Fundamentos de Matemática para a Computação

MAC 105

Aula 2

28 de Abril, Quarta-feira, 2021

Coelho & Sinai
IME, University of São Paulo

Hoje

O plano é conversarmos hoje sobre:

Hoje

O plano é conversarmos hoje sobre:

1. Números primos
2. Prova de Euclides de que há infinitos primos, segunda tentativa
3. Vendo padrões falsos
4. Algoritmo de divisão, começar

(Revisão)

Definição. Um número inteiro p é chamado um número primo se seus únicos divisores são 1 e p.

Ques. Podemos criar/descobrir uma fórmula eficiente para gerar o n'ésimo primo, como uma função de n?

Ninguem sabe, aínda!

Definição. Um fator de n **não-trivial** é um fator q de n, t.q. $1 < q < n$.

(Revisão)

O Teorema Fundamental da Aritmética

Todos os números inteiros positivos maiores do que 1 podem ser decompostos num produto de números primos, e este decomposição e única.

Plano

Nos começaremos cada aula com um problema concreto e, no processo de resolvê-lo, desenvolveremos as idéias matemáticas, notações, e definições relevantes.

Plano

Nos começaremos cada aula com um problema concreto e, no processo de resolvê-lo, desenvolveremos as idéias matemáticas, notações, e definições relevantes.

Problema.

Plano

Nos começaremos cada aula com um problema concreto e, no processo de resolvê-lo, desenvolveremos as idéias matemáticas, notações, e definições relevantes.

Problema.

Euler (1772) descobriu que o polinômio

Plano

Nos começaremos cada aula com um problema concreto e, no processo de resolvê-lo, desenvolveremos as idéias matemáticas, notações, e definições relevantes.

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

Plano

Nos começaremos cada aula com um problema concreto e, no processo de resolvê-lo, desenvolveremos as idéias matemáticas, notações, e definições relevantes.

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ

ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

$$p(1) = 43, \text{ um primo}$$

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

$$p(1) = 43, \text{ um primo}$$
$$p(2) = 47, \text{ um primo}$$

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

$$p(1) = 43, \text{ um primo}$$
$$p(2) = 47, \text{ um primo}$$
$$p(3) = 53, \text{ um primo}$$

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

PARÉCÉ
ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

$$p(1) = 43, \text{ um primo}$$
$$p(2) = 47, \text{ um primo}$$
$$p(3) = 53, \text{ um primo}$$

Portanto, eles são todos primos!

Problema.

Euler (1772) descobriu que o polinômio

$$p(x) := x^2 + x + 41$$

ser igual a um número primo, para as primeiras 39 entradas inteiras ...

Vamos descobrir mais.

$$p(1) = 43, \text{ um primo}$$
$$p(2) = 47, \text{ um primo}$$
$$p(3) = 53, \text{ um primo}$$

Portanto, eles são todos primos! (verdadeira ?!?)

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

...

$p(39) := 1601$, um primo

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

...

$p(39) := 1601$, um primo

$p(41) = 41^2 + 41 + 41 =$

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

...

$p(39) := 1601$, um primo

$p(41) = 41^2 + 41 + 41 = \ 41(41 + 1 + 1)$

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

...

$p(39) := 1601$, um primo

$p(41) = 41^2 + 41 + 41 = 41(41 + 1 + 1)$

$= 41 * 43,$ não e primo!

Problema.

$$p(x) := x^2 + x + 41$$

$p(1) = 43$, um primo

$p(2) = 47$, um primo

$p(3) = 53$, um primo

...

$p(39) := 1601$, um primo

$p(41) = 41^2 + 41 + 41 = 41(41 + 1 + 1)$

$= 41 * 43,$ não e primo!

De fato, $p(40)$ também não e primo.

Existe outras polinômios assim?

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Podemos experimentar: $p(1) = 4567$, um primo

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Podemos experimentar: $p(1) = 4567$, um primo

$p(2) = 4243$, um primo

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Podemos experimentar: $p(1) = 4567$, um primo

$p(2) = 4243$, um primo

...

$p(57) = 4903$, um primo

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Podemos experimentar: $p(1) = 4567$, um primo

$p(2) = 4243$, um primo

...

$p(57) = 4903$, um primo

O padrão forte!

Existe outras polinômios assim?

$$\text{Seja } p(n) := 6n^2 - 342n + 4903$$

Podemos experimentar: $p(1) = 4567$, um primo

$p(2) = 4243$, um primo

...

$p(57) = 4903$, um primo

O padrão forte!

Mas, $p(58) = 5251 = 59 * 89$, então não e primo.... ;(

Para obter mais informações, você pode pesquisar ‘prime-generating polynomials’, na Wikipédia.

Para obter mais informações, você pode pesquisar 'prime-generating polynomials', na Wikipédia.

Questão. Existe um polynômio $p(x)$, com coeficientes inteiros, t.q. $p(n)$ é SEMPRE primo, para todos os valores inteiros positivos de n?

Para obter mais informações, você pode pesquisar ‘prime-generating polynomials’, na Wikipédia.

Questão. Existe um polynômio $p(x)$, com coeficientes inteiros, t.q.
$p(n)$ é SEMPRE primo, para todos os valores inteiros positivos de n?

Tarefa para casa (Homework).

Se você acha que existe, provar isso.

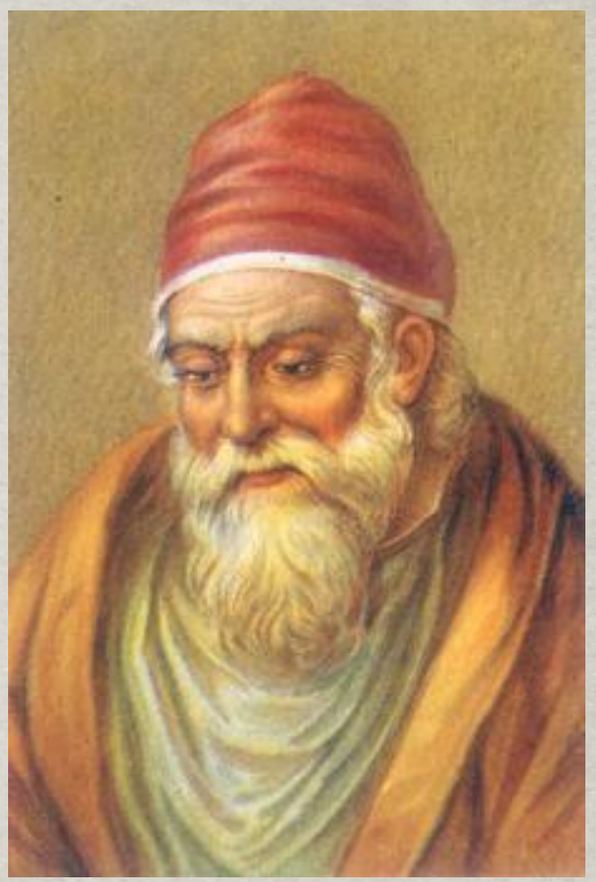
Se você acha que não existe, provar isso.

Livro maravilhoso:

Paulo Ribenboim, **The Little Book of Big Primes**,
New York, Springer-Verlag, 1991.

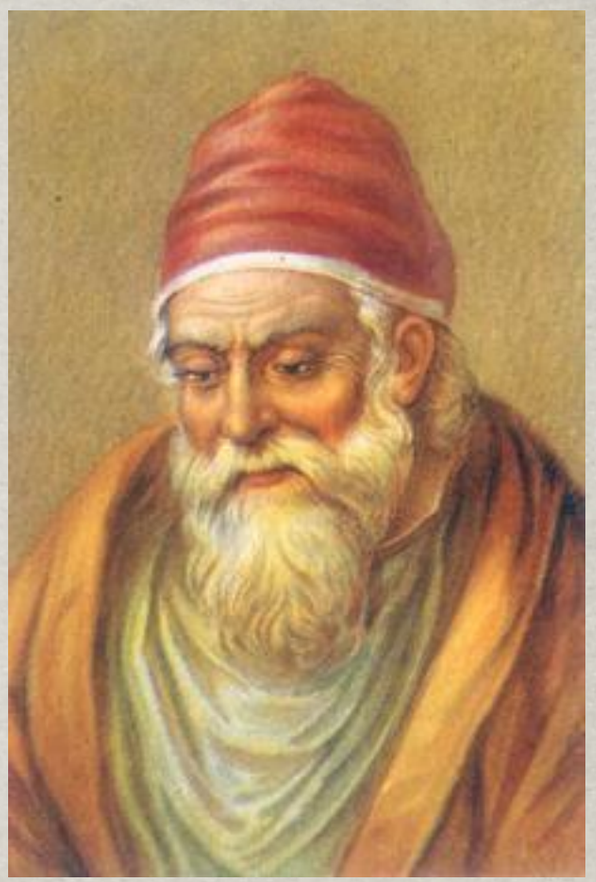
Teoréma de Euclides.

Existe infinitos números primos.



Teoréma de Euclides.

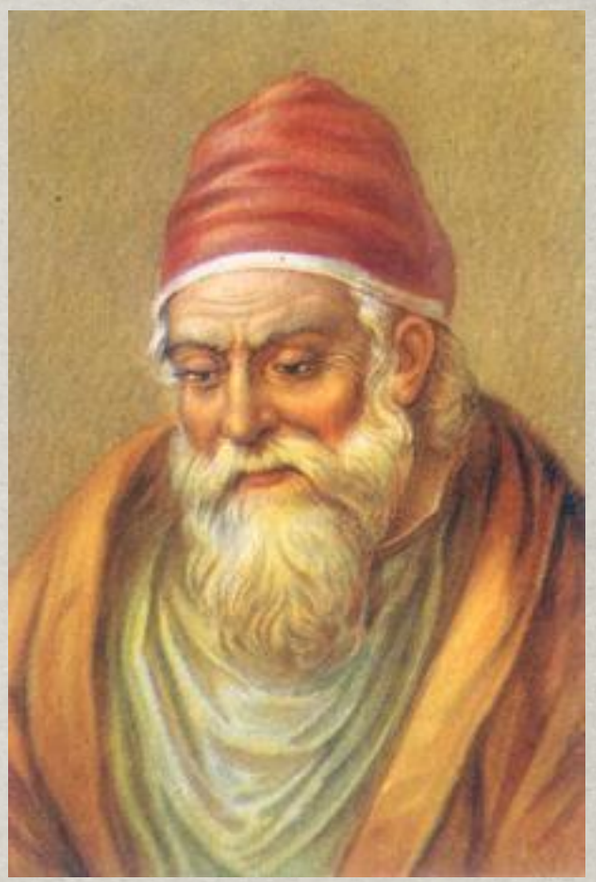
Existe infinitos números primos.



Prova. (Segunda tentativa)

Teoréma de Euclides.

Existe infinitos números primos.

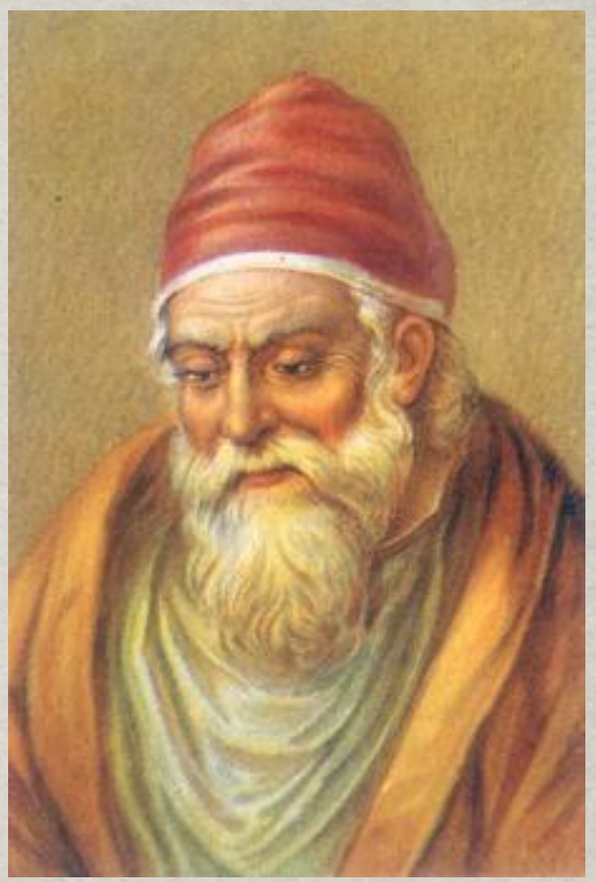


Prova. (Segunda tentativa)

Podemos começar assumindo que existem apenas finitos primos, aplicar as leis da lógica (dedução) e chegar a uma contradição.

Teoréma de Euclides.

Existe infinitos números primos.



Prova. (Segunda tentativa)

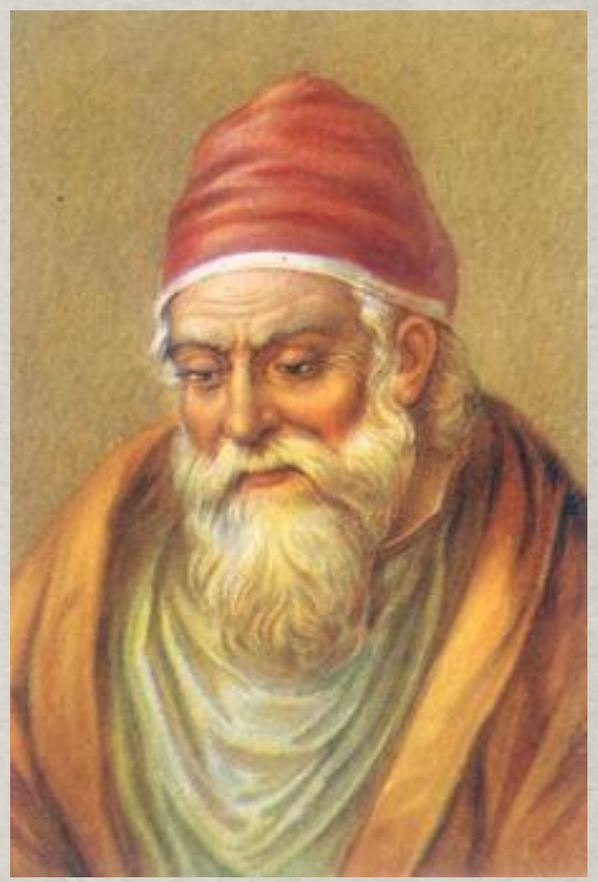
Podemos começar assumindo que existem apenas finitos primos, aplicar as leis da lógica (dedução) e chegar a uma contradição.

Vamos supor que temos apenas os primos:

$$2, 3, 5, 7, 11, 13, 17, ..., p_N,$$

Teoréma de Euclides.

Existe infinitos números primos.



Prova. (Segunda tentativa)

Podemos começar assumindo que existem apenas finitos primos, aplicar as leis da lógica (dedução) e chegar a uma contradição.

Vamos supor que temos apenas os primos:

$$2, 3, 5, 7, 11, 13, 17, ..., p_N,$$

($p_1 := 2$, por definição)

Vamos considerar o número

$$M := (p_1 p_2 \cdots p_N) + 1,$$

Vamos considerar o número

$$M := (p_1 p_2 \cdots p_N) + 1,$$

que é maior do que todos os nossos primos.

Vamos considerar o número

$$M := (p_1 p_2 \cdots p_N) + 1,$$

que é maior do que todos os nossos primos.

Como M é maior do que qualquer um de nossa lista finita de primos, M não pode ser primo, por hipótese.

Vamos considerar o número

$$M := (p_1 p_2 \cdots p_N) + 1,$$

que é maior do que todos os nossos primos.

Como M é maior do que qualquer um de nossa lista finita de primos, M não pode ser primo, por hipótese.

Observe algum fator primo não trivial de M,
e chame ele 'q', então $1 < q < M$. (porque?)

Vamos considerar o número

$$M := (p_1 p_2 \cdots p_N) + 1,$$

que é maior do que todos os nossos primos.

Como M é maior do que qualquer um de nossa lista finita de primos, M não pode ser primo, por hipótese.

Observe algum fator primo não trivial de M,
e chame ele 'q', então $1 < q < M$. (porque?)

Podemos assumir que existe um fator primo q,
pelo Teorema Fundamental da Aritmética.

Agora, como este fator q (fator de M) é primo,
q q deve ser um dos primos em nossa lista finita.

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

por algum número inteiro n.

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

por algum número inteiro n.

(isso implica) $\implies$ $p_k \cdot n - (2 \cdot 3 \cdots p_N) = 1$

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

por algum número inteiro n.

(isso implica) $\implies$ $p_k \cdot n - (2 \cdot 3 \cdots p_N) = 1$

Porém, agora temos p_k é fator do lado esquerda, então

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

por algum número inteiro n.

(isso implica) $\implies$ $p_k \cdot n - (2 \cdot 3 \cdots p_N) = 1$

Porém, agora temos p_k é fator do lado esquerda, então p_k é fator de 1, um contradição.

Agora, como este fator q (fator de M) é primo, q q deve ser um dos primos em nossa lista finita.

Em outras palavras, $q = p_k$, por algum k com $1 \leq k \leq N$.

Mas q é fator de M, então:

$$M = q \cdot n = (2 \cdot 3 \cdots p_N) + 1$$

por algum número inteiro n.

(isso implica) $\implies$ $p_k \cdot n - (2 \cdot 3 \cdots p_N) = 1$

Porém, agora temos p_k é fator do lado esquerda, então p_k é fator de 1, um contradição.

QED

Crítica?

Algoritmo de divisão

Algoritmo de divisão

Dados dois números inteiros, positivos a, b, com $b \neq 0$, existem inteiros únicos q e r, tais que:

Algoritmo de divisão

Dados dois números inteiros, positivos a, b, com $b \neq 0$, existem inteiros únicos q e r, tais que:

$$a = bq + r,$$

Algoritmo de divisão

Dados dois números inteiros, positivos a, b, com $b \neq 0$, existem inteiros únicos q e r, tais que:

$$a = bq + r,$$

e $$0 \leq r < b.$$

Algoritmo de divisão

Dados dois números inteiros, positivos a, b, com $b \neq 0$, existem inteiros únicos q e r, tais que:

$$a = bq + r,$$

e $\quad 0 \leq r < b.$

Lembrar: $0 \leq r < b$ (!)

Isso é muito utíl das provas.

Top 7 excuses for not doing homework

1. I accidentally divided by zero and my paper burst into flames.
2. I could only get arbitrarily close to my textbook. I couldn't actually reach it.
3. I have the proof, but there isn't room to write it in this margin.
4. I was watching the World Series and got tied up trying to prove that it converged.
5. I have a solar powered calculator and it was cloudy.
6. I locked the paper in my trunk, but a four-dimensional dog got into the trunk and ate it.
7. I could have sworn I put the homework inside a Klein bottle, but this morning I couldn't find it.

Se cuidem!