

# Material Teórico - Módulo Aritmética dos Restos

## Aritmética Modular - Parte 3

### Tópicos Adicionais

**Autor: Ulisses Lima Parente**

**Revisor: Prof. Antonio Caminha M. Neto**

**19 de maio de 2023**



**PORTAL DA  
MATEMÁTICA**  
OBMEP

Na parte 2 dessa aula, mostramos que se  $\text{mdc}(a,n) = 1$ , então  $\bar{a}$  possui um inverso multiplicativo módulo  $n$ , digamos  $\bar{c}$ , logo, a congruência linear  $ax \equiv b \pmod{n}$  possui uma única solução módulo  $n$ , dada por  $x \equiv bc \pmod{n}$ .

O teorema abaixo generaliza esse resultado, apontando condições para a existência de soluções da congruência linear  $ax \equiv b \pmod{n}$ , bem como para a quantidade de soluções incongruentes módulo  $n$ .

**Teorema 1.** *Sejam  $a, b$  e  $n > 0$  números inteiros, tais que  $\text{mdc}(a,n) = d$ . Se  $d \nmid b$ , então a congruência linear  $ax \equiv b \pmod{n}$  não possui solução. Se  $d \mid b$ , então  $ax \equiv b \pmod{n}$  possui exatamente  $d$  soluções duas a duas incongruentes, módulo  $n$ .*

Perceba que, se  $x_0$  for uma solução de  $ax \equiv b \pmod{n}$ , então  $n \mid (ax - b)$ , logo, existe  $y_0$  inteiro tal que  $ax_0 - b = ny_0$ , ou seja, junto com a solução  $x_0$  da congruência linear, existe um número inteiro  $y_0$  tal que  $ax_0 - ny_0 = b$ .

Desse modo, o par  $(x_0, y_0)$  é uma solução da equação diofantina linear  $ax - ny = b$ . Portanto, antes de demonstrarmos o teorema 1, apresentamos o teorema abaixo, sobre existência e caracterização de soluções de equações diofantinas lineares.

**Teorema 2.** *Sejam  $a, b, c$  números inteiros e  $d = \text{mdc}(a,b)$ . Em relação à equação diofantina linear  $ax + by = c$ , temos que:*

- (a) *Se  $d \nmid c$ , então a equação não possui soluções.*
- (b) *Se  $d \mid c$ , então a equação possui infinitas soluções. Além disso, se o par  $(x_0, y_0)$  for uma dessas soluções, então todas as demais soluções são dadas por*

$$\begin{cases} x = x_0 + \frac{b}{d} \cdot k \\ y = y_0 - \frac{a}{d} \cdot k \end{cases}$$

**Prova.** Se a equação diofantina linear  $ax + by = c$  possui uma solução  $(x,y)$ , então, como  $d \mid a$  e  $d \mid b$ , concluímos que

$d \mid (ax + by)$ , ou seja,  $d \mid c$ . Portanto, se  $d \nmid c$ , então a equação  $ax + by = c$  não pode ter solução.

Por outro lado, se  $d \mid c$ , então existe  $q$  inteiro tal que  $c = qd$ . Mas, uma vez que  $d = \text{mdc}(a, b)$ , o teorema de Bézout garante a existência de inteiros  $m$  e  $n$  tais que

$$am + bn = d.$$

Multiplicando ambos os lados da última igualdade por  $q$ , obtemos

$$q(am + bn) = qd \implies a(qm) + b(qn) = c.$$

Logo, o par  $(x, y) = (qm, qn)$  é solução de  $ax + by = c$ .

Além disso, se o par  $(x_0, y_0)$  for uma solução qualquer de  $ax + by = c$ , então o par formado pelos inteiros  $x$  e  $y$  dados por

$$(*) \begin{cases} x = x_0 + \frac{b}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases}$$

em que  $k \in \mathbb{Z}$ , também é uma solução da equação  $ax + by = c$ . Com efeito, temos que  $ax_0 + by_0 = c$  e

$$\begin{aligned} ax + by &= a \left( x_0 + \frac{b}{d} \cdot k \right) + b \left( y_0 - \frac{a}{d} \cdot k \right) \\ &= ax_0 + \frac{ab}{d} \cdot k + by_0 - \frac{ab}{d} \cdot k \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Resta provar que as soluções dadas por  $(*)$  são as únicas soluções da equação diofantina. Para isso, vamos considerar  $(x, y)$  uma solução qualquer de  $ax + by = c$  e mostrar que essa solução é da forma  $(*)$ , para algum  $k \in \mathbb{Z}$ . De fato, como  $(x_0, y_0)$  também é solução, temos  $ax_0 + by_0 = c$ , logo,

$$\begin{aligned} (ax + by) - (ax_0 + by_0) &= c - c \implies ax + by - ax_0 - by_0 = 0 \\ &\implies ax - ax_0 = by_0 - by \\ &\implies a(x - x_0) = b(y_0 - y). \end{aligned}$$

Dividindo ambos os membros da última igualdade por  $d$ , obtemos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y);$$

daí, segue que  $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$ . Agora, veja que

$$\text{mdc}(a, b) = d \implies \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Assim,

$$\frac{b}{d} \mid \frac{a}{d}(x - x_0) \implies \frac{b}{d} \mid (x - x_0).$$

Concluimos, portanto, que existe  $k \in \mathbb{Z}$  tal que  $x - x_0 = \frac{b}{d} \cdot k$ , ou, o que é o mesmo,

$$x = x_0 + \frac{b}{d} \cdot k.$$

Substituindo  $x - x_0 = \frac{b}{d} \cdot k$  em  $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$ , obtemos

$$\begin{aligned} \frac{a}{d} \cdot \frac{b}{d} \cdot k &= \frac{b}{d}(y_0 - y) \implies \frac{a}{d} \cdot k = y_0 - y \\ &\implies y = y_0 - \frac{b}{d} \cdot k. \end{aligned}$$

□

**Exemplo 3.** Decida se a equação diofantina linear a seguir tem soluções. Em caso afirmativo, encontre todas elas:

$$14x - 31y = 8.$$

**Solução.** Calculando  $\text{mdc}(14, -31) = \text{mdc}(14, 31)$  pelo método das divisões sucessivas, obtemos

	2	4	1	2
31	14	3	2	1
3	2	1	0	

Daí,  $\text{mdc}(14, -31) = 7 \mid 14$ , logo, a equação  $14x - 31y = 8$  possui infinitas soluções.

Para encontrar uma dessas soluções, vamos, antes, encontrar inteiros  $m$  e  $n$  tais que  $14m - 31n = 1$ . Em seguida, multiplicamos ambos os membros da igualdade por 8 e, assim, chegamos a uma solução particular de  $14x - 31y = 8$ . Com efeito, podemos escrever

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (14 - 4 \cdot 3) \\ &= 3 - 1 \cdot 14 + 4 \cdot 3 \\ &= 5 \cdot 3 - 1 \cdot 14 \\ &= 5 \cdot (31 - 2 \cdot 14) - 1 \cdot 14 \\ &= 5 \cdot 31 - 10 \cdot 14 - 1 \cdot 14 \\ &= 5 \cdot 31 - 11 \cdot 14, \end{aligned}$$

de sorte que  $14 \cdot (-11) - 31 \cdot (-5) = 1$ . Agora, multiplicando os dois membros da última igualdade por 8, obtemos

$$8 \cdot (14 \cdot (-11) - 31 \cdot (-5)) = 8 \cdot 1 \iff 14 \cdot (-88) - 31 \cdot (-40) = 8.$$

Portanto, o par  $(-88, -40)$  é uma solução particular de  $14x - 31y = 8$ . Desse modo, utilizando o teorema 2, as soluções dessa equação são dadas por

$$\begin{cases} x = -88 + \frac{-31}{1}k = -88 - 31k \\ y = -40 - \frac{14}{1}k = -40 - 14k \end{cases}.$$

□

**Observação 4.** *No exemplo 3, podemos encontrar uma solução particular de  $14x - 31y = 14$  sem recorrer ao método das divisões sucessivas. Com efeito, basta notar que  $14 \cdot 5 - 31 \cdot 2 = 70 - 62 = 8$ , logo,  $(x_0, y_0) = (5, 2)$  é uma solução particular. Desse modo, obtemos soluções*

$$\begin{cases} x = 5 + \frac{-31}{1}k = 5 - 31k \\ y = 2 - \frac{14}{1}k = 2 - 14k \end{cases}.$$

Veja que a solução  $(-88, -40)$ , que foi encontrada lá, pode ser obtida aqui fazendo  $k = 3$ .

**Prova do teorema 1.** Como vimos acima, resolver a congruência linear  $ax \equiv b \pmod{n}$  é equivalente a resolver a equação diofantina linear  $ax - ny = b$ . Mas essa última equação tem solução se, e somente se,  $d \mid b$ , em que  $d = \text{mdc}(a, n)$ .

Ademais, utilizando o teorema 2, quando  $d \mid b$ , as soluções de  $ax - ny = b$  são dadas por

$$\begin{cases} x = x_0 - \frac{n}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases},$$

em que  $(x_0, y_0)$  é uma solução particular de  $ax - ny = b$ . Logo, as soluções de  $ax \equiv b \pmod{n}$  são dadas por  $x = x_0 - \frac{n}{d}k$ .

Como estamos interessados em saber o número de soluções incongruentes módulo  $n$ , vamos tentar encontrar condições para que duas soluções sejam congruentes módulo  $n$ . Temos que

$$\begin{aligned} x_0 - \frac{n}{d}k_1 \equiv x_0 - \frac{n}{d}k_2 \pmod{n} &\iff \frac{n}{d}k_1 \equiv \frac{n}{d}k_2 \pmod{n} \\ &\iff \frac{n}{d}k_1 \equiv \frac{n}{d}k_2 \pmod{\frac{n}{d} \cdot d} \\ &\iff k_1 \equiv k_2 \pmod{d}. \end{aligned}$$

Portanto, quando  $d \mid b$ , a congruência linear  $ax \equiv b \pmod{n}$  possui exatamente  $d$  soluções incongruentes módulo  $n$ , que são dadas por

$$x_0, x_0 - \frac{n}{d}, x_0 - \frac{n}{d} \cdot 2, \dots, x_0 - \frac{n}{d} \cdot (d - 1).$$

□

**Exemplo 5.** *Encontre, caso existam, as soluções de cada congruência linear abaixo:*

(a)  $8x \equiv 6 \pmod{12}$ .

(b)  $12x \equiv 3 \pmod{9}$ .

### Solução.

(a) Pelo teorema 1, a congruência  $8x \equiv 6 \pmod{12}$  não possui soluções, uma vez que  $\text{mdc}(8,12) = 4$  e  $4 \nmid 6$ .

(b) Como  $\text{mdc}(12,9) = 3$  e  $3 \mid 3$ , podemos utilizar novamente o teorema 1 para concluir que a congruência linear  $12x \equiv 3 \pmod{9}$  possui exatamente 3 soluções incongruentes módulo 9. Vamos repetir a ideia utilizada na demonstração do teorema para encontrar essas soluções.

Como a congruência  $12x \equiv 3 \pmod{9}$  tem solução, então, para cada uma dessas soluções  $x$ , deve existir  $y$  inteiro tal que  $12x - 3 = 9y$ , ou seja,  $12x - 9y = 3$ . Veja que o par  $(x_0, y_0) = (1, 1)$  é uma solução de  $12x - 9y = 3$  e as 3 soluções incongruentes de  $12x \equiv 3 \pmod{9}$  são dadas por  $x_0 \equiv 1 \pmod{9}$ ,  $x_1 \equiv 1 - \frac{9}{3} \pmod{9}$  e  $x_2 \equiv 1 - \frac{9}{3} \cdot 2 \pmod{9}$ , ou seja,  $x_0 = 1$ ,  $x_1 \equiv -2 \equiv 7 \pmod{9}$  e  $x_2 \equiv -5 \equiv 4 \pmod{9}$ .  $\square$

**Exemplo 6.** *O triplo de um número natural pode deixar resto 7 quando dividido por 18?*

**Solução.** A pergunta feita no enunciado do problema é equivalente a “A congruência linear  $3x \equiv 7 \pmod{18}$  tem solução?”

Utilizando o teorema 1, concluímos que a resposta a essa pergunta é **não**, pois  $\text{mdc}(3,18) = 3$  e  $3 \nmid 7$ . Portanto, não existe número natural cujo triplo deixe resto 7 quando dividido por 18.  $\square$

**Exemplo 7.** *Existe um número natural cujo dobro deixe resto 11 quando dividido por 15?*

**Solução.** De modo similar ao que foi feito no exemplo anterior, podemos trocar a pergunta feita no enunciado por “A congruência linear  $2x \equiv 11 \pmod{15}$  tem solução?”

Utilizando o teorema 1 novamente, concluímos que a resposta agora é **sim**, pois  $\text{mdc}(2,15) = 1$  e obviamente  $1 \nmid 11$ . Portanto, existe número natural cujo triplo deixa resto 11 quando dividido por 18.

Para encontrar um tal número, basta resolver a equação diofantina linear  $2x - 15y = 11$ . Mas  $(x_0, y_0) = (13, 1)$  é

claramente uma solução. Logo, o dobro de 13 deixa resto 11 quando dividido por 15. Note que os números naturais da sequência  $13 + 15 = 28$ ,  $13 + 15 \cdot 2 = 43$ ,  $13 + 15 \cdot 3 = 58$ , ..., todos deixam resto 11 quando divididos por 15. Entretanto, todos esses números são congruentes módulo 15, como era de se esperar, pois, de acordo com o teorema 1, a congruência linear  $2x \equiv 11 \pmod{15}$  possui uma única solução módulo 15, uma vez que  $\text{mdc}(2,15) = 1$ .  $\square$

Como vimos na aula anterior, uma solução de  $ax \equiv 1 \pmod{n}$  é chamada **inverso** de  $a$  módulo  $n$ . Além disso, se  $\text{mdc}(a,n) = 1$ , então a congruência linear  $ax \equiv 1 \pmod{n}$  possui uma única solução módulo  $n$ , ou seja,  $a$  possui um único inverso módulo  $n$ .

**Proposição 8.** *Seja  $p$  um número primo. Então  $a \in \mathbb{Z}$  é o seu próprio inverso módulo  $n$  se, e somente se,  $a \equiv 1 \pmod{p}$  ou  $a \equiv -1 \pmod{p}$ .*

**Prova.** Se  $a$  é o seu próprio inverso módulo  $p$ , então  $a$  é solução de  $ax \equiv 1 \pmod{p}$ , o que acarreta  $a^2 \equiv 1 \pmod{p}$ . Daí, obtemos  $p \mid (a^2 - 1)$ , logo,  $p \mid (a - 1)(a + 1)$ . Agora, como  $p$  é primo, segue que  $p \mid (a - 1)$  ou  $p \mid (a + 1)$ . Se ocorre o primeiro caso, então  $a \equiv 1 \pmod{p}$  e, se ocorre o segundo, então  $a \equiv -1 \pmod{p}$ .  $\square$

## Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores apresentem outros exemplos e questionem os alunos sobre a existência de soluções de congruências lineares. É importante que os alunos saibam diferenciar as congruências que possuem solução das que não possuem e, a partir daí, encontrar essas soluções, quando for o caso. Também é importante que fique claro quando duas soluções de uma congruência linear são incongruentes. Entender esse conceito parte fundamental para entender o teorema 1.



## Sugestões de Leitura Complementar

1. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*. Rio de Janeiro, SBM, 2022.
2. D. Fomim, S. Genkin e I. Itenberg. *Círculos Matemáticos: A Experiência Russa*. Rio de Janeiro, IMPA 2012.
3. J. P. O. Santos. *Introdução à Teoria dos Números*. Rio de Janeiro, IMPA, 2000.

Portal OBMEP