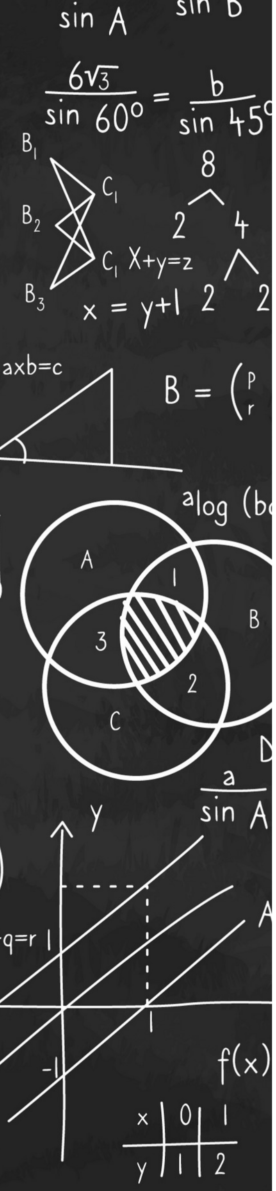

MATEMÁTICA DISCRETA 2

Aula 18
Ordem e Raízes Primitivas mod n
Função Tau; Função Sigma

Cristiane Loesch

Brasília
2025

Ordem modular de um inteiro

Definição: Sejam $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(m,n) = 1$ o menor número $e \in \mathbb{N}$ que satisfaz a relação:

$$m^e \equiv 1 \pmod{n}$$

é chamado de ordem de m módulo n, e denotado:

$$e = \operatorname{ord}_n(m)$$

Ordem modular de um inteiro

Definição: Sejam $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(m,n) = 1$ o menor número $e \in \mathbb{N}$ que satisfaz a relação:

$$m^e \equiv 1 \pmod{n}$$

é chamado de ordem de m módulo n, e denotado:

$$e = \mathrm{ord}_n(m)$$

EXEMPLO: Encontrar a ordem de:

a) 2 módulo 7

$$2^3 \equiv 1 \pmod{7}$$

$$\mathrm{ord}_7(2) = 3$$

Observe que:

$$2^j \not\equiv 1 \pmod{7}$$

$$j = 1, 2$$

Ordem modular de um inteiro

Definição: Sejam $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(m,n) = 1$ o menor número $e \in \mathbb{N}$ que satisfaz a relação:

$$m^e \equiv 1 \pmod{n}$$

é chamado de ordem de m módulo n, e denotado:

$$e = \mathrm{ord}_n(m)$$

EXEMPLO: Encontrar a ordem de:

a) 2 módulo 7 $\mathrm{ord}_7(2) = 3$

b) 2 módulo 11

c) 2 módulo 5

d) 9 móduloo 10

Ordem modular de um inteiro

Definição: Sejam $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(m, n) = 1$ o menor número $e \in \mathbb{N}$ que satisfaz a relação:

$$m^e \equiv 1 \pmod{n}$$

é chamado de ordem de m módulo n, e denotado:

$$e = \mathrm{ord}_n(m)$$

EXEMPLO: Encontrar a ordem de:

a) 2 módulo 7 $\mathrm{ord}_7(2) = 3$

b) 2 módulo 11 $\mathrm{ord}_{11}(2) = 10$

c) 2 módulo 5 $\mathrm{ord}_5 2 = 4$

d) 9 módulo 10 $\mathrm{ord}_{10} 9 = 2$

Exemplo (c) resolvido:

$$2^1 \equiv 2 \pmod{5}$$

$$2^2 \equiv 4 \equiv -1 \pmod{5}$$

$$2^3 \equiv -2 \pmod{5}$$

$$2^4 \equiv -4 \equiv 1 \pmod{5}$$

Ordem modular de um inteiro

Lema: Sejam m inteiro positivo e a inteiro tal que $mdc(a, m) = 1$. Seja $h = \text{ord}_m a$. Então, temos que:

$$a^k \equiv 1 \pmod{m} \Leftrightarrow h|k$$

- Parte 1: $a^k \equiv 1 \pmod{m} \Rightarrow h|k$.
  Suponhamos que não, isto é, que h não divide k. Pelo algoritmo da divisão, temos que existem interios q (quociente) e r (resto) tais que

  $$k = h \cdot q + r \quad 0 < r < h$$

  Daí, temos que:

  $$\begin{aligned} 1 \equiv a^k &\equiv a^{h \cdot q + r} \pmod{m} \\ &\equiv \left(a^h\right)^q \cdot a^r \pmod{m} \\ &\equiv 1^q \cdot a^r \pmod{m} \\ 1 &\equiv a^r \pmod{m} \end{aligned}$$

  Notemos que o resultado encontrado é absurdo, pois $r < h = \text{ord}_m a$

- Parte 2: $a^k \equiv 1 \pmod{m} \Leftarrow h|k$.
  Seja q inteiro positivo tal que $k = h \cdot q$. Daí, temos que:

  $$a^k \equiv \left(a^h\right)^q \equiv 1^q \equiv 1 \pmod{m}$$

  Daí, por exemplo, pelo teorema de Euler, podemos concluir que: $\text{ord}_m a \mid \varphi(m)$.

Fonte: Barbosa, A. (2024)

Ordem modular de um inteiro

Definição: Sejam $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $mdc(m,n) = 1$ o menor número $e \in \mathbb{N}$ que satisfaz a relação:

$$m^e \equiv 1 \pmod{n}$$

é chamado de ordem de m módulo n, e denotado:

$$e = \text{ord}_n(m)$$

Se $m \in \mathbb{Z}$, $n \in \mathbb{N}$ e $\text{ord}_n(m) = \varphi(n)$ tal m é denominado RAÍZ PRIMITIVA MÓDULO N

Raízes primitivas módulo n

*função totiente descrita à seguir

Definição: Seja $n \in \mathbb{Z}$ positivos e $g \in \mathbb{Z}$, diz-se que g é uma raíz primitiva módulo n se

$$mdc(g, n) = 1$$

e

$$\mathrm{ord}_n(g) = \varphi(n)$$

em que $\varphi(n)$ é a função totiente de Euler (vide slide extra).

Raízes primitivas módulo n

*função totiente descrita à seguir

EXEMPLOS:

Exemplo (c) anterior

$$2^1 \equiv 2 \pmod 5$$
$$2^2 \equiv 4 \equiv -1 \pmod 5$$
$$2^3 \equiv -2 \pmod 5$$
$$2^4 \equiv -4 \equiv 1 \pmod 5$$

$\longrightarrow \mathrm{ord}_5 2 = 4 \longrightarrow \phi(5)=5\cdot\left(1-\frac{1}{5}\right)=5\cdot\left(\frac{4}{5}\right)=4$

Logo, 2 é raíz primitiva módulo 5
e 4 é o número de coprimos de 5 menores do que ele

Exemplo (d) anterior

$$9^1 \equiv 9 (mod\,10)$$
$$9^2 \equiv 81 \equiv 1 (mod\,10)$$

$\longrightarrow \mathrm{ord}_{10} 9 = 2 \longrightarrow \phi(10)=10\cdot\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=10\cdot\left(\frac{1}{2}\right)\left(\frac{4}{5}\right)=4$

Logo, 9 não é raíz primitiva módulo 10
e 4 é o número de coprimos de 10 menores do que ele

Função Totiente de Euler (extra)

$\varphi(n)$ → conta a quantidade de números inteiros positivos menores ou iguais a n que são coprimos de n, ou seja, os números k tais que:

$$\mathrm{mdc}(k, n) = 1$$

* CASOS:

1) n =p e p é primo, então $\varphi(p) = p - 1$, , pois todos os números entre 1 e p-1 são coprimos com p

2) n é uma potência de um primo $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$

3) n pode ser fatorado em potências de primos

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

* A função totiente é uma função multiplicativa

$(\mathrm{mdc}(m, n) = 1)$,

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

Função Totiente de Euler (extra)

$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

EXEMPLOS (CHATGPT)

1. $n = 6$: A fatoração de 6 é $6 = 2 \cdot 3$. Assim:

$$\varphi(6) = 6\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 2$$

   Os números coprimos com 6 são 1 e 5.

2. $n = 12$: A fatoração de 12 é $12 = 2^2 \cdot 3$. Assim:

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$$

   Os números coprimos com 12 são $1, 5, 7,$ e 11.

3. $n = 15$: A fatoração de 15 é $15 = 3 \cdot 5$. Assim:

$$\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$$

   Os números coprimos com 15 são $1, 2, 4, 7, 8, 11, 13,$ e 14.

Raízes primitivas módulo n

Definição: Seja $n \in \mathbb{Z}$ positivos e $g \in \mathbb{Z}$ diz-se que g é uma raíz primitiva módulo n se

$$mdc(g, n) = 1$$

e

$$\text{ord}_n(g) = \varphi(n)$$

em que $\varphi(n)$ é a função totiente de Euler (vide slide extra).

Proposição 1:
Se $m \in \mathbb{Z}$, $d, n \in \mathbb{N}$ tal que $(m, n) = 1$, então $m^d \equiv 1 \pmod{n}$ se, e somente se, $\text{ord}_n(m)|d$.

Demonstração: Se $\text{ord}_n(m)|d$, então $d = \text{ord}_n(m)h$ para algum $h \in \mathbb{N}$, então

$$m^d \equiv \left(m^{\text{ord}_n(m)}\right)^h \equiv 1 \pmod{n}.$$

Por outro lado, se $m^d \equiv 1 \pmod{n}$, então $d \geq \text{ord}_n(m)$. Assim, existe q e r inteiros tal que $d = q \cdot \text{ord}_n(m) + r$ com $0 \leq r < \text{ord}_n(m)$. Logo, $1 \equiv m^d \equiv \left(m^{\text{ord}_n(m)}\right)^q m^r \equiv m^r \pmod{n}$. Como $r < \text{ord}_n(m)$ e a ordem é o menor número e tal que $m^e \equiv 1 \pmod{n}$, temos que $r = 0$. Em outras palavras, temos que $\text{ord}_n(m)|d$.

Fonte: Rispoli, V. (2024)

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

$$3^2 \equiv 9 \equiv 2 \bmod 7$$

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

$$3^2 \equiv 9 \equiv 2 \bmod 7$$

$$3^3 \equiv 27 \equiv 6 \bmod 7$$

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

$$3^2 \equiv 9 \equiv 2 \bmod 7$$

$$3^3 \equiv 27 \equiv 6 \bmod 7$$

$$3^4 \equiv 81 \equiv 4 \bmod 7$$

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

$$3^2 \equiv 9 \equiv 2 \bmod 7$$

$$3^3 \equiv 27 \equiv 6 \bmod 7$$

$$3^4 \equiv 81 \equiv 4 \bmod 7$$

$$3^5 \equiv 243 \equiv 5 \bmod 7$$

Raízes primitivas módulo n

EXEMPLO: o número 3 é raíz primitiva de 7

$$3^1 \equiv 3 \bmod 7$$

$$3^2 \equiv 9 \equiv 2 \bmod 7$$

$$3^3 \equiv 27 \equiv 6 \bmod 7$$

$$3^4 \equiv 81 \equiv 4 \bmod 7$$

$$3^5 \equiv 243 \equiv 5 \bmod 7$$

$$3^6 \equiv 729 \equiv 1 \bmod 7$$

Logo, 3 é raíz primitiva mod 7

* OBS: se continuarmos observaremos uma periodicidade nos restos a partir de k = 6

3, 2, 6, 4, 5, 1 foram todos os resíduos diferentes de 0 mod 7

Raízes primitivas módulo n

EXEMPLO: Determine a ordem de 3 mod 25 e verifique se 3 é raíz primitiva mod 25

$$\mathrm{ord}_n(g) = \varphi(n)$$

1) quem é $\varphi(25)$?

2) ordem encontrar k tal que $3^k \equiv 1 \pmod{25}$

Raízes primitivas módulo n

EXEMPLO: Determine a ordem de 3 mod 25 e verifique se 3 é raíz primitiva mod 25

$$\mathrm{ord}_n(g) = \varphi(n)$$

1) quem é $\varphi(25)$? $25 = 5^2$. $\longrightarrow \varphi(p^k) = p^k \cdot \left(1 - \frac{1}{p}\right) \longrightarrow \varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20 \longrightarrow \varphi(25) = 20$

$p = 5$

$k = 2$

2) ordem encontrar k tal que $3^k \equiv 1 \pmod{25}$

Raízes primitivas módulo n

EXEMPLO: Determine a ordem de 3 mod 25 e verifique se 3 é raíz primitiva mod 25

$$\mathrm{ord}_n(g) = \varphi(n)$$

1) quem é $\varphi(25)$? $25 = 5^2$. $\longrightarrow \varphi(p^k) = p^k \cdot \left(1 - \frac{1}{p}\right) \longrightarrow \varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20 \longrightarrow \varphi(25) = 20$

$p = 5$

$k = 2$

2) ordem encontrar k tal que $3^k \equiv 1 \pmod{25}$

Utilizar os divisores de 20, pois $k \in \{1, 2, 4, 5, 10, 20\}$

Raízes primitivas módulo n

EXEMPLO: Determine a ordem de 3 mod 25 e verifique se 3 é raíz primitiva mod 25

$$\mathrm{ord}_n(g) = \varphi(n)$$

1) quem é $\varphi(25)$? $25 = 5^2$. $\longrightarrow$ $\varphi(p^k) = p^k \cdot \left(1 - \frac{1}{p}\right)$ $\longrightarrow$ $\varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20$ $\longrightarrow$ $\varphi(25) = 20$

$p = 5$

$k = 2$

2) ordem encontrar k tal que $3^k \equiv 1 \pmod{25}$

Utilizar os divisores de 20, pois $k \in \{1, 2, 4, 5, 10, 20\}$

$$\begin{aligned}
3^1 &\equiv 3 \pmod{25} \\
3^2 &\equiv 9 \pmod{25} \\
3^4 &\equiv 6 \pmod{25} \\
3^5 &\equiv 18 \pmod{25} \\
3^{10} &\equiv 24 \pmod{25} \\
3^{20} &\equiv 1 \pmod{25},
\end{aligned}$$

Logo, 3 é raíz primitiva mod 25

Raízes primitivas módulo n

Corolários importantes:

1) Se $m \in \mathbb{Z}$, $d, n \in \mathbb{N}$ com $(m, n) = 1$ então $\operatorname{ord}_n(m^d) = \dfrac{\operatorname{ord}_n(m)}{(d, \operatorname{ord}_n(m))}$.

Exemplo: se $\operatorname{ord}_{25}(3) = 20$ e $(5, 20) = 5$ → $\operatorname{ord}_{25}(3^5) = \operatorname{ord}_{25}(3)/(5, 20) = 4$

2) Se $m \in \mathbb{Z}$, $d, n \in \mathbb{N}$ com $(m, n) = 1$ então $\operatorname{ord}_n(m^d) = \operatorname{ord}_n(m)$ se, e somente se, $(d, \operatorname{ord}_n(m)) = 1$.

Exemplo: $\operatorname{ord}_7(2) = 3$ → $\operatorname{ord}_7(2^2) = \operatorname{ord}_7(2) = 3$

Fonte: Rispoli, V. (2024)

Raízes primitivas módulo n

Teorema 1:

Se $m \in \mathbb{Z}$ e $n \in \mathbb{N}$ com $(m, n) = 1$. Se m é uma raiz primitiva módulo n, então $\{m^j\}_{j=1}^{\varphi(n)}$ é um sistema de reduzido de resíduos módulo n.

Demonstração: Precisamos mostrar que $(m^j, n) = 1$ e que $m^i \equiv m^j \pmod{n}$ se, e somente se, $i = j$. Como $(m, n) = 1$, então $(m^j, n) = 1$. Se $m^i \equiv m^j \pmod{n}$, então pelo Lema 1, isto acontece se, e somente se, $i \equiv j \pmod{\operatorname{ord}_n(m)}$. Entretanto, para $1 \leq i, j \leq \varphi(n)$, isto acontece se, e somente se, $i = j$.

EXEMPLO:

Vimos que 2 é raíz primitiva de 11, pelo teorema, o conjunto

$$\{2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\}$$

é um sistema reduzido de resíduos módulo 11.

Fonte: Rispoli, V. (2024)

Raízes primitivas módulo n

Teorema 2:
Se $n \in \mathbb{N}$ tem uma raiz primitiva, então ele tem $\varphi(\varphi(n))$ raízes primitivas incongruentes.

Demonstração: Seja m uma raiz primitiva módulo n. Pelo **Teorema 1**, outra raiz primitiva deve ser da forma m^e com $1 \leq e \leq \varphi(n)$. Mas, pelo **Corolário 3**, $\text{ord}_n(m) = \text{ord}_n(m^e)$ se, e somente se, $(e, \varphi(n)) = 1$, e existe exatamente $\varphi(\varphi(n))$ tais inteiros e.

EXEMPLO:
Vimos que 2 é raíz primitiva de 11, pelo teorema, então 11 possui exatamente $\varphi(\varphi(11)) = 4$ raízes primitivas

Fonte: Rispoli, V. (2024)

Raízes primitivas módulo n

EXEMPLO:

Suponha que queremos determinar todas as soluções da equação diofantina

$$3^a + 1 = 2^b$$

para inteiros não negativos a, b. Suponha que $a > 1$. Então $2^b \equiv 1 \pmod 9$. Entretanto, $\text{ord}_9(2) = 6$, assim $6|b$ pela **Proposição 1**. Portanto, existe um inteiro m tal que $b = 6m$. Além disso, pelo **Teorema de Fermat**,

$$2^b \equiv (2^6)^m \equiv 1 \pmod 7,$$

e consequentemente $7|(2^b - 1) = 3^a$, o que é uma contradição. Portanto, $a = 0, 1$ para $b = 1, 2$, respectivamente, são as únicas soluções.

Fonte: Rispoli, V. (2024)

Raízes primitivas módulo n

EXEMPLO:

Verificar LEMAS E EXEMPLOS em:

https://www.obm.org.br/content/uploads/2024/02/Nivel_2_Ordem_Armando_Barbosa_SO2024.pdf

Verificar tabela de raízes primitivas em:

https://pt.wikipedia.org/wiki/Raiz_primitiva_m%C3%B3dulo_n

Acesso em 18/01/2025

Funções Multiplicativas

Uma função aritmética (ou uma função da teoria dos números) denominada *f* é uma função multiplicativa se:

$$f(mn) = f(m)f(n)$$

sempre que *m* e *n* são relativamente primos.

As funções constante

$$f(n) = 1 \quad \text{pois} \quad f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$$

e identidade

$$g(n) = n^k \quad \text{pois} \quad g(mn) = (mn)^k = m^k n^k = g(m)g(n)$$

são funções multiplicativas.

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Multiplicativas

EXEMPLOS:

1. A função **tau** ($\tau(n)$), que conta o número de divisores de n, é multiplicativa.
2. A função **sigma** ($\sigma(n)$), que soma os divisores de n, também é multiplicativa.
3. A função **phi de Euler** ($\phi(n)$), que conta os números inteiros menores que n e coprimos a ele, é multiplicativa.

Aplicações:

→ criptogtrafia
→ algoritmos de fatoração
→ otimização de algoritmos
→ etc.

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

→ são usadas para descrever as propriedades dos divisores de números inteiros

Seja um número N inteiro positivo, tal número pode ser escrito como um produto de números primos (p_i, com ordem ascendente, p.ex., $p_1=2$, $p_2=3$, $p_3=5$, ...) elevado a uma certa potência inteiras (k_i, $k_i>1$)

$$N= p_1^{k1} \cdot p_2^{k2} \cdot p_3^{k3} \ldots$$

EXEMPLO: N = 16

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

→ são usadas para descrever as propriedades dos divisores de números inteiros

Seja um número N inteiro positivo, tal número pode ser escrito como um produto de números primos (p_i, com ordem ascendente, p.ex., $p_1=2$, $p_2=3$, $p_3=5$, ...) elevado a uma certa potência inteiras (k_i, $k_i>1$)

$$N= p_1^{k1} \cdot p_2^{k2} \cdot p_3^{k3} \dots$$

EXEMPLO: N = 16

divisores: 1, 2, 4, 8, 16

$N = 2^4$

Funções Tau e Sigma

FUNÇÃO TAU [τ(n)]

→ ou, função do número de divisores de N

→ conta quantos divisores positivos um inteiro N possui

$$\boxed{\tau(n)=(K_1+1)(K_2+1)(K_3+1)\ldots}$$

EXEMPLO:

a) N = 16

b) N = 72 000

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

FUNÇÃO TAU [τ(n)]

→ ou, função do número de divisores de N

→ conta quantos divisores positivos um inteiro N possui

$$\boxed{\tau(n)=(K_1+1)(K_2+1)(K_3+1)\ldots}$$

EXEMPLO:

a) N = 16

$\tau(16)= 4+1 =5$

b) N = 72 000

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

FUNÇÃO TAU [τ(n)]

→ ou, função do número de divisores de N

→ conta quantos divisores positivos um inteiro N possui

$$\boxed{\tau(n)=(K_1+1)(K_2+1)(K_3+1)\ldots}$$

EXEMPLO:

a) N = 16

$\tau(16)= 4+1 =5$

b) N = 72 000

$72\,000 = 2^5 \,.\, 3^2 \,.\, 5^3$ → $\tau(N)= (5+1)(2+1)(3+1) = 72$

Funções Tau e Sigma

FUNÇÃO SIGMA [σ(n)]

→ ou, função da soma dos divisores de N

→ calcula a soma dos divisores positivos um inteiro N possui

$$\boxed{\sigma(n) = \sum_{d|n} d}$$

EXEMPLO:

a) N = 16

b) N = 12

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

FUNÇÃO SIGMA [σ(n)]

→ ou, função da soma dos divisores de N

→ calcula a soma dos divisores positivos um inteiro N possui

$$\boxed{\sigma(n) = \sum_{d|n} d}$$

EXEMPLO:

a) N = 16

$\sigma(16) = 1+2+4+8+16=31$

b) N = 12

$\sigma(12) = 1+2+3+4+6+12=28$

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4)

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4)

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)
= f(1 . 1)+f(1 . 2)+f(1 . 3)+f(1 . 4)+f(2 . 3)+f(3 . 4) escrever como multiplicacao

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)
= f(1 . 1)+f(1 . 2)+f(1 . 3)+f(1 . 4)+f(2 . 3)+f(3 . 4)
= f(1)f(1)+f(1)f(2)+f(1)f(3)+f(1)f(4)+f(2)f(3)+f(3)f(4)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)
= f(1 . 1)+f(1 . 2)+f(1 . 3)+f(1 . 4)+f(2 . 3)+f(3 . 4)
= f(1)f(1)+f(1)f(2)+f(1)f(3)+f(1)f(4)+f(2)f(3)+f(3)f(4)
= f(1)[f(1)+f(2)+f(4)] + f(3)[f(1)+f(2)+f(4)]

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

F(12) = F(3 . 4) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)
= f(1 . 1)+f(1 . 2)+f(1 . 3)+f(1 . 4)+f(2 . 3)+f(3 . 4)
= f(1)f(1)+f(1)f(2)+f(1)f(3)+f(1)f(4)+f(2)f(3)+f(3)f(4)
= f(1)[f(1)+f(2)+f(4)] + f(3)[f(1)+f(2)+f(4)]
= [f(1)+f(3)][f(1)+f(2)+f(4)]

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

$$\boxed{F(n) = \sum_{d|n} f(d)}$$

Função multiplicativa

EXEMPLO:

a) F(12) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)

b) (TEOREMA) F (m . n) = F(m) . F(n)

$$\begin{aligned} F(12) = F(3 \,.\, 4) &= f(1)+f(2)+f(3)+f(4)+f(6)+f(12) \\ &= f(1 \,.\, 1)+f(1 \,.\, 2)+f(1 \,.\, 3)+f(1 \,.\, 4)+f(2 \,.\, 3)+f(3 \,.\, 4) \\ &= f(1)f(1)+f(1)f(2)+f(1)f(3)+f(1)f(4)+f(2)f(3)+f(3)f(4) \\ &= f(1)[f(1)+f(2)+f(4)] + f(3)[f(1)+f(2)+f(4)] \\ &= [f(1)+f(3)][f(1)+f(2)+f(4)]= F(3)F(4) \end{aligned}$$

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

Do Teorema que diz que se f é uma função multiplicativa então F(n) , também o será dado que

$$F(n) = \sum_{d|n} f(d)$$

e dos conceitos apresentados antes. Define-se que:

$$\boxed{\sum_{d|n} f(d) = \sum_{d|n} 1 = \tau(n) \qquad \sum_{d|n} g(d) = \sum_{d|n} d = \sigma(n)}$$

são funções multiplicativas, dado que se o mdc(m, n) =1

$$\tau(m\,.\,n) = \tau(m)\,\tau(n)$$
$$\sigma(m\,.\,n) = \sigma(m)\,\sigma(n)$$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

EXEMPLO: N=36

N=4 . 9

mdc(4,9)=1

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

EXEMPLO: N=36

N=4 . 9

mdc(4,9)=1

$$\tau(4 \,.\, 9) = \tau(4)\,\tau(9) = \tau(2^2)\,\tau(3^2) = (2+1)(2+1) = 3 \,.\, 3 = 9$$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

Funções Tau e Sigma são funções multiplicativas

EXEMPLO: N=36

N=4 . 9

mdc(4,9)=1

$\tau(4 \,.\, 9) = \tau(4)\,\tau(9) = \tau(2^2)\,\tau(3^2) = (2+1)(2+1) = 3\,.3 = 9$

$\sigma(4 \,.\, 9) = \sigma(4)\,\sigma(9) = (1+2+4)(1+3+9) = 91$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7
2^3	4	15

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7
2^3	4	15
2^4	5	31

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7
2^3	4	15
2^4	5	31
2^5	6	63
2^6	7	127
2^7	8	255

$$\sigma=2^{\tau}-1$$

$$N=2^{n}$$

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Observe que:

N	τ	σ
2^1	2	3
2^2	3	7
2^3	4	15
2^4	5	31
2^5	6	63
2^6	7	127
2^7	8	255

$\sigma=2^{\tau}-1$

$N=2^{n}$

N	τ	σ
3^1	2	4
3^2	3	13
3^3	4	40
3^4	5	121
3^5	6	364
3^6	7	1093
3^7	8	3280

$\sigma=3^{\tau}-1$

$N=3^{n}$

Figuras : University of Florida

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Assim, podemos dizer que:

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p^{\tau} - 1}{p - 1} \right)$$

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Assim, podemos dizer que:

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p^{\tau} - 1}{p - 1} \right)$$

EXEMPLO: N=16

$16 = 2^4$

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Assim, podemos dizer que:

$$\sigma(n)=\prod_{i=1}^{k}\left(\frac{p^{\tau}-1}{p-1}\right)$$

EXEMPLO: N=16

$16 = 2^4$

$\tau(16)= 4+1 =5$

$\sigma(N) = (2^{4+1}-1)/(2-1)$
$= (2^5-1)/1$
$= 32-1$
$=31$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Assim, podemos dizer que:

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p^{\tau} - 1}{p - 1} \right)$$

EXEMPLO: N=16

$16 = 2^4$

$\tau(16) = 4+1 = 5$

$\sigma(N) = (2^{4+1}-1)/(2-1)$
$= (2^5-1)/1$
$= 32-1$
$=31$

N	τ	σ
2^1	2	3
2^2	3	7
2^3	4	15
2^4	5	31

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

Assim, podemos dizer que:

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p^{\tau} - 1}{p - 1} \right)$$

EXEMPLO: N=16

$16 = 2^4$

$\tau(16) = 4+1 = 5$

$$\begin{aligned}\sigma(N) &= (2^{4+1}-1)/(2-1) \\ &= (2^5-1)/1 \\ &= 32-1 \\ &= 31\end{aligned}$$

IDEIA: Se estivéssemos numa situação fictícia e quiséssemos saber de quantas formas diferentes podemos dividir 16 crianças a função tau nos daria esta informação, teríamos 5 maneiras diferentes de dividir tais crianças (em arranjos de 1, 2, 4, 8, ou 16 crianças). Agora, se se quiséssemos formar todos os tipos de arranjo possíveis teríamos com a função sigma o número necessário de crianças para satisfazê-lo (28).

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p^{\tau} - 1}{p - 1} \right)$$

EXEMPLO: N=12

$12 = 2^2 . 3$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

$$\sigma(n)=\prod_{i=1}^{k}\left(\frac{p^{\tau}-1}{p-1}\right)$$

EXEMPLO: N=12

$12 = 2^2 \, . \, 3$

$\sigma(N) = [(2^{2+1}-1)/(2-1)] \, . \, [(3^{1+1}-1)/(3-1)]$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

$$\sigma(n)=\prod_{i=1}^{k}\left(\frac{p^{\tau}-1}{p-1}\right)$$

EXEMPLO: N=12

$12 = 2^2 . 3$

$\sigma(N) = [(2^{2+1}-1)/(2-1)] . [(3^{1+1}-1)/(3-1)]$
$= [(2^3-1)/(1)] . [(3^2-1)/(2)]$
$= [7] . [8/2]$
$= 7 . 4$
$= 28$

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

$$\sigma(n)=\prod_{i=1}^{k}\left(\frac{p^{\tau}-1}{p-1}\right)$$

EXEMPLO: N=13

$13 = 13^1$

σ(N) = [(13^{1+1}-1)/(13-1)]
= [(13^2-1)/(12)]
= (169-1)/12
= 168/12
= 14 → ressaltando que 13 tem apenas 2 divisores, ele menos e 1

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)

Funções Tau e Sigma

EXEMPLO:
Aplicação simples em computação → Criptografia de Chave Pública.

As funções tau e sigma podem ser utilizadas na identificação de vulnerabilidades entre os números definidos para a chave. No caso da criptografia RSA, por exemplo, a chave pública é definida por

$$N = p \cdot q$$

em que p e q são números primos.
Um número n com muitos divisores, $\tau(n)$, ou uma soma alta de divisores, $\sigma(n)$, pode ser um candidato fraco para criptografia, pois pode ter fatores p e q menores ou mais previsíveis e seus divisores tornam n mais suscetível a ataques baseados em fatoração.

Antes de usar um número n como chave pública em RSA, um sistema pode calcular $\tau(n)$ e $\sigma(n)$ para garantir que n não seja um número altamente composto ou com propriedades que o tornem fácil de fatorar.

Funções Tau e Sigma

EXEMPLO:
Aplicação simples em computação → Criptografia de Chave Pública.

Considerando este exemplo pedi ao ChatGPT que criasse uma situação para ilustrar:

Número Menos Robusto ($n = 77$):

- $p = 7, q = 11$
- $n = 7 \cdot 11 = 77$
- $\tau(77) = 4$ (Divisores: $1, 7, 11, 77$)
- $\sigma(77) = 1 + 7 + 11 + 77 = 96$

Número Mais Robusto ($n = 143$):

- $p = 11, q = 13$
- $n = 11 \cdot 13 = 143$
- $\tau(143) = 4$ (Divisores: $1, 11, 13, 143$)
- $\sigma(143) = 1 + 11 + 13 + 143 = 168$

Escolha Ainda Mais Segura ($n = 209$):

- $p = 11, q = 19$
- $n = 11 \cdot 19 = 209$
- $\tau(209) = 4$ (Divisores: $1, 11, 19, 209$)
- $\sigma(209) = 1 + 11 + 19 + 209 = 240$

Funções Tau e Sigma

EXEMPLO:
Aplicação simples em computação → Criptografia de Chave Pública.

```
def divisores(n):
    return [i for i in range(1, n + 1) if n % i == 0]

def tau(n):
    return len(divisores(n))

def sigma(n):
    return sum(divisores(n))
```

```
def verificar_seguranca(n):
    if tau(n) > 10 or sigma(n) > 100:  # Critérios hipotéticos
        return f"{n} é fraco para RSA."
    else:
        return f"{n} é seguro para RSA."

# Exemplos
print(verificar_seguranca(15))  # Fraco: fatores pequenos
print(verificar_seguranca(77))  # Potencialmente seguro
```

Funções Tau e Sigma

A conexão entre as funções Tau e Sigma

$$\sigma(n)=\prod_{i=1}^{k}\left(\frac{p^{\tau}-1}{p-1}\right)$$

Ideia – extra:
Se estivéssemos numa situação fictícia e quiséssemos saber de quantas formas diferentes podemos dividir 16 crianças a função tau nos daria esta informação, teríamos 5 maneiras diferentes de dividir tais crianças (em arranjos de 1, 2, 4, 8, ou 16 crianças). Agora, se se quiséssemos formar todos os tipos de arranjo possíveis teríamos com a função sigma o número necessário de crianças para satisfazê-lo (28).

As discussões e os teoremas, assim como outros exemplos desta parte do conteúdo podem ser encontrados no capítulo 8 de Koshy, T. (2007)