Monitoria

- Relação de Equivalência:

" Uma relação de equivalência ($\sim$) é uma relação binária que satisfaz:

1) $a \sim a$ (Reflexiva)

2) $a \sim b \Rightarrow b \sim a$ (simétrica)

3) $a \sim b$ e $b \sim c \Rightarrow a \sim c$ (transitiva)

* obs/ Vejam classes de equivalência.

Congruência

Def: Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b são congruentes modulo m se $m \mid a-b$

- Prop. 3.2.2 (pág 104): Seja m um inteiro fixo. Dois inteiros a e b são congruentes módulo m $\Leftrightarrow$ eles têm o mesmo resto quando divididos por m.

Rascunho: relação de equivalência é

cong. módulo 5

Seja $j \in \mathbb{Z}$, $j = q \cdot 5 + r$, $r \in \{0, 1, 2, 3, 4\}$

$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0 \pmod 5\} = \{$ multiplos de 5 $\}$

$= 5\mathbb{Z}$, Sejam $a, b \in \bar{0}$, i.e

$a \equiv 0 \pmod 5$, $b \equiv 0 \pmod 5 \Rightarrow$

$a \equiv 0 \pmod 5$ e $0 \equiv b \pmod 5 \Rightarrow a \equiv b \pmod 5$

Ex 1 (i) $11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv ? \pmod 7$

$11 \equiv ? \pmod 7 \Rightarrow 11 \equiv 4 \pmod 7$

$\rightarrow 18 \equiv 4 \pmod 7$

obs: $18 - 4 = 14 \equiv 0 \pmod 7 \Rightarrow \underbrace{18 - 4 + 4}_{18} \equiv 4 \pmod 7$

$2322 \equiv 5 \pmod 7$

$\rightarrow 13 \equiv 6 \pmod 7$

obs: $14 \equiv 0 \pmod 7 \Rightarrow 13 \equiv -1 \pmod 7 \Rightarrow 13 \equiv 6 \pmod 7$

$19 \equiv 5 \pmod 7$

$$11 \cdot 18 \cdot 2322 \cdot 13 \cdot 19 \equiv \underbrace{4 \cdot 4}_{16} \cdot \underbrace{5 \cdot 6}_{30} \cdot 5 \pmod 7$$

$$16 \equiv 2 \pmod 7 \qquad 30 \equiv 2 \pmod 7$$

$$\underbrace{4 \cdot 4}_{16} \cdot \underbrace{5 \cdot 6}_{30} \cdot 5 \equiv 2 \cdot 2 \cdot 5 \pmod 7$$

$$\therefore 20 \equiv 6 \pmod 7$$

(ii) (Dica) $1 + 2 + \ldots + 2^{19}$

Considere a par, então $a = 2k$.

$$2^a = 2^{2 \cdot k} = 4^k \quad \left(4 \equiv 0 \pmod 4 \right) \Rightarrow$$

$$4^k \equiv 0^k = 0 \pmod 4$$

Agora, seja a ímpar, então $a = 2k+1$

$$2^{2k+1} = 2 \cdot 4^k \quad \left(4^k \equiv 0 \pmod 4 \right)$$

(...) Continuem

Ex 2 $\quad a \equiv b \pmod{r} \iff as \equiv bs \pmod{rs}$

($\Rightarrow$) $\quad a \equiv b \pmod{r} \Rightarrow r \mid a-b \Rightarrow$

$(a-b) = r \cdot k \Rightarrow s(a-b) = rs \cdot k \Rightarrow$

$rs \mid s(a-b) \Rightarrow as \equiv bs \pmod{rs}$

$as - bs$

($\Leftarrow$) $\quad as \equiv bs \pmod{rs} \Rightarrow rs \mid as - bs \Rightarrow$

$(a-b) \cdot s = rs \cdot k \Rightarrow (a-b) = r \cdot k \Rightarrow$

$s \neq 0$

$r \mid (a-b) \Rightarrow a \equiv b \pmod{r}$

Ex3) $X^2 \equiv 0 \pmod m$ e $X \equiv 0 \pmod m$

$\Downarrow$ $\Downarrow$

($m \mid X^2$ $\quad$ $m \mid X$

$m = p^2 \cdot \_\_ \Rightarrow p^2 \mid m$. $\quad X = p \cdot \_\_$)

obs: Seja $z \in \mathbb{Z}$, pelo TFA,

$\_\_\_\_ z = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$

Queremos provar que $m = p_1 \cdots p_k$ (livre de quadrados)

Suponha por absurdo que $m = p^2 \cdot c$. (Observe que p primo)

(...) Observe que $x = pc$ é solução de $X^2 \equiv 0 \pmod m$

$\rightarrow X^2 = (pc)^2 = (p^2 c) \cdot c = m \cdot c \Rightarrow m \mid X^2 - 0 \Rightarrow$

$X^2 \equiv 0 \pmod m$. Agora, note que $x = pc$ não é solução de $X \equiv 0 \pmod m$. Caso fosse verdade

$m = p^2 c \mid pc \Rightarrow pq = (p^2 c) \cdot k \Rightarrow 1 = p \cdot k \Rightarrow$

$p \mid 1$ (contradição). Logo, $m = p_1 \cdots p_k$. Note que se X é solução de $X^2 \equiv 0 \pmod m \Rightarrow$

$m \mid X^2 \Rightarrow p_i \mid X^2, \; i = 1, \ldots, k \overset{(*)}{\Rightarrow} p_i \mid X, \; i = 1, \ldots, k \Rightarrow$

$m \mid X$ (porque?) $\Rightarrow X \equiv 0 \pmod m$ ∎

Ex6) $\{a_1, \ldots, a_n\}$ é s.c. de resíduos módulo m.

obs: Def: Uma coleção de m inteiros $\{a_1, \ldots, a_m\}$ é um sistema completo de resíduos modulo m se cada inteiro é congruente modulo m a um único a_i (ie, $\forall j \in \mathbb{Z}$, $\exists\, i \in \{1, \ldots, m\}$ tq $j \equiv a_i \pmod m$ e $j \not\equiv a_j \pmod m$ $j \neq i$)

obs: $a_i \not\equiv a_j \pmod m$

Queremos que $\{aa_1, \ldots, aa_n\}$ seja sc. de resíduos módulo n ($mdc(a, n) = 1$)

Primeiro vamos provar que $aa_i \not\equiv aa_j \pmod n$, $i \neq j$. Suponha que $aa_i \equiv aa_j \pmod n$. Pela Prop. 3.2.4, $a_i \equiv a_j \pmod n$, contradição.

Seja $z \in \mathbb{Z}$. Então $z \equiv a_j \pmod n$ para algum $j \in \{1, \dots, n\}$. Note que existe uma correspondência (biunívoca) entre $\{a_1, \dots, a_n\}$ e $\{aa_1, \dots, aa_n\}$, daí existe $i \in \{1, \dots, n\}$ tq $a \cdot a_i \equiv a_j \pmod n$. Logo, por transitividade $z \equiv a \cdot a_i \pmod n$

□

Ex 7 (Teoria)

Considere uma eq. da forma $X \equiv b \pmod{m}$

Como $mdc(1, m) = 1$, essa eq. tem soluções. Note

$m \mid X - b \Rightarrow X - b = my \Rightarrow X - my = b$

Queremos $mdc(1, -m) = 1$. Daí

$$\underbrace{1}_{r} \cdot 1 + \underbrace{0}_{s} \cdot (-m) = 1 \qquad (ax + by = c)$$

Assim, um sol. particular é $x_0 = b$ e a sol. geral é: $x = b - mt$, $t \in \mathbb{Z}$

Item (11) $5x \equiv 2 \pmod{26}$ $(\gcd(5, 26) = 1)$

$26 \mid 5x - 2 \Rightarrow 5x - 2 = 26y \Rightarrow$

$5x - 26y = 2$ (eq. diofantina) OK

2 opções:

$5x \equiv 2 \pmod{26} \Rightarrow 25x \equiv 10 \pmod{26}$

$25 \equiv -1 \pmod{26}$. Então $-1x \equiv 10 \pmod{26} \Rightarrow$

$x \equiv -10 \pmod{26} \Rightarrow x \equiv 16 \pmod{26}$ //

$0 \equiv 26 = 10 + 16 \pmod{26}$

Ex 4 (d. ca)

$n^6 = (n^3)^2$

$$n^7 - n = n(n^6 - 1) = n\left((n^3)^2 - 1^2\right) =$$

$$n(n^3 - 1)(n^3 + 1) = n(n-1)(n^2 + n + 1)(n^3 + 1) =$$

$$n\underbrace{(n-1)(n^2}_{\text{PDf (e-disaplimas)}} + n + 1)\underbrace{(n+1)(n^2}_{\text{PDf (e-disaplimas)}} - n + 1)$$