/ /

UFRS - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 21 de Março de 2017

Vamos estudar dois algoritmos de fatoração

1) Algoritmo "ingênuo"
2) Algoritmo de Fermat

- ALGORITMO "INGÊNUO": -> ALGORITMO DA ESCOLA

↳ Dado um inteiro $n \geq 2$, tentamos dividir n por todos os primos menores ou iguais a n.

EXEMPLO: $n = 28$

28	2
14	2
7	7
1	↳ FATORES

$n = 2^2 \cdot 7$

EXEMPLO: $n = 148$

148	2
74	2
37	37
1	↳ FATORES

$n = 2^2 \cdot 37$

EXEMPLO: $n = 360$

360	2
180	2
90	2
45	3
15	3
5	5
1	↳ FATORES

$n = 2^3 \cdot 3^2 \cdot 5$

-> Preciso testar todos os potenciais divisores no intervalo $2 \leq d \leq n$

-> Cada teste envolve uma conta de divisão (preciso testar se o resto da divisão de n por d é zero)

-> Eficiência terrível

Uma pequena melhoria que podemos aplicar a este algoritmo é:

↳ Seja $n \geq 2$ um número composto. Seja $f > 1$ o menor fator (maior ao que 1) de n. Então f é primo e $f \leq \sqrt{n}$. Em particular, como f é um número inteiro, $f \leq \lfloor \sqrt{n} \rfloor$

↳ PARTE INTEIRA DE $\sqrt{n}$

Como f é fator de n,

$n = f \cdot n' \Longrightarrow n' = \frac{n}{f}$ → O RESULTADO DA DIVISÃO SERÁ INTEIRO

↳ INTEIRO

Como f é o menor fator,

$f \leq n'$

$f \leq \frac{n}{f}$

$f^2 \leq n$

$f \leq \sqrt{n}$

Suponha, por contradição, q f é composto. Então,

$f = a \cdot b, \quad 1 < a \leq b < f$

$n = f \cdot n'$

$n = a \cdot b \cdot n'$

$\Downarrow$

a é fator de n
$a < f$

} Contradição com a hipótese de que f é o menor fator de n.

Logo, f é primo.

Uma consequência desse resultado é que, se n não possui nenhum fator menor ou igual a $\sqrt{n}$, então n é primo.

- ALGORITMO DE FERMAT
  - MATEMÁTICO FRANCÊS (TOULOUSE, SUL DA FRANÇA) SÉCULO XVI OU XVII

IDEIA: Dado $n \geq 2$, busco encontrar dois inteiros x e y tais que

$$n = x^2 - y^2.$$

$$n = x^2 - y^2 = (x+y) \cdot (x-y)$$

DOIS FATORES DE N

Para encontrar x e y, o algoritmo começa com um "palpite otimista": ele supõe que n é um quadrado perfeito, isto é, o palpite inicial é $x = \lceil \sqrt{n} \rceil$ e $y = 0$.

Se o palpite inicial não funcionar (isto é, se $n \neq x^2 - y^2$), o algoritmo incrementa x de uma unidade e recalcula y pela fórmula

$$y = [\sqrt{x^2 - n}].$$

Enquanto os palpites não funcionarem (enquanto $n \neq x^2 - y^2$), repito o processo (até um certo limite).

- PSEUDO CÓDIGO DO ALGORITMO DE FERMAT:

-> ENTRADA: inteiro ímpar $n \geq 3$

-> SAÍDA: Dois fatores de n ou uma mensagem de que n é primo

-> INSTRUÇÕES:

1) $x \leftarrow [\sqrt{n}]$, $y \leftarrow 0$

2) Enquanto $(n \neq x^2 - y^2)$ faça:

2.1) $x \leftarrow x + 1$

2.2) $y \leftarrow [\sqrt{x^2 - n}]$

2.3) Se $(x = (n+1)/2)$, então:

2.3.1) Pare e informe que n é primo.

3) Retorne $(x+y)$ e $(x-y)$.

OBS 1: Se n for par, um de seus fatores é 2. Podemos então dividir n por 2 sucessivas vezes até obter um número ímpar e então aplicar Fermat a este número.

OBS 2: Se eu desejar obter a fatoração completa de n, eu posso aplicar Fermat novamente aos fatores retornados e assim sucessivamente.

OBS 3: Os fatores retornados pelo Algoritmo de Fermat não são necessariamente primos.

/ /

EXEMPLO: $n = 1342127$

x	y	$n = x^2 - y^2$
1158	0	NÃO
1159	33	NÃO
1160	58	NÃO
1161	76	NÃO
1162	90	NÃO
1163	102	NÃO
1164	113	SIM

$x+y = 1277$

$x-y = 1054$

$(x+y)(x-y) = 1342158$

Proposição: Seja $n \geq 3$ ímpar e composto. Então, é possível encontrar valores de x e y tais que $n = x^2 - y^2$ e $\lceil \sqrt{n} \rceil \leq x \leq \frac{(n+1)}{2}$. (Logo, se x alcança $\frac{n+1}{2}$ no algoritmo, n realmente é primo).

n é composto

↓

$n = a \cdot b$, $1 < a \leq b \leq n$

Pelo algoritmo, obtenho:

↓

$n = (x-y)(x+y)$

$a = x - y$

$b = x + y$

$a + b = 2x$

$x = \frac{a+b}{2}$

$b = x + y$

$y = b - x = b - \frac{(a+b)}{2} = \frac{2b - a - b}{2} = \frac{b-a}{2}$

$x = \frac{a+b}{2}$, $y = \frac{b-a}{2}$

Como n é ímpar, a e b também são ímpares.

Logo, a+b e b-a são pares, o que significa que x e y são realmente inteiros.

Quero mostrar que o valor de $x = \frac{a+b}{2}$ satisfaz as condições $\lfloor \sqrt{n} \rfloor \leq x < \frac{n+1}{2}$. Vamos começar com $x < \frac{n+1}{2}$

$x < \frac{n+1}{2}$

$\Updownarrow$

$\frac{a+b}{2} < \frac{n+1}{2}$

$\Updownarrow$

$a+b < n+1$

$\Updownarrow$

$a+b < ab+1$

$\Rightarrow b-1 < ab-a$

$\Updownarrow$

$b-1 < a(b-1)$

$\Updownarrow$

$a > 1$

↳ CONDIÇÃO VERDADEIRA

Agora, vamos mostrar que:

$x \geq \sqrt{n}$

Como $\sqrt{n} \geq \lfloor \sqrt{n} \rfloor$, se $x \geq \sqrt{n}$, então $x \geq \lfloor \sqrt{n} \rfloor$ que é o resultado desejado.

$x \geq \sqrt{n}$

$\Updownarrow$

$\frac{a+b}{2} \geq n$

$\Updownarrow$

$a+b \geq 2\sqrt{n}$

$\Rightarrow (a+b)^2 \geq 4n$

$\Updownarrow$

$a^2 + 2ab + b^2 \geq 4n$

$\Updownarrow$

$a^2 + 2ab + b^2 \geq 4ab$

$\Updownarrow$

$a^2 - 2ab + b^2 \geq 0$

$\Updownarrow$

$(a-b)^2 \geq 0$

↳ CONDIÇÃO VERDADEIRA