Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Teoria de Números e Aplicações

Renahn dos Santos Lopes[1], Adriana Wagner[2]
UFMS, Aquidauana, MS

Nesse trabalho, usando o conceito de congruência modular apresentaremos algumas aplicações. Os resultados aqui apresentados fazem parte do estudo do Projeto de Iniciação Científica Voluntária- Teoria de Números e Aplicações, tendo como base [1] e [2].

Definição 1. *Se a e b são inteiros dizemos que a é* ***congruente*** *a b módulo m, $(m > 0)$ se $m \mid (a - b)$. Denotamos por $a \equiv b \ (mod\ m)$. Se $m \nmid (a - b)$ dizemos que a é* ***incongruente*** *a b módulo m.*

Exemplo 1. *Temos que $16 \equiv 4 \ (mod\ 2)$ pois $2|(16 - 4)$. Como $5 \nmid 6$ e $17 - 11 = 6$ temos que 17 é incongruente a 11 módulo 5.*

Proposição 1. *Se a e b são inteiros temos que $a \equiv b \ (mod\ m)$ se, e somente se, existir uma inteiro k tal que $a = b + kn$.*

Proposição 2. *Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1) $a \equiv b \ (mod\ m)$
2) *Se* $a \equiv b \ (mod\ m)$ *então* $b \equiv a \ (mod\ m)$
3) *Se* $a \equiv b \ (mod\ m)$ *e* $b \equiv d \ (mod\ m)$ *então* $a \equiv d \ (mod\ m)$

Teorema 1. *Sejam a, b, c, d e m inteiros tais que $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$ então*

1) $a + c \equiv b + c \ (mod\ m)$; $a - c \equiv b - c \ (mod\ m)$
2) $a + c \equiv b + d \ (mod\ m)$; $a - c \equiv b - d \ (mod\ m)$
3) $ac \equiv bc \ (mod\ m)$; $ac \equiv bd \ (mod\ m)$

Definição 2. *Se h e k são dois inteiros com $h \equiv k \ (mod\ m)$, dizemos que ké um resíduo de h módulo m.*

Definição 3. *O conjunto dos inteiros $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo m se: $r_i \not\equiv r_j \ (mod\ m)$ para $i \neq j$; para todo inteiro n existe um r_i tal que $n \equiv r_i \ (mod\ m)$.*

Exemplo 2. *Temos que $\{0, 1, 2, \cdots, m - 1\}$ é um sistema completo de resíduos módulo m.*

Teorema 2. *Se k inteiros $r_1, r_2, \cdots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.*

Proposição 3. *Sejam a um inteiro qualquer, r um inteiro não negativo e m um inteiro maior que 1. Se r é o resto da divisão euclidiana de a por m, então $a \equiv r \ (mod\ m)$.*

[1] renahn.lopes@ufms.br
[2] adriana.wagner@ufms.br

Proposição 4. *Se m é um inteiro maior que 1, então o conjunto $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \ (mod\ m)\}$ é uma relação de equivalência sobre o conjunto dos números inteiros. Neste caso, a classe de equivalência de a, denotado por $\bar{a}$, é dado por $\bar{a} = \{b \in \mathbb{Z} \mid a \equiv b \ (mod\ m)\}$ e denotamos por $\mathbb{Z}_m$ o conjunto de todas as classes de equivalência distintas definidas pela relação de congruência.*

Exemplo 3. *Para $m = 7$ temos que $\mathbb{Z}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$.*

Dado o conceito de congruência modular e seus resultados, vamos ver duas aplicações desse contexto, o relógio analógico, o código de barras e o número ISBN.

Exemplo 4. *Relógio Analógico*

Considere um relógio analógio. Se agora são 13 horas, qual será a posição do ponteiro menor? Notemos que 13 dividido por 12 deixa reto igual a 1. Assim, o ponteiro pequeno estará no número 1. Observemos que 13 horas é congruente a 1 hora, módulo 12; Portanto, as horas marcadas num relógio analógico constituem um exemplo clássico de congruência, nesse caso com módulo 12, aplicado ao cotidiano das pessoas.

Exemplo 5. *Código de Barras*

Um dos códigos de barras mais usados no mundo todo é o EAN-13, usado para a identificação da maioria dos artigos que normalmente compramos. É constituído de 13 algarismos, sendo que o último é o dígito de controle. Nesse caso, é usado a congruência módulo 10 e os fatores que constituem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita, correspondendo a cada um dos 12 primeiros números do código. Considere a sequência 789891201904 formada pelos 12 primeiros dígitos de um código de barras, devemos multiplicá-los, nessa ordem, por $1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3$ e somar os produtos obtidos, isto é, $1 \cdot 7 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 1 + 1 \cdot 2 + 3 \cdot 0 + 1 \cdot 1 + 3 \cdot 9 + 1 \cdot 0 + 3 \cdot 4 = 118$. O dígito que está faltando, que vamos representar por D deve ser tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 10, isto é, $118 + D$ deve ser múltiplo de 10, ou seja, $118 + D \equiv 0 \ (mod\ 10)$. Assim, $D = 2$.

Exemplo 6. *ISBN*

O ISBN (International Standard Book Number/ Padrão Internacional de Numeração de Livro) é um padrão numérico de 10 dígitos criado com o objetivo de fornecer uma espécie de registro para publicações monográficas, como livros, artigos e apostilas. É formado por uma sequência de 9 primeiros dígitos, que devem ser multiplicados, nessa ordem, por $10, 9, 8, 7, 6, 5, 4, 3, 2$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por I deve ser tal que ao ser acrescentado à soma S obtida, deve gerar um múltiplo de 11, isto é, $S + I \equiv 0 \ (mod\ 11)$. Por exemplo, consideremos 852121146 os 9 primeiros dígitos do ISBN do livro [2], então $S = 10 \cdot 8 + 9 \cdot 5 + 8 \cdot 2 + 7 \cdot 1 + 6 \cdot 2 + 5 \cdot 1 + 4 \cdot 1 + 3 \cdot 4 + 2 \cdot 6 = 193$. Assim, para que $(193 + I) \equiv 0 \ (mod\ 11)$ devemo ter $I = 4$.

Referências

[1] J. P. O. Santos. **Introdução à Teoria dos Números**. 3a. ed. Rio de Janeiro: IMPA, 2009. ISBN: 978854401427.

[2] J. C. Silva e O. R. Gomes. **Estruturas Algébricas para Licenciatura: Elementos de Aritmética Superior- V. 2**. 5a. ed. São Paulo: Blucher, 2018. ISBN: 9788521211464.