione (6) ha esattamente 12 soluzioni, ossia

$$\begin{array}{llllll} x=-6, & x=-4, & x=-7, & x=-3, & x=-28, & x=18, \\ y=127, & y=-63, & y=84, & y=-20, & y=105, & y=-41, \end{array}$$

$$\begin{array}{llllll} x=-9, & x=-1, & x=-51, & x=41, & x=-97, & x=92, \\ y=67, & y=-3, & y=172, & y=-108, & y=309, & y=-260. \end{array}$$

Esercizio 2 *Trovare le soluzioni intere delle equazioni diofantee*

$$2x^2 - xy - 9x + 5y + 2001 = 0, \quad y^2 - xy + 5x + 1 = 0, \quad (x+1)(y+1) = 2xy.$$

Punti razionali su una conica. Il luogo di zeri di un polinomio di secondo grado nelle variabili x, y si chiama *conica.* Vi sono casi degeneri in cui la conica è vuota (ad esempio $x^2 + y^2 = -1$) o si riduce ad un solo punto (ad esempio $x^2 + y^2 = 0$), o è una retta (ad esempio $x^2 = 0$), o l'unione di due rette (ad esempio $xy = 0$). Negli altri casi, otteniamo un'*iperbole*, una *parabola*, oppure un'*ellisse* (se i suoi assi sono uguali, si tratta di un cerchio). Ad esempio, il luogo dei punti descritto dall'equazione (6) è un'iperbole, come mostra la formula (8).

Consideriamo la conica più familiare di tutte, ossia il cerchio di centro $(0, 0)$ e raggio 1, che è descritto dall'equazione

$$x^2 + y^2 = 1. \tag{9}$$

Le soluzioni intere di questa equazione sono ovviamente soltanto le coppie $(1, 0)$, $(0, 1)$, $(-1, 0)$, $(0, -1)$. Vogliamo determinare tutte le soluzioni *razionali* di (9), ossia l'insieme dei punti (x, y) sul cerchio che hanno per ascissa x e per ordinata y due numeri razionali, cioè due frazioni.

Possiamo procedere nel modo seguente. Fissiamo un punto razionale sul cerchio, ad esempio $(-1, 0)$. Tracciamo la retta per questo punto di coefficiente angolare t. Questa retta intersecherà il cerchio in un secondo punto (x, y) (oltre a $(-1, 0)$). Affermiamo che se t è un numero razionale, allora (x, y) ha coordinate razionali. Infatti, come vedremo tra un attimo, l'ascissa di questo secondo punto di intersezione è soluzione di un polinomio di secondo grado i cui coefficienti sono razionali (dipendono dai coefficienti dell'equazione (9) e da t). In generale, un polinomio di secondo grado con coefficienti razionali non ha radici razionali (nella formula risolutiva compare una radice quadrata). In questo caso però sappiamo che $x = -1$ è soluzione (poiché $(-1, 0)$ è un'intersezione). Per il Teorema di Ruffini, il polinomio in questione è divisibile per $x + 1$. Effettuando la divisione tra polinomi a coefficienti razionali si ottiene un polinomio a coefficienti razionali. Ci si riduce quindi ad un polinomio di grado uno a coefficienti razionali, che pertanto ha una radice razionale.

D'altra parte, tutti i punti razionali sul cerchio si trovano in questo modo. Infatti, se (x, y) è un punto razionale sul cerchio diverso da $(-1, 0)$, allora la retta passante per $(-1, 0)$ e per (x, y) ha coefficiente angolare $y/(x + 1)$, che è un numero razionale.

Questo ragionamento ha validità generale: se C è una conica, tutti punti razionali su C si trovano fissando un qualunque punto razionale P ed individuando le seconde intersezioni di C con una qualunque retta passante per P ed avente coefficiente angolare razionale.

Vediamo di attuare quanto detto nel caso dell'equazione (9), avendo fissato il punto $(-1, 0)$. Si tratta di trovare le soluzioni del sistema

$$\begin{cases} x^2 + y^2 = 1, \\ y = t(x + 1). \end{cases} \tag{10}$$

Sostutuendo l'espressione per y dalla seconda equazione nella prima otteniamo

$$x^2 + t^2(x + 1)^2 = 1,$$

ossia

$$(1 + t^2)x^2 + 2t^2 x + t^2 - 1 = 0. \tag{11}$$

Sappiamo già che $x = -1$ è soluzione di questa equazione, quindi il polinomio sopra è divisibile per $x + 1$. Infatti,

$$(1 + t^2)x^2 + 2t^2 x + t^2 - 1 = (x + 1)((1 + t^2)x + t^2 - 1).$$

Perciò l'altra soluzione di (11) è soluzione di

$$(1+t^2)x + t^2 - 1 = 0,$$

cioè

$$x = \frac{1-t^2}{1+t^2}.$$

Sostituendo questo valore di x nella seconda equazione di (10), troviamo

$$y = \frac{2t}{1+t^2}.$$

Concludiamo che tutte i punti razionali sul cerchio sono quelli della forma

$$(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right), \tag{12}$$

al variare di t tra tutti i numeri razionali. Si osservi che questa è la parametrizzazione del cerchio che si trova associando ad un punto P sul cerchio il numero $t = \tan(\theta/2)$, dove θ è l'angolo $\widehat{AOP}$, con $A = (1,0)$.

Esercizio 3 *Determinare i punti razionali sull'iperbole di equazione*

$$x^2 - y^2 = 1,$$

e sull'ellisse di equazione

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

dove a, b sono numeri razionali non nulli.

Terne pitagoriche. Una delle equazioni diofantee più famose è

$$a^2 + b^2 = c^2, \tag{13}$$

come equazione nelle incognite a, b, c. Per il Teorema di Pitagora, le soluzioni intere e positive di questa equazione sono le terne (a, b, c) per cui esiste un triangolo rettangolo di cateti a, b e di ipotenusa c. Per questo motivo, tali terne si dicono *terne pitagoriche*: corrispondono ai triangolo rettangoli con tutti i tre lati interi. Mostriamo come la conoscenza dei punti razionali sul cerchio permetta di determinare tutte le possibili terne Pitagoriche.

Iniziamo con l'osservare che se (a, b, c) è una terna pitagorica con un fattore comune d, allora la terna $(a/d, b/d, c/d)$ è ancora pitagorica. Quindi è sufficiente determinare tutte le terne pitagoriche *primitive*, ossia quelle per cui il massimo comun divisore tra a, b, c è 1: tutte le altre si otterranno moltiplicando i tre numeri di una terna primitiva per lo stesso intero positivo. Se poniamo

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

e dividiamo l'equazione (13) per c^2, troviamo l'equazione

$$x^2 + y^2 = 1.$$

Ci interessano quindi le soluzioni razionali di questa equazione, che per quanto visto prima sono date dalla formula (12). Scrivendo il numero razionale t in (12) come $t = m/n$, con m, n interi primi tra loro, otteniamo

$$x = \frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2}, \quad y = \frac{b}{c} = \frac{2mn}{n^2 + m^2}. \tag{14}$$

Sia p un numero primo diverso da 2 che divide sia $2mn$ che n^2+m^2. Dato che $p \neq 2$ divide $2mn$, necessariamente divide almeno uno tra m e n. Ma dovendo dividere anche n^2+m^2, divide anche il quadrato dell'altro, e quindi l'altro. Questo contraddice il fatto che m, n fossere primi tra loro. Quindi i numeri $2mn$ e m^2+n^2 hanno al più il fattore 2 in comune, e questo avviene se e solamente se n ed m sono entrambi dispari (non possono essere entrambi pari, essendo primi tra loro). Consideriamo il caso in cui m e n abbiano parità diversa. Allora se (a, b, c) è un terna di interi positivi con massimo comun divisore uno che verifica (14), necessariamente

$$a = n^2 - m^2, \quad b = 2mn, \quad c = n^2 + m^2.$$

Se invece n e m sono entrambi dispari, (14) implica

$$a = \frac{n^2 - m^2}{2}, \quad b = mn, \quad c = \frac{n^2 + m^2}{2}.$$

Ma essendo numeri dispari, $n = 2k+1$ e $m = 2h-1$, da cui

$$a = 2(k+h)(k-h+1), \quad b = (k+h)^2 - (k-h+1)^2, \quad c = (k+h)^2 + (k-h+1)^2.$$

Dato che $k+h$ e $k-h+1$ hanno parità diversa, questo caso si riduce al precedente, ma si è scambiato a con b. Concludiamo che le terne pitagoriche (a, b, c) con massimo comun divisore 1 sono tutte e sole le terne

$$a = n^2 - m^2, \quad b = 2mn, \quad c = n^2 + m^2,$$

con $n > m$ interi positivi primi tra loro, di parità diversa, e le terne ottenute scambiando a con b.

Esercizio 4 (impegnativo) *Dimostrare che l'equazione*

$$x^4 + y^4 = z^4$$

non ha soluzioni intere diverse da $x = y = z = 0$.

3 Per saperne di più

Un'eccellente libro per approfondire la consoscenza della matematica elementare, ma non solo, è il classico

Richard Courant, Herbert Robbins, *Che cos'è la matematica?*, Bollati Boringhieri, 2000.

Per prepararsi alle gare di matematica a qualsiasi livello, uno strumento molto utile è il volumetto

Massimo Gobbino, *Schede olimpiche*, Edizioni Cremonese, 2005.

Questi appunti si basano sulle *Schede olimpiche* N11, N12 e N13. Nelle *Schede olimpiche* si trova anche un ricco elenco di siti internet dove trovare problemi ed altro materiale.