MAT0164 - Números Inteiros: Uma introdução à Matemática

3ª Prova - 28/06/2017

Nome: _____

Nº USP: _____

Questão	
1	
2	
3	
4	
5	
Nota	

Atenção:

1 - Leia os enunciados com atenção!

2 - Justifique cuidadosamente todas as suas afirmações.

3 - Boa prova!

1. **(2,5)**

   (a) Resolva o sistema de congruências: $X \equiv -1 (\text{mod} 41)$ e $2X \equiv -1 (\text{mod} 43)$;

   (b) Use o resultado do item (a) para determinar o resto da divisão de 40! por 1763. $(1763 = 41 \times 43)$

(a) $X \equiv -1 \pmod{41}$

$2X \equiv -1 \pmod{43}$

$1 = (-1) \times 43 + 2 \times 22 \Rightarrow 2 \times 22 \equiv 1 \pmod{43}$

Logo $2X \equiv -1 \pmod{43} \iff$

$X \equiv -22 \pmod{43} \iff X \equiv 21 \pmod{43}$

Seja $N = 41 \times 43$, $n_1 = 41$ $n_2 = 43$

$N_1 = \frac{N}{n_1} = 43$

$N_2 = \frac{N}{n_2} = 41$

$\text{mdc}(43, 41) = 1$

$\underbrace{-20}_{r_1} \times 43 + 21 \times 41 = 1$

$x_0 = (-20)(43) \times -1 + 21 \times 21 \times 41 = 18941$

A solução geral é $\boxed{x = 18941 + 1763t, t \in \mathbb{Z}}$

(b) Pelo Teorema de Wilson, $40 \equiv -1 \pmod{41}$

$42! \equiv -1 \pmod{43}$

$42 \cdot 41 \cdot 40! \equiv -1 \pmod{43}$

Mas $42 \times 41 \equiv (-2) \times (-1) \pmod{43}$

Logo $2 \times 40! \equiv -1 \pmod{43}$

Assim, $40!$ é uma solução do sistema de congruências do item (a). Como o resto da divisão por 1763 é maior do que 0 e menor do que 1763, devemos encontrar $t_0 \in \mathbb{Z}$ tal que $0 < 18941 + 1763t_0 < 1763$.

$t_0 = -10$

$\boxed{r = 1311}$

MAT0164 - Números Inteiros: Uma introdução à Matemática

3ª Prova - 28/06/2017

Nome: _____

Nº USP: _____

Questão	
1	
2	
3	
4	
5	
Nota	

Atenção:

1 - Leia os enunciados com atenção!

2 - Justifique cuidadosamente todas as suas afirmações.

3 - Boa prova!

1. **(2,5)**

(a) Resolva o sistema de congruências: $X \equiv -1 (\text{mod} 29)$ e $2X \equiv -1 (\text{mod} 31)$;

(b) Use o resultado do item (a) para determinar o resto da divisão de 28! por 899. $(899 = 29 \times 31)$

(a) $x \equiv -1 \pmod{29}$

$2x \equiv +1 \pmod{31}$

$\text{mdc}(2,31) = 1$

$1 = (1) \times 31 + 2 \times (-15)$

Assim $-15 \cdot 2 \equiv 1 \pmod{31}$

$2x \equiv -1 \pmod{31} \equiv x \equiv 15 \pmod{31}$

$\begin{cases} x \equiv -1 \pmod{29} \\ x \equiv 15 \pmod{31} \end{cases}$

$N = 29 \times 31$

$n_1 = 29 \quad n_2 = 31$

$31 = N_1 = N/n_1 \quad N_2 = N/n_2 = 29$

$\text{mdc}(29,31) = 1 \quad 1 = 15 \times 29 + (-14) \times 31$

Pelo Teorema Chinês, uma solução x_0 do sistema é $x_0 = -1 \cdot (-14) \times 31 + 15 \times 15 \times 29$

$x_0 = 6959$

$X = 6959 + 899t, \quad t \in \mathbb{Z}$

(b) Note que pelo Teorema de Wilson,

$28! \equiv -1 \pmod{29}$

e $30! \equiv -1 \pmod{31}$

Mas $30! = 30 \cdot 29 \cdot 28! \equiv (-1)(-2)28! \equiv 2 \cdot 28! \equiv -1 \pmod{31}$

Então $28!$ é solução do sistema de congruências em (a).

Então, o resto r da divisão de $28!$ por 899 é tal que $0 \leq r < 899$

Queremos então t_0 tal que $x = 6959 + 899 t_0 < 899$

Como $t_0 = -7$ obtemos $r = 666$

A

2. **(2,5)**

(a) Mostre que a equação $X^3 - \overline{2} = \overline{0}$ não tem solução em Z_{61}.

(b) Determine todas as soluções da equação $X^2 - \overline{1} = \overline{0}$ em $\mathbb{Z}_{21}$.

(a) Suponha que existe $\overline{a} \in \mathbb{Z}_{61}$ tal que $\overline{a}^3 = \overline{2}$. Como $61 \nmid \overline{a}$,

$\overline{a}^{60} \equiv \overline{1}$ pelo Teorema de Fermat.

$\Rightarrow \overline{2}^{20} = \overline{1}$

Mas $2^6 \equiv 64 \equiv 3 \pmod{61}$

$(2^6)^3 \equiv 3^3 \pmod{61}$

$2^{18} \times 2^2 \equiv 3^3 \cdot 2^2 \equiv 47 \pmod{61}$.

absurdo, pois $\overline{a}^{60} = \overline{2}^{20}$,

(b) $x^2 - \overline{1} = \overline{0}$

$\overline{a}^2 = \overline{1} \Rightarrow a \cdot a \equiv 1 \pmod{21} \Rightarrow$

$mdc(a, 21) = 1$

Vamos então procurar entre esses números!

$\overline{1}^2 = \overline{1}$ e $(\overline{20})^2 = (-\overline{1})^2 = \overline{1}$

$\overline{2}^2 = \overline{4}$ e $(-\overline{2})^2 = (\overline{19})^2 = \overline{4}$

$\overline{4}^2 = \overline{16}$ e $\overline{17}^2 = (-\overline{4})^2 = \overline{16}$

$\overline{5}^2 = \overline{4}$ e $(-\overline{5})^2 = \overline{16}^2 = \overline{4}$

$\overline{8}^2 = \overline{1}$ e $(-\overline{8})^2 = \overline{13}^2 = \overline{1}$

$\overline{10}^2 = \overline{16}$ e $(-\overline{10})^2 = \overline{11}^2 = \overline{16}$

Assim as soluções de $x^2 = \overline{1}$ são

$\overline{1}, \overline{20}, \overline{8}, \overline{13}$

2. **(2,5)**

(a) Mostre que a equação $X^3 - \bar{5} = \bar{0}$ não tem solução em Z_{73}.

(b) Determine todas as soluções da equação $X^2 - \bar{1} = \bar{0}$ em $\mathbb{Z}_{15}$.

(a) Suponha que existe $a \in \mathbb{Z}$ tal que $\bar{a}^3 = 5$. É claro que $p = 73 \nmid a$.
Pelo Teorema de Fermat, teríamos que ter $(a^{72} \equiv 1 \pmod{73}) \iff (a^3)^{24} \equiv 1 \pmod{73}$
Mas, $5^{24} \equiv (5^3)^8 \equiv (-21)^8 \equiv ((-21)^2)^4 \equiv 3^4 \pmod{73}$
Logo $5^{24} \equiv 81 \equiv 8 \pmod{73}$. Absurdo!
Logo $\nexists\, a \in \mathbb{Z}$ tal que $\bar{a}^3 = \bar{5}$.

(b) $\varphi(15) = \varphi(3)\varphi(5) = 2.4 = 8$
Se $a \in \mathbb{Z}$ é tal que $\bar{a}^2 = \bar{1}$, então, $\mathrm{mdc}(a, 15) = 1$.
$\{\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}\}$
$\bar{1}^2 = \bar{1}$, $(-\bar{1})^2 = \bar{14}^2 = \bar{1}$
$\bar{2}^2 = \bar{4}$ $(-\bar{2})^2 = \bar{13}^2 = \bar{4}$
$\bar{4}^2 = \bar{1}$ $(-\bar{4})^2 = \bar{11}^2 = \bar{1}$
$\bar{7}^2 = \bar{4}$ $(-\bar{7})^2 = \bar{8}^2 = \bar{4}$
Assim, as soluções da equação são:
$\bar{1}, \bar{14}, \bar{4}, \bar{11}$.

A e B

3. **(2,5)**

(a) Seja p um número primo tal que $p+2$ também é primo. Mostre que

$$4[(p-1)!+1]+p \equiv 0(\text{mod } p(p+2)).$$

Sugestão: $4[(p-1)!+1]+p = 2[2(p-1)!+1]+p+2$.

(b) Mostre que a recíproca do resultado do item (a) também vale, isto é, mostre que se n e $n+2$ são inteiros positivos tais que $4[(n-1)!+1]+n \equiv 0(\text{mod } n(n+2))$ então n e $n+2$ são números primos.

(a) Pelo Teorema de Wilson, temos que se p e $p+2$ são primos,

$(p-1)! + 1 \equiv 0 \pmod p$

$\Rightarrow 4[(p-1)! + 1] + p \equiv 0 \pmod p$

Também, $(p+1)! + 1 \equiv 0 \pmod{p+2}$

$\Rightarrow (p+1)\,p\,(p-1)! + 1 \equiv 2(p-1)! + 1 \pmod{p+2}$

Logo $2[2(p-1)! + 1] + p + 2 \equiv 0 \pmod{p+2}$

$4[(p-1)! + 1] + p \equiv 0 \pmod{p+2}$

Como $p, p+2$ são primos distintos, $\text{mdc}(p, p+2) = 1$. Logo pelo Teorema de Euclides, $4[(p-1)! + 1] \equiv 0 \pmod{p(p+2)}$.

(b) Se $n > 1$ é ímpar, $n+2$ também é ímpar.

Se $4[(n-1)! + 1] + n \equiv 0 \pmod n \Rightarrow (n+1)! + 1 \equiv 0 \pmod n$

$4[(n-1)! + 1] \equiv 0 \pmod n \Rightarrow \text{mdc}(n, 4) = 1$

$\Rightarrow n$ é primo pela recíproca do Teorema de Wilson.

Também $2[2(n-1)! + 1] + n + 2 \equiv 0 \pmod{n+2}$

$\Rightarrow 2[2(n-1)! + 1] \equiv 0 \pmod{(n+2)}$

$\Rightarrow \text{mdc}(n+2, 2) = 1$

$2(n-1)! + 1 \equiv 0 \pmod{n+2}$

$\Rightarrow (n+1)! + 1 \equiv 0 \pmod{n+2}$

$\Rightarrow n+2$ é primo pela recíproca

Se $n = 2k$

$k = 1 \quad n = 2$

$n+2 = 4$

$4 \nmid 4[1! + 1] + 2$, pois $4 \nmid 2$.

4 não satisfaz a condição.

A condição não é válida para $n=2$, mas não para $n+2=4$.

Se $n = 2k$, $k > 2$, então $n > 4$ é composto

$\Rightarrow n \mid (n-1)!$

Assim $4[(n-1)! + 1] + n \equiv 4 \pmod{n}$

Logo $4[(n-1)! + 1] + n \equiv 4 \pmod{n} \neq 0$

A

4. **(2,5)**

(a) Determine todos os elementos inversíveis de $\mathbb{Z}_{20}$ e seus inversos.

(b) Determine todas as soluções não congruentes de $12X \equiv 4 (\text{mod} 20)$.

(a) $\varphi(20) = \varphi(4) \times \varphi(5) = 2 \times 4 = 8$

$\{\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}\}$

$\overline{1} \cdot \overline{1} = \overline{1}$

$\overline{19} \times \overline{19} = -\overline{1} \times -\overline{1} = \overline{1}$

$\overline{3} \times \overline{7} = \overline{1} \iff (-\overline{3})(-\overline{7}) = \overline{1} \Rightarrow \overline{17} \times \overline{13} = \overline{1}$

$\overline{9} \times \overline{9} = \overline{1} \iff (-9)(-9) = \overline{1} \Rightarrow \overline{11} \times \overline{11} = \overline{1}$

ELEMENTO INVERSÍVEL	INVERSO
$\overline{1}$	$\overline{1}$
$\overline{3}$	$\overline{7}$
$\overline{7}$	$\overline{3}$
$\overline{9}$	$\overline{9}$
$\overline{11}$	$\overline{11}$
$\overline{13}$	$\overline{17}$
$\overline{17}$	$\overline{13}$
$\overline{19}$	$\overline{19}$

(b) $12X \equiv 4 (\text{mod} 20)$

$\text{mdc}(12, 20) = 4 \mid 4$

$12X \equiv 4 (\text{mod} 20) \iff$

$3X \equiv 1 (\text{mod} 5)$

$2 * 3 = 6 \equiv 1 (\text{mod} 5)$

Logo $X \equiv 2 (\text{mod} 5)$

Assim, $X = 2 + 5t$, $t \in \mathbb{Z}$

As soluções não congruentes mod 20 são $4 = \text{mdc}(12, 20)$.

$X = 2_0 + 5t$, $t = 0, 1, 2, 3$,

Temos então $x_0 = 2$, $x_1 = 7$, $x_2 = 12$, $x_3 = 17$.

(Se você pensar em $\mathbb{Z}_{20}$, a equação $\overline{12}X = \overline{4}$ tem 4 soluções distintas).

4. **(2,5)**

(a) Determine todos os elementos inversíveis de $\mathbb{Z}_{28}$ e seus inversos.

(b) Determine todas as soluções não congruentes de $12X \equiv 4 (\text{mod} 28)$.

(a) $\varphi(28) = \varphi(4)\varphi(7) = 12$

Temos 12 elementos inversíveis

$\{\overline{1}, \overline{3}, \overline{5}, \overline{9}, \overline{11}, \overline{13}, \overline{15}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{27}\}$

$\overline{1}^2 = \overline{1}$ e $(-\overline{1})^2 = \overline{27}^2 = \overline{1}$

$1 = 28 - 3\times 9$. Logo o inverso de $\overline{3}$ é $-\overline{9} = \overline{19}$

$\overline{3} \times \overline{19} = \overline{1}$

$1 = 2\times 28 - 5\times 11 \Leftrightarrow -5\times 11 \equiv 1 (\text{mod } 28)$

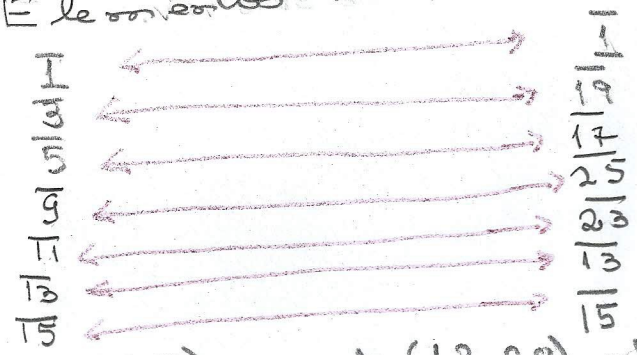
Assim $\overline{5}^{-1} = -\overline{11} = \overline{17}$

$1 = 28 - 3\times 9$. Logo $\overline{9}^{-1} = -\overline{3} = \overline{25}$

$\overline{11}^{-1} = -\overline{5} = \overline{23}$

$\overline{13}^{-1} = \overline{13}$ e $\overline{15}^{-1} = \overline{15}$

Assim; Elementos Inversíveis:



(b) $12X \equiv 4 (\text{mod } 28)$ $\quad mdc(12, 28) = 4$ e $4 \mid 4$

Logo $12X \equiv 4 (\text{mod } 28) \Leftrightarrow$

$3X \equiv 1 (\text{mod } 7)$

$\Leftrightarrow 5 \cdot 3X \equiv 5 (\text{mod } 7)$

$\Leftrightarrow X \equiv 5 (\text{mod } 7)$

$\Leftrightarrow X = 5 + 7t, \quad t \in \mathbb{Z}$

As soluções não congruentes mod 28 são $4 = mdc(12, 28)$ e são dadas por

$$X = 5 + \frac{28}{4} t, \quad t = 0, 1, 2, 3$$

$x_0 = 5 \quad x_1 = 12 \quad x_2 = 19 \quad x_3 = 26$

(Ou seja em $\mathbb{Z}_{28}$ a equação linear $\overline{12}X = \overline{4}$ tem 4 soluções: $\overline{5}, \overline{12}, \overline{19}, \overline{26}$)