編號： 153 系所：工程科學系乙組 科目：計算機數學

本試題是否可以使用計算機： □可使用 ， ☑不可使用 （請命題老師勾選）

1. For a RSA public key system, to encrypt a text, x, is to perform the formula: $y = x^n \mod z$, where n is the public key and z is called the "public modulus". Suppose that you are give two prime numbers, 17 and 23, and $n = 31$. Use RSA algorithm to
   (1) (5%) Derive the 'z'?
   (2) (5%) Prove or disprove that $s = 159$ is a private key.
   (3) (5%) Encrypt $x = 31$ using public key n and z

2. The Tower of Hanoi is a puzzle consisting of three pegs mounted on a board and n disks of various sizes with holes in their centers. It is assumed that if a disk is on a peg, only a disk of smaller diameter can be placed on top of the first disk. Give all the disks stacked on one peg, named the *Source* peg, the problem is to transfer the disks to another peg, named the *Destination* peg, by moving one disk at a time. (The third peg is named as the *Auxiliary* peg.) Given the algorithm as follows:

```
TowerOfHanoi ( n, Source, Destination, Auxiliary )
 {

If n = 0 then return ;

if n > 0 then
        TowerOfHanoi(n - 1, Source, Auxiliary, Destination)
        move disk n from Source to Destination
        TowerOfHanoi(n - 1, Auxiliary, Destination, Source)
    end if
 }
```

   (1) (10%) What is the complexity of the algorithm?
   (2) (10%) Prove that the algorithm is optimal.

3. The n-cube is a graph that has 2^n nodes, $n \geq 1$, which is represented by vertices labeled 0, 1, …, 2^{n-1}. An edge connects two vertices if the binary representation of their labels differs in exact one bit.
   (1) (5%) Draw a 3-cube.
   (2) (5%) Prove that the n-cube is bipartite for all $n \geq 1$.
   (3) (10%) Show an example and prove that the n-cube can simulate (embed) a ring with 2^n processors.

（背面仍有題目,請繼續作答）

4. (1)Suppose that applicant A_1 is qualified for skills K_2, K_4 and K_5; applicant A_2 is qualified for skills K_1, and K_3; applicant A_3 is qualified for skills K_1, K_3 and K_5; and applicant A_4 is qualified for skills K_3 and K_5.

   (i) (5%) Find a maximal matching.

   (ii) (5%) Is there a complete matching?

   (2) (5%) Let $P = \{p_1, p_2, p_3, p_4, p_5\}$ be a set of five (distinct) points in the ordinary Euclidean plane each of which has integer coordinates. Show that some pair has a midpoint that has integer coordinates.

5. We use C-programming-language-like logic operators for the following Boolean equations. Prove or disprove the equations:

   (1) (5%) $(x_1 \&\& x_2) \,||\, (!x_1 \&\& x_3) \,||\, (!x_1 \&\& x_2 \&\& !x_3) = x_2 \,||\, (!x_1 \,||\, x_3)$

   (2) (5%) $(x_1 \&\& x_2 \&\& x_3) \,||\, !(x_1 \,||\, x_3) = (x_1 \&\& x_3) \,||\, (!x_1 \&\& !x_3)$

6. Define a nondeterministic finite-state automata consists of (I, S, f, A, σ), where I is a finite set of input symbols, S is a finite set of states, f is a next-state function from $S \times I$ into the power set of S, A is a subset of S of accepting states, and an initial state σ.

   (1) (5%)Draw the transition diagram of the nondeterministic finite-state automaton (I, S, f, A, σ), where $I = \{a, b\}$, $S = \{\sigma_0, \sigma_1, \sigma_2\}$, and $A = \{\sigma_2\}$

	Input: a	Input: b
σ_0	$\{\sigma_0\}$	$\{\sigma_2\}$
σ_1	$\{\sigma_0, \sigma_1\}$	Empty set
σ_2	$\{\sigma_2\}$	$\{\sigma_0, \sigma_1\}$

   (2) (5%) Is the string *aabaaba* accepted by the nondeterministic finite-state automaton in (1)?

   (3) (10%) Find a finite-state automaton equivalent to the nondeterministic finite-state automaton in (1).