

EXERCÍCIO PROGRAMA 1 (CONTINUAÇÃO)

Data de entrega: 10/10/2003

Algoritmo da divisão para polinômios. Sejam $a(x)$ e $b(x)$ polinômios. Suponha que o polinômio $b(x)$ seja *mônico*, isto é, o monômio de maior grau em $b(x)$ tem coeficiente 1. Neste caso, podemos dividir $a(x)$ por $b(x)$, obtendo polinômios $q(x)$ e $r(x)$ tais que

$$a(x) = q(x)b(x) + r(x).$$

Lembre que, neste processo, sempre temos que o grau de $r(x)$ é menor que o grau de $b(x)$. Acima, $q(x)$ é o *quociente* e $r(x)$ é o *resto* da divisão de $a(x)$ por $b(x)$.

Aritmética de polinômios módulo um polinômio. Seja $p(x)$ um polinômio mônico. A aritmética de polinômios pode ser feita ‘módulo $p(x)$ ’, da mesma forma podemos fazer aritmética ‘módulo p ’. A regra novamente é a seguinte. Ao considerarmos nossos polinômios, podemos sempre dividir por $p(x)$, e podemos identificar nossos polinômios com os respectivos restos desta divisão.

Os cálculos. Aqui, faremos aritmética de polinômios módulo certos polinômios especiais, e também usaremos coeficientes em $\mathbb{Z}/p\mathbb{Z}$, para certos valores de p .

Escreva um programa para fazer os cálculos abaixo.

1. Em $(\mathbb{Z}/2\mathbb{Z})[x]$: seja $p(x) = x^4 + x + 1$. Calcule

$$x^{15} \pmod{p(x)}.$$

2. Em $(\mathbb{Z}/3\mathbb{Z})[x]$: seja $p(x) = x^4 + x^3 + x^2 - x - 1$. Calcule

$$x^{80} \pmod{p(x)}$$

3. Em $(\mathbb{Z}/7\mathbb{Z})[x]$: sejam $p_1(x) = x^4 - x^3 - x^2 - 2x - 2$ e $p_2(x) = x^4 - 3x^3 + 5x^2 + 2x + 3$. Calcule

$$x^{2400} \pmod{p_1(x)} \quad \text{e} \quad x^{2400} \pmod{p_2(x)}.$$

Escolha qualquer polinômio $a(x) \neq 0$, e calcule

$$a(x)^{2400} \pmod{p_1(x)} \quad \text{e} \quad a(x)^{2400} \pmod{p_2(x)}.$$

Escolha qualquer polinômio $b(x) \neq 0$, e calcule

$$b(x)^{1200} \pmod{p_1(x)} \quad \text{e} \quad b(x)^{1200} \pmod{p_2(x)}.$$

Você consegue encontrar um polinômio $b(x)$ para o qual o resultado é diferente?