Aula 18. Função de Euler

18.1 Como calcular $\varphi(n)$?

Na aula passada vimos as seguinte regras quais ajudam calcular os valores da função $\varphi(n)$.

Regra 1:

$$\varphi\left(p^{\alpha}\right) = p^{\alpha} - p^{\alpha-1}$$

se p é um primo. **Regra 2**:

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

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

Sabendo essas regras, temo como calcular $\varphi(n)$ para qualquer valor n, na seguinte maneira. Pelo Teorema fundamendal da Aritmetica, temos que qualquer inteiro positivo n pode ser escrito como

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

onde $p_1, \ldots, p_k$ são primos distintos e $\alpha_1, \ldots, \alpha_k$ inteiros positivos. Assim

$$\varphi(n) = \varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) \overset{Regra2}{=} \varphi(p_1^{\alpha_1}) \cdot \ldots \varphi(p_k^{\alpha_k}) \overset{Regra1}{=} \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right)$$

Ou seja

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k-1}\right)$$

Exemplo 18.1

Suponha que $n = 90$. Assim $90 = 2 \cdot 3^2 \cdot 5$. Temos

$$\varphi(90) = \varphi(2 \cdot 3^2 \cdot 5) \overset{Regra2}{=} \varphi(2) \cdot \varphi(3^2) \cdot \varphi(5) \overset{Regra1}{=} 1 \cdot (3^2 - 3) \cdot 4 = 24.$$

Exemplo 18.2

Suponha que $n = 760$. Assim $760 = 2^3 \cdot 5 \cdot 19$. Temos

$$\varphi(760) = \varphi(2^3 \cdot 5 \cdot 19) \overset{Regra2}{=} \varphi(2^3) \cdot \varphi(5) \cdot \varphi(19) \overset{Regra1}{=} (2^3 - 2^2) \cdot 4 \cdot 18 = 144.$$

18.2 *Prova da Regra 1*

Seja $n = p^\alpha$ com p um primo e $\alpha \geqslant 1$. Escrevendo todos inteiros entre 1 e p^α, temos:

$$\begin{array}{cccc} 1 & 2 & \dots & \cancel{p} \\ p+1 & p+2 & \dots & \cancel{2p} \\ 2p+1 & 2p+2 & \dots & \cancel{3p} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \cancel{p^{\alpha-1}p} \end{array}$$

Observem que

$$\begin{aligned} \text{mdc}(p, p^\alpha) &= p, \\ \text{mdc}(2p, p^\alpha) &= p, \\ &\dots \\ \text{mdc}(p^{\alpha-1}p, p^\alpha) &= p, \end{aligned}$$

assim esses elementos devemos excluir. No total a tabela tem p^α elementos. Assim no total tem exatamente $p^\alpha - p^{\alpha-1}$ elementos a nessa tabela com $\text{mdc}(a, p^\alpha) = 1$, ou seja

$$\varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1}.$$

Para ilustrar o fato vamos ver os seguintes exemplos faceis.

Exemplo 18.3

Suponha que $p = 2$, $\alpha = 3$. Neste caso temos a seguinte tabela.

$$\begin{array}{cc} 1 & \cancel{2} \\ 3 & \cancel{4} \\ 5 & \cancel{6} \\ 7 & \cancel{8} \end{array}$$

Assim, temos $\varphi\left(2^3\right) = 2^3 - 2^2 = 4$.

Exemplo 18.4

Suponha que $p = 3$, $\alpha = 2$. Neste caso temos a seguinte tabela.

$$\begin{array}{ccc} 1 & 2 & \cancel{3} \\ 4 & 5 & \cancel{6} \\ 7 & 8 & \cancel{9} \end{array}$$

Assim, temos $\varphi\left(3^2\right) = 3^2 - 3 = 6$.

18.3 Prova da Regra 2

Vamos mostrar Regra 2

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

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

Define os seguintes conjuntos:

$$C(n) = \{1, 2, \ldots, n\}$$
$$R(n) = \{a \in C(u) \mid \text{mdc}(a, n) = 1\}$$

Observem que

$$R(n) = \varphi(n),$$

para todo n. Assim vamos definir função:

$$f : R(n \cdot m) \to R(n) \times R(m).$$

Observem que para todo $t \in R(n \cdot m)$ temos que $\text{mdc}(t, n \cdot m) = 1$. Reduzindo t modulo n e m temos que existem $a \in C(n)$ e $b \in C(m)$ tais que

$$t \equiv a (\text{mod}\, n), \qquad t \equiv b (\text{mod}\, m),$$

Agora lembrando que se $\text{mdc}(n, m) = 1$ assim

$$\text{mdc}(a, n \cdot m) = 1 \iff \begin{array}{l} \text{mdc}(a, n) = 1, \\ \text{mdc}(a, m) = 1. \end{array}$$

Pos outro lado:

$$x \equiv y (\text{mod}\, n) \implies \text{mdc}(x, u) = \text{mdc}(y, 4)$$

Assim, temos que $\text{mdc}(a, n) = 1$ ou seja $a \in R(n)$ e $\text{mdc}(b, m) = 1$ ou seja $b \in R(m)$. Portanto temos que

$$t \mapsto (a, b)$$

de fato define a função

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

Vamos mostrar que f é bijetora, ou seja f é injetora (i.e. se $f(t) = f(t')$ assim $t = t'$) e é sobrejetora (i.e. para todo $(a, b) \in R(n) \times R(m)$ existe $t \in R(n \cdot m)$ com $f(t) = (a, b)$).

Sobrejetora: Suponha que $(a, b) \in R(n) \times R(m)$. O sistema

$$\begin{cases} x \equiv a (\text{mod}\, n) \\ x \equiv b (\text{mod}\, m) \end{cases}$$

tem uma unica solução modulo $n \cdot m$, pelo Teorema Chinés de Resto. Se s é solução do sistema acima, assim existe unico $t \in C(u \cdot m)$ com $t \equiv s (\text{mod}\, n \cdot m)$. Agora,

$$\begin{bmatrix} t \equiv a (\text{mod}\, n) \\ \text{mdc}\,(a, n) = 1 \end{bmatrix} \implies \text{mdc}(t, m) = 1$$

Analogamente

$$\begin{bmatrix} t \equiv b(\mathrm{mod}\, m) \\ \mathrm{mdc}\,(b,m) = 1 \end{bmatrix} \qquad \Longrightarrow \qquad \mathrm{mdc}(t,n) = 1$$

Assim $\mathrm{mdc}(t, n \cdot m) = 1$, ou seja $t \in R(n \cdot m)$. Portanto f é sobrejetora.

Injetora: Segue pelo unicidade de t acima.

Como f é injetora e sobrejetora assim f é bijetora, portanto

$$\#R(n \cdot m) = \#R(n) \cdot \#R(m)$$

Mas

$$\begin{aligned} \varphi(n \cdot m) &= \#R(n \cdot m), \\ \varphi(n) &= \#R(n), \\ \varphi(m) &= \#R(m), \end{aligned}$$

Portanto

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

Exemplo 18.5

amos ilustrar como função f foi construida num exemplo quando $n = 4$ e $m = 5$. Neste caso:

$$\begin{aligned} R(20) &= \{1,3,7,9,11,13,17,19\}, \\ R(4) = \{1,3\}, R(5) &= \{1,2,3,4\}, \\ R(4) \times R(5) &= \{(1,1),(1,2),(1,3),(1,4)(3,1),(3,2),(3,3),(3,4)\} \end{aligned}$$

Agora a função $f : R(20) \to R(4) \times R(5)$ é

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

Que é obviamente bijetora. Ou seja

$$\varphi(4 \cdot 5) = \varphi(4) \cdot \varphi(5).$$

18.4 Exemplos

Exemplo 18.6

Vamos mostrar que

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

se e somente se n é impar.
Suponha que $\varphi(2n) = \varphi(n)$, assim escrevemos n com $2^a m$ com $\text{mdc}(2, m) = 1$. Temos

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

Assim $\varphi(2n) = \varphi(n)$ apenas possivel quando $a = 0$, ou seja n é impar.
Por outro lado se n é impar, assim $\text{mdc}(2, n) = 1$, logo

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

Observação 18.1

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

$$\begin{aligned}\varphi(n) &= \varphi\left(p_1^{k_1} \cdot \ldots p_s^{r_s}\right) = \left(p_1^{k_1} - p_1^{k_1-1}\right) \cdot \ldots \cdot \left(p_s^{k_s} - p_s^{t_s-1}\right) \\ &= \underbrace{p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}}_{n} \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right) \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right).\end{aligned}$$

Exemplo 18.7

Suponha que $n = 360$ assim $n = 2^3 \cdot 3^2 \cdot 5$. Aplicando Observação acima temos

$$\begin{aligned}\varphi(360) &= 360 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \\ &= 360 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 96\end{aligned}$$

Exemplo 18.8

Vamos encontrar todos n tal gue

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

Aplicando observação acima, temos

$$\begin{aligned}
&\varphi(u) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \left(1 - \frac{1}{p_s}\right) = \frac{1}{2} \\
&\Rightarrow \left(1 - \frac{1}{p_1}\right) \cdot \ldots \left(1 - \frac{1}{p_s}\right) = \frac{1}{2} \\
&\Rightarrow \quad 2\,(p_1 - 1) \cdot \ldots (p_s - 1) = p_1 \cdot \cdots \cdot p_k
\end{aligned}$$

Lado esquerdo da ultima igualdade é par, assim $p_1 = 2$. Cancelando 2 de dois lados recebemos

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

Assim $n = p^k$ é única solução.

18.5 *Mais uma propriedade*

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

$$\begin{aligned}
\varphi(1) &= 1, \\
\varphi(2) &= 1, \\
\varphi(5) &= 4, \\
\varphi(10) &= \varphi(2) \cdot \varphi(5) = 4,
\end{aligned}$$

e

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

Se $n = 18$, os divisores positivos de 18 são: $1, 2, 3, 6, 9, 18$. Temos:

$$\begin{aligned}
\varphi(1) &= 1, \\
\varphi(2) &= 1, \\
\varphi(3) &= 2, \\
\varphi(6) &= \varphi(2) \cdot \varphi(3) = 2, \\
\varphi(9) &= 6, \\
\varphi(18) &= \varphi(2) \cdot \varphi(9) = 6.
\end{aligned}$$

e

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(9) + \varphi(18) = 1 + 1 + 2 + 2 + 6 + 6 = 18 = n.$$

Proposição 18.1

Seja n um inteiro positivo. Então:

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

com somatório sobre todos divisores positivos de n

Prova

Seja

$$C(n) = \{1, \ldots, n\}.$$

Definamos também

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

Claro que, se $d \nmid a$, assim $\text{mdc}(n, a) \neq d$, logo $S_d =$. Por outro lado $C(n)$ é união de todos S_d sobre divisores positivos de n. Temos:

$$\begin{aligned} a \in S_d &\Leftrightarrow 1 \leqslant a \leqslant n, \text{ e } \text{mdc}(a, n) = d \\ &\Leftrightarrow 1 \leqslant a \leqslant n, \text{ e } \quad \text{mdc}\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \\ &\Leftrightarrow a = a'd, \text{com } 1 \leqslant a' \leqslant \frac{n}{d}, \text{ e } \text{mdc}\left(a', \frac{n}{d}\right) = 1. \end{aligned}$$

Logo $\#S_d = \varphi\left(\frac{n}{d}\right)$. Assim

$$n = \#C(n) = \sum_{d|n} \#S_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d).$$

Exercício 18.1: (Trabalho p/ casa)

Encontre todos n tal que
a) $\varphi(n) = 10$
b) $\varphi(n) = 4$
Resposta: a) 11, 22
Resposta: b) 5, 8, 10, 12

Exercício 18.2: (Trabalho p/ casa)

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

Exercício 18.3: (Trabalho p/ casa)

Calcule $\varphi(2500), \varphi(81.000)$,
Resposta: 1000, 21600

Exercício 18.4: (Trabalho p/ casa)

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