HW7

3.3 Exercise

13

13. The conventional algorithm for evaluating a polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ at $x = c$ can be expressed in pseudocode by

$$
\begin{aligned}
&\textbf{procedure } \textit{polynomial}(c, a_0, a_1, \ldots, a_n : \text{ real numbers}) \\
&\quad \text{power} := 1 \\
&\quad y := a_0 \\
&\quad \textbf{for } i := 1 \text{ to } n \\
&\quad\quad \text{power} := \text{power} \cdot c \\
&\quad\quad y := y + a_i \cdot \text{power} \\
&\quad \textbf{return } y \quad \{y = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0\}
\end{aligned}
$$

- a) Evaluate $3x^2 + x + 1$ at $x = 2$ by working through each step of the algorithm showing the values assigned at each assignment step.
- b) Exactly how many multiplications and additions are used to evaluate a polynomial of degree n at $x = c$? (Do not count additions used to increment the loop variable.)

answer

- a)
  $y = 1$
  $y = 3$
  $y = 15$
- b)
  multiplation: $2n$
  addition: n

18

18. How much time does an algorithm take to solve a problem of size n if this algorithm uses $2n^2 + 2n$ operations, each requiring 10^{-9} seconds, with these values of n?

- a) 10
- b) 20
- c) 50
- d) 100

answer

- a) $2(10)^2 + 2(10) = 220$ operations
  $220 \times 10^{-9} = 2.2 \times 10^{-7}$ seconds
- b) $2(20)^2 + 2(20) = 840$ operations
  $840 \times 10^{-9} = 8.4 \times 10^{-7}$ seconds
- c) $2(50)^2 + 2(50) = 5100$ operations
  $5100 \times 10^{-9} = 5.1 \times 10^{-6}$ seconds
- d) $2(100)^2 + 2(100) = 20200$ operations
  $20200 \times 10^{-9} = 2.02 \times 10^{-5}$ seconds

30

30. Analyze the worst-case time complexity of the algorithm you devised in Exercise 34 of Section 3.1 for finding all terms of a sequence that are greater than the sum of all previous terms. (section 3.1 34. Devise an algorithm that finds all terms of a finite sequence of integers that are greater than the sum of all previous terms of the sequence.)

answer

the algorithm:

```python
def find_greater_than_prefix_sum(seq):
    result = []
    prefix_sum = 0
    for num in seq:
        if num > prefix_sum:
            result.append(num)
        prefix_sum += num
    return result
```

the algorithm is $O(n)$ when dealing with a n element sequence.

4.1 Exercise

17

17. Suppose that a and b are integers, $a \equiv 4 \pmod{13}$, and $b \equiv 9 \pmod{13}$. Find the integer c with $0 \leq c \leq 12$ such that

- a) $c \equiv 9a \pmod{13}$.
- b) $c \equiv 11b \pmod{13}$.
- c) $c \equiv a + b \pmod{13}$.
- d) $c \equiv 2a + 3b \pmod{13}$.
- e) $c \equiv a^2 + b^2 \pmod{13}$.
- f) $c \equiv a^3 - b^3 \pmod{13}$.

answer

- a) $c = 10$
- b) $c = 8$
- c) $c = 0$
- d) $c = 9$
- e) $c = 6$
- f) $c = 11$

38

38. Find each of these values.

- a) $(19^2 \bmod 41) \bmod 9$
- b) $(32^3 \bmod 13)^2 \bmod 11$
- c) $(7^3 \bmod 23)^3 \bmod 22$

answer

- a) 6
- b) 9
- c) 21

49

49. Show that $\mathbb{Z}_m$ with multiplication modulo m, where $m \geq 2$ is an integer, satisfies the closure, associative, and commutativity properties, and 1 is a multiplicative identity.

answer

- **Closure 封闭性**
  For any $a, b \in \mathbb{Z}_m$, we have

$$a \cdot b \bmod m \in \mathbb{Z}_m$$

  Pf:
  $\mathbb{Z}_m = \{0, 1, ..., m-1\}$
  If $a, b \in \mathbb{Z}_m$,
  then $a, b \in \mathbf{Z}^+$
  then $a \cdot b \in \mathbf{Z}^+$
  then $a \cdot b \mod m \in \mathbf{Z}^+$ and $0 \leq (a \cdot b \mod m) \leq m-1$
  then $a \cdot b \mod m \in \mathbb{Z}_m$
  Q.E.D
- **Associativity 结合律**
  For any $a, b, c \in \mathbb{Z}_m$, we have

$$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod m$$

Pf:
we know that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
It's obvious that if $a = b$, then $a \equiv b \pmod m$
So $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod m$
Q.E.D

- **Commutativity 交换律**
  For any $a, b \in \mathbb{Z}_m$, we have

$$a \cdot b \equiv b \cdot a \pmod m$$

  Pf:
  we know that $a \cdot b = b \cdot a$
  It's obvious that if $a = b$, then $a \equiv b \pmod m$
  So $a \cdot b \equiv b \cdot a \pmod m$.
  Q.E.D

- **Multiplicative Identity 乘法单位元**
  For any $a \in \mathbb{Z}_m$, we have

$$1 \cdot a \equiv a \cdot 1 \equiv a \pmod m$$

  Pf:
  $a \cdot 1 \equiv a \pmod m$:
  we know $a \cdot 1 = a$
  so $a \cdot 1 \equiv a \pmod m$

$a \cdot 1 \equiv 1 \cdot a \pmod m$:
By Commutativity.