TEOREMA DE EULER

A função φ de Euler

DEF: Seja $m > 0$. Considere o conjunto

$$A = \{x \mid 0 \leq x < m \mid \text{mdc}(x, m) = 1\}.$$

Então $\varphi(m) \overset{\text{def}}{=} |A|$ = número de elementos do conjunto A.

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}$$

$$\varphi(m) = |A|$$

Exemplos

(1) $\varphi(10) = |\{x \mid 1 \leq x < 10 \mid \text{mdc}(x, 10) = 1\}| = |\{1, 3, 7, 9\}| = 4$

(2) $\varphi(12) = |\{1, 5, 7, 11\}| = 4$

(3) $\varphi(27) = |\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}| = 18$

(4) Se p é um número primo, então $\varphi(p) = p - 1$.

$$\varphi(p) = |\{1, 2, 3, \ldots, p-1\}| = p - 1.$$

Proposição 5: Se p é um número primo, $p>0$ então $\varphi(p^k) = (p-1)p^{k-1}$ para todo $k \geq 1$.

Demonstração: Queremos determinar o número de elementos de $A = \{x \in \mathbb{Z},\ 1 \leq x < p^k \mid mdc(x, p^k) = 1\}$.

Note que $mdc(x, p^k) \neq 1 \iff p \mid x$.

Assim $A = \underbrace{\{1, 2, \ldots, p^k\}}_{p^k \text{ elementos}} - \underbrace{\{1 \leq x < p^k \mid p \mid x\}}_{\text{múltiplos de } p}$.

Quantos são os múltiplos de p entre 1 e p^k?

$p, 2p, 3p, \ldots, (p-1)p$
$p^2, 2p^2, 3p^2, \ldots, (p-1)p^2$
$\ldots\ldots\ldots\ldots$
$p^{k-1}, 2p^{k-1}, \ldots\ldots, (p-1)p^{k-1}$

} múltiplos de $p < p^k$. São p^{k-1} números

Logo $|A| = \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

Logo $\varphi(p^k) = p^{k-1}(p-1)$. ∎

Para podermos calcular $\varphi(n)$ para todo inteiro n, precisamos mostrar que a função φ é multiplicativa, isto é, mostrar que se $\text{mdc}(a,b)=1$ então $\varphi(ab)=\varphi(a)\varphi(b)$.

Lembrar:

SISTEMA COMPLETO DE RESÍDUOS MÓDULO m

$S=\{a_1, a_2, \ldots, a_m\}$ é um sistema completo de resíduos módulo m se:

(1) Para todo $a \in \mathbb{Z}$ existe $a_i \in S$ tal que $a \equiv a_i \pmod m$.

(2) Se $i \neq j$ então $a_i \not\equiv a_j \pmod m$.

$\Leftrightarrow$

Para todo $a \in \mathbb{Z}$ existe um único i, $1 \leq i \leq m$ tal que $a \equiv a_i \pmod m$.

OBSERVAÇÃO: Se $a_1, \ldots, a_m$ são m inteiros não congruentes dois a dois módulo m então $S=\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos módulo m.

Seja $a \in \mathbb{Z}$. Pelo Algoritmo da Divisão, existem

$q, r \in \mathbb{Z}$ tais que $a = qm + r$.
$0 \leq r < m$

$$a \equiv r \pmod{m} \quad (1)$$

Para cada $a_i \in S$, $\exists\, q_i, r_i$, $0 \leq r_i < m$ tais que

$$a_i = q_i m + r_i .$$

É claro que se os elementos de S são dois a dois não congruentes módulo m, então, se $i \neq j$, $r_i \neq r_j$. Assim

$$\{r_1, r_2, \ldots, r_m\} = \{0, 1, \ldots, m-1\}$$

Logo se $a \equiv r \pmod{m}$ e $0 \leq r < m$, então $r = r_i$, para algum $i = 1, \ldots, m$.

$\Rightarrow a \equiv a_i \pmod{m}$. É claro que a_i é único.

TEOREMA: Se $\text{mdc}(a, m) = 1$ então $\varphi(ab) = \varphi(a)\varphi(b)$.

(A função fi de Euler é multiplicativa.)

Demonstração:

Temos o seguinte resultado:

$$\text{mdc}(x, ab) = 1 \iff \text{mdc}(x, a) = \text{mdc}(x, b) = 1.$$

$A = \{ x \in \mathbb{Z},\ 1 \leq x \leq ab \mid \text{mdc}(x, ab) = 1 \}$ (Por def: $|A| = \varphi(ab)$)

Queremos mostrar que $|A| = \varphi(a)\varphi(b)$.

Para isso, vamos "contar" os elementos de A.

Disponha os elementos de 1 até ab assim:

1	2	3	...	k	...	(b−1)	b
b+1	b+2	b+3	...	b+k	...	b+(b−1)	2b
2b+1	2b+2	2b+3	...	2b+k	...	2b+(b−1)	3b
⋮	⋮	⋮		⋮		⋮	⋮
(a−1)b+1	(a−1)b+2	(a−1)b+3	...	(a−1)b+k	...	(a−1)b+(b−1)	ab

$ab - 1$

Cada linha contém $\varphi(b)$ elementos x com $\text{mdc}(x, b) = 1$.

Se $\text{mdc}(k, b) = 1$ então todos os elementos da k-ésima coluna têm a mesma propriedade.

Temos $\varphi(b)$ colunas com essa propriedade.

Cada coluna $\{k, b+k, \dots, (a-1)b+k\}$ tem a elementos.

Esses elementos são dois a dois não congruentes módulo a:

Sejam i e j com $0 \leq j, i \leq a-1$.

Se $ib + k \equiv jb + k \pmod{a} \Rightarrow$

$a \mid ib - jb \Rightarrow a \mid (i-j)b \Rightarrow a \mid (i-j)$.

$\text{mdc}(a, b) = 1$

Se $i - j \neq 0$, então $0 < |i-j| < a$ e então $a \nmid (i-j)$.

Logo $i - j = 0 \Rightarrow i = j$.

Logo $\{k, b+k, \dots, (a-1)b+k\}$ é um sistema completo de resíduos módulo a.

Nesse conjunto temos $\varphi(a)$ elementos primos com a.

Assim $|A| = \varphi(a)\varphi(b)$, como queríamos. ∎

Seja $n \in \mathbb{Z}$, $n > 1$. Pelo TFA existem $p_1, \dots, p_k$ primos, $p_1 < p_2 < \dots < p_k$ tais que $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Então

$$\varphi(n) = \varphi(p_1^{r_1})\,\varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k})$$

$$= (p_1-1)\,p_1^{r_1-1}\,(p_2-1)\,p_2^{r_2-1} \cdots (p_k-1)\,p_k^{r_k-1}$$

$$= (p_1-1)(p_2-1)\cdots(p_k-1)\,p_1^{r_1-1}\,p_2^{r_2-1}\cdots p_k^{r_k-1}$$

Exemplos

(1) $\varphi(300) = \varphi(2^2 \times 3 \times 5^2) = (2-1)(3-1)(5-1)\times 2 \times 5 = 8 \times 2 \times 5 = 16 \times 5 = 80.$

(2) Determine todos os inteiros positivos m tais que

$\varphi(m) = 12$, $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$

$$\varphi(m) = (p_1-1)\cdots(p_k-1)\,p_1^{r_1-1}\cdots p_k^{r_k-1}, \quad p_1 < \cdots < p_k$$

$p_k - 1 \mid 12 \Rightarrow$

$p_k \leq 13.$

Os primos que podem aparecer na decomposição de m são $2, 3, 5, 7, 11, 13$

Se o 13 aparecer só podemos ter $m = 13$ e $m = 26$.

Suponha então que $m = 2^{x_1} 3^{x_2} 7^{x_3}$.

Como $\varphi(7) = 6$, $0 \leq x_3 \leq 1$ e $\varphi(2^{x_1} 3^{x_2}) = 2$, se $x_3 = 1$

Temos que $\varphi(2^2) = 2$, $\varphi(3) = 2$ e $\varphi(2 \times 3) = 2$

Os números são 21, 42, 28.

Se $x_3 = 0$, $m = 2^{x_1} 3^{x_2}$

$\varphi(m) = 2^{x_1 - 1} \cdot 2\, 3^{x_2 - 1} \Rightarrow 2^{x_1} 3^{x_2 - 1} = 2^2 \cdot 3 \Rightarrow x_1 = 2$ e $x_2 = 2$

$\Rightarrow m = 24$.

Os números são:

13, 26, 21, 42, 28, 24

Seja $A = \{ i \mid 0 \leq i \leq m-1 \text{ com } \text{mdc}(i, m) = 1 \}$ e seja a tal que $\text{mdc}(a, m) = 1$.

Seja $B = \{ ai \mid i \in A \}$. É claro que $\text{mdc}(ai, m) = 1$ para todo $i \in A$.

Dado $j \in A$ existe um único $i \in A$ tal que

$$ai \equiv j \pmod{m}.$$

(A congruência $aX \equiv j \pmod{m}$ tem solução, pois $\text{mdc}(a, m) = 1 \mid j$ e suas soluções são todas congruentes mod m.
Logo existe um único i, com $0 \leq i \leq m-1$ tal que
$ai \equiv j \pmod{m}$. É claro que $\text{mdc}(i, m) = 1$, pois $\text{mdc}(j, m) = 1$
$\Rightarrow \text{mdc}(ai, m) = 1 \Rightarrow \text{mdc}(i, m) = 1$.).

É claro que se $i \in A$, $ai \equiv j$, $0 \leq j \leq m-1$ e $\text{mdc}(j, m) = 1$.

Vamos agora provar o Teorema de Euler.

TEOREMA (Euler) Se $\text{mdc}(a, m) = 1$ então $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Demonstração:

Para cada $i \in A$, $ai \equiv j \pmod{m}$, $j \in A$ único.

Então $\prod_{i \in A} a.i \equiv \prod_{j \in A} j \pmod{m}$.

$$a^{\varphi(m)} \prod_{i \in A} i \equiv \prod_{j \in A} j \pmod{m}$$

$$a^{\varphi(m)} x \equiv x \pmod{m}$$

Mas $\text{mdc}(x, m) = 1$ pois $x = \prod_{i \in A} i$ e $\text{mdc}(i, m) = 1$

Logo $a^{\varphi(m)} \equiv 1 \pmod{m}$, como queríamos. ∎