Bruno Rizzi (1935-1995) e la teoria dei numeri

Franco Eugeni

Presidente Accademia Piceno Aprutina dei Velati

Direttore Uni-Macagno

La matematica discreta

- A) matematica finita: campi di Galois, Geometrie finite, Disegni, …
- B) matematica del numerabile: teoria dei numeri, numeri primi, funzioni aritmetiche, …
- C) applicazioni: crittografia, crittoanalisi, firma elettronica, autenticazione,…

10^{87}

MATEMATICA FINITA: ESEMPI

- **Come disporre 10 macchine in un parcheggio da 100 posti!**

$$\binom{100}{10} = \binom{100}{90} = \frac{100 \cdot 99 \cdot \ldots \cdot 91}{10 \cdot 9 \cdot \ldots \cdot 3 \cdot 2 \cdot 1} > 9^{10}$$

10^{87}

- **Costruire famiglie di 110 decine di posti tali che assegnati due posti esiste una sola decina che li contiene!**

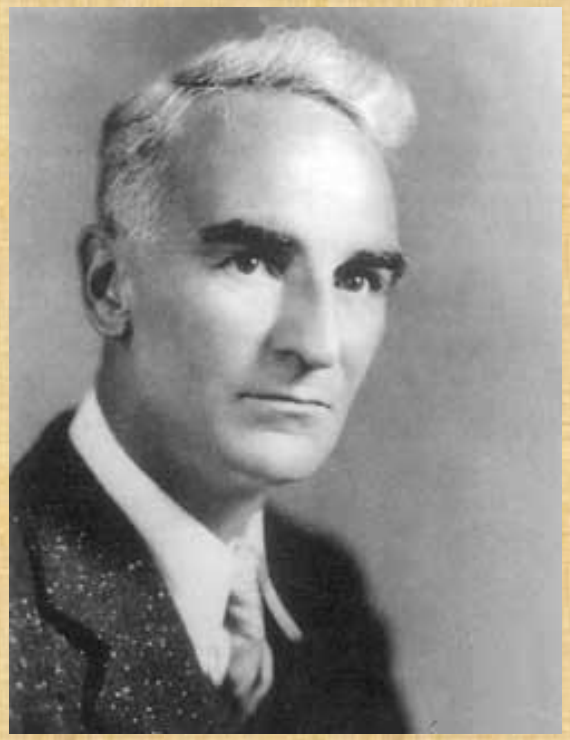
$$\left(\begin{pmatrix}100\\10\end{pmatrix}\right) > \begin{pmatrix}9^{10}\\110\end{pmatrix} = \frac{9^{10}\cdot\left(9^{10}-1\right)\cdot\ldots\cdot\left(9^{10}-110\right)}{110!} > 10^{110}$$

Distanza terra-Alpha Centauri 10^{13} km !

Massa della terra 5,98 x 10^{24} Kg !

Numero degli Elettroni dell'universo 10^{87}

Teoria delle funzioni aritmetiche



Eric Temple Bell
(1883 - 1960)

Michele Cipolla
(1880-1947)

Franco Pellegrino (1908 - 1979)

Libero Docente in Teoria dei Numeri
Ricercatore presso

l'Istituto Nazionale di Alta Matematica fondato da Francesco Severi.

La funzione di Eulero

- **Se *n* è un numero naturale, allora**

$$\Phi(n)$$

è la cardinalità dell'insieme M dei numeri *m* non superiori ad *n* e primi con n, cioè l'insieme M dei numeri m, tali che:

$$1 \leq m \leq n$$

$$(m\ ;\ n) = 1$$

Proprietà della funzione di Eulero

(Proprietà moltiplicativa)

$$\forall m,n \quad t.c.(m;n)=1 \Rightarrow$$

$$\Phi(m \bullet n) = \Phi(m)\Phi(n)$$

(Formule di calcolo)

$$\Phi(n) = n\sum_{p|n}(1-\frac{1}{p})$$

$$\sum_{d|n} \Phi(d) = n$$

Proprietà varie della $\Phi(n)$

1. è il numero delle radici primitive della equazione

$$x^n = 1$$

2. Dalla congruenza di Eulero

$$(a;m) = 1 \Rightarrow a^{\Phi(m)} \equiv 1 (\mathrm{mod}\, m)$$

Nell'anello delle classi resto mod *m* l'inversa della classe a, esiste se a è primo con *m*, ed è

$$a \cdot a^{\Phi(m)-1} = 1$$

La teoria delle funzioni aritmetiche

- Una funzione aritmetica è una funzione

$$f : \mathbb{N} \longrightarrow \mathbb{C}$$

$\mathbb{N}$ naturali da 1 in poi

$\mathbb{C}$ campo dei numeri complessi

$\mathcal{H}$ insieme delle funzioni aritmetiche

Struttura vettoriale di $\mathcal{H}$

$\forall n \in \mathbb{N}$, poniamo

$\forall$

- $(f+g)(n) := f(n) + g(n)$
- $(kf)(n) := k\, f(n)$

quali che siano le funzioni f,g e il numero complesso k

Spazio hilbertiano numerico complesso

Moltiplicazione integrale "convoluzione"

Per ogni n di $\mathbb{N}$, poniamo

$$(f \times g)(n) := \sum_{d|n} f(d)g(n/d)$$

$(\mathcal{H}, +, \times)$ è un anello commutativo ed integro, anzi un'algebra (con la moltiplicazione per lo scalare k).

E' a fattorizzazione essenzialmente unica !

Struttura dell'anello $\mathcal{H}$

funzioni invertibili : f(1) diverso da zero!

Isomorfismi

L’algebra delle funzioni aritmetiche è’ isomorfa all’algebra dei polinomi con una infinità numerabile di variabili, rispetto alla somma ordinaria e la moltiplicazione di polinomi! Questa algebra è a fattorizzazione essenzialmente unica!

(Cashwell ed Everett (1961)).

L’algebra delle funzioni aritmetiche è’ isomorfa all’algebra delle serie formali di Dirichlet rispetto alla somma ordinaria e la moltiplicazione ordinaria!

La funzione u costantemente pari ad uno

u(n)=1 per ogni n !

La funzione unità a

a(n) =1 se n =1, a(n) =0 se n >1

La funzione identica N

N(n)=n per ogni n

Sono tutte funzioni moltiplicative!

La funzione $\nu(n)$ data dal numero dei divisori di n

$$\nu(p^{\alpha}) = \alpha + 1$$
$$\nu\left(\Pi p_i^{\alpha_i}\right) = \Pi(\alpha_i + 1)$$

La funzione $\sigma(n)$ data dalla somma dei divisori di n

$$\sigma(p^{\alpha}) = 1 + p + \ldots + p^{\alpha} = p^{\alpha} - 1 / p - 1$$
$$\sigma(\Pi p^{\alpha}) = \Pi \sigma(p^{\alpha})$$

Funzioni moltiplicative, invertibili per essere f(1) =1!

$$\Phi, \mu, u, a, N, \nu, \sigma$$

La funzione **a** è l'elemento unità per l'operazione X

- Infatti, per ogni funzione f , si ha:

$$f \mathbin{X} a = a \mathbin{X} f = f$$

$$(fXa)(n) = f(n)a(1) + \ldots + f(n/d)\, a(d) + \ldots = f(n)$$

essendo :

$a(1) = 1$ e $a(d) = 0$ se $d > 1$

La funzione μ di Mobius è una funzione moltiplicativa definita come segue:

$$\mu(1) = 1$$

$$\mu(p_1 p_2 \ldots . p_k) = (-1)^k$$

$$\mu(n) = 0$$

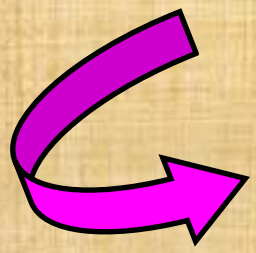
se...n...non..è..libero..da..quadrati!

$$\mu \times u = a$$

$$(\mu \times u)(1) = \mu(1)u(1) = 1 = a(1)$$

$$(\mu \times u)(p^{\alpha}) = {}_{\mu}\mu(1)u(p^{\alpha}) + \mu(p)u(p^{\alpha-1}_{\mu}) = 0 = a(p^{\alpha})$$

$$(\mu \times u)\left[\Pi p^{\alpha}\right] = \Pi\left[(\mu \times u)(p^{\alpha})\right] = 0 = a\left[\Pi p^{\alpha}\right]$$



$$u, \mu$$

sono una l'inversa dell'altra rispetto all'operazione X !

Si passa al calcolo simbolico!

$$\sum_{d|n} \Phi(d) = n$$

$$\sum_{d|n} \Phi(d) = \sum_{d|n} \Phi(d) u(n/d) = n = N(n)$$

$$\Phi \times u = N \qquad \Phi = N \times \mu$$

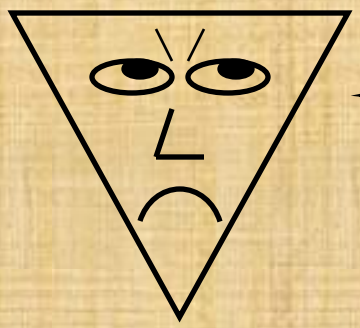
CRITTOGRAFIA

T ⌧ M ⟶ M ⌧ R

Disturbi

T ⌧ *La nuova formula è* ⌧ R

MXPTZSTRPUE



Ho letto tutto ma non ho capito niente!

Il problema dell'Autenticazione e della firma

Pagare al Signor C:
£ Un Milione

MANIPOLAZIONE ILLEGALE

Pagare a Mr. X:
£ Dieci Milioni

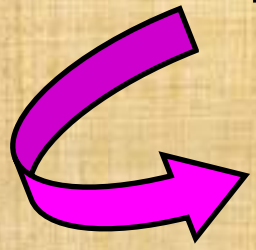
CODICE RSA

1977

Rivest – Shamir – Adleman

CIFRARI A CHIAVE PUBBLICA

… è un numero ottenuto dal prodotto di due numeri primi molto grandi che restano segreti



Funzione di Eulero
Teorema di Fermat-Eulero

- **N = pq**
- **N noto in pubblico elenco , p e q NO**

Il problema è calcolare p e q dalla:

$\Phi(pq)$ **=(p-1)(q-1) = pq - (p+q) +1 …….da cui:**

pq = N

p+q = N+1 - $\Phi(N)$

Dovrei conoscere $\Phi(N)$ **senza passare per i primi di scomposizione!**

NON LO SAPPIAMOFARE!

L’algebra delle serie formali di Dirichlet

s è la variabile complessa

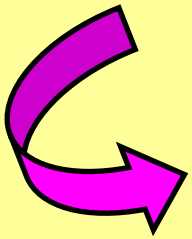
$$F(s) = \sum_{n=1}^{\infty} f(n) n^{-s}$$

$$F(s)G(s) = \sum_{n=1}^{\infty} (f \times g)(n) n^{-s}$$

La zita di Rieman e la sua inversa

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty} u(n) n^{-s}$$

$$M(s) = \sum_{n=1}^{\infty} \mu(n) n^{-s}$$



$$M(s)\zeta(s) = \sum_{n=1}^{\infty} (\mu \times u)(n) n^{-s} = a(1) = 1$$

La serie formale della $\Phi(n)$

$$E(s) = \sum_{n=1}^{\infty} \Phi(n) n^{-s} = \sum_{n=1}^{\infty} (N \times \mu)(n) n^{-s} =$$

$$= \sum_{n=1}^{\infty} N(n) n^{-s} \sum_{n=1}^{\infty} \mu(n) n^{-s} = \frac{1}{\zeta(s)} \sum_{n=1}^{\infty} n^{-(s-1)} =$$

$$= \frac{\zeta(s-1)}{\zeta(s)}$$