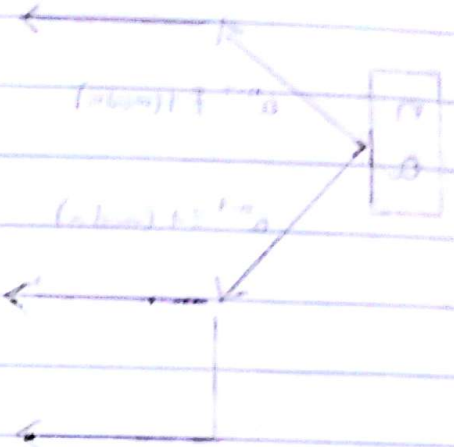
/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 25 de Abril de 2017

- AULA PASSADA



- TESTE BASEADO NO TEOREMA DE FERMAT:

Quero testar se n é primo ou composto.

Seleciono uma base $1 < a < n$.

Se $a^{n-1} \not\equiv 1 \pmod{n}$, n com certeza é composto. Neste caso, a é uma testemunha de que n é composto.

Se $a^{n-1} \equiv 1 \pmod{n}$, o resultado do teste é inconclusivo.

n pode ser primo ou n pode ser composto (neste caso, n é um pseudoprimo para a base a)

Se testarmos com várias bases e o resultado der sempre inconclusivo, a probabilidade de ser primo aumenta.

E se eu testar com todas as bases? (Inviável na prática)

Se n for primo, obviamente o resultado vai ser inconclusivo para todas.

Suponha então que n é composto. Seja então f um fator de n ($\underbrace{1 < f < n}_{(*)}$)

$$n = f \cdot n'$$

Vamos realizar o teste escolhendo f como base:

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

Suponha que $f^{n-1} \equiv 1 \pmod{n}$ então $f^{n-1} - 1$ é multiplo de n. Em outras palavras, n divide $f^{n-1} - 1$.

f divide n
f divide $f^{n-1} - 1$
⇒ f divide $f^{n-1} - 1$
⇓
$f^{n-1} - 1 = f \cdot t$

$f^{n-1} - 1 = f \cdot t$
$f^{n-1} - f \cdot t = 1$
$f(f^{n-2} - t) = 1$
⇓
f divide 1
↳ $f = 1$ } (**)

(*) + (**) ⇒ Contradição

Portanto,

$f^{n-1} \not\equiv 1 \pmod{n}$

(quando n é composto e $1 < f < n$ é fator de n)
⇓
Pelo teste, f será uma testemunha de que n é composto.

Logo, se n é composto, o teste não pode produzir resultado inconclusivo para todas as bases.

/ /

Infelizmente, existem números, conhecidos como, Números de Carmichael, que são números compostos, mas que

$$a^{n-1} \equiv 1 \pmod{n} \rightarrow \text{(TESTE INCONCLUSIVO)}$$

para toda base a tal que $MDC(a,n) = 1$.

Em outras palavras, para estes números, encontrar uma base que nos permita ter certeza que n é composto (isto é, uma base b tal que $b^{n-1} \not\equiv 1 \pmod{n}$) é equivalente a encontrar um fator de n.

Assim, para estes números, o teste é tão difícil quanto a fatoração quanto a fatoração direta do número.

Infelizmente ao quadrado, existem infinitos Números de Carmichael.

Assim, na prática, o teste me permite determinar com certeza que alguns números são compostos, mas não que um número é primo. Além disso, o teste é inútil para números como os Números de Carmichael.

OBSERVAÇÃO: Para ser um número de Carmichael, o número deve ser composto. Números primos também satisfazem a condição

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

para todo a tal que $MDC(a,n) = 1$, mas não são números de Carmichael.

561 é o menor número de Carmichael,

$561 = 3 \cdot 11 \cdot 17$ (COMPOSTO)

Para não termos que lidar constantemente com a condição $MDC(a,n)=1$, podemos definir um número de Carmichael como um número composto tal que $a^n \equiv a \pmod n$ para todo $1<a<n$.

$2 \leq a \leq 560$

$a^{561} \equiv \pmod{561}$

$\Downarrow$

$a^{561} \equiv (a^2)^{280} \cdot a \equiv a \pmod 3$ ($a^2 \equiv 1$)

$a^{561} \equiv (a^{10})^{56} \cdot a \equiv a \pmod{11}$ ($a^{10} \equiv 1$) → Módulos Primos

$a^{561} \equiv (a^{16})^{35} \cdot a \equiv a \pmod{17}$ ($a^{16} \equiv 1$)

$a^{561} \equiv a \pmod 3$

$a^{561} \equiv a \pmod{11}$ ⟹

- 3 divide $a^{561}-a$ — $MDC(3,11)=1$
- 11 divide $a^{561}-a$ — $MDC(3,17)=1$
- 17 divide $a^{561}-a$ — $MDC(11,17)=1$

$a^{561} \equiv a \pmod{17}$

LEMA DA SEGUNDA SEMANA DE AULA: Se $MDC(a,b)=1$, a divide c e b divide c, então ab divide c.

O MDC entre dois primos distintos é sempre 1.

CONCLUSÃO: O produto $3 \cdot 11 \cdot 17 = 561$ divide $a^{561}-a$. Logo,

$a^{561} \equiv a \pmod{561}$

561 é número de Carmichael.

/ /

• TEOREMA DE KORSELT:

Seja $n \geq 2$ um inteiro composto. n é um número de Carmichael se e somente se, para todo fator primo p de n, as seguintes condições são satisfeitas:

(1) $p-1$ divide $n-1$ (n deixa resto 1 na divisão por $p-1$)

(2) p^2 não divide n. (p só aparece uma vez na fatoração de n)

(⇑)

Suponha que, para todo fator primo p de n, as condições (1) e (2) são satisfeitas.

Seja $2 \leq a \leq n-1$, pela condição (2),

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k$$
$$(p_1 < p_2 < p_3 < \ldots < p_k)$$

Vou calcular a^n módulo p_i, para todo $1 \leq i \leq k$.

Pelo Teorema de Fermat,

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

Divido n por $p_i - 1$:

$$n = (p_i - 1) \cdot q + r$$

Pela condição (1): $r = 1$.

$a^n \equiv a^{(p_i - 1)\cdot q + 1} \equiv \underbrace{\left(a^{p_i - 1}\right)^q}_{\equiv 1} \cdot a \equiv a \pmod{p_i}$

p_i divide $a^n - a$, para todo $1 \leq i \leq k$

Logo, o produto $p_1 p_2 \cdots p_k = n$ divide $a^n \equiv a \pmod{n}$

⇓

$a^n \equiv a \pmod{n}$, para todo $2 \leq a \leq n-1$

⇓

Logo, n é um número de Carmichael.

- FALTA MOSTRAR:

- NÚMERO DE CARMICHAEL → (1)
- NÚMERO DE CARMICHAEL → (2)

→ MAIS FÁCIL (PRECISA DE UM RESULTADO CHAMADO "TEOREMA DA RAIZ PRIMITIVA", QUE É DADO NO SEGUNDO FINAL DO CURSO)