De uma prisão ateniense a um duelo parisiense

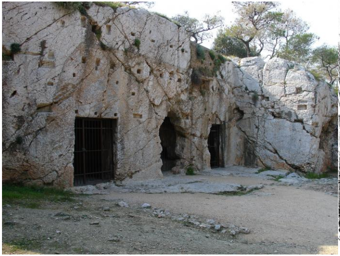
Presentation · October 2017

Ermelindo Paulo Breviglieri Schultz
Universidade Federal do Paraná

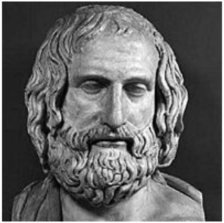
De uma prisão ateniense a um duelo parisiense

Semana **ABER**ta de Informática

2017



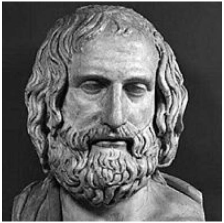
Anaxágoras de Clazomene



510 aC — 428 aC
Filósofo

Anaxágoras de Clazomene

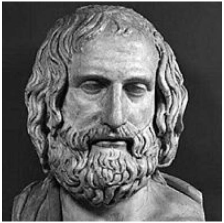
- subversivo



510 aC — 428 aC
Filósofo

Anaxágoras de Clazomene

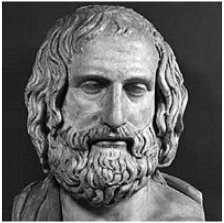
- subversivo: ímpio



510 aC — 428 aC
Filósofo

Anaxágoras de Clazomene

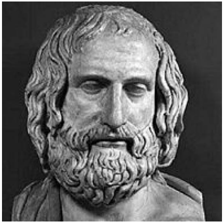
- subversivo: ímpio: "Sol e a lua não são deuses"



510 aC — 428 aC
Filósofo

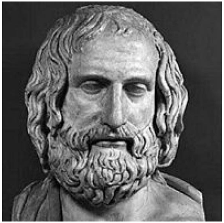
Anaxágoras de Clazomene

- subversivo: ímpio: "Sol e a lua não são deuses"
- preso em Atenas ($\approx$ 450 aC)



510 aC — 428 aC
Filósofo

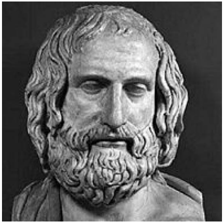
Anaxágoras de Clazomene



510 aC — 428 aC
Filósofo

- subversivo: ímpio: "Sol e a lua não são deuses"
- preso em Atenas ($\approx$ 450 aC)
- solto por Péricles e enviado para Lâmpsaco.

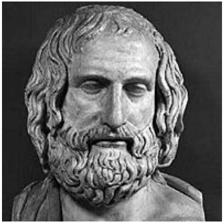
Anaxágoras de Clazomene



510 aC — 428 aC
Filósofo

- subversivo: ímpio: "Sol e a lua não são deuses"
- preso em Atenas ($\approx$ 450 aC)
- solto por Péricles e enviado para Lâmpsaco.

Anaxágoras de Clazomene



510 aC — 428 aC
Filósofo

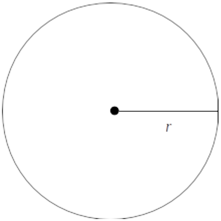
- subversivo: ímpio: "Sol e a lua não são deuses"
- preso em Atenas ($\approx$ 450 aC)
- solto por Péricles e enviado para Lâmpsaco.

- problema da *Quadratura do Círculo*

Quadratura do Círculo

Quadratura do Círculo

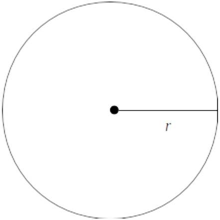
dado
um círculo



Quadratura do Círculo

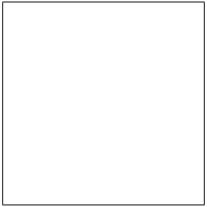
dado

um círculo



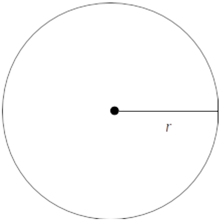
obtenha

um quadrado com a mesma área



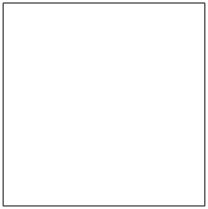
Quadratura do Círculo

dado
um círculo



área $= \pi r^2$

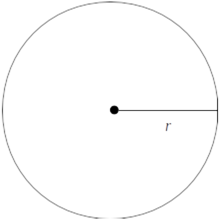
obtenha
um quadrado com a mesma área



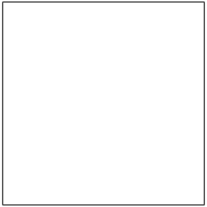
Quadratura do Círculo

dado
um círculo

obtenha
um quadrado com a mesma área



área $= \pi r^2$

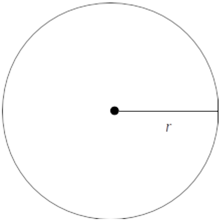


lado $= r\sqrt{\pi}$

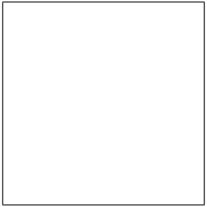
Quadratura do Círculo

dado
um círculo

obtenha
um quadrado com a mesma área



área $= \pi r^2$



lado $= r\sqrt{\pi}$

utilizando apenas régua e compasso

Construções com Régua e Compasso

Construções com Régua e Compasso

duas operações disponíveis:

Construções com Régua e Compasso

duas operações disponíveis:

1. traçar segmento de reta passando por dois pontos dados

Construções com Régua e Compasso

duas operações disponíveis:

1. traçar segmento de reta passando por dois pontos dados

Construções com Régua e Compasso

duas operações disponíveis:

1. traçar segmento de reta passando por dois pontos dados

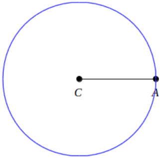
2. traçar (arco de) circunferência com centro e raio dados

Construções com Régua e Compasso

duas operações disponíveis:

1. traçar segmento de reta passando por dois pontos dados

2. traçar (arco de) circunferência com centro e raio dados



Exemplo

dados uma reta r e um ponto P

Exemplo

dados uma reta r e um ponto P

Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P

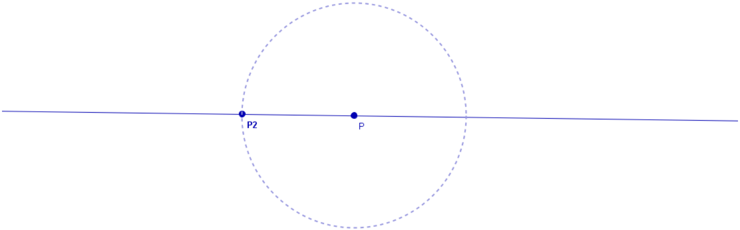
Exemplo

dados uma reta r e um ponto P

obtenha uma reta perpendicular a r que passa por P

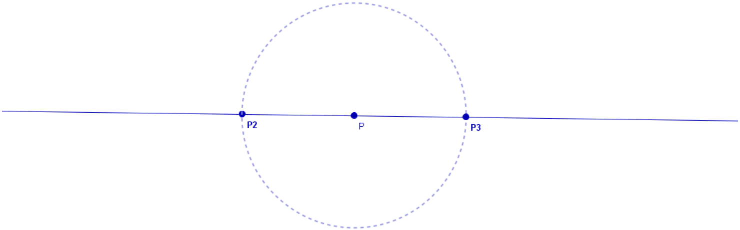
Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



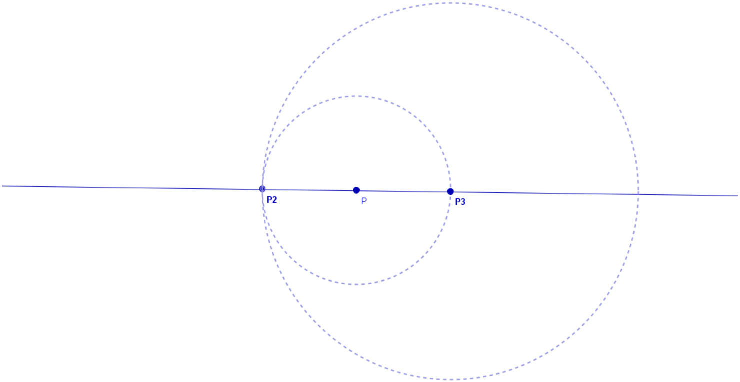
Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



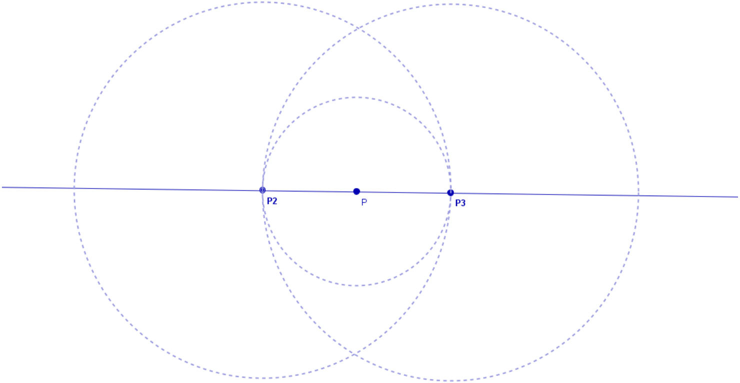
Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



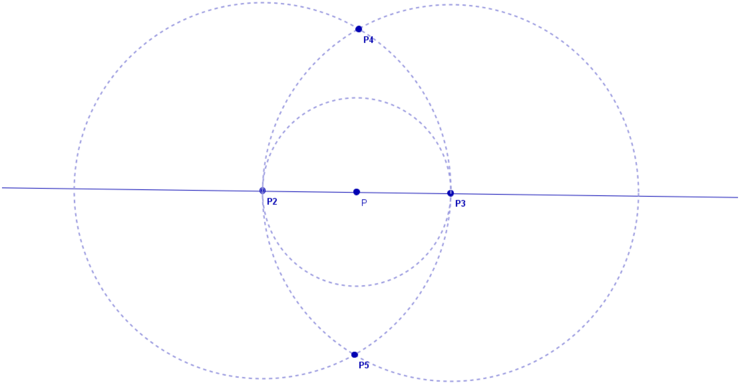
Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



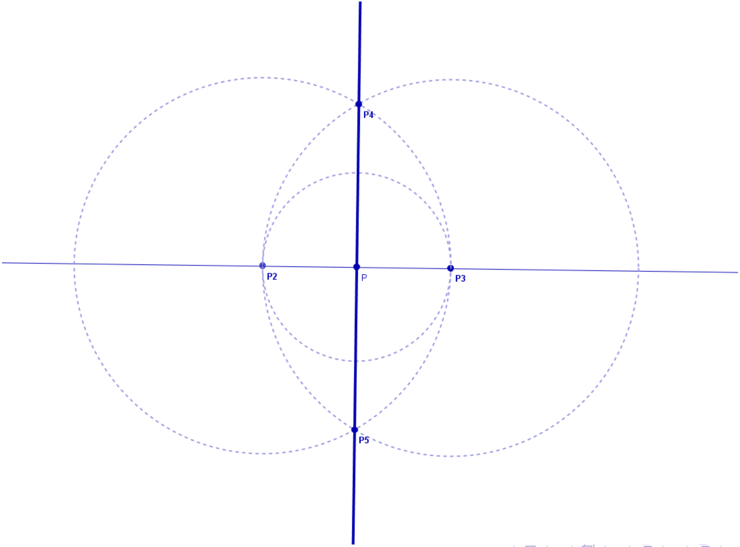
Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



Exemplo

dados uma reta r e um ponto P
obtenha uma reta perpendicular a r que passa por P



Computação

dado ...

obtenha ...

usando somente ...

Computação

dado . . . ← entrada

obtenha . . .

usando somente . . .

Computação

dado $\ldots \leftarrow$ entrada

obtenha $\ldots \leftarrow$ saída

usando somente . . .

Computação

dado ... ← entrada

obtenha ... ← saída

usando somente ... ← operações disponíveis

Computação

dado . . . ← entrada

← problema computacional

obtenha . . . ← saída

usando somente . . . ← operações disponíveis

Computação

dado ... $\leftarrow$ entrada

$\leftarrow$ problema computacional

obtenha ... $\leftarrow$ saída

usando somente ... $\leftarrow$ modelo de computação

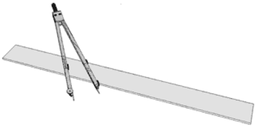
Computação

dado . . . ← entrada

← problema computacional

obtenha . . . ← saída

usando somente . . . ← modelo de computação



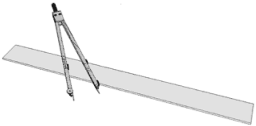
Computação

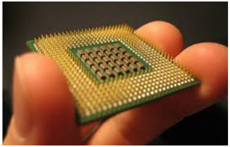
dado ... $\leftarrow$ entrada

$\leftarrow$ problema computacional

obtenha ... $\leftarrow$ saída

usando somente ... $\leftarrow$ modelo de computação





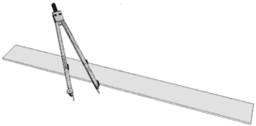
Computação

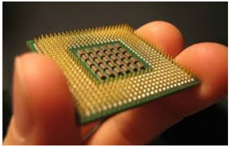
dado . . . ← entrada

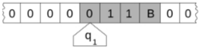
← problema computacional

obtenha . . . ← saída

usando somente . . . ← modelo de computação







Outros Problemas em Aberto

Outros Problemas em Aberto

Duplicação do Cubo

Outros Problemas em Aberto

Duplicação do Cubo

dado um cubo,

Outros Problemas em Aberto

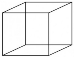
Duplicação do Cubo

dado um cubo,
obtenha outro cubo com o dobro de seu volume

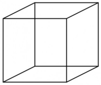
Outros Problemas em Aberto

Duplicação do Cubo

dado um cubo,
obtenha outro cubo com o dobro de seu volume



lado $= \ell$

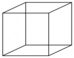


lado $= \ell\sqrt[3]{2}$

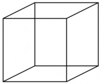
Outros Problemas em Aberto

Duplicação do Cubo

dado um cubo,
obtenha outro cubo com o dobro de seu volume



lado $= \ell$



lado $= \ell\sqrt[3]{2}$

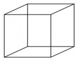
Trissecção do ângulo

Outros Problemas em Aberto

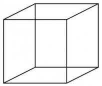
Duplicação do Cubo

dado um cubo,

obtenha outro cubo com o dobro de seu volume



lado $= \ell$



lado $= \ell\sqrt[3]{2}$

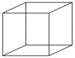
Trissecção do ângulo

dadas duas retas não paralelas formando o ângulo α

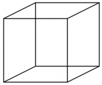
Outros Problemas em Aberto

Duplicação do Cubo

dado um cubo,
obtenha outro cubo com o dobro de seu volume



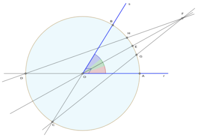
lado $= \ell$



lado $= \ell\sqrt[3]{2}$

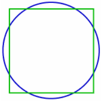
Trissecção do ângulo

dadas duas retas não paralelas formando o ângulo α
obtenha o ângulo $\frac{\alpha}{3}$

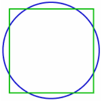


Problemas Equivalentes

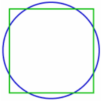
Problemas Equivalentes

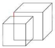


Problemas Equivalentes

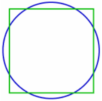
 $\equiv$ construir segmento de tamanho $\sqrt{\pi}$

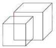
Problemas Equivalentes

 $\equiv$ construir segmento de tamanho $\sqrt{\pi}$

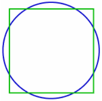


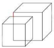
Problemas Equivalentes

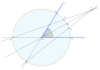
 $\equiv$ construir segmento de tamanho $\sqrt{\pi}$

 $\equiv$ construir segmento de tamanho $\sqrt[3]{2}$

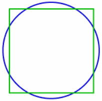
Problemas Equivalentes

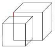
 $\equiv$ construir segmento de tamanho $\sqrt{\pi}$

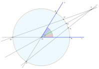
 $\equiv$ construir segmento de tamanho $\sqrt[3]{2}$



Problemas Equivalentes

 $\equiv$ construir segmento de tamanho $\sqrt{\pi}$

 $\equiv$ construir segmento de tamanho $\sqrt[3]{2}$

 $\equiv$ construir segmento de tamanho $\cos(\alpha/3)$

Números Construtíveis

número x é *construtível*

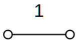
Números Construtíveis

número x é *construtível*

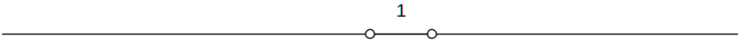
$$\equiv$$

é possível construir um segmento de comprimento x
a partir de um segmento de comprimento 1

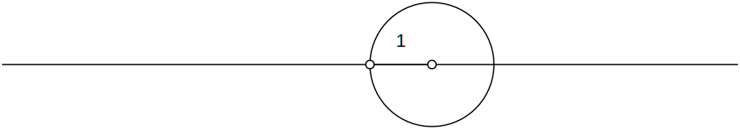
Inteiros são construtíveis



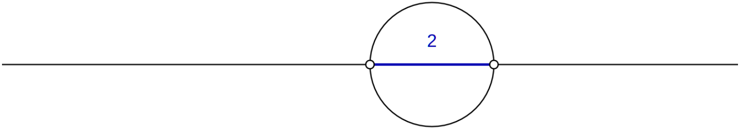
Inteiros são construtíveis



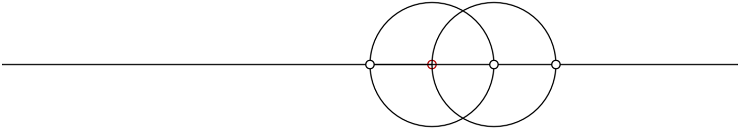
Inteiros são construtíveis



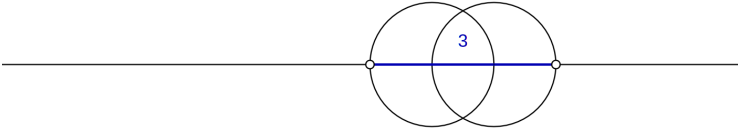
Inteiros são construtíveis



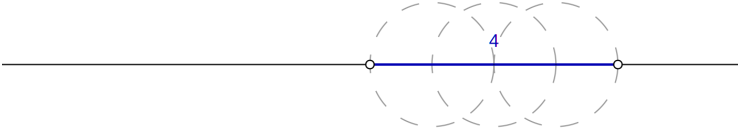
Inteiros são construtíveis



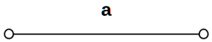
Inteiros são construtíveis



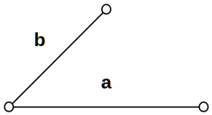
Inteiros são construtíveis



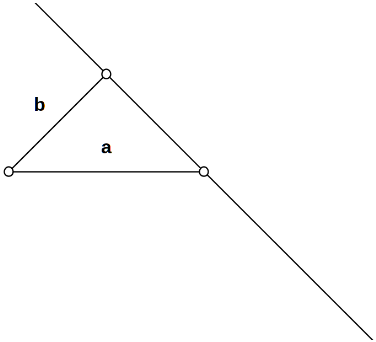
Racionais são construtíveis



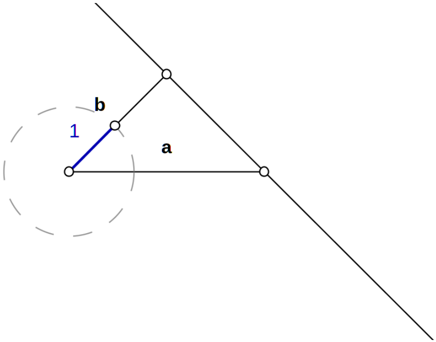
Racionais são construtíveis



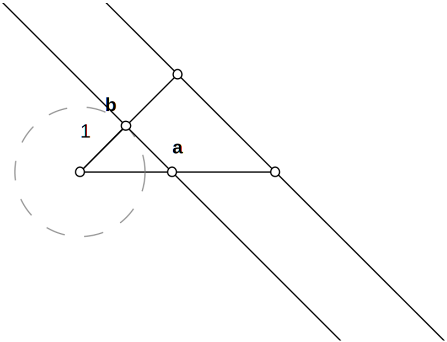
Racionais são construtíveis



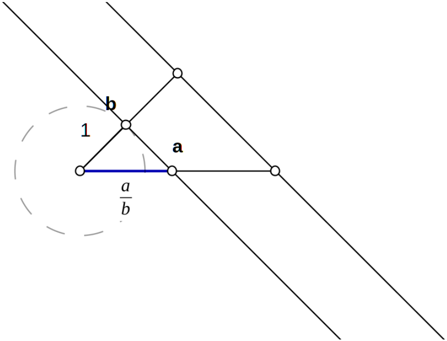
Racionais são construtíveis



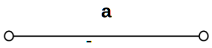
Racionais são construtíveis



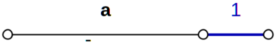
Racionais são construtíveis



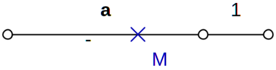
Raízes quadradas de números construtíveis são construtíveis



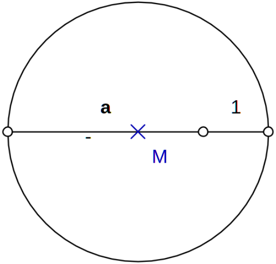
Raízes quadradas de números construtíveis são construtíveis



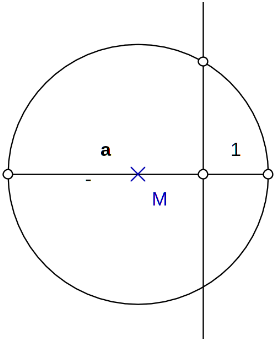
Raízes quadradas de números construtíveis são construtíveis



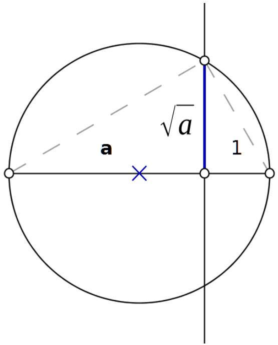
Raízes quadradas de números construtíveis são construtíveis



Raízes quadradas de números construtíveis são construtíveis



Raízes quadradas de números construtíveis são construtíveis



Figuras Geométricas $\times$ Números

Figuras Geométricas $\times$ Números

quadratura do círculo de raio r

Figuras Geométricas $\times$ Números

quadratura do círculo de raio $r \preceq$ construção de $r\sqrt{\pi}$

Figuras Geométricas $\times$ Números

quadratura do círculo de raio $r \preceq$ construção de $r\sqrt{\pi}$

duplicação do cubo de lado ℓ

Figuras Geométricas $\times$ Números

quadratura do círculo de raio $r \preceq$ construção de $r\sqrt{\pi}$

duplicação do cubo de lado $\ell \preceq$ construção de $\ell\sqrt[3]{2}$

Figuras Geométricas $\times$ Números

quadratura do círculo de raio $r \preceq$ construção de $r\sqrt{\pi}$

duplicação do cubo de lado $\ell \preceq$ construção de $\ell\sqrt[3]{2}$

trissecção do ângulo α

Figuras Geométricas $\times$ Números

quadratura do círculo de raio $r \preceq$ construção de $r\sqrt{\pi}$

duplicação do cubo de lado $\ell \preceq$ construção de $\ell\sqrt[3]{2}$

trissecção do ângulo $\alpha \preceq$ construção de $\cos(\alpha/3)$

Todo Número é Construtível?

Todo Número é Construtível?

ou será que existem números não construtíveis?

Todo Número é Construtível?

ou será que existem números não construtíveis?

o modelo de computação da régua e compasso é capaz de computar qualquer número?

Todo Número é Construtível?

ou será que existem números não construtíveis?

o modelo de computação da régua e compasso é capaz de computar qualquer número?

ou existem números que não são computáveis nesse modelo?

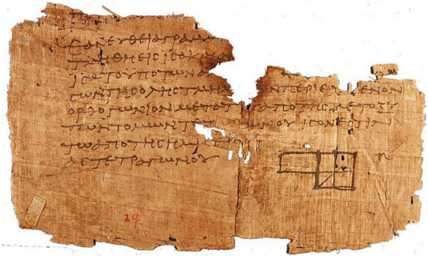
Euclides de Alexandria

$\approx$ 300 aC

Euclides de Alexandria

≈ 300 aC

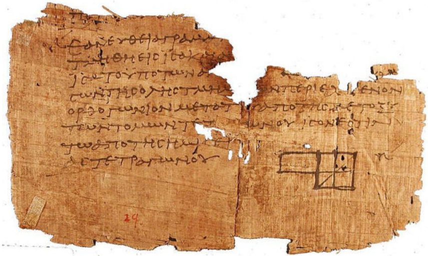
Elementos



Euclides de Alexandria

$\approx$ 300 aC

Elementos

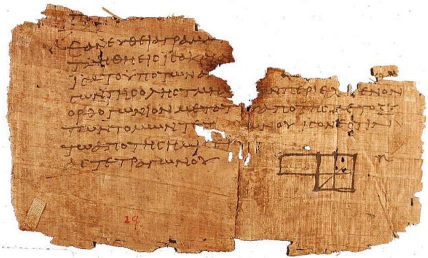


um dos livros mais influentes da história

Euclides de Alexandria

≈ 300 aC

Elementos



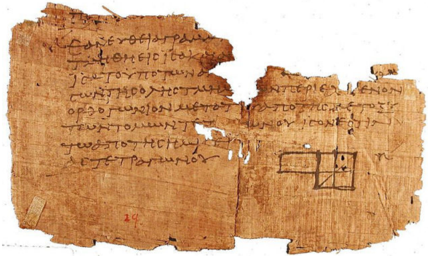
um dos livros mais influentes da história

modelo de rigor lógico

Euclides de Alexandria

≈ 300 aC

Elementos



um dos livros mais influentes da história

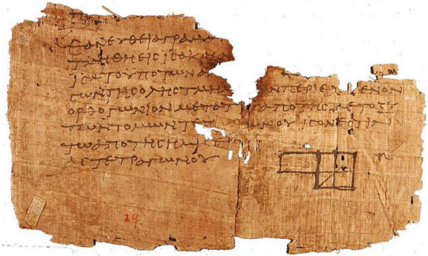
modelo de rigor lógico

axiomatização da geometria

Euclides de Alexandria

$\approx$ 300 aC

Elementos



um dos livros mais influentes da história

modelo de rigor lógico

axiomatização da geometria

provas: construções com régua e compasso

De repente ...

De repente ...

... passaram dois mil e duzentos anos ...

Évariste Galois
1811 — 1832

De repente . . .

. . . passaram dois mil e duzentos anos . . .

Évariste Galois
1811 — 1832

subversivo

De repente . . .

. . . passaram dois mil e duzentos anos . . .

Évariste Galois
1811 — 1832

subversivo: ativista republicano

De repente . . .

. . . passaram dois mil e duzentos anos . . .

Évariste Galois
1811 — 1832

subversivo: ativista republicano

expulso da faculdade

De repente . . .

. . . passaram dois mil e duzentos anos . . .

Évariste Galois
1811 — 1832

subversivo: ativista republicano

expulso da faculdade

preso várias vezes

De repente . . .

. . . passaram dois mil e duzentos anos . . .

Évariste Galois
1811 — 1832

subversivo: ativista republicano

expulso da faculdade

preso várias vezes

morto em um duelo

Solução de equações por radicais

Solução de equações por radicais

resolver uma equação usando somente

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{}$

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{}$

dada

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{\ }$

dada uma equação com incógnita x

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{\ }$

dada uma equação com incógnita x

obtenha

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{}$

dada uma equação com incógnita x

obtenha um valor de x que a satisfaça

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{\ }$

dada uma equação com incógnita x

obtenha um valor de x que a satisfaça

usando somente

Solução de equações por radicais

resolver uma equação usando somente

- as quatro operações aritméticas: $+$, $-$, $\times$, $/$
- radiciação: $\sqrt{}$

dada uma equação com incógnita x

obtenha um valor de x que a satisfaça

usando somente $+$, $-$, $\times$, $/$ e $\sqrt{}$

Outro problema computacional milenar

Outro problema computacional milenar

grau 2

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara?

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824)

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824): solução geral

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824): solução geral = algoritmo

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824): solução geral = algoritmo
- Galois (1832)

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824): solução geral = algoritmo
- Galois (1832)
  - existem equações insolúveis

Outro problema computacional milenar

grau 2: $ax^2 + bx = c$: séc. XX aC (Babilônia)

- Bhāskara: 1114 — 1185 (Índia)

graus 3 e 4: $ax^4 + bx^3 + cx^2 + dx = e$: sec XVI (Itália)

grau ≥ 5

- impossível: Abel — Ruffini (1824): solução geral = algoritmo
- Galois (1832)
  - existem equações insolúveis
  - caracterização das que tem solução

Extensões de Corpos . . .

Extensões de Corpos . . .

um corpo

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito)

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo)

Extensões de Corpos ...

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio: $\sqrt{-1}$

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio: $\sqrt{-1}$
- e tudo mais necessário para que seja corpo

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio: $\sqrt{-1}$
- e tudo mais necessário para que seja corpo:
  $2 + \sqrt{-1}, \quad 3\sqrt{-1}, \quad \sqrt{-1}^3, \ \ldots$

Extensões de Corpos . . .

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio: $\sqrt{-1}$
- e tudo mais necessário para que seja corpo:
  $2 + \sqrt{-1}, \quad 3\sqrt{-1}, \quad \sqrt{-1}^3, \ \ldots$

o resultado é o corpo $\mathbb{R}(\sqrt{-1})$

Extensões de Corpos ...

um corpo ($+$, $\times$, tudo que tem direito): $\mathbb{R}$

um polinômio irredutível (sem raízes no corpo): $x^2 + 1$

extensão do corpo:

- inclusão de uma raiz do polinômio: $\sqrt{-1}$
- e tudo mais necessário para que seja corpo:
  $2 + \sqrt{-1}, \quad 3\sqrt{-1}, \quad \sqrt{-1}^3, \ \ldots$

o resultado é o corpo $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

formam um grupo

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

formam um grupo

grupo **solúvel**

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

formam um grupo

grupo **solúvel** $\implies$ polinômio solúvel por radicais

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

formam um grupo

grupo **solúvel** $\implies$ polinômio solúvel por radicais

---

a explicação acima contém graves simplificações

. . . e Grupos

automorfismos sobre $\mathbb{R}(\sqrt{-1})$ que mantém $\mathbb{R}$ invariante

formam um grupo

grupo **solúvel** $\implies$ polinômio solúvel por radicais

---

a explicação acima contém graves simplificações

caso os sintomas persistam, procure um algebrista

Solução de Equações por Radicais

Solução de Equações por Radicais

todo grupo com até quatro elementos é solúvel

Solução de Equações por Radicais

todo grupo com até quatro elementos é solúvel

para todo $n > 4$ existe polinômio cujo grupo não é solúvel

Solução de Equações por Radicais

todo grupo com até quatro elementos é solúvel

para todo $n > 4$ existe polinômio cujo grupo não é solúvel

Construtibilidade de Números

Construtibilidade de Números

$$x \text{ é construtível}$$
$$\Updownarrow$$
$$\text{é possível estender } \mathbb{Q} \text{ a } \mathbb{Q}(x) \text{ passo a passo}$$

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$\mathbb{Q} \to \mathbb{Q}(x_1)$

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to,$$

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to, \ldots$$

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to, \ldots, \to (\mathbb{Q}(x_1)\ldots(x_{n-1}))\,(x)$$

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to, \ldots, \to (\mathbb{Q}(x_1)\ldots(x_{n-1}))\,(x)$$

de forma que em cada passo o polinômio irredutível tem grau 2

Construtibilidade de Números

x é construtível

$$\Updownarrow$$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to, \ldots, \to (\mathbb{Q}(x_1)\ldots(x_{n-1}))\,(x)$$

de forma que em cada passo o polinômio irredutível tem grau 2

$$\Downarrow$$

o grau do polinômio irredutível de x é potência de 2

Construtibilidade de Números

x é construtível

$\Updownarrow$

é possível estender $\mathbb{Q}$ a $\mathbb{Q}(x)$ passo a passo

$$\mathbb{Q} \to \mathbb{Q}(x_1) \to (\mathbb{Q}(x_1))(x_2) \to, \ldots, \to (\mathbb{Q}(x_1)\ldots(x_{n-1}))\,(x)$$

de forma que em cada passo o polinômio irredutível tem grau 2

$\Downarrow$

o grau do polinômio irredutível de x é potência de 2

A Quadratura do Círculo é Impossível

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

porque π não é raiz de nenhum polinômio em $\mathbb{Q}$

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

porque π não é raiz de nenhum polinômio em $\mathbb{Q}$
π é transcendente

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

porque π não é raiz de nenhum polinômio em $\mathbb{Q}$
π é transcendente (Lindemann, 1882)

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

porque π não é raiz de nenhum polinômio em $\mathbb{Q}$
π é transcendente (Lindemann, 1882)

$\sqrt{\pi}$ também tem que ser transcendente

A Quadratura do Círculo é Impossível

$r\sqrt{\pi}$ não é construtível

porque $\sqrt{\pi}$ não é construtível

porque π não é raiz de nenhum polinômio em $\mathbb{Q}$
π é transcendente (Lindemann, 1882)

$\sqrt{\pi}$ também tem que ser transcendente

A Duplicação do Cubo é Impossível

A Duplicação do Cubo é Impossível

$\ell\sqrt[3]{2}$ não é construtível

A Duplicação do Cubo é Impossível

$\ell\sqrt[3]{2}$ não é construtível

porque $\sqrt[3]{2}$ não é construtível

A Duplicação do Cubo é Impossível

$\ell\sqrt[3]{2}$ não é construtível

porque $\sqrt[3]{2}$ não é construtível

porque o polinômio irredutível do qual $\sqrt[3]{2}$ é raiz é $x^3 - 2$

A Duplicação do Cubo é Impossível

$\ell\sqrt[3]{2}$ não é construtível

porque $\sqrt[3]{2}$ não é construtível

porque o polinômio irredutível do qual $\sqrt[3]{2}$ é raiz é $x^3 - 2$

e seu grau não é potência de 2

A Duplicação do Cubo é Impossível

$\ell\sqrt[3]{2}$ não é construtível

porque $\sqrt[3]{2}$ não é construtível

porque o polinômio irredutível do qual $\sqrt[3]{2}$ é raiz é $x^3 - 2$

e seu grau não é potência de 2

A Trissecção de $\alpha = \pi/3$ é Impossível

A Trissecção de $\alpha = \pi/3$ é Impossível

$\cos(\alpha/3) = \cos(\pi/9)$ não é construtível

A Trissecção de $\alpha = \pi/3$ é Impossível

$\cos(\alpha/3) = \cos(\pi/9)$ não é construtível

o polinômio irredutível do qual $\cos(\pi/9)$ é raiz tem grau 3

A Trissecção de $\alpha = \pi/3$ é Impossível

$\cos(\alpha/3) = \cos(\pi/9)$ não é construtível

o polinômio irredutível do qual $\cos(\pi/9)$ é raiz tem grau 3

que não é potência de 2

A Trissecção de $\alpha = \pi/3$ é Impossível

$\cos(\alpha/3) = \cos(\pi/9)$ não é construtível

o polinômio irredutível do qual $\cos(\pi/9)$ é raiz tem grau 3

que não é potência de 2

Resumo

Resumo

dois exemplos de modelos de computação

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso
- cálculos com operações aritméticas e radicais

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso
- cálculos com operações aritméticas e radicais

problemas computacionais para cuja solução o esforço de pesquisa atravessou mais de dois mil anos

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso
- cálculos com operações aritméticas e radicais

problemas computacionais para cuja solução o esforço de pesquisa atravessou mais de dois mil anos

- quadratura do círculo, duplicação do cubo etc

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso
- cálculos com operações aritméticas e radicais

problemas computacionais para cuja solução o esforço de pesquisa atravessou mais de dois mil anos

- quadratura do círculo, duplicação do cubo etc
- construtibilidade de números

Resumo

dois exemplos de modelos de computação

- construções com régua e compasso
- cálculos com operações aritméticas e radicais

problemas computacionais para cuja solução o esforço de pesquisa atravessou mais de dois mil anos

- quadratura do círculo, duplicação do cubo etc
- construtibilidade de números
- solução de equações por radicais

Moral da História

Moral da História

“Computação não trata de computadores (...) no mesmo sentido em que (...) biologia não trata de microscópios (...). A razão porque se confunde Computação e computador é a mesma pela qual os antigos egípcios confundiam geometria com os instrumentos de medição: quando um assunto é novo (...) é muito fácil confundir o que há de essencial nele com os instrumentos utilizados”

Hal Abelson

Moral da História

"Computação não trata de computadores (...) no mesmo sentido em que (...) biologia não trata de microscópios (...). A razão porque se confunde Computação e computador é a mesma pela qual os antigos egípcios confundiam geometria com os instrumentos de medição: quando um assunto é novo (...) é muito fácil confundir o que há de essencial nele com os instrumentos utilizados"

Hal Abelson

"A razão de ser da computação [numérica] é 'insight', não os números."

Richard Hamming