3. Equazioni diofantee

Consideriamo il seguente problema: una persona vuol acquistare dei biglietti gratta e vinci per una spesa complessiva di 100 euro. Può acquistare solamente biglietti da 5 euro o da 10 euro. Quanti biglietti dell'uno o dell'altro tipo può prendere per arrivare alla soglia dei 100 euro? Se indichiamo con x il numero di biglietti da 5 euro e con y il numero di biglietti da 10 euro, il problema equivale a risolvere l'equazione $5x + 10y = 100$ e trovare le soluzioni intere non negative.
Quella appena scritta è un esempio di *equazione diofantea*, cioè un'equazione della quale si cercano le **soluzioni intere**, se esistono.
Altri esempi di equazioni diofantee sono di seguito riportati.

❶ $z^2 = (x^2 - 1)(y^2 - 1) + 1981$ con $x, y, z \in \mathbb{Z}$ (*IMO Jury 1981*);

❷ $x^n + y^n = z^n$ con $x, y, z \in \mathbb{Z}$, $n \geq 3$ intero (*Ultimo Teorema di Fermat*);

❸ $x^2 + y^2 + z^2 = x^3 + y^3 + z^3$ con $x, y, z \in \mathbb{Z}$ (*MMO 1994*);

❹ $a^3 + b^3 = 9$ con $a, b \in \mathbb{Z}$ (*British Mathematical Olympiad 1987A*);

❺ $p^2 + q^2 = pqn + 1$ con p, q primi, $n \in \mathbb{Z}^+$ (*Olimpiadi della Matematica, Provinciali 2010*).

Tali equazioni devono il loro nome al matematico greco *Diofanto* (250 d.C. circa) che per primo analizzò una equazione le cui soluzioni erano ristrette ai numeri razionali.

Potremmo presentare innumerevoli altri esempi di equazioni diofantee, ma ciò che le accomuna è la mancanza, in generale, di metodi risolutivi standard.

3.1 Equazioni diofantee lineari

Presentiamo, adesso, le idee chiave che permettono di risolvere le equazioni diofantee lineari in due variabili, cominciando dalla seguente definizione.

Definizione 3.1.1. Si definisce **equazione diofantea lineare** nelle incognite x e y, ogni equazione del tipo

$$ax + by = c$$

con $a, b, c \in \mathbb{Z}$, di cui si vogliono determinare le soluzioni intere.

Dal punto di vista geometrico, risolvere l'equazione diofantea $ax + by = c$ equivale a determinare i punti del piano cartesiano a coordinate intere appartenenti alla retta di equazione $ax + by = c$, come mostrato nel seguente grafico.

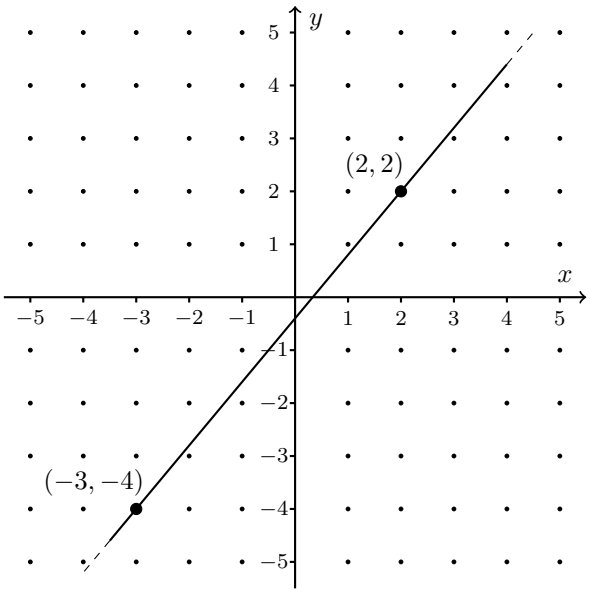

Figura 3.1: alcune soluzioni della diofantea $6x - 5y = 2$.

Un'equazione del tipo precedente, essendo a coefficienti ed incognite intere, può avere oppure non avere soluzioni; in ogni caso, se ha una soluzione ne possiede infinite. Vedremo adesso un criterio che permette di stabilire quando una diofantea lineare possiede oppure no soluzioni e, in caso positivo, come costruirle.

Proposizione 3.1.2. *L'equazione diofantea $ax + by = c$ ammette soluzioni se e solo se (a, b) è un divisore di c. In particolare, se a e b sono primi tra loro, l'equazione ammette sempre soluzioni.*

Dimostrazione. Poniamo $d = (a, b)$ e supponiamo che $(\overline{x}, \overline{y})$ sia una soluzione dell'equazione data, cioè che $a\overline{x} + b\overline{y} = c$. Poiché $d \mid a$ e $d \mid b$, si ha che $d \mid (a\overline{x} + b\overline{y})$ e quindi $d \mid c$.
Viceversa, supponiamo che $d \mid c$ e dimostriamo che l'equazione ammette soluzioni intere. Essendo d un divisore di c, esiste $u \in \mathbb{Z}$ tale che $c = du$. Inoltre, per il teorema di Bézout, si ha che $d = ah + bk$ per qualche $h, k \in \mathbb{Z}$. Moltiplicando ambo i membri di quest'ultima uguaglianza per u, si ottiene $du = ahu + bku$, cioè $c = a(hu) + b(ku)$, e quindi la coppia (hu, ku) è una soluzione dell'equazione. □

Ad esempio, hanno soluzioni le equazioni $3x + 5y = 2$ (una soluzione è data dalla coppia $(-1, 1)$) e $8x + 6y = 14$ (una soluzione è la coppia $(7, -7)$).
Non ha invece soluzioni l'equazione $6x - 9y = 7$ in quanto $(6, 9) = 3$ non è un divisore di 7.

La proposizione precedente pone le condizioni per l'esistenza o meno delle soluzioni di una diofantea lineare in due incognite, ma non dice come determinare tutte le soluzioni qualora ne esista una. La proposizione seguente mostra come determinarle tutte[1].

Proposizione 3.1.3. *Sia $ax + by = c$ una equazione diofantea tale che $d = (a, b)$ sia un divisore di c. Detta $(\overline{x}, \overline{y})$ una soluzione particolare dell'equazione, tutte e sole le infinite soluzioni sono date dalle coppie (x, y) con*

$$x = \overline{x} + k \cdot \frac{b}{d}, \qquad y = \overline{y} - k \cdot \frac{a}{d}$$

al variare di $k \in \mathbb{Z}$ ed essendo le coppie $\left(k \cdot \frac{b}{d}, -k \cdot \frac{a}{d}\right)$ tutte e sole le soluzioni dell'omogenea associata $ax + by = 0$.

Dimostrazione. Sia $(\overline{x}, \overline{y})$ una fissata soluzione dell'equazione $ax + by = c$. È facile verificare che la coppia $\left(\overline{x} + k \cdot \frac{b}{d}, \overline{y} - k \cdot \frac{a}{d}\right)$ è ancora una soluzione dell'equazione al variare di $k \in \mathbb{Z}$. Infatti, sostituendo nell'equazione si ottiene $a\overline{x} + ak \cdot \frac{b}{d} + b\overline{y} - bk \cdot \frac{a}{d} = a\overline{x} + b\overline{y} = c$, dove l'ultima uguaglianza è giustificata dal fatto che

[1] Il primo matematico a descrivere un metodo risolutivo delle equazioni lineari fu l'indiano *Brahmagupta* nel settimo secolo d. C.

$\left(k \cdot \frac{b}{d}, -k \cdot \frac{a}{d}\right)$ è soluzione dell'omogenea associata e quindi $ak \cdot \frac{b}{d} - bk \cdot \frac{a}{d} = 0$.
Viceversa, sia (x', y') una soluzione dell'equazione assegnata. Si ha quindi $ax' + by' = c = a\overline{x} + b\overline{y}$, cioè $a(x' - \overline{x}) = b(\overline{y} - y')$, da cui $\frac{a}{d}(x' - \overline{x}) = \frac{b}{d}(\overline{y} - y')$. Essendo $\frac{b}{d}$ e $\frac{a}{d}$ coprimi, da ciò segue che $\frac{b}{d}$ divide $(x' - \overline{x})$ e quindi esiste $k \in \mathbb{Z}$ tale che $x' - \overline{x} = k \cdot \frac{b}{d}$, cioè $x' = \overline{x} + k \cdot \frac{b}{d}$.
Sostituendo, infine, $k \cdot \frac{b}{d}$ in $\frac{a}{d}(x' - \overline{x}) = \frac{b}{d}(\overline{y} - y')$, si ottiene $\frac{a}{d} \cdot k\frac{b}{d} = \frac{b}{d}(\overline{y} - y')$, da cui $y' = \overline{y} - k \cdot \frac{a}{d}$.
In definitiva, le soluzioni dell'equazione completa si ottengono sommando una soluzione particolare alle soluzioni dell'omogenea associata. □

Vediamo un esempio applicativo.

Esempio 3.1.1. Dire se l'equazione diofantea $51x + 132y = 9$ ammette soluzioni e, in caso di risposta affermativa, determinarle tutte.

Soluzione. Osserviamo che $(51, 132) = 3$ è un divisore di 9 e quindi l'equazione ammette soluzioni.
Consideriamo l'equazione omogenea associata $51x + 132y = 0$ e determiniamone le soluzioni. Esse sono date da $x = k \cdot \frac{132}{3} = 44k$ e $y = -k \cdot \frac{51}{3} = -17k$, con $k \in \mathbb{Z}$.
Determiniamo adesso una soluzione particolare dell'equazione completa utilizzando il teorema di Bézout e l'algoritmo euclideo delle divisioni successive per la determinazione del massimo comune divisore di due interi.
Per il teorema di Bézout esistono $h, j \in \mathbb{Z}$ tali che $51h + 132j = 3$. Determiniamo i coefficienti h e j utilizzando il succitato algoritmo:

$$\begin{aligned}
&\text{(D1)} && 132 = 2 \cdot 51 + 30\\
&\text{(D2)} && 51 = 1 \cdot 30 + 21\\
&\text{(D3)} && 30 = 1 \cdot 21 + 9\\
&\text{(D4)} && 21 = 2 \cdot 9 + 3\\
&\text{(D5)} && 9 = 3 \cdot 3.
\end{aligned}$$

Cerchiamo, adesso, di scrivere 3 come combinazione lineare intera di 132 e 51. Così, dalla quarta relazione possiamo scrivere 3 come combinazione intera di 21 e 9 e dalla terza possiamo ricavare 9 come combinazione intera di 21 e 30. Mettendo assieme le due informazioni, otterremo 3 come combinazione intera di 21 e 30. Proseguendo così otterremo 3 come combinazione intera di 51 e 30 (dalla seconda relazione), ed infine di 132 e 51 (dalla prima relazione), che è quello a cui vogliamo arrivare. Riassumiamo quanto detto:

$$3 \overset{(D4)}{=} 21 - 2 \cdot 9 \overset{(D3)}{=} 21 - 2 \cdot (30 - 21) = -2 \cdot 30 + 3 \cdot 21 \overset{(D2)}{=} -2 \cdot 30 + 3 \cdot (51 - 30) =$$
$$3 \cdot 51 - 5 \cdot 30 \overset{(D1)}{=} 3 \cdot 51 - 5 \cdot (132 - 2 \cdot 51) = -5 \cdot 132 + 13 \cdot 51.$$

In conclusione,

$$3 = 13 \cdot 51 - 5 \cdot 132 \qquad (*)$$

quindi i coefficienti di Bézout sono $h = 13$ e $j = -5$.
Ora, ritornando all'equazione diofantea $51x + 132y = 9$, osserviamo che moltiplicando la $(*)$ per 3 si ottiene

$$39 \cdot 51 - 15 \cdot 132 = 9,$$

da cui è possibile ricavare una soluzione della suddetta equazione, cioè $\overline{x} = 39$ e $\overline{y} = -15$.
Tutte le soluzioni dell'equazione assegnata sono dunque

$$x = 39 + 44k, \qquad y = -15 - 17k$$

al variare di $k \in \mathbb{Z}$. ■

Esempio 3.1.2. Determinare la somma di tutti gli interi a e b, con $0 < a < b$, che verificano la relazione $3 \cdot [a, b] + 5 \cdot (a, b) = 123$, essendo $[a, b]$ e (a, b) rispettivamente il minimo comune multiplo e il massimo comune divisore di a e b.

Soluzione. Poniamo $x = [a, b]$ e $y = (a, b)$. Risolviamo allora l'equazione diofantea $3x + 5y = 123$, con la condizione $x \geq y > 0$. Essa ammette soluzioni in quanto $(3, 5) = 1$ è un divisore di 123. Consideriamo l'omogenea associata $3x + 5y = 0$ e determiniamone le soluzioni. Esse sono date da $x = 5k$ e $y = -3k$, con $k \in \mathbb{Z}$.
Determiniamo adesso una soluzione particolare dell'equazione completa. Per il teorema di Bézout esistono $h, j \in \mathbb{Z}$ tali che $3h+5j = 1$. Senza applicare l'algoritmo di Euclide, si ricava facilmente che $h = 2$ e $j = -1$, cioè

$$3 \cdot 2 + 5 \cdot (-1) = 1.$$

Moltiplicando ambo i membri per 123 si ottiene

$$3 \cdot 246 + 5 \cdot (-123) = 123,$$

da cui si ottiene la soluzione particolare $\overline{x} = 246$ e $\overline{y} = -123$.
La soluzione generale della diofantea è quindi data da $x = 246+5k$ e $y = -123-3k$, al variare di $k \in \mathbb{Z}$.
Dovendo essere $x \geq y > 0$, si ha $-123-3k > 0$, cioè $k < -41$, e $246+5k \geq -123-3k$, cioè $k \geq -46$; quindi dovrà essere $-46 \leq k \leq -42$. Pertanto

- per $k = -46$ si ottiene $x = 16$ e $y = 15$;
- per $k = -45$ si ottiene $x = 21$ e $y = 12$;
- per $k = -44$ si ottiene $x = 26$ e $y = 9$;
- per $k = -43$ si ottiene $x = 31$ e $y = 6$;
- per $k = -42$ si ottiene $x = 36$ e $y = 3$.

Ricordando che il minimo comune multiplo è multiplo del massimo comune divisore, l'unica coppia accettabile è $x = 36$ e $y = 3$. Le coppie $(a; b)$ verificanti le condizioni del problema e aventi 36 come minimo comune multiplo e 3 come massimo comune divisore sono $(3; 36)$ e $(9; 12)$. Pertanto la somma di tutti i valori trovati è 60. ■

3.1.1 Teorema di Frobenius

Nel paragrafo precedente abbiamo visto che l'equazione diofantea $ax + by = c$ ammette (infinite) soluzioni se e solo se (a, b) è un divisore di c e che, in particolare, ciò accade sempre se $(a, b) = 1$.
Consideriamo il caso in cui gli interi a, b sono positivi e coprimi e determiniamo quando l'equazione ammette soluzioni non negative, cioè soluzioni (x, y) per cui $x, y \geq 0$. Naturalmente se $c < 0$, l'uguaglianza $ax + by = c$, con $x, y \geq 0$, non potrà mai sussistere; quindi deve essere $c \geq 0$. In tal caso, comunque, non sempre esistono soluzioni. Ciò equivale a dire che non tutti gli interi positivi sono esprimibili come combinazione lineare intera non negativa di a e b. Vale, infatti, il seguente teorema.

Teorema 3.1.4 (Frobenius)**.** *Siano a, b interi positivi. Se $(a, b) = 1$, il più grande intero positivo non esprimibile nella forma $ax + by$, con $x, y \geq 0$ interi, è $ab - a - b$. Inoltre, il numero di interi positivi che non si possono scrivere in tal forma è pari ad $\dfrac{(a-1)(b-1)}{2}$.*

Dimostrazione. Prima parte. Innanzitutto, diciamo che un intero c è *ottenibile* se è possibile scriverlo nella forma $ax + by$, con $x, y \geq 0$ interi. Disponiamo, ora, tutti gli interi non negativi a formare una tabella, nel modo seguente:

0,	1,	2,	...,	r,	...,	a-2,	a-1
a,	a+1,	a+2,	...,	a+r,	...,	2a-2,	2a-1
2a,	2a+1,	2a+2,	...,	2a+r,	...,	3a-2,	3a-1
3a,	3a+1,	3a+2,	...,	3a+r,	...,	4a-2,	4a-1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Osserviamo che nella prima colonna si trovano tutti i naturali multipli di a, nella seconda quelli che divisi per a danno resto 1, nella terza quelli che divisi per a danno resto 2 e così via, fino all'ultima in cui si trovano i naturali che divisi per a danno resto $a-1$.

Osserviamo ancora che se c è uno degli interi appartenente alla tabella, tutti gli interi ad esso sottostanti[2] sono della forma $c+ka$, con k numero naturale. Pertanto, se c è ottenibile, lo sono anche tutti gli interi ad esso sottostanti.

Ora, tutti i multipli di b (anch'essi presenti nella tabella) sono ovviamente ottenibili. Faremo vedere adesso che di tali multipli, quelli della forma hb, con $0 \leq h \leq a-1$, si distribuiscono, all'interno della precedente tabella, uno per colonna. Infatti, se per assurdo esistessero due multipli rb e sb, con $0 \leq r < s \leq a-1$, appartenenti alla medesima colonna, dovendo dare lo stesso resto nella divisione per a, la loro differenza $b(s-r)$ sarebbe multipla di a cioè, ricordando che $(a,b)=1$, $s-r$ sarebbe multiplo di a, e quindi a sarebbe un divisore di $s-r$. Ciò è assurdo in quanto $0 < s-r < a$.
Abbiamo quindi finora provato che tutti i multipli di b della forma hb (ottenibili), con $0 \leq h \leq a-1$, si distribuiscono uno per colonna e che tutti gli interi ad essi sottostanti sono ottenibili. Facciamo vedere che se prendiamo uno di questi multipli, nessuno degli interi sovrastanti[3] è ottenibile.
A tale scopo, sia hb fissato, con $0 \leq h \leq a-1$. Tutti gli interi ad esso sovrastanti sono della forma $hb-ka$, per qualche k numero naturale. Ora, se fosse $hb-ka = ax+by$, con $x, y \geq 0$ interi, si avrebbe $by \leq ax+by = hb-ka < hb$, da cui $0 \leq y < h < a$. D'altra parte, si ha che hb, $hb-ka$, $ax+by$ e by danno lo stesso resto nella divisione per a, quindi $hb-by = b(h-y)$ è multiplo di a. Essendo $(a,b)=1$, ne segue che $h-y$ è multiplo di a. Ma ciò è assurdo in quanto $0 < h-y < a$. Di conseguenza, tutti gli interi sovrastanti hb non sono ottenibili.

Ne segue che il più grande intero non ottenibile è quello immediatamente sovrastante il maggiore dei multipli di b della forma hb, con $0 \leq h \leq a-1$, cioè immediatamente sovrastante $(a-1)b$. Tale intero non può che essere $(a-1)b-a = ab-b-a$.

Seconda parte. Dalla prima parte della dimostrazione segue immediatamente che il numero totale dei naturali non ottenibili è pari al numero dei naturali della tabella sovrastanti i multipli di b della forma hb, con $0 \leq h \leq a-1$.
Ora, se k è il numero di elementi presenti nella colonna $i-$esima e sovrastanti hb, allora $hb = ka+i$, da cui $k = \dfrac{hb-i}{a}$. Il totale degli elementi non ottenibili si ottiene quindi sommando tutti i valori di k al variare di $0 \leq h, i \leq a-1$, e

[2] cioè appartenenti alla stessa colonna di c ma alle righe successive a quella in cui è collocato c.
[3] cioè appartenenti alla stessa colonna ma alle righe precedenti.

dividendo tutto per a (altrimenti ogni addendo sarebbe contato a volte), cioè

$$\frac{1}{a}\sum_{h=0}^{a-1}\sum_{i=0}^{a-1}\frac{hb-i}{a}=\frac{1}{a^2}\sum_{h=0}^{a-1}\left(\sum_{i=0}^{a-1}hb-\sum_{i=0}^{a-1}i\right)=\frac{1}{a^2}\sum_{h=0}^{a-1}\left(hba-\frac{(a-1)a}{2}\right)=$$
$$\frac{ba}{a^2}\sum_{h=0}^{a-1}h-\frac{(a-1)a}{2a^2}\sum_{h=0}^{a-1}1=b\cdot\frac{(a-1)a}{2a}-\frac{(a-1)a}{2a}=\frac{(b-1)(a-1)}{2}$$

che è quanto volevasi dimostrare. □

Dal Teorema di Frobenius segue, ad esempio, che il più grande intero positivo a non potersi scrivere come combinazione lineare intera a coefficienti non negativi di 18 e 35 è $18\cdot 35-18-35=577$. Ciò vuol dire che tutti gli interi maggiori o uguali a 578 sono esprimibili come somma di un multiplo (non negativo) di 18 e di un multiplo (non negativo) di 35, mentre non tutti gli interi positivi minori di 578 sono esprimibili nel modo indicato.

Osservazione 3.1.5. Osserviamo che nel caso in cui $d=(a,b)>1$, gli unici interi non negativi esprimibili come combinazione lineare intera a coefficienti non negativi di a e b sono multipli di d, per cui non esiste un valore massimo tra quelli non esprimibili nel modo indicato.

Esempio 3.1.3. Un bersaglio è costituito da due cerchi concentrici. Un giocatore lancia contro il bersaglio un numero infinito di frecce, una alla volta, ottenendo a punti se colpisce il cerchio interno, b punti se colpisce la corona circolare esterna, con $a>b$. Il punteggio complessivo si ottiene sommando i punteggi parziali ottenuti dopo ogni lancio. Sapendo che non è possibile ottenere esattamente 65 punteggi, tra cui 38, quali sono i valori di a e b ?

Soluzione. Il punteggio parziale ottenuto dal giocatore ad un certo punto del gioco è del tipo $ax+by$, con $x,y\in\mathbb{N}$. Osserviamo inoltre che $(a,b)=1$ in quanto, se fosse $(a,b)=d>1$ tutti gli infiniti punteggi non multipli di d non sarebbero ottenibili, contro il fatto che solamente 65 punteggi non sono ottenibili. Inoltre, per il teorema di Frobenius, si ha che $\frac{(a-1)(b-1)}{2}=65$ da cui $(a-1)(b-1)=130$. Dovendo essere $a>b$, le uniche possibilità sono allora $a=131$ e $b=2$ oppure $a=66$ e $b=3$ oppure $a=27$ e $b=6$ o ancora $a=14$ e $b=11$.
Il caso $a=131$ e $b=2$ si scarta in quanto per $x=0$ e $y=19$ si ottiene il punteggio $38=131\cdot 0+2\cdot 19$; anche i casi in cui $a=66$ e $b=3$ e in cui $a=27$ e $b=6$ si scartano in quanto si avrebbe $(a,b)>1$.
Di conseguenza, l'unica soluzione accettabile è proprio $a=14$ e $b=11$ che, come facilmente si verifica, soddisfa tutte le condizioni del problema. ■

3.2 Equazioni diofantee non lineari

Nella risoluzione di equazioni diofantee non lineari non esistono, in generale, algoritmi risolutivi standard, ma delle tecniche che, usate opportunamente, permettono in alcuni casi di mostrare la non esistenza di soluzioni, in altri di determinarle direttamente o indirettamente, consentendo di estrapolare informazioni utili sulle incognite. La scelta della tecnica da seguire dipende, spesso, dalle prime informazioni che si riescono a ricavare sulle soluzioni, sostituendo ad esempio dei valori e determinando qualche soluzione immediata, la parità, ecc.. Inoltre, se sostituendo una serie di valori alle incognite non si riesce a trovare una soluzione, si può tentare di dimostrare che la diofantea non ha soluzioni.

Abbiamo visto che le equazioni diofantee lineari sono impossibili oppure ammettono un numero infinito di soluzioni. Le equazioni diofantee non lineari sono fondamentalmente di uno dei seguenti tipi:

❶ equazioni senza soluzioni;

❷ equazioni con un numero finito di soluzioni (a volte solo quella banale fatta da zeri);

❸ equazioni con un numero infinito di soluzioni in forma parametrizzata.

Per dimostrare che una equazione non ha soluzioni o ne ha solo un numero finito, di solito è preferibile utilizzare il metodo della discesa infinita, già applicato nel primo capitolo del presente libro, o ragionare sulla parità dei termini o ancora manipolare l'equazione fattorizzandola.
Nel caso di equazioni con un numero infinito di soluzioni in forma parametrizzata, si può cercare di determinarle in maniera costruttiva.[4]

Gli esempi che seguono chiariranno meglio i concetti sopra esposti.

Esempio 3.2.1. Determinare tutte le coppie di interi (x, y) che sono soluzioni dell'equazione

$$x^2 = y^2 + 12.$$

Soluzione. Riscriviamo diversamente l'equazione nella forma

$$x^2 - y^2 = 12$$

[4] Esistono altre potenti tecniche risolutive che fanno uso degli strumenti dell'*aritmetica modulare* ma che non presentiamo perché esulano dagli obiettivi del presente volume.

da cui, fattorizzando, si ottiene

$$(x-y)(x+y)=12.$$

Di conseguenza $x-y$ e $x+y$ devono essere divisori di 12 il cui prodotto è 12. La tabella seguente mostra le varie possibilità (in colonna):

$x-y$	1	2	3	4	6	12	-1	-2	-3	-4	-6	-12
$x+y$	12	6	4	3	2	1	-12	-6	-4	-3	-2	-1

Analizziamo i vari casi:

- se $\begin{cases} x-y=1 \\ x+y=12 \end{cases}$ sommando membro a membro si ottiene $2x=13$, cioè $x=\dfrac{13}{2}$ che non è un numero intero, quindi in tal caso non si ottiene alcuna coppia di soluzioni;
- se $\begin{cases} x-y=2 \\ x+y=6 \end{cases}$ sommando membro a membro si ottiene $2x=8$, cioè $x=4$ e quindi $y=2$;
- se $\begin{cases} x-y=3 \\ x+y=4 \end{cases}$ sommando membro a membro si ottiene $2x=7$, che come nel primo caso non dà soluzioni intere;
- se $\begin{cases} x-y=4 \\ x+y=3 \end{cases}$ sommando membro a membro si ottiene $2x=7$, che non dà soluzioni intere;
- se $\begin{cases} x-y=6 \\ x+y=2 \end{cases}$ sommando membro a membro si ottiene $2x=8$, cioè $x=4$ e quindi $y=-2$;
- se $\begin{cases} x-y=12 \\ x+y=1 \end{cases}$ sommando membro a membro si ottiene $2x=13$, che non dà soluzioni intere.

Nel caso in cui i divisori sono entrambi negativi, si ottengono coppie di numeri opposti a quelli ottenuti nel caso in cui i divisori sono entrambi positivi (già analizzati). Di conseguenza tutte le coppie di interi, soluzioni dell'equazione data, sono: $(4,2)$, $(4,-2)$, $(-4,-2)$, $(-4,2)$. ■

Se analizziamo l'esempio precedente, ci rendiamo conto che nel caso in cui i fattori $x-y$ e $x+y$ hanno diversa parità il problema non ha soluzione. Possiamo così generalizzare la risoluzione della diofantea

$$x^2-y^2=k$$

con $k \in \mathbb{Z}$, nel modo seguente.
Fattorizziamo il primo membro:

$$(x-y)(x+y) = k.$$

Le soluzioni della diofantea si ottengono ponendo $x - y = a$ e $x + y = b$, al variare dei divisori a e b di k tali che $a \cdot b = k$, e risolvendo quindi il sistema

$$\begin{cases} x - y = a \\ x + y = b \end{cases}$$

Le soluzioni sono date da

$$x = \frac{a+b}{2} \qquad \text{e} \qquad y = \frac{b-a}{2}$$

che sono numeri interi se e solo se a e b hanno la stessa parità (entrambi pari o entrambi dispari). Quest'ultima condizione si realizza per qualunque scelta di coppie di divisori (a, b), con $a \cdot b = k$, se k è dispari (in quanto tutti i divisori di k sono dispari). Nel caso in cui k è pari, si hanno due situazioni diverse a seconda che k sia divisibile per 2 ma non per 4 o k sia divisibile almeno per 4. Infatti:

- se k è divisibile per 2 ma non per 4, ogni coppia di divisori (a, b) di k è costituita da un numero pari e da uno dispari e pertanto il sistema

  $$\begin{cases} x - y = a \\ x + y = b \end{cases}$$

  non ammette mai soluzioni intere;

- se k è divisibile almeno per 4, esisteranno coppie di divisori (a, b) entrambi pari e coppie (a', b') di divisori di parità diversa. Le coppie del primo tipo generano soluzioni intere della diofantea, le coppie del secondo tipo no.

In definitiva abbiamo dimostrato che **l'equazione diofantea $x^2 - y^2 = k$ ammette soluzioni intere se e solo se k è dispari oppure k è divisibile almeno per 4, è impossibile se e solo se k è divisibile per 2 ma non per 4.**

Ad esempio, le diofantee $x^2 - y^2 = -10$ e $x^2 - y^2 = 574$ non ammettono soluzioni intere in quanto -10 e 574 sono pari ma non divisibili per 4. Ammettono, invece, soluzioni intere le equazioni diofantee $x^2 - y^2 = 19$, $x^2 - y^2 = 20$ o $x^2 - y^2 = -56$.

Esempio 3.2.2. (Olimpiadi della Matematica, Provinciale 2011) Siano x e y due interi positivi tali che $x^2 - y^2$ è positivo, multiplo di 2011 e ha esattamente 2011 divisori positivi. Quante sono le coppie ordinate (x, y) che verificano tali condizioni?

Soluzione. Osserviamo che 2011 è un numero primo e quindi, affinchè $x^2 - y^2$ abbia 2011 divisori positivi e sia multiplo di 2011, deve essere necessariamente $x^2 - y^2 = 2011^{2010}$. Bisogna quindi risolvere la diofantea

$$x^2 - y^2 = 2011^{2010}.$$

Per quanto visto in precedenza, le soluzioni si ottengono risolvendo il sistema

$$\begin{cases} x - y = a \\ x + y = b \end{cases}$$

dove a e b sono divisori positivi di 2011^{2010} (sono entrambi positivi in quanto $x, y > 0$ e $x^2 - y^2 > 0$) e quindi $a = 2011^k$ e $b = 2011^h$, con $h, k \in \mathbb{N}$, $h + k = 2010$. Risolvendo il sistema si ottengono le soluzioni

$$x = \frac{2011^h + 2011^k}{2} \qquad \text{e} \qquad y = \frac{2011^h - 2011^k}{2}$$

al variare di h, k come precedentemente indicato. Dovendo essere $y > 0$, necessariamente $h > k$ e quindi $1006 \leq h \leq 2010$. Poiché ogni valore di h (e quindi di k) determina univocamente una coppia di soluzioni della diofantea, le coppie cercate sono 1005. ■

Esempio 3.2.3. Determinare tutte le coppie ordinate (x, y) di interi che sono soluzione della diofantea $xy = x + y + 5$.

Soluzione. Riscriviamo la diofantea nel modo seguente $xy - x - y + 1 = 6$, cioè

$$(x - 1)(y - 1) = 6.$$

$x - 1$ e $y - 1$ devono essere, quindi, due divisori di 6 il cui prodotto è 6 e di conseguenza avremo le seguenti possibilità:

- $x - 1 = 1$ e $y - 1 = 6$, da cui si ottiene la soluzione $(2, 7)$;
- $x - 1 = 2$ e $y - 1 = 3$, che dà come soluzione la coppia $(3, 4)$;
- $x - 1 = 3$ e $y - 1 = 2$, che dà come soluzione la coppia $(4, 3)$;

- $x-1=6$ e $y-1=1$, che dà come soluzione la coppia $(7,2)$;
- $x-1=-1$ e $y-1=-6$, che dà come soluzione la coppia $(0,-5)$;
- $x-1=-2$ e $y-1=-3$, che dà come soluzione la coppia $(-1,-2)$;
- $x-1=-3$ e $y-1=-2$, che dà come soluzione la coppia $(-2,-1)$;
- $x-1=-6$ e $y-1=-1$, che dà come soluzione la coppia $(-5,0)$.

Le soluzioni sono quindi le coppie ordinate $(2,7)$, $(7,2)$, $(3,4)$, $(4,3)$, $(0,-5)$, $(-5,0)$, $(-1,-2)$ e $(-2,-1)$. ■

Esempio 3.2.4. Determinare tutte le coppie ordinate di interi (x,y) tali che $x^2+4=4y(4y-2)$.

Soluzione. Eliminando le parentesi a destra dell'uguale, si ottiene $x^2+4=16y^2-8y$, cioè $x^2+5=16y^2-8y+1$ da cui

$$(4y-1)^2-x^2=5.$$

Gli unici due quadrati la cui differenza è 5 sono 9 e 4, quindi avremo i seguenti casi:

- $4y-1=3$ e $x=2$, che dà come soluzione la coppia $(2,1)$;
- $4y-1=3$ e $x=-2$, che dà come soluzione la coppia $(-2,1)$;
- $4y-1=-3$ e $x=\pm 2$, che non danno soluzioni intere in quanto $y=-\dfrac{1}{2}$.

In conclusione, le uniche coppie ordinate di soluzioni sono $(2,1)$ e $(-2,1)$. ■

Esempio 3.2.5. Risolvere negli interi l'equazione $x^6+x^5y+xy^5+y^6=0$.

Soluzione. Fattorizzando il primo membro si ottiene $(x+y)(x^5+y^5)=0$, da cui si ricava che $x=-y$. Pertanto, le soluzioni intere dell'equazione assegnata sono tutte e sole le coppie del tipo $(k,-k)$ (si verifica facilmente che $(k,-k)$ è soluzione) per ogni $k\in\mathbb{Z}$. ■

Osservazione 3.2.1. Osserviamo che le equazioni presentate negli esempi 3.2.3 e 3.2.5 sono *simmetriche* in x e y, nel senso che se si scambia la variabile x con la variabile y si ottiene la medesima equazione di partenza. Pertanto, se (a,b) è soluzione, anche (b,a) lo è.

Esempio 3.2.6. Determinare tutte le terne ordinate di interi (x, y, z) tali che $4z^2 - x^2 = 2y^2$.

Soluzione. Una soluzione è chiaramente la terna $(0, 0, 0)$. Osserviamo ora che, essendo $4z^2$ e $2y^2$ pari, x deve essere pari, quindi $x = 2t$ per qualche t intero. L'equazione diventa così: $4z^2 - 4t^2 = 2y^2$ da cui, dividendo ambo i membri per 2, segue che anche y deve essere pari, cioè $y = 2v$ per qualche v intero. Si ottiene così l'equazione

$$z^2 - t^2 = 2v^2.$$

Fattorizzando il primo membro abbiamo che $(z - t)(z + t) = 2v^2$, da cui segue che v non può essere dispari[5]. Di conseguenza, per ogni valore di v pari, si ottengono soluzioni dell'equazione assegnata, quindi l'equazione ha infinite soluzioni che possono essere scritte nella forma $(a, 4b, c)$, con $b \in \mathbb{Z}$, $a = 2t$, $c = h$ tali che (t, h) è soluzione della diofantea $h^2 - t^2 = 2u^2$, con $u = 2b$. ■

3.3 Frazioni continue ed equazioni di Pell

Presentiamo adesso un'applicazione dell'algoritmo euclideo delle divisioni successive per la determinazione del massimo comune divisore di due interi. Dimostreremo, infatti, che ogni numero razionale può essere scritto come *frazione finita continua*, così come ogni numero irrazionale come frazione continua infinita, ed useremo questo risultato nella risoluzione delle *equazioni di Pell*.

3.3.1 Frazioni continue finite

Iniziamo con un esempio, considerando la frazione $\frac{185}{79}$. Applicando l'algoritmo euclideo alla determinazione del massimo comune divisore di 185 e 79 si ottiene

$$\begin{aligned} &\text{(passo 1)} && 185 = 79 \cdot 2 + 27 \\ &\text{(passo 2)} && 79 = 27 \cdot 2 + 25 \\ &\text{(passo 3)} && 27 = 25 \cdot 1 + 2 \\ &\text{(passo 4)} && 25 = 2 \cdot 12 + 1. \end{aligned}$$

[5] Infatti, se fosse v dispari, $2v^2$ sarebbe divisibile per 2 ma non per 4 e quindi l'equazione $z^2 - t^2 = 2v^2$ sarebbe impossibile