Ciclo 5 – Encontro 1

A ARITMÉTICA DOS RESTOS

Nível 3
PO: Márcio Reis
11º Programa de Iniciação Científica Jr.

A aritmética dos restos

- Apostila 1: INICIAÇÃO À ARITMÉTICA, de Abramo Hefez.

  Seções 4.1 a 4.4:

  Congruências;

  Critérios de multiplicidade e restos;

  Congruências e somas;

  Congruências e produtos.

Congruências

Vamos agora introduzir a grande ideia de Gauss de desenvolver uma aritmética dos restos da divisão por um certo número fixado, o que já foi explorado nas Seções 2.2 e 2.3.

Definição. Seja dado um número inteiro m maior do que 1. Diremos que dois números inteiros a e b são *congruentes módulo* m se a e b possuírem mesmo resto quando divididos por m. Neste caso, simbolizaremos esta situação como segue:

$$a \equiv b \mod m.$$

Quando a e b não são congruentes módulo m, escreve-se

$$a \not\equiv b \mod m.$$

Congruências

Exemplos:

1) $15 \equiv 8 \bmod 7$, pois o restos das divisões de 15 e de 8 por 7 são os mesmos (iguais a 1).

2) $27 \equiv 32 \bmod 5$, pois os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2).

3) $31 \not\equiv 29 \bmod 3$, pois o resto da divisão de 31 por 3 é 1, enquanto o resto da divisão de 29 por 3 é 2.

Congruências

Demonstração. De fato, pelo algoritmo da divisão, podemos escrever

$$a = mq_1 + r_1 \quad \text{e} \quad b = mq_2 + r_2,$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor que $r_1 \leq r_2$ (se o contrário ocorrer, basta trocar os papéis de r_1 e r_2). Assim, podemos escrever

$$b - a = m(q_2 - q_1) + r_2 - r_1.$$

Logo, m divide $b - a$ se, e somente se, m divide $r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide $b - a$ se e somente se $r_2 - r_1 = 0$, ou seja, se e somente se $r_2 = r_1$. □

Congruências

Problema 4.1. Verifique se são verdadeiras ou falsas as seguintes afirmações:

$35 \equiv 27 \bmod 4$; $72 \equiv 32 \bmod 5$; $83 \equiv 72 \bmod 5$; $78 \equiv 33 \bmod 9$.

Problema 4.2. Se $a \equiv b \bmod 4$, mostre que $a \equiv b \bmod 2$.

Problema 4.3. Mostre que $10^n \equiv 1 \bmod 9$, para todo número natural n.

Congruências

Problema 4.1. Verifique se são verdadeiras ou falsas as seguintes afirmações:

$$35 \equiv 27 \bmod 4; \quad 72 \equiv 32 \bmod 5; \quad 83 \equiv 72 \bmod 5; \quad 78 \equiv 33 \bmod 9.$$

35 por 4: resto 3; 27 por 4: resto 3 – VERDADEIRO
72 por 5: resto 2; 32 por 5: resto 2 – VERDADEIRO
83 por 5: resto 3; 72 por 5: resto 2 – FALSO
78 por 9: resto 6; 33 por 9: resto 6 – VERDADEIRO

Congruências

Problema 4.2. Se $a \equiv b \bmod 4$, mostre que $a \equiv b \bmod 2$.

$$a \equiv b \; mod \; 4 \Rightarrow 4 \mid b - a$$

$$a \equiv b \; mod \; 4 \Rightarrow 2 \times 2 \mid b - a$$

$$\Rightarrow 2 \mid b - a \Rightarrow a \equiv b \; mod \; 2$$

Congruências

Problema 4.3. Mostre que $10^n \equiv 1 \bmod 9$, para todo número natural n.

$$10^1 - 1 = 9$$
$$10^2 - 1 = 99$$
$$10^3 - 1 = 999$$
$$\ldots$$
$$10^n = 9\ldots9$$
$$9 \mid 10^n - 1 \Rightarrow 10^n \equiv 1 \; mod \; 9$$

Critérios de Multiplicidade e Restos

É fácil determinar o resto da divisão de um inteiro n por 2, pois esse é 0 ou 1, dependendo de n ser par ou ímpar.

Para facilitar a determinação do resto da divisão de um inteiro n por 3 ou por 9, podemos utilizar os conhecimentos já adquiridos, evitando o trabalho de efetuar a divisão em questão.

De fato, sabemos da Seção 2.3 que se $n_r \dots n_1 n_0$ é a escrita de n no sistema decimal, então

$$n - (n_r + \cdots + n_1 + n_0) = (10^r - 1)n_r + \cdots + (10 - 1)n_1.$$

Como o segundo membro da igualdade acima é divisível por 3 e por 9, o mesmo ocorre com o primeiro membro, logo

$$n \equiv (n_r + \cdots + n_1 + n_0) \bmod 3; \text{ e } \bmod 9.$$

Critérios de Multiplicidade e Restos

Assim, pela definição de congruência, temos os seguintes fatos:

O resto da divisão por 3 (*respectivamente por* 9) *de um número* $n = n_r \dots n_1 n_0$, *escrito no sistema decimal, é igual ao resto da divisão por* 3 (*respectivamente por* 9) *do número* $n_r + \cdots + n_1 + n_0$.

Congruências e Somas

Proposição 4.2. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja m um inteiro maior do que 1. Se $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então $a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então m divide $b_1 - a_1$ e divide $b_2 - a_2$. Logo

$$m \text{ divide } (b_1 - a_1) \pm (b_2 - a_2) = (b_1 \pm b_2) - (a_1 \pm a_2),$$

mostrando que $b_1 \pm b_2 \equiv a_1 \pm a_2 \bmod m$. □

Conclui-se que as congruências de mesmo módulo somam-se e subtraem-se membro a membro tal qual as igualdades.

Congruências e Somas

O resto da divisão da soma $a+b$ de dois números a e b por um outro número $m>1$ depende apenas dos restos da divisão de a e de b por m e não desses números em si.

Congruências e Produtos

Proposição 4.3. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja m um inteiro maior do que 1. Se $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então $a_1 \times a_2 \equiv b_1 \times b_2 \bmod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então m divide $a_1 - b_1$ e $a_2 - b_2$. Por outro lado, como

$$a_1 \times a_2 - b_1 \times b_2 = a_1 \times (a_2 - b_2) + b_2 \times (a_1 - b_1),$$

segue que m divide $a_1 \times a_2 - b_1 \times b_2$, o que prova o resultado. □

Congruências e Produtos

O resto da divisão do produto $a \times b$ de dois números a e b por um outro número $m > 1$ depende apenas dos restos da divisão de a e de b por m e não desses números em si.

Exercício 1

Um inteiro é dito um *quadrado perfeito* quando ele é o quadrado de um inteiro. Usando congruências, encontre os possíveis algarismos das unidades de um quadrado perfeito.

Exercício 1 - Solução

Solução: Seja $n = m^2$ um quadrado perfeito, com m inteiro. Tem-se $m \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8$ ou $9 \pmod{10}$. Assim, $n = m^2 \equiv 0, 1, 4, 9, 16, 25, 36, 49, 64$ ou $81 \pmod{10}$. Mas, $16 \equiv 6 \pmod{10}$, $25 \equiv 5 \pmod{10}$, $36 \equiv 6 \pmod{10}$, $49 \equiv 9 \pmod{10}$, $64 \equiv 4 \pmod{10}$ e $81 \equiv 1 \pmod{10}$. Assim, $n = m^2 \equiv 0, 1, 4, 5, 6$ ou $9 \pmod{10}$. Assim, os possíveis algarismos das unidades de um quadrado perfeito são $0, 1, 4, 5, 6$ ou 9.

Exercício 2

Usando congruências, prove que $30^{99} + 61^{100}$ é divisível por 31.

Exercício 2 - Solução

Solução: Como $30^{99} + 61^{100} \equiv (-1)^{99} + (-1)^{100} = -1 + 1 = 0 \pmod{31}$, então $30^{99} + 61^{100}$ é divisível por 31.

Exercício 3

Usando congruências, encontre o resto da divisão do número $10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10.000.000.000}$ por 7.

Exercício 3 - Solução

Solução: Tem-se $10^{10} \equiv 3^{10} = (3^3)^3 \cdot 3 = 27^3 \cdot 3 \equiv (-1)^3 \cdot 3 = -3 \pmod 7$, $10^{100} = (10^{10})^{10} \equiv (-3)^{10} = 3^{10} \equiv -3 \pmod 7$, $10^{1000} = (10^{100})^{10} \equiv (-3)^{10} = 3^{10} \equiv -3 \pmod 7$; em geral, $10^{10^n} \equiv -3 \pmod 7$, para todo n inteiro positivo. Assim, $10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10.000.000.000} \equiv (-3) + (-3) + \cdots + (-3) = 10 \cdot (-3) = -30 \equiv 5 \pmod 7$ e, logo, o resto da divisão de $10^{10} + 10^{100} + 10^{1000} + \cdots + 10^{10.000.000.000}$ por 7 é igual a 5.

Exercício 3 – Solução 2

(*Maneira alternativa de mostrar que* $10^{10^n} \equiv -3\ (mod\ 7)$, *para todo* n *inteiro positivo*: Seja n um inteiro positivo. Como $10^n \equiv 0^n = 0 \equiv 4\ (\mathrm{mod}\ 2)$ e $10^n \equiv 1^n = 1 \equiv 4\ (\mathrm{mod}\ 3)$, então $10^n - 4$ é múltiplo de 2 e de 3 e, logo, $10^n - 4$ é múltiplo de $\mathrm{mmc}(2,3) = 6$, ou seja, $10^n \equiv 4\ (\mathrm{mod}\ 6)$, isto é, $10^n = 6q + 4$, para algum inteiro q. Assim, $10^{10^n} = 10^{6q+4} = (10^6)^q \cdot 10^4 \equiv (3^6)^q \cdot 3^4 = ((3^3)^2)^q \cdot 81 = (27^2)^q \cdot 81 \equiv ((-1)^2)^q \cdot (-3) = 1 \cdot (-3) = -3\ (\mathrm{mod}\ 7)$).

Exercício 4

Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine os restos da divisão de $a+b$, $a-b$ e de $b-a$ por 7

SUGESTÃO: Para o último resto, observe que $-4 \equiv 3 \bmod 7$.

Exercício 4 - Solução

$$a \ por \ 7 : resto \ 6$$
$$b \ por \ 7 : resto \ 2$$
$$a + b \equiv 6 + 2 \mod 7 = 1$$
$$a - b \equiv 6 - 2 \mod 7 = 4$$
$$b - a \equiv 2 - 6 \mod 7 = 3$$

Exercício 5

Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine o resto da divisão de $a \times b$ por 7.

Exercício 5 - Solução

$$a\ por\ 7 : resto\ 6$$
$$b\ por\ 7 : resto\ 2$$
$$a \times b \equiv 6 \times 2 \mod 7 = 5$$

Exercício 6

Sejam a, b, c e m números inteiros e com $m > 1$. Mostre que se $a \times c \equiv b \times c \bmod m$ e se $\text{mdc}(c, m) = 1$, então $a \equiv b \bmod m$.

Exercício 6 - Solução

$$Se\ a \times c \equiv b \times c\ mod\ m$$
$$\Rightarrow m \mid b \times c\ -\ a \times c$$
$$\Rightarrow m \mid c(b-a)$$
$$\Rightarrow (1)\ m \mid c\ , (2)\ m \mid b\ -\ a$$

$$Como\ mdc(c, m) = 1,\ c \nmid m$$

$$\Rightarrow Se\ m \mid b\ -\ a$$
$$\Rightarrow a \equiv b\ mod\ m$$

Estudar para o próximo encontro!

Próximo encontro: 04/11, sexta, às 20h

Módulo: "Princípios Básicos de Contagem"
http://matematica.obmep.org.br/index.php/modulo/ver?modulo=15
Vídeoaulas: "Permutação com Repetição" e "Exercícios de Permutação com Repetição".

Módulo: "Métodos Sofisticados de Contagem"
http://matematica.obmep.org.br/index.php/modulo/ver?modulo=16
Vídeoaulas: "Permutação Circular", "Exercícios sobre Permutação Circular – Parte 1", "Exercícios sobre Permutação Circular – Parte 2", "Exercícios sobre Permutação Circular – Parte 3", "Exercícios sobre Permutação Circular – Parte 4", "Exercícios de Combinação e Permutação Circular – Parte 1" e "Exercícios de Combinação e Permutação Circular – Parte 2".