/ /

UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 28 de Março de 2017

- FORMULAS PARA GERAR NÚMEROS PRIMOS:

1) FÓRMULAS POLINOMIAIS

2) FÓRMULAS EXPONENCIAIS

2.1) NÚMEROS DE MERSENNE $(2^n - 1)$ -> DÁ MAIS OU MENOS BOM

2.2) NÚMEROS DE FERMAT $(2^{2^x} + 1)$ -> DÁ RUIM

3) FÓRMULAS FATORIAIS

1) FÓRMULAS POLINOMIAIS

POLINÔMIO (1 VARIÁVEL): $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$

Gostaria de obter um polinômio $f(x)$ tal que, para todo número natural $n$, $f(n)$ seja um número primo.

↳ Podemos mostrar que, para qualquer polinômio de uma variável, seja de que grau for, existem infinitos naturais $n$ tais que $f(n)$ é composto.

Vamos mostrar isso para polinômios de grau 2.

$f(x) = ax^2 + bx + c$

Se, para todo natural $n$, $f(n)$ for composto, já tenho o resultado desc-

jado.

Suponha então que exista um natural $m$. Tal que $f(m) = p$, onde $p$ é primo.

Vamos calcular $f(m+hp)$:

$$f(m+hp) = a(m+hp)^2 + b(m+hp) + c =$$
$$= a(m^2 + 2mhp + h^2p^2) + bm + bhp + c =$$
$$= am^2 + 2amhp + ah^2p^2 + bm + bhp + c =$$
$$= (\underbrace{am^2 + bm + c}_{p}) + 2amhp + ah^2p^2 + bhp =$$
$$= p + 2amhp + ah^2p^2 + bhp =$$
$$= p - (1 + 2amh + ah^2p + bh) :$$

Concluímos então que $f(m+hp)$ é composto sempre que

$$\cancel{1} + 2amh + ah^2p + bh > \cancel{1}$$

$$\Updownarrow$$

$$2amh + ah^2p + bh > 0$$
$$h(2am + ahp + b) > 0$$

Posso supor que $h > 0$

$$2am + ahp + b > 0$$
$$ahp > -b - 2am$$
$$h > \frac{-b-2am}{ap}$$

**Conclusão:** Sempre que $h > \frac{-b-2am}{ap}$, $f(m+hp)$ é composto. Tenho infinitos va-

lores de h.

3) Fórmulas Fatoriais:

Fatorial (n!) → Produto de todos os naturais positivos menores ou iguais a n

Exemplo: $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Primorial ($n^{\#}$) → Produto de todos os primos menores ou iguais a n.

Exemplos: $2^{\#} = 2$ $\quad$ $5^{\#} = 5 \cdot 3 \cdot 2 = 30$

$3^{\#} = 3 \cdot 2 = 6$ $\quad$ $6^{\#} = 5^{\#}$

$4^{\#} = 3 \cdot 2 = 6$ $\quad$ $7^{\#} = 7 \cdot 5 \cdot 3 \cdot 2 = 210$

*Tentativa de obter primos

| p | $p^{\#} + 1$ | |
|---|---|---|
| 2 | 3 | ✓ |
| 3 | 7 | ✓ |
| 5 | 31 | ✓ |
| 7 | 211 | ✓ |
| 11 | 2311 | ✓ |
| 13 | $30031 = 59 \cdot 509$ | × |

Teorema: Existem infinitos números primos.

Prova por contradição: suponha que existe uma quantidade finita de números primos. Então, existe um primo p. que é o maior primo de todos. Isso significa que todo número maior que p é composto.

Seja $n = p^{\#} + 1$, $n > p$, logo n é composto.

Então, existe um primo q que divide n.

/ /

Se $q$ é primo, $q \leq p$.

Sendo assim, $q$ divide $p^{\#}$,

$n = qK$

$p^{\#} = q \cdot K'$

$n = p^{\#} + 1$

$qK = qK' + 1$

$q(K - K') = 1$

$\Downarrow$

$q$ divide $1$

$\Downarrow$

$q = 1$

CONTRADIÇÃO: com o fato de que $q$ é primo. Logo, existem realmente infinitos números primos.

- CRIVO DE ERATÓSTENES

ENTRADA: inteiro positivo $n$

SAÍDA: Lista de todos os primos menores ou iguais a $n$.

ATRATIVO DO CRIVO: OBTÉM essa lista sem realizar nenhuma conta de divisão, que são as mais caras computacionalmente

CRIVO QUE FAZ DIVISÃO NÃO É O CRIVO REAL!

EXEMPLO: n = 36

| | | | | |
|---|---|---|---|---|
| | 3 | 5 | 7 | ~~9~~ |
| 11 | 13 | ~~15~~ | 17 | 19 |
| ~~21~~ | 23 | ~~25~~ | ~~27~~ | 29 |
| 31 | ~~33~~ | ~~35~~ | | |

PRIMOS: 2, 3, 5, 7, 11, 13, 17, 19, 21, 23, 29, 31

PROBLEMA: Alguns números são cortados mais de uma vez. Não dá para resolver completamente, mas é possível minimizá-lo.

↳ DUAS MELHORIAS:

- 1ª MELHORIA:

Até que valor preciso cortar antes de parar?

Todo número da lista é menor ou igual a n. Se o número for composto, ele possui pelo menos um fator menor ou igual a sua raiz. Se K é composto, K tem pelo menos um fator $\leq [\sqrt{K}]$

$K \leq n$

$[\sqrt{K}] \leq [\sqrt{n}]$

Se K tem fator $\leq [\sqrt{K}]$, K tem fator $\leq [\sqrt{n}]$. Então, todo número composto da lista tem algum fator menor ou igual a $[\sqrt{n}]$.

Logo, só preciso cortar até $[\sqrt{n}]$

EXEMPLO: $[\sqrt{36}] = 6$ → Corto até 5

| | | | | | |
|---|---|---|---|---|---|
| 3 | 5 | 7 | ~~9~~ | 11 | 13 |
| ~~15~~ | 17 | 19 | ~~21~~ | 23 | ~~25~~ |
| ~~27~~ | 29 | 31 | ~~33~~ | ~~35~~ | |

/ /

- SEGUNDA MELHORIA

Quando estou fazendo um dos cortes, a partir de que ponto devo começar a cortar?

Suponha que estou cortando de K em K. Se eu tenho na lista algum número composto com algum fator menor do que K, então ele já foi cortado em algum corte anterior.

PERGUNTA: Qual é o menor número composto divisível por K e que não possui nenhum fator menor que K?

$$t = K \cdot \underbrace{t'}_{\geq K}$$

$$t' \geq K$$

$$t \geq K \cdot K = K^2$$

CONCLUSÃO: Quando estou cortando de K em K, todos os multiplos de K que forem menores do que $K^2$ já foram cortados em cortes anteriores. Posso começar o corte de K em K no valor $K^2$

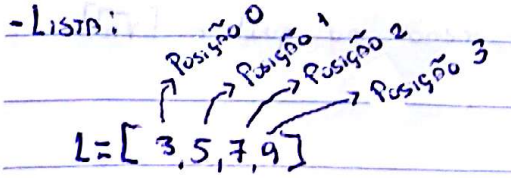
~~3~~ ~~5~~ 7 ~~9~~

11 13 ~~15~~ 17 19

~~21~~ 23 ~~25~~ ~~27~~ 29

31 ~~33~~ ~~35~~

- LISTA:




```
L=[ ] # LISTA VAZIA

L.append (3) # adicionando o valor no fim da lista
```

L[2] ← VALOR NA POSIÇÃO 2 DA LISTA L

L = [2] + L # FINAL

| POSIÇÃO | VALOR |
|---|---|
| 0 | 3 |
| 1 | 5 |
| 2 | 7 |
| ⋮ | ⋮ |
| j | $2_j + 3$ |
| ⋮ | ⋮ |
| $\frac{n-3}{2}$ | n |
| ⋮ | ⋮ |
| $\frac{k^2-3}{2}$ | $k^2$ |

←

- MATÉRIA PRIMEIRA PROVA

- CAPÍTULO 1 -> MENASCHÉ
- CAPÍTULO 1 -> COLLIER
- CAPÍTULO 2 -> COLLIER
- CAPÍTULO 8 -> COLLIER

} E CORRESPONDENTES DO MENASCHÉ