GAUSS (1834) : DE NEXU INTER MULTITUDINEM CLASSIUM, IN QUAS FORMAE BINARIAE SECUNDI GRADUS DISTRIBUUNTUR, EARUNQUE DETERMINANTEM

Leonardo Colzani   Università degli Studi di Milano-Bicocca

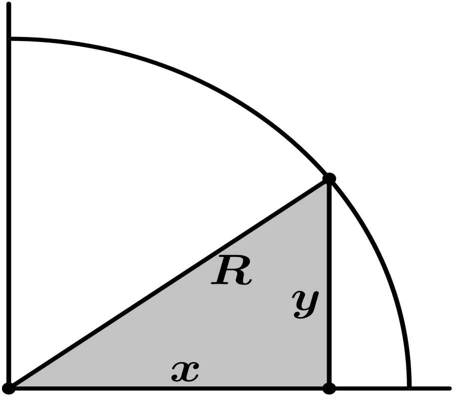
Prerequisiti

Non è necessario essere fluenti in greco e latino. È sufficiente conoscere un po' di geometria analitica. Le forme binarie di secondo grado nel titolo sono l'equazione di un cerchio nel piano cartesiano.

Teorema (Pitagora) :
Il quadrato sull'ipotenusa è la somma dei quadrati sui cateti.

Corollario :
L'equazione di un cerchio con centro nell'origine e raggio R è

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



$$R = \sqrt{x^2 + y^2}$$

Un problema (falsamente) elementare

Problema :
In quanti modi diversi si può cambiare una banconota da 10 euro in pezzi da 1, 2, 5 euro?

Incognite :

$$\begin{cases} x & \text{monete da 1 euro,} \\ y & \text{monete da 2 euro,} \\ z & \text{banconote da 5 euro,} \end{cases}$$

Relazione tra le incognite :

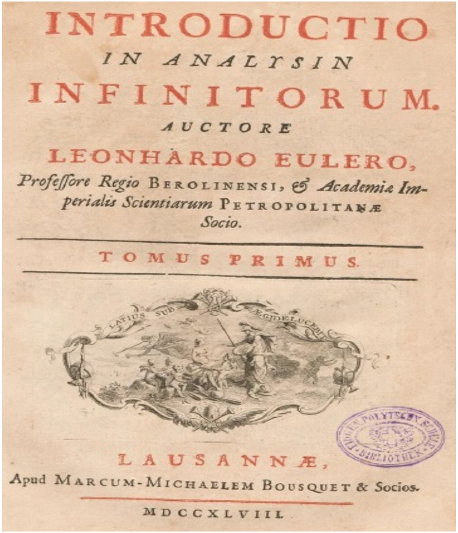
$$x,\ y,\ z \geq 0, \quad 1 \cdot x + 2 \cdot y + 5 \cdot z = 10.$$

Esempio :
Il cambio di 10 euro in quattro monete da un euro, tre da due euro, e nessuna banconota, corrisponde alla soluzione $(x, y, z) = (4, 3, 0)$.

Leonardo Eulero (1707-1783)

In quanti modi diversi si può scomporre un numero intero positivo nella somma di interi positivi ?

Leonhardo Eulero *"Introductio in Analysin Infinitorum"*, *Caput XVI*, *De partitione numerorum*.


INTRODUCTIO
IN ANALYSIN
INFINITORUM.
AUCTORE
LEONHARDO EULERO,
Professore Regio BEROLINENSI, & Academiæ Imperialis Scientiarum PETROPOLITANÆ Socio.

TOMUS PRIMUS.

LAUSANNÆ,
Apud MARCUM-MICHAELEM BOUSQUET & Socios.
MDCCXLVIII.

Diofanto d'Alessandria (III secolo d.C.)

Problema :
Dato un polinomio con coefficienti interi in un certo numero di variabili $P(x, y, z, ...)$ ed un intero n, determinare se esistono e, se esistono, trovare esplicitamente le soluzioni intere $(x, y, z, ...)$ dell'equazione

$$P(x, y, z, ...) = n.$$

Problema del cambio di monete :
Se i tagli delle monete sono A, B, C,..., e la somma da cambiare è n, contare il numero di soluzioni intere non negative dell'equazione

$$Ax + By + Cz + ... = n.$$

Interpretazione geometrica :
$\{Ax + By = n\}$ Equazione di una retta nel piano cartesiano.
$\{Ax + By + Cz = n\}$ Equazione di un piano nello spazio.

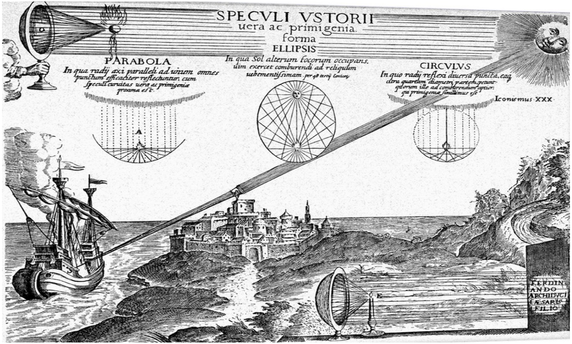
Forme lineari e quadratiche

Definizione :
Le forme lineari sono polinomi omogenei di primo grado con coefficienti interi in un certo numero di variabili $P(x, y, z, ...)$.

Definizione :
Le forme quadratiche sono polinomi omogenei di secondo grado con coefficienti interi in un certo numero di variabili $P(x, y, z, ...)$.

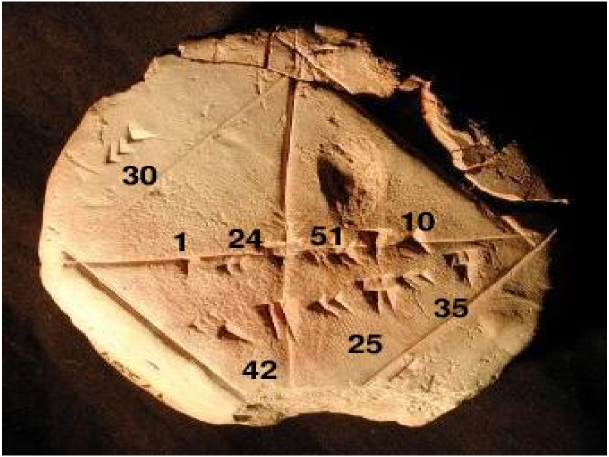
Coniche :

$$Ax^2+Bxy+Cy^2 = n.$$



Pitagora (VI secolo a.C.) : Tutto è numero

YBC 7289 : Teorema di Pitagora in Mesopotamia 4000 anni fa



$$\sqrt{2} = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = \frac{30547}{21600} = 1.41421...$$

Pitagora (VI secolo a.C.) e Euclide (IV secolo a.C.) : $x^2 + y^2 = z^2$

Problema :
Trovare tutti i triangoli rettangoli con lati interi.
Trovare tutte le soluzioni intere dell'equazione $x^2 + y^2 = z^2$.

Esempi :
$(3, 4, 5) \quad (5, 12, 13) \quad (8, 15, 17) \quad (7, 24, 25) \quad (20, 21, 29)$ ...

Teorema (Euclide, Elementi, Libro X) :
Le soluzioni (x, y, z) senza divisori comuni dell'equazione

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

si ottengono a partire da due interi m e n, primi tra lora, uno pari e l'altro dispari, con la formula

$$\begin{cases} x = m^2 - n^2 \ , \\ y = 2mn \ , \\ z = m^2 + n^2 \ . \end{cases}$$

Plimpton 322 : Terne pitagoriche prima di Pitagora

Archimede di Siracusa (III secolo a.C.) : $x^2 - n \cdot y^2 = 1$

Misura del cerchio : $x^2 - 3 \cdot y^2 = 1$ $\qquad \dfrac{x}{y} = \dfrac{1351}{780} \approx \sqrt{3}.$

Problema dei buoi : $x^2 - 410286423278424 \cdot y^2 = 1$ $\qquad (206545).$

Equazioni diofantee

Una equazione diofantea è un'equazione algebrica con coefficienti interi di cui si ricercano le soluzioni intere.

Teorema facile :
Un intero che diviso per 4 dà resto 3 non è mai somma di due quadrati di numeri interi, $4n + 3 \neq x^2 + y^2$.

Teorema difficile (Fermat 1640 e Eulero 1747) :
Ogni numero primo che diviso per 4 dà resto 1 è somma di due quadrati, $p = x^2 + y^2$, e questa scomposizione è unica.

Teorema più difficile (Lagrange 1770) :
Ogni intero positivo è somma di quattro quadrati, $n = x^2 + y^2 + z^2 + w^2$.

Teorema ancora più difficile (Gauss 1796 e Legendre 1797) :
Un intero positivo è somma di tre quadrati, $n = x^2 + y^2 + z^2$, se e solo se non è della forma $4^h \left(8^k + 7\right)$.

$x^n + y^n = z^n$

Pierre de Fermat

(Beaumont de Lomagne
17 agosto 1601 - Castres
12 gennaio 1665)

Lisez Euler, il est le maître de nous tous

Leonhardo Eulero

(Basilea 15 aprile 1707 - San Pietroburgo 18 settembre 1783)

Se fossi stato ricco, probabilmente non mi sarei dato alle matematiche

Giuseppe Luigi Lagrangia

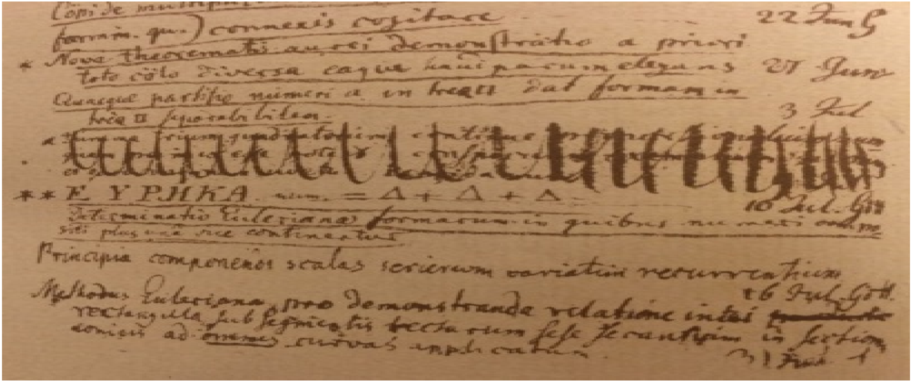
(Torino 25 gennaio 1736 - Parigi 10 aprile 1813)

Princeps mathematicorum

Johann Friedrich Carl Gauss

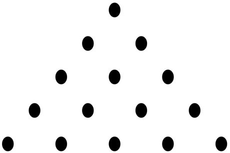
(Braunschweig 30 aprile 1777 - Gottinga 23 febbraio 1855)

(10 Luglio 1796) EYPHKA : $num = \Delta + \Delta + \Delta$



Teorema (Gauss) :
Ogni numero è somma di tre numeri triangolari :

$$n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2}.$$



G.H.Hardy & S.Ramanujan : $x^3 + y^3 = n$

*I (**Hardy**) remember once going to see him (**Ramanujan**) when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. No, he replied, it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways.*

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

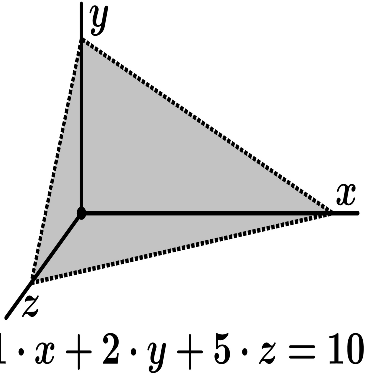
Geometria dei numeri

Molti problemi di teoria dei numeri hanno una interpretazione geometrica in spazi a più dimensioni. La dimensione è il numero delle incognite.

Problema :
In quanti modi diversi si può cambiare una banconota da 10 euro in pezzi da 1, 2, 5 euro?

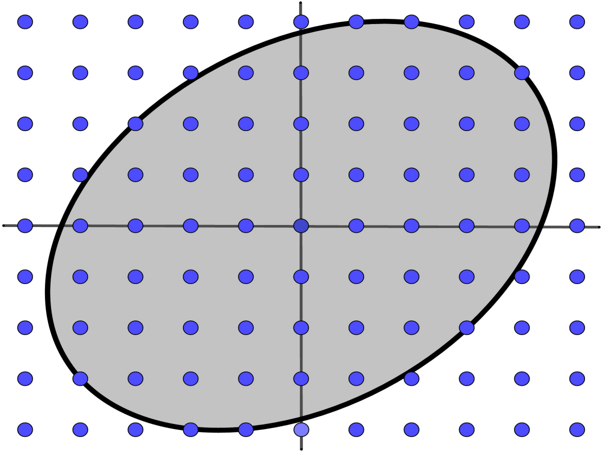
Interpretazione geometrica :
Le soluzioni (x, y, z) sono i punti a coordinate intere nel triangolo

$$\{x, y, z \geq 0,\ 1 \cdot x + 2 \cdot y + 5 \cdot z = 10.\}.$$



Geometria dei numeri

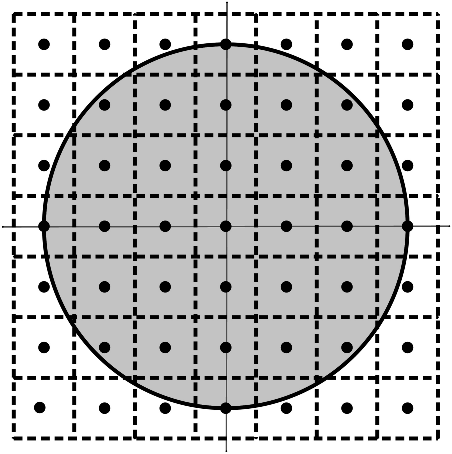
Problema :
Contare il numero di punti $(x, y, z, w, ...)$ con coordinate intere in una regione di uno spazio di dimensione uguale al numero di variabili.



Geometria con la carta a quadretti: Area e punti interi

Per stimare l'area di una figura basta dividere il piano in piccoli quadrati, e contare i quadrati contenuti nella figura. Per eliminare l'ambiguità dei quadrati solo parzialmente contenuti nella figura, si può decidere di contare solo i quadrati con centro contenuto nella figura.

Ogni punto intero è il centro di un quadrato con lato 1. L'area di una figura è circa uguale all'area dei quadrati con centri nella figura. Per stimare l'area basta contare i punti interi. Per stimare i punti interi basta calcolare l'area.



Disquisitiones Arithmeticae

Nelle *Disquisitiones Aritmeticae - Sectio quinta - De formis aequationibusque indeterminatis secundi gradus* (1801) Gauss studia le equazioni diofantee di secondo grado:

$$Ax^2 + Bxy + Cy^2 \; = \; n.$$

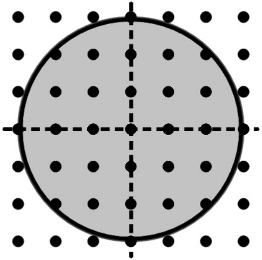
Nella memoria *De nexu inter multitudinem classium, in quas formae binariae secundi gradus distribuuntur, earunque determinantem* (1834) Gauss studia il numero di soluzioni intere della disequazione

$$Ax^2 + Bxy + Cy^2 \; \leq \; n.$$

Problema del cerchio di Gauss

Contare i punti interi nel cerchio con centro nell'origine e raggio R

$$x^2 + y^2 \; \leq \; R^2$$



Area di un cerchio di raggio R : $\quad \pi \cdot R^2$

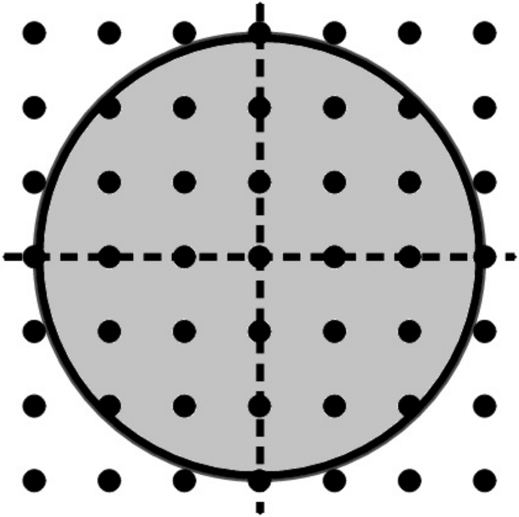
L'area di un cerchio di raggio 3 è $\pi \cdot 3^2$, ed il cerchio con centro l'origine e raggio 3 contiene 29 punti interi.

Se si uguaglia l'area $\pi \cdot 3^2$ ai 29 punti interi, si ottiene una approssimazione di π :

$$\pi \cdot 3^2 \approx 29$$

$$\pi \approx 29/9 = 3,222...$$

$$\frac{|\pi - 29/9|}{\pi} \approx 2,5\%$$



Punti interi in un cerchio (formula esplicita)

Teorema :

Il numero di punti con coordinate intere nel cerchio $\left\{x^2 + y^2 \leq R^2\right\}$ è

$$\sum_{-R \leq n \leq +R} \left(1 + 2\left[\sqrt{R^2 - n^2}\right]\right).$$

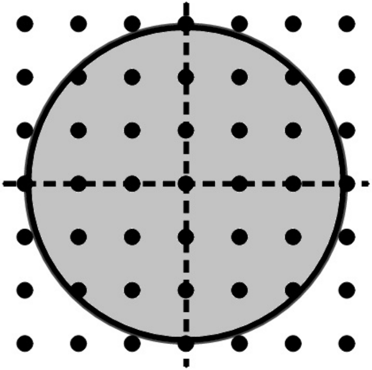
N.B. $[X]$ è la parte intera di X, si buttano via le cifre dopo la virgola.

$$x^2 + y^2 \ \leq \ R^2,$$

$$y^2 \ \leq \ R^2 - x^2,$$

$$|y| \ \leq \ \sqrt{R^2 - x^2}.$$

In ogni retta $x = n$ i punti interi sono $1 + 2\left[\sqrt{R^2 - n^2}\right]$.



Punti interi in un cerchio (formula furba)

Teorema (Gauss 1834) :
Il numero di punti con coordinate intere nel cerchio $\left\{x^2+y^2 \leq R^2\right\}$ è

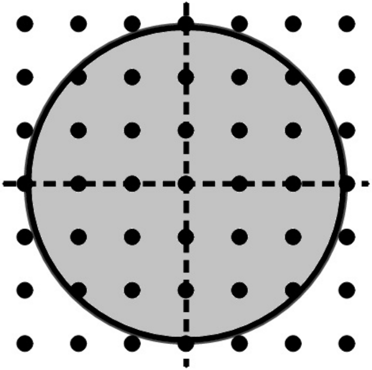
$$1+4\,[R]+4\left[R/\sqrt{2}\right]^2+8\sum_{R/\sqrt{2}<n<R}\left[\sqrt{R^2-n^2}\right].$$

N.B. $[X]$ è la parte intera di X, si buttano via le cifre dopo la virgola.

$N(R) \;=\;$ Numero di punti interi nel cerchio $\left\{x^2+y^2 \leq R^2\right\}$.

R	$N(R)$	$N(R)-\pi R^2$
10	317	3
100	31417	1
1000	3141549	-44
10000	314159053	-212

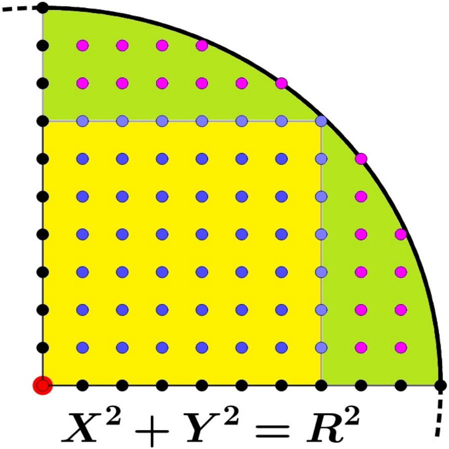
N.B. : $\pi \;=\; 3,1415926535\ldots$



Punti interi in un cerchio

I punti interi nel cerchio si possono dividere in quattro sottoinsiemi :

$$\begin{cases} A = \{\text{Origine}\}\,, \\ B = \{4 \text{ Semiassi}\}\,, \\ C = \{4 \text{ Quadrati }\}\,, \\ D = \{8 \text{ Segmenti di cerchio}\}\,. \end{cases}$$



$$A + B + C + D \;=\; 1 + 4\,[R] + 4\left[R/\sqrt{2}\right]^2 + 8 \sum_{R/\sqrt{2}<n<R} \left[\sqrt{R^2 - n^2}\right].$$

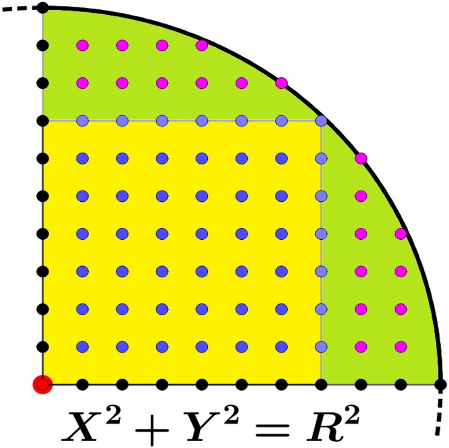
Punti interi in un cerchio di raggio 10

$\{\text{Origine}\} = 1$

$\{\ 4\ \text{Semiassi}\} = 4 \times 10$

$\{\ 4\ \text{Quadrati}\} = 4 \times 7^2$

$\{\ 8\ \text{Segmenti}\} = 8 \times (6 + 4)$

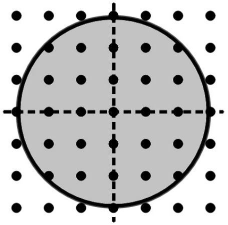


$$1 + 4 \times 10 + 4 \times 7^2 + 8 \times (6 + 4) = 317$$

$$317 = 3,17 \times 10^2 \qquad \pi \approx 3,17$$

Discrepanza tra area e punti interi in un cerchio

R	$N(R)$	$N(R) - \pi R^2$
10	317	3
100	31417	1
1000	3141549	-44
10000	314159053	-212

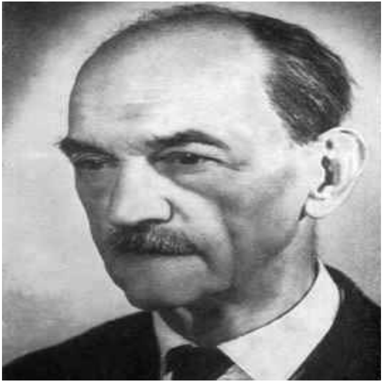


Teorema (Gauss 1834) :
In un cerchio di raggio $R \geq 1$ la differenza tra il numero di punti interi $N(R)$ e l'area πR^2 è minore del perimetro $2\pi R$,

$$\left| N(R) - \pi R^2 \right| \ < \ 2\pi R.$$

Congettura (aperta da più di 100 anni) :
La differenza tra l'area ed il numero di punti interi è molto più piccola del perimetro. Questa differenza non è mai troppo più grande della radice quadrata del perimetro.

V.Jarnik & H.Steinhaus



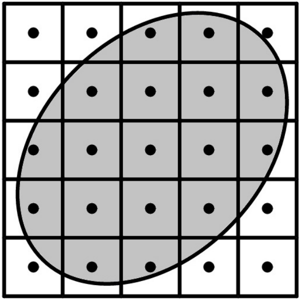
Teorema (Jarnik e Steinhaus 1947) :
La differenza tra il numero di punti interi N e l'area A all'interno di una curva piana semplice di lunghezza $L \geq 1$ è minore del perimetro,

$$|N - A| < L.$$

Discrepanza tra area e punti interi

Teorema (Jarnik e Steinhaus) : Se $N(\Omega)$ è il numero di punti interi in un dominio piano Ω e se $A(\Omega)$ e $L(\Omega)$ sono l'area ed il perimetro del dominio, allora

$$|N(\Omega) - A(\Omega)| \; < \; L(\Omega).$$

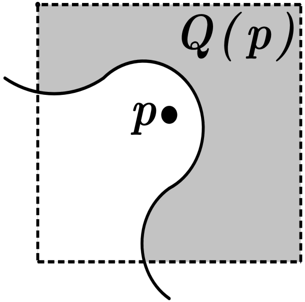


Dimostrazione : Ad ogni punto intero p si associa il quadrato $Q(p)$ con centro nel punto e lati di lunghezza uno paralleli agli assi.

$$
\begin{aligned}
&|N(\Omega) - A(\Omega)| \\
&= \left| \sum_p N\left(\Omega \cap Q(p)\right) - A\left(\Omega \cap Q(p)\right) \right| \\
&\leq \sum_p \left| N\left(\Omega \cap Q(p)\right) - A\left(\Omega \cap Q(p)\right) \right| .
\end{aligned}
$$

Discrepanza tra area e punti interi

Un quadrato esterno alla curva dà un contributo 0 sia all'area che ai punti interi, quindi non contribuisce all'errore. Un quadrato interno alla curva dà un contributo 1 sia all'area che ai punti interi, quindi non contribuisce all'errore. Solo i quadrati che intersecano la curva danno un contributo all'errore, e il contributo di ognuno di questi quadrati è minore della lunghezza della parte di curva contenuta nel quadrato.

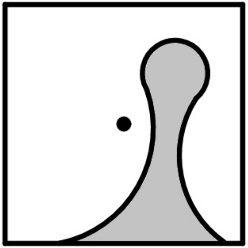


$$\sum_p |N(\Omega \cap Q(p)) - A(\Omega \cap Q(p))| \leq \sum_p L(\Omega \cap Q(p)) = L(\Omega).$$

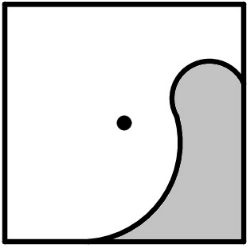
Discrepanza tra area e punto intero in un quadrato

$$N\left(\Omega \cap Q(p)\right) - A\left(\Omega \cap Q(p)\right) \leq L\left(\Omega \cap Q(p)\right).$$

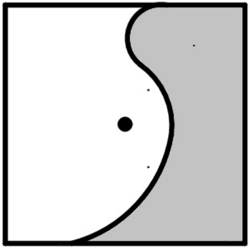
Il contributo all'errore di ogni quadrato è uguale all'area della parte di quadrato che non contiene il punto intero, e quest'area è minore della lunghezza della parte di curva contenuta nel quadrato.



(1) La curva entra ed esce dallo stesso lato.



(2) La curva entra ed esce da lati adiacenti.



(3) La curva entra ed esce da lati opposti.

Nelle figure il dominio può essere sia la parte chiara che quella scura, ma l'errore è la parte scura, quella che non contiene il punto intero.

Georg Alexander Pick

Georg Alexander Pick
(Vienna 10 agosto 1859 - Campo di concentramento di Theresienstadt 26 luglio 1942)

Teorema (Pick 1899) :
In un poligono semplice con vertici in punti interi, l'area A, il numero di puntiinteri interni al poligono I, ed il numero di punti interi sul bordo B, sono legati dalla relazione

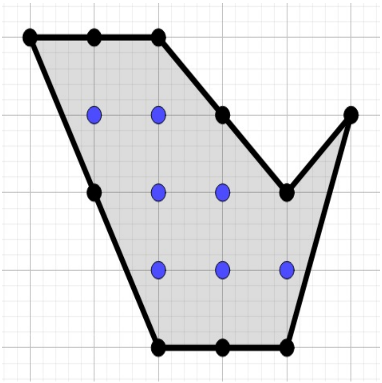
$$A = I + B/2 - 1.$$

Poligoni interi

Teorema (Pick 1899) :
In un poligono semplice con vertici in punti interi, l'area A, il numero di puntiinteri interni al poligono I, ed il numero di punti interi sul bordo B, sono legati dalla relazione

$$A = I + B/2 - 1.$$

Dimostrazione :
(1) Se la formula vale per due poligoni disgiunti P e Q, allora vale anche per la loro unione $P \cup Q$.
(2) La formula vale per i triangoli.
(3) Ogni poligono può essere scomposto in triangoli.

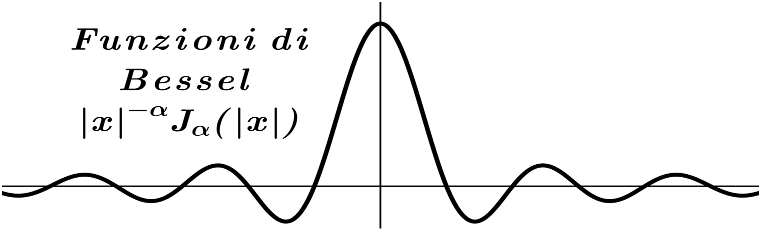


$$\begin{cases} \text{Punti interni } I = 7 \\ \text{Punti sul bordo } B = 10 \\ \text{Area } A = I + B/2 - 1 = 11 \end{cases}$$

Media e varianza del numero di punti interi in una sfera

Teorema :
Il numero di punti a coordinate interi in una sfera in $\mathbb{R}^d$ con raggio R e centro x è una funzione periodica di del centro con sviluppo in serie di Fourier

$$\sum_{n\in\mathbb{Z}^d} R^{d/2}|n|^{-d/2}J_{d/2}\left(2\pi R|n|\right) exp\left(2\pi in\cdot x\right).$$




GRAZIE PER L'ATTENZIONE