6 - Teoremas de Fermat/Euler

Teorema de Fermat

Teorema de Fermat - Seja $a \in \mathbb{Z}$ e p um primo tal que $p \nmid a$. Então:

$$a^{p-1} \equiv_p 1$$

Corolário : p primo $\Rightarrow$ $a^p \equiv_p a$ $\forall a \in \mathbb{Z}$

Exemplo : Queremos calcular o resto da divisão de 5^{42} por 11.

Como 11 é primo e $11 \nmid 5$, pelo T. Fermat, $5^{10} \equiv_{11} 1$ e portanto

$$5^{42} = (5^{10})^4 \times 5^2 \equiv_{11} 1^4 \times 5^2 = 25 \equiv_{11} 3$$

Teorema de Fermat - Demonstração

Demonstração: Consideremos os seguintes $p-1$ múltiplos de a:

$$a, 2a, 3a \cdots , (p-1)a$$

Como p é primo e $p \nmid a$ então p não divide nenhum destes múltiplos de a.
Por outro lado, todos estes múltiplos dão restos distintos quando divididos por p, pois se tivessemos $k_1 a \equiv_p k_2 a$, com $k_1 > k_2$, teríamos $(k_1 - k_2)a \equiv_p 0$, ou seja teríamos $p \mid (k_1 - k_2)a$. Logo,

$$a \times 2a \times 3a \times \cdots \times (p-1)a \equiv_p 1 \times 2 \times 3 \times \cdots \times (p-1)$$

ou seja $\quad a^{p-1}(p-1)! \equiv_p (p-1)!$

Como $(p-1)!$ é primo com p, temos que $\quad a^{p-1} \equiv_p 1$

Função de Euler

Para cada $n \in \mathbb{N}$, representa-se por $\phi(n)$ o número de inteiros positivos, menores ou iguais a n, que são primos com n. A função $\phi : \mathbb{N} \to \mathbb{N}$, assim definida, diz-se a função de Euler .

Exemplos :

$n = 6 \quad 1, 2, 3, 4, 5, 6 \quad$ logo $\quad \phi(6) = 2$

$n = 9 \quad 1, 2, 3, 4, 5, 6, 7, 8, 9 \quad$ logo $\quad \phi(9) = 6$

$n = 7 \quad 1, 2, 3, 4, 5, 6, 7 \quad$ logo $\quad \phi(7) = 6$

Função de Euler - propriedades

A função de Euler tem as seguintes propriedades:

1. p primo $\Rightarrow$ $\phi(p) = p - 1$
2. p primo e $\alpha \in \mathbb{N}$ $\Rightarrow$ $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$
3. $n, m \in \mathbb{N}$ e m.d.c.$(n, m) = 1$ $\Rightarrow$ $\phi(nm) = \phi(n)\phi(m)$
4. Se $n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \cdots\ p_k^{\alpha_k}$ é a decomposição em primos de n:

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})\ (p_2^{\alpha_2} - p_2^{\alpha_2-1})\ \cdots\ (p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

Exemplo : Como $180 = 2^2 \times 3^2 \times 5$ temos que:

$$\phi(180) = \phi(2^2)\ \phi(3^2)\ \phi(5) = (2^2 - 2^1)\ (3^2 - 3^1)\ (5 - 1) = 2 \times 6 \times 4 = 48$$

Teorema de Euler

Teorema de Euler - Seja $a \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que m.d.c.$(n, a) = 1$. Então:

$$a^{\phi(n)} \equiv_n 1$$

Nota : Se n for primo $\phi(n) = n - 1$ e obtemos $a^{n-1} \equiv_n 1$. Ou seja, nesse caso obtemos o Teorema de Fermat.

Exemplo : Queremos calcular o resto da divisão de 5^{44} por 14.

Como 14 é primo com 5, pelo T. Euler , $5^{\phi(14)} \equiv_{14} 1$. Como $14 = 2 \times 7$ temos que $\phi(14) = \phi(2)\phi(7) = (2-1)(7-1) = 1 \times 6 = 6$ e portanto

$$5^{44} = (5^6)^7 \times 5^2 \equiv_{14} 1^7 \times 5^2 = 25 \equiv_{14} 11$$

Teorema de Euler - Demonstração

Demonstração: Sejam $r_1, r_2, \cdots r_{\phi(n)}$ os inteiros positivos inferiores a n que são primos com n e consideremos os seguintes múltiplos de a:

$$r_1 a, r_2 a, r_3 a, \cdots, r_{\phi(n)} a$$

Como n é primo com a então n é primo com todos estes múltiplos de a. Logo todas as congruências lineares da forma $ax \equiv_n r_j$ têm uma única solução inferior a n que é prima com n, ou seja, existe um r_i tal que $ar_i \equiv_n r_j$
Por outro lado, todos estes múltiplos dão restos distintos quando divididos por n. Se tivessemos $r_i a \equiv_n r_j a$, dividindo por a que é primo com n, teríamos $r_i \equiv_n r_j$. Logo,

$$r_1 a \times r_2 a \times r_3 a \times \cdots \times r_{\phi(n)} a \equiv_n r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)}$$

e portanto

$$a^{\phi(n)} \times r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)} \equiv_n r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)}$$

Como m.d.c.$(n, r_i) = 1$, para todo i, dividindo por $r_1 \times r_2 \times r_3 \times \cdots \times r_{\phi(n)}$, obtemos $a^{\phi(n)} \equiv_n 1$

Teorema de Wilson

Teorema de Wilson : p primo $\Rightarrow$ $(p-1)! \equiv_p -1$

Demonstração: Ver apontamentos.

Exemplo : Vamos testar o Teorema de Wilson para $p = 13$:

$$12! = 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12 =$$

$$(2\times 7)(3\times 9)(4\times 10)(5\times 8)(6\times 11)\times 12 \equiv_{13} 1\times 1\times 1\times 1\times 12 = 12 \equiv_{13} -1$$