Teoria dei Numeri
Cenni storici

Alessandra Bernardi

19 febbraio 2018, Trento

Persone

- Pitagora (600 a.C)
- Euclide (300 a.C)
- Diofante (250 d.C)
- **Fermat** ($\sim$ 1601–1665) Teoria dei numeri.
- Eulero (1707–1783)
- Lagrange (1736–1813)
- Legendre (1752–11833)
- Gauss (1777–1855)
- Dedekind (1831–1916) Teoria Algebrica dei numeri.
- Kronecker (1823–1891)
- Kummer (1810–1893)
- Eisenstein (1823–1852)
- Minkowski (1864–1909)
- Dirichlet (1805–1859)
- Riemann (1826–1866) Metodi Analitici.
- Hadamard (1865–1963)
- La Vallée Poussin (1866–1962)
- Hilbert (1862–1943)
- Andrew Wiles (1953–) Metodi Geometrici.

Pitagora (600 a.C)

Il teorema di Pitagora forse è di origine babilonese.
Di sicuro a Pitagora si può attribuire la scoperta degli intervalli (scala musicale).
Per i pitagorici la matematica ha un aspetto mistico:

- Numeri amicabili: $\sum$(divisori di n)$= m$, $\sum$(divisori di m)$= n$ (es. 220, 284), (6=1+2+3 numero perfetto).
- Tutto è un numero (razionale).

Questa credenza andò in frantumi con la scoperta di $\sqrt{2}$:

$$1^2 + 1^2 = x^2 \Rightarrow x = \sqrt{2}.$$

MUSICA

Pitagora (600 a.C)

Il teorema di Pitagora forse è di origine babilonese.
Di sicuro a Pitagora si può attribuire la scoperta degli intervalli (scala musicale).
Per i pitagorici la matematica ha un aspetto mistico:

- Numeri amicabili: $\sum$(divisori di n)$= m$, $\sum$(divisori di m)$= n$ (es. 220, 284), (6=1+2+3 numero perfetto).
- Tutto è un numero (razionale).

Questa credenza andò in frantumi con la scoperta di $\sqrt{2}$:

$$1^2 + 1^2 = x^2 \Rightarrow x = \sqrt{2}.$$

MUSICA

Pitagora e la musica

Pitagora si era accorto che la nostra percezione del suono poteva essere messa in relazione a grandezze misurabili:

$$\begin{array}{cccccccc} DO_1 & DO_2 & SOL_2 & DO_3 & MI_3 & SOL_3 & SIb_3 & DO_4 \\ n & 2n & 3n & 4n & 5n & 6n & 7n & 8n \end{array}$$

(lunghezza della corda e frequenza) Da queste si calcolano le altre:

$$\text{Una quinta di } DO_1 : \; SOL_1 = \frac{SOL_2}{2} = \frac{3n}{2}$$

$$RE_1 = \frac{RE_2}{2} = \frac{1}{2}\left(\frac{3SOL_1}{2}\right) = \frac{9}{8}SOL_1, \; (RE_2 \text{ è una quinta di } SOL)$$

Pitagora e la musica

Con i rapporti di quinta e ottava si possono creare le altre note della scala:

Nota	DO_1	RE_1	MI_1	FA_1	SOL_1	LA_1	SI_1	DO_2
Frequenza	1	9/8	81/64	4/3	3/2	27/16	243/128	2

1 tono, rapporto tra le frequenze $= 9/8$,
1 semitono, rapporto tra le frequenze $= 256/243$.

Solo due tipi di intervalli: tono e semitono.
9/8 e 256/243 non sono proporzionali $\Rightarrow$ NON SI PUÒ DIVIDERE L'OTTAVA IN PARTI PROPORZIONALI.
Problema quando si cambia tonalità.

Pitagora e la musica

Un altro problema della scala pitagorica è il rapporto di terza e di sesta che dopo alcune ottave "stona" con le prime. Questo problema viene risolto dalla "intonazione naturale" di Gioseffo Zarlino (1558 Venezia) (ma non lo trattiamo).

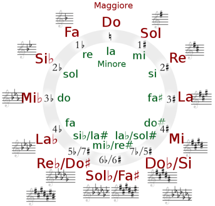
Questo problema dell'intonazione si vede dal ciclo delle quinte che si usa per accordare uno strumento ad accordatura fissa percorrendo il ciclo delle quinte.

Dopo 7 ottave si ritorna alla nota fondamentale MA il DO_8 pitagorico (nemmeno quello naturale) non coincide con quello del ciclo delle quinte.

Pitagora e la musica

Un altro problema della scala pitagorica è il rapporto di terza e di sesta che dopo alcune ottave "stona" con le prime. Questo problema viene risolto dalla "intonazione naturale" di Gioseffo Zarlino (1558 Venezia) (ma non lo trattiamo).
Questo problema dell'intonazione si vede dal ciclo delle quinte che si usa per accordare uno strumento ad accordatura fissa percorrendo il ciclo delle quinte.
Dopo 7 ottave si ritorna alla nota fondamentale MA il DO_8 pitagorico (nemmeno quello naturale) non coincide con quello del ciclo delle quinte.

Pitagora e la musica



DO_1 " ha frequenza" 1. Dopo 12 quinte il DO_8 "ha frequenza" $\left(\frac{3}{2}\right)^{12} = \frac{531441}{4096}$.
Ripartiamo da questa nota (con questa frequenza) e torniamo indietro di 6 ottave, dovremo atterrare al DO_2, MA $\frac{DO_8}{2^6} = \frac{3^{12}}{2^{18}} = \frac{531441}{262144} > 2 = DO_2$

STONA!

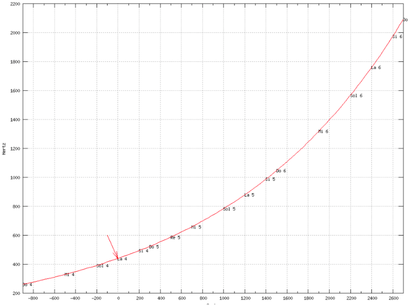
Il problema è che nel temperamento pitagorico le frequenze delle ottave sono multiple di 2^n mentre nel ciclo delle quinte le frequenze sono multiple di $\left(\frac{3}{2}\right)^n$ e NESSUNA potenza di 2 è anche potenza di $3/2$.

Per poter risolvere questo problema serve di nuovo $\sqrt{2}$ (o meglio $\sqrt[12]{2}$) (ma lo hanno scoperto solo nel 1700).

L'altezza percepita di un intervallo musicale non si basa sulle differenze delle frequenze tra i due suoni che lo compongono ma sul loro rapporto. Quindi data una nota, per ottenerne un'altra basta moltiplicare o dividere la frequenza per un dato numero: non percepiamo la differenza tra due note ma la differenza dei loro logaritmi.

$$\log \frac{\nu_2}{\nu_1} = \log \nu_2 - \log \nu_1 .$$

Perciò la disposizione più naturale per le frequenze è la scala logaritmica (*temperamento equabile*).



Ogni ottava è divisa in 12 intervalli uguali (semitoni) e si distribuiscono le note lungo la scala logaritmica. Il rapporto di ottava è fissato a 2. Quindi un intervallo di un semitono è $\sqrt[12]{2}$.
Perciò la frequenza di ogni nota (corrispondente ad un tasto del pianoforte) prima o dopo è moltiplicata per $\sqrt[12]{2}$.
In questo modo i rapporti di frequenza sono identici a partire da qualunque punto della scala, quindi si può passare da una tonalità all'altra senza problemi di accordatura.

Euclide (300 a.C)

Con Euclide si può dire che nasca la matematica come scienza logico-deduttiva.
Negli "Elementi" si parla di

- *Numero primo*,
- Cardinalità infinita dei numeri primi,
- Divisione euclidea,
- Teorema fondamentale dell'aritmetica (*Ogni numero naturale si scrive in modo "unico" come prodotto di numeri primi*),
- Se $n = 2^{p-1}(2^p - 1)$ e se $2^p - 1$ è primo, allora n è un numero perfetto ($\sum$ (divisori di $N)_{>0} = N$). Ci vorrà però Eulero per dimostrare che ogni numero perfetto è di questa forma.

Diofante (250 d.C)

È il primo a studiare soluzioni intere (o razionali) di equazioni a più incognite (*Equazioni Diofantee*):

- $ax + by = 1$ ha soluzione $\Leftrightarrow$ $\mathrm{MCD}(a, b) = 1$.
- $x^2 - Dy^2 = 1$ (Equazione di Pell 1611–1685) ha infinite soluzioni intere.
- $x^n + y^n = z^n$ ha infinite soluzione per $n = 2$ (Pitagora), 0 soluzioni per $n > 2$ (ultimo teorema di Fermat, A. Wiles 1994).

Fermat ($\sim$ 1601–1665)

Rilegge Diofante e nasce la teoria dei numeri.
Fu il primo che cercò dei metodi propri dell'aritmetica che non fossero applicazioni dell'analisi o della geometria all'aritmetica. Ma di questi metodi conosciamo solo quello della "discesa infinita": *Sia* $\{a_n\} \subset \mathbb{N}$ *una successione di numeri naturali infinita, quindi* a_n *è costante da un certo indice in poi. Se si riesce a dimostrare che questo è vero anche per un valore più piccolo di* n *allora si ha l'assurdo.*

Example

L'equazione diofantea di secondo grado

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

non ha soluzioni intere non banali.
Supponiamo ne esista una (la più piccola): $x_0^2 + y_0^2 = 3(z_0^2 + w_0^2)$, quindi $x_0^2 + y_0^2 \equiv 0\,(mod\,3)$, perciò $3|x_0$ e $3|y_0$, dunque $(3x_1)^2 + (3y_1)^2 = 3(z_0^2 + w_0^2)$ da cui si ha $3(x_1^2 + y_1^2) = z_0^2 + w_0^2$. Come prima $3|z_0$ e $3|w_0$. Quindi $x_1^2 + y_1^2 = 3(z_1^2 + w_1^2)$ ma $(x_0, y_0, z_0, w_0) > (x_1, y_1, z_1, w_1)$. Assurdo.

Fermat ($\sim$ 1601–1665)

Theorem (Piccolo teorema di Fermat)

Se $a \in \mathbb{Z}$ e p primo, allora

$$a^p \equiv a \,(mod\, p).$$

Theorem (Teorema dei due quadrati)

Se p è un primo dispari, allora

$$p \equiv x^2 + y^2 \Leftrightarrow p \equiv 1 \,(mod\, 4).$$

(La dim. è dovuta a Eulero.)

Theorem (Teorema dei quattro quadrati)

Ogni numero naturale si scrive come somma di al più quattro quadrati.
(La dim. è dovuta a Lagrange.)

Theorem (Equazione di Fermat per $n = 3$)

Se $x^3 + y^3 = z^3$ allora $xyz = 0$.

Fermat ($\sim$ 1601–1665)

Ho trovato una bellissima dimostrazione del fatto che l'equazione

Theorem (Fermat Last Theorem)

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

non ha soluzione intere non banali se $n \geq 3$

ma il margine è troppo stretto perché io possa riportarla qui.

Fermat ha dato la dim solo per $n = 3, 4$.

Per risolvere questa congettura i matematici hanno inventato la teoria degli ideali, la teoria algebrica dei numeri... A. Wiles con l'aiuto di Taylor nel 1995 riuscì a dimostrarlo usando (l'allora inaspettata) teoria delle curve ellittiche.

Fermat ($\sim$ 1601–1665)

Ho trovato una bellissima dimostrazione del fatto che l'equazione

Theorem (Fermat Last Theorem)

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

non ha soluzione intere non banali se $n \geq 3$

ma il margine è troppo stretto perché io possa riportarla qui.
Fermat ha dato la dim solo per $n = 3, 4$.
Per risolvere questa congettura i matematici hanno inventato la teoria degli ideali, la teoria algebrica dei numeri... A. Wiles con l'aiuto di Taylor nel 1995 riuscì a dimostrarlo usando (l'allora inaspettata) teoria delle curve ellittiche.

Fermat ($\sim$ 1601–1665)

Ho trovato una bellissima dimostrazione del fatto che l'equazione

Theorem (Fermat Last Theorem)

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

non ha soluzione intere non banali se $n \geq 3$

ma il margine è troppo stretto perché io possa riportarla qui.
Fermat ha dato la dim solo per $n = 3, 4$.
Per risolvere questa congettura i matematici hanno inventato la teoria degli ideali, la teoria algebrica dei numeri... A. Wiles con l'aiuto di Taylor nel 1995 riuscì a dimostrarlo usando (l'allora inaspettata) teoria delle curve ellittiche.

1729: Goldbach informa Eulero:

Theorem (di Fermat FALSO)

$$2^{2^n} + 1 \textit{ è primo}$$

Il controesempio lo troverà **Eulero**:

$$\text{per } n = 5: \ 641 | 2^{2^5} + 1.$$

Eulero ha dimostrato tante delle affermazioni di Fermat:

- Ha generalizzato l'equazione di Fermat,
- Ha dimostrato il caso $n = 3$ dell'equazione di Fermat,
- Ha dimostrato il teorema dei due quadrati.

Eulero è noto come il "calcolatore spregiudicato":

$$1 - 1 + 1 - 1 + 1 - 1 + \cdots = \frac{1}{2}.$$

Eulero ha rimesso in moto la teoria dei numeri.

Lagrange (1736–1813)

- Dimostra il teorema dei 4 quadrati.
- Risolve l'equazione di Pell: Se D non è un quadrato, l'equazione $x^2 - Dy = 1$ ha un'infinità di soluzioni intere.
- Getta le basi delle Forme quadratiche intere: è stato il primo ad accorgersi che forme quadratiche congruenti rappresentano gli stessi interi (classificazione delle forme quadratiche per congruenza).

Legendre (1752–11833)

Credeva di aver dimostrato la legge di reciprocità quadratica ma gli sarebbe servito il teorema di Dirichlet.

Theorem (Legge di reciprocità quadratica)

Siano p, q primi dispari.

- *Se $p \equiv 1 \pmod 4 \Rightarrow x^2 \equiv p \pmod q$ ha soluzione sse $y^2 \equiv q \pmod p$ ha una soluzione;*
- *Se p e q sono entrambi $\equiv 3 \pmod 4 \Rightarrow x^2 \equiv p \pmod q$ ha soluzione sse $y^2 \equiv q \pmod p$ non ha soluzione.*

Theorem (Teorema di Dirichlet)

Dati due numeri interi coprimi a e b, esistono infiniti primi della forma $a + nb$, dove $b > 0$ $(n \in \mathbb{N})$.
(Equivalentemente: Ogni progressione aritmetica siffatta contiene infiniti numeri primi.)

Gauss (1777–1855)

Nel 1801 pubblica "Disquisitiones arithmeticae": Spartiacque nella storia della teoria dei numeri. Oltre a trattare argomenti già noti introduce molte novità:

- Per la prima volta si vede la notazione $a \equiv b\,(mod\; n)$,
- Forme quadratiche (composizione, teoria del genere, calcolo del class number di campi quadratici, prima dimostrazione della legge di reciprocità quadratica),
- Polinomi ciclotomici (= polinomio monico le cui radici sono tutte e sole le radici n-esime dell'unità) (questo porta alla costruzione con riga e compasso del poligono regolare con 17 lati).

"La matematica è la regina delle scienze e la teoria dei numeri è la regina della matematica."

Dopo Gauss l'accelerazione è notevole: Dedekind (1831–1916), allievo di Gauss, getta le basi della teoria algebrica dei numeri. Importanti contributi sono dovuti a Kronecker (1823–1891), Kummer (1810–1893), Eisenstein (1823–1852), Minkowski (1864–1909).
Nel frattempo Dirichlet (1805–1859) introduce metodi analitici, ma è Riemann (1826–1866), altro allievo di Gauss, ad usare metodi analitici complessi ed ad aprire orizzonti nuovi.
La congettura di Riemann è tuttora IL problema aperto della matematica. Lo studio dei lavori e dei metodi di Riemann porteranno Hadamard (1865–1963) e de La Vallée Poussin (1866–1962) a dimostrare (1896), in modo indipendente, il teorema dei numeri primi.

Da Hilbert (1862–1943) a oggi

Hilbert (1862–1943), nel 1897 pubblica "Theorie der algebraischen Zahlkoerper" (Zahlbericht). Questo libro rimarrà per decenni il testo di riferimento della teoria dei numeri. Con questo testo e lavori annessi Hilbert sistema la teoria algebrica dei numeri e la "class field theory". Altri contributi importanti di Hilbert riguardano il problema di Waring:

$$a_1^d + \cdots + a_r^d = n$$

con $a_i, n \in \mathbb{Z}$ (importantissimi risvolti in geometria algebrica e nella decomposizione tensoriale in moltissime applicazioni attuali - Filogenetica, Quantum Information, Signal Processing, Big Data Analysis...)

$$F = L_1^d + \cdots + L_r^d$$

con L_i forme lineari e F polinomio omogeneo di grado d.
Dopo Hilbert l'accelerazione è ancora maggiore.
La teoria dei numeri è stata prima elementare, poi algebrica e analitica, adesso è anche geometrica.