/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 30 de Maio de 2017

- AULA PASSADA:

- TESTE DE LUCAS:

Seja n um inteiro positivo (ímpar). Então, n é primo se e somente se existe $2 \leq b \leq n-1$, tal que:

(1) $b^{n-1} \equiv 1 \pmod{n}$ e (2) $b^{(n-1)/p} \not\equiv 1 \pmod{n}$, para todo fator primo p de $n-1$.

- AGORA:

- TESTE DE LUCAS MELHORADO:

Seja n um inteiro positivo (ímpar). Então, n é primo se e somente se, para cada fator primo p_i de $n-1$, existe um $2 \leq b_i \leq n-1$ tal que

(1) $b_i^{n-1} \equiv 1 \pmod{n}$

(2) $b_i^{(n-1)/p} \not\equiv 1 \pmod{n}$

EXEMPLO: n = 103 (Lucas: b = 5)

$b = 2$, $n-1 = 102 = 2 \cdot 3 \cdot 17$

$2^{102} \equiv 1 \pmod{103}$ ✓ $2^{102/17} \equiv 2^6 \equiv 64 \pmod{103}$ ✓

$2^{102/2} \equiv 2^{51} \equiv 1 \pmod{103}$ ×

$2^{102/3} \equiv 2^{34} \equiv 46 \pmod{103}$ ✓

/ /

b = 3

$3^{102} \equiv 1 \pmod{103}$

$3^{51} \equiv 102 \pmod{103}$

103 é primo.

EXEMPLO 2: n = 109 (LUCAS: b = 6)

$n-1 = 108 = 2^2 \cdot 3^3$

b = 2

$2^{108} \equiv 1 \pmod{109}$ ✓

$2^{108/2} \equiv 2^{54} \equiv 108 \pmod{109}$ ✓

$2^{108/3} \equiv 2^{36} \equiv 1 \pmod{109}$ ✗

b = 3

$3^{108} \equiv 1 \pmod{109}$

$3^{36} \equiv 83 \pmod{109}$

109 é primo.

- DEMONSTRAÇÃO:

Seja p_i um fator primo de n-1. Seja b_i, tal que:

(1) $b_i^{n-1} \equiv 1 \pmod{n}$

(2) $b_i^{(n-1)/p} \not\equiv 1 \pmod{n}$

Por (1) e pelo Lema-chave a ordem de b_i (vamos chamá-la de s_i) divide $n-1$. $\longrightarrow$ $n-1 = s_i \cdot t$

Por (2) e pelo lema chave, s_i não divide $(n-1)/p_i$. Vamos escrever a fatoração de $(n-1)$

$$n-1 = p_1^{\ell_1} p_2^{\ell_2} \dots p_i^{\ell_i} \dots p_k^{\ell_k}$$

s_i divide $n-1$

↳ s_i tem os mesmos fatores primos de $n-1$

$s_i = p_1^{f_1} p_2^{f_2} \dots p_i^{f_i} \dots p_k^{f_k}$, onde $f_j \leq \ell_j$, para todo $1 \leq j \leq k$

No caso particular do fator p_i que estamos analisando:

$f_i \leq \ell_i$

Por outro lado,

$$\frac{(n-1)}{p_i} = p_1^{\ell_1} p_2^{\ell_2} \dots p_i^{\ell_i - 1} \dots p_k^{\ell_k}$$

s_i não divide $(n-1)/p_i$

↳ $f_i > \ell_i - 1$

$f_i \leq \ell_i$

$f_i > \ell_i - 1$

$\Big\} \; f_i = \ell_i$

Logo, s_i é a ordem de b_i

S_i é a ordem de b_i

↳ S_i é a ordem do subgrupo cíclico gerado por b_i

↳ Pelo teorema de Lagrange, a ordem de um subgrupo divide a ordem do grupo.

↳ S_i divide $\phi(n)$

$p_i^{e_i}$ divide S_i

S_i divide $\phi(n)$

} $p_i^{e_i}$ divide $\phi(n)$

Esse raciocínio é valido para todos os fatores de $n-1$.

$p_1^{e_1}$ divide $\phi(n)$

$p_2^{e_2}$ divide $\phi(n)$

$\vdots$

$p_k^{e_k}$ divide $\phi(n)$

} $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ divide $\phi(n)$

$\underbrace{p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}}_{n-1}$ divide $\phi(n)$

$n-1$ divide $\phi(n)$

$\Downarrow$

$n-1 \leq \phi(n)$

↳ Potências de primos distintos

Resultado geral: $\phi(n) \leq n-1$

$n-1 \leq \phi(n)$

$\phi(n) \leq n-1$

} $\phi(n) = n-1$

$\Downarrow$

n é primo.

Vamos estudar agora mais dois algoritmos de fatoração, específicos para a fatoração de números de Mersenne e Fermat, respectivamente.

1) Método de Fermat para a fatoração dos números de Mersenne

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

Lembrando: Se n é composto, M(n) é certamente composto. Se n é primo, M(n) pode ser primo ou composto.

Seja então M(p) com p primo. Suponha que q é um fator primo de $M(p) = 2^p - 1$

Se q divide $2^p - 1$

$\Downarrow$

$2^p - 1 \equiv 0 \pmod q$

$\Downarrow$

$2^p \equiv 1 \pmod q$

Como $2^p \equiv 1 \pmod q$, pelo lema chave, a ordem de 2 divide p.

Divisores de p $\begin{cases} 1 \\ 6 \\ p \end{cases}$

Ordem de 2 é 1 ou p.

$2^1 \not\equiv 1 \pmod q$

A ordem de 2 é p.

Pelo pequeno teorema de Fermat,

$2^{q-1} \equiv 1 \pmod q$

Pelo lema chave,

/ /

A ordem de 2, que é p, divide q-1.

$$\Downarrow$$

$$q-1 = p \cdot t$$

$$\Downarrow \quad \nearrow \text{IMPAR}$$

$$q = 1 + \underbrace{p \cdot t}_{\text{PAR}} \rightarrow \text{PAR}$$

$$\downarrow \quad \text{IMPAR}$$

Se assumirmas $p \geq 3$, p é impar.

$M_{(p)} = 2^p - 1$ também é impar

↳ Todo fator de $M_{(p)}$ também é impar

↳ q é impar

t é par

↳ $t = 2 \cdot r$

$$q = 1 + 2rp$$

Logo, se q é um fator primo de $M_{(p)}$, então q tem o formato

$$q = 1 + 2rp$$

Suponha que q é o menor fator primo de $M_{(p)}$

$$q \leq \sqrt{M_{(p)}} = \sqrt{2^p - 1} < \sqrt{2^p}$$

$$1 + 2rp < \sqrt{2^p}$$

$$2rp < \sqrt{2^p} - 1$$

$$r < \frac{\sqrt{2^p} - 1}{2p}$$

Busco o fator q no formato

$q = 1 + 2rp,$

Com r no intervalo

$$1 \leq r < \frac{\sqrt{2^p} - 1}{2p}$$

Como testar se q é fator de $M_{(p)}$?

Testo se $2^p \equiv 1 \pmod{q}$

EXEMPLO: $M_{(11)} = 2^{11} - 1 = 2047$

$$r < \frac{\sqrt{2^{11}} - 1}{2 \cdot 11} = \frac{2^{5,5} - 1}{2} = \frac{45,\ldots - 1}{22} = \frac{44,000}{22} = 2,\ldots$$

$$\Downarrow$$

$1 \leq r \leq 2$

$\hookrightarrow r = 1$ ou $r = 2$

$r = 1$

$q = 1 + 2rp = 1 + 2 \cdot 1 \cdot 11 = 1 + 22 = 23$

$2^{11} \equiv 1 \pmod{23}$? SIM!

R	A	E	IMPAR
1	2	11	SIM
2	4	5	SIM
8	16	2	NÃO
8	3	1	SIM
1	9	0	NÃO

Logo, 23 é fator de $M_{(11)}$

2) Método de Euler para a fatoração de números de Fermat

$$F(k) = 2^{2^k} + 1, \quad k \geq 0$$

Suponha que q é um fator primo de $F(k)$.

Então, $f(k) \equiv 0 \pmod q$

$$\Downarrow$$

$$2^{2^k} + 1 \equiv 0 \pmod q$$

$$\Downarrow$$

$$2^{2^k} \equiv -1 \pmod q$$

Elevo os dois lados ao quadrado:

$$(2^{2^k})^2 \equiv (-1)^2 \equiv 1 \pmod q$$
$$2^{2^k \cdot 2} \equiv 1 \pmod q$$
$$2^{2^{k+1}} \equiv 1 \pmod q$$

Pelo lema chave, a ordem de 2 divide 2^{k+1}. Logo, a ordem de 2 é 2^t, com $t \leq k+1$.

Mas,

$$2^{2^k} \equiv 1 \not\equiv -1 \pmod q$$

Então pelo lema chave, a ordem de 2 não divide 2^k

A ordem de 2 divide 2^{k+1}

A ordem de 2 não divide 2^k

} A ordem de 2 é igual a 2^{k+1}

Pelo teorema de Fermat, $2^{q-1} \equiv 1 \pmod q$

Pelo lema chave, a ordem de 2, que é 2^{k+1}, divide $q-1$.

$$q-1 = 2^{k+1} \cdot t$$

$$\Downarrow$$

$$q = 1 + 2^{k+1} \cdot t$$

Suponha que q é o menor fator primo de $F(k)$. Então,

$$q \leq \sqrt{F(k)} = \sqrt{2^{2^k}+1} \leq \sqrt{2^{2^k}} + 1$$

$$1 + 2^{k+1} \cdot t \leq \sqrt{2^{2^k}} + 1$$

$$t \leq \frac{\sqrt{2^{2^k}}}{2^{k+1}} = \frac{2^{(2^k)/2}}{2^{k+1}} = \frac{2^{2^{k-1}}}{2^{k+1}} = 2^{2^{k-1} - k - 1}$$

$$1 \leq t \leq 2^{2^{k-1} - k - 1}$$

Exemplo: $F(5) = 2^{2^5} + 1 = 2^{32} + 1$

$$t \leq 2^{2^{5-1} \cdot 5 - 1} = 2^{2^4 - 6} = 2^{16-6} = 2^{10} = 1024$$

$$1 \leq t \leq 1024$$

$t = 1 \rightarrow q = 1 + 2^6 \cdot 1 = 65$

Testará se

$$2^{32} \equiv -1 \pmod{65}$$

/ /

$t=2 \rightarrow q = 1 + 2^6 \cdot 2 = 129$

Testará se

$2^{32} \equiv -1 \pmod{129}$ NÃO!

⋮

$t=10 \rightarrow q = 1 + 2^6 \cdot 10 = 1 + 640 = 641$

$2^{32} \equiv -1 \pmod{641}$ SIM!

Logo, 641 é fator de $F(5)$