類組：電機類　科目：離散數學(300C)　　共 4 頁 第 1 頁

※請在答案卷內作答

一、問答、計算題（共9題：合計100分）

答題說明：

1. 請依題號順序書寫於答案卷，並清楚標註題號。
2. 每題題目前會說明配分。例如：[5 points]即代表本子題答對可得五分。

1. [8 points] Two players take turns removing 1, 2, 3, 4, or 5 cards from a stack of 2020 cards. The player who takes the last card *loses*. Is there a strategy for one of the players to always win? If yes, which player is this and what is his strategy? If not, why not? Briefly explain.

2. [12 points] Include all relevant calculations and explanations:
(a) [6 points] Find all integers x that satisfy the congruence $54x \equiv 2 \pmod{89}$.
(b) [6 points] Find the remainder of $47^{200} \pmod{19}$.

3. [12 pts] Let a_n denote the number of ways to tile a $3 \times (2n)$ grid of square using 2×1 tiles.
(a) [6 points] Derive a recurrence relation for a_n.
(b) [6 points] Solve for a_n explicitly.

4. [9 pts] For two positive integers, we write $m \prec n$ if the sum of the (distinct) prime factors of the first is less than or equal to the product of the (distinct) prime factors of the second. For example, $225 \prec 15$, because $3 + 5 \leq 3 \cdot 5$.
(a) [3 points] Is this relation reflexive? Explain.
(b) [3 points] Is this relation transitive? Explain.
(c) [3 points] Is this relation anti-symmetric? Explain.

注意：背面有試題

5. [10 pts] Use Figure 1 to answer the following questions.
(a) [5 points] What's the chromatic number of this graph? Show your work.
(b) [5 points] Show where to delete an edge to decrease the chromatic number.

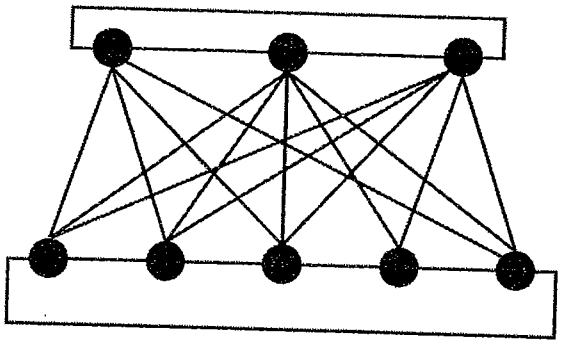

Fig. 1. Undirected Graph

6. [14 points] To build a minimum spanning tree, at each step, Prim's algorithm proposes to add the edge (u, v) such that the weight of (u, v) is minimum among all edges where u is in the tree and v is not in the tree. Therefore, each step maintains a minimum spanning tree of the vertices that have been included thus far. When all vertices have been included, a MST is constructed.
(a) [7 points] Prove the correctness of Prim's algorithm.
(b) [7 points] Prove or disprove that there is a unique minimum spanning tree in a connected weighted graph if the weights of the edges are all different.

7. [16 points] Please write a recurrence relation for describing the worst case time complexity of each of the following algorithms and determine the asymptotic complexity of the function defined by the recurrence relation. Please justify your solution using either substitution, a recursion tree or induction. Note that:

* You **CANNOT** use the Master theorem.
* All arithmetic operations take constant time.
* Simplify and express your answer as n^k or $n(logn)$ wherever possible.
* Just give exponential lower bounds if the algorithm takes exponential time.

(a) [8 points]

Algorithm 1 FunctionA(array1,n)

```
1: // array1 is an array of n integers
2: if n ≤ 18 then
3:    return (array1[n]);
4: end if
5: x ← 0;
6: for i ← 1 to 4 do
7:    for j ← 1 to n − i do
8:       for k ← 1 to ⌈n/2⌉ do
9:          array1[j] ← array1[k] − array1[n − j];
10:      end for
11:   end for
12:   x ← x + FunctionA(array1, ⌈n/2⌉);
13: end for
14: return x
```

(b) [8 points]

Algorithm 2 FunctionB(array1,n)

```
1: // array1 is an array of n integers
2: if n ≤ 3 then
3:    return (array1[1]);
4: end if
5: for i ← 1 to n do
6:    for j ← ⌊n/3⌋ to ⌊2n/3⌋ do
7:       array1[j] ← array1[i] − array1[j];
8:    end for
9: end for
10: x ← FunctionB(array1, ⌊2n/3⌋);
11: return x
```

注意：背面有試題

8. [10 points] Let $f : X \to Y$ be a function from a set X to a set Y and $g : Y \to Z$ be a function from a set Y to a set Z. Suppose that $g \circ f$ is a one-to-one correspondence.
(a) [5 points] Should f be a one-to-one correspondence? If not, what condition should f satisfy? Provide proofs and/or examples justifying your answers.
(b) [5 points] Should g be a one-to-one correspondence? If not, what condition must g satisfy? Provide proofs and/or examples justifying your answers.

9. [9 points] In RSA, the plaintext message can be recovered from a ciphertext message when the decryption key d, which is an inverse of e modulo $(p-1)(q-1)$, is known. To see this, note that if $de \equiv 1 \pmod{(p-1)(q-1)}$, there is an integer k such that $de = 1 + k(p-1)(q-1)$. It follows that

$$C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}. \tag{1}$$

By Fermat's little theorem, it follows that $M^{p-1} \equiv 1 (\text{mod } p)$ and $M^{q-1} \equiv 1 (\text{mod } q)$. Consequently, we have $C^d \equiv M \pmod{pq}$.
(a) [5 points] Let $n = 22$, and $e = 3$. What's the decryption key (d)? Briefly justify your answer.
(b) [4 points] Explain why it is that one can find the decryption key in part (a), but in general having only n or e will not let you easily find the decryption key for real-world instances of RSA.