# Congruências

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

22 de junho de 2020

# Congruência

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que $a$ é congruente a $b$ módulo $n$, e escrevemos

$$a \equiv b \ (mod \ n)$$

se $n|a-b$, ou seja, se $a$ e $b$ deixam o mesmo resto na divisão por n.

# Exemplo

$$17 \equiv 3 \ (mod \ 7)$$

# Exemplo

$$17 \equiv 3 \ (mod \ 7)$$

$$10 \equiv -5 \ (mod \ 3)$$

# Exemplo

$$17 \equiv 3 \ (mod \ 7)$$

$$10 \equiv -5 \ (mod \ 3)$$

$$12 \equiv 0 \ (mod \ 4)$$

# Exemplo

$$17 \equiv 3 \ (mod\ 7)$$

$$10 \equiv -5 \ (mod\ 3)$$

$$12 \equiv 0 \ (mod\ 4)$$

Mostre que a congruência módulo $n$ é uma relação de equivalência.

# Propriedades: Soma e diferença

Podemos somar e subtrair "membro a membro":

$$\begin{cases} a \equiv b \,(mod\ n) \\ c \equiv d \,(mod\ n) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \,(mod\ n) \\ a - c \equiv b - d \,(mod\ n) \end{cases}$$

Em particular, se $a \equiv b \,(mod\ n)$, então $ka \equiv kb \,(mod\ n)$ para todo $k \in \mathbb{Z}$.

# Demonstração

Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ fixo, porém arbitrário.

Se $n|a-b$ e $n|c-d$, então $n|(a-b)+(c-d)$ se, e somente se $n|(a+c)-(b+d)$, concluindo a propriedade da soma.

De forma similar, temos que se $n|a-b$ e $n|c-d$, então $n|(a-b)-(c-d)$ se, e somente se, $n|(a-c)-(b-d)$, concluindo a propriedade da diferença.

# Demonstração

Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ fixo, porém arbitrário.

Se $n|a-b$ e $n|c-d$, então $n|(a-b)+(c-d)$ se, e somente se $n|(a+c)-(b+d)$, concluindo a propriedade da soma.

De forma similar, temos que se $n|a-b$ e $n|c-d$, então $n|(a-b)-(c-d)$ se, e somente se, $n|(a-c)-(b-d)$, concluindo a propriedade da diferença.

# Propriedades: Produto

Podemos multiplicar "membro a membro":

$$\begin{cases} a \equiv b \ (mod\ n) \\ c \equiv d \ (mod\ n) \end{cases} \Rightarrow \quad ac \equiv bd \ (mod\ n)$$

Em particular, se $a \equiv b \ (mod\ n)$, então $a^k \equiv b^k \ (mod\ n)$ para todo $k \in \mathbb{Z}$.

# Demonstração

Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ fixo, porém arbitrário.

Se $n|a-b$ e $n|c-d$, então $n|(a-b)c$ e $n|(c-d)b$ e portanto $n|(a-b)c+(c-d)b$, logo $n|ac-bd$. Portanto, segue a propriedade da multiplicação.

# Demonstração

Sejam $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ fixo, porém arbitrário.

Se $n|a-b$ e $n|c-d$, então $n|(a-b)c$ e $n|(c-d)b$ e portanto $n|(a-b)c+(c-d)b$, logo $n|ac-bd$. Portanto, segue a propriedade da multiplicação.

Justifique a implicação: Se $a \equiv b\ (mod\ n)$, então $a^k \equiv b^k\ (mod\ n)$ para todo $k \in \mathbb{Z}$.

# Propriedades: Cancelamento

Se $mdc(c, n) = 1$, então

$$ac \equiv bc \ (mod \ n) \Leftrightarrow a \equiv b \ (mod \ n).$$

# Demonstração

($\Rightarrow$) Suponha que $mdc(c, n) = 1$. Assim,

$$n|ac - bc \Leftrightarrow n|(a - b)c$$

Pela Proposição: Se $mdc(a, b) = 1$ e $a|bc$, então $a|c$, concluímos que

$$n|a - b$$

($\Leftarrow$) Imediato.

As propriedades vistas nos slides anteriores mostram que a relação de *congruência módulo n* tem um comportamento muito similar à relação de igualdade usual.

Estas propriedades tornam as congruências úteis em problemas de divisibilidade.

# Exemplo:

Mostremos que $31|20^{15} - 1$. Isto é, o resto da divisão de $20^{15}$ por 31 é 1.

Esse problema é equivalente a demonstrar que $20^{15} \equiv 1 \ (mod\ 31)$.

Veja que:

$$20 \equiv x \ (mod\ 31)$$

# Exemplo:

Mostremos que $31|20^{15} - 1$. Isto é, o resto da divisão de $20^{15}$ por 31 é 1.

Esse problema é equivalente a demonstrar que $20^{15} \equiv 1 \ (mod\ 31)$.

Veja que:

$$20 \equiv -11 \ (mod\ 31) \tag{1}$$

# Exemplo:

Assim,

$$20^2 \equiv (-11)^2 \ (mod\ 31) \Leftrightarrow 20^2 \equiv 121 \ (mod\ 31)$$

Analisemos 121 com 31, segundo a relação de congruência.

$$121 \equiv x \ (mod\ 31)$$

# Exemplo:

Assim,

$$20^2 \equiv (-11)^2 \ (mod\ 31) \Leftrightarrow 20^2 \equiv 121 \ (mod\ 31)$$

Analisemos 121 com 31, segundo a relação de congruência.

$$121 \equiv -3 \ (mod\ 31)$$

# Exemplo:

Portanto, temos que

$$20^2 \equiv -3 \ (mod\ 31) \tag{2}$$

Multiplicando as equações (1) e (2), temos:

$$20^3 \equiv 33 \ (mod\ 31)$$

# Exemplo:

Analisemos 33 com 31, segundo a relação de congruência temos:

$$33 \equiv 2 \ (mod\ 31)$$

Portanto,

$$20^3 \equiv 2 \ (mod\ 31)$$

# Exemplo:

Elevando ambos os lados por 5, temos:

$$(20^3)^5 \equiv 2^5 \ (mod\ 31) \Leftrightarrow 20^{15} \equiv 32 \ (mod\ 31)$$

Como $32 \equiv 1 \ (mod\ 31)$, concluímos que

$$20^{15} \equiv 1 \ (mod\ 31).$$

Portanto, o resto da divisão de $20^{15}$ por 31 é 1.

# Referências

**MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E.** Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

**GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O** Matemática Concreta. LTC, São Paulo, 1995

**NIVEN, I. E.; ZUCKERMAN, N.S.** An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

# Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: https://viniciuswasques.github.io/home/