Monitoria: Ex 4, 5, 10, 15

Ex 4: Em $\mathbb{Z}_m$, m não primo.

1) $gr(fg)$ pode ser diferente de $gr(f) + gr(g)$.

Como m não é primo, existe $\bar{a} \in \mathbb{Z}_m$ tal que $mdc(a, m) \neq 1$. Logo, $\bar{a}$ é divisor de zero e, portanto, existe $\bar{b} \in \mathbb{Z}_m$, $\bar{b} \neq 0$ tal que $\bar{a} \cdot \bar{b} = \bar{0}$.

Tome $f = \bar{a}x$ e $g = \bar{b}x$. Assim,

$gr(f) = 1$ e $gr(g) = 1$, mas $fg = \bar{0}$ que não possui grau definido (ou $gr(fg) = -\infty$)

2) Para verificar o item (c) use o exemplo anterior.

$\blacksquare$

Ex 5: $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

(a) Considere $f = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$, $a_i \in \mathbb{Z}_5$, $i = 0, \dots, 4$

Veja que para cada a_i temos 5 possibilidades, logo, temos $\underset{a_4}{\underline{5}} \cdot \underset{a_3}{\underline{5}} \cdot \underset{a_2}{\underline{5}} \cdot \underset{a_1}{\underline{5}} \cdot \underset{a_0}{\underline{5}} - 1^{(*)}$

polinômios de grau ≤ 4

(*) Estamos retirando o caso $f = 0$.

Ex 10: $f = 5x^4 + 3x^3 + 1$, $g = 3x^2 + 2x + 1$

$f, g \in \mathbb{Z}_7[x]$

$$
\begin{array}{l|l}
5x^4 + 3x^3 + 0x^2 + 0x + 1 & 3x^2 + 2x + 1 \\
\hline
-5x^4 - 8x^3 - 4x^2 & 4x^2 + \ldots \\
\hline
0 + 2x^3 + 3x^2 + 0x + 1 &
\end{array}
$$

1) $\underset{4}{3}x \equiv 5 \pmod 7 \iff x \equiv 25 \pmod 7 \iff$

$x \equiv 4 \pmod 7$

2) $-5 \equiv 2 \pmod 7$ / 3) $-4 \equiv 3 \pmod 7$

Continuem (...)

Ex 13: Dem:

Temos que $f = g \cdot q + r$, $0 \leq gr(r) < gr(g)$.

Seja d um divisor comum de f e g, ou seja, $d | f$ e $d | g \Rightarrow$

$d | f$, $d | g \cdot q \Rightarrow d | f - gq = r$.

Logo, $d | g$ e $d | r$. Portanto, d é um divisor comum de g e r

$\blacksquare$

Ex 15 (Dica)

Dem:

Inicialmente, observe que pelo Alg. da divisão, existem $q, r \in K[x]$ tal que

$$f = g \cdot q + r, \quad 0 \leq gr(r) < gr(g)$$

Usando as ideias do ex 13, temos que $mdc(f,g) \mid g$ e $mdc(f,g) \mid r$. Considere $d = mdc(g,r) \Rightarrow d \mid g$ e $d \mid r \Rightarrow d \mid f$. Logo, $d \mid mdc(f,g)$.

Então, $mdc(f, g) = mdc(g, r)$ (Por que?)