Material Teórico - Módulo Aritmética dos Restos

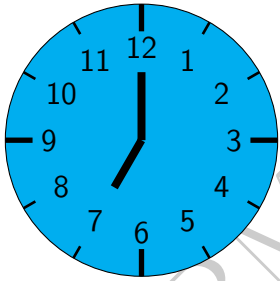
Aritmética Modular - Parte 1

Tópicos Adicionais

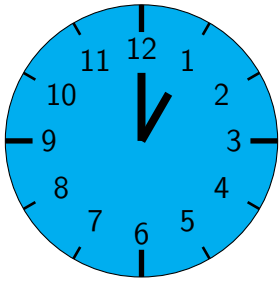
Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

24 de março de 2023

Em algum momento você já se deparou uma igualdade do tipo "$7 + 6 = 1$"? Em que contexto uma igualdade como essa faz sentido? Ao longo deste material, veremos que igualdades como a que foi apresentada acima fazem sentido quando estivermos tratando da "Aritmética dos Restos". Para iniciar, observe o relógio abaixo, que marca o início das aulas na escola de Joaquim.



Agora, imagine que o pai de Joaquim, após deixar o filho na escola no horário marcado no relógio, retorna para buscá-lo exatamente 6 horas depois. Qual o horário do retorno do pai de Joaquim à escola? É claro que, uma vez que o pai retorna 6 horas depois, o resultado da soma $7 + 6$ é o horário do seu retorno. Assim, ele retorna às $7 + 6 = 13$ horas. Entretanto, veja, na próxima figura, o horário que o relógio da escola está marcando no momento do retorno.



Isso acontece porque relógios desse tipo marcam, no máximo, 12 h. Assim, para um horário superior a 12 h, o

relógio marca a diferença entre esse horário e 12 h. Portanto, nesse contexto, a igualdade $7 + 6 = 1$ faz sentido. Para diferenciar a igualdade em $7 + 6 = 1$ da igualdade usual, escrevemos $7 + 6 \equiv 1 \pmod{12}$, que é lida como "sete mais seis é congruente a um módulo doze". A seguir, apresentamos uma definição formal para a ideia de congruência que vimos acima.

Definição 1. *Sejam a, b e n inteiros, com $n > 0$. Dizemos que a é **congruente** a b **módulo** n se $n \mid (a-b)$. Nesse caso, escrevemos $a \equiv b \pmod{n}$.*

Por exemplo, temos $13 \equiv 1 \pmod{12}$, pois $12 \mid (13 - 1)$ e $19 \equiv 3 \pmod{8}$, pois $8 \mid (19 - 3)$. Listamos, na proposição abaixo, algumas propriedades das congruências de números.

Proposição 2. *Sejam a, b, c e n números inteiros com $n > 0$. Então*

(*i*) $a \equiv a \pmod{n}$.

(*ii*) *Se* $a \equiv b \bmod n$), *então* $b \equiv a \pmod{n}$.

(*iii*) *Se* $a \equiv b \pmod{n}$) *e* $b \equiv c \pmod{n}$, *então* $a \equiv c \pmod{n}$.

(*iv*) *Se* $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$, *então* $a + c \equiv b + d \pmod{n}$ *e* $ac \equiv bd \pmod{n}$.

Prova.

(i) Como $m > 0$ temos que $m \mid (a - a)$, logo, $a \equiv a \pmod{n}$.

(ii) Se $a \equiv b \pmod{n}$, então $m \mid (a - b)$. Assim, como $b - a = -(a - b)$, temos que $m \mid (b - a)$, ou seja, $b \equiv a \pmod{n}$.

(iii) Se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $n \mid (a - b)$ e $n \mid (b - c)$. Logo, $n \mid [(a - \cancel{b}) + (\cancel{b} - c)]$. Daí, obtemos $n \mid (a - c)$, ou seja, $a \equiv c \pmod{n}$.

(iv) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $n \mid (a - b)$ e $n \mid (c - d)$. Daí, obtemos $n \mid [(a - b) + (c - d)]$. Mas

$(a-b)+(c-d) = a-b+c-d = (a+c)-(b+d)$, assim, $n \mid [(a+c)-(b+d)]$, ou seja,

$$a + c \equiv b + d \pmod{n}.$$

Agora, perceba que

$$\begin{aligned} ac - bd &= ac - ad + ad - bd \\ &= a(c-d) + d(a-b). \end{aligned}$$

Daí, concluímos que $n \mid (ac - bd)$, ou seja,

$$ac \equiv bd \pmod{n}$$

□

Observação 3. *Por satisfazer as propriedades (i), (ii) e (iii) da proposição 2, dizemos que a relação de congruência entre dois números inteiros é* ***reflexiva***, ***simétrica*** *e* ***transitiva***, *respectivamente. Por isso, dizemos que a relação de congruência é uma* ***relação de equivalência*** *em* $\mathbb{Z}$.

Corolário 4. *Nas condições da proposição 2, se* $a \equiv b (\mathrm{mod}\, n)$, *então* $a + c \equiv b + c (\mathrm{mod}\, n)$ *e* $ac \equiv bc (\mathrm{mod}\, n)$.

Prova. Basta notar que $c \equiv c (\mathrm{mod}\, n)$, para c,n inteiros, com $n > 1$. □

Proposição 5. *Sejam* a, b, c *e* $n > 0$ *inteiros. Se* $ac \equiv bc (\mathrm{mod}\, n)$, *então* $a \equiv b (\mathrm{mod}\, \frac{n}{d})$, *em que* $d = \mathrm{mdc}\,(c,n)$.

Prova. Se $ac \equiv bc (\mathrm{mod}\, n)$, então $n \mid (ac - bc)$. Logo, existe q inteiro, tal que $ac - bc = c(a-b) = qn$. Dividindo ambos os membros dessa igualdade por d, obtemos $\frac{c}{d}(a-b) = q \cdot \frac{n}{d}$. Daí, $\frac{n}{d} \mid \left[\frac{c}{d}(a-b)\right]$. Como $\mathrm{mdc}\,(\frac{c}{d}, \frac{n}{d}) = 1$, concluímos que $\frac{n}{d} \mid (a-b)$, ou seja, $a \equiv b (\mathrm{mod}\, \frac{n}{d})$. □

Se $d = \mathrm{mdc}\,(c,n) = 1$, então obtemos o seguinte corolário da proposição 5, que funciona como uma espécie de lei do cancelamento para as congruências.

Corolário 6. *Sejam a, b, c e $n > 0$ inteiros, tais que* $\mathrm{mdc}\,(c,n) = 1$. *Se $ac \equiv bc (\mathrm{mod}\, n)$, então $a \equiv b (\mathrm{mod}\, n)$.*

Proposição 7. *Sejam a, b, $n > 0$ e $m > 0$ inteiros. Se $a \equiv b (\mathrm{mod}\, n)$, então $a^m \equiv b^m (\mathrm{mod}\, n)$.*

Prova. Se $a \equiv b (\mathrm{mod}\, n)$, então $n \mid (a - b)$. Utilizando a identidade algébrica

$$a^m - b^m = (a-b)\left(a^{m-1} + a^{m-2}b + \ldots + ab^{m-1} + b^{m-1}\right),$$

concluímos que se $n \mid (a - b)$, então $n \mid (a^m - b^m)$. Daí, obtemos $a^m \equiv b^m (\mathrm{mod}\, n)$. □

A seguir, vamos utilizar as propriedades apresentadas nas proposições acima para resolver alguns problemas interessantes.

Exemplo 8. *Encontre o resto na divisão de 8^{2023} por 7.*

Solução. Perceba que $7 \mid (8 - 1)$, logo, $8 \equiv 1 (\mathrm{mod}\, 7)$. Utilizando a proposição 7, obtemos $8^{2023} \equiv 1^{2023} (\mathrm{mod}\, 7)$, ou seja, $8^{2023} \equiv 1 (\mathrm{mod}\, 7)$. Assim, $7 \mid \left(8^{2023} - 1\right)$. Portanto, existe q inteiro, tal que $8^{2023} - 1 = 7q$. Mas isso implica $8^{2023} = 7q + 1$. Por unicidade, concluímos que 1 é o resto na divisão de 8^{2023} por 7. □

Observação 9. *No exemplo 8, concluímos que 1 é o resto na divisão de 8^{2023} por 7 a partir da congruência $8^{2023} \equiv 1 (\mathrm{mod}\, 7)$. Podemos repetir o argumento de unicidade para garantir que se $a \equiv r (\mathrm{mod}\, n)$ e $0 \leq r < n$, então r é o resto na divisão de a por n.*

Exemplo 10. *Encontre o resto na divisão de 8^{2023} por 9.*

Solução. Temos que $8 \equiv -1 (\mathrm{mod}\, 9)$, pois $8 - (-1) = 9$. Portanto, fazendo usso da proposição 7, obtemos

$$8^{2023} \equiv (-1)^{2023} (\mathrm{mod}\, 9) \Longrightarrow 8^{2023} \equiv -1 (\mathrm{mod}\, 9).$$

Mas $-1 \equiv 8 (\mathrm{mod}\, 9)$, logo, utilizando o item (iii) da proposição 2, obtemos $8^{2023} \equiv 8 (\mathrm{mod}\, 9)$. Portanto, o resto na divisão de 8^{2023} por 9 é igual a 8. □

Podemos repetir as ideias utilizadas nos exemplos 8 e 10 para provar a seguinte peoposição.

Proposição 11. *Sejam n e k inteiros positivos. Então*

(*i*) $(n+1)^k$ *deixa sempre resto* 1 *quando dividido por* n.

(*ii*) *Se k é par, então $(n-1)^k$ deixa resto* 1 *quando dividido por n e, se k é ímpar, então $(n-1)^k$ deixa resto $n-1$ quando dividido por n.*

Prova. Temos que $n+1 \equiv 1 (\mathrm{mod}\, n)$, pois $(n+1)-1 = n$. Logo, utilizando a proposição 7, obtemos.

$$(n+1)^k \equiv 1^k \pmod{n} \Longrightarrow (n+1)^k \equiv 1 \pmod{n}.$$

Portanto, o resto na divisão de $(n+1)^k$ por n é igual a 1. Também temos que $n-1 \equiv -1 (\mathrm{mod}\, n)$, pois $(n-1)-(-1) = n$. Agora, recorde que $(-1)^k = 1$, se k é par e $(-1)^k = -1$, se k é ímpar. Assim, se k é par, podemos utilizar a proposição 7 para obter

$$(n-1)^k \equiv (-1)^k \pmod{n} \Longrightarrow (n-1)^k \equiv 1 \pmod{n}.$$

Daí, $(n-1)^k$ deixa resto 1 quando dividido por n. Por outro lado, se n é ímpar, então

$$(n-1)^k \equiv (-1)^k \pmod{n} \Longrightarrow (n-1)^k \equiv -1 \pmod{n}.$$

Como $-1 \equiv n-1 (\mathrm{mod}\, n)$, por transitividade, obtemos $(n-1)^k \equiv n-1 (\mathrm{mod}\, n)$. Logo, o resto na divisão de $(n-1)^k$ por n é $n-1$. □

Exemplo 12. *Mostre que $62^{2023} + 41^{2022}$ é divisível por* 21.

Solução. Inicialmente, veja que $62 \equiv -1 \pmod{21}$, pois $62-(-1) = 63$ e $21 \mid 63$. Além disso, $41 \equiv -1 \pmod{21}$, pois $41-(-1) = 42$ e $21 \mid 42$. Desse modo, utilizando a proposição 7, obtemos

$$62^{2023} \equiv (-1)^{2023} \pmod{21} \Longrightarrow 62^{2023} \equiv -1 \pmod{21}$$

e

$$41^{2022} \equiv (-1)^{2022} \pmod{21} \Longrightarrow 41^{2022} \equiv 1 \pmod{21}.$$

Agora, utilizando o item (iv) da proposição 2, obtemos

$$62^{2023} + 41^{2022} \equiv -1 + 1 \pmod{21}$$

$$\Longrightarrow 62^{2023} + 41^{2022} \equiv 0 \pmod{21}.$$

Desse modo, concluímos que $62^{2023} + 41^{2022}$ é divisível por 21. □

Considere um número inteiro positivo n. Quando dividimos um inteiro qualquer m por n, encontramos únicos quociente q e resto r, inteiros, tais que r é um elemento do conjunto $R = \{0,1,2,\ldots,n-1\}$. Para cada $r \in R$, podemos pensar no conjunto $\overline{r}$ dos inteiros que deixam resto r quando divididos por n. Os conjuntos $\overline{r}$ são denominados **classes de resíduos** módulo n. Perceba que qualquer número inteiro pertence a algum conjunto $\overline{r}$ e, além disso, um número inteiro não pode pertencer a dois desses conjuntos, pois o resto na divisão por n é único. Por satisfazer essas propriedades, dizemos que R é um **sistema completo de resíduos** módulo n. Utilizamos a notação $\mathbb{Z}_n$ para representar o conjunto das classes de resíduos módulo n. Assim, temos

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

Agora, considere o problema abaixo.

Exemplo 13. *De quantos modos é possível comprar selos que custam R$* 10,00 *e R$* 14,00 *gastando exatamente* 100 *reais?*

Solução. Vamos denotar por x a quantidade de selos que custam R$ 10,00 e por y a quantidade de selos que custam R$ 14,00. Como devem ser gastos exatamente 100 reais, obtemos a equação diofantina linear

$$10x + 14y = 100.$$

Dividindo os dois membros da equação acima por 2, obtemos a equação (equivalente)

$$5x + 7y = 50.$$

Veja que $5x$ e 50 são ambos múltiplos de 5, logo, temos que $5x \equiv 0 \pmod 5$ e $50 \equiv 0 \pmod 5$. Daí, obtemos $7y \equiv 0 \pmod 5$ ou, de outro modo, $7y \equiv 7 \cdot 0 \pmod 5$. Agora, como $\text{mdc}\,(7,5) = 1$, podemos cancelar o 7 na congruência anterior para obter $y \equiv 0 \pmod 5$. Daí, concluímos que y deve ser múltiplo de 5. Se $y = 0$, então a quantidade de selos de R$ 10,00 deve ser $100 \div 10 = 10$ e, se $y = 5$, então a quantidade de selos de R$ 10,00 deve ser $(100 - 5 \cdot 14) \div 10 = 3$. □

Observação 14. *É claro que o exemplo 13 pode ser resolvido de um modo bem mais elementar, sem apelar para a ideia de congruência. Entretanto, optamos por resolvê-lo desse modo para abordar um assunto que estudaremos nas próximas aulas: como resolver congruências lineares do tipo* $ax \equiv b (\text{mod}\, n)$.

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores deixem os alunos refletirem sobre os exemplos apresentados por alguns minutos, antes de explicarem as soluções. Ressaltamos a importância de que os alunos tentem encontrar as soluções por meios próprios. Por outro lado, ainda que eles não as encontrem, ou apresentem uma solução errada, esse processo é fundamental para a aprendizagem.

Idealmente, apresente aos alunos outros exemplos que possam ser resolvidos com as técnicas utilizadas nos exemplos 8, 10 e 12. As referências listas a seguir contém vários deles.

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.