Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

O Teorema de Euler e Aplicações

Douglas Matheus Gavioli Dias[1]
Faculdade de Engenharia de Ilha Solteira, UNESP, Ilha Solteira, SP
Jaime Edmundo Apaza Rodriguez[2]
Departamento de Matemática, UNESP, Ilha Solteira, SP

1 Introdução

Neste trabalho apresentamos o Teorema de Euler na Teoria do Números (Teorema de Fermat-Euler). Usaremos algumas propriedades das congruências lineares, assim como dos sistemas reduzidos de resíduos. Este teorema e suas consequências são importantes no estudo do sistema criptográfico RSA.

2 Função φ de Euler, sistemas reduzidos, Teorema de Euler e uma aplicação

A função totiente de Euler, $\varphi(n)$, conta o número de inteiros, entre 1 e n, que sejam coprimos com n. Para $n > 1$, $\varphi(n)$ corresponde à quantidade de números naturais não múltiplos de n que vão de 0 a $n-1$. Se $n = 1$, então $\varphi(1) = 1$

Por definição, $\varphi(n) \leq n-1$ para todo $n \geq 2$, e, se $n = p$ for primo, se tem que $\varphi(p) = p-1$. (se p um primo, nenhum $n \in \mathbb{N}$ entre 0 e $p-1$ é múltiplo de p).

Proposição 2.1 (Proposição)**.** *Sejam $m, a, b, c \in \mathbb{Z}$ com $m > 1$ e $mdc(c, m) = 1$. Se $ac \equiv bc\,(mod\ m)$, então $a \equiv b\,(mod\ m)$.*

Definição 2.1. *O conjunto dos inteiros $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo n se:*

(1) *$r_i \neq r_j\ (mod\ m)$, para $i \neq j$*

(2) *Para todo inteiro m existe um r_i tal que $m \equiv r_i (mod\ m)$.*

Por exemplo, o conjunto $\{0, 1, 2, \cdots n-1\}$ é um sistema completo de resíduos módulo n.

[1]mgaviolidias@hotmail.com
[2]jaime@mat.feis.unesp.br

2.1 Sistema reduzido de resíduos

Um sistema reduzido de resíduos módulo n é um conjunto de $\varphi(n)$ inteiros $r_1, r_2, \cdots, r_{\varphi(n)}$ tais que cada elemento deste conjunto é relativamente primo com n, e se $i \neq j$, então $r_i \not\equiv r_j (\text{mod } m)$.

Por exemplo, o conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8 e $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. Para se obter um sistema reduzido basta retirar os elementos do sistema completo que não são relativamente primos com n.

Teorema 2.1 (Teorema de Euler)**.** *[2] Sejam $n, a \in \mathbb{Z}$ com $n > 1$ e $mdc(a, n) = 1$. Então:*

$$a^{\varphi(n)} \equiv 1 \, (mod \; n).$$

Demonstração: Seja $r_1, r_2, ..., r_{\varphi(n)}$ um sistema reduzido de resíduos módulo n. Se verifica que $ar_1, ar_2, ..., ar_{\varphi(n)}$ também é um sistema reduzido de resíduos módulo n, onde $a \in \mathbb{Z}$ tal que $mdc(a, n) = 1$. Portanto temos que

$$a^{\varphi(n)} r_1 \cdot r_2 \cdots r_{\varphi(n)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \; (\text{mod } n).$$

Daqui segue então que $a^{\varphi(n)} \equiv 1 \, mod(n)$.

Observar que isto significa que o resíduo de dividir $a^{\varphi(n)}$ por n é 1, ou que n é divisor de $a^{\varphi(n)} - 1$.

Teorema 2.2. *(Pequeno Teorema de Fermat) [1] Seja $a \in \mathbb{Z}$ e p primo tal que $mdc(a, p) = 1$. Então*

$$a^{p-1} \equiv 1 \; (mod \; p).$$

Demonstração: Basta observar que, sendo p primo, $\varphi(p) = p - 1$.

3 Conclusões

Podemos observar o poder do Teorema de Euler, em conjunto com a função Totiente de Euler, para mostrar, entre outras questões, propriedades relativas à divisibilidade e resolver exercícios sobre o cálculo de resíduos, sem a necessidade de efetuar as divisões.

Referências

[1] A. Hefez, *Aritmética*, Coleção PROFMAT, Sociedade Brasileira de Matemática, Rio de Janeiro, 2014.

[2] J. P. de O. Santos. *Introdução à Teoria dos Números*, Coleção Matemática Universitária, IMPA, 1998.