UNIVERSITA’ DEGLI STUDI DI TRENTO

Facoltà di Scienze Matematiche, Fisiche e Naturali

Relazione

ALGEBRA E TEORIA DEI NUMERI NELLA CULTURA GRECA E ARABA

Studentessa: **Lucia Segnana**

Matricola: **156519**

INTRODUZIONE

La teoria dei numeri è il secondo grande campo della matematica che ci viene dai Pitagorici attraverso Euclide. Il teorema di Pitagora ha portato i matematici allo studio di quadrati e somme di quadrati; Euclide ha richiamato l'attenzione ai numeri primi dimostrando che sono infiniti.
Le ricerche di Euclide erano basate sul cosiddetto algoritmo euclideo, un metodo per trovare il massimo comune divisore di due numeri naturali. I comuni divisori sono la chiave per i risultati di base sui numeri primi, in particolare sulla fattorizzazione unica in numeri primi, che dice che ogni numero naturale si può esprimere come prodotto di numeri primi e che tale rappresentazione è unica.
Un'altra scoperta dei Pitagorici, l'irrazionalità di $\sqrt{2}$, ha ripercussioni nel mondo dei numeri naturali. Poiché $\sqrt{2} \neq m/n$ per qualsiasi numero naturale *m*, *n*, non esiste una soluzione dell'equazione $x^2 - 2y^2 = 0$ appartenente ai numeri naturali. Ma, sorprendentemente, ci sono soluzioni nei numeri naturali di $x^2 - 2y^2 = 1$ e infatti sono infinite.
Lo stesso vale per l'equazione $x^2 - Ny^2 = 1$ per ogni numero naturale non quadrato N.
Quest'ultima equazione, detta equazione di Pell, è forse meno famosa solo dell'equazione di Pitagora $x^2 + y^2 = z^2$, tra tutte le equazioni che ricercano soluzioni intere. Metodi per risolvere l'equazione di Pell per un numero qualsiasi N sono stati scoperti dai matematici indiani.
Le equazioni che cercano soluzioni intere o razionali sono chiamate diofantine, dopo Diofanto. I metodi che ha usato per risolvere le equazioni diofantine quadratiche e cubiche sono ancora oggi di grande interesse.

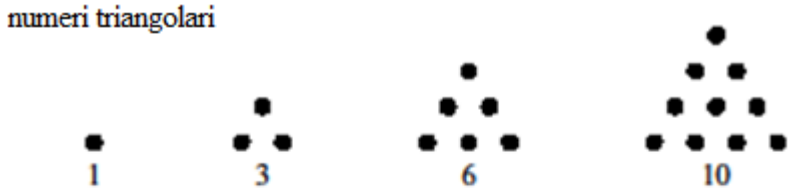
IL RUOLO DELLA TEORIA DEI NUMERI

Per i matematici, la teoria dei numeri è stata importante quasi tanto la geometria. Nonostante questo, la teoria dei numeri non è mai stata sottoposta ad un trattamento sistematico come invece la geometria elementare con gli Elementi di Euclide.
In tutte le fasi del suo sviluppo, la teoria dei numeri ha avuto lacune evidenti a causa dell' intrattabilità di problemi elementari, infatti la maggior parte dei vecchi problemi irrisolti nella matematica, sono semplici questioni sui numeri naturali.
Il ruolo dunque della teoria dei numeri nella storia della matematica è leggermente diversa da quella della geometria. Mentre quest'ultima ha giocato un ruolo unificante e stabilizzante, al punto tale da ritardare un ulteriore sviluppo e creando talvolta l'impressione popolare che la matematica sia un soggetto statico; la teoria dei numeri è stata uno stimolo al progresso e al cambiamento. Prima del 1800, solo pochi matematici hanno contribuito ai progressi nella teoria dei numeri, anche se erano dei grandi della matematica, come Diofanto, Fermat, Eulero, Lagrange e Gauss.
Cercheremo di analizzare i progressi nella teoria dei numeri scaturiti dalle sue connessioni profonde con altre parti della matematica, in particolare con la geometria, visto che questi sono i più significativi per la matematica nel suo complesso, anche se questo comporterà escluderne altri ugualmente interessanti.

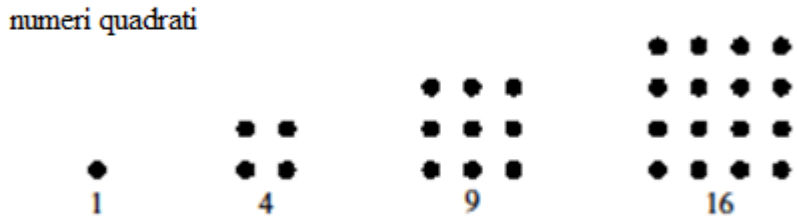
NUMERI POLIGONALI, PRIMI E PERFETTI

Numeri poligonali

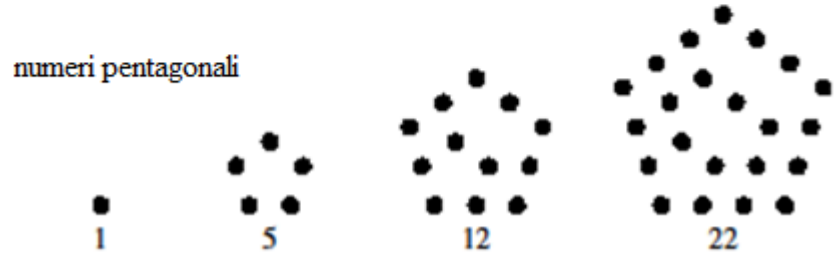
I numeri poligonali, che sono stati studiati dai Pitagorici, sono nati da un trasferimento ingenuo di idee geometriche alla teoria dei numeri. Dalla figura è facile calcolare un'espressione per il *m*-esimo numero n-gonale come somma di una certa serie aritmetica e per dimostrare, per esempio, che un quadrato è la somma di due numeri triangolari. Oltre al lavoro di Diofanto, che contiene i risultati impressionanti sulle somme di quadrati, i risultati greci sui numeri poligonali erano di questo tipo elementare.



$$t_{k+1} = t_k + k + 1$$



$$q_{k+1} = (k+1)^2$$



$$p_{k+1} = \frac{3k^2 - k}{2}$$

Nel complesso, non ci sono grandi teoremi sui numeri poligonali, tranne forse i due seguenti.
I numeri primi sono stati considerati nel contesto geometrico, come i numeri senza rappresentazione rettangolare. Un numero primo, non avendo divisori a parte se stesso e 1, ha solamente una rappresentazione "lineare".
Naturalmente questo è solo una riaffermazione della definizione di primi e la maggior parte dei teoremi sui numeri primi richiedono idee più potenti. Questa è la prova che esistono infiniti numeri primi, che troviamo nel Libro IX degli Elementi di Euclide.

Teorema (Euclide): I numeri primi sono infiniti.

Dimostrazione (per assurdo): prendiamo una collezione finita di primi $p_1, p_2, \dots, p_n$, possiamo considerarne un altro $p = p_1\, p_2\, \cdots\, p_3 + 1$.
Questo numero non è divisibile da $p_1, p_2, \dots, p_n$. Quindi se p è un primo e $p > p_1, p_2, \dots, p_n$, oppure ha un divisore primo $\neq p_1, p_2, \dots, p_n$.

I Greci hanno costruito l'algoritmo di divisione e dimostrato il teorema di unicità di fattorizzazione su $\mathbb{Z}$. Dati $a, b \in \mathbb{Z}\ \exists!\ q, r \in \mathbb{Z}$ t. c. $a = qb + r$; $\forall a \in \mathbb{Z}$, $a = p_1, \dots p_r$ con p_i primi. Questa scrittura è unica a meno del segno.

Numeri perfetti

Un numero perfetto è quello che è uguale alla somma dei suoi divisori propri (includendo l'1, ma escludendo se stesso). Ad esempio, $6 = 1 + 2 + 3$ è un numero perfetto, come è $28 = 1 + 2 + 4 + 7 + 14$. Anche se questo concetto risale ai Pitagorici, si conoscono solamente due teoremi sui numeri perfetti. Euclide conclude il IX libro degli Elementi dimostrando che se $2^n - 1$ è primo, allora $2^{n-1}(2^n - 1)$ è perfetto. Questi numeri perfetti sono naturalmente anche pari e Eulero (1849), anche se in una pubblicazione postuma, ha dimostrato che ogni numero pari perfetto è nella forma di Euclide. La dimostrazione di Eulero è sorprendentemente semplice.

Proposizione: Se $2^n - 1$ è primo, allora $2^{n-1}(2^n - 1)$ è perfetto.

Dimostrazione : Supponiamo che $2^n - 1 = p$ sia primo.
I divisori di $2^{n-1}(2^n - 1)$ sono: $1, 2, 2^2, \dots, 2^{n-1}$ e

$$(2^n - 1),\ 2(2^n - 1),\dots\ 2^{n-2}(2^n - 1) = p,\ 2p, \dots\dots, 2^{n-2}p$$

cioè $\sum_{i=0}^{n-1} 2^i + \sum_{i=0}^{n-2} 2^i\ p$.

Sapendo che $(x^n - 1) = (x - 1)(x^{n-1} + \dots + x + 1)$,

possiamo scrivere $\sum_{i=0}^{n-1} x^i = \frac{x^n - 1}{x - 1}$ da cui segue che

$$\sum_{i=0}^{n-1} 2^i = 2^i = 2^n - 1 \text{ e } \sum_{i=0}^{n-2} 2^i = 2^{n-1} - 1.$$

Allora $\sum_{i=0}^{n-1} 2^i + \sum_{i=0}^{n-2} 2^i\ p = (2^n - 1) + (2^n - 1)(2^{n-1} - 1) = 2^{n-1}(2^n - 1)$.

Non è noto se vi siano numeri perfetti dispari; questo potrebbe essere il più antico problema aperto in matematica.

In vista del teorema di Eulero, l'esistenza di numeri perfetti pari dipende dall'esistenza di primi nella forma $2^n - 1$. Questi sono noti come numeri primi di Mersenne, dopo Marin Mersenne (1588-1648), che per primo ha attirato l'attenzione sul problema del riconoscimento dei numeri primi in questa forma. Non è noto se esistono infiniti numeri primi di Mersenne, anche se uno più grande sembra si riesca a trovare con una certa regolarità. Negli ultimi anni ogni nuovo primo trovato è stato un primo di Mersenne, dando un corrispondente numero perfetto. Il record del 1/02/2014 stabilisce che $2^{57885161} - 1$ sia il più grande primo di Mersenne trovato finora.

Teorema (Eulero): Se *a* è perfetto pari, allora $a = 2^{n-1}(2^n - 1)$ con $(2^n - 1)$ primo.

Il problema è trovare *n* tale che $(2^n - 1) = p$ sia primo. Questo numero è detto primo di Mersenne.
Per $n = 2$ $p = 3$ $a = 6$
Per $n = 3$ $p = 7$ $a = 23$
Per $n = 4$ $p = 15$ $a = 120$.
In quest'ultimo caso 15 non è un numero primo e dunque non è di Mersenne, da cui segue perciò che 1206 non è perfetto.
Quindi come *n* non posso mai prendere un numero pari perché altrimenti posso sempre scomporlo.

L'ALGORITMO DI EUCLIDE

Questo algoritmo è noto da dopo Euclide, perché la sua prima apparizione conosciuta è nel VII libro degli Elementi. Tuttavia, secondo il parere di molti storici, l'algoritmo e alcune delle sue conseguenze erano probabilmente note già in precedenza. Il merito di Euclide è senza dubbio la presentazione magistrale dei fondamenti della teoria dei numeri, basata sul suo algoritmo.
L'algoritmo di Euclide è usato per trovare il massimo comune divisore (MCD) di due numeri interi positivi a, b. Il primo passo è di costruire la coppia (a_1, b_1), dove

$$a_1 = max\,(a,b) - min\,(a,b),$$
$$b_1 = \min(a,b),$$

e poi si ripete semplicemente questa operazione sottraendo il numero minore numero da quello maggiore. Cioè, se la coppia costruita al passo i è (a_i, b_i), allora la coppia costruita a passo $i + 1$ è

$$a_{i+1} = max\,(a_i,b_i) - min\,(a_i,b_i),$$
$$b_{i+1} = \min((a_i,b_i).$$

L'algoritmo termina nella prima fase quando $a_{i+1} = b_{i+1}$ e questo valore comune valore è il $MCD\,(a,b)$. Questo perché prendendo le differenze si conservano tutti i divisori comuni; quindi quando $a_{i+1} = b_{i+1}$ abbiamo

$$MCD\,(a,b) = MCD\,(a_1,b_1) = \cdots = MCD\,(a_{i+1},b_{i+1}) = a_{i+1} = b_{i+1}.$$

La pura semplicità dell'algoritmo fa sì che si possa trarre alcune conseguenze importanti. Euclide, naturalmente, non ha usato la nostra notazione, ma comunque i suoi risultati sono vicini ai seguenti.

1. **Teorema**: $a_n = b_n = MCD\,(a,b)$
   Dimostrazione: Se $c|a$ e $c|d$ allora $c|a_i$ e $c|b_i \Rightarrow c = a_n = b_n$.

   Corollario: Se $MCD\,(a,b) = 1$, allora ci sono interi m, n tali che $ma + nb = 1$.
   Queste equazioni

   $$a_1 = max\,(a,b) - min\,(a,b),$$
   $$b_1 = \min(a,b),$$
   $$\vdots$$
   $$a_{i+1} = max\,(a_i,b_i) - min\,(a_i,b_i),$$
   $$b_{i+1} = \min((a_i,b_i)$$

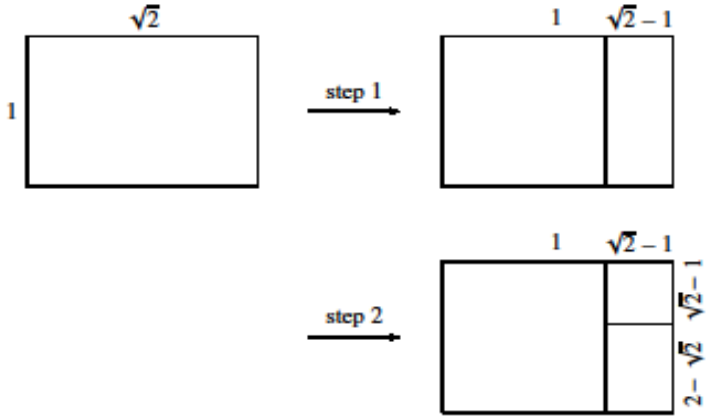
   dimostrano in primo luogo che a_1, b_1 sono combinazioni lineari integrali, $ma + nb$, di a e b, e quindi lo sono anche a_2, b_2, quindi lo sono anche a_3, b_3,…, ed infine questa vale per $a_{i+1} = b_{i+1}$. Ma $a_{i+1} = b_{i+1} = 1$, perciò $MCD\,(a,b) = 1$; quindi $1 = ma + nb$ per alcuni interi m, n.

2. **Proposizione**: Se p è un numero primo che divide ab, allora p divide a o b (la proprietà del divisore primo).
   Dimostrazione: supponiamo che p non divida a. Allora poichè p ha altri divisori tranne 1, abbiamo $MCD\,(p,a) = 1$. Quindi dal risultato precedente otteniamo m, n interi tali che $ma + np = 1$.
   Moltiplicando ogni parte per b otteniamo $mab + nbp = b$.
   Per ipotesi, p divide ab; quindi p divide entrambi i termini sul sinistro lato, e quindi p divide anche il lato destro b.

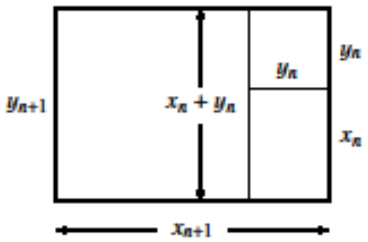
3. **Teorema** (teorema fondamentale dell'aritmetica): Ogni numero intero positivo ha una fattorizzazione unica in numeri primi.
   $\forall\, a \in \mathbb{Z}\ \ \exists!\ \ p_1, \ldots, p_r$ primi unici a meno di segno tali che $a = p_1 \cdot \ldots \cdot p_r$
   Dimostrazione: Supponiamo, per assurdo che qualche intero n abbia due prime diverse fattorizzazioni:
   $a = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$. Rimuovendo i fattori comuni, se necessario, si può supporre che ci sia un p_i che non è tra i q. Ma questo contraddice il precedente risultato, perché p_i divide $a = q_1 q_2 \cdots q_k$, ma non divide individualmente nessun $q_1, q_2, \cdots, q_k$, dal momento che questi sono numeri primi $\neq p_i$.

Sembra che il metodo usato dai greci fosse il metodo di anthyphairesis.
Date due lunghezze a, b, si può definire la sequenza $(a_1, b_1), (a_2, b_2), \ldots$, per sottrazione ripetuta della lunghezza minore alla maggiore. Se a, b sono multipli interi di alcune unità, allora il processo termina …. ma se $b \,/\, a$ è irrazionale, continua sempre. Possiamo ben immaginare che i Pitagorici siano stati interessati all' anthyphairesis applicata ad $a = 1,\ b = \sqrt{2}$.

Ecco cosa succede se le misure non sono dei numeri razionali. Rappresentiamo a, b lati di un rettangolo, e ogni sottrazione del numero più piccolo al più grande è rappresentato da un taglio sul lato più corto. Notiamo che il rettangolo rimanente dopo la fase 2, con i lati $\sqrt{2} - 1$ e $\sqrt{2} - 2 = \sqrt{2}\,(\sqrt{2} - 1)$, e che è un rettangolo proporzionale a quello di partenza, tranne che il lato lungo è ora verticale anziché orizzontale. Ne consegue che le operazioni simili si ripetano sempre, il metodo di antifaresi non finisce mai, e questo è un'altra dimostrazione che $\sqrt{2}$ è irrazionale.



Ci interessa soprattutto la relazione tra i successivi rettangoli simili. Se poniamo i lati lunghi e corti dei successivi rettangoli simili x_{n+1}, y_{n+1} e x_n, y_n, possiamo ricavare un rapporto di ricorrenza per x_{n+1}, y_{n+1}dalla figura:



esattamente i rapporti dei Pitagorici! La differenza è che i nostri x_n, y_n non sono interi e soddisfano $x^2 - 2y^2 = 0$, non $x^2 - 2y^2 = 1$.

Tuttavia, si ha dalla figura soprastante l'interpretazione più naturale di queste relazioni . La scoperta che le stesse relazioni generano soluzioni di $x^2 - 2y^2 = 1$, comporta il desiderio che possibilmente l'algoritmo di Euclide termini con $x_1 = y_1 = 1$. Se i Pitagorici avessero iniziato con $x_1 = y_1 = 1$ e applicato le relazioni di ricorrenza, allora potrebbero aver ben trovato che (x_n, y_n) soddisferebbero $x^2 - 2y^2 = (-1)^n$.

EQUAZIONE DI PELL

L'equazione diofantina $x^2 - Ny^2 = 1$, dove N è un numero intero non quadrato, è nota come equazione di Pell perché Eulero erroneamente ha attribuito una soluzione di essa al matematico inglese del 17 ° secolo Pell (mentre dovrebbe essere attribuita a Brouncker). L'equazione di Pell è probabilmente l'equazione diofantina più conosciuta dopo l'equazione $a^2 + b^2 = c^2$ per le terne pitagoriche, e per certi versi è più importante. Risolvere l'equazione di Pell è il passo principale nella soluzione dell'equazione generale diofantina quadratica in due variabili. L'equazione di Pell fa la sua prima apparizione nelle fondamenta della matematica greca.
L'esempio più semplice dell'equazione di Pell,

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

è stata studiata dai pitagorici in relazione alla $\sqrt{2}$. Se x, y sono soluzioni estese a questa equazione, allora $x/y \approx \sqrt{2}$ e infatti i pitagorici trovarono un modo per generare soluzioni sempre più estese mediante le relazioni ricorrenti:

$$x_{n+1} = x_n + 2\, y_n\ ,$$
$$y_{n+1} = x_n + y_n\ .$$

Utilizzando le relazioni che compaiono nell'antifararesi, con breve calcolo si ottiene che

$$x^2{}_{n+1} - 2y^2{}_{n+1} = -\left(x^2{}_n - 2y^2{}_n\right),$$

così se (x_n, y_n) soddisfa $x^2 - 2y^2 = \pm 1$, allora (x_{n+1}, y_{n+1}) soddisfa $x^2 - 2y^2 = \mp 1$.

Partendo con la soluzione banale $(x_0, y_0) = (1, 0)$ di $x^2 - 2y^2 = 1$, otteniamo infinite soluzioni $(x_2, y_2), (x_4, y_4), \ldots$ dell'equazione $x^2 - 2y^2 = 1$. (Le coppie (x_n, y_n) erano conosciute come numeri laterali e diagonali perché il rapporto y_n / x_n tende a quello del lato e della diagonale in un quadrato.)
Ma inizialmente queste relazioni di ricorrenza come possono essere state scoperte? Van der Waerden (1976) e Fowler (1980, 1982) suggeriscono che la chiave è l'algoritmo di Euclide applicato ai segmenti, un'operazione che i greci chiamavano antifaresi, vista precedentemente.
Molte altri esempi dell'equazione di Pell $x^2 - Ny^2 = 1$ si verificano nella matematica greca e queste possono essere comprese in un modo analogo,applicando antifaresi al rettangolo di lati $1, \sqrt{N}$.
Nel VII secolo d.C. il matematico indiano Brahmagupta ha dato una relazione di ricorrenza per le soluzioni generali di Pell $x^2 - Ny^2 = 1$.

Soluzione dell'equazione di Pell nella matematica indiana

Gli indiani hanno chiamato l'algoritmo di Euclide il "polverizzatore" perché rompe i numeri fino ai pezzi più piccoli. Per ottenere una ricorrenza, bisogna sapere quando un rettangolo è proporzionale all'originale, un fatto che è stato rigorosamente dimostrato solo nel 1768 da Lagrange. Il lavoro europeo sull' equazione di Pell, che ha avuto inizio nel 17 ° secolo con Brouncker e altri, è basata sulla frazione continua di $\sqrt{N}$, sebbene ciò equivale per la stessa cosa come antifaresi.
Un aspetto interessante della teoria è il rapporto molto irregolare tra N e il numero di passi di antifaresi prima che un rettangolo proporzionale ricorra all'originale. Se il numero di passi è grande, la più piccola soluzione non banale di $x^2 - Ny^2 = 1$ è enorme. Un esempio famoso è il cosiddetto problema del bestiame di Archimede (287-212 a.C.). Questo problema porta all'equazione

$$x^2 - 4729494y^2 = 1,$$

la cui soluzione più piccola è stata trovata da Krummbiegel e Amthor (1880) ed ha 206.545 cifre!

Un matematico indiano del 600 riuscì a trovare le soluzioni intere di$(x_1^2 - Ny_1^2)$con $N \neq a^2, a \in \mathbb{N}$. La soluzione è la seguente:

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

Prendiamo l'equazione della forma $x^2 - N\,y^2 = k_i$ con $i = 1, 2$

Se x_1, y_1sono soluzioni di $x^2 - N\,y^2 = k_1$ e x_2, y_2 sono soluzioni di $x^2 - N\,y^2 = k_2$, allora

$x = x_1x_2 + Ny_1y_2$ e $y = x_1y_2 + x_2y_1$ sono soluzioni di $x^2 - N\,y^2 = k_1k_2$.

Se $k_1 = k_2 = 1$, $(x_1, y_1)\,(x_2, y_2)$ è soluzione di $x^2 - N\,y^2 = 1$, allora

$(x_1x_2 + Ny_1y_2,\ x_1y_2 + x_2y_1)$ è soluzione di $x^2 - N\,y^2 = 1$.

Se $k_1 = k_2$, allora

$$\left(\frac{x_1x_2+Ny_1y_2}{k_1^2}, \frac{x_1y_2+x_2y_1}{k_1^2}\right)$$

sono soluzioni di $x^2 - N\,y^2 = 1$.

LE TERNE PITAGORICHE

Pitagora visse intorno al 500 a.C., ma la storia del Teorema di Pitagora comincia molto tempo prima, almeno dal 1800 a.C. in Babilonia. La prova è una tavoletta di argilla che elenca sistematicamente un numero elevato di coppie di interi (a, c) per cui vi è un numero intero b che soddisfa $a^2 + b^2 = c^2$.
Terne intere (a, b, c) che soddisfano il teorema di Pitagora, per esempio (3 , 4 , 5) , (5 , 12 , 13), (8 , 15 , 17), sono note ora come terne pitagoriche. Presumibilmente i Babilonesi erano interessati alla loro interpretazione come i lati del triangolo rettangolo. In ogni caso , il problema di trovare terne pitagoriche interessava anche in altre civiltà antiche: van der Waerden (1983) fornisce esempi provenienti dalla Cina (tra il 200 a.C. e il 220 D.C.) e in India (tra 500 e 200 a.C.). La comprensione più completa del problema in tempi antichi è stato raggiunto nella matematica greca, tra Euclide (circa 300 a.C.) e Diofanto (circa 250 d.C.) .
Ora sappiamo che la formula generale per la generazione di terne pitagoriche è

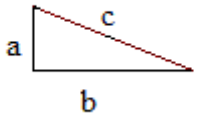
$$a = (p^2 - q^2)r, \qquad b = 2qpr, \qquad c = (p^2 + q^2)r$$

È facile vedere che $a^2 + b^2 = c^2$ quando a, b, c sono dati da queste formule, e naturalmente a, b, c saranno interi se p , q , r lo sono . Anche se i Babilonesi non hanno avuto il vantaggio della nostra notazione algebrica è plausibile che questa formula, o il caso speciale

$$a = (p^2 - q^2), \qquad b = 2qpr, \qquad c = (p^2 + q^2)$$

(che fornisce tutte le soluzioni a, b, c , senza comun divisore) è all'origine per le terne elencate. Le formule meno generali sono state attribuite a Pitagora stesso (attorno al 500 a.C.) ed a Platone; una soluzione equivalente alla formula generale è data negli Elementi di Euclide, nel X libro. Per quanto ne sappiamo, questa è la prima affermazione della soluzione generale e la prima dimostrazione che è generale. La dimostrazione di Euclide è essenzialmente aritmetica, come ci si aspetterebbe poiché il problema sembra appartenere all'aritmetica.
Tuttavia, vi è una soluzione molto più sorprendente, che utilizza l'interpretazione geometrica delle terne pitagoriche. Questo emerge dal lavoro di Diofanto.

Teorema: Dato un triangolo rettangolo come in figura, vale $a^2 + b^2 = c^2$.



Ci sono molte dimostrazioni. Una è questa. Partendo da due quadrati uguali, togliamo 4 triangoli rettangoli uguali a quello di partenza. Nella figura 1 otteniamo due quadrati a^2, b^2 mentre nella figura 2 ottengo un quadrato c^2. La somma di $a^2 + b^2$ vale c^2.

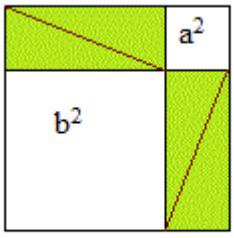


FIGURA 1

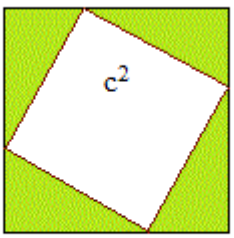


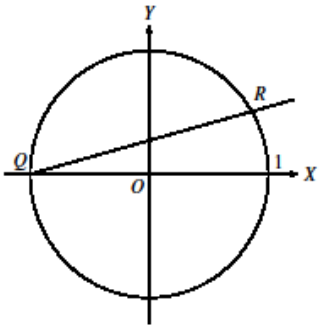
FIGURA 2

Nasce un rapporto tra algebra e geometria.
Nascono così le terne pitagoriche. Certamente già gli Egizi avevano trovato alcuni triangoli rettangoli con lati interi, Diofanto però pose il problema di trovare tutte le soluzioni intere.

Dimostrazione di Diofanto:
Osservazione 1: trovare le soluzioni intere non banali di $a^2 + b^2 = c^2$ è equivalente a trovare tutte le soluzioni razionali di $x^2 + y^2 = 1$

Osservazione 2: parto da una soluzione non banale $Q = (-1, 0)$ di $x^2 + y^2 = 1$. Traccio una retta secante e trovo un altro punto *R*. Ne faccio il sistema:

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



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

Da cui si ha:

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

-1 soluzione banale

$$x_{1,2} = \frac{-t^2 \pm \sqrt{t^4 - t^4 + 1}}{t^2+1} = \frac{-t^2 \pm 1}{t^2+1} = \begin{matrix} \nearrow \\ \searrow \\ \frac{1-t^2}{t^2+1} \end{matrix}$$

Da cui:
$$\begin{cases} x = \dfrac{1-t^2}{t^2+1} \\ y = t\left(\dfrac{1-t^2+t^2+1}{t^2+1}\right) = \dfrac{2t}{t^2+1} \end{cases}$$

Al variare di *t* riesco a coprire tutta la circonferenza. Ottengo una parametrizzazione razionale della circonferenza. Scegliendo *t* razionale, ottengo numeri razionali e viceversa.
Conclusione: scelgo $t = {}^{p}/_{q}$ con $p, q \in \mathbb{N}$

$$\begin{cases} x = \dfrac{1 - \left(\frac{p}{q}\right)^2}{1 + \left(\frac{p}{q}\right)^2} = \dfrac{\frac{q^2-p^2}{q^2}}{\frac{q^2-p^2}{q^2}} = \dfrac{q^2-p^2}{q^2+p^2} \\ y = \dfrac{2\,\frac{p}{q}}{\frac{q^2+p^2}{q^2}} = \dfrac{2pq}{q^2+p^2} \end{cases}$$

Perciò:
$a = q^2 - p^2$
$b = 2pq$
$c = q^2 + p^2$
sono tutte e sole le terne pitagoriche $p, q \in \mathbb{N}$.

$$\begin{cases} a = r(q^2 - p^2) \\ b = (2pq) \\ c = r(q^2 + p^2) \end{cases}$$

Un discepolo di Pitagora ha provato a calcolare la diagonale del quadrato.
Problema: $d = \sqrt{2} = {}^{p}/_{q}$ non è razionale.
Per assurdo prendo *p, q* primi tra loro:
$2q^2 = p^2 \Rightarrow p^2$ pari $\Rightarrow\ p$ pari
$\Rightarrow p = 2r\ \Rightarrow 2q^2 = 4r^2 \Rightarrow q^2 = 2r^2 \Longrightarrow q^2$è pari $\Longrightarrow q$ pari
Ma p, q sono assunti primi tra loro. Assurdo.

IL RITORNO DELLA TEORIA DEI NUMERI

Dopo l'opera di Diofanto, la teoria dei numeri in Europa ha languito per circa 1000 anni . In Asia c'era stato un progresso significativo su temi come l'equazione di Pell. I primi segni di risveglio in Europa arrivarono nel 14° secolo, quando Levi ben Gershon trovò le formule per il numero di permutazioni e combinazioni, utilizzando rudimentali prove di induzione .
L'interesse per la teoria dei numeri guadagnò velocità con la riscoperta di Diofanto da parte di Bombelli e la pubblicazione di una nuova edizione da Bachet de M'eziriac (1621). E' stato questo libro che ha ispirato Fermat e ha lanciato la teoria dei numeri come una disciplina della matematica moderna.
Fermat estese le tecniche di Diofanto, come la corda e il metodo della tangente per la ricerca di punti razionali su curve cubiche.
Egli ha anche spostato l'attenzione dalle soluzioni razionali alle soluzioni intere. Ha dimostrato "piccolo teorema di Fermat " che $n^p p - n$ è divisibile per *p* per ogni primo *p*, ed ha formulato "l'ultimo teorema di Fermat " che $x^n + y^n = z^n$ non ha soluzioni intere positive quando $n > 2$.
Sappiamo che Fermat aveva una prova del suo " ultimo teorema " per $n = 4$, ma sembra abbia commesso un errore nel pensare che avrebbe potuto provarlo per un *n* arbitrario. La prova ora conosciuta utilizza idee altamente sofisticate, non immaginabili nel 17° secolo. Tuttavia, è interessante notare che la dimostrazione moderna riduce l'ultimo teorema di Fermat ad un problema sulle curve cubiche.

TRA DIOFANTO E FERMAT

Alcuni importanti risultati nella teoria dei numeri sono stati scoperti nel Medioevo, anche se non sono riusciti a mettere radici fino a quando furono riscoperti nel 17° secolo o più tardi . Tra questi c'erano la scoperta del triangolo di Pascal e il "teorema del resto cinese" da parte di matematici cinesi e formule per permutazioni e combinazioni di Levi ben Gershon (1321).

I cinesi usarono il triangolo di Pascal come mezzo per generare e tabulare i coefficienti binomiali, cioè i coefficienti che verificano nelle formule

$(a + b)^1 = a + b$

$(a + b)^2 = a^2 + 2ab + b^2$

$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

e così via . Quando i coefficienti binomiali sono tabulati come segue (con una banale riga 1 aggiunta nella parte superiore , corrispondente alla potenza 0 di a + b) ,

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

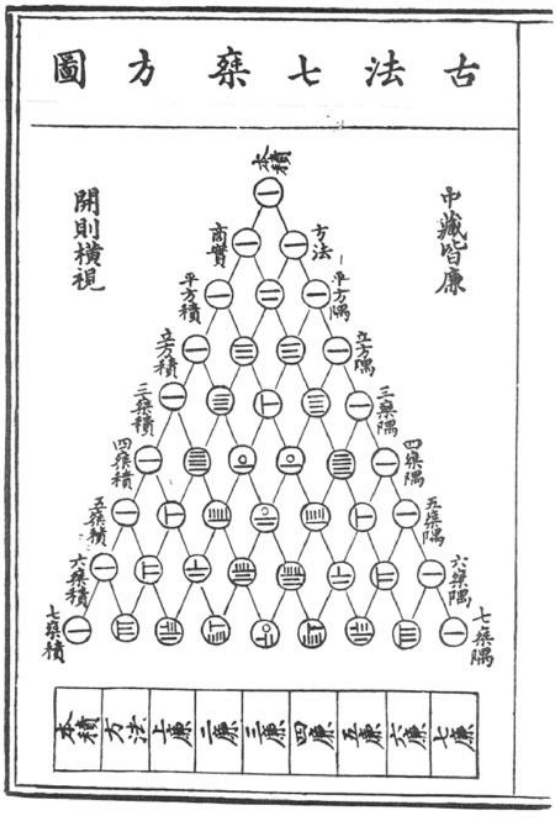
1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

e così via, l'elemento k-esimo $\binom{n}{k}$ dell' n-riga è la somma $\binom{n-1}{k-1}+\binom{n-1}{k}$dei due elementi sopra di esso nell' $(n - 1)$ -esima riga , come segue dalla formula

$$(a + b)^n = (a + b)^{n-1}a + (a + b)^{n-1} b.$$

Il triangolo sembra avere una profondità di sei Yang Huì (1261) e una profondità di otto in Zhu Shijiè (1303). Yang Huì attribuisce il triangolo a Jia Xiàn, vissuto nell' 11° secolo.



il numero $\binom{n}{k}$ appare negli scritti ebraici medievali come il numero di combinazioni di n oggetti presi k alla volta. Levi ben Gershon (1321) dà la formula

$$\binom{n}{k} = \frac{n!}{(n-k)!\,k!}$$

unitamente al fatto che ci sono n! permutazioni di n elementi.

Alla luce di questi risultati, perché chiamiamo la tabella dei coefficienti binomiali "triangolo di Pascal"? Non è ovviamente l'unico esempio di un concetto matematico chiamato con il nome di uno riscopritore, ma in ogni caso Pascal ha sicuramente più merito.

Nel suo trattato, Pascal (1654) univa la teoria algebrica e combinatoria mostrando che gli elementi del triangolo aritmetico possono essere interpretati in due modi: come i coefficienti di $a^{n-k}b^k$ in $(a + b)^n$ come il numero di combinazioni di n oggetti presi k volte. In effetti, ha dimostrato che $(a + b)^n$ è una funzione generatrice per il numero di combinazioni. Come applicazione, ha fondato la teoria matematica della probabilità, risolvendo il problema della divisione equa della posta di gioco e come metodo di dimostrazione ha usato l'induzione matematica per la prima volta in un modo davvero consapevole e inequivocabile.

TRIANGOLI RETTANGOLI RAZIONALI

"L'area di un triangolo rettangolo i cui lati sono numeri razionali non può essere un numero quadrato. sono finalmente riuscito a dimostrare questa proposizione, che è una mia scoperta, anche se non senza fatica. Io do la prova qui, in quanto questo metodo consentirà straordinari sviluppi nella teoria dei numeri**."**

Fermat (1670)

Questa è la 45° osservazione di Fermat su Diofanto, rispondendo ad un problema posto da Bachet: trovare un triangolo rettangolo la cui area equivale ad un numero dato. L'osservazione è importante non solo per il teorema e il metodo annunciato, ma anche perché è la dimostrazione completa lasciata da Fermat nella teoria dei numeri. Come bonus, la dimostrazione risolve implicitamente l'ultimo teorema di Fermat per n = 4 ed è un esempio eccellente del suo "metodo" di discendenza infinita, che ha effettivamente portato a sviluppi straordinari nella teoria dei numeri.
Il principio logico coinvolto nel metodo di Fermat di discendenza è naturalmente lo stesso su cui si basa l'induzione matematica: qualsiasi insieme di numeri naturali ha almeno un elemento. Tuttavia, le circostanze in cui i due metodi possono essere applicati sono molto diverse. Con l'induzione, è necessaria un'ipotesi idonea per fare il passo di induzione; con la discendenza, è invece necessaria una quantità idonea per discendere. In pratica, la discendenza è un metodo molto più speciale, essendo associato con le proprietà geometriche di alcune curve.

Teorema di Fermat
Per ogni $n > 2$, $\nexists\, x, y, z \in \mathbb{Z}$ non nulli tale che $x^n + y^n = z^n$.

Per $n = 2$ otteniamo le terne pitagoriche descritte da Diofanto.
Per $n = 3$ l'ha dimostrato Eulero.
Per $n = 4$ l'ha dimostrato Fermat.

Lemma: Non esistono triangoli rettangoli con lati razionali e area quadrato.
dimostrazione:
Supponiamo per assurdo che esista un tale triangolo. Posso disporre che i lati siano interi e primi tra loro (eventualmente faccio il m.c.m. tra i tre lati razionali e uso quelli come base). Trovo un triangolo rettangolo con lati interi la cui area è un quadrato più piccolo del precedente. Assurdo (Ogni sottoinsieme di $\mathbb{N}$ ha un minimo.)

Dimostro che trovo un triangolo i cui lati sono: $p^2 - q^2, 2pq, p^2 + q^2$.
Possiamo dire che il $M.C.D.(p, q) = 1$ (altrimenti i lati non sarebbero primi tra loro); inoltre $p^2 - q^2$ non è pari $\Rightarrow (p - q), (p + q)$ sarebbero dispari.
Quindi $q, p, p + q, p - q$ sono a due a due primi tra loro.
Perciò se $pq(p^2 - q^2) = pq(p + q)(p - q)$ è un quadrato, allora $p = r^2, q = s^2$

$$(\blacklozenge)\begin{cases} p + q = r^2 + s^2 = t^2 \\ p - q = r^2 - s^2 = u^2 \end{cases}$$

Usiamo l'unicità della fattorizzazione in $\mathbb{Z}$.

$\overset{(\blacklozenge)}{\Longrightarrow} t^2 - u^2 = 2s^2 \Longrightarrow$ o $(t - u)$ o $(t + u)$ è pari $\Rightarrow$ sono pari entrambi

$\Rightarrow t - u = 2a; \quad t + u = t - u + 2u = 2a + 2u = 2(a + u)$

$$\Rightarrow t - u = 2w, \quad t + u = 2x \quad \Rightarrow \quad s^2 = \frac{(t + u)(t - u)}{2} = 2wx.$$

Nota: $M.C.D.(w, x) = 1$ perché $M.C.D.(p, q) = 1$.

Quindi , o $\begin{matrix} w = y^2 \\ x = 2z^2 \end{matrix}$ o $\begin{matrix} w = 2z^2 \\ x = y^2 \end{matrix}$

$\Longrightarrow t = w + x = y^2 + 2z^2$.

Consideriamo il triangolo rettangolo di cateti y^2 e $2z^2$; l'ipotenusa è $h = \sqrt{y^4 + 4z^4}$

$\Rightarrow\ h^2 = (\mathrm{y}^2)^2 + \ (2\mathrm{z}^2)^2 = \frac{1}{2}((y^2 + 2z^2)^2 + (y^2 - 2z^2)^2) = \frac{1}{2}(t^2 + u^2) = r^2 \quad \Rightarrow \quad \mathrm{h} = \mathrm{r} \in \mathbb{N}$

L'area di questo triangolo è $y^2z^2 = (yz)^2$.
L'ipotenusa $h = r < 2pq$ cioè il cateto del triangolo di partenza. Assurdo.

Grande teorema di Fermat *n=4*

dimostrazione: Supponiamo per assurdo che esistano $x, y, z\ \in \mathbb{N}$ tali che $x^4 + y^4 = z^4$. Quindi:

$$x^4 + y^4 = z^4 = (z^2)^2$$

Sia $p = z^2$ e $q = x^2$ e prendiamo il triangolo rettangolo con lati $p^2 - q^2, 2pq, p^2 + q^2$ (Diofanto).
L'area di questo triangolo è

$$\frac{2pq(p^2 - q^2)}{2} = z^2x^2(z^4 - x^4) = z^2x^2y^4 = (zxy^2)^2$$

Assurdo.

Bibliografia:

[1] Mathematics and its History, Johnn Stillwell, Springer, 2010

[2] Appunti del corso