**Terceira prova de Introdução à Teoria dos Números - Mat 223**
**Licenciatura em Matem àtica**
**13 de novembro de 2018**

| Q | N |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| Total | |

Nome : Quase Ricardo Calvarito
N°USP : _____

Prof. Eduardo do Nascimento Marcos

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. Cada questão vale 2 pontos, se sua nota for maior que 10, ela será reduzida a 10. Tomara que seja.

1. Questão:

   Nesta questão cada ítem vale 0,2 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 $\mathbf{max}\{0.2 \times (A - B), 0\}$. Em particular qualquer ítem não respondido não entra no cálculo da nota.

   V 1. Se todo elemento $\bar{x}$, não nulo, em $\frac{\mathbb{Z}}{n\mathbb{Z}}$ é tal que existe $\bar{y}$ com $\bar{x}.\bar{y} = \bar{1}$, então $n$ é primo.

   F 2. No anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$ onde $n$ é um número natural maior que 1 , a equação $x^2 - 1 = 0$ tem no máximo 2 soluções.

   F 3. Se um inteiro $a$ é resíduo quadrático modulo $p$ para $p$ primo então ele é uma raiz primitiva da unidade.

   F 4. Se a equação $x^n = a$ com $n > 0$ e $a$ inteiro tem uma raiz real então essa raiz é inteira.

   V 5. Existe um corpo com 9 elementos.

   F 6. Sejam $a, b, c$ três inteiros. Se $a \mid bc$ e $a \nmid b$ então $a \mid c$.

   V 7. No anel de polinômios $\mathbb{C}[X]$ toda equação polinomial de grau 6 tem uma raiz.

   V 8. Sejam $a$ e $b$ inteiros primos com 22. Então eles são primos entre si se e somente se a equação $ax + by = 22$ tem solução.

   V 9. Se $n$ tem uma raiz primitiva da unidade então para todo inteiro positivo $t$ a equação $x^t = 1$ tem no máximo $t$ soluções no anel $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

   V 10. Sobre o conjunto dos números reais todo polinômios de grau 3 é redutível.

2. Questão:

Prove ou dê contra exemplo.

Se o polinômios $a_n x^n + \cdots + a_0$ com coeficientes inteiros tem uma raiz racional $\frac{p}{q}$ com $mdc(p,q) = 1$ então $p \mid a_0$ e $q \mid a_n$.

$a_n \frac{p^n}{q^n} + \cdots + a_1 \frac{p}{q} + a_0 = 0 \iff$

$a_n p^n + \cdots + a_1 p q^{n-1} = -a_0 q^n$

como $p \mid a_n p^n + \cdots + a_1 p q^{n-1}$ e $mdc(p,q) = mdc(p,q^n) = 1$

segue que $p \mid a_0$

Analogamente

$a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = -a_n p^n$

Como $q \mid a_{n-1} p^{n-1} q + \cdots + a_0 q^n = -a_n p^n$

e $mdc(q, p^n) = 1$ segue que

$q \mid a_n$ ∎

3. Questão:

Prove ou dê contra exemplo:

Seja $m \in \mathbb{Z}, m > 0$ se existe uma raiz primitiva da unidade de ordem $m-1$ então ela é primitiva e $m$ é primo.

$\phi(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) = (p_1^{\alpha_1} \cdots p_m^{\alpha_m})\left(1 - \frac{1}{p_1}\right) \cdots$

Se existe uma raiz primitiva de ordem $m-1$ isso significa que todo elemento em $\mathbb{Z}/m\mathbb{Z} \setminus \{0\}$ é invertível Logo todo $t$ talque $1 \leq t < m$ é primo com $m$ Logo $m$ não tem nenhum divisor $t$ talque $1 < t < m$ logo $m$ é primo.

64 | 19
07 | 3

80 | 48
08 | 4

70 | 19
13 | 3

4. Questão

Encontre uma raiz primitiva de 1 relativa aos seguintes números, diga a seguir quantas raizes primitivas não congruentes existem:
10, 19, 50

para o nº 10 precisamos encontrar uma raiz primitiva impar mod 5 $\phi(5)=4$

$3^2=4$ $2^4=16$ ∴ 2 é raiz primitiva

Logo $7=2+5$ é raiz primitiva impar

Logo 7 é raiz primitiva modulo 10

Existes $\phi(\phi(10))=\phi(\phi(5))=\phi(4)=2$ raizes primitivas não congruentes.

② 19 é primo logo $\phi(19)=18$

Logo a ordem de um elemento inversivel diferente de 1 divide 18 portanto a ordem é 2, 3, 6, 9 ou 18

$2^2=4$ $2^3=8$ $2^6=64\equiv 7$ (mod 19)

$2^9\equiv 2^3\cdot 7=80\equiv 13$

∴ $o(2)=18$ ou seja 2 é uma raiz primitiva

Existem $\phi(18)=\phi(9)=9\left(1-\frac{1}{3}\right)=9-3=6$ raizes primitivas

Existem $\phi(50)=\phi(25)=25\left(1-\frac{1}{5}\right)=25-5=20$ raizes primitivas da unidade

③ $50=2\cdot 5^2$ raizes primitiva de 5 $\phi(5)=4$ ordem 1, 2 4

2 é raiz primitiva mod 5 $2\not\equiv 1 \pmod{25}$

Logo 2 é raiz prim. mod 25 logo $2+25=27$ é raiz

5. Questão:

Prove ou dê contra exemplo: Se $a$ é resíduo quadrático módulo $p$ onde $p$ é um primo ímpar então $a$ não pode ser uma raiz primitiva da unidade.

$a \equiv b^2$ se $a$ é raiz primitiva

como qualquer potencia de $a$

tambem é' potencia de $b$

$b$ tambem é' raiz primitiva

$b = a^n$ para algum $n$ ∴

$b^2 = a^{2n} = a$ ∴ $a^{2n-1} \equiv 1$

agora a ordem de $a$ é' $p-1$

portanto $p-1 \mid 2n-1$

mas $p-1$ é' par $\longrightarrow\!\longleftarrow$.

6. Questão:

Enuncie e demonstre o teorema chinês dos restos.

Enunciado:

Sejam $n_1, \dots, n_k$ dois a dois primos entre si e $a_1, \dots, a_k$ inteiros então o sistema de equações

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

tem solução que é única módulo $n = n_1 \cdot \dots \cdot n_k$

Prova: Existência seja $M_k = \frac{n_1 \cdots n_k}{n_k}$ para todo $i$

Então $\text{mdc}(n_k, M_k) = 1$ logo existem $a_k$ e $b_k$ tais que $a_k n_k + b_k M_k \equiv a_k \pmod{n_k}$

Considere $b_1 M_1 + b_2 M_2 + \dots + b_k M_k = x$

Temos $x \equiv b_i M_i \equiv a_i \pmod{n_i}$ para todo $i$

logo $x$ é solução.

Suponha que $x_1$ é uma solução e seja $x_2$ uma outra solução qualquer.

$n_i \mid x_1 - x_2$ $\therefore$ com $\text{mdc}(n_i, n_j) = 0$

segue que $n \mid x_1 - x_2$ isto é $x_1 \equiv x_2 \pmod{n}$ ∎