Prova substitutiva de Introdução à Teoria dos Números - Mat 223
Licenciatura em Matemática
27 de Novembro de 2018

Nome : _____
N^{o}USP : _____

Prof. Eduardo do Nascimento Marcos

	Q	N
	1	
	2	
	3	
	4	
	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. Anotações não estão permitidas.
5. Boa Prova

1. Questão:

   Nesta questão cada ítem vale 0,25 pontos, sua nota neste ítem será calculada assim: Seja A= número de respostas certas e B o número de respostas erradas a nota na questão é o $\mathbf{max}\{0.25 \times (A - B), 0\}$. Em particular qualquer ítem não respondido não entra no cálculo da nota.

F 1. Existe uma raiz primitiva da unidade módulo 20.

F 2. Num corpo k o conjunto solução da equação $x^2 - 1 = 0$ tem 2 elementos.

V 3. Se um polinômio de grau 3 em $k[x]$, onde k é um corpo, é irredutível então ele certamente não tem raiz nesse corpo.

F 4. Todo anel comutativo, associativo com unidade, que tem 9 elementos é um corpo.

F 5. 19 divide $38^{18} - 1$.

F 6. Seja p um primo impar então todo inteiro não divisível por p é uma raiz primitiva da unidade módulo p.

V 7. O resto da divisão de um quadrado perfeito por 4 deve ser 0 ou 1.

V 8. Sejam a e b inteiros não nulos e c um outro inteiro. Se a equação $ax + by = c$ tem solução então c é um múltiplo de $mdc(a, b)$.

V 9. Uma equação do segundo grau, $ax^2 + bx + c = 0$, em $\mathbb{Z}/n\mathbb{Z}$ com n primo tem no máximo duas soluções .

V 10. Sejam a e b inteiros positivos. Então, $\mathbf{mdc}(a, b) = \mathbf{mmc}(a, b)$ se e somente se $a = b$.

1) os ~~characteristicos~~ que tem raiz primitiva são 2, 4 e os nº da forma p^n com p primo impar ou da forma $2p^n$ " " " " .

2) em $\mathbb{Z}/_{22}$ só existe uma solução $((x^2-1)=(x-1)^2)$

3) Se tivesse raiz seria redutivel

4) $\mathbb{Z}/_{32} \times \mathbb{Z}/_{32}$ não é corpo

5) Se dividisse teríamos 19|1

6) 1 certamente não é raiz primitiva da unidade

7) Sim $x^2 \equiv 0$ ou 1

8) claro $mdc(a,b) \mid ax+by=c$

... $mdc \cdot mmc = ab$ ... nesse caso $\mathbb{Z}/n\mathbb{Z}$ é corpo

2. Questão:

Seja $(F_n)_{n\geq 1}$ a sequência de Fibonatti assim definida:

$$F_1 = F_2 = 1, F_n = F_{n-1} + F_{n-2}, \text{ para } n \geq 2$$

prove ou dê contra exemplo para as seguintes afirmações.

(a) $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$ para $n \geq 2$

(b) $F_2 + F_4 + \cdots + F_{2n} = F_{2n+1} - 1$ para $n \geq 1$

(c) $mdc(F_n, F_{n+1}) = 1$

a) Vamos provar usando indução em n, para $n \geq 2$.

1) $n = 2$ $\quad F_4 = F_1 + F_3$? ou seja $F_4 = \overset{F_1 + F_3}{1 + 2} = 3$?

como $F_4 = F_3 + F_2 = 2 + 1 = 3$ o resultado vale

assuma que o resultado vale para k com $k \geq 2$

Calculemos $F_1 + F_3 + \cdots + F_{2k-1} + F_{2(k+1)-1} \overset{HI}{=}$

$$F_{2k} + F_{2k+1} = F_{2k+2} = F_{2(k+1)}$$

e o resultado segue por indução.

b) Novamente usaremos indução para $n \geq 1$

Para $n = 1$ temos o ~~lado esquerdo~~

$F_2 \overset{?}{=} F_3 - 1$ o lado esquerdo vale 1 e o direito $2 - 1 = 1$

Logo o resultado vale para $n = 1$.

assuma o resultado válido para $n = k$ $k \geq 1$

& calculemos o lado esquerdo, assumindo isto,

para $n = k + 1$

$$F_2 + F_4 + \cdots + F_{2k} + F_{2k+2} = F_{2k+1} - 1 + F_{2k+2}$$

$$= F_{2k+3} - 1 = F_{2(k+1)+1} - 1$$ que a fórmula do lado

direito para $k + 1$. O resultado segue por indução

c) Novamente indução em n, $n = 1$ $mdc(F_1, F_2) = mdc(1, 1) = 1$

assuma que vale para $n = k$ então

$mdc(F_{k+1}, F_{k+2}) = mdc(F_{k+1}, F_k + F_{k+1}) = mdc(F_{k+1}, F_k)$

$= 1$ e.q.d.

3. Questão:

Mostre que se $n > 1$ então a soma

$$1 + 1/2 + \cdots 1/n$$

não é um número inteiro.

Prova

Seja 2^k a maior potencia de 2 que aparece em algum nº do conjunto $\{1, 2, \ldots, n\}$

Então ele aparece só uma vez e no nº $= 2^k$ pois se $2^k \alpha < n$ com $n \geq 2$

Então $2^{k+1} < n$ logo

$$1 + \frac{1}{2} + \cdots + \frac{1}{2^k} + \cdots + \frac{1}{n} =$$

$$\frac{1}{2^k} + \frac{x}{2^{k-1}\alpha}$$ onde α é impar, x é inteiro

Se multiplicarmos por $2^{k-1}\alpha$ temos

$\frac{\alpha}{2} + x$ que não é inteiro

Logo como $(2^{k-1}\alpha)\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\right)$ não é inteiro segue que

$1 + \frac{1}{2} + \cdots + \frac{1}{n}$ não é inteiro

4. Questão: Demonstrar que a equação $6x^2 + 5x + 1 \equiv 0(\textbf{mod}\ m)$ tem solução para qualquer valor natural de $m > 1$.

a) Se $mdc(3, m) = 1$ então 3 é invertível mod m

e temos $6(-3^{-1})^2 + 5(-3^{-1}) + 1 =$

$2 \cdot 3^{-1} - 5 \cdot 3^{-1} + 1 =$

$2\,3^{-1} - 2\,3^{-1} - 3 \cdot 3^{-1} + 1 = 0$

Se $mdc(2, m) = 1$ então

$6(-2^{-1})^2 + 5(-2^{-1}) + 1 =$

$3 \cdot 2^{-1} + 3 \cdot (-2^{-1}) - 1 + 1 = 0$

Agora seja $m = 2^{\alpha_1} 3^{\alpha_2} \cdots p_m^{\alpha_m}$ se $\alpha_1 = 0$ ou $\alpha_2 = 0$ já temos uma solução pelo anterior. assuma $\alpha_1 > 0$ $\alpha_2 > 0$

~~Logo existem~~

Temos Existe m_1 tal que

$6m_1^2 + 5m_1 + 1 \equiv 0 \ (2^{\alpha_1})$ e m_2 tal que

$6m_2^2 + 5m_2 + 1 \equiv 0 \ (3^{\alpha_2} \cdots p_m^{\alpha_m})$

O sistema de equações $x \equiv m_1 \ (2^{\alpha_1})$, $x \equiv m_2 \ (3^{\alpha_2} \cdots p_m^{\alpha_m})$ tem solução

Logo $6x^2 + 5x + 1 \underset{2^{\alpha}}{\equiv} 6m_1^2 + 5m_1 + 1 \equiv 0$

$6x^2 + 5x + 1 \underset{3^{\alpha_2} \cdots p_m^{\alpha_m}}{\equiv} 6m_2^2 + 6m_2 + 1 \equiv 0$

$6x^2 + 5x + 1 \equiv 0 \ (2^{\alpha_1} 3^{\alpha_2} \cdots p_m^{\alpha_m})$ c.q.d.