Uma introdução à teoria analítica dos números

Daniel Luiz Göde[1] Victor Afonso[1], Victor Antônio Nascimento[1]

Universidade Federal de Santa Catarina - Campus Blumenau

24 de outubro de 2018

Resumo

Apresentamos uma breve introdução a conceitos importantes da teoria analítica dos números, com o intuito de apresentarmos o teorema de Euler. Para tal, apresentamos alguns resultados importantes que envolvem congruências e a função de Euler.

Definição de Congruência entre números

Seja a e b dois números inteiros, dizemos que a é congruente a b módulo m se m divide (a-b). Denotamos isso como

$$a \equiv b(mod\ m)$$

Se m não divide (a-b) falamos que a e b são incongruentes módulo m, denotamos isto como

$$a \not\equiv b(mod\ m).$$

Exemplos

Já que $2|(11-3)$ temos

$$11 \equiv 3(mod 2).$$

Como 5 não divide 6 e $6 = 17 - 11$ temos que

$$17 \not\equiv 11(mod 5).$$

Definição da função de euler

A função de euler, denotada por

$$\phi(n)$$

É definida como o número de inteiros positivos menores ou iguais a n que são relativamente primos a n.

Exemplo

Se tomarmos $n = 8$, teremos que

$$\phi(8) = 4$$

já que o total de números relativamente primos a 8 menores ou iguais a 8 são 4 $(1, 3, 5, 7)$.

Definição de sistema reduzido de resíduos módulo m

Um sistema reduzido módulo m é um conjunto de $\phi(m)$ inteiros $(r_1, r_2, r_3, ...r_{\phi(m)})$ relativamente primos a m e incongruentes entre si módulo m.

Exemplo

Se tomarmos $m = 15$, teremos que um sistema reduzido de resíduos módulo 15 é

$$(1, 2, 4, 7, 8, 11, 13, 14)$$

e temos que

$$(3, 6, 12, 21, 24, 33, 39, 42)$$

é, também, um sistema reduzido de resíduos módulo 15.

Teorema

Seja a um inteiro positivo tal que,

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

Se

$$r_1, r_2, r_3, ..., r_{(m)}$$

É um sistema reduzido de resíduos módulo m, então

$$ar_1, ar_2, \dots ar_{(m)}$$

É, também, um sistema reduzido de resíduos módulo m.

Demonstração

Como na sequência $ar_1, ar_2, \dots, ar_{(m)}$ temos (m) elementos, devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m.
É fácil ver que, se

$$mdc(a, m) = 1 \ \ \& \ \ mdc(r_i, m) = 1$$

então

$$mdc(ar_i, m) = 1$$

Agora basta mostrar que $ar_i \not\equiv ar_j(mod\ m)$ se $i \neq j$ Já que $mdc(a, m) = 1$ então se

$$ar_i \equiv ar_j(mod\ m)$$

temos que

$$r_i \equiv r_j(mod\ m)$$

o que implica que $i = j$, já que r_i e r_j fazem parte do mesmo sistema reduzido módulo m.

C. Q. D.

Teorema de Euler

Se m é positivo e $(a, m) = 1$ então

$$a^{\phi(m)} = 1(mod\ m).$$

Nota-se que esse teorema é uma generalização do pequeno teorema de fermat, que afirma que

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

sendo p primo e $mdc(a, p) = 1$. Já que $\phi(p)$ de todo p primo é igual a $p - 1$

Demonstração

No Teorema anterior é demonstrado que os elementos $ar_1, ar_2, \dots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se o $mdc(a, m) = 1$ e $r_1, r_2, \dots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m. Isto significa que ar_i é congruente a exatamente um dos, r_j, com $1 \leq j \leq \phi(m)$, e portanto o produto dos ar_i deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1.ar_2 \dots ar_{\phi(m)} \equiv r_1.r_2 \dots ar_{\phi(m)}(mod\ m)$$

ou seja,

$$a^{\phi(m)} r_1.r_2 \dots r_{\phi(m)} \equiv r_1.r_2 \dots r_{\phi(m)}(mod\ m)$$

Como

$$mdc(r_1.r_2 \dots r_{\phi(m)}, m) = 1$$

então

$$a^{\phi(m)} \equiv 1(mod\ m).$$

C.Q.D

Exemplo

Seja:

$$a = 5, m = 8$$

Sistema de resíduos reduzido módulo $8 = 1, 3, 5, 7$

$$5x1 = 5(mod 8)$$
$$5x3 = 7(mod 8)$$
$$5x5 = 1(mod 8)$$
$$5x7 = 3(mod 8)$$

Multiplicando-se as congruências, temos que:

$$5^4(1x3x5x7) = (1x3x5x7)(mod 8)$$

já que $mdc(1x3x5x7, 8) = 1$, podemos dividir $(1x3x5x7)$ dos dois lados, obtendo

$$5^4 = 1(mod 8).$$

Referêcias

PLÍNIO DE OLVEIRA SANTOS, José. Introdução à Teoria dos Números: $1^a edição. Rio de Janeiro : Sociedade Brasileira de Matemática, 1998$