Álgebra 1

Lista 04

(Inteiros Coprimos e Primos)

4.1. (Um produto pode dividir). Se m.d.c.$(a, b) = 1$ e ambos a e b dividem c, demonstre que ab divide c.

Se $mdc(a, b) = 1$, então $\exists\ x, y \in \mathbb{Z}$ tal que $ax + by = 1(1)$

Além disso, como $a \mid c$ e $b \mid c$ temos:

$c = ak_1, k_1 \in \mathbb{Z}$ e $c = bk_2, k_2 \in \mathbb{Z}$

Fazendo $c \cdot (1) : c = cax + cby$

Substituindo em (2) e (3) : $c = ab(k_2x) + ab(k_1y)$

$c = ab(k_2x + k_1y)$, como $k_2x + k_1y \in \mathbb{Z}$

Logo, $ab \mid c$

4.2. (Teorema da raiz integral). Demonstre que: se a equação $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ onde $n > 0$ e a_0 são inteiros, possui uma raiz racional, então esta raiz é um número inteiro. (Dica: use o Exercício 3.7.)

Seja $x = \frac{p}{q}$ a racional dessa equação na forma mais simples tal que $mdc(p, q) = 1$.

Substituindo essa raiz temos :

$$(\frac{p}{q})^n + a_{n-1}(\frac{p}{q})^{n-1} + \ldots + a_0 = 0(\cdot q^n)$$
$$p^n + a_{n-1}(p)^{n-1}q + \ldots + a_0q^n = 0$$
$$p^n = -a_{n-1}(p)^{n-1}q + \ldots - a_0q^n$$
$$p^n = q \cdot (-a_{n-1}(p)^{n-1} + \ldots - a_0q^{n-1})$$

Assim, $q \mid p^n$

Conteúdo, $mdc(p, q) = 1$, ou seja, são primos entre si

Então, a única maneira de q dividir p é se q for 1 ou -1, porém $q > 0$.

Portanto, $q = 1 \Rightarrow x = \frac{p}{q} = p \in \mathbb{Z}$

4.3. (Mersenne e Fermat). Seja n um inteiro > 1. Mostre que:

(i) se $2^n - 1$ é um primo, então n deve ser primo;

Contrapositiva: Se n é composto, então $2^{n-1} - 1$ deve ser composto

Suponha que n é composto, ou seja, $n = rs$, com $r \cdot s > 1$.

Sabendo que $(x - y \mid x^k - y^k)$ temos que : $2^r - 1 \mid (2^r)^s - 1$, ou seja, $2^n - 1$ não é primo, contradição

Logo, n é primo.

(ii) se $2^n + 1$ é um primo então n deve ser uma potência de 2. (Dica: se d for um inteiro > 1...)

Suponha que $p \neq 2$ é um fator primo de n.Então, $n = n'p$ para algum $n' \in \mathbb{N}^*$.

Como p é ímpar segue que : $2^{n'} + 1 \mid (2^{n'})^p + 1^p = 2^n + 1$

Logo, $2^{n'}+1$ têm um divisor diferente de 1 e de 2^n+1, contradição pois 2^n+1 é primo

Portanto, o único fator primo de n é 2,e $n=2^m,$ com $n \in \mathbb{N}^*$

4.4. (Valoração p-ádica de $n!$). Sejam n um inteiro ≥ 1 e p um primo. Se, para cada número real x, denotarmos por $[x]$ o maior inteiro $\leq x$, prove que o maior inteiro N tal que p^N divide $n!$ é dado por $N=\sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$.

4.5. (O polinômio x^2+x+41 não produz só primos). Prove que dentre os números representados pelo polinômio $a_nx^n+\ldots+a_0$, onde $n>0$ e a_0 são inteiros com $a_n>0$, existe uma infinidade de números não primos.