SME0230 - Introdução à Programação de Computadores
Primeiro semestre de 2017

Professora: Marina Andretta (andretta@icmc.usp.br)
Monitores: Douglas Buzzanello Tinoco (douglas.tinoco@usp.br)
Amanda Carrijo Viana Figur (amanda.figur@usp.br)

Exercícios de laboratório 8

Data: 25/05/2017.

Data máxima de entrega: 02/06/2017, até às 23h59min. Exercícios entregues fora do prazo não serão aceitos.

Forma de entrega: Os exercícios deverão ser entregues por e-mail para

`exercicios.sme0230.2017@gmail.com`

e o título do e-mail deverá ser `IPC2017_Ex8`. Cada exercício deve estar em um arquivo, chamado

`Ex8-<`*i*`>-IPC-<`*número usp*`>.c`

com `<`*i*`>` o número do exercício e `<`*número usp*`>` o número USP do aluno.
No início do arquivo deve haver um comentário com o nome e o número USP do aluno.

Exercício 1

Dado um número inteiro positivo $n > 1$, podemos descrever o conjunto

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$$

que é conjunto dos resultados possíveis da operação `x % n` (o resto da divisão de x por n), com $x \in \mathbb{N}$.
Ou seja, dado $x \in \mathbb{N}$, $\overline{x} =$ `x % n`.

Por exemplo:
Quando $n = 5$, temos $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.
Para $x = 15$, temos: $\overline{x} = \overline{15} =$ `15 % 5` $= \overline{0}$.
Para $y = 1753$, temos: $\overline{x} = \overline{1753} =$ `1753 % 5` $= \overline{3}$.

Podemos definir algumas operações com esses números. Dados $a, b, c \in \mathbb{N}$, temos:

$$\overline{a+b} = \overline{a} + \overline{b},$$

$$\overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Por exemplo:
Quando $n = 4$, temos $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. Vamos considerar os números 2 e $7 \in \mathbb{Z}$:

$$\overline{2+7} = \overline{9} = \overline{2} + \overline{7} = \overline{2} + \overline{3} = \overline{5} = \overline{1}.$$

$$\overline{2 \cdot 7} = \overline{14} = \overline{2} \cdot \overline{7} = \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}.$$

Escreva um programa em linguagem C que receba um número n e exiba o conjunto $\mathbb{Z}_n$. Em seguida, receba dois números naturais a, b e implemente **pelo menos** as seguintes funções:

1. Uma função que seja capaz de calcular os valores de $\overline{a}$ e $\overline{b}$.

2. Uma função que faça a operação `soma` de $\overline{a}$ e $\overline{b}$.

3. Uma função que faça a operação `multiplicação` de $\overline{a}$ e $\overline{b}$.

4. Uma função que receba um número $m > 0$, $m \in \mathbb{N}$, e seja capaz de calcular o valor de $(\overline{a})^m$ (ou seja a m-ésima `potência` de $\overline{a}$). Você **deve** usar a função `multiplicação` ao implementar esta função.

Note que os números digitados podem não ser válidos: seu programa deve prever este caso. Represente $\mathbb{Z}_n$ utilizando **vetores alocados dinamicamente!**

Não esqueça de fazer comentários e indentar o código corretamente!

Dica: pode ser que este exercício seja útil para o exercício a seguir.

Exercício 2

Dado um polinômio de grau p com coeficientes naturais e um número $n > 0$, $n \in \mathbb{N}$,

$$P(x) = a_p x^p + a_{p-1} x^{p-1} + ... + a_2 x^2 + a_1 x + a_0,$$

podemos construir a partir de $P(x)$ o chamado **polinômio reduzido** $\overline{P}(x)$ com coeficientes em $\mathbb{Z}_n$ da seguinte maneira:

$$\overline{P}(x) = \overline{a_p} x^p + \overline{a_{p-1}} x^{p-1} + ... + \overline{a_2} x^2 + \overline{a_1} x + \overline{a_0}.$$

Veja o seguinte exemplo:

$$P(x) = 3x^5 + 534!x^2 + 1, \text{ com } n = 2$$

O **polinômio reduzido** com coeficientes em $\mathbb{Z}_2$ seria:

$$\overline{P}(x) = \overline{1}x^5 + \overline{1}$$

Podemos, inclusive, calcular todos os valores de $\overline{P}(x)$ em $\mathbb{Z}_2$ (já que o conjunto é finito basta substituir x por um elemento de $\mathbb{Z}_2$ e fazer as operações). Veja abaixo:

$$\overline{P}(\overline{0}) = \overline{1} \cdot (\overline{0})^5 + \overline{1} \Rightarrow$$
$$\overline{P}(\overline{0}) = \overline{1}.$$

$$\overline{P}(\overline{1}) = \overline{1} \cdot (\overline{1})^5 + \overline{1} \Rightarrow$$
$$\overline{P}(\overline{1}) = \overline{0}.$$

Escreva um programa em linguagem C que receba do usuário um número $p > 0$, os coeficientes $a_i \in \mathbb{N}$, para $i = 0, ..., p$, de um polinômio $P(x)$, um número n e exiba o **polinômio reduzido** $\overline{P}(x)$. Além disso calcule todos os valores possíveis de $\overline{P}(x)$, com $x \in \mathbb{Z}_n$.

Todos os seus polinômios devem ser representados por **vetores alocados dinamicamente!** Note que os valores digitados pode não ser válido: seu programa deve prever este caso. Seu código **deve** estar modularizado, isto é, organizado por funções.

Não esqueça de fazer comentários e indentar o código corretamente!