UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 23 de Março de 2017

Os dois algoritmos de fatoração vistos são ineficientes no caso geral. Entretanto, eles podem ser eficientes em alguns casos particulares.

- ALGORITMO INGÊNUO: é eficiente quando todos os fatores do número são pequenos (mesmo que o número seja grande)

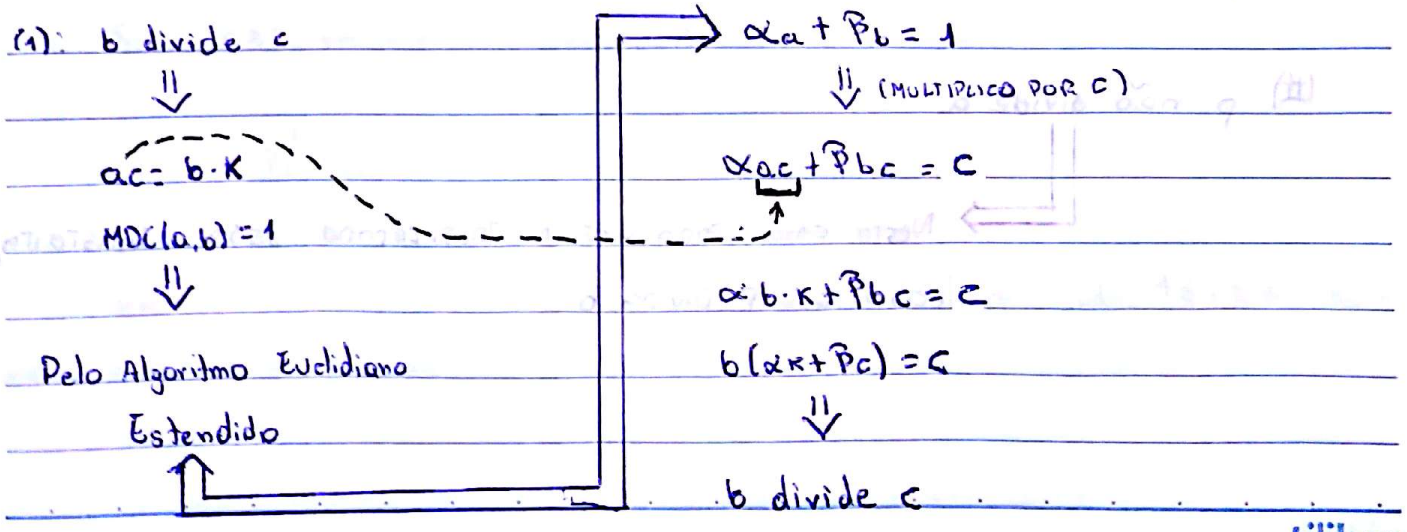
- ALGORITMO DE FERMAT: Lembrando, se $n = a \cdot b$, então $x = \frac{a+b}{2}$ e $y = \frac{b-a}{2}$. Tanto x quanto y vão aumentar de valor aos poucos no algoritmo até alcançarem os valores corretos.

Logo, quanto menor for o valor de $(b-a)$, mais rápido o algoritmo chega ao valor correto de y. Assim, o Algoritmo de Fermat é eficiente quando os dois fatores do número são próximos entre si (mesmo que o número seja grande).

LEMA: Sejam a, b, c inteiros positivos tais que $MDC(a,b) = 1$, então:

(1): Se b divide ac, então b divide c.

(2): Se a e b dividem c, então ab divide c.



tilibra

/ /

(2):

a divide c $\Rightarrow$ $c = a \cdot \ell$

b divide c $\Rightarrow$ $c = b \cdot m$

$c = a \cdot \ell$
$\in$
b divide c
} b divide $a \cdot \ell$

Como MDC $(a, b) = 1$, pelo resultado (1), se b divide $a\ell$, então b divide ℓ ($\ell = b \cdot m$)

$c = a\ell = (a.b)\, n$

$\Downarrow$

ab divide c

PROPRIEDADE FUNDAMENTAL DOS PRIMOS: seja p um número primo e a, b inteiros positivos. Se p divide ab, então p divide a ou p divide b

Inicialmente, temos dois casos possíveis:

(I) p divide a $\Rightarrow$ PROPRIEDADE SATISFEITA

(II) p não divide a

$\Rightarrow$ NESTE CASO, PARA QUE A PROPRIEDADE SEJA SATISFEITA, PRECISO QUE P DIVIDA b

tilibra

Preciso mostrar que, se p não divide a, então p divide b

MDC (a, p) =

p PRIMO

↳ DIVISORES DE p → 1 E p

↓

CANDIDATOS A MDC (a, p)

↓

DIVISOR COMUM

↓

TAMBÉM 1 E p

Se MDC (a, p) = p, isso significa que p divide a, o que contraria a hipótese.

Logo, MDC (a, p) = 1

Como MDC (a, p) = 1, pelo resultado (1) do lema anterior, como p divide ab, então p divide b.

TEOREMA FUNDAMENTAL DA ARITMÉTICA (TEOREMA DA FATORAÇÃO ÚNICA):

Seja $n \geq 2$ um inteiro. Então, existe uma fatoração:

$$n = p_1^{\ell_1} \cdot p_2^{\ell_2} \cdot \ldots \cdot p_K^{\ell_K},$$

onde $p_1 < p_2 < \ldots < p_K$ são primos distintos e $\ell_i \geq 1$ para todo $1 \leq i \leq K$. Além disso, essa fatoração é única.

tilibra

- EXISTÊNCIA: dois algoritmos que calculam a fatoração:
  - ↳ INGÊNUO
  - ↳ FORMAT

- UNICIDADE:
  - ↳ PROVA POR CONTRADIÇÃO

OBS: Se 1 fosse primo, não haveria unicidade da fatoração.

EXEMPLO: $n = 24$

$n = 2^3 \cdot 3$

$n = 1 \cdot 2^3 \cdot 3$

$n = 1^2 \cdot 2^3 \cdot 3$

$n = 1^3 \cdot 2^3 \cdot 3$

⋮

Suponha por contradição que existem inteiros positivos com mais de uma fatoração distinta. Seja n o menor destes números.

$$n = p_1^{\ell_1} \cdot p_2^{\ell_2} \dots p_k^{\ell_k} = q_1^{f_1} \cdot q_2^{f_2} \cdot \dots q_s^{f_s}$$

Da primeira fatoração, tenho que p_1 divide n.

⇓

p_1 divide $q_1^{f_1} \cdot q_2^{f_2} \dots q_t^{f_t}$

↓

PRIMO

Pela propriedade fundamental dos primos, como p_1 divide $q_1^{f_1} \cdot q_2^{f_2} \cdot \dots \cdot q_t^{f_t}$, então p_1 divide algum q_i, para algum $1 \leq i \leq t$.

Mas p_1 é primo e q_i também

tilibra

p_1 divide q_i
p_1 primo
q_i primo
$\Big\}\ p_1 = q_i$

$$n = p_1^{\ell_1} p_2^{\ell_2} \dots p_k^{\ell_k} = q_1^{\ell_1} q_2^{\ell_2} \dots q_{i-1}^{\ell_{i-1}} \cdot p_1^{\ell_i} \cdot q_{i+1}^{\ell_{i+1}} \dots q_t^{\ell_t}$$

Posso dividir tudo por p_1.

Seja n' o quociente da divisão de n por p_1 $(n = p_1 \cdot n')$

$$n' = p_1^{\ell_1 - 1} p_2^{\ell_2} \dots p_k^{\ell_k} = q_1^{\ell_1} q_2^{\ell_2} \dots q_{i-1}^{\ell_{i-1}} \cdot p_1^{\ell_i - 1} \cdot q_{i+1}^{\ell_{i+1}} \dots q_t^{\ell_t}$$

Tenho então um outro número (n') com duas fatorações distintas.

Mas $n' < n$, o que contradiz a hipótese de que n é o menor inteiro positivo com duas fatorações distintas.

Logo, a fatoração realmente é única.

- FORMULAS PARA OBTER NÚMEROS PRIMOS:

IDEIA: obter alguma função z, tal que, para qualquer inteiro positivo n, $z(n)$ seja primo.

1) Funções Polinomiais

2) Funções Exponenciais

3) Funções Fatoriais

tilibra

/ /

2) Fórmulas Exponenciais

↳ Números de Mersenne

↳ Números de Fermat

- NÚMEROS DE MERSENNE

$M(n) = 2^n - 1$

↳ NÚMERO INTEIRO POSITIVO

n	M(n)	n	M(n)
1	1	7	127
2	3		
3	7		
4	15		
5	31		
6	63		

RESULTADO: Se n é composto, M(n) com certeza é composto. Se n é primo, M(n) pode ser primo ou não.

- NÚMEROS DE FERMAT

$F(K) = 2^{2^K} + 1$

K	F(K)
0	3
1	5
2	17
3	257
4	65537

Infelizmente, estes são os únicos primos conhecidos na sequência de números de Fermat.

:(→ QUE TISTO!

tilibra