



Prof. André Vignatti — DINF - UFPR



# NA GRÉCIA ANTIGA

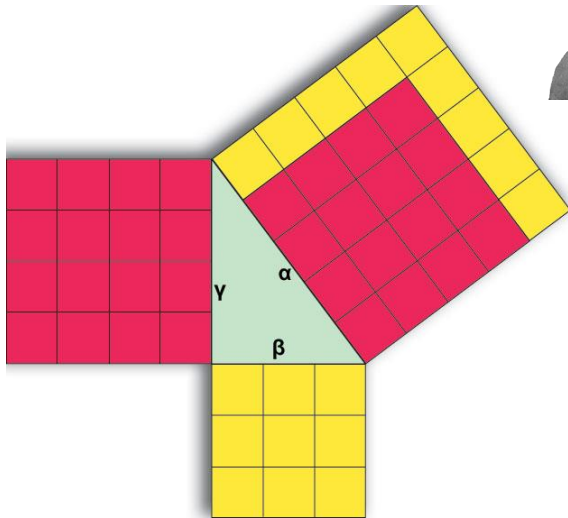
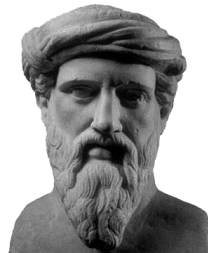


Pensadores: como ganhar uma discussão?



## 1ª Tentativa: Argumentos Visuais

Ex: Teorema de Pitágoras



## 2ª Tentativa: Argumentos Lógicos:

1. Deus é Amor
2. Amor é Cego
3. Steve Wonder é Cego

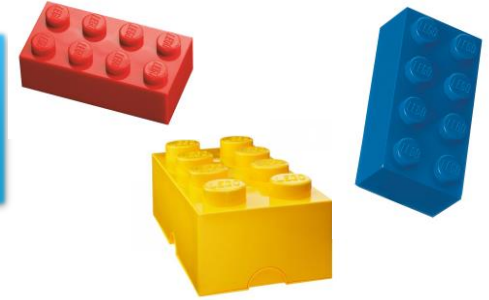
CONCLUSÃO: Steve Wonder é Deus!



VERDADEIRO OU FALSO?

# AXIOMAS E TEOREMAS

**Axioma:** verdade evidente, aceita sem questionamentos



**Teorema:** verdade deduzida logicamente através de outras verdades



Grécia Antiga: o que é “deduzir logicamente”?





# PAUSA DE 2000 ANOS...





# LÓGICA BOOLEANA ( $\approx 1847$ )

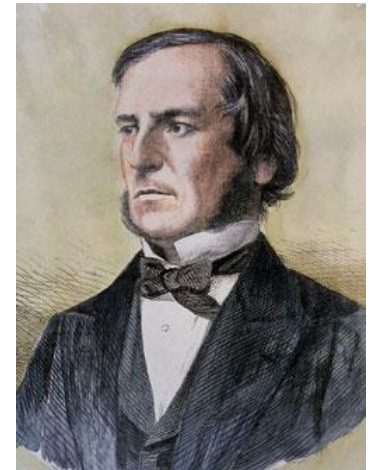
Deduções Lógicas = Fazer “contas” com lógica

## Álgebra Booleana:

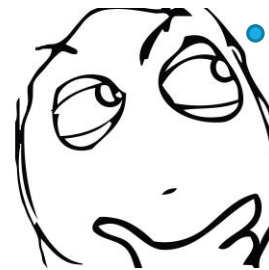
- operadores: e, ou, não
- operandos: V, F

## Exemplos:

- “2 é *par*” é VERDADEIRO
- “3 é *par*” é FALSO
- “2 é *par* e 3 é *par*” é FALSO
- “2 é *par* e 4 é *par* e 6 é *par* e 8 é *par* e 10 é *par* e 12 é *par* e 14 é *par* e 16 é *par* e 18 é *par* e 20 é *par* e 22 é *par* e 24 é *par* e 26 é *par* ...” é VERDADEIRO



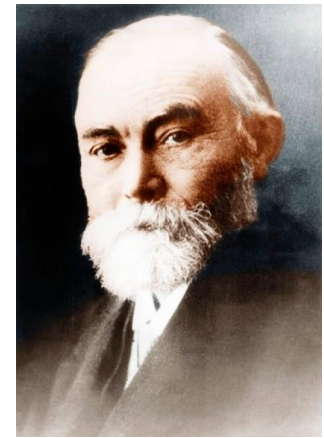
Construções com  
fundações sólidas  
e boa argamassa



# LÓGICA DE PREDICADOS ( $\approx 1884$ )

Melhora a lógica booleana:

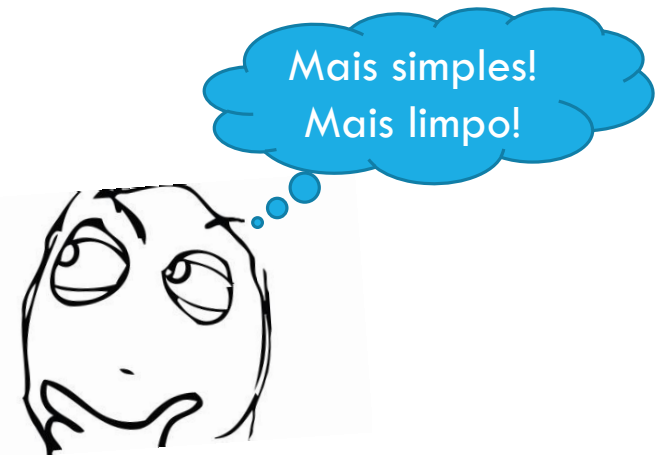
- **Variáveis**
- **Quantificadores** ( $\forall$ ,  $\exists$ )



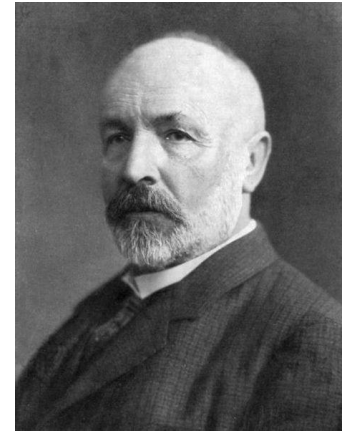
Gottlob Frege

Exemplo: “ $p(x) : x$  é par”

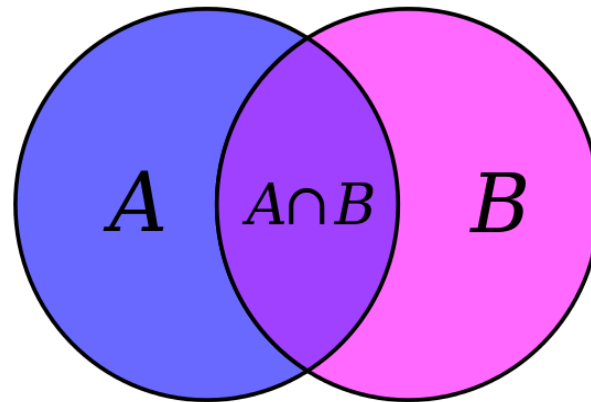
- $p(2)$  é VERDADEIRO
- $p(3)$  é FALSO
- “ $p(x), \forall x = 2k$ ” é VERDADEIRO



# TEORIA DOS CONJUNTOS ( $\approx 1870$ )



Georg Cantor



Estuda “coleções de objetos”:

- Objetos: qualquer coisa

objetos = V, F

- Intersecção:  $A \cap B$

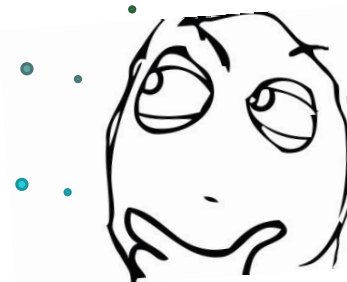
$a \in b$

- União:  $A \cup B$

$a \text{ ou } b$

- Complemento:  $\bar{A}$

$\text{não } a$



# JUNTANDO LÓGICA E CONJUNTOS:



Vamos ver um exemplo...



# PARADOXO DE RUSSELL ( $\approx 1901$ )

Livros autorreferentes: que contém referências a si mesmos

Christos Papadimitriou explica:



Um pouco mais formal:

*“o conjunto de todos os conjuntos que não se contêm a si próprios como membros”*

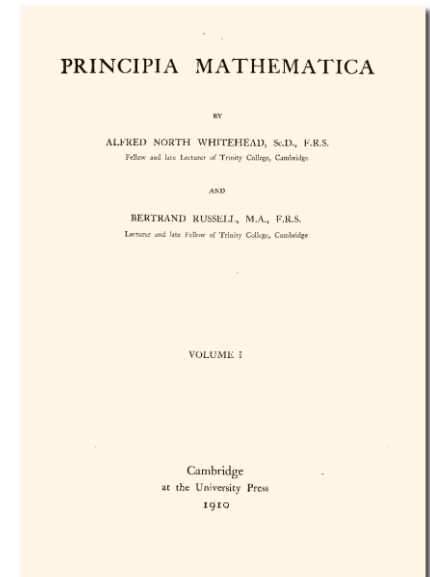
Em “matematiquês”:

$$\{A \mid A \notin A\}$$

# PRINCIPIA MATHEMATICA ( $\approx 1912$ )

Após 10 anos: “Principia Mathematica”:

- Reescreveu toda a base da matemática
- Objetivo: **provar matematicamente qualquer coisa**
- Complicado, mas bem fundamentado



Na pág. 379, a prova que  $1+1=2$ , vejamos:

\*54.43.  $\vdash :: \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

*Dem.*

$\vdash . *54.26 . \supset \vdash :: \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

[\*51.231]  $\equiv . \iota'x \cap \iota'y = \Lambda .$

[\*13.12]  $\equiv . \alpha \cap \beta = \Lambda \quad (1)$

$\vdash . (1) . *11.11.35 . \supset$

$\vdash :: (\exists x, y) . \alpha = \iota'x . \beta = \iota'y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \quad (2)$

$\vdash . (2) . *11.54 . *52.1 . \supset \vdash . \text{Prop}$

From this proposition it will follow, when arithmetical addition has been defined, that  $1 + 1 = 2$ .

# NOVAS INDAGAÇÕES... (DÉCADA DE 1920)

Apesar do sucesso, *Principia Mathematica* levantou questões...

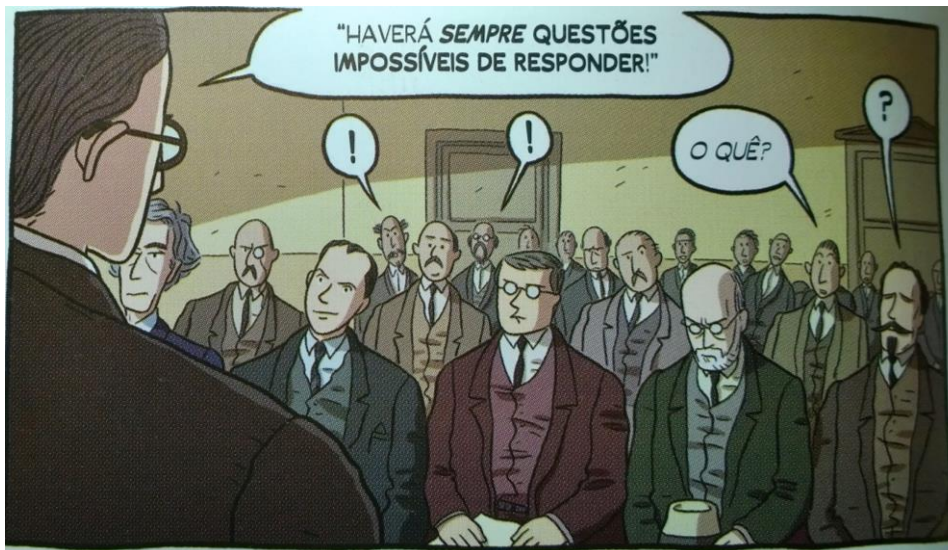
Existe um sistema lógico-formal que seja:

1. **Consistente?** (não leva a contradições)
2. **Completo?** (não permite verdades indemonstráveis)
3. **Decidível?** (existe passo-a-passo para decidir se uma verdade se segue dos axiomas ou não)

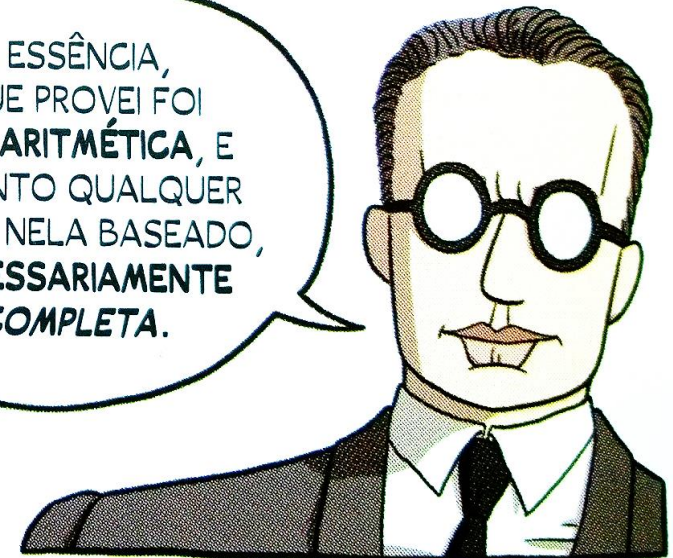


# INCOMPLETUDE ( $\approx 1931$ )

Em 1931, aos 25 anos de idade, Kurt Gödel abalou o mundo da matemática



EM ESSÊNCIA,  
O QUE PROVEI FOI  
QUE A **ARITMÉTICA**, E  
PORTANTO QUALQUER  
SISTEMA NELA BASEADO,  
É **NECESSARIAMENTE**  
**INCOMPLETA**.





Pulitzer Prize-Winner  
20th-anniversary Edition With a new preface by the author



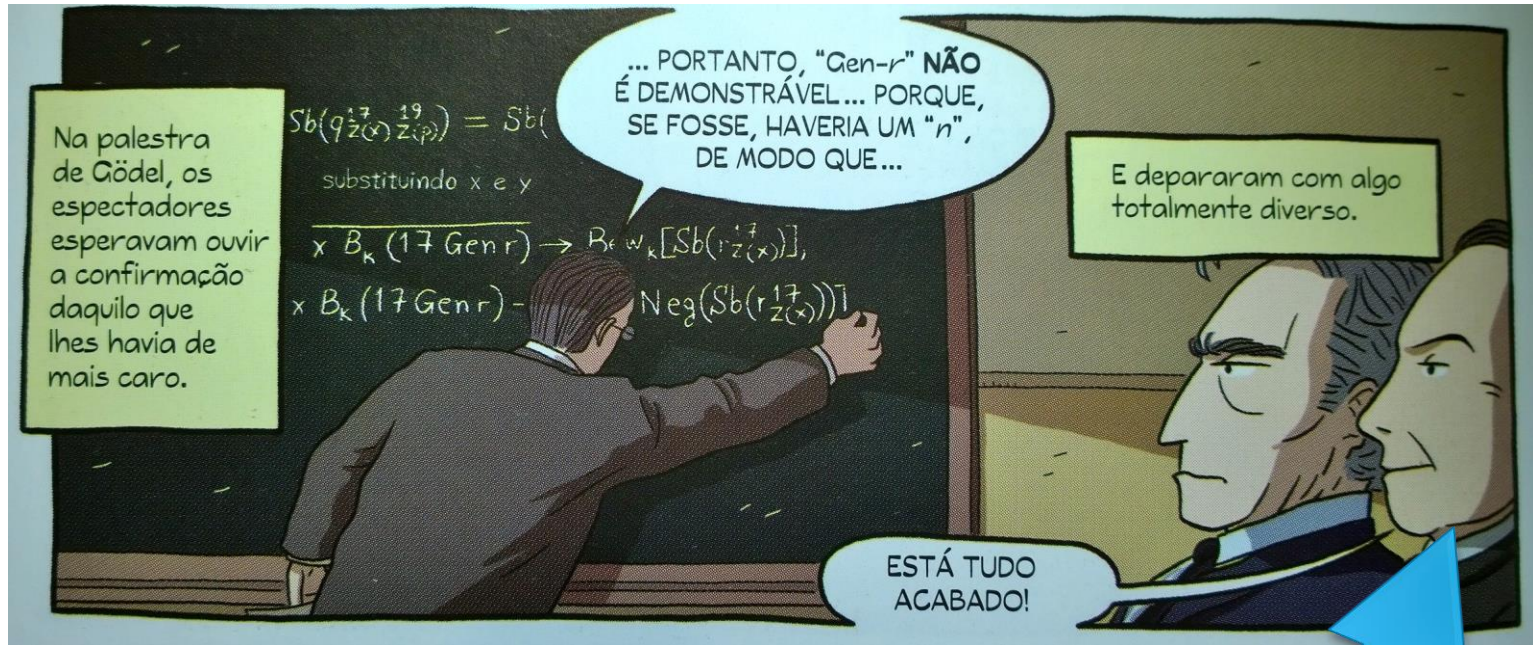
# GÖDEL, ESCHER, BACH:

||||| *an Eternal Golden Braid* |||||

DOUGLAS R. HOFSTADTER

*A metaphorical fugue on minds and machines in the spirit of Lewis Carroll*

# INCOMPLETUDE ( $\approx 1931$ )



A frase clássica de Von Neumann "*Está tudo acabado*" resume a essência da demonstração de Gödel:

- **O Teorema da Incompletude significava o fim de um sonho de 2500 anos**

Esse é John Von Neumann

# INDECIDIBILIDADE ( $\approx 1936$ )

A **decidibilidade** também teve uma resposta decepcionante...

Lembrando...

A Lógica é Decidível?

Ou seja, existe um **passo-a-passo** para decidir se uma verdade **se segue** de axiomas ou não?

Em 1936, foi provado que a lógica era **indecidível!**

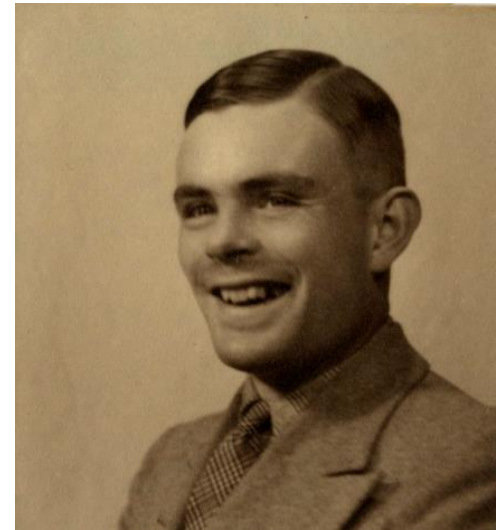


# INDECIDIBILIDADE ( $\approx 1936$ )

## O que Turing fez?

Formalizou matematicamente:

- “passo-a-passo”: **algoritmo**
- “verdade seguir-se de axiomas”: **computação**



Alan Turing

## Como Turing fez?

- Definiu um modelo matemático que executava **algoritmos** e realizava **computação**
- Provou que o **Problema da Parada** era *indecidível*
- O modelo ficou conhecido como **Máquina de Turing**



# LIMITES LÓGICOS: PROBLEMA DA PARADA

Dois algoritmos:







e



Diz se um algoritmo  
**pára** ou **executa**  
**eternamente**



1. Ei  ! Eu páro?
2. Se  diz que eu **PARO** então  
 Execute para  
sempre
3. Senão,  
 Pára a  
execução



faz o **oposto** do que



tinha dito que fazia

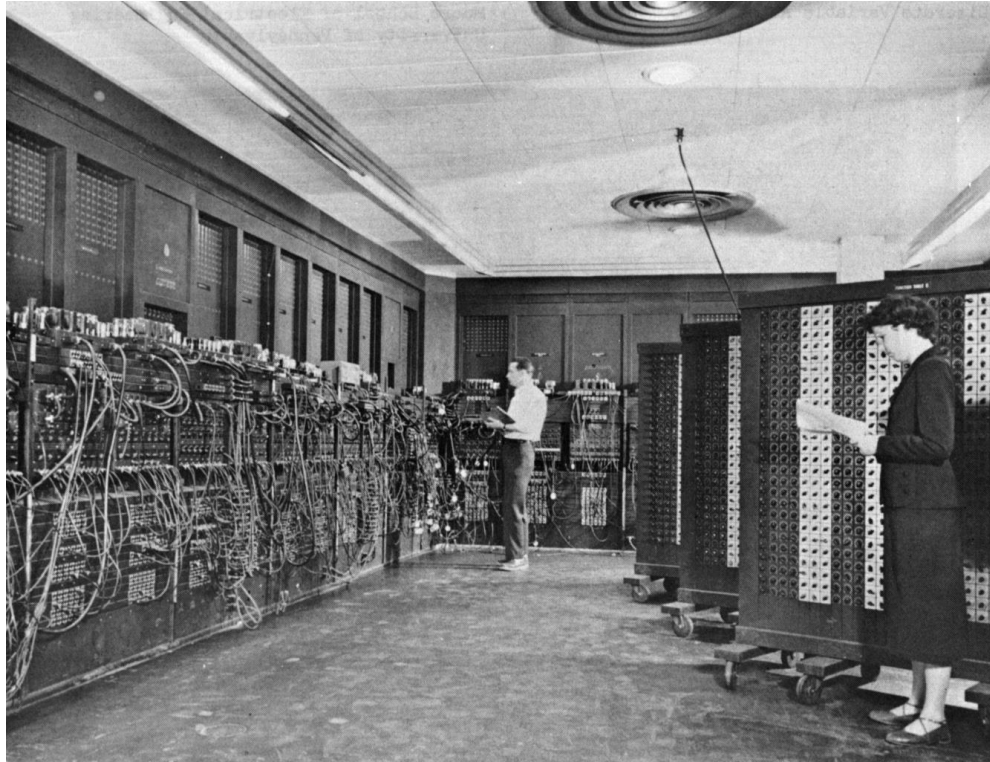
Uma contradição!

Logo,  **não pode existir!**

É uma **limitação** da computação!

# MÁQUINA DE TURING E COMPUTADORES

Legal seria a máquina **abstrata** se tornar **concreta**...



**ENIAC (1946):** 1º dispositivo físico a simular completamente a Máquina de Turing

Computadores não podem fazer tudo!

Mas **o que** eles podem fazer? E **como**?

# TRÊS DÉCADAS DE ALGORITMOS

## **1940s:**

- (1942) Transformada Rápida de Fourier
- (1945) Merge Sort
- (1947) Algoritmo Simplex

## **1950s:**

- (1952) Codificação de Huffman
- (1956) Algoritmo de Kruskal
- (1957) Algoritmo de Prim
- (1959) Algoritmo de Dijkstra

## **1960s:**

- (1962) Árvores AVL
- (1962) Quicksort
- (1962) Ford-Fulkerson
- (1964) Heapsort

# ORDENAÇÃO

Algoritmo “força-bruta”:  $n!$

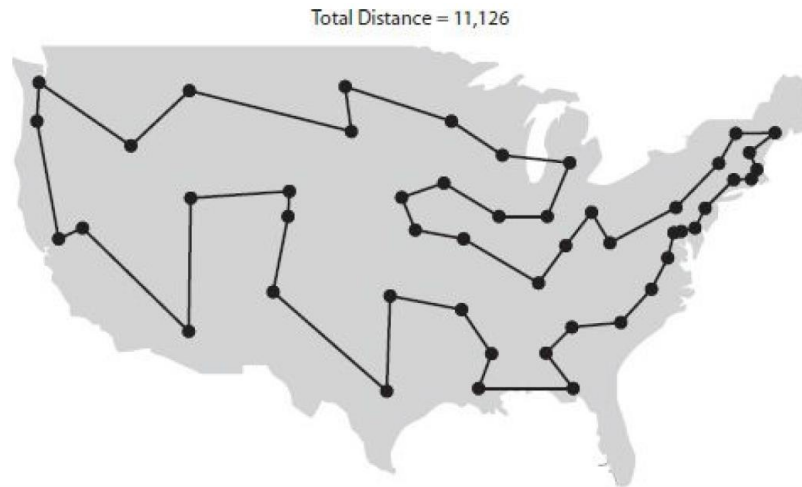
Algoritmo “esperto”:  $n \log_2 n$

$n$	$n!$	$n \log_2 n$
10	3.6 milhões	320
100	$\approx 10^{157}$	650
1000		10000
1 milhão		20 milhões



# CAIXEIRO VIAJANTE

Maria: vendedora nos 48 estados dos EUA. Fazia essa rota: (total=11126 Km)



Depto de Viagens: “Maria, pode fazer melhor?”

Programou para testar as soluções e pegar a melhor:

- 1 semana depois o programa **não havia parado...**
- **48! possibilidades**

48! é igual a

12.413.915.592.536.072.670.862.289.047.373.375.038.521.486.354.677.760.000.000.000

# MORAL DA HISTÓRIA

Alguns problemas são:

- “**fáceis**”: ordenação, ...



**Têm solução esperta**

- “**difíceis**”: caixeiro viajante, ...

Pergunta “**P = NP ?**”:

**informalmente** é sobre “Problemas Fáceis  
versus Difíceis”



# COMPLEXIDADE COMPUTACIONAL — NO OESTE

Objetivo: complexidade dos algoritmos e dificuldade de problemas



**1ª Tentativa:** pensamento e comunicação humana

**1943** — modelo de redes neurais

**1950s**

- **Stephen Kleene** - *autômato finito*: versão limitada da máquina de Turing
- **Noam Chomsky** — *gramáticas livre de contexto*: como humanos geram frases



# COMPLEXIDADE COMPUTACIONAL — 1960

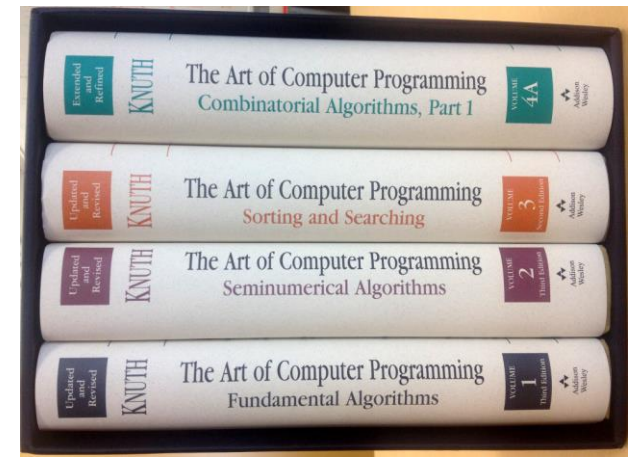
## Pesquisa de Hartmanis e Stearns

- Ideia: uso de **tempo** e **memória** por algoritmos
- “*On the Computational Complexity of Algorithms*”: nascimento da complexidade moderna



## Pesquisa de Donald Knuth

- Matemática rigorosa para analisar algoritmos
- “*The Art of Computer Programming* Vol 1, 2, 3, ...”

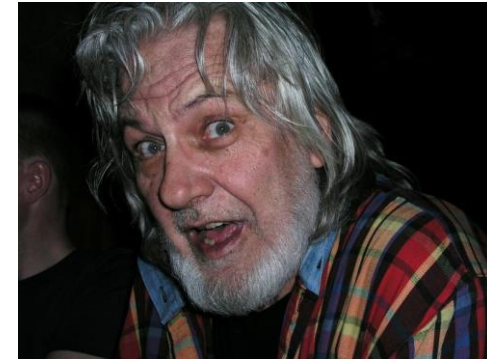




# TRATABILIDADE E EFICIÊNCIA – 1960

## “*Paths, Trees and Flowers*” - Jack Edmonds

- 1º algoritmo eficiente para emparelhamento
- Discussão sobre tempo **polinomial** X **exponencial**



“The Dude”

## “*Intrinsic Comp. Difficulty of Functions*” – Alan Cobham

- **Tese de Cobham:** algoritmo eficiente é de tempo polinomial

**Surgimento de “ $P = NP$  ?”**

# ENQUANTO ISSO, NO LESTE...

**Guerra Fria:** outra história independente...



- **“Perebor” (Перебор)**: busca através da força bruta
- **“cibernética teórica”**: termo para complexidade computacional
- **Andrey Kolmogorov**: complexidade via informação algorítmica
- **Leonid Levin**: orientado de Kolmogorov, desenvolveu pesquisa no problema **“P versus NP”**

# CARTA DE GÖDEL PARA VON NEUMANN



1956: carta de Gödel para Von Neumann sobre “ $P = NP$  ?”

- Carta descoberta em **1988!**
- Von Neumann morreu em 1957
- Talvez **nunca foi lida** por Von Neumann
- Gödel não sabia ser um problema importante

# TEORIA NATURAL OU ARTIFICIAL?

Uma **ideia científica** vem da **natureza**,  
ou da **criatividade humana**?

- Como aliens se comunicariam com nós?
- Se aliens no mesmo nível intelectual dos humanos desenvolveram, então é algo natural!
- Problema “**P = NP?**”- três fontes independentes: **EUA, USSR, Carta Godel-Von Neumann**