國立嘉義大學 112 學年度
資訊工程學系碩士班招生考試試題

科目：離散數學（共六題，共 100 分）

1. Solve the following recurrence relations. (20%)

(a) Homogeneous recurrence relation: (n is the integer variable)

$$a_n - 6a_{n-1} = -8a_{n-2.}\ n > 1, a_0 = 4, a_1 = 13;$$

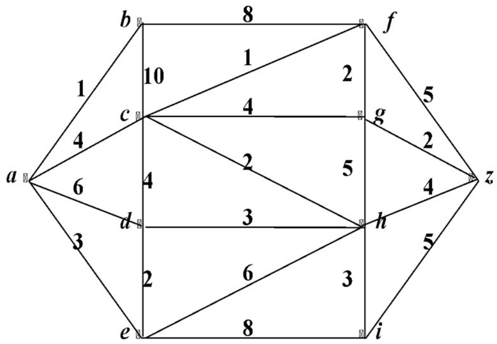
(b) Nonhomogeneous recurrence relation:

$$a_n = 4a_{n-1} + 8n > 1,\ n > 0,\ a_0 = 2;$$

2. Apply Dijkstra algorithm to determine a shortest path from *a* to *z* in the following graph.

(a) Please show the shortest path. The path should be represented by tracing a sequence of visited vertices, such as (*a*, *b*, *f*, *z*). (10%)

(b) Please evaluate the length of the shortest path. (10%)



3. Let R be a binary relation on the set of all positive integers such that

$$R = \{(a,b) \in R \mid a \times b \text{ is an even integer}\}$$

Please answer the following questions and explain your reasons.

(a) Is relation *R* antisymmetric? (5%)

(b) Is relation *R* irreflexive? (5%)

4. Use mathematical induction to prove

$$2 - 2 \times 9 + 2 \times 9^2 - \cdots + 2 \times (-9)^n = (1 - (-9)^{n+1})/5$$

whenever n is a nonnegative integer. (10%)

5. Partial ordering relation:

(a) Please describe the binary relation of partial ordering by using the following example: let T be a set of positive integers, and let R be a binary relation on T such that (x, y) for $x, y \in T$ is in R if x divides y. (5%)

(b) The binary relation can be represented graphically. Represent the elements in T by points and use arrows to represent the ordered pairs in R. Please show that the above-mentioned directed graph has no cycles if deleting the self-loops from the poset (T, R). (5%)

(c) Please draw **Hasse diagrams** for the posets (T_1, R) and (T_2, R) where $T_1 = \{8,\ 168,\ 4,\ 112,\ 28\}$, $T_2 = \{9, 6, 72, 1512, 108, 3, 36\}$ and R is defined above. Please explain whether they are lattices or not. (10%)

6. The following is an algorithm for fast modular exponentiation:

> **Procedure** *fast modular exponentiation* (b: integer, $e = (a_{k-1}a_{k-2} \dots a_1 a_0)_2$ expressed as the binary representation, m: positive integer)
> $result = 1$;
> **for** $i = k - 1$ **to** 0 {
> $result = (result * result)$ **mod** m;
>   **if** ($a_i == 1$)
> $result = (result * b)$ **mod** m;
> }
> **return** $result$; // the result equals b^e **mod** m

(a) Please describe how to calculate b^{83} mod m (i.e., the exponent $e = (83)_{10}$: decimal representation) by the above algorithm and explain it is correct. (10%)

(b) If there is a k-bit exponent e with $\left\lceil \frac{k}{2} \right\rceil$ bits of "1", where $\lceil\ \rceil$ denotes a ceiling function. How many times of multiplications in this algorithm to calculate b^e mod m. Please explain your answer. (10%)