Luigi Verolino

Introduzione alle equazioni diofantee

ATENEAPOLI Editore

Introduzione alle equazioni diofantee

Università degli Studi di Napoli Federico II

Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione

Via Claudio, 21 – 80125 [Napoli]

verolino@unina.it

ATENEAPOLI Editore

Introduzione alle equazioni diofantee
ISBN: 978-88-97840428

edizioni Ateneapoli s.r.l.
via Pietro Colletta, 12 (80139) Napoli
www.ateneapoli.it

http://www.ateneapolieditore.it/libri/

Renato Caccioppoli

Napoli, 1904 – Napoli, 1959

"Per tre cose vale la pena di vivere: la Matematica, la Musica e l'Amore"

Indice

Introduzione

Scopo di questo libello è introdurre lo studente liceale ed universitario alle *equazioni diofantee*, anche dette diofantine, adoperando, per lo più, concetti e tecniche ampiamente studiati nella scuola secondaria superiore, vale a dire senza ricorrere al formalismo delle Frazioni Continue e senza adoperare l'Aritmetica Modulare. Parecchi esempi svolti aiuteranno a rendere più comprensibili e piani i passaggi più astratti della teoria sviluppata. Una particolare attenzione verrà dedicata allo studio delle equazioni diofantee lineari.

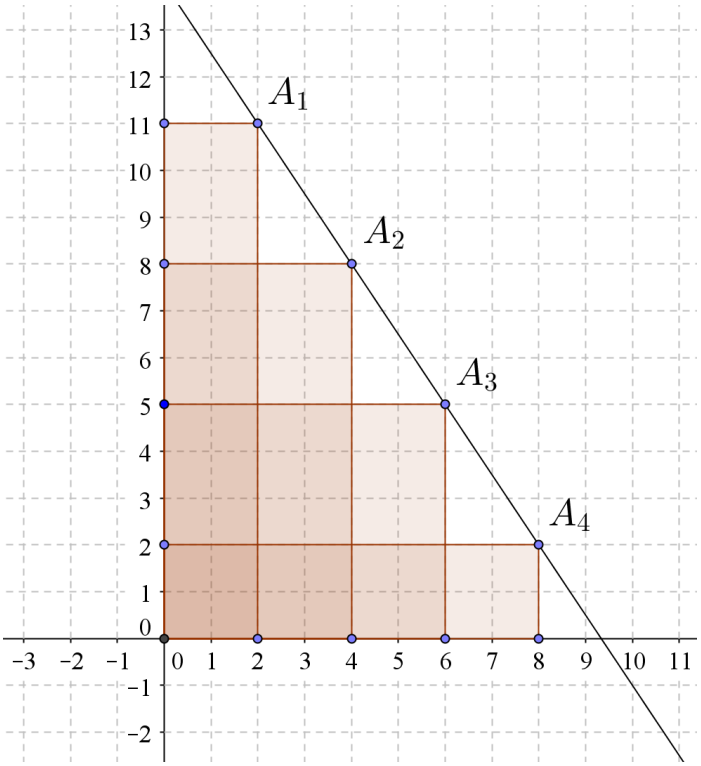
Le equazioni diofantee sono equazioni per le quali si cercano soltanto soluzioni intere e compaiano in diversi problemi, anche piuttosto semplici della vita quotidiana. Esistono anche i sistemi di equazioni diofantee che rappresentano una naturale estensione delle equazioni. Ad esempio, si immagini che un negoziante debba acquistare un certo numero di maglioni a collo basso da 40 € ed un certo numero di maglioni a collo alto da 60 €, avendo a disposizione 560 €. Si desidera sapere quanti maglioni di un tipo e quanti dell'altro riesce ad acquistare, nell'ipotesi di voler spendere l'intera cifra a disposizione. Indicando con b il numero di maglioni a collo basso acquistati, ovviamente intero, essendo improbabile che il negoziante voglia acquistare mezzo maglione, e con a quello dei maglioni a collo alto, deve essere

$$40b + 60a = 560 \quad \rightarrow \quad 2b + 3a = 28\,.$$

Si tratta di un'equazione in due incognite con coefficienti interi di cui si ricercano le soluzioni intere.

b	11	8	5	2
a	2	4	6	8

Qualche elementare considerazione numerica fornisce i risultati presentati nella tabella precedente. Dunque, il negoziante ha alcune possibilità, rappresentate dai quattro punti evidenziati in figura, e deciderà di approvvigionarsi di un tipo oppure dell'altro tipo di maglione, a seconda delle scorte di magazzino che possiede. È opportuno sottolineare che, se non vi fosse stato il vincolo delle soluzioni intere, il problema avrebbe ammesso infinite soluzioni, rappresentate da tutti i punti che si trovano sulla retta di seguito disegnata.



Se il negoziante dell'esempio appena sviluppato avesse avuto a disposizione solamente di 550 €, decidendo sempre di spendere l'intera somma a disposizione, come sarebbe cambiata la soluzione? Ebbene, sembra incredibile, ma non esiste alcuna combinazioni di numeri interi che soddisfa l'equazione

$$40x + 60y = 550 \quad \rightarrow \quad 4x + 6y = 55\,.$$

È facile convincersi di quanto affermato, osservando che il primo membro è sempre un numero pari, mentre il secondo è dispari.

Sorgono allora spontanee alcune domande: è giusto chiedersi se esistano soluzioni di un'equazione diofantea, se ve ne siano altre accanto a quelle facili da trovare, se esistano finite oppure infinite soluzioni, se sia possibile trovare una lista delle soluzioni e quale procedura si debba adoperare per calcolarle tutte. A queste domande si tenterà di dare una risposta nelle pagine che seguono, con la malcelata speranza di poter introdurre questi argomenti nella ordinaria didattica di Matematica della secondaria superiore e fare in modo che non risultino appannaggio soltanto di coloro, già particolarmente dotati, che prendono parte alle fasi finali delle Olimpiadi della Matematica.

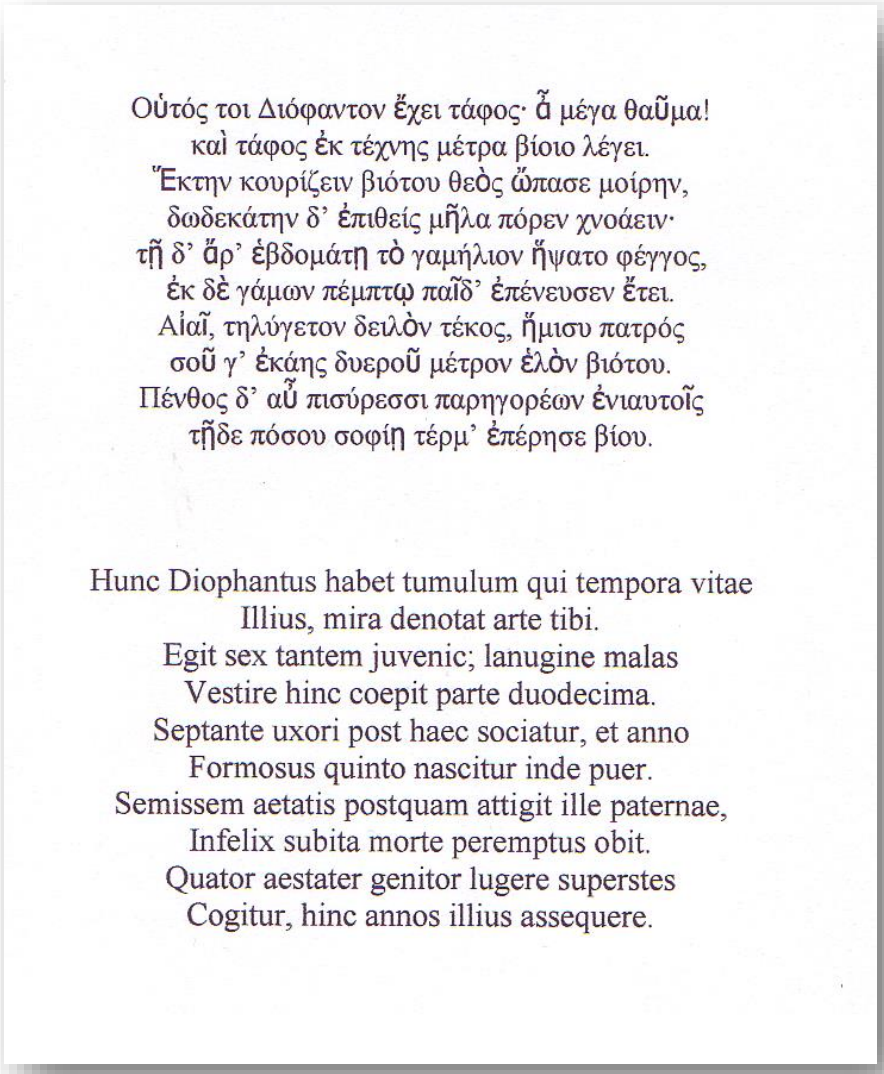
Un consiglio prima di terminare questa introduzione. Il lettore attento deve tener presente che un libro di Matematica non può essere letto in fretta e non deve pretendere di capire tutte le parti del libro alla prima lettura. Deve sentirsi libero di saltare le parti più complicate, per ritornarvi in seguito: spesso ciò che da principio appare oscuro viene chiarito da qualche osservazione successiva. D'altra parte, certi capitoli contengono materiale ben familiare al lettore e possono essere letti molto rapidamente.

Considerazioni storiche

Diofanto, vissuto nel III secolo dopo Cristo, è considerato l'iniziatore del calcolo algebrico. Scrisse un trattato sui numeri poligonali e sulle frazioni, ma la sua opera principale sono gli *Arithmetica*, un trattato in tredici volumi dei quali soltanto sei sono giunti fino a noi. La sua fama è principalmente legata a due argomenti: le equazioni indeterminate ed il simbolismo matematico.

Ben poco si sa della sua vita e quel poco è stato trasmesso da Herbert Westren Turnbull (31 agosto 1885 – 4 maggio 1961), un storico inglese della Matematica che ha rinvenuto e tradotto l'epigramma greco, noto come *Epitaffio di Diofanto*. Si

tratta di un problema aritmetico proposto sotto forma di epigramma e fa parte di una raccolta di quarantasei indovinelli, che il grammatico latino Metrodoro, durante il VI secolo dopo Cristo, incluse nell'Antologia Greca. Tutti i quesiti corrispondono ad equazioni di primo grado ad un'incognita. Ecco il testo dell'indovinello.



Οὑτός τοι Διόφαντον ἔχει τάφος· ἆ μέγα θαῦμα!
καὶ τάφος ἐκ τέχνης μέτρα βίοιο λέγει.
Ἕκτην κουρίζειν βιότου θεὸς ὤπασε μοίρην,
δωδεκάτην δ' ἐπιθείς μῆλα πόρεν χνοάειν·
τῇ δ' ἄρ' ἑβδομάτῃ τὸ γαμήλιον ἥψατο φέγγος,
ἐκ δὲ γάμων πέμπτῳ παῖδ' ἐπένευσεν ἔτει.
Αἰαῖ, τηλύγετον δειλὸν τέκος, ἥμισυ πατρός
σοῦ γ' ἑκάης δυεροῦ μέτρον ἑλὸν βιότου.
Πένθος δ' αὖ πισύρεσσι παρηγορέων ἑνιαυτοῖς
τῇδε πόσου σοφίῃ τέρμ' ἐπέρησε βίου.

Hunc Diophantus habet tumulum qui tempora vitae
Illius, mira denotat arte tibi.
Egit sex tantem juvenic; lanugine malas
Vestire hinc coepit parte duodecima.
Septante uxori post haec sociatur, et anno
Formosus quinto nascitur inde puer.
Semissem aetatis postquam attigit ille paternae,
Infelix subita morte peremptus obit.
Quator aestater genitor lugere superstes
Cogitur, hinc annos illius assequere.

Questa tomba rinchiude Diofanto e, con grande meraviglia, dice matematicamente quanto ha vissuto. La sua giovinezza durò un sesto della sua vita; poi la sua barba iniziò a crescere dopo un dodicesimo; si sposò dopo un settimo e gli nacque un figlio

dopo cinque anni. Il figlio visse la metà degli anni del padre e il padre morì quattro anni dopo il figlio. Quanti anni visse Diofanto?

Detta x l'età di Diofanto, il problema si traduce nell'equazione

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x \quad \rightarrow \quad x = 84\,.$$

Se l'epitaffio corrisponde a verità, Diofanto morì all'età di ottantaquattro anni.
Le innovazioni degli *Arithmetica* ebbero grande influenza sul pensiero algebrico arabo e giunsero in Italia assai più tardi: nel 1621, fu pubblicata la prima traduzione degli *Arithmetica*, curata dal grande algebrista italiano Raffaele Bombelli. La fama di Diofanto è legata anche ad un altro fatto: egli fu il primo ad usare un simbolismo matematico che non era non basato solo sul linguaggio naturale, ma che usava in modo sistematico le lettere per abbreviare le incognite. È un vero peccato che egli stesso non sia stato consapevole della portata della sua innovazione: con ogni probabilità ritenne di aver trovato semplicemente un sistema che consentiva di ridurre la scrittura, non un sistema simbolico automatico di estrema efficacia e precisione. Il sintetico simbolismo matematico oggi in uso è una conquista di non più di quattro secoli fa e dunque è relativamente recente rispetto ai millenni precedenti in cui la Matematica è stata prevalentemente descrittiva e basata sull'uso della parola.

Indovinelli diofantei

Un altro indovinello di tipo diofanteo è stato proposto, qualche anno fa, quale test di ingresso agli studi universitari tecnico-scientifici. Ecco il testo.

Fra tre anni Matteo avrà il doppio dell'età che Sara aveva tre anni fa, mentre ora il quadruplo degli anni di lui è pari al quintuplo degli anni di lei. Se è possibile determinarlo, qual è l'età di Matteo e di Sara?

Si indichi con x l'età di Matteo e con y quella di Sara. Per determinare queste due incognite intere, è sufficiente impostare un sistema lineare di equazioni, utilizzando le due condizioni imposte dal testo dell'indovinello. Precisamente, l'affermazione contenuta nel testo *fra tre anni Matteo avrà il doppio dell'età che Sara aveva tre anni fa*, in termini analitici, si trasforma nell'equazione

$$x + 3 = 2(y - 3) \quad \rightarrow \quad x - 2y = -9 \, .$$

Similmente, l'affermazione *ora il quadruplo degli anni di lui è pari al quintuplo degli anni di lei*, diventa

$$4x - 5y = 0 \, .$$

Mettendole insieme, risulta il sistema di due equazioni lineari

$$\begin{cases} x - 2y = -9 \, , \\ 4x - 5y = 0 \, , \end{cases}$$

la cui soluzione costituisce l'obiettivo dell'esempio. Prima però di risolverlo, è opportuno verificare che esso ammetta un'unica soluzione, per cui è necessario verificare che il determinante

$$\begin{vmatrix} 1 & -2 \\ 4 & -5 \end{vmatrix} = 3 \neq 0$$

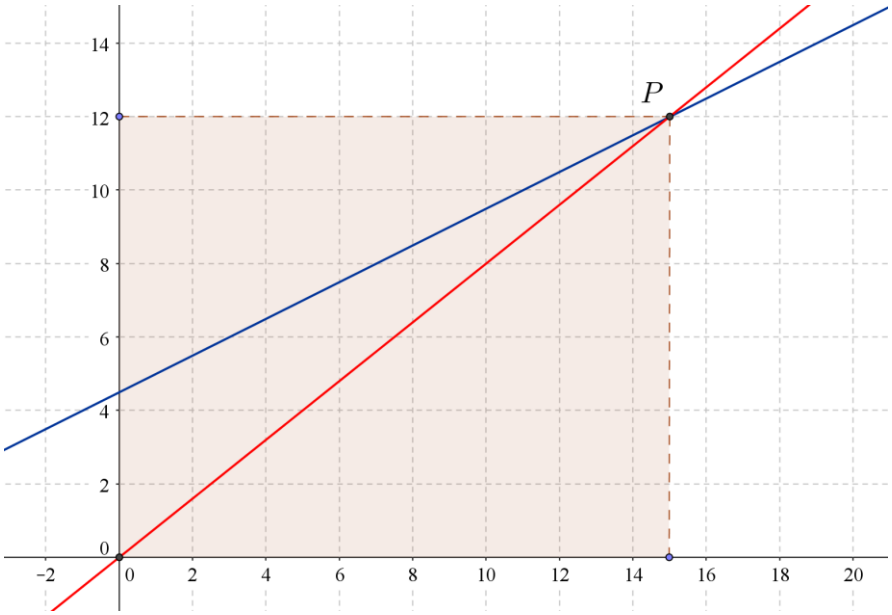
sia diverso da zero. Si ottiene allora che

$$x = 15\,,\quad y = 12\,,$$

cioè Matteo ha quindici anni e Sara ne ha dodici. La figura che segue illustra in maniera grafica l'intersezione tra le due rette

$$y = \frac{x+9}{2}\quad \text{(blu)}\,,\quad y = \frac{4}{5}x\quad \text{(rossa)}\,,$$

cioè la soluzione grafica dell'indovinello: l'asse delle ascisse rappresenta l'età di Matteo, quello delle ordinate indica invece l'età di Sara, il punto P è la soluzione del problema.



Esempio 1 – Si verifichi che una soluzione dell'equazione diofantea

$$y^2 = x^2 + 9\quad (x, y \in \mathbb{Z})$$

è costituita dalla coppia $x = 4, y = 5$.

Si ottiene immediatamente per sostituzione

$$5^2 = 4^2 + 9 = 16 + 9 = 25\,.$$

È possibile scambiare il ruolo delle due variabili, cioè assumere quale nuova coppia di soluzione $x = 5, y = 4$?

Come sostiene Harold Davenport nel suo libro di *Aritmetica superiore: un'introduzione alla teoria dei numeri*, non esiste probabilmente ramo della teoria dei numeri che presenti maggiori difficoltà della teoria, se così può essere chiamata, delle equazioni diofantee. Un'occhiata alla letteratura molto estesa fa pensare ad una messe di risultati non correlati riguardanti equazioni di tipo speciale, scoperti con artifici di estrema ingegnosità, ma che non sembrano ricomporsi in alcuna teoria di tipo generale. Talvolta, dopo che un'equazione era stata risolta con qualche metodo di carattere particolare, si è potuto costruire una teoria attorno a quella soluzione, in modo da gettar luce sulla sua natura ed in modo da poter comprendere il suo grado di generalità. Ma le difficoltà intrinseche di questo soggetto sono così notevoli che la portata di una tale teoria è di solito assai limitata. Laddove, a partire da equazioni diofantee di tipo particolare, si sia potuto sviluppare una teoria estesa, come nel caso delle forme quadratiche, questa è stata presto considerata come se ricoprisse un ruolo indipendente.

Una delle prove di ammissione per i chimici ed i biologi alla Scuola Normale Superiore di Pisa, una delle più prestigiose istituzioni culturali del nostro paese, per l'anno accademico 2014-2015 era rappresentata dall'esempio che segue, in cui si mostra come un buon grafico possa essere di grande aiuto per arrivare alla soluzione dell'equazione diofantea.

Esempio 2 – Trovare tutte le soluzioni intere dell'equazione

$$xy + x + y + 2 = 0\,.$$

La prima cosa da fare è esplicitare in funzione di y l'equazione assegnata. Si può allora scrivere che

$$y = -\frac{x+2}{x+1} = -1 - \frac{1}{x+1}\,, \quad (x \neq -1)\,.$$

Si tratta dell'iperbole traslata, con centro in $C(-1,-1)$, riportata nella figura che segue. Si mostrerà ora come si ottengono le soluzioni intere da un'attenta osservazione di questo grafico.
Si nota che, considerando il solo intervallo $x < -2$, la funzione ha come codominio l'insieme

$$-1 < y < 0\,.$$

Ciò comporta che non esistono soluzioni intere in questo intervallo.
La prima soluzione intera si trova nel punto

$$A(-2,0)\,.$$

Per $-2 < x < 0$, l'unico intero candidabile, cioè $x = -1$, rappresenta un asintoto verticale per la funzione. Per ulteriore controllo, si ritorni all'equazione non esplicitata e, sostituendo $x = -1$, si ottiene un'uguaglianza impossibile

$$xy + x + y + 2 = 0 \;\rightarrow\; x = -1 \;\rightarrow\; 1 = 0 \text{ (assurdo).}$$

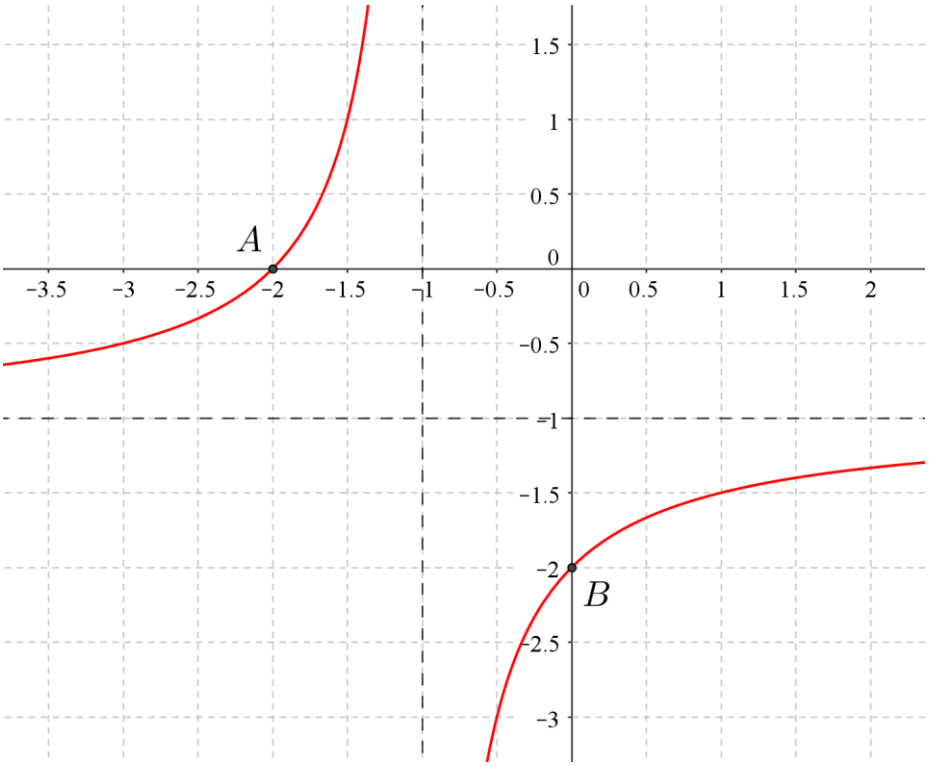
La seconda soluzione intera si incontra nel punto

$$B(0,-2)\,.$$

Per $x > 0$, la funzione ha come codominio l'insieme

$$-2 < y < -1$$

e ciò comporta che non esistono soluzioni intere in questo intervallo.



Vale la pena notare, in definitiva, che le due soluzioni trovate sono simmetriche, potendosi scambiare i ruoli delle due variabili: si tratta di una circostanza prevedibile, dato che questa proprietà di simmetria è ben visibile nell'equazione di partenza.

Equazioni diofantee

Riprendendo la definizione, un'*equazione diofantea* è un'equazione in una o più incognite con coefficienti interi di cui si ricercano le soluzioni intere. Lo studio

delle equazioni diofantee rappresenta uno degli argomenti più difficili della moderna Matematica e talvolta, nella ricerca di una soluzione, si procede tra mille difficoltà, adottando metodi particolari, utili solo in casi speciali. L'esempio più famoso di equazione diofantea è

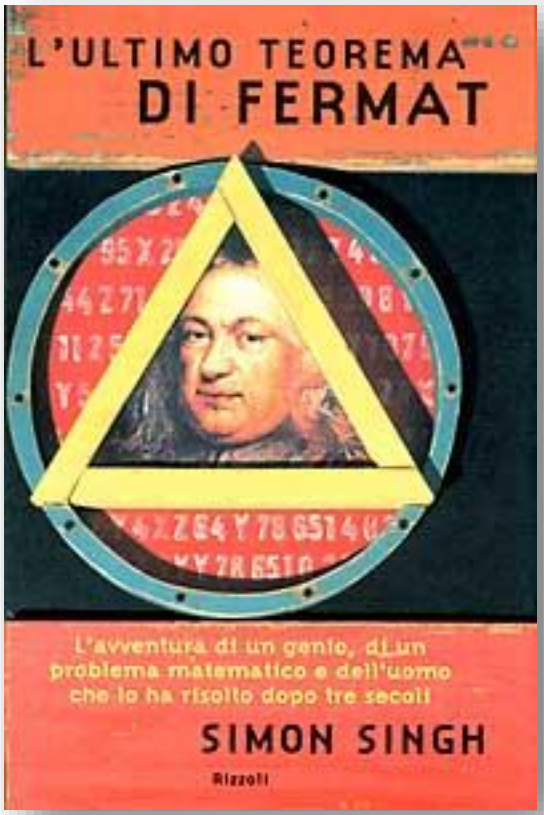
$$x^n + y^n = z^n \quad \text{con} \quad x, y, z \in \mathbb{Z}\,, \quad n \in \mathbb{N} > 2\,.$$

Si tratta di un'equazione che venne formulata da Pierre de Fermat nel 1637 e che è stata risolta dal professor Andrew Wiles soltanto nel 1994: essa presenta soltanto la soluzione banale $x = y = z = 0$.

La storia di questa equazione è durata quasi quattrocento anni e non è ancora finita, dato che si cerca una dimostrazione più semplice di quella di Wiles che è talmente complicata da essere perfettamente comprensibile, in ogni dettaglio, soltanto a pochissimi specialisti al mondo. Verso la metà del 1600, Fermat, detto il principe dei matematici dilettanti, lascia su uno dei libri della sua biblioteca un'annotazione a margine proprio dell'*Arithmetica* di Diofanto: «Ho trovato una brillante dimostrazione del fatto che $x^n + y^n = z^n$ non ha soluzioni intere per

$n > 2$». Per $n = 2$ l'equazione si riduce al ben noto teorema di Pitagora e, fin dai tempi più remoti, gli uomini hanno compilato elenchi di terne di numeri interi, come 3, 4, 5, che la verificano.

Negli anni successivi alla morte di Fermat, matematici professionisti e semplici appassionati si sono cimentati nel ricostruire la dimostrazione di Fermat, ma senza successo. Nel Novecento nessun matematico pensa più che sia utile e serio studiare ulteriormente questa congettura. Fino a qualche anno fa, quando un ragazzo dodicenne, Andrew Wiles appunto, decise di dedicare la sua vita a questo problema. Ma, dopo quaranta anni di ricerca e l'annuncio della soluzione, si scoprì che la dimostrazione da lui trovata conteneva un errore. Questa intrigante storia è magistralmente raccontata nel libro di Simon Singh *L'ultimo teorema di Fermat*, edito da Rizzoli.



Altri esempi di equazioni diofantee, certamente meno famose, sono

$$7x - 2y = 5\,,\quad x^2 - 4y^2 = 1\,,\quad xy = 6\,.$$

Soluzioni intriganti

Cercare soluzioni intere per un'equazione diofantea non è uno scherzo da matematici originali. Sono tanti i casi in cui un problema pretende di essere risolto in termini interi: non si possono, ovviamente, considerare frazioni di esseri umani, ma non si possono neanche considerare frazioni delle valute, oltre quelle ufficialmente riconosciute. Qualunque conto in euro non può che essere espresso da un numero intero di centesimi di euro. Per fare in modo che il lettore cominci ad intuire le strategie di soluzione di un'equazione diofantea, si presentano alcuni esempi risolti, per lo più basati sull'idea che un numero intero può ottenersi per fattorizzazione solo per certi valori di altri due interi. Ad esempio, un esempio concreto di fattorizzazione si ottiene determinando tutti gli interi n per $n^2 + 2$ è un quadrato, per cui basta imporre

$$n^2 + 2 = k^2 \quad \rightarrow \quad (k - n)(k + n) = 2\,.$$

Ricordando sempre di lavorare con gli interi, sussistono logicamente i casi:

1. $k - n = 1\,,\quad k + n = 2$;
2. $k - n = 2\,,\quad k + n = 1$;
3. $k - n = -1\,,\quad k + n = -2$;
4. $k - n = -2\,,\quad k + n = -1$.

Nessuna delle precedenti possibilità fornisce una soluzione intera per n, per cui si può concludere che $n^2 + 2$ non è il quadrato di alcun numero intero.

Segue un esempio che approfondisce la tecnica appena presentata.

Esempio 3 – Si determinino le soluzioni dell'equazione diofantea

$$xy - 2(x + y) = 0\,.$$

Si osservi preliminarmente che l'equazione assegnata è simmetrica, per cui il ruolo delle due variabili si può scambiare. Inoltre, le soluzioni positive della precedente equazione diofantea hanno la seguente interpretazione geometrica: determinare i lati di un rettangolo per il quale il valore numerico che esprime la misura dell'area xy è uguale a quello che esprime la misura del perimetro. Come si dimostrerà tra poche righe, vi sono dunque solo due soluzioni: il quadrato di lato 4 e il rettangolo di dimensioni 6 e 3.
Si può anzitutto riscrivere l'equazione come

$$xy - 2x - 2y = 0 \quad \rightarrow \quad x(y - 2) - 2y = 0\,.$$

Poi, si aggiunge e si sottrae quattro ad entrambi i membri, in modo che

$$x(y - 2) + 4 - 2y - 4 = 0 \quad \rightarrow \quad x(y - 2) - 2(y - 2) = 4\,,$$

da cui finalmente si ottiene la forma fattorizzata

$$(x - 2)(y - 2) = 4.$$

Dovendo i due fattori dare come prodotto quattro, si possono verificare soltanto i sei casi seguenti:

1) il primo fattore vale -4 ed il secondo vale -1;
2) entrambi i fattori valgono -2;

3) il primo fattore vale -1 ed il secondo vale -4;
4) il primo fattore vale 1 ed il secondo vale 4;
5) entrambi i fattori valgono 2;
6) il primo fattore vale 4 ed il secondo vale 1.

Da quanto detto, discendono le soluzioni riassunte nella tabella che segue.

$x-2$	$y-2$	x	y
-4	-1	-2	1
-2	-2	0	0
-1	-4	1	-2
1	4	3	6
2	2	4	4
4	1	6	3

Il metodo esposto in questo esempio è del tutto generale e viene detto metodo della fattorizzazione, proprio perché consiste nel fattorizzare uno dei due membri dell'equazione, e, nei casi in cui si riesce ad applicare, fornisce in maniera piana, elegante ed elementare tutte le soluzioni intere dell'equazione assegnata.

L'esempio che segue, invece, illustra una tecnica di soluzione un pochino diversa dalla fattorizzazione appena discussa, ma sempre capace di ricercare soluzioni tra gli interi: essa consiste nella delimitazione di una delle due variabili in un intervallo di ampiezza piccola, possibilmente minore di due, in modo tale che le possibili scelte di una delle variabili siano limitate e di numero poco elevato. Quando si è in presenza di pochi casi, la cosa più semplice da fare è enumerarli e poi di studiarli uno alla volta. Un esempio chiarirà in maniera questa nuova tecnica di soluzione, fornendo, tra le altre cose, anche la procedura generale per applicarla.

Esempio 4 – Si provi che l'equazione diofantea

$$y^3 = x(x+1)(x+2)$$

non ha soluzioni costituite da interi positivi.

Indicato con $x \in \mathbb{Z} > 0$ un generico numero intero positivo, dato che

$$x^3 < x(x+1)(x+2) < (x+2)^3 ,$$

si può scrivere la catena di disuguaglianze

$$x^3 < y^3 < (x+2)^3 .$$

Da essa, estraendo la radice cubica, discende che

$$x < y < x+2 .$$

Ora, dovendo essere y un numero intero, deve per forza risultare

$$y = x+1$$

e l'equazione data diventa equivalente a

$$y^3 = (x+1)^3 = x(x+1)(x+2) \quad \rightarrow \quad x^2 + 2x + 1 = x^2 + 2x .$$

Dato che questa equazione di secondo grado in x non ha soluzioni, allora si può concludere che nemmeno la diofantea ne ha, cioè la tesi desiderata.

Segue ora un'equazione in tre variabili, che ha sicuramente una complessità superiore rispetto ad una in due variabili. Tuttavia, con qualche piccola accortezza, il metodo della fattorizzazione fornirà la soluzione.

Esempio 5 – Si dimostri che l'equazione diofantea

$$x^2 + y^2 = 3 + z^2$$

ha infinite soluzioni.

Dovendo solo provare che esistono infinite soluzioni, si comincia a scrivere che

$$x^2 - 3 = z^2 - y^2 = (z - y)(z + y)$$

e si pone, ad esempio,

$$z + y = x^2 - 3\,, \quad \mathrm{z} - \mathrm{y} = 1\,,$$

con la consapevolezza che le soluzioni di questo sistema sono da considerare soltanto come una parte dell'insieme di tutte le soluzioni. Procedendo su questa linea, si ottiene

$$y = \frac{x^2 - 4}{2}\,, \quad z = \frac{x^2 - 2}{2}\,.$$

Appare evidente che, se si sceglie x tra i numeri pari

$$x = 2n \quad \text{con} \quad n \in \mathbb{Z}\,,$$

è possibile effettivamente ottenere infinite le soluzioni intere

$$y = 2n^2 - 2\,,\quad z = 2n^2 - 1\,.$$

Più difficile è trattare i casi in cui che le soluzioni non esistono, come suggerisce l'esempio che segue.

Esempio 6 – Si dimostri che l'equazione

$$x^2 - 10y^2 = 2$$

non ha soluzioni in $\mathbb{Z}$.

Riscrivendo l'equazione come

$$x^2 = 2 + 10y^2\,,$$

si capisce immediatamente che, dovendo essere il secondo membro pari, deve necessariamente essere

$$x = 2n \quad \text{con} \quad n \in \mathbb{Z}\,.$$

Sostituendo e dividendo per due, si ottiene

$$2n^2 = 1 + 5y^2\,,$$

da cui si deduce che, essendo il primo membro pari, anche il secondo deve esserlo. Ciò implica che y deve essere dispari, cioè

$$y = 2m + 1 \quad \text{con} \quad m \in \mathbb{Z}\,.$$

Sostituendo di nuovo nell'equazione, risulta

$$2n^2 = 1 + 5(2m+1)^2 \quad \rightarrow \quad n^2 = 3 + 10m^2 + 10m\,.$$

L'ultima equazione scritta impone che n sia dispari, per cui

$$n = 2p + 1 \quad \text{con} \quad p \in \mathbb{Z}\,,$$

si può scrivere

$$4p^2 + 4p + 1 = 3 + 10m(m+1) \quad \rightarrow \quad 2p^2 + 2p - 5m(m+1) = 1\,.$$

Ebbene, si è giunti finalmente ad una contraddizione: dato che il prodotto $m(m+1)$ è sempre divisibile per due, si può dire che il primo membro è divisibile per due, mentre il secondo non lo è. Si scioglie l'assurdo, ammettendo che l'equazione assegnata non abbia soluzioni.

Terne pitagoriche

È ben noto che in un triangolo rettangolo di cateti a, b e di ipotenusa c si ha

$$a^2 + b^2 = c^2$$

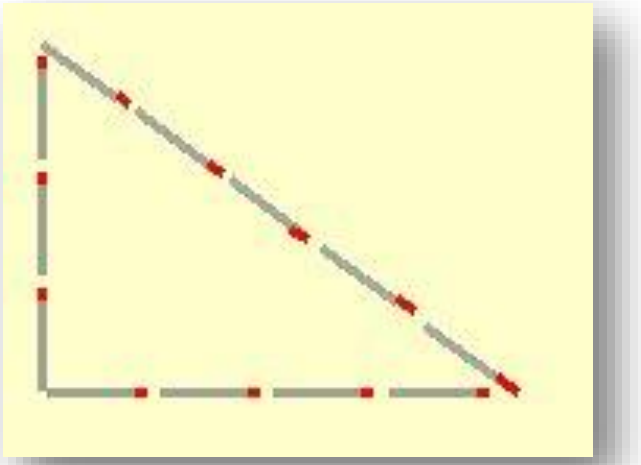
Ad esempio, la terna

$$a = 3\,, \quad b = 4\,, \quad c = 5 \quad \rightarrow \quad 3^2 + 4^2 = 5^2$$

è una terna pitagorica e lo sono anche le infinite terne

$$a_k = 3k\,,\quad b_k = 4k\,,\quad c_k = 5k \quad \text{con} \quad k \in \mathbb{N}\,.$$

Esistono dunque infinite terne di numeri interi che soddisfano questa relazione.



Ebbene, la ricerca delle terne pitagoriche coincide con la soluzione di un'equazione diofantea che, come già accennato, presenta infinite soluzioni.
C'è una famosa tavoletta del periodo paleo-babilonese, nota come *Plimpton 322*, che dimostra come il problema aritmetico, collegato a quello geometrico del teorema di Pitagora, fosse già noto ben prima dei greci.
Questa tavoletta era originariamente molto più grande, ma la parte conservata permette ancora di interpretare correttamente il significato delle colonne di numeri che presenta: oggi resta una tavoletta di argilla, parzialmente scheggiata, larga circa 13 *cm*, alta 9 *cm* ed avente uno spessore di 2 *cm*. L'editore newyorkese George Arthur Plimpton la comprò dall'antiquario Edgar James Banks nel 1922 circa e la lasciò in eredità, con tutta la sua collezione, alla *Columbia University* a

metà degli anni trenta. Secondo Banks, la tavoletta viene da Senkereh, un sito nel sud dell'Iraq, corrispondente all'antica città babilonese di Larsa.

Si ritiene che la tavoletta sia stata scritta intorno al 1800 $a.C.$, basandosi anche sullo stile della scrittura cuneiforme. Il contenuto principale di *Plimpton 322* è una tabella di numeri, con quattro colonne e quindici righe, in notazione sessagesimale babilonese. La quarta colonna è semplicemente una lista di numeri da 1 a 15. La seconda e terza colonna sono completamente visibili nella tavoletta residua.

Purtroppo, l'angolo che comprende la prima colonna è scheggiato ed esistono due ipotesi verosimili su quali potrebbero essere i numeri mancanti. Secondo una attenibile interpretazione, la tabella non è altro che una lista di terne pitagoriche, i cui numeri sono le soluzioni del teorema di Pitagora.

Lo studio delle terne babilonesi conferma la conoscenza da parte loro delle formule fondamentali per la costruzione delle terne stesse. Sono formule che tradizionalmente vengono attribuite a Diofanto, che negli *Arithmetica* raccolse 189 problemi risolti, applicando diversi metodi che rivelano la sua straordinaria abilità.

Le formule delle terne pitagoriche, comunque, sono molto semplici: limitando la ricerca a quelle che si chiamano *terne primitive*, cioè quelle terne con a e b primi fra loro, dati due numeri interi qualsiasi m e n, con $m > n$, si ha

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

È facile verificare che vale il teorema di Pitagora

$$a^2 + b^2 = m^4 + n^4 - 2m^2n^2 + 4m^2n^2 = c^2 \,.$$

Se si prende per m un valore qualsiasi e $n = 1$, si otterranno delle terne pitagoriche per le quali la differenza fra l'ipotenusa e il cateto maggiore sarà sempre pari a

$$a = m^2 - 1 \,, \quad b = 2m \,, \quad c = m^2 + 1 \quad \rightarrow \quad c - a = 2 \,.$$

Ad esempio, posto m=6 e n=1, si ha la terna 35, 12 e 37.

Si osserva ancora che, in generale, la differenza fra il numero più grande e quello più piccolo della terna è uguale al quadrato della differenza fra i due numeri generatori

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

Ad esempio, posto $m = 5$ e $n = 2$, si ottiene la terna $21, 20$ e 29 e, dato che la differenza fra i due numeri generatori $m - n = 3$, si ha che numeri $c - b = 9$.
La somma fra il numero più grande della terna e quello più piccolo è invece uguale al quadrato della somma dei due numeri generatori

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

Nell'esempio precedente si ha $m + n = 5 + 2 = 7$ e la somma dei due numeri è $29 + 20 = 49 = 7^2$.

Esempio 7 – Si dimostri che non esiste alcuna terna pitagorica in cui a e b siano entrambi dispari.

Si supponga che a e b siano entrambi dispari, cioè sia

$$a = 2n + 1\,,\quad b = 2m + 1 \quad \text{con} \quad n, m \in \mathbb{N}\,.$$

Allora, deve essere

$$c^2 = 4n^2 + 4m^2 + 4n + 4m + 2 = 2(2n^2 + 2m^2 + 2n + 2m + 1)\,,$$

vale a dire che c^2 è il doppio di un numero dispari. Ciò non è possibile, poiché se si immagina che c sia un numero pari $c = 2k$ con $k \in \mathbb{N}$, allora

$$2k^2 = 2n^2 + 2m^2 + 2n + 2m + 1\,,$$

vale a dire al primo membro compare un numero pari, mentre al secondo membro è presente un dispari. Provi l'attento lettore a completare la dimostrazione mostrando che a e b non possono essere entrambi pari.

Si passerà nei prossimi paragrafi allo studio delle equazioni diofantee lineari, per la soluzione delle quali esistono sostanzialmente due tecniche: un metodo dovuto al grande Leonardo Eulero e quello detto delle divisioni successive. Essi rappresentano la parte centrale di ciò che si va dicendo e verranno presentati di qui a poco. Prima di illustrarle, tuttavia, è indispensabile mostrare un algoritmo per la ricerca del massimo comun divisore tra interi.

Algoritmo per il massimo comun divisore

Non è sempre agevole determinare il massimo comun divisore tra due interi. La via più agevole è probabilmente quella indicata dall'algoritmo di Euclide delle divisioni successive, anche dette *divisioni iterate*.

Siano dati, ad esempio, i due numeri interi $a = 40278$ e $b = 8494$. Si comincia ad eseguire la divisione intera, quella con il resto, tra il dividendo a ed il divisore b, ottenendo un quoziente ed un resto; si proceda poi dividendo il divisore per il resto, fin quando non si ottiene un resto nullo. Nel caso in esame, si ottengono i risultati di seguito riportati.

1	$40278 = 8494 \cdot 4 + 6302$
2	$8494 = 6302 \cdot 1 + 2192$
3	$6302 = 2192 \cdot 2 + 1918$
4	$2192 = 1918 \cdot 1 + 274$
5	$1918 = 274 \cdot 7 + 0$

Il massimo comun divisore tra 40278 e 8494 è l'ultimo resto non nullo nel processo delle divisioni iterate, cioè 274.

Una volta compreso l'algoritmo euclideo per la ricerca del massimo comun divisore tra interi, si passa a presentare un'identità, dovuta al matematico francese Étienne Bézout (Nemours, 31 marzo 1730 – Avon, 27 settembre 1783),

secondo cui, se a e b sono interi, non entrambi nulli, ed il loro massimo comune divisore è d, esistono due interi n e m, per cui risulta

$$an + bm = d\,.$$

Ad esempio, il massimo comun divisore tra $a = 12$ e $b = 46$ è pari a $d = 2$, come prova la tabella di seguito riportata.

1	$46 = 12 \cdot 3 + 10$
2	$12 = 10 \cdot 1 + 2$
3	$10 = 2 \cdot 5 + 0$

Per determinare una coppia di interi che verifichi l'identità di Bézout, si può partire dal massimo comun divisore e procedere a ritroso, ricavando nelle varie righe il resto, per cui

$$2 = 12 - 10 \cdot 1 = 12 - 46 + 12 \cdot 3 = 12 \cdot 4 - 46 \quad \rightarrow \quad n = 4\,,\ \ m = -1\,.$$

Tuttavia, è opportuno segnalare che la coppia di interi (n, m) trovata non è univocamente determinata, dato che, ad esempio, risulta ugualmente

$$12 \cdot 27 - 46 \cdot 7 = 2 \quad \rightarrow \quad n = 27\,,\ \ m = -7\,.$$

In effetti, come si avrà modo di discutere in maggior dettaglio nel seguito, a partire da una qualsiasi soluzione (n_0, m_0), si dimostra che l'insieme delle soluzioni è costituito da coppie del tipo

$$n_k = n_0 - k\frac{b}{d}\,,\ \ m_k = m_0 + k\frac{a}{d} \quad \text{con} \quad k \in \mathbb{Z}\,.$$

È immediato verificare che

$$an_k + bm_k = d \quad \forall k \in \mathbb{Z}\,.$$

Sostituendo, infatti, si può agevolmente scrivere

$$an_k + bm_k = an_0 - \frac{ab}{d}k + bm_0 + \frac{ab}{d}k = d \quad \forall k \in \mathbb{Z}\,.$$

Questa stessa proprietà si può estendere ad un insieme arbitrario di numeri: dati r interi $(a_1, a_2, \cdots, a_r)$, se d è il loro massimo comun divisore esiste una r −upla di interi $(n_1, n_2, \cdots, n_r)$, per cui

$$a_1 n_1 + a_2 n_2 + \cdots + a_r n_r = d\,.$$

Equazioni diofantee lineari

Un'equazione diofantea lineare in due variabili è un'equazione della forma

$$ax + by = c\,,$$

con a, b, c numeri interi. Lo scopo è ovviamente quello di cercare soluzioni intere dell'equazione assegnata. Nell'*Aryabhatiya*, un compendio delle conoscenze matematiche del tempo, scritto dal matematico, astronomo ed astrologo indiano Aryabhata attorno al 500 dopo Cristo, compare un algoritmo per risolvere un'equazione diofantea lineare.
Vale la pena sottolineare subito che non sempre un'equazione lineare ammette soluzioni *intere*. Ad esempio, l'equazione

$$2x + 4y = 5$$

non ha soluzioni intere, dato che il primo membro, qualunque siano i valori interi dati a x e y, fornisce un numero pari che, quindi non potrà mai coincidere con il secondo membro che è un numero dispari. Per contro, un'equazione lineare in due variabili ammette sempre infinite soluzioni *reali*, che possono essere interpretate come gli infiniti punti di una retta.

Detto, allora, $d = MCD(a, b)$ il massimo comun divisore tra gli interi a e b, sussiste il seguente teorema: condizione necessaria e sufficiente affinché l'equazione $ax + by = c$ abbia soluzioni intere è che il termine noto c sia divisibile per d.

Ad esempio, l'equazione diofantea

$$2x + 6y = 7$$

non ammette alcuna soluzione, dato che il secondo membro non è divisibile per il $MCD(2, 6) = 2$. Per contro, l'equazione diofantea

$$x - 5y = 4$$

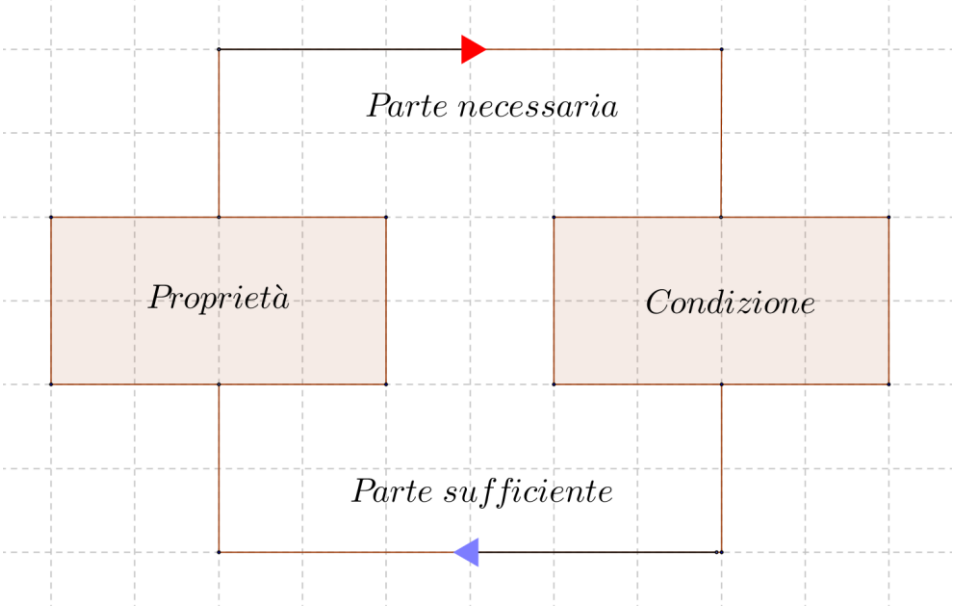
ammette soluzioni, essendo il secondo membro divisibile per

$$1 = MCD(1, -5)\ .$$

Lo schema logico di un teorema, che si strutturi in una parte necessaria ed in una parte sufficiente, è riportato nella figura che segue. Si dimostra la parte necessaria quando, ponendo per ipotesi la proprietà in discussione, si vuole dimostrare la condizione che la caratterizza. Al contrario, quando si pone per ipotesi la condizione e per tesi la proprietà, si sta dimostrando la parte sufficiente.

Nel caso in esame si può dire che

$$\begin{array}{lcl} \text{proprietà} & \rightleftharpoons & ax + by = c \text{ abbia soluzioni ,} \\ \text{condizione} & \leftrightharpoons & \text{il termine noto } c \text{ è divisibile per } d \text{ .} \end{array}$$



Si comincia tradizionalmente dalla parte necessaria, essendo questa più semplice, nella maggior parte dei casi.

Parte necessaria

$$\begin{cases} \text{IPOTESI: l'equazione } ax + by = c \text{ ammette soluzioni intere .} \\ \text{TESI: il termine noto } c \text{ è divisibile per } d = MCD(a, b) \text{ .} \end{cases}$$

Si supponga che l'equazione $ax + by = c$ abbia soluzioni intere e si indichi una di esse con la coppia (x_0, y_0), per cui risulta

$$ax_0 + by_0 = c \text{ .}$$

Siccome si sa che $d = MCD(a, b)$, allora si può scrivere che $a = nd$ e $b = md$ con $n, m \in \mathbb{Z}$. Sostituendo nell'equazione, si nota che il primo membro è divisibile per d, per cui anche il secondo membro c deve essere divisibile per d, in modo che

$$(nx_0 + my_0)d = c \quad \rightarrow \quad nx_0 + my_0 = \frac{c}{d}.$$

Da ciò segue che il rapporto al secondo membro

$$\frac{c}{d} = \frac{\text{termine noto}}{MCD(a, b)}$$

è un numero intero, dato che tale è il primo membro, e, quindi, il termine noto c è divisibile per d, come si voleva dimostrare.

La seconda parte della dimostrazione è la parte sufficiente, che si ottiene scambiando l'ipotesi con la tesi della parte necessaria.

Parte sufficiente

$$\begin{cases} \text{IPOTESI: il termine noto } c \text{ è divisibile per } d = MCD(a, b). \\ \text{TESI: l'equazione } ax + by = c \text{ ammette soluzioni intere.} \end{cases}$$

Per l'identità di Bézout devono esistere due interi p, q, per cui

$$ap + bq = d\,.$$

Dato che, per ipotesi, c è divisibile per d, allora deve esistere un intero k, per cui si può porre $c = kd$. Moltiplicando la precedente relazione per k, si ottiene

$$akp + bkq = kd = c\,.$$

Ciò vuol dire che la coppia

$$x_0 = kp\,,\ \ y_0 = kq\,,$$

rappresenta una soluzione dell'equazione diofantea assegnata.

Un esempio chiarirà meglio come si applichi il risultato espresso dal teorema appena dimostrato.

Esempio 8 – Si verifichi che l'equazione diofantea

$$x - 5y = 4$$

ammette le infinite soluzioni

$$x = 9 - 5k\,,\ \ y = 1 - k \ \ \text{con} \ \ k \in \mathbb{Z}\,.$$

Basta sostituire nell'equazione assegnata, per ottenere

$$9 - 5k - 5(1 - k) = 9 - 5k - 5 + 5k = 4 \ \ \forall k \in \mathbb{Z}\,.$$

A questo punto della trattazione, si può passare ad illustrare le due principali tecniche per la determinazione, qualora esistano, delle soluzioni di un'equazione diofantea lineare e si comincerà proprio con un metodo dovuto al grande Leonardo Eulero.

Metodo di Eulero

Si supponga di volere risolvere l'equazione diofantea

$$7x + 3y = 53\,.$$

Dato che il termine noto è divisibile per il $MCD(7,3) = 1$, essa ammette soluzioni. Queste saranno determinate con un metodo dovuto ad Eulero, la cui procedura è molto semplice ed inizia con la scelta del più piccolo coefficiente, in valore assoluto, tra a e b. Nel caso in esame è quello della y, per cui si esplicita l'equazione rispetto a questa variabile

$$7x + 3y = 53 \quad \rightarrow \quad y = \frac{53 - 7x}{3}\,.$$

Eseguendo la divisione al secondo membro, si ottiene

$$y = \frac{53 - 7x}{3} = \frac{51 - 6x + 2 - x}{3} = 17 - 2x + \frac{2 - x}{3}.$$

Per ottenere una soluzione intera, bisogna imporre che il resto sia un numero intero, per cui

$$\frac{2 - x}{3} = k \quad \rightarrow \quad x = 2 - 3k \quad \text{con} \quad k \in \mathbb{Z}.$$

Sostituendo nella y il valore di x appena trovato, in una sola iterazione, si ottengono le soluzioni dell'equazione proposta

$$x = 2 - 3k\,, \quad y = 17 - 2(2 - 3k) + k = 13 + 7k \quad \text{con} \quad k \in \mathbb{Z}.$$

Quale che sia il valore di k, purché intero, si ottiene una delle infinite soluzioni intere del problema assegnato.
Eulero propose questo metodo iterativo, moderno e stimolante, nella sua *Algebra*, scritta in tedesco e stampata per la prima volta, in traduzione russa, nel 1768 a San Pietroburgo.
Vale la pena osservare che non è sempre così immediato applicare questo metodo e talvolta sono richieste diverse iterazioni, come illustra l'esempio che segue.

Esempio 9 – Si determinino le soluzioni dell'equazione diofantea

$$8x + 5y = 81\,.$$

Dato che il $MCD(8, 5) = 1$, l'equazione data ammette soluzione e si comincia al esplicitarla rispetto alla variabile con il minore, in valore assoluto, coefficiente tra x e y, in questo caso y, ottenendo

$$y = \frac{81 - 8x}{5}.$$

Si dividano ora per 5 i numeri 81 e 8, mettendo in evidenza i resti

$$y = 16 - x + \frac{1 - 3x}{5}.$$

Si ponga poi

$$t = \frac{1 - 3x}{5} \quad \rightarrow \quad y = 16 - x + t \quad \text{con} \quad t \in \mathbb{Z},$$

vale a scrivere

$$3x + 5t = 1.$$

Si noti che, essendo x e y due numeri interi, allora tale è anche t e, pertanto, si può dire che si è ottenuto un'equazione diofantea, i cui coefficienti sono minori di quelli dell'equazione di partenza. L'idea base del metodo euleriano è tutta qui: le soluzioni (x, y) dell'equazione assegnata sono ricavabili immediatamente dalle soluzioni di una nuova equazione diofantea con i coefficienti più piccoli rispetto a quella considerata in origine.

Il procedimento ora introdotto può evidentemente essere iterato. Proseguendo con l'esempio, si risolva l'equazione ottenuta nella variabile avente il minore coefficiente in valore assoluto, stavolta x,

$$x = \frac{1 - 5t}{3} = -t + \frac{1 - 2t}{3}.$$

Posto allora

$$u = \frac{1-2t}{3} \quad \rightarrow \quad x = -t + u \quad \text{con} \quad u \in \mathbb{Z}\,,$$

si ottiene la nuova diofantea

$$3u + 2t = 1\,.$$

Anche quest'equazione ha i coefficienti più piccoli rispetto a quella del passo precedente e, continuando ad iterare, si ricava

$$t = \frac{1-3u}{2} = -u + \frac{1-u}{2}\,,$$

da cui discende la nuova posizione

$$k = \frac{1-u}{2} \quad \rightarrow \quad u = 1 - 2k \quad \text{con} \quad k \in \mathbb{Z}\,.$$

Sostituendo a cascata, si perviene alla soluzione

$$x = 2 - 5k\,, \quad y = 13 + 8k\,.$$

Questa equazione presenta infinite soluzioni, alcune delle quali sono riportate nella tabella che segue.

k	$\cdots$	-2	-1	0	1	2	$\cdots$
x	$\cdots$	12	7	2	-3	-8	$\cdots$
y	$\cdots$	-3	5	13	21	29	$\cdots$

Tuttavia, se all'equazione data si fosse associata la condizione di non negatività per x e y, una condizione non rara nelle situazioni applicative, si sarebbe dovuto risolvere il sistema di disequazioni

$$\begin{cases} 2-5k \geq 0\,, \\ 13+8k \geq 0\,, \end{cases} \quad \rightarrow \quad -\frac{13}{8} \leq k \leq \frac{2}{5} \quad \rightarrow \quad k=-1 \ \wedge \ k=0\,.$$

La tabella che segue riassume in forma schematica le soluzioni in questo secondo caso.

k	-1	0
x	7	2
y	5	13

Metodo delle divisioni successive

Sia data l'equazione lineare diofantea

$$ax+by=c$$

e sia c divisibile per $d=MCD(a,b)$. Allora, l'equazione data ha infinite soluzioni, tutte e sole esprimibili per mezzo delle relazioni

$$x=x_p+kb\,, \quad y=y_p-ka \quad \text{con} \quad k\in\mathbb{Z}\,,$$

dove la coppia (x_p,y_p) rappresenta una soluzione particolare.

↦ Si comincia col mostrare che la soluzione fornita soddisfa l'equazione diofantea. Sostituendo si può scrivere facilmente

$$a(x_p + kb) + b(y_p - ka) = ax_p + by_p = c\,.$$

↦ Viceversa, supponendo che (x_p, y_p) sia una soluzione dell'equazione diofantea, allora per qualsiasi altra soluzione (x, y) deve verificarsi che

$$ax + by = c = ax_p + by_p\,,$$

ovvero, posto $a = d\alpha$ e $b = d\beta$ con $MCD(\alpha, \beta) = 1$, si può scrivere

$$\alpha(x - x_p) = \beta(y_p - y)\,.$$

Questa ultima uguaglianza comporta che $y_p - y$ deve essere divisibile per α e che $x - x_p$ deve essere divisibile per β, vale a dire che deve esistere un intero m per cui risulta

$$\frac{x - x_p}{\beta} = m = \frac{y_p - y}{\alpha} \quad \rightarrow \quad \begin{cases} x = x_p + m\beta\,, \\ y = y_p - m\alpha\,. \end{cases}$$

Senza perdere in generalità, si può porre $m = kd$ ed ottenere la soluzione desiderata

$$x = x_p + kb\,, \;\; y = y_p - ka \;\; \text{con} \;\; k \in \mathbb{Z}\,.$$

Si osservi che i due termini kb e $-ka$ rappresentano tutte le infinite soluzioni dell'equazione omogenea, cioè quella avente il termine noto nullo, per cui il teorema appena dimostrato si può anche enunciare dicendo che la soluzione di

un'equazione diofantea lineare si ottiene sommando una qualsiasi soluzione dell'equazione completa alle infinite soluzioni dell'equazione omogenea.
Si propone ora un semplice esempio per applicare la formula risolutiva trovata.

Esempio 10 – Si risolva l'equazione diofantea

$$2x + 3y = 5\,.$$

Dato che il termine noto è divisibile per il $MCD(2,3) = 1$, si può dire che l'equazione data ammette soluzione. Inoltre, dato che la coppia

$$x_p = 1\,,\ \ y_p = 1$$

è una soluzione particolare, si conclude che la soluzione generale vale

$$x = 1 + 3k\,,\ \ y = 1 - 2k \quad \text{con} \quad k \in \mathbb{Z}\,.$$

Nell'esempio appena svolto è stato piuttosto semplice trovare una soluzione particolare (x_p, y_p): in generale, potrebbe non essere così semplice ed allora bisogna ricorrere all'identità di Bézout. Si consideri, ad esempio, l'equazione

$$11x + 8y = 3\,.$$

Dato che il termine noto $c = 3$ è divisibile per il $MCD(11,8) = 1$, essa ammette soluzioni, che valgono

$$x = x_p + 8k\,,\ \ y = y_p - 11k \quad \text{con} \quad k \in \mathbb{Z}\,.$$

Si deve determinare soltanto un integrale particolare (x_p, y_p). Posto allora $a = 11$ e $b = 8$, eseguendo le divisioni iterate, si costruisce la tabella di seguito riportata.

1	$11 = 8 \cdot 1 + 3$
2	$8 = 3 \cdot 2 + 2$
3	$3 = 2 \cdot 1 + 1$
4	$2 = 2 \cdot 1 + 0$

Da essa, procedendo a ritroso, si determina l'integrale particolare desiderato, dato che

- dalla terza riga si ricava che $1 = 3 - 2$,
- dalla seconda riga di scende che $1 = 3 - (8 - 3 \cdot 2)$,
- dalla prima riga si conclude che $1 = 11 - 8 - [8 - (11 - 8) \cdot 2]$.

Elaborando quest'ultima relazione, si può scrivere

$$1 = 11 \cdot 3 + 8 \cdot (-4)\,,$$

per cui, moltiplicando membro a membro per $c = 3$, si ottiene

$$3 = 11 \cdot 9 + 8 \cdot (-12)$$

e concludere che una soluzione particolare vale

$$x_p = 9\,, \quad y_p = -12\,.$$

Ancora un esempio, che mette in luce un diverso aspetto delle equazioni diofantee: le soluzioni possono essere in numero limitato, per la presenza di una limitazione nella ricerca delle stesse.

Esempio 11 – Si determini il più grande numero naturale $s < 100$, per il quale l'equazione diofantea

$$8x + 12y = s$$

ammette soluzione e risolverla.

Come è ben noto, un'equazione diofantea ammette soluzione se e solo se il massimo comun divisore tra i coefficienti delle incognite divide il termine noto. Nel caso in esame, dato che

$$MCD(8, 12) = 4\,,$$

si può dire che il più grande numero naturale minore di 100, divisibile per 4, è il numero 96. L'equazione diofantea, pertanto, diventa

$$8x + 12y = 96 \quad \rightarrow \quad 2x + 3y = 24$$

e, poiché una soluzione particolare è costituita dalla coppia

$$x_0 = 12\,, \;\; y_0 = 0\,,$$

si può concludere che la soluzione generale vale

$$x = 12 - 3k\,, \;\; y = 2k \;\; \text{con} \;\; k \in \mathbb{Z}\,.$$

Seguono ora due interessanti esercizi, che rappresentano situazioni concrete in cui è possibile applicare le tecniche di soluzione appena apprese e che mostrano la varietà di situazioni da cui possono scaturire equazioni diofantee.

Esempio 12 – Su un foglio di carta illimitato sono segnati due punti A e B. Si disponga di tre righe prive di suddivisioni, una lunga 8 cm, l'altra lunga 11 cm, la terza illimitata; dire con quale precisione si può misurare la distanza dei due punti A e B.

La prima cosa da fare è passare la linea illimitata per A e B, in modo che possa diventare un riferimento per tutte le successive misure. Poi, partendo da A, si possono riportare i due segmenti di 8 cm e 11 cm, ciascuno un certo numero di volte sia avanti che dietro. Pertanto, le distanze D che si riescono a misurare, espresse sempre in centimetri, sono riconducibili alla combinazione lineare

$$D = 8n + 11m \quad \text{con} \quad n, m \in \mathbb{Z}\,,$$

che rappresenta geometricamente punti posti su un piano nello spazio (n, m, D). Dunque, n e m sono due interi relativi e, per come è stata definita, anche la distanza D è espressa da un numero intero non negativo. Pertanto, si presentano due casi possibili, schematicamente discussi di seguito.

α Qualora la distanza da misurare $D = AB$ coincidesse con un valore intero, allora si potrebbe misurare con esattezza, vale a dire con un errore di misura nullo, scegliendo tra gli infiniti interi

$$n = -4D - 11h\,, \quad m = 3D + 8h\,, \quad \text{essendo } h \in \mathbb{Z}\,.$$

β Se invece la distanza da misurare fosse espressa da un numero reale, potendosi comunque porre nella forma $D = D_0 \pm \alpha$, con D_0 intero positivo e α numero reale positivo, pari al massimo a $1/2$, per quando detto al punto precedente, si conclude che la massima precisione ottenibile è unitaria.

Esempio 13 – Due cercatori d'oro hanno due grandi sacchi di pezzi d'oro. Il primo ha solo pezzi da *15 grammi*, il secondo pezzi da *21 grammi*. Può il primo pagare esattamente al secondo un debito di *27 grammi* d'oro? Potrebbe invece il secondo pagare esattamente al primo un debito di *29 grammi* d'oro?

L'equazione lineare

$$15x + 21y = 27 \quad \rightarrow \quad 5x + 7y = 9$$

ammette infinite soluzioni, dato che $MCD(15, 21) = 3$, e sono, come si può controllare per verifica diretta, pari a

$$x = 6 + 7n\,, \quad y = -3 - 5n \quad \text{con} \quad n \in \mathbb{Z}\,.$$

Pertanto, il primo cercatore può pagare al secondo il debito di 27 *grammi* di oro, dandogli sei suoi pezzi e ricevendone in cambio tre, dal momento che

$$15 \cdot 6 - 21 \cdot 3 = 27\,.$$

Nel secondo caso, l'equazione lineare

$$15x + 21y = 29$$

non ammette soluzioni intere, dato che il termine noto $c = 29$ non è divisibile per $MCD(15, 21) = 3$.

È possibile generalizzare la tecnica presentata all'equazione

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c\ ,$$

con $a_i, c \in \mathbb{Z}$. Detta omogenea associata l'equazione

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$$

e tenuto conto che si cercano le soluzioni in $\mathbb{Z}$, è possibile dimostrare che, se questa equazione ammette una soluzione $(x_{10}, x_{20}, \cdots, x_{n0})$, allora ne ammette infinite: basta, infatti, verificare per sostituzione che anche $(kx_{10}, kx_{20}, \cdots, kx_{n0})$ è soluzione $\forall k \in \mathbb{Z}$. Se esiste una soluzione dell'equazione completa, ne esistono infinite, dato che tutte le soluzioni della completa si ottengono sommando ad una sua particolare soluzione una qualsiasi soluzione della omogenea.
Vale il seguente *teorema* che qui si riporta senza dimostrazione: se il termine noto c è divisibile per

$$d = MCD(a_1, a_2, \cdots, a_n,)\ ,$$

allora l'equazione completa ammette soluzioni.

Esempio 14 – Si risolva l'equazione diofantea lineare in tre variabili

$$12x + 45y + 20z = 20\ .$$

Si osserva anzitutto che l'equazione ammette infinite soluzioni, dato che il termine noto è divisibile per

$$MCD(12, 45, 20) = 1 .$$

La soluzione generale dell'equazione omogenea

$$12x_0 + 45y_0 + 20z_0 = 0$$

si ottiene facilmente, ponendo $y_0 = 4k$ con $k \in \mathbb{Z}$, di modo che

$$3x_0 + 5z_0 = -45k .$$

Si ottiene, allora,

$$x_0 = -15k - 5h , \quad y_0 = 4k , \quad z_0 = 3h \quad \text{con} \quad h, k \in \mathbb{Z} .$$

Inoltre, dato che una soluzione particolare dell'equazione completa è pari a

$$x_p = 0 , \quad y_p = 0 , \quad z_p = 1 ,$$

si ottiene la soluzione dell'equazione completa

$$x = -15k - 5h , \quad y = 4k , \quad z = 1 + 3h \quad \text{con} \quad h, k \in \mathbb{Z} .$$

Equazioni diofantee di secondo grado

Si consideri l'equazione diofantea

$$x^2 + (x+2)y - 2x - 4 = 0\,.$$

Si tratta di un'equazione di secondo grado di tipo particolare, in quanto un'incognita, nell'esempio la y, compare soltanto al primo grado. È possibile allora ricavare la y in funzione della x mediante una formula che non faccia comparire radici quadrate, come accadrebbe invece se l'equazione fosse di secondo grado anche rispetto alla y. Operando la divisione tra polinomi, risulta

$$y = \frac{-x^2 + 2x + 4}{x+2} = 4 - x - \frac{4}{x+2} \quad \text{con} \quad x \neq -2\,.$$

Se $x = -2$, l'equazione non esplicitata non ammette soluzione. Allora, dato che x è un intero, l'espressione precedente fornisce un valore intero per y se e solamente se $x + 2$ divide 4. I divisori di 4 sono

$$\pm 1\,, \quad \pm 2\,, \quad \pm 4\,.$$

Ad essi corrispondono i valori di x

$$x = -2 \pm 1\,, \quad x = -2 \pm 2\,, \quad x = -2 \pm 4$$

e le soluzioni dell'equazione diofantea riassunte nella tabella che segue.

x	-6	-4	-3	-1	0	2
y	11	10	11	1	2	1

Esempio 15 – Si risolva l'equazione diofantea

$$(x+1)(y+1) = 2xy\,.$$

Prima di esplicitare l'equazione, vale la pena osservare che, per $x = 1$, l'equazione fornisce la soluzione

$$2(y+1) = 4y \quad \rightarrow \quad 2y = 2 \quad \rightarrow \quad y = 1\,.$$

L'equazione assegnata, allora, si riscrive facilmente nella forma equivalente

$$y = \frac{x+1}{x-1} = 1 + \frac{2}{x-1} \quad \text{con} \quad x \neq 1\,.$$

Orbene, dato che x rappresenta un numero intero, l'espressione precedente fornisce un valore intero per y se e solamente se $x - 1$ divide 2, cioè se

$$x = 1 \pm 1\,, \quad x = 1 \pm 2\,.$$

Si noti che per l'equazione data, come si evince anche dalle soluzioni di seguito riportate in tabella, il ruolo delle due variabili si può scambiare e che la colonna riportata in rosso rappresenta una soluzione che è stata determinata prima di trasformare l'equazione in forma esplicita.

x	-1	0	1	2	3
y	0	-1	1	3	2

Punti razionali di una conica

Una conica rappresenta il luogo geometrico dei punti di un polinomio di secondo grado nelle variabili x e y. Vi sono casi degeneri in cui la conica è vuota, come può essere $x^2 + y^2 = -4$, oppure si riduce ad un solo punto, ad esempio $x^2 + y^2 = 0$,

oppure è una retta, come $x^2 = 0$, oppure l'unione di due rette, ad esempio $x(y-1) = 0$. Negli altri casi, si ottiene un'iperbole, una parabola, un'ellisse e, se i suoi assi sono uguali, si ottiene una circonferenza.

Per la ricerca dei punti razionali di una conica, si può procedere nella maniera che segue. Data, ad esempio, la circonferenza con centro nell'origine e raggio unitario

$$x^2 + y^2 = 1\,,$$

si fissa un punto razionale su di essa, come può essere esempio $(-1, 0)$, e si traccia la retta per questo punto di coefficiente angolare generico m. Questa retta intersecherà la circonferenza in un secondo punto (x, y). Ebbene, se m è un numero razionale, allora (x, y) ha coordinate razionali. Infatti, l'ascissa di questo secondo punto di intersezione è soluzione di un polinomio di secondo grado i cui coefficienti sono razionali, dipendendo dai coefficienti dell'equazione e da m. In generale, un polinomio di secondo grado con coefficienti razionali non ha radici razionali, dato che nella formula risolutiva compare una radice quadrata. In questo caso però è noto che $x = -1$ è una soluzione, essendo una delle due intersezioni: il polinomio in questione è allora divisibile per $x + 1$. Effettuando la divisione tra polinomi a coefficienti razionali, si ottiene un polinomio a coefficienti razionali di primo grado, che pertanto ha un'unica radice razionale. D'altra parte, tutti i punti razionali sulla circonferenza si trovano in questo modo. Infatti, se il punto (x, y) è un razionale sul cerchio diverso da $(-1, 0)$, allora la retta passante per questo punto e per l'altra intersezione (x, y) ha coefficiente angolare $y/(x+1)$, che è un numero razionale. Risolvendo, dunque, il sistema

$$\begin{cases} x^2 + y^2 = 1\,, \\ y = m(x+1)\,, \end{cases} \quad \rightarrow \quad (1+m^2)x^2 + 2m^2x + t^2 - 1 = 0\,,$$

si ottengono le soluzioni razionali

$$x_1 = -1\,, \quad x_2 = \frac{1-m^2}{1+m^2}\,,$$
$$y_1 = 0\,, \quad y_2 = \frac{2m}{1+m^2}\,.$$

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 qualsiasi retta passante per P ed avente coefficiente angolare razionale. Un esempio chiarirà ancor meglio quanto appena discusso.

Esempio 15 – Si determinino i punti razionali sull'iperbole di equazione

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

Fissato il punto $A(-1, 0)$, si tratta di studiare le intersezioni

$$\begin{cases} x^2 - y^2 = 1\,, \\ y = m(x+1)\,. \end{cases}$$

Risulta, dunque, che

$$x^2 - m^2(x+1)^2 = 1 \quad \rightarrow \quad (1-m^2)x^2 - 2m^2x - m^2 - 1 = 0\,.$$

È già noto che una soluzione di questa equazione vale $x_1 = -1$, come peraltro è semplice verificare. L'altra soluzione si può determinare adoperando la regola di Ruffini oppure risolvendo l'equazione di secondo grado ed è pari a

$$x_2 = \frac{1+m^2}{1-m^2}.$$

Sostituendo questo valore di x nella generica retta, si ottiene

$$y_2 = \frac{2m}{1-m^2}.$$

Si conclude che, a parte il punto $A(-1,0)$, tutti i punti razionali sull'iperbole assegnata hanno coordinate pari a

$$P\left(\frac{1+m^2}{1-m^2}, \frac{2m}{1-m^2}\right),$$

al variare di m tra tutti i numeri razionali.
Nel paragrafo che segue si presenterà lo studio di alcune equazioni diofantee non lineari, per le quali non esistono tecniche generali di soluzione.

Equazioni diofantee non lineari

Non esiste una tecnica generale per risolvere le equazioni diofantee non lineari e, per questo, nel seguito verrà mostrata soltanto qualche tecnica di soluzione, per mezzo di alcuni esempi. Forse la bellezza delle equazioni diofantee risiede proprio nel fatto che il solutore deve mostrare una notevole inventiva, quando affronta una particolare equazione, non sapendo *a priori* se esistono o meno soluzioni, se sono finite oppure infinite.

Il primo esempio consiste nello studio di un'equazione che, per semplicità, presenta solo un numero finito di soluzioni.

Esempio 16 – Si dimostri che le soluzioni intere positive dell'equazione

$$x + y + z = xyz$$

sono numeri distinti e che l'unica soluzione è costituita dalla terna 1, 2, 3.

Data la evidente simmetria dell'equazione, i ruoli delle tre variabili si possono scambiare, in modo che le tre terne

$$\begin{aligned} &x = 1\,, \quad y = 2\,, \quad z = 3\,, \\ &x = 2\,, \quad y = 3\,, \quad z = 1\,, \\ &x = 3\,, \quad y = 1\,, \quad z = 2\,, \end{aligned}$$

sono da considerarsi come un'unica soluzione. Detto ciò, si comincia a dimostrare che le soluzioni intere positive dell'equazione non possono coincidere. Se, ragionando per assurdo, esistesse una soluzione per cui $x = y = z$, allora dovrebbe essere

$$x + x + x = x^3 \quad \rightarrow \quad x_1 = 0\,, \;\; x_{2,3} = \pm\sqrt{3}\,,$$

che ammette come soluzione in $\mathbb{N}$ solo la soluzione banale. Se, invece, si fosse supposto più debolmente $x = y$, nemmeno si sarebbero avute soluzioni intere, dato che

$$2x + z = zx^2 \quad \rightarrow \quad x_{1,2} = 1 \pm \sqrt{1 + z^2}\,,$$

laddove il radicando non può mai fornire un quadrato perfetto, come si può provare con il metodo della fattorizzazione, tranne nel caso $z = 0$ che però è escluso dal testo.

Stabilito che le tre radici devono essere rappresentate da interi positivi differenti, senza perdere in generalità, si porrà $x > y > z$. In tal caso risulta

$$3x > xyz \quad \rightarrow \quad yz < 3 \, .$$

Questa ultima condizione si può verificare solamente nei seguenti due casi:

1. quando $y = z = 1$, da cui discende $x + 2 = x$, un'equazione palesemente assurda;
2. quando $y = 2$ e $z = 1$, da cui discende l'equazione $x + 3 = 2x$, che fornisce appunto la soluzione $x = 3$

Si conclude che la terna

$$x = 3 \, , \;\; y = 2 \, , \;\; z = 1 \, ,$$

rappresenta, a meno delle permutazioni possibili, l'unica soluzione del problema. Ecco un possibile problema che rappresenta l'equazione appena risolta.

Antonella e Luigi hanno tre figli. Lino, loro vecchio amico, li incontra e chiede informazioni sulle età della loro prole. Per tutta risposta, i due gli dicono che la somma delle età dei tre pargoli è uguale al loro prodotto. Al che Lino capisce che tra i tre non ci sono gemelli e che, forzatamente, essi hanno rispettivamente 1, 2 *e* 3 *anni. Come può Lino essere tanto sicuro?*

Si conclude questo esercizio con un citazione di Enrico Giusti, tratta dal libro *La Matematica in cucina*, edito da Bollati Boringhieri nel 2004:

«in Matematica, per indovinare quale sarà il risultato, tutti i mezzi sono buoni: disegno, sogno, visita alla cartomante, ma per dimostrarlo c'è solo un metodo, quello di passare logicamente dalle ipotesi (e dalle cose che si conoscono già, perché sono state dimostrate prima) alla conclusione».

Il secondo esempio presenta ancora un caso in cui sono il numero delle soluzioni possibili non è troppo elevato.

Esempio 17 - Determinare tutte le coppie (x, y) di numeri interi tali che

$$x^4 + 3x^2y^2 + 9y^4 = 12^{2006} .$$

Se si utilizzano le due nuove incognite

$$x = Na\,, \quad y = Nb \quad \text{con} \quad a, b \in \mathbb{Z}\,,$$

l'equazione assegnata diventa

$$a^4 + 3a^2b^2 + 9b^4 = \frac{3^{2006} \cdot 2^{4012}}{N^4} = 9 \cdot \left(\frac{3^{501} \cdot 2^{1003}}{N}\right)^4 .$$

Ebbene, scegliendo l'intero

$$N = 2^{1003} \cdot 3^{501}\,,$$

essa si può riscrivere nella forma equivalente

$$a^4 + 3a^2b^2 + 9b^4 = 9 \quad \rightarrow \quad a^4 + 3a^2b^2 = 9(1 - b^4)\,.$$

Osservando questa nuova equazione, si può affermare che essa è palesemente assurda nel caso $ab \neq 0$, essendo il primo membro sempre maggiore di zero, mentre il secondo è negativo, sicché

$$a^4 + 3a^2b^2 > 9(1 - b^4) \quad \forall ab \neq 0 \, .$$

Se $b = 0$, l'equazione non ammette soluzioni intere, mentre, se $a = 0$, sussistono le soluzioni intere $b = \pm 1$, vale a scrivere $y = \pm N$.

Il terzo esempio mostra una tecnica assai efficace, per dimostrare l'assenza di soluzioni. La tecnica è del tutto simile all'inchiodatura scacchistica, in cui un pezzo è costretto a non muoversi per evitare la cattura di un altro: il pezzo bloccato viene gergalmente detto *inchiodato*.

Esempio 18 – Si determinino le soluzioni intere e positive dell'equazione

$$y^2 = x(x + 1)(x + 2)(x + 3) \, .$$

Prima di mostrare come si risolva l'equazione data, si consideri il polinomio a secondo membro, cioè sia

$$P(x) = x(x + 1)(x + 2)(x + 3) \, .$$

Moltiplicando tra loro ordinatamente il primo e quarto fattore, poi il secondo e terzo, si può scrivere

$$P(x) = (x^2 + 3x)(x^2 + 3x + 2) = (x^2 + 3x)^2 + 2(x^2 + 3x) \, .$$

Aggiungendo e sottraendo 1, il polinomio diventa

$$P(x) = (x^2 + 3x + 1)^2 - 1 \,,$$

vale a dire che $P(x) + 1$ è il quadrato di un numero intero positivo, per ogni valore di x nei numeri naturali.
Sussistono, allora, le due disuguaglianze per l'equazione diofantea

$$(x^2 + 3x)^2 < \boxed{y^2 = (x^2 + 3x + 1)^2 - 1} < (x^2 + 3x + 1)^2 \,.$$

Liberandosi dei quadrati e ricordando di lavorare con interi positivi, risulta che

$$x^2 + 3x < y < x^2 + 3x + 1 \,,$$

cioè ogni possibile valore di y, soluzione dell'equazione è compreso ed *inchiodato* tra due interi consecutivi. Pertanto, si conclude che l'equazione data non ammette soluzioni tra gli interi positivi.

Nell'esempio che segue entra nella mischia delle equazioni diofantee anche il fattoriale, definito come prodotto di interi

$$n! = n \cdot (n - 1) \cdot \cdots 2 \cdot 1 \,,$$

a patto che n sia un numero naturale. Per convenzione, si assume che $0! = 1$.

Esempio 19 – Si determinino le soluzioni dell'equazione diofantea

$$x^2 = 2 + y! \,.$$

Si riporta anzitutto una tabella con il fattoriale dei primi cinque naturali.

y	0	1	2	3	4
$y!$	1	1	2	6	24

Questa tabella aiuta a giungere alla seguente conclusione: per $0 \leq y \leq 4$, il secondo membro fornisce un solo quadrato perfetto soltanto nel caso $y = 2$, per cui risulta

$$x^2 = 4 \quad \rightarrow \quad x = \pm 2 \, .$$

Se risulta $y \geq 5$, allora $y!$ è divisibile per 10, data la presenza di almeno un prodotto $2 \cdot 5$. Quindi, $2 + y!$ termina con un 2: nessun quadrato di intero può terminare con un 2 e, pertanto, il problema non ammette soluzioni per $y \geq 5$.
Si potrebbe essere indotti a pensare che un cambiamento, anche modesto, dell'equazione appena discussa non produca grosse sorprese, ma non è così. Per quanto a conoscenza dell'autore, sempre a caccia di novità al riguardo, non è noto se l'equazione

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

abbia soltanto le soluzioni riportate nella tabella che segue.

x	y	Verifica
± 5	4	$1 + 4! = 25 = 5^2$
± 11	5	$1 + 5! = 121 = 11^2$
± 71	7	$1 + 7! = 5041 = 71^2$

Segue ora un esempio più complesso che richiede una certa attenzione nei calcoli e che presuppone la conoscenza dello sviluppo

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) .$$

Esempio 20 – Si dimostri che nessuno degli interi

$$A_n = n^2 + n + 1$$

è divisibile per 5.

Si comincia a risolvere il quesito proposto, riscrivendo, senza alcuna perdita di generalità, l'intero n come

$$n = 5a + r \quad \text{con} \quad a \in \mathbb{N} \quad \text{e} \quad r = 0, 1, 2, 3, 4 .$$

Il generico elemento della successione, allora, diventa

$$A_n = n^2 + n + 1 = 25a^2 + 10ar + 5a + r^2 + r + 1$$

e si nota che tutti i termini al secondo membro dell'ultima relazione scritta sono divisibili per 5, mentre il termine il termine $r^2 + r + 1$ non lo è, come prova la tabella che segue.

r	0	1	2	3	4
$r^2 + r + 1$	1	3	7	13	21

Esiste anche una maniera differente per dimostrare che i numeri interi

$$A_n = n^2 + n + 1$$

non siano divisibile per 5.
Si supponga che, per assurdo, lo siano. Allora, anche i numeri

$$M_n = (n-2)^2 + 2 = n^2 + n + 1 - 5(n-1)$$

devono esserlo. Ciò è assurdo, in quanto il quadrato $(n-2)^2$ termina sempre con le cifre $1, 4, 5, 6, 9$, per cui $(n-2)^2 + 2$ termina sempre con $1, 3, 6, 7, 8$. E proprio qui sta la contraddizione, non terminando mai per 5.
Si è così dimostrato l'asserto richiesto.

Segue ora un esempio che ricorda molto da vicino l'equazione di Fermat, pur se ha una sostanziale differenza. Si proceda, come sempre, con la massima cautela.

Esempio 21 – Si dimostri che l'equazione diofantea

$$x^n + y^n = x^n y^n \quad \text{con} \quad n \in \mathbb{N} \geq 1$$

ammette la sola soluzione banale.

Operando qualche manipolazione algebrica sull'equazione assegnata

$$x^n y^n - x^n - y^n = 0 \quad \rightarrow \quad x^n y^n - x^n - y^n + 1 = 1\,,$$

essa si può riscrivere nella forma equivalente

$$(x^n - 1)(y^n - 1) = 1\,.$$

Poiché le uniche fattorizzazioni significative dell'unità sono

$$(+1)\cdot(+1) = (-1)\cdot(-1) = 1\,,$$

bisogna esaminare le due possibilità

$$\begin{cases} x^n - 1 = 1\,, \\ y^n - 1 = 1\,, \end{cases} \quad \begin{cases} x^n - 1 = -1\,, \\ y^n - 1 = -1\,. \end{cases}$$

La prima non fornisce alcuna soluzione intera; la seconda invece fornisce la sola soluzione banale.

L'equazione appena discussa somiglia molto all'equazione di Fermat: tuttavia, mentre quella di Fermat contiene tre incognite, la precedente ne ha solo due. Appare evidente che questa circostanza ha delle ripercussioni e, col senno di poi, per chi conosce la vicenda dell'equazione di Fermat, la presenza di una incognita in più nasconde una montagna di difficoltà terribili. È vero che a colpo d'occhio i due problemi sembrano veramente simili e risulta difficile immaginare che la sola presenza di una incognita in più abbia richiesto ai migliori matematici delle varie epoche, circa quattrocento anni per una soluzione, che oltretutto si avvale di metodi sviluppati praticamente negli ultimi cinquanta anni e di cui pochissimi matematici al mondo hanno piena padronanza, tanto è vero che è aperta la caccia ad una soluzione più elementare di quella proposta da Andrew Wiles.

Nell'esempio che segue si ritorna ad utilizzare il fattoriale di un numero intero.

Esempio 22 – Si dimostri che l'equazione diofantea

$$1! + 2! + \cdots + x! = y^2$$

non ammette soluzioni per $x > 4$.

Sia, tanto per cominciare, $x = 5$. Allora, l'equazione diventa

$$1! + 2! + 3! + 4! + 5! = 153 = y^2$$

e si nota che non esiste alcuna soluzione per y e che il primo membro, quando viene diviso per 10, fornisce resto 3, vale a dire che esso termina con un tre. Se si ripete la medesima operazione per altri valori di x, si trova che il primo membro

$$f(x) = 1! + 2! + \cdots + x!$$

termina sempre con un tre, come suggerisce la tabella che segue.

x	5	6	7	8	9	10
$f(x)$	153	873	5913	46233	409113	4037913

Per quale motivo il primo membro termina sempre con un tre finale? La spiegazione è semplice, dato che basta osservare che la somma dei fattoriali dei primi quattro interi positivi è pari a

$$1! + 2! + 3! + 4! = 33\ .$$

Ammesso che $x > 4$, ogni nuovo addendo del fattoriale dell'intero x, contenendo sicuramente un due ed un cinque, termina con uno zero finale. Risulta allora che tutti i primi membri che contengono più di quattro termini di somma devono terminare con un tre.

Da quanto dimostrato segue che l'equazione diofantea assegnata non può avere soluzioni, dal momento che nessun quadrato ha come ultima cifra un tre.

Discesa infinita

Il metodo della discesa infinita venne sviluppato da Pierre de Fermat verso il 1630, nel tentativo di dimostrare che non esistono soluzioni intere dell'equazione

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

Oggi è diffusamente usato per le equazioni diofantee e si può interpretare come una variante della dimostrazione per induzione. Applicando questo metodo per dimostrare che una proposizione è falsa, infatti, si suppone che essa sia valida per un certo n; se si riesce a dimostrare che questo implica che essa sia valida anche per un altro intero m minore di n, la dimostrazione è fatta. Ripetendo il ragionamento, dovrebbe esistere un terzo numero p minore di m per cui vale ancora la proposizione; iterando questo ragionamento si ottiene che esistono infiniti numeri interi positivi minori di n che la verificano. Questo è assurdo, per il principio del buon ordinamento, secondo cui ogni insieme di numeri naturali non vuoto contiene un numero che è più piccolo di tutti gli altri, cioè un qualsiasi sottoinsieme non vuoto dei numeri naturali ammette minimo, e quindi la proposizione è falsa. Come sempre, un esempio vale di più di mille parole.
L'equazione diofantea

$$x^2 + y^2 + z^2 = 2xyz$$

Ammette sicuramente la soluzione banale $x = y = z = 0$. La domanda che sorge naturale è: può ammettere una soluzione non banale?
La prima osservazione da fare è che se uno tra i tre interi x, y, z fosse nullo, necessariamente lo sarebbero anche gli altri due. Dunque, se esiste una soluzione non banale, i tre interi sono tutti diversi da zero.

Si supponga, per assurdo, che esista una soluzione non banale. Dato che il secondo membro dell'equazione rappresenta un numero pari, allora anche il primo deve esserlo e, quindi, almeno uno dei tre deve essere pari. Sia $x = 2x_1$ e, pertanto,

$$4x_1^2 + y^2 + z^2 = 4x_1yz \, .$$

Segue che anche $y = 2y_1$ e $z = 2z_1$ sono pari, in modo che

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1 \, .$$

Si è punto ed a capo. Per i tre nuovi interi x_1, y_1, z_1 si può ripetere quanto già detto e fatto; essi sono pari e si possono introdurre altri interi, per cui

$$x_2^2 + y_2^2 + z_2^2 = 16x_2y_2z_2 \, .$$

In queste due iterazioni si è sempre diviso per due e questa divisione potrebbe continuare all'infinto: si conclude che l'unica possibile soluzione è quella banale.

Esempio 23 – Si determinino le soluzioni intere dell'equazione

$$x^3 + 2y^3 = 4z^3 \, .$$

L'equazione data ammette sicuramente la soluzione banale

$$x = y = z = 0 \, .$$

Ne ammetterà altre? Non è facile rispondere a questa domanda, ma una cosa si può con certezza affermare: la variabile intera x deve essere pari, cioè

$$x = 2n\,.$$

L'equazione, eliminando un fattore due, si può riscrivere nella forma equivalente

$$4n^3 + y^3 = 2z^3\,.$$

La struttura di questa nuova equazione impone che anche y deve essere pari e, pertanto, conviene porre

$$y = 2m\,.$$

Si ottiene allora, sempre semplificando un fattore due, che

$$2n^3 + 4m^3 = z^3\,.$$

Dunque, anche z è pari e questo modo di ragionare si può ripetere ciclicamente, innestando una discesa infinita ed imponendo per le tre incognite la forma funzionale

$$x = 2^p\alpha\,,\quad y = 2^p\beta\,,\quad z = 2^p\gamma\quad \text{con}\quad p \in \mathbb{N}\quad \text{e}\quad \alpha,\beta,\gamma = -1,0,1\,.$$

Appare evidente che

$$\alpha^3 + 2\beta^3 = 4\gamma^3$$

e che quest'ultima equazione ammette la sola soluzione banale.
Si è in tal modo dimostrato che l'equazione diofantea assegnata ammette la sola soluzione banale.

Un legame con gli irrazionali

Infine, si vuole presentare un uso strumentale delle equazioni diofantee, secondo cui esse servono per dimostrare un'altra proprietà richiesta. In particolare, in questo paragrafo si mostrerà, per mezzo di un esempio, come esse possano essere adoperate con successo per mostrare l'irrazionalità di alcuni numeri.

Esempio 24 – Si dimostri che $\log_{10} 21$ è irrazionale.

Apparentemente non sembra vi sia alcuna connessione con le equazioni diofantee, ma, a ben vedere, il legame è molto stretto. Si supponga per assurdo che esistano due numeri interi a e b, coprimi, per cui

$$\log_{10} 21 = \frac{a}{b} \quad \rightarrow \quad 21 = 10^{a/b} \quad \text{con} \quad b \neq 0 \,.$$

Elevando ambo i membri alla potenza b, si ottiene

$$21^b = 10^a \,.$$

Ora, è evidente che quest'ultima relazione, che è un'equazione diofantea, è falsa, dato che 21^b contiene come fattori soltanto 3 e 7, mentre 10^a ha quali fattori primi 2 e 5. Si scioglie l'assurdo, ammettendo che il numero $\log_{10} 21$ sia irrazionale.
Provi il lettore attento ad usare la tecnica appena mostrata per dimostrare la irrazionalità di $\log_{10} 2$.
Alla stessa maniera si riesce a provare l'irrazionalità degli infiniti numeri $\sqrt{4n-1}$, con $n \geq 1$. Infatti, se si suppone per assurdo che esistano due numeri interi a e b, coprimi, per cui

$$\sqrt{4n-1} = \frac{a}{b} \quad \text{con} \quad b \neq 0\,,$$

allora deve anche essere

$$4n - 1 = \frac{a^2}{b^2} \quad \rightarrow \quad 4nb^2 = a^2 + b^2 \quad \rightarrow \quad (4n-1)b^2 = a^2\,.$$

Questa ultima uguaglianza è palesemente assurda, dal momento che il primo ed il secondo membro devono essere divisibili per b^2, eventualità possibile solo se l'intero a è divisibile per l'intero b, contro l'ipotesi che i due interi siano coprimi.

Un'equazione veramente complicata

La discussione che segue riporta un interessante esercizio, nel quale si chiede di determinare le soluzioni intere positive x, y, z, p dell'equazione

$$x^p + y^p = p^z$$

con p primo. Prima entrare, tuttavia, nel vivo della soluzione dell'esercizio, è opportuno trovare il minimo della funzione

$$f(x) = x^p + (1-x)^p \quad \text{nell'intervallo} \quad I = [0,1]$$

e con p numero primo dispari. Si tratta di un problema classico, risolubile applicando una disuguaglianza, dimostrata nel 1906 dal matematico ed ingegnere danese Johan Ludwig William Valdemar Jensen (Nakskov, 8 maggio 1859 – Copenaghen, 5 marzo 1925), una disuguaglianza che lega in generale il valore di una funzione convessa al valore della medesima funzione calcolata nel valor medio del suo argomento.

Nel caso in esame, tuttavia, si preferisce determinare il valore minimo della funzione considerata, piuttosto che applicare la disuguaglianza di Jensen, sconosciuta alla maggior parte degli allievi di secondaria superiore.
Si osserva allora che la funzione $f(x)$ è sempre positiva in I e, dal momento che

$$f(0) = f(1) = 1\,,$$

essa ammetterà, per il Teorema di Rolle, almeno un massimo nell'intervallo compatto in esame. Inoltre, le prime due derivate valgono

$$f'(x) = p[x^{p-1} - (1-x)^{p-1}]\,,\quad f''(x) = p(p-1)[x^{p-2} + (1-x)^{p-2}]\,.$$

Ebbene, la derivata prima si annulla quando

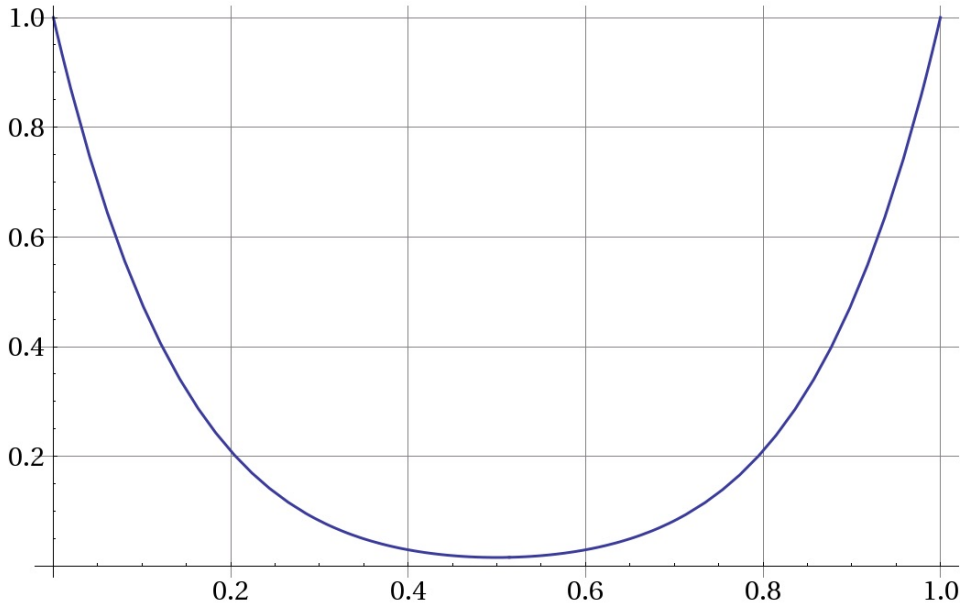
$$x^{p-1} = (1-x)^{p-1}\,,$$

eventualità che accade una sola volta nel compatto I, essendo il primo membro sempre crescente strettamente ed il secondo membro strettamente decrescente per $0 < x < 1$, precisamente nel punto di scissa $x = 1/2$. Dato che

$$f''\left(\frac{1}{2}\right) = p(p-1)\left[\left(\frac{1}{2}\right)^{p-2} + \left(\frac{1}{2}\right)^{p-2}\right] = \frac{2p(p-1)}{2^{p-2}} > 0\,,$$

in corrispondenza di questo punto, la funzione presenta un minimo relativo, che vale

$$f\left(\frac{1}{2}\right) = \frac{1}{2^p} + \frac{1}{2^p} = \frac{1}{2^{p-1}}\,.$$



Pertanto, si conclude che

$$\frac{1}{2^{p-1}} \leq f(x) \leq 1 \quad \text{in} \quad I = [0,1]\,,$$

come d'altra parte suggerisce la figura riportata in precedenza, che illustra il caso particolare $p = 7$, per cui

$$\frac{1}{2^6} = \frac{1}{64} \leq f(x) \leq 1 \quad \text{in} \quad I = [0,1]\,.$$

Venendo all'esercizio, si può dire che, dal momento che p è un numero primo, vale la pena distinguere i tre seguenti casi:

a) il caso $p = 2$,
b) il caso $p = 3$,
c) il caso $p \geq 5$.

Nei primi due casi il problema ammette soluzione, nel terzo non ammette soluzione. La discussione disgiunta di queste tre situazioni consente di mostrare diverse strategie di approccio al problema.

$\boxed{a}$ Se $p = 2$, allora l'equazione diventa

$$x^2 + y^2 = 2^z \,.$$

Si nota immediatamente che il secondo membro è un intero pari, per cui anche il primo lo deve essere. Sono allora possibili due casi:

- quello in cui x e y sono entrambi dispari;
- quello in cui x e y sono entrambi pari.

• Se x e y sono entrambi *dispari* e positivi, allora vuol dire che si può porre

$$x = 2a + 1\,, \quad y = 2b + 1 \quad \text{con} \quad a, b \in \mathbb{N} > 0\,.$$

Sostituendo nell'equazione, risulta la nuova relazione

$$(2a + 1)^2 + (2b + 1)^2 = 2^z\,,$$

che, dopo qualche manipolazione algebrica, diventa

$$2a^2 + 2b^2 + 2a + 2b = 2^{z-1} - 1 \quad \text{con} \quad z \in \mathbb{N} > 0\,.$$

Ebbene, quest'ultima relazione è palesemente assurda, dato che il primo membro rappresenta un numero pari, mentre il secondo membro è dispari.

• Se invece x e y sono entrambi pari e positivi, allora si può porre

$$x = 2x_1 \,, \;\; y = 2y_1$$

e l'equazione diventa

$$x_1^2 + y_1^2 = 2^{z-2} \,.$$

Da quanto precede, si può affermare che anche le nuove incognite x_1 e y_1 devono essere pari e, pertanto, si può scrivere

$$x_1 = 2x_2 \,, \;\; y_1 = 2y_2 \,,$$

e la nuova equazione è pari a

$$x_2^2 + y_2^2 = 2^{z-4} \,.$$

Dopo k iterazioni, si giunge a

$$x_k^2 + y_k^2 = 2^{z-2k} \,,$$

in cui si è posto

$$x_{k-1} = 2x_k \,, \;\; y_{k-1} = 2y_k \,.$$

L'indice k della iterazione viene scelto in maniera tale da avvicinarsi il più possibile all'intero positivo z, sicché

per $z = 2k$ (pari), $x_k^2 + y_k^2 = 1$ e non si ha alcuna soluzione,
per $z = 2k + 1$ (dispari), $x_k^2 + y_k^2 = 2$ si ha $x_k = y_k = 1$.

Tornando indietro, si ottengono finalmente i valori delle tre incognite

$$x = 2^k x_k = y = 2^k y_k = 2^k \,, \;\; z = 2k + 1 \,.$$

La verifica della soluzione ottenuta è piuttosto semplice e si realizza per sostituzione, dato che

$$2^{2k} + 2^{2k} = 2 \cdot 2^{2k} = 2^{2k+1} \,.$$

b Se $p = 3$, allora l'equazione diventa

$$x^3 + y^3 = 3^z \,.$$

Si supponga che gli interi x e y non siano coprimi, cioè che

$$MCD(x, y) = \delta > 1 \,.$$

Allora si può porre

$$x = \delta a \,, \;\; y = \delta b \;\; \text{con} \;\; MCD(a, b) = 1$$

e l'equazione diventa

$$\delta^3 (a^3 + b^3) = 3^z \,.$$

Si deduce agevolmente che il termine 3^z deve essere divisibile per δ^3, come pure che 3^z è divisibile per δ. Così, è possibile assumere, senza perdere in generalità, che

$$MCD(x, y) = 1\,,$$

e ricercare solamente le soluzioni primitive, se esistono. Le altre si otterranno dalle primitive moltiplicando per una potenza intera di 3. Pertanto, scomponendo l'equazione assegnata come

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 3^z\,,$$

deve essere

$$x + y = 3^n \quad \text{con} \quad n < z\,.$$

Dato che gli interi x e y sono coprimi, si può anche affermare che x non è divisibile per 3: se lo fosse, anche y dovrebbe essere divisibile per 3, in opposizione al fatto che sono coprimi. L'equazione diventa

$$x^3 + (3^n - x)^3 = 3^{3n} - 3^{2n+1}x + 3^{n+1}x^2 = 3^z\,,$$

che consente di affermare che il primo membro di questa equazione è divisibile per 3^{n+1}, ma non per 3^{n+2}. Si conclude, pertanto, che $z = n + 1$ e si ottiene l'equazione di secondo grado

$$3^{3n} - 3^{2n+1}x + 3^{n+1}x^2 = 3^{n+1} \quad \rightarrow \quad x^2 - 3^n x + 3^{2n-1} - 1 = 0\,.$$

Il discriminante di questa equazione quadratica

$$\Delta = 3^{2n} - 4 \cdot 3^{2n-1} + 4 = 4 - 3^{2n-1}$$

risulta positivo solo per $n = 1$, negativo per $n > 1$ e non si annulla mai. Posto allora $n = 1$, per cui $\Delta = 4 - 3 = 1$, si hanno le due soluzioni distinte

$$x_1 = 1\,,\ \ y_1 = 3 - x_1 = 2 \quad \rightarrow \quad x_2 = 2\,,\ \ y_2 = 3 - x_2 = 1\,,$$

che danno origine ai due insiemi di soluzioni, riassunti nella tabella che segue, dove si assume che $k \in \mathbb{N}$.

x	y	z
3^k	$2 \cdot 3^k$	$3k + 2$
$2 \cdot 3^k$	3^k	$3k + 2$

Si noti la simmetria delle soluzioni e che, in entrambi i casi, la verifica è immediata, osservando che

$$3^{3k} + 8 \cdot 3^{3k} = 3^{3k+2}\,.$$

c Sia $p \geq 5$, vale a dire che p è un primo dispari. Se gli interi x e y non sono coprimi, vale a dire che

$$MCD(x, y) = \delta > 1\,,$$

si può sempre porre

$$x = \delta a\,,\ \ y = \delta b \quad \text{con} \quad MCD(a, b) = 1$$

e l'equazione diventa

$$\delta^p(a^p + b^p) = p^z \,.$$

Si deduce agevolmente che il termine p^z deve essere divisibile per δ^p, come pure che p^z è divisibile per δ. Così, è possibile assumere, senza perdere in generalità, che

$$MCD(x, y) = 1 \,,$$

e ricercare solamente le soluzioni primitive, qualora esistono. Le altre si otterranno dalle primitive moltiplicandole per una potenza intera di p.
Ebbene, dato che, adoperando la regola di Ruffini, è agevole verificare lo sviluppo notevole

$$x^p + y^p = (x + p)(x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}) \,,$$

si può constatare che $x^p + y^p$ è divisibile per $x + y$ e, quindi, si può scrivere che

$$x + y = p^n \quad \text{con} \quad n < z \,.$$

Dato che gli interi x e y sono coprimi, si può anche dire che x non è divisibile per p, tanto è vero che se lo fosse, anche y dovrebbe essere divisibile per p, in opposizione al fatto che sono coprimi. L'equazione, pertanto, assume la nuova forma

$$x^p + (p^n - x)^p = p^z \,.$$

Orbene, grazie alla formula del binomio di Newton, il primo membro di questa equazione

$$x^p + (p^n - x)^p = \sum_{i=1}^{p} \binom{p}{i} p^{ni} (-x)^{p-i}$$

risulta divisibile per p^{n+1}, ma non per p^{n+2}. Discende che $z = n + 1$ e

$$x^p + (p^n - x)^p = p^{n+1} ,$$

che è una relazione estremamente restrittiva. In effetti, applicando la disuguaglianza di Jensen, risulta per $p \geq 5$

$$x^p + (p^n - x)^p = p^{np} \left[\left(\frac{x}{p^n} \right)^p + \left(1 - \frac{x}{p^n} \right)^p \right] \geq \frac{p^{np}}{2^{p-1}} .$$

Allora, dato che $p \geq 5$, si conclude che

$$\frac{p^{np}}{2^{p-1}} = 2 \left(\frac{p^n}{2} \right)^p \geq \frac{p^{5n}}{16}$$

e, pertanto, risulta

$$x^p + (p^n - x)^p \geq \frac{p^{5n}}{16} .$$

Orbene, dal momento che, sempre per $p \geq 5$, risulta

$$\frac{p^{5n}}{16} > p^{n+1} \quad \text{per} \quad n \in \mathbb{N} ,$$

come si può verificare riscrivendo la precedente relazione nella forma equivalente

$$p^{n-1/4} > 2\,,$$

e si può concludere che

$$x^p + (p^n - x)^p > p^{n+1}\,,$$

cioè che non esiste alcuna soluzione intera positiva per l'equazione diofantea assegnata per $p \geq 5$, che era esattamente quanto si desiderava dimostrare.

Nel paragrafo che segue verrà fatta una breve discussione, al fine di collegare le equazioni diofantee con i numeri primi.

Collegamento con i numeri primi

Quanto detto per le equazioni diofantee ha anche uno stretto legame con i numeri primi. In questo senso, infatti, si vuole dimostrare che *ogni numero primo, diverso da due, si può scrivere in un unico modo come differenza di due quadrati di interi*. È questa una proprietà che getta un ponte tra questi due grandi capitoli di Teoria dei Numeri.
È ben noto che un generico numero intero, non necessariamente positivo, possa essere espresso come somma di due quadrati perfetti, simbolicamente

$$n = a^2 - b^2\,.$$

Indicato con d è un divisore di n, ovvimante inferiore a $\sqrt{n}$, allora una possibile soluzione di questa equazione sarà

$$a = \frac{n + d^2}{2d} \ , \quad b = \frac{n - d^2}{2d} \ ,$$

facendo attenzione ad accettare solo i valori interi di a e b.

Ad esempio, nel caso $n = 48$, i divisori di 48 sono $1, 2, 3, 4, 6, 8, 12, 16, 24$ e 48. Poiché $\sqrt{48} \cong 6.928$, si prenderanno in considerazione solo i divisori $1, 2, 3, 4$ e 6. Applicando le formule riportate ed osservando che per $d = 1$ e $d = 3$ si ottengono valori non interi per a e b, si avranno tre possibili soluzioni:

- $d = 2 \ , \quad a = 13 \ , b = 11 \ , \quad 48 = 13^2 - 11^2 \ ;$
- $d = 4 \ , \quad a = 8 \ , b = 4 \ , \quad 48 = 8^2 - 4^2 \ ;$
- $d = 6 \ , \quad a = 7 \ , b = 1 \ , \quad 48 = 7^2 - 1 \ .$

Dalle precedenti considerazioni si deduce che tutti gli *interi dispari* avranno almeno una soluzione; per quanto riguarda i *numeri pari*, invece, si deve notare che quelli che, divisi per due, danno un numero dispari, non hanno soluzioni.

Orbene, indicato con $n = p > 2$ è un numero primo, l'unico divisore d sarà 1, per cui si potrà asserire che un numero primo è sempre esprimibile in uno ed un solo modo come differenza di due quadrati esatti:

$$p = a^2 - b^2 \quad \text{con} \quad a = \frac{p + 1}{2} \ , \quad b = \frac{p - 1}{2} \ .$$

Ad esempio, si può scrivere che

$$3 = 2^2 - 1 \ , \ \ 13 = 7^2 - 6^2 \ , \ \ 29 = 15^2 - 14^2 \ .$$

Tobia Ravà, *Bosco dei numeri primi*, sublimazione su raso acrilico (2011).

Una affascinante lettura sui numeri primi è il libro di Marcus Du Sautoy *L'enigma dei numeri primi. L'ipotesi di Riemann, il più grande mistero della Matematica*, edito da Rizzoli nel 2004.

Un sistema di equazioni diofantee

Prima di terminare, è giusto presentare la soluzione di un sistema di equazioni diofantee, allo scopo di mostrare che le tecniche apprese per le singole equazioni si applicano, quale naturale estensione, ai sistemi.
Si consideri il sistema di equazioni diofantee

$$\begin{cases} m^3 - n^3 - q^3 = 3^{mnq} \,, \\ m^2 = 2(n+q) \,, \end{cases}$$

e si voglia dimostrare che non ammette soluzioni intere.

Per raggiungere questo obiettivo, si osserva che la seconda equazione impone che m sia un intero pari $m = 2m_1$ con $m_1 \in \mathbb{Z}$, sicché essa diventa

$$2m_1^2 = n + q \ .$$

Ebbene, da questa relazione si evince che i due interi n e q devono essere entrambi pari oppure entrambi dispari, affinché la loro somma sia pari. Questa conclusione, trasportata nella prima equazione, dimostra l'assurdo, dato che il primo membro

$$m^3 - n^3 - q^3 = 3^{mnq}$$

è pari, in quanto somma algebrica di un numero pari e di due pari oppure di un numero pari e di due dispari, mentre il secondo membro, nei casi in cui rappresenta un numero intero, essendo una potenza di tre, è sempre dispari. L'uguaglianza risulta, pertanto, impossibile e così il sistema assegnato non ammette alcuna soluzione intera.

Si può, in definitiva, affermare che l'esempio appena sviluppato dimostra la sostanziale uguaglianza della logica e delle tecniche risolutive per la soluzione delle equazioni e dei sistemi diofantei.

Considerazioni conclusive

In queste brevi note si è proposto una possibile via per introdurre l'allievo di secondaria superiore oppure universitario al fantastico mondo delle equazioni diofantee, adoperando solamente considerazioni elementari o poco più. Ringrazio in anticipo tutti i lettori di questo libro ad inviarmi errori oppure incongruenze in esso inevitabilmente presenti.

Si tratta di una introduzione, è vero, ma si spera che la lettura sia risultata piacevole e che, parafrasando il grande matematico tedesco Lazarus Fuchs, il

lettore si sia convinto che *la Matematica è un grandioso e vasto paesaggio aperto a tutti gli uomini a cui il pensare arrechi gioia, ma poco adatto a chi non ami la fatica del pensare.*

Immanuel Lazarus Fuchs
Moschin, 5 maggio 1833 – Berlino, 26 aprile 1902

Se poi quanto scritto non sia piaciuto al lettore oppure addirittura si fosse riusciti ad annoiarlo, *credete che non s'è fatto apposta*.

di Piergiorgio Odifreddi
professore ordinario di logica matematica all'Università di Torino
e visiting professor alla Cornell University di Ithaca (New York)

Difficoltà esponenziali

Alcuni problemi sono semplici da enunciare ma assurdamente difficili da risolvere

Tra le tante curiosità elementari riguardanti i numeri piccoli, una delle più profonde è il fatto che 8 e 9 differiscono per una sola unità. La curiosità risiede nel fatto che 8 è un cubo, e 9 un quadrato: si tratta dunque di due potenze, rispettivamente di 2 e di 3, che insieme forniscono una soluzione all'equazione diofantea esponenziale $3^n - 2^m = \pm 1$. L'aggettivo «diofanteo» indica il tipo di equazioni polinomiali a valori interi studiate da Diofanto verso il 250 della nostra era, mentre «esponenziale» specifica che alcune delle incognite stanno appunto a esponente.

Nel 1343 il talmudista francese Levi ben Gershon, detto Gersonide, dimostrò nell'*Armonia dei numeri* che le uniche altre potenze di 2 e 3 che differiscono per una sola unità sono le coppie (1,2), (2,3) e (3,4), che corrispondono a esponenti banali. Detto altrimenti, l'equazione precedente non ha altre soluzioni non banali, oltre a (8,9).

Il padre di Gersonide si chiamava Catalan, e per ironia della sorte fu proprio il matematico francese Eugène Catalan, nel 1844, a domandarsi se 8 e 9 fossero le uniche due potenze non banali, in qualunque base, che differiscono per una sola unità. La risposta positiva divenne nota come congettura di Catalan, ed è stata confermata soltanto nel 2002 da Preda Mihailescu, con una complicata dimostrazione. In altre parole, a non avere soluzioni non banali oltre a (8,9) non è solo l'equazione precedente, ma anche la più generale $x^n - y^m = \pm 1$.

Mente eccelsa. Srinivasa Ramanujan, uno dei più grandi matematici di sempre, nato nel 1887 e deceduto nel 1920.

Questa situazione è tipica della teoria dei numeri in generale, e delle equazioni diofantee esponenziali in particolare: problemi semplici da enunciare, suggeriti da ovvi esempi, si rivelano assurdamente difficili da risolvere. Il caso più conosciuto è quello dell'ultimo teorema di Fermat, enunciato nel 1637, che richiedeva di determinare per quali esponenti n ci fossero soluzioni intere all'equazione $x^n - y^n = z^n$.

La dimostrazione, come è noto, richiese 350 anni di ricerche e fu trovata da Andrew Wiles nel 1995. Come già per la congettura di Catalan, anche per l'ultimo teorema di Fermat l'unica soluzione risultò quella già nota da tempi immemorabili: il caso dei quadrati e delle terne pitagoriche, come 3, 4 e 5, in cui banalmente 3 al quadrato più 4 al quadrato è uguale a 5 al quadrato.

A un altro esempio famoso si arriva, ancora una volta, partendo da osservazioni a prima vista innocue. Già i Pitagorici avevano introdotto i numeri triangolari, che si possono rappresentare disponendo pallini a triangolo, si generano mediante la formula $z(z + 1)/2$ e sono 1, 3, 6, 10, 15, eccetera. Fu invece padre Marin Mersenne ad attirare, nei *Pensieri fisico-matematici* del 1644, l'attenzione sui numeri che differiscono di un'unità dalle potenze di 2 e si generano mediante la formula $2^m - 1$ e sono 1, 3, 7, 15, eccetera.

Come si vede, 1, 3 e 15 appartengono a entrambe le liste, e sono dunque numeri di Mersenne triangolari. Per trovare anche i rimanenti basta uguagliare le formule che descrivono i numeri triangolari da un lato e i numeri di Mersenne dall'altro. In un paio di passaggi si arriva a un'equazione diofantea esponenziale del tipo $2^{m+3} = (2z + 1)^2 + 7$.

Nel 1913 Srinivasa Ramanujan annunciò, senza dimostrazione, che l'equazione $2^n = x^2 + 7$ ha soluzioni solo per n uguali a 3, 4, 5, 7 e 15, corrispondenti a valori di x pari a 1, 3, 5, 11 e 181. La sua affermazione divenne nota come congettura di Ramanujan, fu riproposta indipendentemente nel 1943 da Wilhelm Ljunggren e dimostrata nel 1948 da Trygve Nagell, entrambi matematici norvegesi.

Per quanto riguarda i numeri di Mersenne triangolari, il valore 3 non è applicabile perché produce un esponente 0. Dai valori 4, 5 e 7 si ricavano gli esponenti 1, 2 e 4, e dunque i numeri 1, 3 e 15, che già conoscevamo. E dal valore 15 si ricavano l'esponente 12 e il numero 4095. Poiché l'equazione di Ramanujan non ha altre soluzioni, la lista 1, 3, 15 e 4095 esaurisce l'insieme dei numeri di Mersenne triangolari. Un altro bell'esempio di problema semplice a soluzione complicata: anzi, si può ben dire, di difficoltà esponenziale.

SPL/Contrasto

Esercizi non svolti

In tutte le discipline, ma soprattutto in Matematica, sapere vuol dire saper fare. Ecco, dunque, un discreto numero di esercizi che consentono all'allievo di mettersi alla prova e di ritornare a considerare quanto scritto nelle precedenti pagine, perché, come diceva Giacomo Leopardi, *non si impara mai pienamente una scienza difficile, per esempio la Matematica, dai soli libri*. Pertanto, il miglior modo di imparare la Matematica è facendola. Per questo ogni libro di Matematica che si rispetti conterrà dei problemi, alcuni dei quali esigono molta meditazione. Si raccomanda al lettore di svolgere con attenzione tutti gli esercizi proposti: solo in questo modo la Matematica acquisterà per lui un significato sempre più profondo.

⊙ Un gruppo è formato da 20 persone tra donne, uomini e bambini. L'ammontare disponibile è di 20 € e viene distribuito per intero. Ad ogni donna vengono dati 0.7 €, ad ogni uomo 2 € e ad ogni bambino 0.3 €. Quanti sono gli uomini, le donne ed i bambini?
Risultato: gli uomini sono otto, la donna è una sola, i bambini sono undici.

⊙ Si trovino i valori interi di n, per cui il numero $n^2 + 340$ risulta un quadrato
Risultato: l'insieme delle soluzioni è $\{\pm 84, \pm 12\}$.

⊙ Posto $a = 16$, si determinino b e c, in modo che (a, b, c) sia una terna pitagorica primitiva.
Risultato: si ha la terna $(16, 63, 65)$.

⊙ Sia $a = 2n$, si determinino b e c, in modo che (a, b, c) sia una terna pitagorica primitiva.
Risultato: si ha la terna $(2n, n^2 - 1, n^2 + 1)$.

⊙ Si vuole determinare i triangoli rettangoli, con i lati interi, tali che il perimetro coincida con l'area.

Risultato: si ottengono le terne $(5, 12, 13)$ e $(6, 8, 10)$.

⊙ Si determinino tutte le soluzioni dell'equazione diofantea

$$324x + 81y = 26\,.$$

Risposta: l'equazione non ammette soluzioni intere.

⊙ Si verifichi la tabella, controllando il valore del massimo comun divisore tra le coppie di interi proposte.

a	b	$MCD(a,b)$
444	100	4
220	121	11
680	324	4
2240	1024	64
1134	525	21

⊙ Si verifichi, adoperando il metodo di Eulero, che le soluzioni dell'equazione diofantea

$$18x + 45y = 27$$

valgono

$$x = -1 - 5k\,,\quad y = 1 + 2k \quad \text{con} \quad k \in \mathbb{Z}\,.$$

⊙ Si determinino tutte le soluzioni dell'equazione diofantea

$$125x + 147y = 13\,.$$

Risposta: $x = 260 + 147k\,,\ \ y = -221 - 125k\,,\ \ k \in \mathbb{Z}\,.$

⊙ Si determinino tutte le soluzioni dell'equazione diofantea

$$7x + 5y = 153\,.$$

Risposta: $x = 74 - 5k\,,\ \ y = -73 + 7k\,,\ \ k \in \mathbb{Z}\,.$

⊙ Si determini il più grande numero naturale $s < 60$, per cui l'equazione diofantea

$$72x + 18y = s$$

ammette soluzione e risolverla.
Risultato: risulta $s = 54$ e la soluzione è

$$x = k\,,\ \ y = 3 - 4k \ \ \text{con} \ \ k \in \mathbb{Z}\,.$$

⊙ Si determini il più piccolo numero naturale $s > 20$, per cui l'equazione diofantea

$$15x + 9y = s$$

ammette soluzione e risolverla.
Risultato: risulta $s = 21$ e la soluzione è

$$x = 2 + 3k\,,\ \ y = -1 - 5k \ \ \text{con} \ \ k \in \mathbb{Z}\,.$$

⊙ Si determinino tutte le soluzioni dell'equazione diofantea

$$6x + 10y + 15z = 3\,.$$

Risposta: $x = -2 + 5t\,,\ \ y = -3 + 6t + 3s\,,\ \ z = 3 - 6t - 2s\,,\ \ t, s \in \mathbb{Z}\,.$

⊙ Si determinino le soluzioni intere dell'equazione

$$y^2 - xy + 5x + 1 = 0\,.$$

Risultato: è riportato nella tabella che segue.

x	-17	-17	-5	-5	25	25	37	37
y	-21	4	-8	3	7	18	6	31

⊙ Si determinino i punti razionali sulla parabola di equazione

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

Risultato: si hanno i punti $P(m/2, 1 + m^2/2\,)$, con $m \in \mathbb{Q}$.

⊙ Usando il metodo della discesa infinita, si dimostri che l'equazione diofantea

$$x^2 + y^2 = 3z^2$$

ammette la sola soluzione banale.

⊙ Sia data la funzione

$$f(x) = \frac{3^x - 1}{2^x - 1}.$$

Si dimostri che l'unico punto a coordinate intere è $P(1, 2)$.

⊙ Il prodotto di tre numeri interi positivi consecutivi non può essere il cubo di un numero intero. Facoltativo: Mostrare che il prodotto di k numeri interi positivi consecutivi non può essere la potenza k-esima di un numero intero.

⊙ Si dimostri che l'equazione diofantea

$$x^2 = y^5 - 4$$

non ammette soluzioni.
Suggerimento: se si osserva che x e y possono essere entrambi pari o dispari, dalla discussione di questi due casi discende l'assurdo.

⊙ Quali sono i numeri naturali n tali che $7 \cdot 2^n$ può essere scritto come somma di due cubi di numeri positivi dispari?
Risultato: l'unico numero naturale è $n = 2$.

⊙ Si dice *pitagorico* un triangolo rettangolo se le lunghezze dei suoi lati sono numeri interi. Si dimostri che in ogni triangolo rettangolo pitagorico il raggio del cerchio inscritto ha lunghezza intera.

⊙ Siano p, q due numeri primi. Si dimostri che l'equazione

$$\frac{p}{x^2}+\frac{q}{y^2}=1$$

ammette soluzioni intere $x, y \in \mathbb{Z}$, se e solo se $p+q$ è un quadrato.

⊙ Si risolva l'equazione diofantea

$$-2x^3+5x^2y+4xy^2-3y^3=3\,.$$

Risultato: si ha un'unica soluzione per $x=0$ e $y=-1$.

⊙ Si dimostri che non ha soluzioni l'equazione diofantea

$$-2x^3+5x^2y+4xy^2-3y^3=6\,.$$

⊙ Si dimostri che l'equazione diofantea esponenziale

$$5^x-8^y=1$$

non ammette alcuna soluzione.

Suggerimento: se si osserva che $x, y>1$ e si pone $8=5+3$, l'equazione, sviluppando la potenza y −esima, diventa palesemente assurda

$$5^x-\sum_{k=1}^{y}\binom{y}{k}5^k 3^{y-k}=4\,.$$

⊙ Si dimostri che l'equazione diofantea esponenziale

$$2^x - 1 = 3^y$$

ammette la sola soluzione $x = 2, y = 1$ negli interi positivi.

Suggerimento: posto $x, y > 0$ e dato che

$$3^y - 1 = 2 \cdot (3^{y-1} + 3^{y-2} + \cdots + 3 + 1)\,,$$

l'equazione diventa

$$2^{x-1} - 2 = 3^{y-1} + 3^{y-2} + \cdots + 3\,,$$

da cui, dovendo il primo membro essere divisibile per 3, discende la soluzione.

⊙ Si dimostri che l'equazione diofantea esponenziale

$$3^x + 2 = 5^y$$

ammette la sola soluzione $x = y = 1$.

⊙ Si dimostri che l'equazione diofantea esponenziale

$$4^x + 5^y = 6^z$$

ammette la sola soluzione $x = 0$, $y = 1$ e $z = 1$.

Suggerimento: posto

$$4^x = 6^z - 5^y = (5 + 1)^z - 5^y\,,$$

l'equazione diventa

$$4^x - 1 = \sum_{k=1}^{z} \binom{z}{k} 5^k - 5^y$$

e la soluzione riportata diventa evidente.

⊙ Si dimostri che l'equazione diofantea

$$x^3 + y^3 + z^3 = 400$$

non ammette soluzioni.

Suggerimento: si studi l'equazione primitiva

$$a^3 + b^3 + c^3 = 50 \quad \text{con} \quad x = 2a\,, \quad y = 2b\,, \quad z = 2c\,.$$

⊙ Si determinino le soluzioni dell'equazione diofantea

$$\frac{1}{x} + \frac{1}{y} = 1\,.$$

Risultato: si ha un'unica soluzione per $x = y = 2$.

⊙ Si determinino le soluzioni dell'equazione diofantea

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{7}\,.$$

Risultato: si tratta di un caso in cui sono presenti diverse soluzioni, tutte riassunte nella tabella che segue.

x	-42	6	8	14	56
y	6	-42	56	14	8

⊙ Si determinino le soluzioni dell'equazione diofantea

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=2\,.$$

Risultato: si hanno le soluzioni riportate nella tabella che segue.

x	1	2	2
y	2	1	2
z	2	2	1

⊙ Sia m un intero positivo. Si dimostri che la soluzione dell'equazione diofantea $10^x = m$ è intera oppure irrazionale.

Suggerimento: posto $x = \log_{10} m$, basta provare quanto richiesto sul logaritmo decimale.

⊙ Si verifichi che, per ogni intero positivo n, il numero

$$N = n^2 + 1$$

non è divisibile per 3.

Suggerimento: se si pone che $N = 3k$ con $k \in \mathbb{N}$ e, senza alcuna perdita di generalità, si scrive $n = 3a + r$ con $a \in \mathbb{Z}$ e $r = 0, 1, 2$, si ottiene

$$9a^2 + 6a + 1 + 1 = 3k \quad \rightarrow \quad 3k - 9a^2 - 6a = 2\,,$$

che è un'uguaglianza palesemente assurda.

⊙ Si mostri che, per ogni intero positivo n, il numero

$$5^n + 2 \cdot 3^{n-1} + 1$$

è divisibile per 8.

Suggerimento: si utilizzi il*principio di induzione*, partendo dal primo valore che vale 8 e si ottiene per $n = 1$.

⊙ Qual è il più grande intero N tale che

$$n^5 - 5n^3 + 4n$$

sia divisibile per N qualunque sia l'intero n?

Suggerimento: basta osservare che

$$n^5 - 5n^3 + 4n = (n-2)(n-1)n(n+1)(n+2)\,,$$

per concludere che $N = 120$.

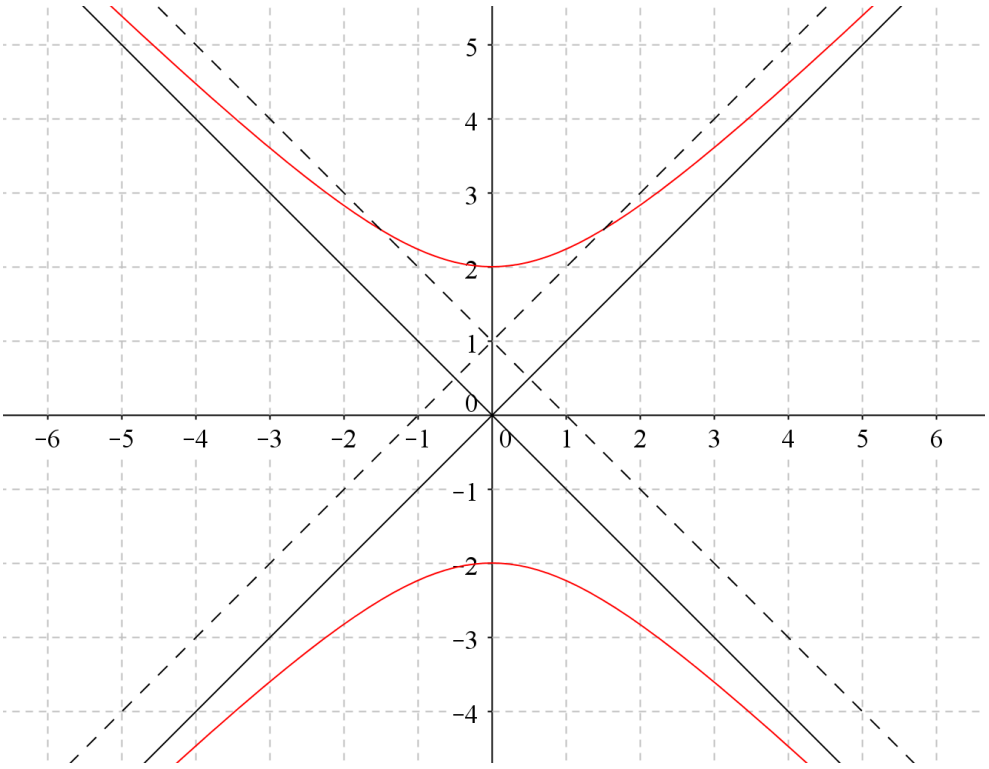
⊙ Si dimostri che l'equazione diofantea esponenziale

$$x^2 + 4 = y^2$$

ammette le soluzioni

$$x = 0\,,\quad y = \pm 2\,.$$

Suggerimento: si costruisca con precisione e si osservi con attenzione il grafico dell'iperbole equilatera, magari disegnando gli asintoti obliqui e le rette distanti un'unità da questi.



⊙ Si mostri che l'equazione diofantea non lineare

$$x^3 + 7 = y^3$$

ammette le soluzioni riportate nella tabella che segue.

x	-2	1
y	1	2

Suggerimento: basta riscrivere l'equazione assegnata nella forma equivalente

$$7 = y^3 - x^3 \;\rightarrow\; 7 = (y - x)(y^2 + xy + x^2)$$

e considerare le poche possibilità di fattorizzare il numero primo 7 .

⊙ Si propone un problema classico, che vanta una tradizione millenaria. Se un gallo costa 5 monete, una gallina 3 monete e con una moneta si possono comprare 3 pulcini, quanti galli, galline e pulcini si possono comprare con 100 monete, volendo comprare in tutto 100 polli?

Risultato: Chang Chhiu-Chien, nel suo trattato *Matematica classica*, scritto intorno all'anno 250 dopo Cristo, fornisce le risposte riassunte nella tabella che segue.

x	4	8	12
y	18	11	4
z	78	81	84

Riflettiamo ora su cos'è la Matematica. Di per sé è un sistema astratto, un'invenzione dello spirito umano, che come tale nella sua purezza non esiste. È sempre realizzato approssimativamente, ma, come tale, è un sistema intellettuale, è una grande, geniale invenzione dello spirito umano. La cosa sorprendente è che questa invenzione della nostra mente umana è veramente la chiave per comprendere la natura, che la natura è realmente strutturata in modo matematico e che la nostra matematica, inventata dal nostro spirito, è realmente lo strumento per poter lavorare con la natura, per metterla al nostro servizio attraverso la tecnica.

Papa Benedetto XVI
Colloquio con i giovani, 6 aprile 2006

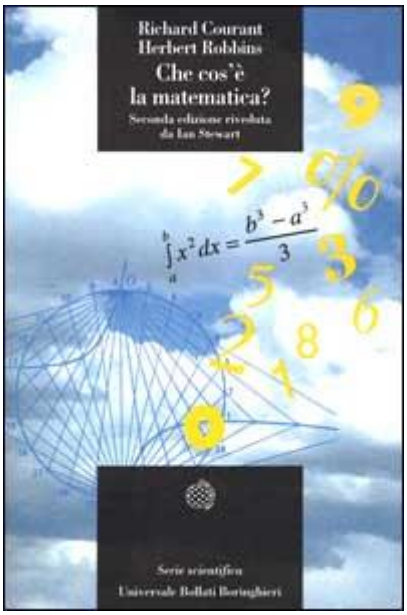
Bibliografia

Già nel testo sono state consigliate alcune letture, pensate per approfondire i diversi aspetti trattati. Qui di seguito si fornisce un modesto elenco di opere generali sull'argomento.

• Un ottimo libro per approfondire la conoscenza della Matematica elementare, ma non solo, è il classico di Richard Courant e Herbert Robbins

Che cos'è la matematica?,

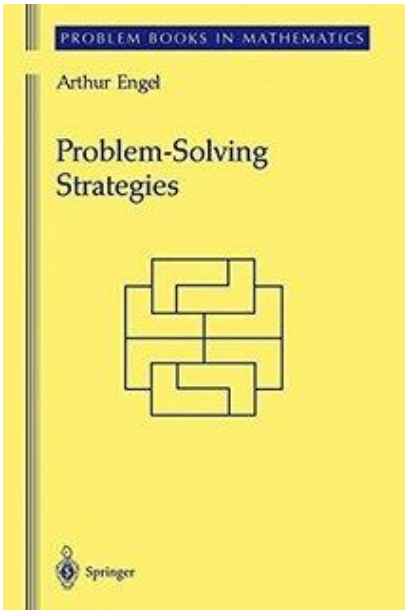
edito per i tipi di Bollati Boringhieri, 2000.



• Per prepararsi alle gare di matematica a qualsiasi livello, uno strumento molto utile è il volume in lingua inglese, ormai classico, ma sempre validissimo di Arthur Engel

Schede olimpiche,

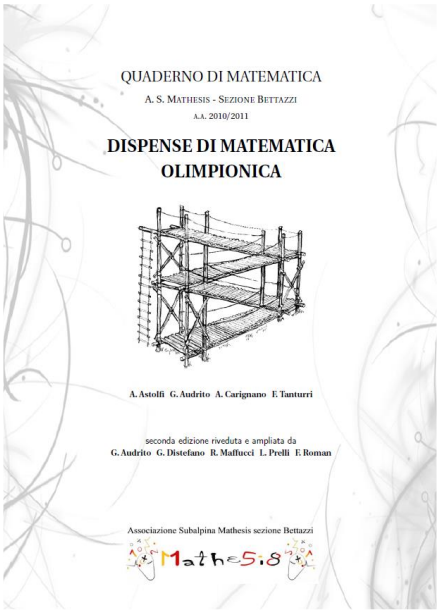
edito da Springer nel 1991.



• In rete si trovano le

Dispense di Matematica olimpica

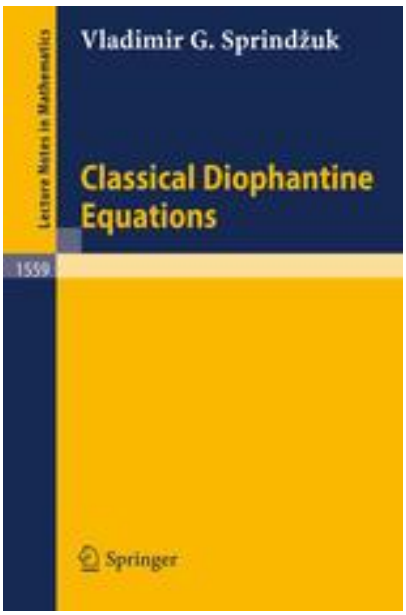
di A. Astolfi, G. Audrito, A. Carignano, F. Tanturri, pubblicate a cura della Sezione Bettazzi della Associazione Subalpina Mathesis, per la prima volta nell'anno accademico 2010 – 2011.



• Più avanzato è il testo di Vladimir Gennadievich Sprindzuk

Classical diophantine equations,

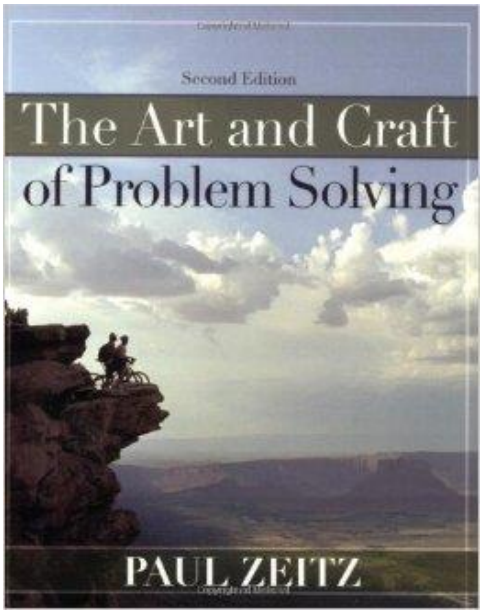
edito dalla Springer nel 2008.



• Altro ottimo testo è quello di Paul Zeitz

The art and craft of problem solving,

edito da John Wiley & Sons nel 2007.



Ardo dal desiderio di spiegare e la mia massima soddisfazione è prendere qualcosa di ragionevolmente intricato e renderlo chiaro passo dopo passo. È il modo più facile per chiarire le cose a me stesso.

Isaac Asimov