Material Teórico - Módulo Aritmética dos Restos

Aritmética Modular - Parte 2

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

19 de abril de 2023

Na parte 1 deste material, apresentamos o conjunto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\},$$

formado pelas **classes de restos módulo** n, em que n é um número inteiro positivo. Recordamos que um número inteiro a pertence a $\overline{r}$ quando r é o resto na divisão de a por n.

Agora, vamos estender o conceito de classe de resto a qualquer número inteiro, definindo $\overline{a}$ como o subconjunto de $\mathbb{Z}$ formado pelos números que deixam o mesmo resto que a quando divididos por n. Assim, se a e b são números inteiros, temos $\overline{a} = \overline{b}$ se, e somente se, a e b deixam o mesmo resto quando divididos por n.

Os conjuntos $\overline{a}$ também são denominados **classe de resíduos módulo** n. Veja que a e b deixam o mesmo resto na divisão por n se, e somente se, $a \equiv b (\mathrm{mod}\, n)$. Logo, temos que

$$\overline{a} = \overline{b} \iff a \equiv b (\mathrm{mod}\, n).$$

Recordemos as seguintes propriedades das congruências, as quais também foram apresentadas na primeira parte deste material:

(i) Se a, b, c, d e $n > 0$ são números inteiros, então

$$a \equiv c (\mathrm{mod}\, n) \text{ e } b \equiv d (\mathrm{mod}\, n) \Longrightarrow a + b \equiv c + d (\mathrm{mod}\, n).$$

(ii) Se a, b, c, d e $n > 0$ são números inteiros, então

$$a \equiv c (\mathrm{mod}\, n) \text{ e } b \equiv d (\mathrm{mod}\, n) \Longrightarrow a \cdot b \equiv c \cdot d (\mathrm{mod}\, n).$$

Essas duas propriedades nos permitem definir as operações de **adição** e **multiplicação** de classes de restos, ademais da seguinte forma:

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{e} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Por exemplo, em $\mathbb{Z}_4$, temos

$$\overline{2} + \overline{3} = \overline{5} = \overline{1} \text{ e } \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}.$$

As tabelas a seguir apresentam todas as possíveis somas e produtos em $\mathbb{Z}_4$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Perceba que $\overline{0}$ funciona como elemento neutro da adição e $\overline{1}$ funciona como elemento neutro da multiplicação em $\mathbb{Z}_4$. Além disso, diferentemente do que acontece com a multiplicação de números inteiros, temos a possibilidade de a multiplicação de duas classes diferentes de $\overline{0}$ resultar em $\overline{0}$. De fato, temos $\overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$.

Note também que $\overline{3} \cdot \overline{3} = 1$. Por isso, dizemos que 3 é igual ao seu próprio **inverso multiplicativo** módulo 4. De modo geral, dizemos que $\overline{b}$ é o **inverso** de $\overline{a}$ se $\overline{a} \cdot \overline{b} = \overline{1}$.

É claro que, qualquer que seja $n > 1$, a classe $\overline{1}$ é sempre igual a seu próprio inverso módulo n; por outro lado, $\overline{0}$ não possui inverso módulo n.

Observando a tabela da multiplicação módulo 4, notamos ainda que $\overline{2}$ não possui inverso, pois na linha dessa classe não aparece $\overline{1}$ como resultado. Logo, as únicas classes que possuem inverso módulo 4 são $\overline{1}$ e $\overline{4}$.

Já em $\mathbb{Z}_5$, temos $\overline{4} + \overline{3} = \overline{7} = \overline{2}$ e $\overline{2} \cdot \overline{3} = \overline{6} = \overline{1}$. Veja, a seguir, as tabelas da adição e multiplicação em $\mathbb{Z}_5$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observando as linhas da tabela da multiplicação em $\mathbb{Z}_5$, podemos notar que os inversos de $\overline{2}$, $\overline{3}$ e $\overline{4}$ são respectivamente iguais a $\overline{3}$, $\overline{2}$ e $\overline{4}$.

Agora, veja a tabela completa da multiplicação em $\mathbb{Z}_{10}$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observando as linhas dessa tabela, percebemos que os inversos de $\overline{3}$, $\overline{7}$ e $\overline{9}$ são respectivamente iguais a $\overline{7}$, $\overline{3}$ e $\overline{9}$. As demais classes não possuem inverso. Veja que 1, 3, 7 e 9 são os números naturais menores do que 10 e que não possuem fatores primos em comum com 10, ou seja, que são relativamente primos com 10.

Vejamos, agora, a tabela das multiplicações em $\mathbb{Z}_{11}$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{10}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{10}$	$\overline{2}$	$\overline{5}$	$\overline{8}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{1}$	$\overline{5}$	$\overline{9}$	$\overline{2}$	$\overline{6}$	$\overline{10}$	$\overline{3}$	$\overline{7}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{4}$	$\overline{9}$	$\overline{3}$	$\overline{8}$	$\overline{2}$	$\overline{7}$	$\overline{1}$	$\overline{6}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{1}$	$\overline{7}$	$\overline{2}$	$\overline{8}$	$\overline{3}$	$\overline{9}$	$\overline{4}$	$\overline{10}$	$\overline{5}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{3}$	$\overline{10}$	$\overline{6}$	$\overline{2}$	$\overline{9}$	$\overline{5}$	$\overline{1}$	$\overline{8}$	$\overline{4}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{10}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{10}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{10}$	$\overline{0}$	$\overline{10}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Na tabela de multiplicações em $\mathbb{Z}_{11}$, podemos observar que todas as classes possuem inverso, exceto $\overline{0}$.

Como você já deve ter notado, a existência do inverso multiplicativo de uma classe de restos $\overline{a}$, módulo n, está fortemente ligada ao fato de os números inteiros a e n não possuírem fatores primos em comum. Mais precisamente, temos a seguinte

Proposição 1. *Sejam a e n inteiros, com $n > 1$. Então, $\overline{a}$ possui inverso multiplicativo módulo n se, e somente se,* $\text{mdc}\,(a,n) = 1$.

Prova. Invocaremos um importante resultado visto no módulo "Algoritmo de Euclides Estendido, Relação de Bézout e Equações Diofantinas": sejam p e q números inteiros. Então $\text{mdc}\,(p,q) = 1$ se, e somente se, existe um par de inteiros r e s tal que $pr + qs = 1$.

Assim, se $\text{mdc}\,(a,n) = 1$, então existe um par de inteiros r e s tal que $ar + ns = 1$. Daí, obtemos

$$\begin{aligned}\overline{1} &= \overline{ar + ns}\\ &= \overline{ar} + \overline{ns}\\ &= \overline{a} \cdot \overline{r} + \overline{n} \cdot \overline{s}\\ &= \overline{a} \cdot \overline{r} + \overline{0} \cdot \overline{s}\\ &= \overline{a} \cdot \overline{r}.\end{aligned}$$

Dessa forma, $\overline{r}$ é o inverso de $\overline{a}$.

Por outro lado, admitindo que $\overline{a}$ possua inverso e denotando por $\overline{b}$ essa classe, temos que $\overline{ab} = \overline{a} \cdot \overline{b} = \overline{1}$ módulo n. Desse modo, o produto ab deixa resto 1 quando dividido por n. Assim, $n \mid (ab - 1)$, de sorte que existe c inteiro tal que $ab - 1 = nc$. Portanto, $ab - nc = 1$, donde concluímos que $\text{mdc}\,(a,n) = 1$. □

No que segue, utilizaremos a noção de inverso multiplicativo, módulo n (quando tal inverso existir) para resolver congruências do tipo

$$ax \equiv b (\text{mod}\, n),$$

as quais são denominadas **conguências lineares**. Antes, porém, vamos entender o que significa *resolver* uma congruência desse tipo.

Inicialmente, recordemos a ideia utilizada para resolver uma equação do tipo $ax = b$ em $\mathbb{R}$, em que $a \neq 0$ e b são números reais: multiplicamos os dois lados da igualdade pelo inverso multiplicativo de a para obter

$$\begin{aligned} ax = b &\iff a^{-1}ax = a^{-1} \cdot b \\ &\iff 1 \cdot x = \frac{b}{a} \\ &\iff x = \frac{b}{a}. \end{aligned}$$

Assim $x = \frac{b}{a}$ é a única solução da equação $ax = b$. Também podemos resolver eessa equação da seguinte maneira:

$$\begin{aligned} ax = b &\iff ax = 1 \cdot b \\ &\iff ax = a \cdot a^{-1} \cdot b \\ &\iff \cancel{a}x = \cancel{a} \cdot a^{-1} \cdot b \\ &\iff x = a^{-1} \cdot b \\ &\iff x = \frac{b}{a}. \end{aligned}$$

Essa estratégia é conhecida como "Lei do cancelamento", ferramenta bastante utilizada para resolver problemas que envolvem equações com coeficientes reais. Por exemplo, para resolver a equação $2x = 6$, podemos escrever $2x = 2 \cdot 3$ e aplicar a lei do cancelamento para obter

$$\cancel{2}x = \cancel{2} \cdot 3 \iff x = 3.$$

De modo similar, resolver a congruência $ax \equiv b (\mathrm{mod}\, n)$, em que a, b e $n > 0$ são números inteiros, significa encontrar os números inteiros x que satisfazem essa congruência, ou seja, $\overline{ax} = \overline{b}$ modulo n.

Entretanto, se encontrarmos uma solução, teremos, de fato, uma infinidade delas, pois se $ax_1 \equiv b (\mathrm{mod}\, n)$, então $ax_2 + \kappa n \equiv b (\mathrm{mod}\, n)$, $\forall \kappa \in \mathbb{Z}$.

Assim, para que os números inteiros x_1 e x_2 representem soluções *diferentes* de $ax \equiv b (\mathrm{mod}\, n)$, devemos ter $\overline{x_1} \neq \overline{x_2}$, ou seja, $x_1 \not\equiv x_2 (\mathrm{mod}\, n)$.

Ao tentar resolver a congruência linear $2x \equiv 8 (\mathrm{mod}\, 6)$ utilizando a lei do cancelamento, *obteríamos*

$$2x \equiv 8 (\mathrm{mod}\, 6) \iff \cancel{2}x \equiv \cancel{2} \cdot 4 (\mathrm{mod}\, 6) \iff x \equiv 4 (\mathrm{mod}\, 6).$$

De fato, qualquer número inteiro que seja congruente a 4 módulo 6 é solução de $2x \equiv 8 (\mathrm{mod}\, 6)$, pois, utilizando as propriedades das congruências apresentadas no material anterior, temos que

$$\begin{aligned} x \equiv 4 (\mathrm{mod}\, 6) &\implies 2x \equiv 2 \cdot 4 (\mathrm{mod}\, 6) \\ &\implies 2x \equiv 8 (\mathrm{mod}\, 6). \end{aligned}$$

O problema aqui é que $x \equiv 4 (\mathrm{mod}\, 6)$ não é a única solução da congruência $2x \equiv 8 (\mathrm{mod}\, 6)$. De fato, utilizando as propriedades das congruências, temos

$$\begin{aligned} x \equiv 7 (\mathrm{mod}\, 6) &\implies 2x \equiv 2 \cdot 7 (\mathrm{mod}\, 6) \\ &\implies 2x \equiv 14 (\mathrm{mod}\, 6) \\ &\implies 2x \equiv 8 (\mathrm{mod}\, 6). \end{aligned}$$

Desse modo, diferentemente do que acontece com as equações lineares, a lei do cancelamento não se aplica às congruências lineares. Entretanto, podemos utilizar a proposição 1, para resolver congruências do tipo $ax \equiv b (\mathrm{mod}\, n)$, quando $\mathrm{mdc}\,(a,n) = 1$. Com efeito, se $\overline{a}$ possui inverso multiplicativo, digamos $\overline{c}$, então

$$\begin{aligned} ax \equiv b (\mathrm{mod}\, n) &\iff \overline{ax} = \overline{b} \\ &\iff \overline{a} \cdot \overline{x} = \overline{b} \\ &\iff \overline{c} \cdot \overline{a} \cdot \overline{x} = \overline{c} \cdot \overline{b} \\ &\iff \overline{1} \cdot \overline{x} = \overline{c} \cdot \overline{b} \\ &\iff \overline{x} = \overline{bc}. \end{aligned}$$

Perceba que os cálculos que fizemos acima escondem uma lei do cancelamento em $\mathbb{Z}_n$. Realmente, observando-os com

atenção, podemos concluir que

$$\begin{aligned} ax \equiv b (\mathrm{mod}\, n) &\iff \overline{ax} = \overline{b} \\ &\iff \overline{a} \cdot \overline{x} = \overline{1} \cdot \overline{b} \\ &\iff \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{c} \cdot \overline{b} \\ &\iff \overline{\not{a}} \cdot \overline{x} = \overline{\not{a}} \cdot \overline{c} \cdot \overline{b} \\ &\iff \overline{1} \cdot \overline{x} = \overline{c} \cdot \overline{b} \\ &\iff \overline{x} = \overline{bc}. \end{aligned}$$

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores proponham aos alunos a tarefa de construir tabelas com as operações de adição e multiplicação de outros sistemas completos de restos, por exemplo, $\mathbb{Z}_7$ e $\mathbb{Z}_8$. É importante que os alunos saibam quais são as classes que possuem inverso multiplicativo. O estudo desses casos particulares facilita o entendimento da proposição 1.

As referências a seguir contém mais sobre classes de resíduos e suas aplicações.

Sugestões de Leitura Complementar

1. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, terceira edição. Rio de Janeiro, SBM, 2022.

2. D. Fomim, S. Genkin e I. Itenberg. *Círculos Matemáticos: A Experiência Russa.* Rio de Janeiro, IMPA 2012.