/ /

UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 23 de Maio de 2017

- AULA PASSADA:

TEOREMA: Seja $(G, *)$ um grupo finito cíclico de ordem t e g um gerador de $(G, *)$. Então, g^m também é um gerador de $(G, *)$ se e somente se $MDC(m, t) = 1$.

- AGORA:

CONSEQUÊNCIA (COROLÁRIO): Se $(G, *)$ é um grupo finito cíclico de ordem t, então $(G, *)$ possui exatamente $\phi(t)$ geradores.

Se $(G, *)$ é cíclico, ele possui pelo menos um gerador g.

Posso escrever G como:

$$G = \underbrace{\{g^0, g^1, g^2, g^3, \cdots, g^{t-1}\}}_{t \text{ elementos}}$$

Pelo teorema anterior, os geradores de $(G, *)$ são os elementos do conjunto.

$$A = \{g^i : 0 \leq i < t \text{ e } MDC(i, t) = 1\}$$

Logo, o número de geradores é igual ao número de elementos do conjunto A.

Quantos valores de i existem no intervalo $0 \leq i < t$ tais que $MDC(i, t) = 1$?

↳ Estes são os valores no intervalo $0 \leq i < t$ que tem inverso módulo t.

⇓

Logo, estes são os elementos de $U(t)$

⇐ $U(t)$ tem $\phi(t)$ elementos

/ /

- PROBLEMA DO LOGARITMO DISCRETO (PLD OU DLP, EM INGLÊS) (FUNDAMENTAL PARA A CRIPTOGRAFIA EL GAMAL):

Seja $(G,*)$ um grupo finito cíclico, g um gerador de $(G,*)$ e h um elemento qualquer de G. O PLD consiste em encontrar o valor do expoente x tal que:

$$g^x = h \text{ em } (G,*).$$

x é conhecido como logaritmo discreto de h na base g.

Por que logaritmo discreto?

No caso real ($\mathbb{R}$), se

$$g^x = h,$$

podemos escrever que

$$x = \log_g^h$$

O nome vem de analogia a esse caso.

Dependendo do grupo $(G,*)$ utilizado, o PLD pode ser muito complexo computacionalmente.

TEOREMA DA RAIZ PRIMITIVA:

- Se p é primo, então $U(p)$ é cíclico.

OBSERVAÇÃO: RAIZ PRIMITIVA = GERADOR.

/ /

DEMONSTRAÇÃO: DAQUI A POUCO!

COROLÁRIO: Se p é primo, então U(p) tem exatamente $\phi(p-1)$ geradores.

NÚMERO DE ELEMENTOS DE $U(p) = \phi(p)$

NÚMERO DE GERADORES DE $U(p) = \phi(p-1)$

DEMONSTRAÇÃO: U(p) tem ordem p-1. Pelo teorema da raiz primitiva, U(p) é cíclico. Pelo corolário anterior, um grupo cíclico de ordem t tem $\phi(t)$ geradores. Logo, U(p) tem $\phi(p-1)$ geradores.

EXEMPLO: U(7)

↳ 7 É PRIMO

NÚMERO DE ELEMENTOS: $\phi(7) = 6$.

$U(7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

NÚMERO DE GERADORES: $\phi(6) = 2$

$\phi(6) = \phi(2 \cdot 3) = \phi(2)\,\phi(3) = 1 \cdot 2 = 2$

FINALIZAÇÃO DA DEMONSTRAÇÃO DO TEOREMA DE KORSELT:

TEOREMA: Seja $n \geq 3$ um número composto. Então, n é um número de Carmichael se e somente se, para cada fator primo p de n, as seguintes condições são satisfeitas:

(1) p-1 divide n-1

(2) p^2 não divide n

Só fizemos:

(1) + (2) => CARMICHAEL

CARMICHAEL => (2)

/ /

. Agora vamos fazer

CARMICHAEL => (1)

Seja n um número de Carmichael. Então, para todo $1 < b < n$,

$$b^n \equiv b \pmod{n}$$

Logo, n divide $b^n - b$

Seja p um fator primo de n.

p divide n

n divide $b^n - b$

$\Rightarrow p$ divide $b^n - b$

$$\Downarrow$$

$$b^n \equiv b \pmod{p}$$

Como p é primo, pelo teorema da raiz primitiva, $U(p)$ é cíclico e tem um gerador g $(1 < g < n)$.

Então $g^n \equiv g \pmod{p}$

Divido n por $p-1$ (que é a ordem de $U(p)$)

$$n = (p-1)q + r \quad 0 \leq r < p-1$$

$$g^n \equiv g \pmod{p}$$

$$g^{(p-1)q+r} \equiv g \pmod{p}$$

$$\left(g^{p-1}\right)^q \cdot g^r \equiv g \pmod{p}$$

$$\Downarrow$$

$$1$$

$g^r \equiv g \pmod p$

$\Downarrow$

$r = 1$

$n = (p-1)q + 1$

$n - 1 = (p-1)q \Rightarrow p-1$ divide $n-1$.

Para realizar a demonstração do teorema da raiz primitiva, preciso de dois resultados auxiliares (lemas):

LEMA 1: Seja $(G, *)$ um grupo abeliano finito, $a, b \in G$, onde a ordem de a é m, a ordem de b é n e $MDC(m,n) = 1$. Então, a ordem de $(a * b)$ é mn.

NOTAÇÃO: Ao invés de $a * b$, vou escrever ab.

$(ab)^{mn} = (ab) * (ab) * \ldots * (ab)$

Como o grupo é abeliano, posso reagrupar os termos

$(ab)^{mn} = a^{mn} * b^{mn} = (a^m)^n * (b^n)^m = e$

(com $a^m \equiv e$ e $b^n \equiv e$)

Pelo lema-chave, a ordem de ab divide mn

Suponha que a ordem de ab é k (k divide mn) -> $(*)$

$(ab)^k = e$

k divide $mn \Rightarrow mn = k \cdot t$

$(ab)^{kn} = a^{kn} b^{kn} =$

$= a^{kn} (b^n)^k = a^{kn}$, onde $b^n = e$

Por outro lado:

$(ab)^{kn} = ((ab)^k)^n = e$, onde $(ab)^k = e$

$\Rightarrow a^{kn} = e$

$\Downarrow$

m (ordem de a) divide kn.

m divide kn
$MDC(m,n)=1$
$\Rightarrow m$ divide k.

$(ab)^{km} = ((ab)^k)^m = e$, onde $(ab)^k = e$

Por outro lado,

$(ab)^{km} = a^{km} b^{km} = (a^m)^k \cdot b^{km} = b^{km}$, onde $a^m = e$

$\Rightarrow b^{km} = e$

n (ordem de b) divide km.

n divide km
$MDC(m,n) = 1$
$\Rightarrow n$ divide k

m divide k
n divide k
$MDC(m,n)=1$
$\Rightarrow mn$ divide $k \to (**)$

$(*) + (**) \Rightarrow mn = k$

LEMA 2: A congruência $x^k \equiv 1 \pmod{p}$, onde p é primo, x é uma variável e k é uma constante fixada, tem, no máximo, k soluções distintas módulo p.

Não vamos demonstrar esse lema.

DEMONSTRAÇÃO DO TEOREMA DA RAIZ PRIMITIVA:

p é primo.

Começo fatorando $p-1$ (ordem de $U(p)$)

$$p-1 = q_1^{e_1} q_2^{e_2} \dots q_t^{e_t}$$

Para cada fator primo q_i, quero achar um elemento h_i em $U(p)$ que tenha ordem $q_i^{e_i}$.

Começo buscando um elemento a_i tal que $a_i^{(p-1)/q_i} \not\equiv 1 \pmod{p}$. Esse elemento precisa existir, porque, pelo lema 2, a congruência $x^{(p-1)/q_i} \equiv 1 \pmod{p}$ tem no máximo $(p-1)/q_i$ soluções e $p-1/q_i < p-1$, que é a quantidade total de elementos em $U(p)$.

Obtido este a_i, calculo:

$$h_i \equiv a_i^{(p-1)/q_1^{e_i}} \pmod{p}$$

Vamos mostrar que h_i realmente tem ordem $q_i^{e_i}$.

$$h_i^{q_1^{e_i}} \equiv a_i^{p-1} \equiv 1 \pmod{p}$$

Logo, pelo lema chave, a ordem de h_i divide $q_i^{e_i}$ mas q_i é primo. Logo, a ordem de h_i é q_i^{u}, onde $u \leq e_i$.

Suponha que $u < e_i$

Temos:

$$h_i^{q_i^u} \equiv 1 \pmod{p}$$

$$a_i^{(p-1)\cdot q_i^u / q_i^{e_i}} \equiv 1 \pmod{p}$$

$$a_i^{(p-1)/q_i^{e_i - u}} \equiv 1 \pmod{p}$$

Pelo lema-chave, a ordem de a_i divide $\frac{(p-1)}{q_i^{e_i-u}}$. Mas, como supomos que $u < e_i$, então $e_i - u > 0$.

Logo, $\frac{(p-1)}{q_i^{e_i-u}}$ divide $\frac{(p-1)}{q_i}$

Assim, se

$$a_i^{(p-1)/q_i^{e_i-u}} \equiv 1 \pmod{p},$$

então,

$$a_i^{(p-1)/q_i} \equiv 1 \pmod{p},$$

o que contradiz a hipótese inicial de que

$$a_i^{(p-1)/q_i} \not\equiv 1 \pmod{p}$$

Logo, a ordem de h_i é $q_i^{e_i}$.

Uma vez obtido todos os $h_1, h_2, \dots, h_t$, calcula:

$g \equiv h_1 h_2 h_3 \dots h_t \pmod p$

Pelo lema 1, como a ordem dos h_i's são potências de primos distintos, a ordem do produto dos h_i's será o produto das ordens. Mas, o produto das ordens é $q_1^{e_1} q_2^{e_2} \dots q_t^{e_t} = p-1$

Logo, g é um gerador de $U(p)$.

ALGORITMO DE GAUSS

- ENTRADA: primo p
- SAÍDA: um gerador g de $U(p)$
- INSTRUÇÕES:
  1) Fatore $p-1$ $(p-1 = q_1^{e_1} q_2^{e_2} \dots q_t^{e_t})$
  2) $g \leftarrow 1$
  3) Para cada fator q_i, faça:
     3.1) $a \leftarrow 2$
     3.2) Enquanto $a^{(p-1)/q_i} \equiv 1 \pmod p$, faça $a \leftarrow a+1$
     3.3) $h \leftarrow (a^{(p-1)/q_i^{e_i}}) \pmod p$
     3.4) $g \leftarrow (g * h) \pmod p$
  4) Retorno g.