Aritmética Modular

Carlos Henrique

Setembro 2025

1 Introdução

A Aritmética é o estudo das operações básicas da matématica: adição, subtração, multiplicação e divisão. Uma observação, no final, multiplicação e divisão são derivações de adição e subtração. Portanto, quando falamos de aritmética, estamos nos referindo a literalmente a base das operações que conhecemos.

$$\begin{aligned} 2+2=4 \qquad & 2-2=0 \\ 2*3=6 \qquad & \frac{6}{2}=3 \end{aligned} \tag{1}$$

1.1 Teoria dos números inteiros

Uma área estudada com frequência na teoria dos números, é o conjunto dos números inteiros, ou seja $x \in \mathbf{Z}$. É nessa área que surgiu os algoritmos de euclides, relação de berzout, identidade berzout, aritmética modular, estudo dos números primos e muito mais. Hoje vamos falar apenas sobre a aritmética modular.

1.2 Divisão euclidiana

Quando estamos falando da operação de divisão com os números inteiros, estamos falando de uma divisão euclidiana, ou seja:

$$a = bq + r \tag{2}$$

Onde:

$$(a, b) \in \mathbf{Z}, b \neq 0, r \geq 0 \tag{3}$$

Isso é muito usado pra analise combinatoria, achar *mdc* e muito mais. No entanto, quando queremos mexer apenas com o resto dessas operações, entramos na aritmética modular, ou o famoso:

$$9 \mod 10 = 9 \tag{4}$$

2 Aritmética Modular

Quando falamos de aritmética modular, estamos falando do resto das divisões euclidianas. No entanto, deve-se seguir algumas regras para que seja uma operação válida.

- a e b devem percenter ao conjunto dos números inteiros
- b não pode ser zero. Isso será demonstrado ao decorrer desse post.
- r deve ser maior ou igual a 0, não podendo ser número negativo.

2.1 Por quê b não pode ser 0?

Isso na verdade é um dos principais problemas da matemática, a divisão por 0 (e também é uma das coisas que as pessoas mais erram). Portanto, vou repetir aqui de uma vez por todas: $\frac{a}{0}$ NÃO É 0. Quando você diz que um número dividido por 0, é 0, você gera uma falha na lógica algebrica da matemática que possibilita provar que 2 = 1 por exemplo. No entanto, uma simples demonstração é essa:

$$\begin{aligned} \frac{2}{0} &= a \\ 0\frac{2}{0} &= 0a \\ 2 = 0 * a &\to \nexists a \end{aligned} \tag{5}$$

Chegando nessa equação, eu te pergunto, que número vezes 0 que da 2? Não existe. Portanto, dividir por 0 não existe.

2.2 Por quê r tem que ser maior ou igual a 0

Essa na verdade é a mais simples de se demonstrar. Caso r seja menor que 0, ou seja, ele ser negativo, as equações ali para chegar nos termos da divisão euclidiana, param de funcionar. Uma vez que a natureza do resto é ser literalmente o resto. Ou seja, o que sobra, o que entra em conflito com o divisor.

2.3 Como resolver operações de módulo?

Isso é bem simples, basta dividir, o que sobrar é literalmente o resto. Uma das formas é fazer por equação também, dessa forma:

$$35 \mod 10$$

$$\begin{aligned} a &= bq + r \\ a = 35, b = 10, q = 3, r &=? \\ (35) &= (10)(3) + r \\ 35 &= 30 + r \\ 35 - 30 &= r \\ 5 &= r \\ 35 \mod 10 &= 5 \end{aligned} \tag{6}$$

Ou até mesmo com número negativo. No entanto, nesse caso eu vou primeiro fazer da forma errada:

$$-35 \mod 10$$

$$\begin{aligned} a &= bq + r \\ a = -35, b = 10, q = 3, r &=? \\ (-35) &= 10(3) + r \\ -35 &= 30 + r \\ -35 - 30 &= r \\ -65 &= r \end{aligned} \tag{7}$$

É literalmente impossivel $r = -65$ ser verdade. Outra forma errada de se fazer também é essa:

$$-35 \mod 10$$

$$\begin{aligned} a = -35, b = 10, q = -3, r =? \\ (-35) = 10(-3) + r \\ -35 = -30 + r \\ -35 + 30 = r \\ -5 = r \end{aligned} \tag{8}$$

Isso ainda está errado porque isso tem que ser verdade $r \geq 0$. Portanto, o correto é achar um quociente que multiplica o divisor, que vai dar um número que torne o $r \geq 0$ e nesse caso é o 4.

$$-35 \mod 10$$

$$\begin{aligned} a = -35, b = 10, q = -4, r =? \\ -35 = 10(-4) + r \\ -35 = -40 + r \\ -35 + 40 = r \\ 5 = r \end{aligned} \tag{9}$$

Agora sim está correto.

2.4 Congruência

Quando essa igualdade acontece:

$$a \mod b = c \mod b$$

Dizemos que a é congruente á c. Ou seja:

$$a \equiv c \pmod b$$

Existem algumas formas de verificar se essa congruência é verdadeira. A primeira delas e a mais simples (e mais manual) é fazendo a operação de modulo de cada um dos lados, por exemplo:

$$13 \equiv 1 \pmod{12}$$

$$\begin{aligned}
13 \mod 12 = 1 &\mod 12 \\
13 &\mod 12 \\
a &= bq + r \\
13 &= 12(1) + r \\
13 &= 12 + r \\
13 - 12 &= r \\
1 &= r \\
\\
1 &\mod 12 \\
1 &= 12(0) + r \\
1 &= 0 + r \\
1 &= r
\end{aligned} \tag{10}$$

Portanto, essa congruência é verdadeira. No entanto, esse método é manual e leva um bom tempo se você estiver trabalhando com números muito grandes.

A segunda maneira é essa:

$$m|(a-b) \to a \equiv b \pmod{m} \tag{11}$$

É verificar se $(a-b)$ é multiplo do modulo m.

2.5 Demonstração da verificação por multiplo

O teorema que queremos demonstrar é esse:

$$a \equiv b \pmod{m} \iff m|(a-b)$$

Portanto, precisamos provar duas coisas:

- Se a e b têm o mesmo resto, então m divide $(a-b)$.