Números Inteiros e Criptografia 2023.1

Hugo Nobrega

Lista de Exercícios 1

Entregue todas as questões marcadas com * até
8 de maio às 20:00 (nova data)

Questão 1. Em sala estamos usando palavras-chave como `enquanto` para fazer *laços de repetição* (também conhecidos como *loops*) em nossos algoritmos, i.e., linhas de código que se repetem diversas vezes, de acordo com algum tipo de condição. Por outro lado, o livro-texto usa instruções do tipo `vá para o passo X` para fazer esses laços.

Nos itens abaixo, converta os algoritmos que usam `enquanto` para que usem apenas `vá para`, e vice-versa, i.e., converta os que usam `vá para` para que usem apenas `enquanto`.

a.

```
Entradas: Naturais a, b
Saídas: O natural a+b

Passo 1: Resultado <- a
         Somar     <- b

Passo 2: Se Somar > 0:
             Resultado <- Resultado + 1
             Somar     <- Somar - 1
             Vá para o passo 2
         Senão:
             Vá para o passo 3

Passo 3: Retorne Resultado
```

*** b.**

```
Entradas: Uma lista de inteiros
Saídas: O produto dos elementos da lista dada na entrada

Passo 1: Resultado <- 1
         Índice    <- 0
         Final     <- Número de elementos de L

Passo 2: Enquanto Índice < Final:
             Atual     <- Elemento de L na posição Índice
             Resultado <- Resultado * Atual
             Índice    <- Índice + 1

Passo 3: Retorne Resultado
```

*** c.**

```
Entradas: Nenhuma
Saídas: Um número natural

Passo 1: Contagem <- 0

Passo 2: Contagem <- Contagem + 1
         Número   <- um número inteiro aleatório de 1 a 10^20

Passo 3: Se Número for 13:
             Retorne Contagem (e pare)
         Senão:
             Vá para o passo 2
```

Questão 2.

Definição 1. Dado um número real x, definimos seu *valor absoluto*, denotado $|x|$, de acordo com os seguintes casos:

$$|x| = \begin{cases} x, & \text{se } x \geqslant 0 \\ -x, & \text{caso contrário.} \end{cases}$$

Prove as seguintes generalizações do Teorema da Divisão Euclidiana: *Dica*: tente adaptar as provas que fizemos em aula.

*** a.**

Teorema 2. *Sejam x, d **inteiros** com $d \neq 0$. Existem únicos **inteiros** q, r tais que*

$$\begin{cases} x = dq + r \\ e \\ 0 \leqslant r < |d| \end{cases}$$

b.

Teorema 3. *Sejam x, d, y **inteiros** com $d \neq 0$. Existem únicos **inteiros** q, r tais que*

$$\begin{cases} x = dq + r \\ e \\ y \leqslant r < y + |d| \end{cases}$$

Questão 3.

*** a.** Enuncie e prove os teoremas de terminação e corretude do algoritmo do enunciado da Questão 1(a).

b. Enuncie e prove os teoremas de terminação e corretude do algoritmo do enunciado da Questão 1(b).

*** c.** Enuncie as conjecturas de terminação e corretude do "algoritmo" do enunciado da Questão 1(c). Explique por que não é possível provar essas conjecturas.

Questão 4. Prove ou refute cada afirmação abaixo.

a. Para todo natural x existe um único natural y tal que $x = y + y$.

*** b.** Para todo natural x existe um único natural y tal que $y = x + x$.

c. Para todo real x existe um único real y tal que $x = y \cdot y$.

d. Para todo real x existe um único real y tal que $y = x \cdot x$.

*** e.** Para todo real $x \geqslant 0$ existe um único real y tal que $x = y \cdot y$.

f. Para todo real $x \geqslant 0$ existe um único real $y \geqslant 0$ tal que $x = y \cdot y$.

*** g.** Para todo natural x existe no máximo um natural y tal que $x = y \cdot y$.

*** h.** Para todo natural x existe pelo menos um natural y tal que $x = y \cdot y$.