(/ /)

UFRJ · Universidade Federal do Rio de Janeiro

Rio de Janeiro, 18 de Março de 2017

·CRITÉRIOS DE DIVISIBILIDADE

DIVISIBILIDADE POR 3: "Um número é divisível por 3 se e somente se a soma dos seus algarismos é divisível por 3".

DIVISIBILIDADE POR 9: "Um número é divisível por 9 se e somente se a soma dos seus algarismos é divisível por 9."

Por quê?

Seja n um inteiro e $n_0, n_1, n_2, \ldots, n_k$ são os algarismos de n (na base 10)

$$n = n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \ldots + n_2 \cdot 10^2 + n_1 \cdot 10 + n_0$$

Vamos considerar n módulo 3.

$$n = n_k \cdot \cancel{10^k}^{1} + n_{k-1} \cdot \cancel{10^{k-1}}^{1} + \ldots + n_2 \cdot \cancel{10^2}^{1} + n_1 \cdot \cancel{10}^{1} + n_0 \equiv \underbrace{n_k + n_{k-1} + \ldots + n_2 + n_1 + n_0}_{\text{SOMA DOS ALGARISMOS}} \pmod 3$$

$10 \equiv 1 \pmod 3$

$10^2 = 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod 3$

$10^t \equiv 1 \pmod 3$, para todo $t \geq 0$

n é divisível por 3

$\Updownarrow$

$n \equiv 0 \pmod 3$

$\Updownarrow$

$n_k + n_{k-1} + \ldots + n_2 + n_1 + n_0 \equiv 0 \pmod 3 \iff$ A soma dos algarismos é divisível por 3.

tilibra

- MÓDULO 9:

$10 \equiv 1 \pmod 9$

$10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \equiv 1 \pmod 9$

$10^t \equiv 1 \pmod 9$, para todo $t \geq 0$

$$n = n_k \cdot \cancel{10^k}^{1} + n_{k-1} \cdot \cancel{10^{k-1}}^{1} + \dots + n_2 \cdot \cancel{10^2}^{1} + n_1 \cdot \cancel{10}^{1} + n_0 \equiv \underbrace{n_k + n_{k-1} + \dots + n_2 + n_1 + n_0}_{\text{SOMA DOS ALGARISMOS}} \pmod 9$$

- MÓDULO 11:

$10 \equiv -1 \pmod{11}$

$10^2 \equiv 10 \cdot 10 \equiv (-1)(-1) \equiv 1 \pmod{11}$

$10^3 \equiv 10 \cdot 10 \cdot 10 \equiv (-1) \cdot (-1) \cdot (-1) \equiv -1 \pmod{11}$

$\vdots$

$$10^t \begin{cases} -1, & \text{se } t \text{ é ímpar} \\ 1, & \text{se } t \text{ é par} \end{cases} \pmod{11}$$

$10^t \equiv (-1)^t \pmod{11}$

$$n \equiv n_k \cdot 10_k + n_{k-1} \cdot 10_{k-1} + \dots + n_2 \cdot \cancel{10^2}^{1} + n_1 \cdot \cancel{10}^{-1} + n_0 \equiv \underbrace{n_0 - n_1 + n_2 - n_3 + n_4 - n_5 + \dots}_{\text{SOMA ALTERNADA DOS ALGARISMOS}} \pmod{11}$$

EXEMPLO: 1232

$2 - 3 + 2 - 1 = 0$ -> SOMA ALTERNADA DOS ALGARISMOS

LOGO, 1232 É DIVISÍVEL POR 11.

• DIVISÃO MODULAR

Vamos pensar inicialmente na divisão entre dois números reais a e b. Dividir a por b $\left(\frac{a}{b}\right)$ é equivalente a multiplicar a pelo inverso multiplicativo de b (normalmente é denotado por b^{-1})

↳ $a \times b^{-1} = a \times \left(\frac{1}{b}\right)$

O inverso multiplicativo de b é o número b^{-1} tal que

$$b \times b^{-1} = 1$$

↳ ELEMENTO NEUTRO DA MULTIPLICAÇÃO

Logo, só é possível dividir a por b se b possuir um inverso multiplicativo. No caso dos reais, todo número diferente de zero tem inverso multiplicativo. Em outros conjuntos, esta restrição pode ser relevante.

Seja um inteiro $n \geq 2$. Vamos considerar o conjunto $\mathbb{Z}_n$

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

↳ INTEIROS MÓDULO N

Para podermos fazer divisões em $\mathbb{Z}_n$, precisamos determinar quais elementos $\bar{a} \in \mathbb{Z}_n$ têm inverso multiplicativo.

O inverso multiplicativo de um elemento $\bar{a}$ em $\mathbb{Z}_n$ é um elemento $\overline{a'}$ tal que

$$\bar{a} \cdot \overline{a'} = \bar{1} \text{ em } \mathbb{Z}_n$$

$$\Updownarrow$$

$$a \cdot a' \equiv 1 \pmod{n}$$

- TEOREMA DA INVERSÃO: As seguintes afirmações são equivalentes:

(1) MDC $(a, n) = 1$
(2) $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$
(3) Existe um inteiro $k > 0$ tal que $a^k \equiv 1 \pmod{n}$

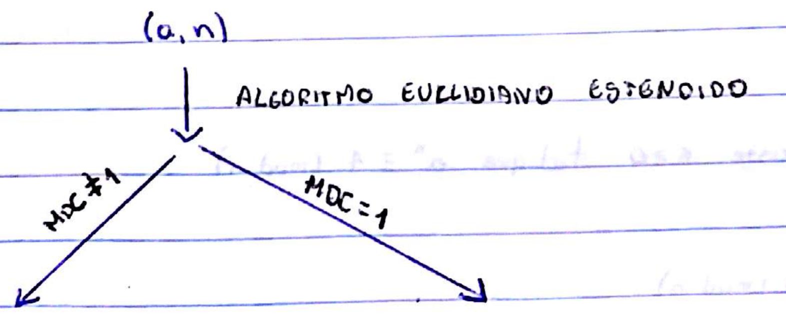
(1) $\Rightarrow$ (2)

Suponha que MDC $(a,n) = 1$. Pelo Algoritmo Euclidiano Estendido, existem α e β tais que

$$\alpha \cdot a + \beta \cdot n = 1$$
$$\alpha \cdot a - 1 = \beta \cdot n$$
$$\Downarrow$$
$$\alpha \cdot a - 1 \text{ é multiplo de } n$$
$$\Updownarrow$$
$$\alpha \cdot a \equiv 1 \pmod{n}$$

α é o INVERSO MULTIPLICATIVO DE a MÓDULO n.

Para determinar se o inverso multiplicativo de a modulo n existe e quem ele é, podemos usar o Algoritmo Euclidiano Estendido



a não tem inverso multiplicativo módulo n

a tem inverso multiplicativo módulo n e α é este inverso.

(2) => (1)

Suponha que $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$. Então, existe a' tal que $a \cdot a' \equiv 1 \pmod{n}$, seja $d = MDC(a,n)$. Quero mostrar que $d = 1$.

Se d é divisor de a e n, então:

$a = d \cdot k$

$n = d \cdot l$

$a a' \equiv 1 \pmod{n}$

$\Updownarrow$

$\underbrace{a}_{dk} a' - 1 = \underbrace{n}_{dl} t$

$dka' - 1 = dlt$

$dka' - dlt = 1$

$d(ka' - lt) = 1$

$\Downarrow$

d divide 1

$\Downarrow$

$d = 1$

(3) => (2)

Suponha que existe $k > 0$ tal que $a^k \equiv 1 \pmod{n}$

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

$\Downarrow$

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

↳ INVERSO MULTIPLICATIVO DE a MÓDULO N.

$(2) \Rightarrow (3)$

Suponha que $\bar{a}$ tem inverso multiplicativo em $\mathbb{Z}_n$. Suponha por contradição, que ($a^k \not\equiv 1 \pmod{n}$ para todo $k > 0$.) $(*)$

$$\left.\begin{array}{l} a^1 \not\equiv 1 \\ a^2 \not\equiv 1 \\ a^3 \not\equiv 1 \\ \vdots \end{array}\right\}$$ Infinitas potências mas finitos resultados possíveis. (to do resultado está em $\mathbb{Z}_n$).

↳ CONJUNTO FINITO

Logo, existem t e u $(t > u)$ tais que

$$a^t \equiv a^u \pmod{n}$$

Seja a' o inverso de a em $\mathbb{Z}_n$

$$a^t \equiv a^u \pmod{n}$$
$$a^t \cdot (a'^u) \equiv a^u \cdot (a'^u) \pmod{n}$$
$$a^t \cdot (a')^u \equiv 1 \pmod{n}$$
$$a^{t-u} \cdot a^u \cdot (a')^u \equiv 1 \pmod{n}$$
$$a^{t-u} \equiv 1 \pmod{n}$$

$t - u > 0$

Seja $m = t - u$

($a^m \equiv 1 \pmod{n}$) $(**)$

$(1) \Longleftrightarrow (2)$
$\Downarrow$
(3)

$(*) + (**) \Rightarrow$ CONTRADIÇÃO

Exemplos de Cálculo de Inverso Multiplicativo:

Inverso de $\bar{2}$ em $\mathbb{Z}_5$

R	q	α	β
2	-	1	0
5	-	0	1
2	0	1	0
1	2	-2	1
0	2	-	-

MDC

Inverso

Forma reduzida: $-2 \equiv 3 \pmod{5}$

3 é o inverso de $\bar{2}$ módulo 5.

Inverso de $\bar{5}$ em $\mathbb{Z}_{40}$

R	Q	α	β
5	-	1	0
40	-	0	1
5	0	1	0
0	8	-	-

$\bar{5}$ não tem inverso multiplicativo em $\mathbb{Z}_{40}$

INVERSO DE $\overline{3}$ EM $\mathbb{Z}_{104}$

R	Q	α	β
3	-	1	0
104	-	0	1
3	0	1	0
2	34	-34	1
1	1	35	-1
0	2	-	-

MDC INVERSO

DEFINIÇÃO: $U(n)$ = conjunto dos elementos de $\mathbb{Z}_n$ que possuem inverso multiplicativo

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

Seja p primo. $\mathbb{Z}_p = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$

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

DEFINIÇÃO: Definimos a ordem de um elemento $\bar{a} \in \mathbb{Z}_n$ como sendo o menor inteiro positivo k tal que $a^k \equiv 1 \pmod{n}$

Como vimos no teorema da inversão (item 3), nem todos os elementos de $\mathbb{Z}_n$ possuem ordem. Apenas possuem ordem os elementos $\bar{a} \in \mathbb{Z}_n$ tais que $MDC(a, n) = 1$.

LEMA-CHAVE: $a^t \equiv 1 \pmod{n}$ se e somente se a ordem de a divide t.

($\Leftarrow$) Seja k a ordem de a. Suponha que k divide t. Então $t = k \cdot t'$

$a^t \equiv a^{kt'} \equiv \underset{\underset{1}{\equiv}}{(a^k)}^{t'} \equiv 1^{t'} \equiv 1 \pmod{n} \rightarrow a^t \equiv 1 \pmod{n}$

(⇓) Suponha que $a^t \equiv 1 \pmod{n}$. Seja K a ordem de a. Vamos dividir t por K.

$t = K \cdot q + r \qquad 0 \leq r < K$

q ↳ QUOCIENTE

r ↳ RESTO

$$1 \equiv a^t \equiv a^{Kq+r} \equiv a^{Kq} \cdot a^r \equiv \underbrace{(a^K)^q}_{\equiv 1} \cdot a^r \equiv a^r$$

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

$$\left.\begin{array}{l} a^r \equiv 1 \\ 0 \leq r < K \\ K \text{ é a ordem de } a \end{array}\right\} \; r = 0$$

$\downarrow$

K divide t.