Semana Olímpica 2019

Profª Ana Paula Chaves

apchaves.math@gmail.com

Nível 1 • Congruência

1. Divisibilidade e Aritmética Modular

Um dos tópicos mais fundamentais da teoria dos números é, sem dúvidas, a *divisão euclidiana*. Dizemos que um inteiro a é *múltiplo* de um outro inteiro b, se existir $n \in \mathbb{Z}$, tal que $a = nb$. Por exemplo, 15 é múltiplo de 5, enquanto 7 *não* é múltiplo de 3. No mesmo espírito, se existe um inteiro n tal que $nb = a$, então dizemos que b é um *divisor* (ou *fator*) de a. Assim, 5 é divisor de 15, enquanto 3 não é divisor de 7. Se b é um divisor de a, então a é múltiplo de b, e dizemos que "b divide a", cuja notação é "$b|a$". Caso contrário, dizemos que "b não divide a" e denotamos isso por "$b \nmid a$".

Contudo, como vimos acima, nem sempre é possível efetuar essa divisão sem deixar vestígios. Na grande maioria das vezes, somos deixados com algum *resto* após a divisão (por exemplo, dividindo 10 por 3, obtemos resto 1, enquanto 3 cópias de 3 se encaixam perfeitamente no 9). Esse resto é encontrado através do famoso *algoritmo da divisão de Euclides*, que descrevemos abaixo:

Algoritmo de Euclides 1. Dados dois inteiros a e b, com $b > 0$, existe um único par de inteiros p e q tais que

$$a = qb + r,$$

com $0 \leq r < b$ ($r = 0 \Leftrightarrow b|a$). Dizemos que q é o *quociente* e r o *resto* da divisão de a por b.

Esse *resto*, é o personagem principal da *aritmética modular*, ou *congruência*:

Definição 2. Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$. Dizemos que a *é congruente a* b *módulo* m, e escrevemos $a \equiv b \ (mod\ m)$, sempre que a e b deixam o mesmo resto na divisão por m.

Por exemplo, $5 \equiv 3 \ (mod\ 2)$ e $48 \equiv 33 \ (mod\ 5)$, pois 5 e 3 deixam resto 1 quando divididos por 2, e 48 e 33 deixam resto 3 quando divididos por 5.

Observação 3. É importante frisar que termos $a \equiv b \ (mod\ m)$, **não** implica que b é o resto da divisão de a por m, mas apenas que a e b deixam o mesmo resto quando divididos por m.

2. Primeiras Propriedades

A seguir, temos uma pequena lista de propriedades inerentes da aritmética modular. Com elas, conseguimos um certo grau de liberdade para realizar operações elementares, semelhante às que realizamos quando temos uma igualdade.

i. Quando divididos por m, cada inteiro possui um <u>único</u> resto no conjunto $\{0, 1, 2, \ldots, m-1\}$. Cada um desses

restos é dito uma *classe de resíduos módulo m*;

ii. $a \equiv b \ (mod\ m)$ é equivalente a $n|a-b$, ou seja, n divide $a-b$;

iii. Se $a \equiv b \ (mod\ m)$ e $p \equiv q \ (mod\ m)$, então $a \pm p \equiv b \pm q \ (mod\ m)$;

iv. Se $a \equiv b \ (mod\ m)$ e $p \equiv q \ (mod\ m)$, então $ap \equiv bq \ (mod\ m)$.

Vamos demonstrar a propriedade **ii.**, pois as demais são consequência imediata desta e deixadas como exercício.

Demonstração: Suponha que $a \equiv b \ (mod\ m)$, ou seja, que os dois deixam o mesmo resto quando divididos por m. Então, efetuando a divisão, temos $a = q_1m + r$ e $b = q_2m + r$, o que nos dá $a - b = (q_1 - q_2)m$, donde $m|a-b$. Agora, suponha que $m|a-b$, ou seja, quando dividimos $a-b$ por m, obtemos resto igual a 0. Pela divisão euclidiana de a e b por m, conseguimos $a = q_1m + r_1$ e $b = q_1m + r_2$, e assim $a - b = (q_1 - q_2)m + (r_1 - r_2)$, e como $a-b$ é divisível por m, bem como $(q_1 - q_2)m$, isso implica que $r_1 - r_2$ também é divisível por m. Porém, sabemos que $-m < r_1 - r_2 < m$, onde o único múltiplo de m deste intervalo é o 0, e com isso $r_1 = r_2$, nos dando $a \equiv b \ (mod\ m)$.

Observação 4. Da propriedade **iv.**, seque que se $a \equiv b \ (mod\ m)$, e tomamos $k \in \mathbb{Z}$ qualquer, isto implica em $ka \equiv kb \ (mod\ m)$, pois $k \equiv k \ (mod\ m)$ é sempre válido. Ainda sob a mesma hipótese, tomando $n \in \mathbb{N}$ qualquer, temos $a^n \equiv b^n \ (mod\ m)$. Para esta última, imagine que estamos usando recursivamente a propriedade **iv.**, fazendo $p = a$ e $q = b$, isto é, multiplicando uma congruência membro a membro, por ela mesma, $n-1$ vezes.

3. Problemas Resolvidos

Exibimos agora, alguns problemas clássicos (e outros nem tanto), com as suas respectivas soluções. O objetivo é aprofundar os conceitos e propriedades que discutimos nas seções anteriores, além, é claro, de compartilhar algumas ideias bacanas.

Problema 1.

Mostre que o resto de um número quando dividido por 9, é o mesmo resto que a soma dos seus dígitos deixa quando também é dividida por 9.

Solução: Digamos que nosso número é N, e que seus dígitos são $d_1, d_2, \ldots, d_k$, de modo que

$$N = d_1 10^{k-1} + d_2 10^{k-2} + \cdots + d_{k-1}10 + d_k.$$

Agora, observe que

$$10 \equiv 1 \ (mod\ 9) \Rightarrow 10^n \equiv 1 \ (mod\ 9),$$

e assim, $d_i 10^{k-i} \equiv d_i \ (mod\ 9)$, para todo $i = 1, 2, \ldots, k$. Somando todas essas congruências, obtemos

$$\begin{aligned} N &\equiv d_1 10^{k-1} + \cdots + d_k \ (mod\ 9) \\ \therefore\ N &\equiv d_1 + \cdots + d_k \ (mod\ 9), \end{aligned}$$

que é exatamente o que queríamos mostrar. □

O problema a seguir é uma aplicação clássica do resultado que mostramos no Problema 1. Originalmente, é o Problema 4 da IMO de 1975, realizada na Bulgária.

Problema 2.

(IMO 1975) **Seja $S(n)$ a soma dos dígitos de n. Se $N = 4444^{4444}$, $A = S(N)$ e $B = S(A)$. Quanto vale $S(B)$?**

Solução: Pelo critério de divisibilidade por 9, sabemos que $N \equiv A \equiv B \ (mod\ 9)$. Primeiro, vamos calcular o resto de N por 9. Como $4444 \equiv 16 \equiv 7 \ (mod\ 9)$, então $4444^{4444} \equiv 7^{4444} (mod\ 9)$, donde precisamos encontrar o resto de 7^{4444}. Note que, $7^2 \equiv 49 \equiv 4 (mod\ 9) \Rightarrow 7^3 \equiv 28 \equiv 1 (mod\ 9)$, donde

$$7^{4444} = 7^{3\cdot 1481+1} = (7^3)^{1481} \cdot 7 \equiv 7 (mod\ 9),$$

$$\therefore\ 7^{4444} \equiv 7 (mod\ 9).$$

Por outro lado, como $N = 4444^{4444} < 10^{5\cdot 4444}$, então $S(N) \geq 5 \cdot 4444 \cdot 4 = 199980$. Além disso, $B = S(A) \leq 1 + 9 \cdot 5 = 46$ e $S(B) \leq 12$. O único inteiro menor ou igual a 12 com resto 7 por 9, é o próprio 7, daí $S(B) = 7$.

Problema 3.

(Russia 2001) **Encontre todos os primos p e q tais que $p + q = (p - q)^3$.**

Solução: Primeiro, note que $(p-q)^3 = p+q \neq 0$, e com isso p e q são dois primos distintos, donde $mdc(p, q) = 1$ e também temos $mdc(p, p+q) = 1$. Agora, note que

$$p - q \equiv (p - q) + (p + q) \ (mod\ p + q)$$

$$\Rightarrow p - q \equiv 2p \ (mod\ p + q)$$

$$\therefore\ \ (p - q)^3 \equiv 8p^3 \ (mod\ p + q).$$

Por outro lado, o problema nos forneceu $(p - q)^3 \equiv 0 \ (mod\ p + q)$, e portanto $8p^3 \equiv 0 \ (mod\ p + q) \Rightarrow p + q \mid 8$, donde a última implicação é consequência de $mdc(p, p + q) = 1$.

Por um argumento análogo, podemos considerar a equação dada, módulo $p - q$:

$$p + q \equiv (p + q) + (p - q) \ (mod\ p - q)$$

$$\Rightarrow p + q \equiv 2p \ (mod\ p - q),$$

e como nos foi dado $p + q \equiv 0 \ (mod\ p - q)$, conseguimos $2p \equiv 0 \ (mod\ p - q)$. Como $mdc(p, q) = 1$, então $mdc(p, p - q) = 1$ e assim $2 \equiv 0 \ (mod\ p-q)$, ou seja $p-q \mid 2$. Concluimos então que os únicos primos p e q que satisfazem $p + q \mid 8$ e $p - q \mid 2$ são 3 e 5.

Problema 4.

Se p, q, s são primos tais que $pqs = 7(p+q+s)$, encontre o valor de $p^2+q^2+s^2$.

Solução: Da igualdade que foi dada, temos que $7|pqs$, e como p, q, s são primos, bem como o 7, um deles deve ser igual à 7. Suponha, sem perda de generalidade, que $p = 7$. Então,

$$7qs = 7(7 + q + s) \Rightarrow qs = 7 + q + s$$

$$\Rightarrow q(s - 1) - s = 7 \Rightarrow (q - 1)(s - 1) = 8.$$

Portanto, pelas possíveis fatorações do 8, as únicas possibilidades para q e s são: $(q, s) = (9, 2), (5, 3), (3, 5)$ e $(2, 9)$, mas dentre elas a únicas que possuem um par de primos são $(3, 5)$ e $(5, 3)$. Portanto, as soluções são (p, q, s) são todas as possíveis permutações de $(3, 5, 7)$, nos dando $p^2 + q^2 + s^2 = 83$.

Problema 5.

Encontre todos os p primos, tais que $2p+1$ e $4p+1$ também são primos.

Solução: Todo primo, exceto 3, é congruente à 1 ou 2 $(mod\ 3)$. Assim, note que $4p+1 \equiv p+1(mod\ 3)$, donde, se ambos p e $4p+1$ são primos, devemos ter $p \equiv 1\ (mod\ 3)$, pois caso contrário, se $p \equiv 2\ (mod\ 3)$, teríamos $4p+1 \equiv 2+1 \equiv 0(mod\ 3)$, o que é um absurdo, já que $4p+1$ é primo. Por outro lado, isso implica que $2p+1 \equiv 0(mod\ 3)$, o que é impossível pois $2p+1$ também é primo. Portanto, nossa única chance de encontrar soluções, é com $p=3$, nos dando $2p+1=7$ e $4p+1=13$, que são de fato primos. Concluímos que $p=3$ é a única solução.

Problema 6.

***(USAJMO 2011)* Encontre todos os inteiros positivos n, tais que $2^n+12^n+2011^n$ é um quadrado perfeito.**

Solução: Vamos analisar a soma $2^n+12^n+2011^n$, módulo 3. Primeiro, temos as seguintes congruências:

$$2011 \equiv 1\ (mod\ 3) \Rightarrow 2011^n \equiv 1\ (mod\ 3);$$

$$12 \equiv 0\ (mod\ 3) \Rightarrow 12^n \equiv 0\ (mod\ 3);$$

$$2 \equiv -1\ (mod\ 3) \Rightarrow 2^n \equiv (-1)^n\ (mod\ 3).$$

Como os quadrados perfeitos módulo 3, são sempre $\equiv 0$ ou $1\ (mod 3)$, então n deve ser ímpar, para que tenhamos $2^n+12^n+2011^n \equiv 1+0+(-1)^n \equiv 0\ (mod\ 3)$. Agora vamos fazer a mesma análise módulo 4, supondo $n>1$. Nesse caso,

$$2011 \equiv -1\ (mod\ 4) \Rightarrow 2011^n \equiv (-1)^n\ (mod\ 3);$$

$$12 \equiv 0\ (mod\ 4) \Rightarrow 12^n \equiv 0\ (mod\ 4);$$

$$\text{e, como } n>1, \text{ temos } 2^n \equiv 0\ (mod\ 4).$$

Juntando essas informações, conseguimos $2^n+12^n+2011^n \equiv 0+0+(-1)^n \equiv -1 \equiv 3\ (mod\ 4)$, onde a penúltima congruência vem de n ser ímpar. Porém, quadrados perfeitos deixam apenas restos 0 ou 1 módulo 4, donde nesse caso $2^n+12^n+2011^n$ não pode ser um quadrado. Portanto, nos resta apenas $n=1$, nos dando $2+12+2011=2025=45^2$.

4. Problemas Propostos

Agora é a sua vez de usar as poderosas ferramentas da congruência. :)

1. Encontre o menor inteiro positivo k, para o qual existe um outro inteiro positivo n tal que 2^n e 2^{n+k} têm a mesma soma de dígitos.

2. Sejam a, b, c três inteiros tais que $7|a^3+b^3+c^3$. Mostre que $7|abc$.

3. Um número N, cujos dígitos são 2,3,4,5,6,9, em alguma ordem, pode ser um quadrado perfeito?

4. Mostre que $3^{2n+1}+2^{n+2}$ é múltiplo de 7 para todo $n \in \mathbb{N}$.

5. Encontre o algarismo das unidades de 7^{7^7}.

6. Mostre que $3^{2n+1} + 2^{n+2}$ é múltiplo de 7 para todo $n \in \mathbb{N}$.

7. (IMO 1964):

(a) Ache todos os inteiros n tais que $7|2^n - 1$

(b) Prove que não existe $n \in \mathbb{N}$, tal que $7|2^n + 1$.

8. Sejam a, b, c inteiros. Mostre que $a^5 + b^5 + c^5 + 5abc(ab + bc + ca)$ é divisível por $a + b + c$.

Referências

[1] T. Andreescu, D. Andrica and Z. Feng, E. Tengan *104 Number Theory Problems*, Birkhauser, Boston, MA, 2007.

[2] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, Projeto Euclides, IMPA, 2010.

[3] E. Carneiro, O. Campos and F. Paiva, *Olimpíadas Cearenses de Matemáatica 1981-2005 (Níveis Júnior e Senior)*, Ed. Realce, 2005.

[4] L. H. Chau, L. H. Khoi, *Selected Problems of the Vietnamese Mathematical Olympiad (1962-2009)*, World Scientific, Danvers MA, 2010.

[5] S. B. Feitosa, B. Holanda, Y. Lima and C. T. Magalhães, *Treinamento Cone Sul 2008*. Fortaleza, Ed. Realce, 2010.

[6] D. Fomin, A. Kirichenko, *Leningrad Mathematical Olympiads 1987-1991*, MathPro Press, Westford, MA, 1994.

[7] D. Fomin, S. Genkin and I. Itenberg, *Mathematical Circles, Mathematical Words, Vol. 7*, American Mathematical Society, Boston, MA, 1966.

[8] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*.