

3ª Prova Mat120 - Álgebra noturno, Turma 48
Licenciatura em Matemática Prof. Eduardo Marcos
18 de junho de 2019

Nome : _____
 N°USP : _____

Prof Eduardo do Nascimento Marcos

Q	N
1	
2	
3	
4	
5	
Total	

1. A prova pode ser feita a lápis;
2. Não é permitido o uso de calculadora;
3. Celulares e outras ferramentas eletrônicas devem ser desligados;
4. Boa Prova
5. Resolva 4 questões.

1ª) **Questão:** (Valor 2,5 pt)

Nesta questão cada item vale 0,2 pontos, sua nota neste item será calculada assim: Seja A = número de respostas certas e B o número de respostas erradas a nota na questão é o $\max\{0,25 \times (A - B), 0\}$. Em particular, qualquer item não respondido não entra no cálculo da nota. Nesta questão não serão olhadas as justificativas você responde V para cada afirmação que pensar que é verdadeira e F para as que pensa que é falsa. Deixa sem resposta as que não quiser responde nem V nem F.

1. Se p é um número inteiro então p sempre divide $(a^p)^p - a$. **F**
2. No anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$ onde n um número qualquer, a equação $x^2 + 1 = 0$ tem máximo 2 soluções. **F**
3. Se uma equação polinomial com coeficientes inteiros tem em \mathbb{Z} como solução 2 inteiros distintos então ela tem solução módulo n para todo inteiro n . **✓**
4. Dados a e b inteiros quaisquer com $b \neq 0$ existem infinitos q e r tais que. $a = bq + r$ **✓**
5. 11 divide $59^{10} - 1$. **✓** (Teorema de Euler)
6. Sejam a, b, c três inteiros. Se $a \mid bc$ e $a \nmid b$ então $a \mid c$ ou $\text{mdc}(a, b) \neq 1$ **✓**
7. O resto da divisão de um decima potência por 11 deve ser 0 ou 1. **✓**
8. Seja K um corpo qualquer e $p(x)$ um polinômio sobre $K[x]$, se $p(a) = 0$ para todo $a \in K$, então $p(x)$ é o polinômio zero. **F**
9. O produto de 4 inteiros consecutivos é sempre um múltiplo de 8. **✓**
10. Sejam a e b inteiros não nulos, então, $\text{mdc}(a, b) = \text{mmc}(a, b)$ se e somente se $a = b$. **F**

não necessárias nesta prova.

1) Falso $4 + (2^2)^2 - 2 = 14$

2) Falso tome $\mathbb{Z}/65\mathbb{Z} \cong \mathbb{Z}/5 \times \mathbb{Z}/13\mathbb{Z}$

aqui há 4 raízes a saber
8, 57, 18, 47 (Pergunta como descobri isso?)

3) como $x \equiv y \Leftrightarrow x' \equiv y' \Rightarrow x + y \equiv y' + z'$
 $x + y \equiv y' + z'$

temos que se $P(x) \equiv 0$ em \mathbb{Z} então

$P(\bar{x}) = \bar{0}$ em $\mathbb{Z}/m\mathbb{Z}$ logo o resultado
é verdadeiro

4) verdadeiro basta por exemplo formar

$r = a - bq$ e variar q

ou seja para cada q inteiro existe um r

logo existem infinitos r .

5) Teorema de Fermat. Como 11 é primo

e $11 \nmid 59$ temos $59^{10} \equiv 1 \pmod{11}$ Logo

$59^{10} - 1 \equiv 0 \pmod{11}$ isto é $11 \mid 59^{10} - 1$.

6) verdadeiro

se $\text{mdc}(a, b) = 1$ teríamos existir x, y tais que

$xa + yb = c$ logo se além disso $a \mid b$ teríamos

$a \mid c$ ou seja

$a \mid b$ e $a + b \mid c$ e $\text{mdc}(a, b) = 1$ então $a \mid c$

e o resultado segue

7) Verdadeira

pois se a não é divisível por 10
então pelo teorema de Fermat

$a^{10} \equiv 1 \pmod{11}$ ou seja resta da
divisão de a por 11 é 1.

8) Falso por exemplo em $\mathbb{Z}/2\mathbb{Z}$

Tome

$x(x-1) = p(x)$ então $p(x)$ não é o

polinômio nulo mas $p(0) = p(1) = 0$

(além se K é um corpo finito

$K = \{a_1, \dots, a_t\}$ então o polinômio

$p(x) = (x-a_1) \dots (x-a_t)$ de grau t

é tal que $p(a_i) = 0$ para todo a_i .)

9) Sim pois existem 2 pares e um deles
é múltiplo de 4 logo o produto
é múltiplo de 8.

10) Falso $\text{mdc}(2, -2) = 2$ mas $2 \neq -2$.

2ª) Questão: (Valor 2,5pt)

Descreva o conjunto solução das seguintes equações diofantinas.

1. $31x + 7y = 4$.

2. $91x - 221y = 2106$.

1) $\text{mdc}(31, 7) = 1$ Logo a equação tem solução,

$y = 5$ e $x = -1$ é uma solução Logo

$$S = \{(-1 + 7t, 5 - 31t) : t \in \mathbb{Z}\}$$

2) $\text{mdc}(91, 221) = ?$

221	91	39	13
182	78	0	
39	13		

$$\begin{array}{r} 2106 \\ 80 \\ 026 \\ 0 \end{array} \quad \begin{array}{r} 11313 \\ 162 \end{array}$$

ou seja a equação tem solução e

Logo a equação é equivalente a

$$7x - 17y = 162$$

$$\begin{array}{r} 2 \quad 2 \\ 17 \overline{) 7} \quad 3 \quad 1 \\ 3 \quad 1 \end{array}$$

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (17 - 2 \cdot 7) =$$

$$7 \cdot 4 - 17 \cdot 2 = 1 \quad \text{Logo}$$

$$7 \cdot 4 \cdot 162 - 17 \cdot 162 \cdot 2 = 162$$

ou seja uma solução particular é $(648, 324)$

$$\text{Logo } S = \{(648 + 17t, 324 + 7t) : t \in \mathbb{Z}\}$$

3ª) Questão: (Valor 2,5 pt) Seja b um inteiro maior que 1, cuja expressão na base 10 é

$$b = r_n 10^n + r_{n-1} 10^{n-1} + \dots + r_1 10 + r_0$$

Prove que:

1. $4|b$ se e só se $4|(r_0 + r_1 10)$.
2. $25|b$ se e só se $25|(r_0 + r_1 10)$.
3. $6|b$ se e só se $3|(r_0 + r_1 + \dots + r_n)$ e $2|r_0$.

Prova 1) $4|b \Leftrightarrow 4|10^2(r_n 10^{n-2} + \dots + r_2) + r_1 10 + r_0$

Como $4|10^2$ temos $4|b \Leftrightarrow 4|r_1 10 + r_0$

2) $25|b \Leftrightarrow 25|10^2(r_n 10^{n-2} + \dots + r_2) + r_1 10 + r_0$

Como $25|10^2(r_n 10^{n-2} + \dots + r_2)$ temos

$25|b \Leftrightarrow 25|r_1 10 + r_0$

3) $6|b \Leftrightarrow 3|b$ e $2|b \Leftrightarrow 3|r_0 + r_1 + \dots + r_n$ e $2|r_0$

4ª) Questão: (Valor 2,5 pt) Determine o quociente e o resto da divisão de $f(x)$ por $g(x)$ nos seguintes casos.

1. $f(x) = x^4 - 1, g(x) = -x^2 + 2$ em $\mathbb{Q}[x]$

2. $f(x) = x^2 + 2, g(x) = 2x - 1$ em $\frac{\mathbb{Z}}{5\mathbb{Z}}[x]$

$$\begin{array}{r} x^4 - 1 \\ \underline{x^2 \cdot x^2} \\ 2x^2 - 1 \\ \underline{2x^2 - 1} \\ 0 \end{array} \quad \begin{array}{r} \overline{-x^2 + 2} \\ -x^2 - 2 \end{array}$$

Logo o quociente é $-x^2 - 2$ e o resto 3

2)
$$\begin{array}{r} x^2 + 2 \\ \underline{x^2 - 3x} \\ 3x + 2 \\ \underline{3x - 4} \\ -6 \end{array} \quad \begin{array}{r} \overline{2x - 1} \\ 3x + 4 \end{array}$$

Logo o quociente é $3x + 4$ e o resto $-6 = \bar{3}$

Prova real

$$(2x - 1)(3x + 4) + \bar{3} =$$

$$x^2 + (8 - 3)x - 4 + 1 = 2x^2 - 3 = x^2 + 2.$$

$$x^2 - 1 = x^2 - 1$$

5ª) Questão: (Valor 2,5 pt)

Mostre que o conjunto dos inteiros primos da forma $4n + 3$ é infinito.

Observe o produto de dois inteiros congruentes a 1 módulo 4 e congruente a 1 módulo 4.

Agora suponha que existem apenas um número finito de primos da forma

$4n + 3$. Seja $S = \{p_1, \dots, p_n\}$ esse conjunto

Considere o inteiro

$\alpha = 4p_1 \dots p_n + 3$ os divisores primos de α são ímpares

mas nem todos podem ser congruentes a 1 módulo 4, pois pela observação α seria congruente a 1 módulo 4

Logo algum $p_i \mid \alpha$ e $p_i \neq 3$ pois $p_i + 4p_2 \dots p_n$

Se $p_i \neq 3$

$p_i \mid \alpha$ e $p_i \mid 4p_2 \dots p_n + 3$ como

$p_i \mid p_2 \dots p_n$ (pois é um dos fatores

teríamos $p_i \mid 3$ ∇ .

E o resultado está mostrado