EXERCÍCIO PROGRAMA 1

Data de entrega: 10/10/2003

Aritmética modulo p. Seja p um número primo. No que segue, escrevemos $\mathbb{Z}/p\mathbb{Z}$ para o conjunto $\{0, 1, \ldots, p-1\}$. Podemos definir operações de soma e produto em $\mathbb{Z}/p\mathbb{Z}$ da seguinte forma: dados a e $b \in \mathbb{Z}/p\mathbb{Z}$, podemos definir $a + b \in \mathbb{Z}/p\mathbb{Z}$ como sendo

$$(a+b) \pmod{p},$$

isto é, o resto da divisão de $a + b$ por p (naturalmente, aqui entendemos por $a + b$ a soma usual de inteiros). Analogamente, podemos definir $ab \in \mathbb{Z}/p\mathbb{Z}$ como sendo

$$(ab) \pmod{p},$$

isto é, o resto da divisão de ab por p (aqui, ab denota o produto usual de inteiros).

Às vezes, ao fazermos contas em $\mathbb{Z}/p\mathbb{Z}$, é conveniente identificarmos inteiros fora do conjunto $\{0, 1, \ldots, p-1\}$ com elementos desse conjunto. A regra é simples: dado qualquer n inteiro, identificamos n com $n \pmod{p}$, o resto da divisão de n por p. Por exemplo, para $p = 7$, temos $7 = 0$, $8 = 1$, e $13 = -1$.

Exemplos. Suponha que $p = 5$. Então, em $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/5\mathbb{Z}$, temos $2 + 4 = 1$ e $2 \times 4 = 3$. Em $\mathbb{Z}/2\mathbb{Z}$ (isto é, $p = 2$), temos $1 + 1 = 0$ e $1 \times 0 = 0$.

Aritmética de polinômios. Consideraremos agora polinômios na variável (ou indeterminada) x, com coeficientes inteiros. Usualmente, o conjunto de tais polinômios é denotado por $\mathbb{Z}[x]$. Você conhece as operações de soma e produto de tais polinômios.

Suponha agora que temos um número primo p fixo. Podemos agora passar a considerar os coeficientes dos nossos polinômios como elementos de $\mathbb{Z}/p\mathbb{Z}$. Por exemplo, se $p = 3$, então os polinômios

$$4x^3 + 8x + 1, \quad x^{10} + 1, \quad \text{e} \quad 5x^2 - x + 1$$

de $\mathbb{Z}[x]$ podem ser entedidos, respectivamente, como os polinômios

$$x^3 + 2x + 1, \quad x^{10} + 1, \quad \text{e} \quad -x^2 - x + 1$$

em $(\mathbb{Z}/3\mathbb{Z})[x]$. Naturalmente, podemos tambem definir a soma e produto de polinômios com coeficientes em $\mathbb{Z}/p\mathbb{Z}$ de forma natural.

Exemplos. Suponha que $p = 3$. Então, em $(\mathbb{Z}/3\mathbb{Z})[x]$, temos

$$(x^3 + 2x + 1) + (x^{10} + 1) + (-x^2 - x + 1) = x^{10} + x^3 - x^2 + x$$

e

$$(x + 1)(2x - 1) = 2x^2 + x - 1, \quad (x + 1)^5 = x^5 - x^4 + x^3 + x^2 - x + 1.$$

Os cálculos. Neste exercício, você deve calcular (isto é, expandir) os seguintes polinômios:

1. Em $(\mathbb{Z}/2\mathbb{Z})[x]$:

$$(1 + x)^3, \quad (1 + x)^4, \quad (1 + x)^{15}, \quad (1 + x)^{16},$$

   e

$$(x^4 + x + 1)^{15}.$$

2. Em $(\mathbb{Z}/3\mathbb{Z})[x]$:

$$(x^4 + x^3 + x^2 - x - 1)^{80}.$$

3. **(Item revisado!)** Em $(\mathbb{Z}/7\mathbb{Z})[x]$:

$$(x^4 - x^3 - x^2 - 2x - 2)^{2400}, \quad (x^4 - 3x^3 + 5x^2 + 2x + 3)^{2400}.$$

   Em vez de imprimir estes polinômios em sua saída (a saída seria muito extensa), escreva seu programa de forma que o usuário pode examinar o coeficiente de x^k para qualquer k. Use seu programa para determinar o coeficiente de x^k para todo $k \leq 20$ e para $k = 9487$, $k = 9485$, e $k = 9370$.

Estratégia. Naturalmente, o que você deve fazer é escrever várias funções em C que manipulam polinômios com coeficientes em $\mathbb{Z}/p\mathbb{Z}$. Para tanto, você vai achar conveniente implementar, inicialmente, funções para calcular somas e produtos em $\mathbb{Z}/p\mathbb{Z}$. Feito isto, a sua tarefa é escrever funções para fazer cálculos com polinômios em $(\mathbb{Z}/p\mathbb{Z})[x]$.

Você deve, *obrigatoriamente*, representar os polinômios em seu programa como listas ligadas, com as células representando os monômios, isto é, parcelas como $3x^5$ (a informação contida na célula correspondente a este monômio seria o par de inteiros $(3, 5)$). Fica a seu critério escolher que tipo de lista ligada usar (linear, circular, com ou sem cabeça, etc). Faça um boa escolha!

Note que este EP tem uma continuação!!!

Observações

1. *Este EP é estritamente individual.* Exercícios semelhantes receberão nota 0.
2. Seja cuidadoso com sua programação (correção, documentação, apresentação, clareza do código, etc), dando especial atenção a suas estruturas de dados. A correção será feita levando isso em conta.
3. Comparem entre vocês o desempenho de seus programas.
4. Entregue o seu EP através do sistema PANDA.

5. Não deixe de incluir em seu código um *relatório* para discutir seu EP: discuta as estruturas de dados usadas, os algoritmos usados, etc. *Se você escrever claramente como funciona seu EP, o monitor terá pouca dificuldade em corrigi-lo, e assim você terá uma nota mais alta.* (Se o monitor sofrer para entender seu código, você pode imaginar o humor dele ao atribuir sua nota.)

Observação final. Enviem dúvidas para a lista de discussão da disciplina.