UMA APLICAÇÃO COTIDIANA DO TEOREMA CHINÊS DOS RESTOS

Celine Ingrid Gomes dos Santos [1]
Thyago Santos de Souza [2]

INTRODUÇÃO

Imaginemos, a princípio, o seguinte problema: Um feirante foi questionado sobre a quantidade de laranjas que ele possuía. Em resposta, ele falou: ao dividir essa quantidade por 7, obtém-se resto 5; ao dividir por 11, obtém-se resto 7; por fim, ao ser dividida por 13, obtém-se resto 3. É possível determinar a cardinalidade desse conjunto de laranjas?

Por meio de alguns problemas cotidianos, como o que fora apresentado, surgiu o Teorema Chinês dos Restos. Como o nome propõe, esse Teorema, segundo Santos (2017), fora formulado na China. Fora apresentado, pela primeira vez, no livro Sunzi's Mathematical Classic (século III), pelo matemático Sun Tzu. Esse problema levou, mais tarde, alguns outros matemáticos a estudarem suas aplicações e casos especiais. Dentre esses, alguns bastante conhecidos na atualidade, como é o caso de Fibbonacci.

Mais adiante, no corpo deste trabalho, iremos apresentar a noção de congruência módulo n, que, como explica Santos (2017), fora introduzida ao Teorema Chinês dos Restos por Carl Friedrich Gauss. O uso e conhecimento da definição e representação de congruência será de suma importância para a compreensão da ilustração do Teorema, bem como sua prova, e, ainda, da resolução do problema descrito no início.

METODOLOGIA

O presente trabalho é fruto de um projeto de Iniciação Científica já concluído, intitulado "Introdução à Teoria de Anéis" e vinculado ao PET – Matemática e Estatística, da UFCG.

A priori, este trabalho fora desenvolvido com o intuito de compreender como o Teorema Chinês dos Restos é aplicado em situações cotidianas que envolvam divisibilidade e

[1] Graduanda do curso de Matemática, da Universidade Federal de Campina Grande – UFCG, e bolsista do PET – Matemática e Estatística / FNDE – celineingridgomess@hotmail.com;
[2] Professor orientador: Doutor, Universidade Federal de Campina Grande – UFCG, thyago@mat.ufcg.edu.br.

congruência. Para tanto, procuramos abordar o tema de maneira clara e objetiva, analisando os resultados presentes nas obras citadas nas referências, por meio de uma pesquisa bibliográfica, e selecionando os de maior relevância para o contexto do trabalho.

O método utilizado para estudo do tema fora o mesmo do projeto de pesquisa: exposições semanais de seminários, sobre temas inclusos na Álgebra. Após esse estudo, fora utilizada a Dissertação de Mestrado de Santos (2017, p.1) para incremento da nota histórica.

Quando esses materiais foram analisados, fora construído, então, o alicerce para o desenvolvimento deste trabalho. Objetivando, desde o início, apresentar as ferramentas necessárias para a compreensão da prova do Teorema Chinês dos Restos, bem como sua aplicação no problema proposto e, acima de tudo, a contribuição para a pesquisa científica.

A motivação para a escolha do tema partira de estudos de temas tangentes, realizados na pesquisa da Iniciação Científica.

REFERENCIAL TEÓRICO

Para o desenvolvimento deste trabalho, a literatura utilizada fora dois livros de Álgebra e uma dissertação de Mestrado Profissional. Todos esses com foco em Teoria dos Números e Aritmética Modular.

Antes de enunciarmos o Teorema Chinês dos Restos, será necessário, sobretudo, apresentarmos a definição de divisibilidade e congruência módulo n e, ainda, alguns lemas. Estes anteriores são tópicos fundamentais no estudo da Teoria dos Números e, no contexto deste trabalho, também serão de suma importância para a demonstração do Teorema. Todos os resultados que serão apresentados aqui podem ser consultados nas referências. Recomendamos Domingues e Iezzi (2003) para uma abordagem mais detalhada do tema.

A prova do Teorema fora baseada na obra de Niven et al. (1991), no entanto, buscamos torná-la mais didática, de modo que o leitor consiga, em uma primeira leitura, compreender a sua essência.

RESULTADOS E DISCUSSÃO

Definição de divisibilidade: Sejam a e b inteiros. Diz-se que $a\ divide\ b$ se é possível encontrar c inteiro tal que $b = ac$. Para indicar que $a\ divide\ b$, usaremos $a|b$.

O Máximo Divisor Comum de dois números inteiros a e b será denotado por $mdc(a, b)$. As seguintes propriedades de Divisibilidade e Máximo Divisor Comum serão utilizadas ao

longo do trabalho. Para mais detalhes, veja, por exemplo, Domingues e Iezzi (2003).

Propriedades:

(i) $a|a$;

(ii) Se $a|b$ e $a|c$, então $a|(bx + cy)$, com $x, y \in \mathbb{Z}$;

(iii) Se $a|b$ e $c|d$, então $ac|bd$.

(iv) Relação de Bezout: Para quaisquer inteiros a e b, existem inteiros x e y tais que $d = ax + by$ é o máximo divisor comum de a e b.

Definição de congruência: Sejam a e b números inteiros quaisquer e n um inteiro estritamente positivo. Diz-se que a é *côngruo* a b *módulo* n se $n \mid (a - b)$, isto é, se $a - b = nq$, para algum q inteiro. Para indicar que a é *côngruo* a b *módulo* n, usaremos a notação

$$a \equiv b \ (mod\ n).$$

Lema 1: Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$ tais que $mdc(a, n) = 1$. Então a congruência do tipo $ax \equiv b \ (mod\ n)$ tem solução $x_0 \in \mathbb{Z}$.

Demonstração: Se $mdc(a, n) = 1$, então, pela relação de Bezout, existem $x, y \in \mathbb{Z}$ tais que

$$ax + ny = 1.$$

Multiplicando a igualdade por b, temos

$$a(xb) + n(yb) = b$$

$$a(xb) - b = n(-yb).$$

Logo, $(xb)a \equiv b \ (mod\ n)$ e, assim, $x_0 = xb$ é solução da congruência. ■

Lema 2: Sejam a e b inteiros tais que $mdc(a, b) = 1$. Se $a \mid c$ e $b \mid c$, então $ab \mid c$.

Demonstração: Pela Relação de Bezout, existem $x, y \in \mathbb{Z}$ tais que

$$ax + by = 1$$

Multiplicando a igualdade por c, obtemos

$$(ac)x + (bc)y = c.$$

Como $a \mid a$ e, por hipótese, $b \mid c$, então $ab \mid ac$ e, portanto, $ab \mid (ac)x$. Analogamente, $b \mid b$ e, novamente, por hipótese, $a \mid c$, então $ab \mid (bc)y$. Logo, $ab \mid [(ac)x + (bc)y]$, ou seja, $ab \mid c$. ■

Teorema Chinês dos Restos: Sejam $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ e $n_1, n_2, \ldots, n_k \in \mathbb{N}$ tais que $mdc(n_i, n_j) = 1$, com $i \neq j$. Então o sistema de congruências

$$\begin{cases} x \equiv b_1 \ (mod\ n_1) \\ x \equiv b_2 \ (mod\ n_2) \\ \quad\quad . \\ \quad\quad . \\ \quad\quad . \\ x \equiv b_k \ (mod\ n_k) \end{cases}$$

tem uma única solução $x_0 \in \mathbb{Z}$, com $0 \leq x_0 < n$, em que $n = n_1\, n_2 \ldots n_k$. Além disso,

$$S = \{x_0 + kn : k \in \mathbb{Z}\}$$

é o conjunto das soluções deste sistema.

Demonstração: (Existência) Sabemos que

$$\frac{n}{n_i} \in \mathbb{Z} \text{ e } mdc(\frac{n}{n_i}, n_i) = 1, i = 1, 2, \ldots, k.$$

Logo, pelo Lema 1, para cada i existe $r_i \in \mathbb{Z}$ tal que

$$\frac{n}{n_i}\, r_i \equiv 1\ (mod\ n_i).$$

Daí, multiplicando a congruência anterior por um $b_i \in \mathbb{Z}$, obtemos:

$$\frac{n}{n_i} r_i b_i \equiv b_i\ (mod\ n_i).$$

Se $i \neq j$, então $n_j \mid \frac{n}{n_i} r_i$

$$\frac{n}{n_i} r_i \equiv 0\ (mod\ n_j).$$

Assim, considere

$$x_0 = \sum_{i=1}^{k} \frac{n}{n_i}\, r_i b_i = \frac{n}{n_1} r_1 b_1 + \frac{n}{n_2} r_2 b_2 + \ldots + \frac{n}{n_k} r_k b_k.$$

No somatório anterior, apenas o termo $\frac{n}{ni}\, r_i b_i$ não é múltiplo de n_i, com $i \neq j$. Então,

$$x_0 \equiv \frac{n}{n_i} r_i b_i\ (mod\ n_i).$$

Mas $\frac{n}{n_i} r_i \equiv 1\ (mod\ n_i)$. Assim,

$$x_0 \equiv b_i\ (mod\ n_i), \text{ para todo } i = 1, 2, \ldots, k.$$

Dessa forma, x_0 é solução do sistema de congruências.

(Unicidade) Sejam $x_1, x_2 \in \mathbb{Z}$ duas soluções do sistema de congruências, com $0 \leq x_1 \leq x_2 < n$. Então, $x_1 \equiv x_2\ (mod\ n_i)$, para todo $i = 1, 2, \ldots, k$. Pelo Lema 2, $x_1 \equiv x_2\ (mod\ n)$, isto é, $n \mid (x_1 - x_2)$. Como $0 \leq x_1 - x_2 < n$, temos $x_1 = x_2$. ■

Agora, após a apresentação desses resultados, temos as ferramentas necessárias para a resolução do problema proposto na introdução:

Em primeiro lugar, para podermos utilizar o Teorema Chinês dos Restos, iremos reescrever as informações dadas no problema como um sistema de congruências:

$$\begin{cases} x \equiv 5\ (mod\ \ 7) \\ x \equiv 7\ (mod\ 11) \\ x \equiv 3\ (mod\ 13) \end{cases}$$

Então, temos $b_1 = 5,\ b_2 = 7, b_3 = 3,\ n_1 = 7, n_2 = 11, n_3 = 13\ e\ n = 1001$.Como

$mdc(\frac{1001}{7}, 7) = mdc(143, 7) = 1$, podemos encontrar r_1, r_2 e r_3 através do método das divisões sucessivas (para mais detalhes, veja Domingues e Iezzi (2003, p. 41)):

$$143 = 7 \cdot 20 + 3$$

$$7 = 3 \cdot 2 + 1$$

$$3 = 1 \cdot 3$$

Daí,

$$1 = 7 - 3 \cdot 2 = 7 - (143 - 7 \cdot 20) \cdot 2 = 7 - (143 \cdot 2 - 7 \cdot 20 \cdot 2) =$$

$$= 7 \cdot 41 + 143 \cdot (-2).$$

Assim, podemos escolher $r_1 = -2$. De modo análogo, podemos escolher, também, $r_2 = 4$ e $r_3 = -1$.

Logo,

$$x_0 = 11 \cdot 13 \cdot (-2) \cdot 5 + 7 \cdot 13 \cdot 4 \cdot 7 + 7 \cdot 11 \cdot (-1) \cdot 3 = 887$$

é a única solução entre 0 e 1001. Portanto, $x_0 = 887$ é a menor solução positiva do problema.

CONSIDERAÇÕES FINAIS

Como fora ilustrado ao longo deste trabalho, o Teorema Chinês dos Restos pode ser aplicado para resolver sistemas de congruências nos quais suas equações possuem módulos primos entre si dois a dois, ou seja, $mdc(n_i, n_j) = 1$. No entanto, um questionamento que pode ser levantado acerca do tema é: E quando o $mdc(n_i, n_j) > 1$?

Para a resolução de problemas com sistemas de congruências que apresentam $mdc(n_i, n_j) > 1$, existem tópicos no conteúdo de Equações Diofantinas Lineares que auxiliam na determinação de uma solução geral para esses casos. Deixamos a cargo do leitor que tenha interesse na área, a procura desse item nas referências, para o desenvolvimento de futuros trabalhos.

Palavras-chave: Teorema Chinês dos Restos, Congruências, Sistema de congruências, Divisibilidade, Máximo Divisor Comum.

REFERÊNCIAS

DOMINGUES, Hygino H; IEZZI, Gelson. Álgebra Moderna. 4 ed. reform. São Paulo: Atual, 2003.

NIVEN, Ivan; ZUCKERMAN, Hebert S.; MONTGOMERY, Hugy L. *An Introduction to the Theory of Numbers*. Wiley (New York), 1991.

SANTOS, A. **Teorema Chinês dos Restos e aplicações**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas. Manaus, p. 1. 2017.