UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 27 de Abril de 2017

- NÚMERO DE CARMICHAEL $\Rightarrow$ (2)

(2) = p^2 não divide n

Suponha que n é um número de Carmichael. Então, ↳ n é composto

$$a^n \equiv a \pmod n$$

Para todo $2 \leq a \leq n-1$ em particular, se p é um fator primo de n, então $2 \leq p \leq n-1$. Logo, $p^n \equiv p \pmod n$ ↳ (*)

Isto é, n divide $p^n - p$

Suponha, por contradição, que p^2 divide n.

Então,

p^2 divide n
n divide $p^n - p$
} p^2 divide $p^n - p$

$$p^n - p = p^2 \cdot t$$
$$p(p^{n-1} - 1) = p^2 \cdot t$$
$$p^{n-1} - 1 = pt$$
$$p^{n-1} - pt = 1$$
$$p(p^{n-2} - t) = 1$$

p divide 1

$$p = 1 \quad (**)$$

(*) + (**) → CONTRADIÇÃO

Logo, p^2 não divide n.

- TESTE DE MILLER (OU MILLER-RABIN)

→ Ideia semelhante à do teste baseado no teorema de Fermat

→ Permite determinar que alguns números são compostos sem fatorá-los.

→ Consegue distinguir mais números compostos do que o Teste anterior.

Suponha que n é primo. Seja $2 \leq a \leq n-1$. Então, pelo teorema de Fermat,

$$a^{n-1} \equiv 1 \pmod{n}$$

$$\Downarrow$$

n divide $a^{n-1} - 1$.

Suponha que n é ímpar e $n \geq 3$. O expoente $n-1$ na potência a^{n-1} é maior ou igual a 2 e par → $\frac{n-1}{2}$ é um número inteiro.

$$a^{n-1} = \left(a^{\frac{n-1}{2}}\right)^2 - 1^2 = \left(a^{\frac{n-1}{2}} + 1\right)\left(a^{\frac{n-1}{2}} - 1\right)$$

Seja $k = \frac{n-1}{2}$

$$a^{n-1} = (a^k + 1)(a^k - 1)$$

n divide $a^{n-1} - 1$. Logo, n divide $(a^k + 1)(a^k - 1)$ → (x)

↳ PELA HIPÓTESE INICIAL, N É PRIMO

PROPRIEDADE FUNDAMENTAL DOS PRIMOS: Se p é primo e p divide $a \cdot b$, então p divide a

ou p divide b

(*) → n divide $a^k + 1$ ou n divide $a^k - 1$

⇓

$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$

ou

$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$

- VAMOS REFINAR UM POUCO ESSA IDEIA:

$n-1$ é par.

Então, posso escrever

$\underbrace{n-1}_{\downarrow} = 2^t \cdot q$, onde q é impar e $t \geq 1$

$a^{n-1} \equiv 1 \pmod{n}$

$a^{2^t \cdot q} \equiv 1 \pmod{n}$

⇓

n divide $\underbrace{a^{2^t \cdot q} - 1}$

↳ PRODUTO NOTÁVEL.

$a^{2^t \cdot q} - 1 = (a^{2^{t-1} \cdot q})^2 - 1^2 = (a^{2^{t-1} \cdot q} + 1)(a^{2^{t-1} \cdot q} - 1)$

⇓

n divide $a^{2^{t-1} \cdot q} + 1$

ou

n divide $a^{2^{t-1} \cdot q} - 1$

⇓

$a^{2^{t-1} \cdot q} \equiv -1 \pmod{n}$ ou $a^{2^{t-1} \cdot q} \equiv 1 \pmod{n}$

FORMATO IGUAL AO DA CONGRUÊNCIA ORIGINAL

↓

POSSO TENTAR REPETIR O PROCESSO

Se $t-1 = 0$,

$$a^{2^{t-1} \cdot q} \equiv 1 \pmod{n}$$

$$\Downarrow$$

$$a^q \equiv 1 \pmod{n}$$

Se $t-1 \geq 1$,

$$a^{2^{t-1} \cdot q} - 1 = \left(a^{2^{t-2} q}\right)^2 - 1^2 = \left(a^{2^{t-2} q} + 1\right)\left(a^{2^{t-2} \cdot q} - 1\right)$$

$$\Downarrow$$

n divide $a^{2^{t-2}} q + 1$

OU

n divide $a^{2^{t-2} \cdot q} - 1$

$$a^{2^{t-2} \cdot q} \equiv -1 \pmod{n}$$

OU

$$a^{2^{t-2} \cdot q} \equiv 1 \pmod{n}$$

↳ POSSO TENTAR REPETIR O PROCESSO DE NOVO

Seja j o menor inteiro não-negativo tal que:

$$a^{2^j \cdot q} \equiv 1 \pmod{n}$$

Se $j = 0$,

$$a^q \equiv 1 \pmod{n}$$

Se $j > 0$,

$$a^{2^j \cdot q} - 1 = \left(a^{2^{j-1} \cdot q}\right)^2 - 1^2 = \left(a^{2^{j-1} \cdot q} + 1\right)\left(a^{2^{j-1} \cdot q} - 1\right)$$

/ /

n divide $a^{2^{j-1}\cdot q} + 1 \Rightarrow a^{2^{j-1}\cdot q} \equiv -1 \pmod{n}$

ou

n divide $a^{2^{j-1}\cdot q} - 1 \Rightarrow \underline{a^{2^{j-1}\cdot q} \equiv 1 \pmod{n}}$

↳ ESSE CASO NÃO PODE ACONTECER

Logo,

$a^{2^{j-1}\cdot q} \equiv -1 \pmod{n}$

Lembrando,

$n-1 = z^t \cdot q$

Então,

$0 \leq j \leq t$

$0 \leq j-1 \leq t-1$

Calculo as potências

$a^q, a^{2\cdot q}, a^{2^2\cdot q}, a^{2^3\cdot q}, \ldots, a^{2^{t-1}\cdot q} \Rightarrow t$ potências

Pelo que vimos, se n é primo, então

$a^q \equiv 1 \pmod{n}$

ou

Alguma das potências da sequência (pode ser a primeira) é congruente a -1

No sentido inverso, se $a^q \not\equiv 1 \pmod{n}$ e $a^{2^u\cdot q} \not\equiv 1 \pmod{n}$, para todo $0 \leq u \leq t$, então n com certeza é composto.

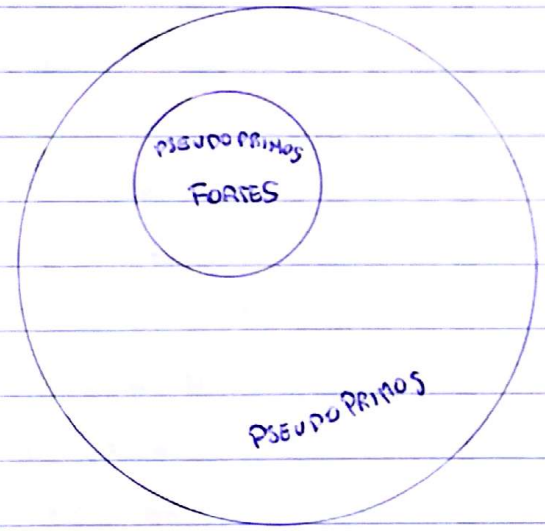
Esse é o Teste de Miller - Rabin.

Assim como o teste anterior, este teste produz como resultados composto ou inconclusivo.

Um número composto que retorna resultado inconclusivo no teste de Miller-Rabin com a base a é chamado de pseudoprimo forte para a base a.

Existem menos pseudoprimos fortes do que pseudoprimos para a base a.

Todo pseudoprimo forte para a base a é um pseudoprimo para a base a. Mas o inverso não é verdadeiro.



EXEMPLO 1: $n=341$ (PSEUDOPRIMO PARA A BASE 2)

$n-1 = 340 = 2^2 \cdot 85^9$

$t = 2$

$q = 85$

$a = 2$

$a^q, a^{2^1 \cdot q}, (a^q)^{2^{t-1}}$

$2^{85} \equiv 32 \not\equiv \pm 1 \pmod{341}$

$2^{170} \equiv 32^2 \not\equiv \pm 1 \pmod{341}$

↓

COMPOSTO

R	A	E	É IMPAR
1	2	85	SIM
2	4	42	NÃO
2	16	21	SIM
32	256	10	NÃO
32	64	5	SIM
2	4	2	NÃO
2	16	1	SIM
32	256	0	NÃO

EXEMPLO 2: $n = 561$ (CARMICHAEL)

$n - 1 = 560 = 2^4 \cdot 35$

$t = 4$

$q = 35$

$a = 2$

R	A	E	IMPAR
1	2	35	SIM
2	4	17	SIM
3	16	8	NÃO
8	256	4	NÃO
8	460	2	NÃO
8	103	1	SIM
263	511	0	NÃO

$2^{35} \equiv 263 \not\equiv \pm 1 \pmod{561}$

$2^{2 \cdot 35} \equiv 263^2 \equiv 166 \not\equiv \pm 1 \pmod{561}$

$2^{2^2 \cdot 35} \equiv 166^2 \equiv 67 \not\equiv \pm 1 \pmod{561}$

$2^{2^3 \cdot 35} \equiv 67^2 \equiv 1 \not\equiv -1 \pmod{561}$

↓

COMPOSTO

EXEMPLO 3: $n = 25$

$a = 7$

$n - 1 = 24 = 2^3 \cdot 3$

$t = 3$

$q = 3$

$7^3 \equiv 18 \not\equiv \pm 1 \pmod{25}$

$7^{2 \cdot 3} \equiv 18^2 \equiv 24 \equiv -1 \pmod{25}$

$7^{2^2 \cdot 3} \equiv$ PROBLEMA ↓

INCONCLUSIVO

↳ 25 É PSEUDO PRIMO FORTE PARA A BASE 7

OBSERVAÇÕES:

1) Não existe o equivalente dos números de Carmichael pro teste de Miller.

2) Ao testar com uma base selecionada aleatoriamente no intervalo $2 \leq a \leq n-1$ e o resultado der Inconclusivo, a chance de n ser primo é $\approx \frac{3}{4}$ e de ser composto é de $\approx \frac{1}{4}$.

Logo, testando com k bases distintas escolhidas aleatoriamente, se os testes derem inconclusivo com todas as bases, a chance de ser composto é de $\approx \frac{1}{4^k}$.

Com 10 bases é menor que 1 em 1 bilhão.

- RESOLUÇÃO DE SISTEMAS DE CONGRUÊNCIAS:

$x \equiv 1 \pmod{13}$

$x \equiv 4 \pmod{15}$

$x \equiv 8 \pmod{19}$

$\rightarrow x \equiv 1 \pmod{13}$

$x - 1 = 13k$

$x = 1 + 13k$

$1 + 13k \equiv 4 \pmod{15}$

$13k \equiv 3 \pmod{15}$

↳ CALCULAR O INVERSO DE 13

$7 \cdot 13k \equiv 7 \cdot 3 \pmod{15}$

$k \equiv 6 + 15l$

$x = 1 + 13k = 1 + 13(6 + 15l) = 1 + 78 + 195l = 79 + 195l$

$x \equiv 79 \pmod{195}$

/ /

$$\begin{cases} x = 79 \pmod{195} \\ x = 8 \pmod{19} \end{cases}$$