Teoria dos Números: Módulo n

Autor: Luca Zanardi Lamardo

1 Introdução

Neste artigo, veremos os conceitos iniciais da base de toda a teoria dos números: analisar expressões *módulo* n. Resumidamente, é uma maneira de se analisar apenas o que ocorre com o resto de números, quando divididos por n.

A maioria dos problemas de teoria dos números vistos em olimpíadas podem ser reduzidos, de um jeito ou outro, à análise das expressões módulo n. Por isso, é essencial que você aprenda bem essa teoria e pratique até a perfeição.

Definição. Dizemos que dois números inteiros a e b são **congruentes módulo n** quando eles deixam o mesmo resto na divisão por n. A representação matemática será escrita da seguinte maneira: $a \equiv b \pmod{n}$. Uma maneira mais formal de definir isso é dizer que $a \equiv b \pmod{n} \iff n|(a-b)$.

Propriedades. Se temos $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, as seguintes proposições são válidas:
i) $a \pm c \equiv b \pm d \pmod{n}$
ii) $a \cdot c \equiv b \cdot d \pmod{n}$
iii) Se temos $m|n$, então $a \equiv b \pmod{n} \implies a \equiv b \pmod{m}$
iv) $a^k \equiv b^k \pmod{n}, \forall\ k \in \mathbb{Z}_+$

Prova.

i) Veja que isso ocorre $\iff n|(a \pm c) - (b \pm d) \iff n|(a-b) \pm (c-d)$, que ocorre, pois $n|(a-b)\ \&\ n|(c-d) \implies n|(a-b) \pm (c-d)$

ii) Considere a representação de a, b, c, d pelo algoritmo de euclides como

$$\begin{cases} a = n \cdot a_0 + r_1 \\ b = n \cdot b_0 + r_2 \\ c = n \cdot c_0 + r_3 \\ d = n \cdot d_0 + r_4 \end{cases}$$

Como $a \equiv b \pmod{n}$, $r_1 = r_2$, e analogamente, $r_3 = r_4$. Dessa forma,

$$\begin{aligned} a \cdot c &= (n \cdot a_0 + r_1) \cdot (n \cdot c_0 + r_3) \\ &= n \cdot (n \cdot a_0 \cdot c_0 + a_0 \cdot r_3 + c_0 \cdot r_1) + r_1 \cdot r_3 \\ &\equiv r_1 \cdot r_3 \ (mod\ n) \end{aligned}$$

Este último passo é verdade pois $n \cdot k \equiv 0 \ (mod\ n)$, já que $n \mid n \cdot k$.
Analogamente:

$$b \cdot d \equiv r_2 \cdot r_4 \pmod{n}$$

Como $r_1 = r_2$ e $r_3 = r_4$ temos que

$$\begin{aligned} a \cdot c &\equiv r_1 \cdot r_3 \\ &\equiv r_2 \cdot r_4 \\ &\equiv b \cdot d \end{aligned}$$

como queríamos demonstrar.

iii) Note que $m \mid n$ e como $a \equiv b \pmod{n} \implies m \mid n \mid (a-b) \implies m \mid (a-b) \implies a \equiv b \pmod{m}$

iv) Note que isso ocorre $\iff n|(a^k - b^k) = (a-b) \cdot (a^{k-1} + a^{k-2} \cdot b + \cdots + b^{k-1})$, que claramente ocorre pois $n|(a-b)$.

Obs. iv) também poderia ter sido provado sem a fatoração, por indução, aplicando (*ii*) repetidas vezes.

A partir de agora, já podemos resolver alguns problemas simples de análise módulo n.

2 Problemas resolvidos

Exemplo 1: Encontre o resto da divisão de 15^{2023} por 7.

Demonstração. Perceba que $15 \equiv 1 \ (mod\ 7)$.
Logo: $15^{2023} \equiv 1^{2023} \equiv 1 \ (mod\ 7)$. □

Exemplo 2: Encontre o resto da divisão de 2^{1234} por 5.

Demonstração. Analisando casos iniciais, podemos perceber o seguinte:

$$\begin{cases} 2^1 \equiv 2 \ (mod\ 5) \\ 2^2 \equiv 4 \ (mod\ 5) \\ 2^3 \equiv 8 \equiv 3 \ (mod\ 5) \\ 2^4 \equiv 16 \equiv 1 \ (mod\ 5) \\ 2^5 \equiv 32 \equiv 2 \ (mod\ 5) \end{cases}$$

A partir daqui, podemos perceber um padrão, pois 2^5 deixa o mesmo resto na divisão por 5 que 2^1. De fato, como $2^4 \equiv 1 \ (mod\ 5)$, $2^5 = 2^4 \cdot 2^1 \equiv 1 \cdot 2^1 \ (mod\ 5)$. Percebendo isso, também podemos aplicar ao caso do problema.Como $1232 = 4 \cdot 308$, concluimos que:

$$\begin{aligned} 2^{1234} =& 2^{1232} \cdot 2^2 \\ &\equiv (2^4)^{308} \cdot 2^2 \\ &\equiv 1^{308} \cdot 2^2 \\ &\equiv 1 \cdot 4 \\ &\equiv 4 \ (mod\ 5). \end{aligned}$$

Dessa maneira, 2^{1234} deixa resto 4 na divisão por 5. □

Exemplo 3: Prove que a equação diofantina $5^x + 1 = y^2 - z^2$ não tem solução onde $(x, y, z) \in \mathbb{Z}$.

Demonstração. Essa questão é um exemplo das clássicas *equações diofantinas*, que são muito conhecidas por serem resolvidas analisando a equação módulo algum número que dê informações úteis.
Nesse caso, analisando a equação módulo 4, teremos:

$$\begin{aligned} y^2 - z^2 &\equiv 5^x + 1 \pmod 4 \\ &\equiv 1 + 1 \\ &\equiv 2 \ (*) \end{aligned}$$

Observe agora um número qualquer $a^2 \pmod 4$:

$$\begin{cases} a \equiv 0 \pmod 4 \Rightarrow a^2 \equiv 0^2 \equiv 0 \pmod 4. \\ a \equiv 1 \pmod 4 \Rightarrow a^2 \equiv 1^2 \equiv 1 \pmod 4. \\ a \equiv 2 \pmod 4 \Rightarrow a^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod 4. \\ a \equiv 3 \pmod 4 \Rightarrow a^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 4. \end{cases}$$

Logo, $a^2 \equiv 0{,}1 \pmod 4$. Voltando a $(*)$, vemos que $y^2 - z^2 \equiv 2 \pmod 4$. Porém, os únicos valores que $y^2 - z^2$ pode assumir $\pmod 4$ são:

$$\begin{cases} 1 - 1 \equiv 0 \pmod 4 \\ 1 - 0 \equiv 1 \pmod 4 \\ 0 - 0 \equiv 0 \pmod 4 \\ 0 - 1 \equiv -1 \equiv 3 \pmod 4 \end{cases}$$

Logo, $2 \equiv y^2 - z^2 \equiv 0, 1$ ou $3 \pmod 4$, absurdo!
Logo, não há tripla (x, y, z)de inteiros positivos tal que $5^x + 1 \equiv y^2 - z^2 \pmod 4$.
Obs.: $-1 \equiv 3 \pmod 4$ é um uso de congruências negativas, e isso ocorre pois $4|(-1-3) = -4$. $\square$

3 Problemas para praticar

Problema 1: Encontre o resto da divisão de 7^{555} por 6.

Problema 2: Encontre o resto da divisão de 23^{128} por 7.

Problema 3: Encontre o resto da divisão de 5^{1000} por 31.

Problema 4: Encontre algarismo das unidades de 73^{73}.

Problema 5: Encontre o resto da divisão de 206^{2005} por 7.

Problema 6: Prove que a equação $x^3 + y^3 = c^6 + 3$ não possui solução onde $(x, y, z) \in \mathbb{Z}$.

Problema 7: Ache todas as soluções de $2^a + 3 = b^2 + c^2$, onde a, b, e c são inteiros positivos.

Problema 8:
a) Prove que $\overline{a_n a_{n-1} \dots a_1 a_0} \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod 9$. (Em particular, $\overline{a_n a_{n-1} \dots a_1 a_0}$ é divisível por 9 $\iff$ $a_n + a_{n-1} + \dots + a_1 + a_0$ é divisível por 9 (critério de divisibilidade por 9)).
b) A partir de a), prove o mesmo, porém módulo 3.

Problema 9: (OBMEP 2017/Adaptado) Prove que $n^3 - n$ é sempre múltiplo de 6, $n \in \mathbb{Z}$.

Problema 10: Prove que a equação $n^3 - n - 1 = k^2 - k + 1$ não possui soluções onde k, n são números inteiros.

Problema 11: Encontre todos $x, y \in \mathbb{Z}_+$ tais que $3^x - 2^y = 7$.

Problema 12: Mostre que, para todo k, n inteiros positivos ímpares, $1^k + 2^k + \dots + (n-1)^k$ é divisível por n.

4 Dicas:

Problema 1: Note que $7 \equiv 1 \pmod 6$.

Problema 2: Perceba que $23 \equiv 2 \pmod 7$, e $8 \equiv 1 \pmod 7$.

Problema 3: Veja que $124 \equiv 0 \pmod{31}$

Problema 4: Note que $3^4 = 81$ termina em 1.

Problema 5: Observe que $203 \equiv 0 \pmod 7$, e $3^3 \equiv -1 \pmod 7$

Problema 6: Analise a equação módulo 7.

Problema 7: Veja o que ocorre se $a > 1$, analisando módulo 4.

Problema 8: Perceba que $\overline{a_n a_{n-1} \ldots a_1 a_0} = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \cdots + 10 \cdot a_1 + a_0$.

Problema 9: Tente fatorar e analisar módulo 2 e módulo 3 separadamente.

Problema 10: Analise a equação módulo 3.

Problema 11: Veja módulo 8 para $y \geq 3$.

Problema 12: Analise congruências negativas ($(n-1) \equiv -1 \pmod n$, por exemplo).

5 Soluções:

Problema 7:

Demonstração. Note que, se $a = 1$, obtemos que $b^2 + c^2 = 5$, e é fácil ver que $(a,b,c) = (1,1,2)$ e $(1,2,1)$ são as únicas soluções nesse caso. Considere agora $a \geq 2$. Note que, nesse caso, 2^a é múltiplo de 4, e então, $b^2 + c^2 \equiv 3 \pmod 4$. Porém, note o que ocorre quando tentamos somar dois quadrados perfeitos, módulo 4:

$$\begin{cases} 0 + 0 \equiv 0 \pmod 4 \\ 1 + 0 \equiv 1 \pmod 4 \\ 0 + 1 \equiv 1 \pmod 4 \\ 1 + 1 \equiv 2 \pmod 4 \end{cases}$$

(Utilizamos o fato já visto anteriormente que $x^2 \equiv 0{,}1 \pmod 4$).

Dessa maneira, teremos que $3 \equiv 0{,}1$ ou $2 \pmod 4$, um absurdo! Logo, as únicas soluções para a equação $2^a + 3 = b^2 + c^2$ são $(1, 1, 2)$ e $(1, 2, 1)$. □

Problema 11:

Demonstração. Primeiro, façamos alguns casos iniciais:

$$\begin{cases} y = 0 : \text{Teremos que } 3^x - 1 = 7 \implies 3^x = 8 \longrightarrow \text{Abs!} \\ y = 1 : \text{Teremos que } 3^x - 2 = 7 \implies 3^x = 9 \implies (x,y) = (2, 1) \text{ é solução.} \\ y = 2 : \text{Teremos que } 3^x - 4 = 7 \implies 3^x = 11 \longrightarrow \text{Abs!} \end{cases}$$

Agora, suponha que $y \geq 3$. Teremos que 2^y será múltiplo de 8, e assim, $3^x \equiv 7 \equiv -1 \pmod 8$. Porém, observe que $3^x \equiv 3$ ou $1 \pmod 8$ (apenas observar que $3^2 \equiv 1 \pmod 8$). Dessa maneira, $3^x \equiv -1 \equiv 1$ ou $3 \pmod 8 \longrightarrow$ Abs! Logo, a única solução do problema é $(x, y) = (2, 1)$. □

Problema 12:

Demonstração. Considere $S = 1^k + 2^k + \cdots + (n-1)^k$. Note que, como n é ímpar,
$S = \left(1^k + 2^k + \cdots + \left(\frac{n-1}{2}\right)^k\right) + \left(\left(\frac{n+1}{2}\right)^k + \cdots + (n-1)^k\right)$.
Assim, podemos analisar S módulo n.
Teremos:
$S \equiv \left(1^k + 2^k + \cdots + \left(\frac{n-1}{2}\right)^k\right) + \left(\left(\frac{n+1}{2}\right)^k + \cdots + (n-1)^k\right) \pmod n$.
Perceba que, como k é ímpar, teremos: $(-x)^k = (-1)^k \cdot x^k = -(x^k)$

Note também que:

$$\begin{cases} n-1 \equiv -1 \pmod{n} \implies (n-1)^k \equiv (-1)^k \equiv -1^k \pmod{n} \\ n-2 \equiv -2 \pmod{n} \implies (n-2)^k \equiv (-2)^k \equiv -2^k \pmod{n} \\ \vdots \\ \dfrac{n+1}{2} \equiv -\dfrac{n-1}{2} \pmod{n} \implies \left(\dfrac{n+1}{2}\right)^k \equiv \left(-\dfrac{n-1}{2}\right)^k \equiv -\left(\dfrac{n-1}{2}\right)^k \pmod{n} \end{cases}$$

Dessa maneira, teremos:

$$\begin{aligned} S &\equiv \left(1^k + 2^k + \cdots + \left(\frac{n-1}{2}\right)^k\right) + \left(\left(\frac{n+1}{2}\right)^k + \cdots + (n-1)^k\right) \\ &\equiv \left(1^k + 2^k + \cdots + \left(\frac{n-1}{2}\right)^k\right) + \left(-\left(\frac{n-1}{2}\right)^k - \cdots - 1^k\right) \end{aligned}$$

Reorganizando os termos, teremos...

$$\begin{aligned} S &\equiv 1^k - 1^k + 2^k - 2^k + \cdots + \left(\frac{n-1}{2}\right)^k - \left(\frac{n-1}{2}\right)^k \\ &\equiv 0 \pmod{n} \end{aligned}$$

$\square$