Propriedades de Divisibilidade e Congruências

Alan Rodrigues dos Santos, Patrícia Cristina Souza dos Santos

Orientador: Prof. Dr. Igor dos Santos Lima

II Workshop de Álgebra da UFG-CAC

e-mail: alansantos2102@hotmail.com, patriciacristina_souza@hotmail.com

Introdução

O conceito de números inteiros congruentes é devido a Carl Friedrich Gauss (1777 – 1855), um dos estudiosos da Teoria dos Números. O trabalho foi baseado nas vídeo-aulas do Pólos Olímpicos de Treinamento Intensivo e no material didático (apostila de Teoria dos Números e de Álgebra *I*) do Prof. Lineu Neto (UnB). Este pôster tem como objetivo central estabelecer propriedades de divisibilidade e de congruências a fim de revisar, aprender ou ensinar um tema essencial em Teoria dos Números. Quem estiver interesse sobre o assunto e quiser aprofundar nesse tema pode assistir ao curso completo disponível no youtube ou estudar pelas referências deste pôster.

Preliminares

Divisibilidade em $\mathbb{Z}$

Definição: Sejam $a, b \in \mathbb{Z}$. Dizemos que b divide a, se existe um d tal que $a = db$.

Exemplo: $7|-21$, pois $7(-3) = -21$.

Teorema: (Regras de divisibilidade) Sejam a, b, c e $d \in \mathbb{Z}$. Então:

(a) $a|a$;

(b) $1|b$;

(c) $a|0$;

(d) Se $0|b$, então $b = 0$;

(e) Se $d|a$ e $d|b$, então $d|(ax+by)$, para quaisquer $x, y \in \mathbb{Z}$;

(f) Se $d|a$ então $a = 0$ ou $|a| \geq |d|$;

(g) Se $a|b$ e $b|c$ então $a|c$.

Máximo Divisor Comum

Definição: Sejam $a, b \in \mathbb{Z}$, não simultaneamente nulos. Definimos o M.D.C. de a e b como sendo o número natural $d = mdc(a, b)$ satisfazendo as seguintes condições:

(i) $d|a$ e $d|b$;

(ii) Se $c \in \mathbb{N}$ tal que $c|a$ e $c|b$, então $c|d (\Rightarrow |c| \leq |d| \Rightarrow c \leq d)$. Em outras palavras, $d = \max[D(a) \cap D(b)]$.

Exemplo

Notação: $D(n) = \{\text{divisores de n}\}$.
$D_+(n) = \{\text{divisores positivos de n}\}$.
$D(45) = \{\pm1, \pm3, \pm5, \pm9, \pm15, \pm45\}$.
$D(36) = \{\pm1, \pm2, \pm3, \pm4, \pm6, \pm9, \pm12, \pm18, \pm36\}$.
$\Rightarrow D(45) \cap D(36) = \{\pm1, \pm3, \pm9\}$.
$\Rightarrow d = mdc(45, 36) = \max[D(45) \cap D(36)] = 9$.

Teorema: (Bezout) Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$. Então existem $x_1, y_1 \in \mathbb{Z}$ tais que $ax_1 + by_1 = d$.

Mais ainda, as combinações lineares inteiras de a e b são exatamente os múltiplos do $mdc(a, b)$.

Mínimo Múltiplo Comum

Definição: Sejam $a, b \in \mathbb{Z}$, ambos não nulos. Definimos o M.M.C. de a e b como sendo o número natural $m = mmc(a, b)$ satisfazendo as seguintes condições:

(i) $a|m$ e $b|m$;

(ii) Se $c \in \mathbb{N}$ tal que $a|c$ e $c|b$, então $m|c (\Rightarrow |m| \leq |c| \Rightarrow m \leq c)$. Em outras palavras, $m = \min[M_+(a) \cap M_+(b)]$.

Propriedades:

(i) $mmc(a, b) = mmc(b, a)$

(ii) $mmc(a, b) = mmc(|a|, |b|)$

(iii) $mmc(a, 1) = |a|$

(iv) Se $a|b$, então $mmc(a, b) = |b|$

Notação: $M(n) = \{\text{múltiplos de n}\}$.
$M_+(n) = \{\text{múltiplos positivos de n}\}$.
Exemplos:

(i) $M(45) = \{45k | k \ \mathbb{Z}\} = \{0, \pm45, \pm90, \pm135, \ldots\}$.

(ii) $M(36) = \{36k | k \in \mathbb{Z}\} = \{0, \pm36, \pm72, \pm108, \ldots\}$.

(iii) $M_+(45) = \{45, 90, 135, \ldots\}$.

(iv) $M_+(36) = \{36, 72, 108, 144, \ldots\}$.

(v) $M_+(45) \cap M_+(36) = \{180, 360, 540, \ldots\}$.

(vi) $m = \min[M_+(45) \cap M_+(36)] = 180$.

Números primos

Definição: Um número inteiro p, com $p > 1$, é chamado de primo se seus únicos divisores positivos são 1 e p. Se $n > 1$ não é primo, então n é dito composto.

Exemplos:

(a) $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ são primos.

(b) 4 é composto (pois $D_+(4) = \{1, 2, 4\}$).

(c) 6 é composto (pois $D_+(6) = \{1, 2, 3, 6\}$).

Congruências

Definição: Dizemos que dois números inteiros a e b são congruentes módulo n se $b - a$ é múltiplo de n, sendo $n \in \mathbb{Z}$ e $n > 0$. Isso equivale a dizer que a e b deixam o mesmo resto na divisão por n. Escrevemos nesse caso $a \equiv b \mod n$.

Observações:

- $a \equiv b \mod n \Rightarrow n|(b-a) \Rightarrow \frac{(b-a)}{n} \in \mathbb{Z} \Rightarrow b = a + kn$, para algum $k \in \mathbb{Z}$.
- Se $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$.

Teorema: (Regras de congruências) Se $a \equiv b \mod n$ e $c \equiv d \mod n$ então:

(i) $a + c \equiv b + d \mod n$.

(ii) $a - c \equiv b - d \mod n$.

(iii) $ka \equiv kb \mod n$, para algum $k \in \mathbb{Z}$.

(iv) $ac \equiv bd \mod n$.

(v) $a^k \equiv b^k \mod n$, para algum $k \in \mathbb{N}$.

(vi) Se $mdc(k, n) = d$, então $ka \equiv kb \mod n \Rightarrow a \equiv b \mod \frac{n}{d}$.

Exemplos:

(1) Calcule o resto da divisão de 4^{100} por 3.
$4 \equiv 1 (\mod 3) \Rightarrow 4^{100} \equiv 1^{100} \mod 3$. Logo o resto é 1.

(2) Calcule o resto da divisão de 4^{100} por 5.
$4 \equiv -1 \mod 5 \Rightarrow 4^{100} \equiv (-1)^{100} \mod 5$. Logo o resto é 1.

(3) Calcule o resto da divisão de 4^{100} por 7.
$4^2 = 16 \equiv 2 \mod 7 \Rightarrow 4^3 = 2 \cdot 4 \equiv 1 \mod 7 \Rightarrow 4^{99} = (4^3)^{33} \equiv 1^{33} = 1 \mod 7 \Rightarrow 4^{100} = 4^{55}4 \equiv 1 \cdot 4 = 4 \mod 7$. Logo o resto é 4.

(4) Qual é o resto da divisão de $36^{36} + 41^{41}$ por 77?
$36 + 41 = 77 \equiv 0 \mod 77 \Rightarrow 41 \equiv -36 \mod 77 \Rightarrow 36^{36}+41^{41} \equiv 36^{36}+(-36)^{41} = [36^{36}-(36^{41})] \mod 77 \equiv 36^{36}(1 - 36^5)\ 77 = 7 \cdot 11$
$\Rightarrow 36^5 \equiv 1^5 = 1 \mod 7 \Rightarrow 7|(36^5 - 1) \Rightarrow 36^5 \equiv 3^5 \equiv \mod 11 \Rightarrow 11|(36^5 - 1) \Rightarrow 77|(36^5 - 1)$. Logo deixa resto 0.

Demonstração: (Regras de divisibilidade) As regras de divisibilidade da letra (a) até (d) são de imediata compreensão.
(e) : se $d|a$ e $d|b$, podemos escrever $a = da_1$ e $b = db_1$, onde $a_1,\ b_1 \in \mathbb{Z}$. Queremos concluir $d|(ax + by)$ onde $x, y \in \mathbb{Z}$. Logo $ax + by = da_1x + db_1y = d(a_1x + b_1y)$.
(f) : Tomando $a = d \cdot a_1$, se $a_1 = 0$, $a = d \cdot 0 = 0$ e se $a_1 \neq 0$, $|a_1| \geq 1$, pois $a_1 \in \mathbb{Z}$ e portanto $|a| = |da_1| = |d||a_1||d|$.
(g) : Se $b = ac_1$ onde c_1 e $c = bc_2 \in \mathbb{Z}$, onde $c_2 \in \mathbb{Z}$, $c = bc_2 = ac_1c_2 \Rightarrow a|c$.

Demonstração: (Regras de congruência) Para provar todas as regras suponha que $n|(b - a)$ e $n|(d - c)$.

(i) $n|[(b - a) + (d - c)] = (b + d) - (a + c)$

(ii) $n|(b + a) - (d + c) = (b - d) + (a - c)$

(iii) $n|k(b - a) = kb - ka$, para algum $k \in \mathbb{Z}$.

(iv) $bd - ac = bd - bc + bc - ac = b(d - c) + c(b - a) \Rightarrow n|(bd - ac)$, pois $n|b(d - c)$, $n|c(b - a)$. Logo $bd \equiv ac \mod n$.

(v) É uma consequência do (iv): $aa \equiv bb \mod n \Rightarrow a^2a \equiv b^2b \mod n$. Agora se $a^2 \equiv b^2 \mod n$ então tem-se $a^{(k+1)} = a^ka \equiv b^ka \equiv b^kb = b^{k+1} \mod n$.

(vi) $k = dk_1,\ n = dn_1,\ mdc(k_1, n_1) = 1$.
$ka \equiv kb \mod n \Rightarrow n|(kb - ka) = k(b - a) \Rightarrow dn_1|dk_1(b - a) \Rightarrow n_1|k_1(b - a) \Rightarrow \frac{n}{d} = n_1|(b - a)$, pois $mdc(n_1, k_1) = 1 \Rightarrow a \equiv b \mod \frac{n}{d}$.

Uma aplicação prática: os calendários. Considere o calendário do mês de janeiro do ano 2000:

D	S	T	Q	Q	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Observe que no domingo, estão os números congruentes com 2 mod 7. Na segunda, estão os números congruentes com 3 mod 7. Na terça, com 4 mod 7. Na quarta, com 5 mod 7 . Na quinta, com 6 mod 7. Na sexta, com 7 mod 7. No sábado, com 1 mod 7.
Em que dia da semana vai cair o dia 25/01/2000, sem consultar o calendário acima?
Basta procurarmos um número congruente com 25 mod 7. Dividindo 25 por 7 dá 3 e resto 4. Logo, $25 \equiv 4 \mod 7$ e como 4 corresponde a uma terça-feira, concluímos que o dia 25/01/2000 cairá numa terça-feira.

Referências

[1] Disponível em: http://www.paulomarques.com.br/arq1-12.htm. Acessado em 25/03/2014 ás 15h35min.

[2] NETO, Lineu. *Álgebra I*. Universidade de Brasília. Departamento de Matemática.1°/2004.

[3] Vídeo-aulas do Pólos Olímpicos de Treinamento Intensivo (youtube).

Este projeto foi financiado pela FAPEG através do edital 05/2013 para realização de eventos.