Aula 15.05.2020

Função de Euler $\varphi(n)$

Lembrete: Como calcular $\varphi(n)$?

Regra 1: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, p - um primo.

Regra 2: $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$, se

$$mdc(n, m) = 1.$$

Assim, pelo T. Fundamental da Aritmetica

$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $p_1, \ldots, p_k$ - primos distintos

$\alpha_1, \ldots, \alpha_k$ - potencias

Assim:

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) \overset{\text{Regra 2}}{=} \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$$

$$\overset{\text{Regra 1}}{=} (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdot \ldots \cdot (p_k^{\alpha_k} - p_k^{\alpha_k - 1}).$$

Exemplos a) $n = 760 = 2^3 \cdot 5 \cdot 19$

$$\Rightarrow \varphi(760) = \varphi(2^3 \cdot 5 \cdot 19)$$

$$= \varphi(2^3) \cdot \varphi(5) \cdot \varphi(19)$$

$$\Rightarrow (2^3 - 2^2) \cdot (5-1) \cdot (19-1)$$

$$= 4 \cdot 4 \cdot 18$$

b) $n = 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$,

2310	2
1155	3
385	5
77	7
11	11

$$\Rightarrow \varphi(n) = \varphi(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11)$$
$$= \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \cdot \varphi(7) \cdot \varphi(11)$$
$$= 1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 = 480$$

A gente já mostrou que **Regra 1** vale

Vamos mostrar **Regra 2:**

$$\varphi(n \cdot m) = \varphi(n)\varphi(m), \text{ se } mdc(n,m) = 1$$

<u>Prova</u>. Define: $C(n) = \{1, 2, \dots, n\}$

$$R(n) = \{a \in C(n) \mid mdc(a,n) = 1\}$$

Assim $\# R(n) = \varphi(n)$

Vamos definir função:

$$f: R(n \cdot m) \longrightarrow R(n) \times R(m)$$

Se $t \in R(n \cdot m)$, assim $mdc(t, n \cdot m) = 1$

Existem $a_1 \in C(n)$, $a_2 \in C(m)$ tal que

$t \equiv a_1 \pmod{n}$ 1, $t \equiv a_2 \pmod{m}$ 2.

<u>Lembrete:</u> Se $mdc(m,n) = 1$, assim

$$mdc(a, n \cdot m) = 1 \iff \begin{cases} mdc(a,n) = 1 \\ mdc(a,m) = 1 \end{cases}$$

Assim

$$mdc(t, n\cdot m) = 1 \Rightarrow \begin{matrix} mdc(t,n) = 1 \\ mdc(t,m) = 1. \end{matrix}$$

Por outro lado:

$$x \equiv y \pmod n \Rightarrow mdc(x,n) = mdc(y,n)$$

Assim:

(1) $\Rightarrow$ $mdc(t,n) = 1 = mdc(a_1, n) \Rightarrow a_1 \in R(n)$

(2) $\Rightarrow$ $mdc(t,m) = 1 = mdc(a_2, n) \Rightarrow a_2 \in R(m)$

Agora defina $f(t) = (a_1, a_2) \in R(n) \times R(m)$.

$\boxed{\text{Objetivo:}}$ Vamos mostrar que f é bijetora isto é injetora e sobrejetora.

$\boxed{\text{Sobrejetora:}}$ Sejam $b_1 \in R(n)$, $b_2 \in R(m)$

Encontramos $t \in R(n\cdot m)$, com $f(t) = (b_1, b_2)$.

O sistema $\begin{cases} x \equiv b_1 \pmod n \\ x \equiv b_2 \pmod m \end{cases}$ (*) tem único

solução pelo Teorema Chinês de Resto, modulo $n.m$. Se s é solução do (*), assim existe único $t \in C(n\cdot m)$ com $t \equiv s \pmod{n\cdot m}$

$$\begin{cases} t \equiv b_1 \pmod n \\ mdc(b_1, n) = 1 \end{cases} \Rightarrow mdc(t,n) = 1$$

Analogamente

$$\begin{cases} t \equiv b_2 \pmod{m} \\ mdc(b_2, m) = 1 \end{cases} \Rightarrow mdc(t, m) = 1$$

Assim $mdc(t, n\cdot m) = 1$, ou seja $t \in R(n\cdot m)$.

$\Rightarrow$ f é sobrejetora.

Injetora: Segue pelo unicidade de t acima.

$\Rightarrow$ f é injetora + sobrejetora

$\Rightarrow$ f é bijetora, assim

$$\begin{array}{ccccc} \#R(n\cdot m) & = & \#R(n) & \cdot & \#R(m) \\ \| & & \| & & \| \end{array}$$

$$\boxed{\varphi(n\cdot m) = \varphi(n)\cdot\varphi(m)}$$

$\square$

Exemplo Mostre que $\varphi(2n) = \varphi(n)$ se e só se n é impar.

Solução. Se $\varphi(2n) = \varphi(n)$, assim escreva

$$n = 2^a \cdot m, \text{ com } mdc(2, m) = 1$$

$$\varphi(n) = \varphi(2^a\cdot m) = (2^a - 2^{a-1})\cdot\varphi(m)$$

$$\|\qquad\qquad\qquad\qquad\qquad\qquad\|$$

$$\varphi(2n) = \varphi(2^{a+1}\cdot m) = (2^{a+1} - 2^a)\cdot\varphi(m)$$

$\Rightarrow a = 0$ e n é impar.

Por outro lado, se n é ímpar, assim $mdc(2,n)=1$ e

$$\varphi(2\cdot n) = \varphi(2)\cdot\varphi(n) = \varphi(n).$$

<u>Exemplo 2</u> Como função f na prova foi construído, com $n=4$ e $m=5$.

Neste caso:

$$R(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

$$R(4) = \{1, 3\}, \quad R(5) = \{1, 2, 3, 4\}$$

$$R(4)\times R(5) = \{(1,1), (1,2), (1,3), (1,4), (3,1), (3,2), (3,3), (3,4)\}.$$

$$f : R(20) \longrightarrow R(4)\times R(5)$$

$$\begin{aligned}
1 &\longmapsto (1,1) & 11 &\longmapsto (3,1)\\
3 &\longmapsto (3,3) & 13 &\longmapsto (1,3)\\
7 &\longmapsto (3,2) & 17 &\longmapsto (1,2)\\
9 &\longmapsto (1,4) & 19 &\longmapsto (3,4)
\end{aligned}$$

e claramente f é bijetora.

$\boxed{\text{Obs:}}$ Se $n = p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$, assim:

$$\varphi(n) = \varphi(p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1})\cdot\ldots\cdot(p_s^{k_s} - p_s^{k_s-1})$$

$$(*) \quad = \underbrace{p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}}_{\shortparallel} \left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right)$$

$$= n\cdot\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_s}\right).$$

Exemplo 3 $n = 360 = 2^3 \cdot 3^2 \cdot 5$

$$\varphi(360) \overset{(*)}{=} 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right)$$

$$= 360 \cdot \frac{1}{\cancel{2}} \cdot \frac{\cancel{2}}{3} \cdot \frac{4}{5} = 96$$

Exemplo 4 Encontre todos n tal que

$$\varphi(n) = \frac{n}{2}$$

Solução Aplicando (*) temos

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) = \frac{n}{2}$$

$$\Rightarrow \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) = \frac{1}{2}$$

$$\Rightarrow \underbrace{2\,(p_1 - 1) \cdot \ldots \cdot (p_s - 1)}_{\text{par}} = p_1 \cdot \ldots \cdot p_k$$

$\Rightarrow$ $p_1 = 2$, assim [cancelando p_1 e 2], temos

$$\underbrace{(p_2 - 1) \cdot \ldots \cdot (p_s - 1)}_{\text{par}} = \underbrace{p_2 \cdot \ldots \cdot p_k}_{\text{impar}}$$

$\Rightarrow$ $n = 2^k$ - única solução.

Exemplo 5 Encontre todos n tais que

$$\varphi(n) = 12.$$

Solução

Seja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, assim

$$\varphi(n) = p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_s - 1)$$

Assim $p_1^{\alpha_1 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \cdot (p_1 - 1) \cdot \ldots \cdot (p_s - 1) = 2^2 \cdot 3$

Assim $p_1 = 3$, e $\alpha_1 = 2$, temos

$$\cancel{3^{2-1}} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \cdot \cancel{(3-1)} \cdot \ldots \cdot (p_s - 1) = 2^{\cancel{2}} \cdot \cancel{3}$$

$$\Rightarrow \quad p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_s^{\alpha_s - 1} \cdot (p_2 - 1) \cdot \ldots \cdot (p_s - 1) = 2$$

$\Rightarrow \quad p_2 = 2$, e $\alpha_2 = 2$, ou seja

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} = 3^2 \cdot 2^2 = 36.$$

De fato $\varphi(36) = \varphi(9) \cdot \varphi(4) = 6 \cdot 2 = 12$ //.

———— // ———— // ————

Considere $n = 10$, os divisores de 10 são: 1, 2, 5, 10. Temos:

$\varphi(1) = 1$

$\varphi(2) = 1$ $\quad \Rightarrow$

$\varphi(5) = 4$

$\varphi(10) = \varphi(2) \cdot \varphi(5) = 4$

$$\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4 = 10.$$

Ou se $n = 18$, assim divisores são:

$1, 2, 3, 6, 9, 18.$

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(6) = 2$ $\Rightarrow$ $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(6) + \varphi(18) = 18$ //

$\varphi(9) = 6$

$\varphi(18) = 6$

Na aula que vem mostremos que

Proposisão Seja n um inteiro positivo.

Assim: $\sum_{d \mid n} \varphi(d) = n$

Com somatorio sobre todos divisores positivos de n.

//

Exercicio (p/ casa).

1) Encontre n tal que $\varphi(n) = 10$, $\varphi(n) = 4$.

2) Mostre que $\varphi(n)$ é par, se $n > 2$.

3) Calcule $\varphi(2500)$, $\varphi(81.000)$, resto da div de 3^{1000} por 2500.

4) Encontre todos n tal que $\varphi(3n) = 2\varphi(n)$.