Theoretical midterm

Name: .....

Data structures and algorithms (GEMAK117-MA)

April 15, 2024

Neptun code: .....

Exercise 1 (12 points)**.** State the following definitions:

a) (1 point) whole remainder, mod operation:

$a \bmod b = \begin{cases} a - \left\lfloor \frac{a}{b} \right\rfloor \cdot b & \text{if } b \neq 0 \\ \text{not defined} & b = 0 \end{cases}$

b) (1 point) time complexity: worst case runtime for inputs on $\leq n$ bits, $T_A(n) = \max_{\substack{x \text{ input} \\ |x| \leq n}} t_A(x)$.

c) (1 point) big O notation: $f(n) = O(g(n))$ if $\frac{f(n)}{g(n)} \leq C$ for $n \geq n_0$, $n_0 \in \mathbb{N}$, $C < \infty$.

d) (1 point) polynomial growth rate: $T(n) = \Theta(n^k)$ for some $k \in \mathbb{R}^+$.

e) (1 point) stack (data structure): LIFO = last in first out subtype of sequence; single access point top[S], both insertion and deletion only possible there.

f) (1 point) open address hash table: table of N rows indexed by $i = 0, 1, \dots, N-1$; data record with key k inserted into first possible row along search sequence $h(k, t)$, $t = 0, 1, \dots, N-1$.

g) (1 point) Fibonacci numbers: number sequence defined as:
$F_0 = 0$, $F_1 = 1$ → initial conditions,
for $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$ → recursion.

h) (1 point) linear combination: for $a, b \in \mathbb{Z}$, their linear combination is an expression $xa + yb$, with $x, y \in \mathbb{Z}$.

i) (1 point) relative primes: $a, b \in \mathbb{Z}$ are relative primes if $\gcd(a, b) = 1$.

j) (1 point) congruence: for $a, b, n \in \mathbb{Z}$,
$a \equiv b \mod n$ if $n \mid (a - b)$

k) (1 point) multiplicative inverse: if $\gcd(a, n) = 1$,
$a^{-1} \mod n = x$ is the only incongruent solution of $ax \equiv 1 \mod n$.

l) (1 point) median: middle element(s) of the sorted dataset

Exercise 2 (5 points)**.** State the following theorems:

a) (1 point) number of digits (in base b): $x \in \mathbb{Z}$ in base b has $n+1 = \lfloor \log_b x \rfloor + 1$ digits.

b) (1 point) recursion of the greatest common divisor: for $a \geq b \in \mathbb{N}$, $\gcd(a, b) = \gcd(b, r)$, $r = a \bmod b$.

c) (1 point) Fermat's little theorem: for any prime p, for all $a = 1, \dots, p-1$, $a^{p-1} \equiv 1 \bmod p$.

d) (2 points) the solvability of the linear congruence equation:

solve: $ax \equiv b \bmod n$.

Let $d^* = \gcd(n, a) = y^* n + x^* a$.

1. if $d^* \nmid b$, no solution exists.
2. if $d^* \mid b$, there are (infinitely many solutions; write) d^* many incongruent solutions:

$x_0 = x^* \frac{b}{d^*} \bmod n$;

for $i = 1, 2, \dots, d^* - 1$, $x_i = x_0 + i \frac{n}{d^*} \bmod n$.

Exercise 3 (3 points)**.** Write down the algorithm for the **partition algorithm**.

```
PARTITION(@A, a, b, x, @q)
// input: array A, a—b index interval, x pivot,
an element from this interval
// output: partitioned array, q = index of last
"small", ≤ x element
i ← a-1
j ← b+1
WHILE i < j DO
      REPEAT
         INC(i)
      UNTIL A_i ≥ x
      REPEAT
         DEC(j)
      UNTIL A_j ≤ x
      IF i < j
         THEN swap A_i ⟷ A_j
         ELSE q ← j
              RETURN(A, j)
(RETURN)
```

Scoring: total 20 points.
10-11 points: 2 (pass),
12-13 points: 3 (mediocre),
14-15 points: 4 (good),
16-20 points: 5 (excellent).