

TERNE PITAGORICHE

di Giancarlo Travaglini*

* Dipartimento di
Matematica e Applica-
zioni, Università di Mila-
no-Bicocca

Le terne pitagoriche sono le soluzioni intere positive x, y, z dell'equazione $x^2 + y^2 = z^2$ e la loro storia si dispiega negli ultimi quattro millenni. In questo articolo si parte da una intrigante tavoletta babilonese del XIX secolo a.C. e si passa poi agli Elementi di Euclide (IV-III secolo a.C.) e a Diofanto di Alessandria (III-IV secolo), si incontra quindi Fermat (XVII secolo), e si arriva ai teoremi di Sierpinski e Wiles nel XX secolo.

Il teorema di Pitagora (Figura 1) è uno dei più famosi risultati della Matematica, e ci dice che se in un triangolo rettangolo indichiamo con a e b le lunghezze dei cateti e con c la lunghezza dell'ipotenusa, allora $a^2 + b^2 = c^2$.

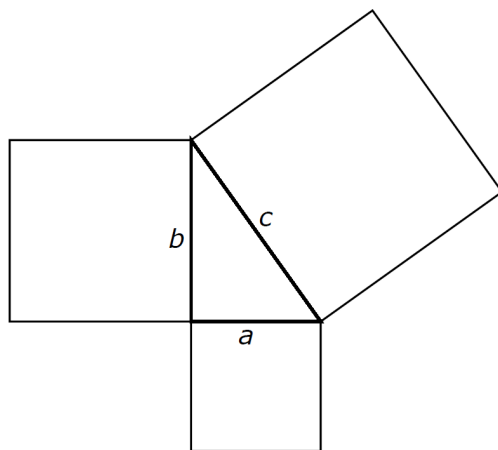


Figura 1: Il teorema di Pitagora: $a^2 + b^2 = c^2$

Quando a, b, c sono numeri interi positivi diciamo che (a, b, c) è una *Terna Pitagorica*.

Se a, b, c sono coprimi (cioè $\text{mcd}(a, b, c) = 1$, dove mcd è il massimo comun divisore), diciamo che (a, b, c) è una *Terna Pitagorica Primitiva*. Ad esempio (3, 4, 5) e (5, 12, 13) sono terne pitagoriche primitive, mentre (6, 8, 10) è una terna pitagorica non primitiva, poiché 6, 8, 10 hanno 2 come divisore comune.

In questo articolo parleremo della storia delle terne pitagoriche e di alcune delle loro principali proprietà. Osserveremo i primi esempi di terne pitagoriche e, a partire da questi, ci porremo alcuni problemi, che in parte risolveremo. La lettura, come ogni lettura in cui si parla di Matematica, richiede un certo impegno, cioè un po' di tempo, con carta e matita a portata di mano. Questo articolo può essere letto da studentesse/studenti del terzo o quarto anno della Scuola Secondaria Superiore di Secondo Grado.

In una terna pitagorica primitiva i numeri a e b non possono essere entrambi pari, altrimenti (poiché $a^2 + b^2 = c^2$) anche c sarebbe pari e quindi a , b e c sarebbero tutti divisibili per 2, dunque non coprimi. Inoltre a e b non possono essere entrambi dispari. Infatti, se fosse $a = 2h + 1$ e $b = 2k + 1$, allora c sarebbe pari (diciamo $c = 2s$), e avremmo

$$4s^2 = c^2 = a^2 + b^2 = (2h + 1)^2 + (2k + 1)^2 = 4(h^2 + h + k^2 + k) + 2 = [\text{un multiplo di } 4] + 2,$$

ma il primo e l'ultimo termine non possono essere uguali, poiché un multiplo di 4 non può essere uguale a [un multiplo di 4] + 2. D'ora in avanti supporremo a dispari e b pari.

La ricerca delle soluzioni intere positive dell'equazione $x^2 + y^2 = z^2$ costituisce una delle più famose *Equazioni Diofantee*, che devono il loro nome a Diofanto di Alessandria (III secolo d.C.), vedi [17], e sono le equazioni polinomiali a coefficienti interi per le quali si cercano solo le soluzioni intere. Nel caso di $x^2 + y^2 = z^2$ siamo di fronte ad uno dei più antichi problemi matematici conosciuti, come testimonia una celebre tavoletta di argilla chiamata Plimpton 322.

1 Plimpton 322

Questa tavoletta, vedi la Figura 2, è parte di una donazione effettuata intorno al 1936 dall'edi-



Figura 2: Plimpton 322 (circa 13cm × 9cm × 2cm).

tore e filantropo George Arthur Plimpton alla Columbia University (322 è il numero assegnato a questo reperto nella collezione).

La tavoletta è stata datata intorno al 1800 a.C. e consiste di una tabella di numeri nella scrittura cuneiforme, in notazione sessagesimale babilonese. Una parte della tavoletta è andata perduta, e si pensa contenesse la colonna b , di cui parleremo tra poco. Vedi [1] per una guida alla lettura di Plimpton 322.

$I :$	a	c	$II :$	a	b	c	$III :$	a	b	c	angolo	(1)
	119	169		119	120	169		119	120	169	$44^{\circ}45'$	
	3367	4825		3367	3456	4825		3367	3456	4825	$44^{\circ}15'$	
	4601	6649		4601	4800	6649		4601	4800	6649	$43^{\circ}47'$	
	12709	18541		12709	13500	18541		12709	13500	18541	$43^{\circ}16'$	
	65	97		65	72	97		65	72	97	$42^{\circ}4'$	
	319	481		319	360	481		319	360	481	$41^{\circ}32'$	
	2291	3541		2291	2700	3541		2291	2700	3541	$40^{\circ}19'$	
	799	1249		799	960	1249		799	960	1249	$39^{\circ}46'$	
	481	769		481	600	769		481	600	769	$38^{\circ}43'$	
	4961	8161		4961	6480	8161		4961	6480	8161	$37^{\circ}26'$	
	45	75		45	60	75		45	60	75	$36^{\circ}52'$	
	1679	2929		1679	2400	2929		1679	2400	2929	$34^{\circ}59'$	
	161	289		161	240	289		161	240	289	$33^{\circ}51'$	
	1771	3229		1771	2700	3229		1771	2700	3229	$33^{\circ}16'$	
	56	106		56	90	106		56	90	106	$31^{\circ}53'$	

Nella tabella I in [1] troviamo, scritti nella nostra notazione, la seconda e la terza colonna di Plimpton 322. Si tratta di terne pitagoriche, più precisamente delle lunghezze dei cateti di lunghezza dispari (cioè a), che in questo caso (ma non in generale, vedi la Tabella 1 più avanti) sono anche i cateti più corti, e delle lunghezze delle ipotenuse (cioè c) in alcune terne pitagoriche.

Nella tabella II in [1] abbiamo inserito una colonna contenente le lunghezze b dei cateti mancanti, ottenendo così quindici terne pitagoriche.

La tabella II non sembra però spiegare l'ordinamento delle righe, che invece appare nella tabella III in [1], dove abbiamo inserito una quarta colonna, che riporta gli angoli opposti ai lati di misura a (vedi la Figura 1), scritti in gradi (approssimati). Vediamo così una successione di angoli che decrescono da circa 45° a quasi 30° .

Vedi [4, 6, 7, 8, 9, 11] per diverse interpretazioni di Plimpton 322.

Osserviamo che i numeri b non hanno divisori primi diversi da 2, 3, 5. Numeri di questo tipo sono chiamati *regolari per la base 60* (vedi [18]), cioè se a/b è una frazione semplificata e b è regolare, allora a/b ha sviluppo sessagesimale finito. Analogamente, nella nostra notazione decimale, una frazione semplificata a/b ha sviluppo decimale finito se e solo se esistono due in-

teri non negativi j, k tali che $b = 2^j 5^k$. Ad esempio $17/20 = 0,85$ ha sviluppo decimale finito, contrariamente a $5/6 = 0,8333\ldots$.

Il passaggio seguente, tratto dal bel libro di J. Conway e R. Guy [2], ci ricorda l'importanza della scrittura sessagesimale.

Il sistema a base 60 veniva utilizzato dagli antichi anche per i calcoli astronomici, e si riflette ancora oggi nel modo in cui misuriamo il tempo, dividendo un'ora in 60 minuti e un minuto in 60 secondi. Nel suo apparente tragitto nei cieli, il sole impiega circa 360 giorni (in effetti 365,242199) per descrivere un cerchio completo, ed è per questo, sembra, che i Babilonesi hanno suddiviso un intero cerchio in 360 gradi.

Circa quindici secoli dopo Plimpton 322, la comprensione delle terne pitagoriche trova il suo punto fermo grazie alla matematica greca. Prima di descriverlo è interessante leggere il commento che segue, tratto dal libro di O. Ore ([10]).

... queste scoperte della matematica babilonese gettano luce sulla storia della scienza greca antica. La conoscenza della matematica greca prima di Euclide è sempre stata piuttosto nebulosa, ed è stato difficile comprendere la rapida evoluzione dalle sue fasi iniziali, rappresentate da Talete di Mileto (circa 600 a.C.) e dai Pitagorici, al bellissimo sistema che si trova sviluppato ai tempi di Euclide (circa 300 a.C.) o probabilmente anche prima. Bisogna ora supporre che i Greci abbiano assorbito dal magazzino babilonese di fatti e metodi matematici molto più di quanto sospettato finora. Questo, tuttavia, va esplicitamente detto, non toglie nulla alla distinzione dei Greci per aver creato il concetto di teoria matematica sistematica come ancora oggi intendiamo e usiamo, basata su assiomi o assunzioni fondamentali e sviluppata nelle sue dimostrazioni mediante deduzioni logiche. Questo risultato è stato uno dei più importanti nella storia del pensiero umano.

2 Il teorema di Euclide

Vediamo ora come è possibile determinare tutte le terne pitagoriche.

È chiaro che se (a, b, c) è una terna pitagorica, allora, per ogni intero positivo m , anche la terna (ma, mb, mc) è pitagorica. È quindi sufficiente determinare le terne primitive, vedremo tra un attimo come. Ricordiamo che abbiamo posto a dispari e b pari.

La seguente caratterizzazione delle terne pitagoriche primitive è attribuita ad Euclide (Figura 3), anche se nel suo libro *Elementi* (vedi [5], Libro X, Proposizione 29), si trova solo la dimostrazione della prima parte del teorema).



Figura 3: Euclide che insegna agli studenti, in un dettaglio della *Scuola di Atene* di Raffaello (Musei Vaticani). Public Domain, <https://commons.wikimedia.org>

Teorema 1 (Euclide) *Siano $u < v$ due numeri interi positivi coprimi e non entrambi dispari. Allora i tre numeri*

$$a = v^2 - u^2, \quad b = 2uv, \quad c = u^2 + v^2 \quad (2)$$

costituiscono una terna pitagorica primitiva. Viceversa, data una terna pitagorica primitiva (a, b, c) , esistono due interi positivi u, v coprimi e non entrambi dispari, per i quali vale (2).

Vedremo due dimostrazioni di questo teorema. La prima è di carattere algebrico ed è abbastanza corta. La seconda, dovuta a Diofanto di Alessandria, è più lunga, ma è comunque interessante, poiché tocca vari punti del programma di Matematica della Scuola Superiore e introduce un metodo applicabile ad altre equazioni diofantee (che, come abbiamo detto sopra, sono le equazioni polinomiali a coefficienti interi, delle quali cerchiamo le soluzioni intere). È riportata nell'Appendice in fondo a questo articolo.

Prima dimostrazione del teorema di Euclide. Poiché

$$(v^2 - u^2)^2 + (2uv)^2 = (u^2 + v^2)^2,$$

$(v^2 - u^2, 2uv, u^2 + v^2)$ è una terna pitagorica. Dimostriamo che è primitiva. Ricordiamo che $0 < u < v$ sono coprimi e non entrambi dispari. Basta mostrare che $(v^2 - u^2)$ e $(u^2 + v^2)$ sono coprimi. Sia d un intero positivo che divide $(v^2 - u^2)$ e $(u^2 + v^2)$. Sommando e sottraendo ve-

diamo che d divide $2v^2$ e $2u^2$. Ricordiamo che u e v non sono entrambi dispari e (essendo coprimi) non sono entrambi pari, quindi $v^2 - u^2$ è dispari e dunque anche il suo divisore d è dispari. Allora, poiché d divide $2v^2$ e $2u^2$, abbiamo che d divide v^2 e u^2 . Ma u^2 e v^2 sono coprimi (poiché u e v lo sono), quindi $d = 1$. Dunque $(v^2 - u^2)$ e $(u^2 + v^2)$ sono coprimi.

Viceversa, sia (a, b, c) una terna pitagorica primitiva (ricordiamo che a è dispari, b è pari, e c è dispari). Allora i numeri interi $\frac{1}{2}(c + a)$ and $\frac{1}{2}(c - a)$ sono coprimi (se fosse $\frac{1}{2}(c + a) = rp$ e $\frac{1}{2}(c - a) = sp$ (con $p > 1$), allora $c = (r + s)p$ e $a = (r - s)p$ non sarebbero coprimi). Inoltre

$$\frac{1}{2}(c + a) \cdot \frac{1}{2}(c - a) = \frac{1}{4}(c^2 - a^2) = \left(\frac{1}{2}b\right)^2.$$

Dunque i numeri coprimi $\frac{1}{2}(c + a)$ and $\frac{1}{2}(c - a)$ devono essere quadrati. Allora esistono interi positivi coprimi u e v tali che $u < v$ e

$$u^2 = \frac{1}{2}(c - a), \quad v^2 = \frac{1}{2}(c + a).$$

Quindi $u^2 + v^2 (= c)$ è dispari e dunque u^2 e v^2 non sono entrambi pari e non sono entrambi dispari, e allora lo stesso vale per u e v . Inoltre $v^2 - u^2 = a$ e infine

$$b^2 = c^2 - a^2 = (u^2 + v^2)^2 - (v^2 - u^2)^2 = 4u^2v^2,$$

cioè $b = 2uv$. ■

3 Le terne pitagoriche e l'ultimo teorema di Fermat

Dato un numero intero $n > 2$ è naturale chiedersi se esistono soluzioni intere positive x, y, z dell'equazione

$$x^n + y^n = z^n. \quad (3)$$

La risposta a questo problema è negativa ed è nota come l'*Ultimo Teorema di Fermat*, uno dei problemi più affascinanti della Matematica, congetturato da Pierre de Fermat (Figura 4) intorno al 1630, quando scrisse il seguente commento sulla sua copia dell'*Aritmetica* di Diofanto:

È impossibile che un cubo sia la somma di due cubi, una quarta potenza sia la somma di due quarte potenze, o, in generale, che qualsiasi numero che sia una potenza maggiore della seconda sia la somma di due potenze simili. Ho scoperto una dimostrazione veramente straordinaria [di questo teorema], ma questo margine è troppo piccolo per contenerla.

Si ritiene che in realtà Fermat abbia provato solo il caso $n = 4$, di cui vediamo ora la dimostrazione, che è una conseguenza del teorema di Euclide, ma è comunque importante e non banale. Si basa sul *Metodo della discesa infinita*, già presente negli Elementi di Euclide ([5], Libro VII, Proposizione 31), ma sviluppato da Fermat.



Figura 4: Pierre de Fermat. Public Domain, <https://commons.wikimedia.org>

Teorema 2 (Fermat) *Non esistono tre interi positivi x, y, z tali che*

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

Dimostrazione. È sufficiente provare che non esistono interi positivi a, b e c tali che

$$a^4 + b^4 = c^2 . \quad (4)$$

Sia c il più piccolo intero positivo tale che (4) ammette soluzioni intere positive a, b, c . Allora (a^2, b^2, c) è una terna pitagorica primitiva (altrimenti c non sarebbe il minimo) e quindi esistono due interi u, v positivi, coprimi e non entrambi dispari tali che

$$a^2 = v^2 - u^2 , \quad b^2 = 2uv , \quad c = u^2 + v^2 . \quad (5)$$

Quindi anche (a, u, v) è una terna pitagorica primitiva e allora esistono due interi positivi s, t coprimi e non entrambi dispari , tali che

$$a = t^2 - s^2 , \quad u = 2st , \quad v = s^2 + t^2 . \quad (6)$$

Quindi $\text{mcd}(s, t) = \text{mcd}(s, v) = \text{mcd}(t, v) = 1$. Poiché $b^2 = 4stv$, deduciamo che s, t e v sono quadrati. Scriviamo $s = j^2, t = k^2$ e $v = \ell^2$. Quindi (5) e (6) implicano

$$c > v = \ell^2 = s^2 + t^2 = j^4 + k^4 ,$$

e questo contraddice la minimalità di c . ■

La non esistenza di soluzioni positive di (3) quando $n \geq 3$ è uno dei principali risultati ottenuti in Matematica negli ultimi decenni. È stata dimostrata nel 1994 da Andrew Wiles (Figura 5), con la collaborazione di Richard Taylor (vedi [14] per la storia di questo problema, vedi anche



Figura 5: Andrew Wiles. Public Domain, <https://commons.wikimedia.org>

il Capitolo 9 della seconda edizione del bellissimo libro di Richard Courant e Herbert Robbins [3] per una idea della dimostrazione di Wiles).

4 Una tabella di terne pitagoriche primitive

Nella Tabella 1 qua sotto siamo partiti dalle coppie (u, v) nel teorema di Euclide e abbiamo scritto le prime terne pitagoriche primitive. Abbiamo deciso questo ordinamento delle righe: innanzitutto la somma $u + v$, poi u . Guardiamo attentamente la Tabella 1 e vediamo cosa ci suggerisce. Ricordiamo che u e v sono numeri interi positivi coprimi e non entrambi dispari, che $u < v$, e che

$$(a, b, c) = (v^2 - u^2, 2uv, u^2 + v^2) \text{ .}$$

u	v	(a, b, c) primitive
1	2	(3, 4, 5)
1	4	(15, 8, 17)
2	3	(5, 12, 13)
1	6	(35, 12, 37)
2	5	(21, 20, 29)
3	4	(7, 24, 25)
1	8	(63, 16, 65)
2	7	(45, 28, 53)
4	5	(9, 40, 41)
1	10	(99, 20, 101)
2	9	(77, 36, 85)
3	8	(55, 48, 73)
4	7	(33, 56, 65)
5	6	(11, 60, 61)
1	12	(143, 24, 145)
2	11	(117, 44, 125)
3	10	(91, 60, 109)
4	9	(65, 72, 97)
5	8	(39, 80, 89)
6	7	(13, 84, 85)
$\vdots$	$\vdots$	$\vdots$

Tabella 1: Le prime terne pitagoriche primitive (a, b, c) descritte dal teorema di Euclide.

Ora poniamoci qualche domanda, sempre guardando la Tabella 1.

Esistono infinite terne pitagoriche primitive?

Sì, ed è una conseguenza banale del teorema di Euclide, dato che possiamo fare assumere ad u e v infiniti valori. Possiamo però dimostrarlo in modo più semplice. Infatti, guardando la Tabella 1 notiamo che esistono molte terne in cui $c = b + 1$:

$$(3, 4, 5) , \quad (5, 12, 13) , \quad (7, 24, 25) , \quad (9, 40, 41) , \quad (11, 60, 61) , \quad (13, 84, 85) .$$

È facile dimostrare che esistono infinite terne (a, b, c) di questo tipo. Infatti queste terne soddisfano il sistema

$$\begin{cases} c = b + 1 \\ a^2 + b^2 = c^2 \end{cases} ,$$

che dà

$$a^2 + b^2 = (b+1)^2, \quad a^2 = 2b+1, \quad b = \frac{a^2-1}{2}, \quad c = \frac{a^2+1}{2}$$

(osserviamo che b e c sono interi poiché a è dispari). Al variare di a tra gli interi positivi dispari otteniamo così le infinite terne

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

Si tratta di terne pitagoriche primitive poiché $\frac{a^2+1}{2}$ e $\frac{a^2-1}{2}$ differiscono di 1, e quindi non possono avere divisori comuni maggiori di 1.

Quali valori possono assumere a , b e c ?

Guardando la Tabella 1, possiamo “indovinare” alcuni fatti su a e b (ricordiamo che a è dispari e b è pari).

Ad esempio, a sembra assumere tutti i valori dispari ≥ 3 (i numeri $a = 3, 5, 7, 9, 11, 13$ appaiono nella tabella). Questo è vero in generale. Infatti, ricordiamo che abbiamo ordinato le terne pitagoriche (prima) secondo la somma $u+v$, che deve essere dispari, e (poi) secondo u . Osserviamo che i numeri dispari $a = 3, 5, 7, 9, 11, 13$ appaiono nelle righe in cui $u+v = a$. Tornando al caso generale, ricordiamo che $a = v^2 - u^2$. Allora, se poniamo $u+v = a$,

$$u+v = a = (v-u)(v+u) \quad \text{se solo se} \quad v-u = 1, \quad \text{cioè} \quad v = u+1.$$

Scegliendo $v = u+1$ vediamo che $a = u+v = 2u+1$ può, al variare di u , essere qualsiasi numero dispari ≥ 3 .

Notiamo che il valore $a = 15$ appare nella seconda riga della Tabella 1, dove però non proviene dalla costruzione precedente, poiché è associato a $u = 1$ e $v = 4$, e quindi $u+v \neq 15$. Se avessimo proseguito la tabella avremmo incontrato nuovamente $a = 15$, associato a $u = 7$ e $v = 8$, cioè alla terna pitagorica $(15, 112, 113)$. Infatti

$$a = 7+8 = 8^2 - 7^2 = 15, \quad b = 2 \cdot 7 \cdot 8 = 112, \quad c = 8^2 + 7^2 = 113.$$

E il numero b ? Nella Tabella 1 tutti i valori di b sono multipli di 4. È sempre vero? Sì, infatti $b = 2uv$, dove uno tra u e v è pari e l'altro è dispari. Allora ogni b è multiplo di 4.

È vero che ogni multiplo positivo di 4 può assumere il ruolo di b in qualche terna pitagorica? Sì, infatti, consideriamo un intero $4k$, con $k \geq 1$ e scegliamo $u = 1$ e $v = 2k$. Allora otteniamo la terna pitagorica primitiva $(4k^2 - 1, 4k, 4k^2 + 1)$.

A questo proposito, la Tabella 1 è un po' fuorviante, poiché ad esempio non vediamo $b = 32$, mentre vediamo valori di b molto più grandi di 32. Osserviamo però che $32 = 2uv$ implica $uv = 16$, con u e v coprimi e non entrambi dispari. L'unica possibilità è $u = 1$ e $v = 16$, che dà $u+v = 17$, mentre la Tabella 1 si ferma a $u+v = 13$.

Ancora un passo e abbiamo dimostrato il seguente risultato.

Teorema 3 *Ogni numero intero $m \geq 3$ è la lunghezza di un cateto in una terna pitagorica.*

Dimostrazione. Abbiamo appena visto che se m è dispari ($e \geq 3$) oppure m è un multiplo positivo di 4, allora m è la lunghezza di un cateto in una terna pitagorica primitiva. Ci rimane il caso $m = 4k + 2$. Sappiamo già che esiste una terna pitagorica primitiva con un cateto di lunghezza $2k + 1$. Raddoppiando questa terna otteniamo un'altra terna (non primitiva) con un cateto di lunghezza $4k + 2$. ■

Cosa possiamo dire su c ? Questa è un'altra storia. Per cominciare, riscriviamo e ordiniamo i valori di c nella Tabella 1. Otteniamo

$$5, 13, 17, 25, 29, 37, 41, 53, 61, 65, 73, 85, 89, 97, \dots$$

Vediamo solo numeri della forma $4k + 1$. In effetti, c deve assumere la forma $4k + 1$. Infatti, scrivendo $u = 2p$ e $v = 2q + 1$ abbiamo

$$c = u^2 + v^2 = (2p)^2 + (2q + 1)^2 = 4p^2 + 4q^2 + 4q + 1 = 4(p^2 + q^2 + q) + 1$$

(il caso u dispari e v pari è analogo). Tuttavia, non ogni numero della forma $4k + 1$ corrisponde a un valore di c nella Tabella 1. Ad esempio, 21 è assente. Dobbiamo pensare che 21 si trovi nelle righe mancanti? No, infatti la tabella contiene tutte le terne pitagoriche primitive con $u + v \leq 13$. Se $c = 21$ apparisse più avanti, quando $u + v \geq 14$, allora avremmo $v \geq 7$, contraddicendo $c = u^2 + v^2 = 21$. Quindi $c = 21$ non appare. Inoltre, 21 non può essere la lunghezza dell'ipotenusa in una terna pitagorica non primitiva. Infatti, $21 = 3 \cdot 7$, e né 3 né 7 possono essere le lunghezze delle ipotenuse in terne pitagoriche, come possiamo verificare direttamente. Dunque non tutti i numeri interi positivi della forma $4k + 1$ possono essere uguali a c in una terna pitagorica.

Vale il seguente teorema, dimostrato da Waclaw Sierpiński (Figura 6) nel 1954. Non scriviamo la dimostrazione, abbastanza lunga, vedi [12, 16], vedi anche [15] per il caso delle terne pitagoriche primitive.

Teorema 4 (Sierpinski) *Un numero intero positivo c è la lunghezza dell'ipotenusa in una terna pitagorica se e solo se c può essere diviso per un numero primo della forma $4k + 1$.*

Le terne pitagoriche “contengono” multipli fissati?

Torniamo a guardare la Tabella 1. Sappiamo che b è sempre un multiplo di 4 (poiché $b = 2uv$, e uno tra u e v è pari). Appaiono altri “multipli”? Notiamo che in ogni terna della tabella appare sia un multiplo di 3, sia un multiplo di 5 (a volte “coincidenti”, come nella terna (15, 8, 17)). Dimostriamo che ogni terna pitagorica primitiva contiene un multiplo di 3. Infatti se u oppure v è multiplo di 3, allora $b = 2uv$ è multiplo di 3. Restano da considerare i casi $u = 3h \pm 1$ e $v = 3k \pm 1$. Allora

$$a = v^2 - u^2 = (3k \pm 1)^2 - (3h \pm 1)^2 = (9k^2 \pm 6k + 1) - (9h^2 \pm 6h + 1) = 3s,$$



Figura 6: Wacław Sierpiński. Public Domain, <https://commons.wikimedia.org>

dove $s = 3k^2 \pm 2k - 3h^2 \mp 6h$. Quindi in questo caso a è un multiplo di 3. Abbiamo così dimostrato che uno tra a e b è sempre un multiplo di 3.

Ora Dimostriamo in modo simile che ogni terna pitagorica primitiva contiene un multiplo di 5. Come prima, basta considerare il caso in cui u e v non sono multipli di 5. Allora possiamo scrivere

$$\begin{aligned} u &= 5h \pm s, \quad \text{dove } s = 1 \text{ oppure } s = 2 \\ v &= 5k \pm t, \quad \text{dove } t = 1 \text{ oppure } t = 2. \end{aligned}$$

Usiamo la notazione $v^2 \pm u^2$ (con il $\pm$ grande), per considerare contemporaneamente $a = v^2 - u^2$

e $c = u^2 + v^2$, tenendolo distinto dal $\pm$ in $\pm s$ e $\pm t$. Allora

$$v^2 \pm u^2 = (5k \pm t)^2 \pm (5h \pm s)^2 = (25k^2 \pm 10kt + t^2) \pm (25h^2 \pm 10hs + s^2) = 5z + t^2 \pm s^2$$

(dove $z = (5k^2 \pm 2kt) \pm (5h^2 \pm 2hs)$). Abbiamo i casi seguenti.

Se $s = 1$ e $t = 1$ allora $v^2 - u^2 = 5z + 1 - 1$ e quindi a è un multiplo di 5.

Se $s = 1$ e $t = 2$ allora $v^2 + u^2 = 5z + 1 + 4$ e quindi c è un multiplo di 5.

Se $s = 2$ e $t = 1$ allora $v^2 + u^2 = 5z + 4 + 1$ e quindi c è un multiplo di 5.

Se $s = 2$ e $t = 2$ allora $v^2 - u^2 = 5z + 4 - 4$ e quindi a è un multiplo di 5.

Abbiamo così dimostrato il seguente risultato (che i Babilonesi avrebbero apprezzato).

Teorema 5 *In ogni terna pitagorica troviamo un multiplo di 3, un multiplo di 4 e un multiplo di 5. Quindi il prodotto abc delle misure dei lati del triangolo è sempre un multiplo di 60.*

Il libro di Sierpinski [13] raccoglie molti problemi di questo tipo.

5 Appendice

Seconda dimostrazione del teorema di Euclide. Dimostriamo solo la seconda parte del teorema. Dunque sia (a, b, c) una terna pitagorica primitiva. Abbiamo osservato all'inizio dell'articolo che a e b non possono essere entrambi pari e non possono essere entrambi dispari, e abbiamo assunto a dispari e b pari. Mostriamo che esiste una corrispondenza biunivoca tra le terne pitagoriche primitive e i punti sulla circonferenza unitaria

$$\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

che hanno come coordinate cartesiane coppie di numeri razionali positivi. Infatti scriviamo l'uguaglianza $a^2 + b^2 = c^2$ nella forma

$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1,$$

ottenendo un punto a coordinate razionali sulla circonferenza unitaria. D'altra parte, osserviamo che se $(a/c, b/\tilde{c})$ è un punto a coordinate razionali sulla circonferenza unitaria, con $\text{mcd}(a, c) = \text{mcd}(b, \tilde{c}) = 1$, allora $c = \tilde{c}$. Infatti abbiamo

$$1 = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{\tilde{c}}\right)^2 = \left(\frac{a\tilde{c}}{c\tilde{c}}\right)^2 + \left(\frac{bc}{\tilde{c}c}\right)^2, \quad a^2\tilde{c}^2 + b^2c^2 = c^2\tilde{c}^2.$$

Allora c^2 divide $a^2\tilde{c}^2$ e quindi (essendo a e c coprimi) c divide $\tilde{c}$; analogamente $\tilde{c}^2$ divide b^2c^2 e quindi $\tilde{c}$ divide c . Dunque

$$c = \tilde{c}. \quad (7)$$

Ora consideriamo, nel piano cartesiano, la retta passante per il punto $(-1, 0)$ e per un punto R avente coordinate razionali positive $(s, t) = (\cos(\theta), \sin(\theta))$ (vedi la Figura 7). L'equazione di questa retta è

$$y = \frac{t}{s+1}(x+1) = w(x+1),$$

dove abbiamo posto $w = t/(s+1)$. Osserviamo che $w = \arctan(\theta/2)$. Ignorando la soluzione $x = -1$ nel sistema

$$\begin{cases} y = w(x+1) \\ x^2 + y^2 = 1 \end{cases}$$

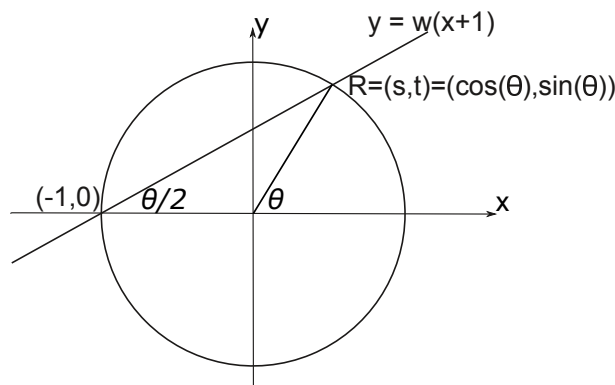


Figura 7: Terne pitagoriche primitive e punti a coordinate razionali sulla circonferenza unitaria.

otteniamo

$$x^2 + w^2(x+1)^2 = 1, \quad x^2 - 1 + w^2(x+1)^2 = 0, \quad x - 1 + w^2(x+1) = 0, \quad x(1+w^2) = 1-w^2,$$

cioè

$$\begin{cases} x = s = \frac{1-w^2}{w^2+1} \\ y = t = w \left(\frac{1-w^2}{w^2+1} + 1 \right) = \frac{2w}{w^2+1}. \end{cases}$$

(ricordando che $s = \cos(\theta)$, $t = \sin(\theta)$, $w = \arctan(\theta/2)$, vedi la Figura 7, otteniamo una identità trigonometrica familiare). Il numero w è minore di 1 e razionale. Possiamo quindi scrivere $w = u/v$ con $0 < u < v$ e $\text{mcd}(u, v) = 1$. Allora

$$\left(\frac{1-w^2}{w^2+1}, \frac{2w}{w^2+1} \right) = \left(\frac{1-u^2/v^2}{u^2/v^2+1}, \frac{2u/v}{u^2/v^2+1} \right) = \left(\frac{v^2-u^2}{u^2+v^2}, \frac{2uv}{u^2+v^2} \right).$$

Considerando le frazioni semplificate $s = a/c$ e $t = b/c$ (vedi (7)) scriviamo

$$\frac{a}{c} = \frac{v^2-u^2}{u^2+v^2}, \quad \frac{b}{c} = \frac{2uv}{u^2+v^2}.$$

Proviamo che u e v non sono entrambi dispari. Infatti, se fossero $u = 2p+1$ e $v = 2q+1$, avremmo

$$\frac{b}{a} = \frac{2uv}{v^2-u^2} = \frac{2(2p+1)(2q+1)}{(2q+1)^2 - (2p+1)^2} = \frac{4(2pq+p+q)+2}{4(q^2-p^2+q-p)} = \frac{2(2pq+p+q)+1}{2(q^2-p^2+q-p)},$$

e quindi a sarebbe pari (altrimenti $a \cdot (2(2pq+p+q)+1)$ sarebbe dispari e non potrebbe essere uguale al numero pari $b \cdot (2(q^2-p^2+q-p))$), contrariamente a quanto abbiamo assunto

in precedenza. Allora la somma $u^2 + v^2$ è dispari e (essendo $\text{mcd}(u, v) = 1$) non ha fattori comuni con $2uv$. Quindi la frazione $2uv/(u^2 + v^2)$ non è semplificabile e allora

$$a = v^2 - u^2, \quad b = 2uv, \quad c = u^2 + v^2,$$

con $0 < u < v$ coprimi e non entrambi dispari. ■

Riferimenti bibliografici

- [1] W. Casselman, *The Babylonian tablet Plimpton 322*.
<https://personal.math.ubc.ca/~cass/courses/m446-03/pl322/pl322.html>
- [2] J. Conway e R. Guy, *Il libro dei numeri*, Hoepli (1999).
- [3] R. Courant e H. Robbins, *Che cos'è la Matematica*, Seconda Edizione riveduta da Jan Stewart, Universale Bollati Boringhieri (2000).
- [4] R. Creighton Buck, *Sherlock Holmes in Babylon*, *American Mathematical Monthly*, **87** (1980), 335–345.
- [5] Euclide, *Elementi*, 300 a.C. <https://mathcs.clarku.edu/~djoyce/java/elements/>
- [6] S. Gibbens, *Ancient Tablet May Show Earliest Use of This Advanced Math*, 2017
<https://www.nationalgeographic.com/history/article/ancient-babylonian-trigonometry-tablet-plimpton-322-video-spd>
- [7] D. Mansfield, *Plimpton 322: A Study of Rectangles*, *Foundations of Science* **26** (2021), 977–1005. <https://link.springer.com/article/10.1007/s10699-021-09806-0>
- [8] D. Mansfield e N. Wildberger, *Plimpton 322 is Babylonian exact sexagesimal trigonometry*, *Historia Mathematica*, **44** (2017), 395–419.
- [9] D. Mansfield e N. Wildberger, *Old Babylonian mathematics and Plimpton 322: A new understanding of the OB tablet Plimpton 322*, YouTube, <https://www.youtube.com/watch?v=L24GzTa0110>
- [10] O. Ore, *Number Theory and its History*, Dover (1988).
- [11] E. Robson, *Neither Sherlock Holmes nor Babylon: A Reassessment of Plimpton 322*, *Historia Mathematica*, **28** (2001), 167–206.
- [12] J. Sally e P. Sally, *Roots to Research*, American Mathematical Society (2007).

- [13] W. Sierpinski, Pythagorean triangles, Dover (2003).
- [14] S. Singh, L'ultimo teorema di Fermat, BUR(1999).
- [15] R. Takloo-Bighash, A Pithagorean Introduction to Number Theory, Springer (2018).
- [16] G. Travaglini, Numbers and Figures, American Mathematical Society (2023).
- [17] Wikipedia, *Diofanto di Alessandria*. https://it.wikipedia.org/wiki/Diofanto_di_Alessandria
- [18] Wikipedia, *Regular number*. https://en.wikipedia.org/wiki/Regular_number

