

Função de Euler $\varphi(n)$. 2

Proposição [da aula passada].

Seja n um inteiro positivo. Então:

$$\sum_{d|n} \varphi(d) = n,$$

Com somatório sobre todos divisores positivos ^{de n .}

Prova Seja $C(n) = \{1, \dots, n\}$

$$S_d = \{a \in C(n) \mid \text{mdc}(n, a) = d\}.$$

Claro que, se $d \nmid a$, assim $\text{mdc}(n, a) \neq d$
 assim $S_d = \emptyset$.

Por outro lado $C(n)$ = união de todos S_d sobre divisores positivos de n .

Alem disso:

$$a \in S_d \Leftrightarrow 1 \leq a \leq n, \text{ e } \text{mdc}(a, n) = d$$

$$\Leftrightarrow 1 \leq a \leq n, \text{ e } \text{mdc}\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

$$\Leftrightarrow a = a'd, \text{ com } 1 \leq a' \leq \frac{n}{d} \text{ e } \text{mdc}\left(a', \frac{n}{d}\right) = 1.$$

Logo $\# S_d = \varphi\left(\frac{n}{d}\right)$. Como $c(n) = \sum_{d|n} S_d$, (2)

$$\begin{aligned} \text{então } n = \# c(n) &= \sum_{d|n} \# S_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \varphi(n). \quad \square \end{aligned}$$

Exemplo. $n=20$. Divisores positivos são:

1, 2, 4, 5, 10, 20:

$$\varphi(1)=1, \varphi(2)=1, \varphi(4)=2, \varphi(5)=4, \varphi(10)=4, \varphi(20)=8$$

$$\begin{aligned} \Rightarrow \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) &= \\ &= 1 + 1 + 2 + 4 + 4 + 8 = 20 // \end{aligned}$$

Exemplo 2 $n=34$. Divisores positivos são:

1, 2, 17, 34.

$$\varphi(1)=1, \varphi(2)=1, \varphi(17)=16, \varphi(34)=\varphi(2) \cdot \varphi(17)=16$$

$$\varphi(1) + \varphi(2) + \varphi(17) + \varphi(34) =$$

$$= 1 + 1 + 16 + 16 = 34 //$$

Exemplo 3 $n=60$.

divisores: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

$$\begin{aligned} \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(12) + \\ + \varphi(15) + \varphi(20) + \varphi(30) + \varphi(60) &= 1 + 1 + 2 + 2 + 4 + 2 + \\ &+ 4 + 4 + 8 + 8 + 16 = 60 // \end{aligned}$$

Inteiros modulo m

3

Lembrete: Se $m > 0$ e a, b inteiros positivos
assim $a \equiv b \pmod{m}$, se $m \mid a - b$

Se $m \in \mathbb{Z}$, $m > 1$, para todo $a \in \mathbb{Z}$, define

$$\bar{a} := \{ b \in \mathbb{Z} \mid b \equiv a \pmod{m} \}.$$

Exemplo a) $m = 2$, $a = 1$, assim

$b \equiv 1 \pmod{2} \Leftrightarrow b$ é ímpar, logo

$$\bar{a} = \bar{1} = \{ \dots, -3, -1, 1, 3, 5, 7, \dots \}$$

b) Se $m = 2$, $a = 4$, assim

$b \equiv 4 \pmod{2} \Leftrightarrow b$ é par, logo

$$\bar{4} = \{ \dots, -4, -2, 0, 2, 4, 6, 8, \dots \}$$

Observe que se $m = 2$, assim:

$$\bar{4} = \bar{2} = \bar{0}$$

Exemplo c) $m = 7$, $a = 11$, assim

$$\bar{a} = \{ \dots, -10, -3, 4, 11, 18, 25, 32, \dots \}$$

Proposição Seja $m \in \mathbb{Z}, m > 1$, Assim

(4)

$$\bar{a} = \{a + km \mid k \in \mathbb{Z}\}$$

"S"

Prova:

Lembrete:

Dois conjuntos X, Y são iguais $\Leftrightarrow X \subset Y$ e $Y \subset X$

" $\subset$ " Seja $b \in \bar{a} \Rightarrow b \equiv a \pmod{m}$
 $\Rightarrow m \mid b-a \Rightarrow m \cdot k = b-a$
 $\Rightarrow b = a + mk \Rightarrow b \in S.$

" $\supset$ " Se $b \in S \Rightarrow b = a + m \cdot k, k \in \mathbb{Z}$
 $\Rightarrow m \mid b-a$
 $\Rightarrow b \equiv a \pmod{m} \Rightarrow b \in \bar{a}.$

Assim $\bar{a} = S \quad \square.$

Proposição 2 Temos que

$$\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$$

Prova " $\Rightarrow$ " Seja $c \in \bar{a}$, assim $c \in \bar{b}$ e

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{m} \end{cases} \Rightarrow a \equiv b \pmod{m}$$

[4] Temos que

(5)

$$\begin{aligned} c \in \bar{a} \Leftrightarrow c \equiv a \pmod{m} &\Leftrightarrow c \equiv b \pmod{m} \\ a \equiv b \pmod{m} &\Leftrightarrow c \in \bar{b} \end{aligned}$$

Assim $\bar{a} = \bar{b}$ $\square$

Corolário Seja $a \in \mathbb{Z}$ e $m > 1$. Se $a, b \in \mathbb{Z}$ com $\bar{a} \neq \bar{b}$, então $\bar{a} \cap \bar{b} = \emptyset$

Prova

Suponha que $\bar{a} \cap \bar{b} \neq \emptyset$, e $c \in \bar{a}, c \in \bar{b}$

$$\begin{aligned} \text{Assim } \begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{m} \end{cases} &\Rightarrow a \equiv b \pmod{m} \\ &\Rightarrow \bar{a} = \bar{b} \quad \square. \end{aligned}$$

Def. Dado $a \in \mathbb{Z}$ e $m > 1$. $\bar{a}$ é chamado representante de a modulo m .

Exemplo: Suponha $m=3$, assim há 3 representantes

$$\bar{0} = \{ \dots, -9, -6, -3, 0, 3, 6, 9, 12, 15, \dots \}$$

$$\bar{1} = \{ -8, -5, -2, 1, 4, 7, 10, 13, 16, \dots \}$$

$$\bar{2} = \{ -7, -4, -1, 2, 5, 8, 11, 14, 17, \dots \}$$

E, em particular

⑥

$$\overline{0} = \overline{6}, \quad \overline{0} = \overline{12}, \dots$$

$$\overline{1} = \overline{4}, \quad \overline{1} = \overline{7}, \dots$$

$$\overline{2} = \overline{23}, \quad \overline{2} = \overline{-1}, \dots$$

Observe que $\overline{0} \cup \overline{1} \cup \overline{2} = \mathbb{Z}$ - todos inteiros.

Definimos o conjunto dos inteiros

módulo m , como conjunto de todas
classes de congruência diferentes.

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\}, \text{ as vezes}$$

escrevemos como $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.

Exemplos

$$\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$$

$$\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$$

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

$\vdots$

$$\mathbb{Z}_{13} = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{12}\}$$

$\vdots$

(7)

Exemplo Qual é inteiro menor positivo b tal que $\overline{b} = \overline{-21}$ modulo $m=8$.

Solução O resto da divisão de -21 por 8 é 3, pois

$$-21 = (-3) \cdot 8 + 3$$

Assim $\overline{3} = \overline{-21}$.

Operações em $\mathbb{Z}_m$

Vamos ver que $\mathbb{Z}_m$ é bem parecido ao $\mathbb{Z}$ introduzindo operações de soma e produto em $\mathbb{Z}_m$.

Soma: $\overline{a} + \overline{b} := \overline{a+b}$

Produto: $\overline{a} \cdot \overline{b} := \overline{ab}$.

Vamos mostrar que as operações são bem-definidas ou seja não dependem de representantes escolhidas.

Isto é dados a, b, a', b' em $\mathbb{Z}$

Com $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$, vamos verificar
que $\overline{a+b} = \overline{a'+b'}$ e $\overline{ab} = \overline{a'b'}$

Prova Temos:

$$\begin{array}{lcl} \bar{a} = \bar{a'} & \stackrel{\text{Prop 2}}{\iff} & a \equiv a' \pmod{m} \\ \bar{b} = \bar{b'} & \stackrel{\text{Prop 2}}{\iff} & b \equiv b' \pmod{m} \end{array}$$

$$\text{Assim temos que } a+b \equiv a'+b' \pmod{m} \\ ab \equiv a'b' \pmod{m}$$

De novo, aplicando Prop. 2, temos

$$\overline{a+b} = \overline{a'+b'} \text{ e } \overline{ab} = \overline{a'b'} \quad \square$$

Isso significa que soma

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$$

$$(\bar{a}, \bar{b}) \longmapsto \bar{a} + \bar{b} := \overline{a+b}$$

e o produto:

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m$$

$$(\bar{a}, \bar{b}) \longmapsto \bar{a} \cdot \bar{b} := \overline{ab}$$

operações bem definidas.

Exemplo.

$$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}, \text{ neste caso}$$

$$\bar{0} = \{\dots, -4, -2, 0, 2, 4, \dots\} - \text{pares}$$

$$\bar{1} = \{\dots, -5, -3, -1, 1, 3, 5, 7, \dots\} - \text{ímpares}$$

Soma entre dois inteiros pares é par

assim $\Rightarrow \bar{0} + \bar{0} = \bar{0}$

Semelhante soma de dois inteiros ímpares

e par $\Rightarrow \bar{1} + \bar{1} = \bar{0}$

Semelhante $\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$. Temos

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Exercício (p/ casa).

- 1) Encontre $\overline{-81}$ em $\mathbb{Z}_{17}$
- 2) Descreva soma e produto em $\mathbb{Z}_3$ e $\mathbb{Z}_7$
- 3) Calcule $\overline{-17} \cdot \overline{21}$ em $\mathbb{Z}_{13}$
 $\overline{101} \cdot \overline{33}$ em $\mathbb{Z}_6$ e $\mathbb{Z}_8$.