UFRJ - Universidade Federal do Rio de Janeiro

Rio de Janeiro, 09 de Maio de 2017

- GRUPOS (CONTINUAÇÃO):

- EXEMPLOS (CONTINUAÇÃO):

9) $(\mathbb{Z}_n, +)$

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$

$+$ é uma operação em $\mathbb{Z}_n$? SIM!

$+$ é associativa? SIM!

Existe elemento neutro? SIM, o $\bar{0}$!

Todo elemento possui inverso? SIM! O inverso de $\bar{a}$ é $-\bar{a}$ ou $\overline{n-a}$.

Então $(\mathbb{Z}_n, +)$ é grupo!

10) $(\mathbb{Z}_n, \times)$

$\times$ é uma operação em $\mathbb{Z}_n$?

$\times$ é associativa? SIM!

Existe o elemento neutro? SIM! o $\bar{1}$!

Todo elemento tem inverso? NÃO! $\bar{a}$ só tem inverso se e somente se $MDC(a,n) = 1$ (em particular, qualquer que seja n, $\bar{0}$ não tem inverso

$(\mathbb{Z}_n, \times)$ não é um grupo

11) $(U(n), \times)$

$U(n)$ = conjunto dos elementos de $\mathbb{Z}_n$ que tem inverso módulo n.

$U(n) = \{\bar{a} \in \mathbb{Z}_n : MDC(\bar{a}, n) = 1\}$

$(U(n), \times)$ é um grupo.

Em particular, $(U(n), \times)$ é um grupo finito e é um grupo comutativo.

Este é o grupo com que vamos trabalhar

Vamos estudar como determinar a quantidade de elementos do conjunto $U(n)$ (ordem do grupo) em função do valor de n. $(n \geq 2)$

- FUNÇÃO ϕ (FI) DE EULER OU FUNÇÃO TOTIENTE

$\phi(n)$ = NÚMERO DE ELEMENTOS DO CONJUNTO $U(n)$

Então, quero exatamente calcular o valor de $\phi(n)$ em função de n.

EXEMPLOS: $U(5) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$\phi(5) = 4$

$U(10) = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$

$\phi(10) = 4$

$U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

$\phi(12) = 4$

$U(15) = \{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$

$\phi(15) = 8$

$U(18) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}\}$

$\phi(18) = 6$

Gostaria de um método sistemático para calcular $\phi(n)$

/ /

O caso mais simples é quando o módulo é um primo p.

$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

$MDC(a,p) = 1$ ou p

$U(p) = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

$U(p) = \mathbb{Z}_p - \{\bar{0}\}$

$\phi(p) = p-1$

Suponha agora que n é composto. Então n tem um fator $1 < f < n$ tal que $n = f \cdot n'$

↳ $MDC(f,n) = f > 1$

↓

$f \notin U(n)$

CONCLUSÃO: 1) $\phi(n) \leq n-1$ ($\bar{0}$ sempre fora)

2) $\phi(n) = n-1$ se e somente se n é primo.

Segundo caso para calcular $\phi(n)$:

$n = p^k$, $k \geq 1$

Para calcular $\phi(p^k)$ preciso determinar quantos números no intervalo $1 \leq a \leq p^k$ satisfazem $MDC(a,p^k) = 1$.

Qualquer que seja a, $MDC(a,p^k) = p^t$, $t \geq 0$.

Então,

$MDC(a, p^k) > 1 \iff p$ é fator de a.

$MDC(a, p^k) = 1 \iff p$ não é fator de a.

Logo, preciso determinar quantos números no intervalo $1 \leq a \leq p^k$ não são multiplos de p.

Mas ao invés de contar quantos números não são múltiplos de p, é muito mais fácil contar quantos são multiplos de p e subtrair do total.

TOTAL: p^k.

Vamos contar os números que são multiplos de p.

Se a é multiplo de p. Então $a = p \cdot a'$

$1 \leq a \leq p^k$

$1 \leq p \cdot a' \leq p^k$

$0 < p a' \leq p^k$

$0 < p a' \leq p^{k-1}$

Para cada valor de a' nesse intervalo, tenho um multiplo de p $a = p \cdot a'$, então tenho p^{k-1} múltiplos de p.

Subtraio então essa quantidade do total:

$p^k - p^{k-1} = p^{k-1}(p-1)$

$\phi(p^k) = p^{k-1}(p-1)$

Vamos agora tentar calcular $\phi(n)$ no caso geral.

TEOREMA: Se m e n são inteiros positivos tais que $MDC(m,n) = 1$, então

$$\phi(mn) = \phi(m) \cdot \phi(n)$$

Supondo o teorema verdadeiro, posso utilizá-lo para calcular $\phi(\ )$

Começo fatorando n:

$$n = p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$$

onde $p_1 < p_2 < p_3 < \dots < p_k$ e $a_i \geq 1$, para todo $1 \leq i \leq k$

$MDC(p_i^{ai}, p_j^{aj}) = 1$, se $i \neq j$, porque p_i e p_j são primos distintos.

Então, posso utilizar o teorema:

$$\phi(n) = \phi(p_1^{a1} p_2^{a2} \dots p_k^{ak}) =$$
$$= \phi(p_1^{a1}) \phi(p_2^{a2}) \dots \phi(p_k^{ak}) =$$

↳ TEOREMA

$$= p_1^{a1-1} p_2^{a2-1} \dots p_k^{ak-1} (p_1 - 1)(p_2 - 1) \dots (p_k - 1)$$

↳ FÓRMULA GERAL PARA O CÁLCULO DE $\phi(n)$

PROBLEMA: Para utilizar a formula, preciso conhecer a fatoração de n, o que pode ser muito complexo em alguns casos.

Entretanto, não se conhece nenhuma outra fórmula geral para o cálculo de $\phi(n)$ que não dependa da fatoração de n.

↳ Esse é um ponto importante para a segurança do RSA

/ /

Exemplos: 1) $n = 5$

2) $n = 10$

3) $n = 12$

4) $n = 15$

5) $n = 18$

1) $n = 5 \leftarrow$ PRIMO

$\phi(n) = n - 1 = 4$

2) $n = 10$

$n = 2 \cdot 5$

$\phi(10) = \phi(2) \cdot \phi(5) = 1 \cdot 4 = 4$

3) $n = 12$

$n = 2^2 \cdot 3$

$\phi(12) = \phi(2^2) \cdot \phi(3) = 2^{2-1} \cdot (2-1) \cdot (3-1) = 2 \cdot 1 \cdot 2 = 4$

4) $n = 15$

$n = 3 \cdot 5$

$\phi(15) = \phi(3) \cdot \phi(5) = (3-1)(5-1) = 2 \cdot 4 = 8$

5) $n = 18$

$n = 2 \cdot 3^2$

$\phi(18) = \phi(2) \cdot \phi(3^2) = (2-1) \cdot 3^{2-1} \cdot (3-1) = 1 \cdot 3 \cdot 2 = 6$