winning strategy-subtraction game

8. (10%) Suppose that two people play a game taking turns removing, 1, 2, 3 or 4 stones at a time from a pile that begins with 22 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

8.【解】 【106 成大電機類題】

先手先拿 2 個,

接著若後手拿 x 個, 則先手接著拿 5-x 個,

並一直以這種策略進行, 則最後先手必可以拿到最後一個.

假設第二人拿了 k 顆 ($k = 1, 2, 3, 4$)

剩下：

$$20 - k$$

第一人立刻拿：

$$5 - k$$

總共一輪拿了：

$$k + (5 - k) = 5$$

👉 每一輪都把石頭數拉回到：

$$20 \to 15 \to 10 \to 5 \to 0$$

最後：

- 對手面對 5
- 對手拿完後，你一定能拿到最後一顆

difference constraints

32.Consider the following system of difference constraints..

A,B,E

$x_2 - x_1 \le 2$ $\quad x_5 - x_3 \le 1$

$x_3 - x_1 \le 1$ $\quad x_6 - x_5 \le 5$

$x_4 - x_2 \le 3$ $\quad x_6 - x_4 \le 2$

$x_3 - x_2 \le 3$ $\quad x_4 - x_5 \le 2$

Which of the following statement(s) is (are) correct.

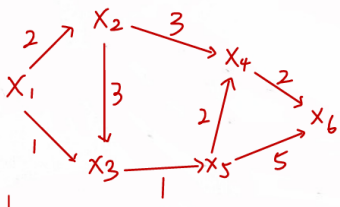
(A) There are infinitely many solutions for x_i's, $i = 1$ *to* 6.

(B) The maximum value of $x_6 - x_1$ is 6

(C) The maximum value of $x_6 - x_1$ is 7) $X_1 \to X_6$ sp=6

(D) The maximum value of $x_4 - x_1$ is 5

(E) The maximum value of $x_4 - x_1$ is 4) $X_1 \to X_4$ sp = 4



若 system 有負 cycle：無解

$X_2 = X_1 + 2$ $\quad X_5 = X_3 + 1$

$X_3 = X_1 + 1$ $\quad X_6 = X_5 + 5$

$X_4 = X_2 + 3$ $\quad X_6 = X_4 + 2$

$X_3 = X_2 + 3$ $\quad X_4 = X_5 + 2$

113 成大

5. (5 points) Consider the trees with vertices {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} that have corresponding degrees (1, 3, 1, 3, 2, 1, 1, 3, 1, 3). How many different spanning trees are there in total?

什麼是 Prüfer sequence？ Prüfer sequence 是一種將具有 n 個節點的 標號樹 （Labeled trees）映射到長度為 $n-2$ 的序列的方法。這種映射是一一對應的（雙射），因此它常被用來證明 凱萊公式（Cayley's formula），即 n 個節點的標號樹總共有 n^{n-2} 棵。

核心特性 序列長度：對於一個有 n 個節點的樹，其 Prüfer sequence 的長度恰好為 $n-2$。度數關係：一個編號為 i 的節點，若其在樹中的 度數（degree） 為 d_i，則該編號 i 在 Prüfer sequence 中會恰好出現 $d_i - 1$ 次。

葉節點（Leaf）：度數為 1 的節點，永遠不會出現在序列中 5。題目給定節點數 $n = 10$，且各節點的度數序列為 $(1, 3, 1, 3, 2, 1, 1, 3, 1, 3)$ 。確認序列長度： 因為 $n = 10$，對應的 Prüfer sequence 長度應為 $10 - 2 = 8$。計算各編號出現次數： 根據 $d_i - 1$ 原則，各編號在序列中出現的次數如下： 編號 2, 4, 8, 10：度數皆為 3，各出現 $3 - 1 = \mathbf{2}$ 次。 編號 5：度數為 2，出現 $2 - 1 = \mathbf{1}$ 次。 其餘編號 (1, 3, 6, 7, 9)：度數為 1，出現 $1 - 1 = 0$ 次。 排列組合計算： 問題轉化為：將這 8 個名額分配給上述編號。這是一個 不盡相異物排列 問題：

$$\frac{8!}{2! \cdot 2! \cdot 2! \cdot 2! \cdot 1!} = \frac{40320}{16} = \mathbf{2520}$$

因此，符合該度數序列的生成樹總共有 2520 棵。

113 台科

2. [10%] Solving the problem of scheduling n jobs on a single processor. Each job j requires processing time t_j without interruption, and has a deadline d_j. If job j starts at time s_j, it will be finished at $f_j = s_j + t_j$. The *lateness* of the job j measures how long it finishes after its deadline, max $\{0, f_j - d_j\}$. The goal is scheduling all jobs to minimize the maximum lateness of a job among the n jobs. Suppose we have six jobs with specified required times and deadlines, as shown in the table below. Please provide the job scheduling using *greedy algorithm*.

	Job 1	Job 2	Job 3	Job 4	Job 5	Job 6
t_j	2	4	2	1	3	3
d_j	7	9	14	8	5	13

利用**Earlist Deadline First**

Job	**Job5**	**Job1**	**Job4**	**Job2**	**Job6**	**Job3**
t_j	3	2	1	4	3	2
d_j	5	7	8	9	13	14
s_j	0	3	5	6	10	13
f_j	3	5	6	10	13	15
$lateness_j$	0	0	0	1	0	1

RSA 109 臺北

1. (10%) Consider an RSA cryptosystem with $p = 11$, $q = 29$, and public-key $(e, n) = (3, 319)$. What is the value of d used in the secret-key? What is the encryption of the message $M = 100$?

已知資料

- p = 11, q = 29
- 公鑰 (e, n) = (3, 319)
- 明文 M = 100

第 1 步：計算 n 與 $\varphi(n)$
$n = p \cdot q = 11 \cdot 29 = 319$
$\varphi(n) = (p-1)(q-1) = 10 \cdot 28 = 280$

第 2 步：計算私鑰 d
私鑰 d 滿足:$d \cdot e \equiv 1 \pmod{\varphi(n)}$

即
$3 \cdot d \equiv 1 \pmod{280}$
檢查 3 的模 280 乘法逆元:
$3 \cdot 187 = 561 \equiv 1 \pmod{280}$
所以
$\boxed{d = 187}$

第 3 步：加密訊息 $M = 100$
RSA 加密公式:
$C = M^e \mod n$
$C = 100^3 \mod 319$
先計算 $100^2 \mod 319$
$100^2 = 10,000$
$10,000 \div 319 \approx 31$ 餘 111
所以
$100^2 \equiv 111 \pmod{319}$
再乘一次 100:
$100^3 \equiv 111 \cdot 100 \mod 319$
$111 \cdot 100 = 11100$
$11100 \div 319 \approx 34$ 餘 254
所以密文：
$\boxed{C = 254}$

答案

- 私鑰： $d = 187$
- 密文： $C = 254$

RSA 113 臺北

1. (20%) Consider an RSA cryptographic system with the public key (n, e) = (649, 387). First, find prime numbers p and q such that $n = pq$. Second, find the value of d in the private key (n, d). Third, decrypt the ciphertext 10 into plaintext. Fourth, encrypt the plaintext 351 into ciphertext. Finally, answer the question "Is it possible to find more than one values of d in the range $0 < d < (p - 1)(q - 1)$ that works in decryption?" If your answer is YES, find all possible values of d; if your answer is NO, give a brief proof.

求 p, q： $n = 649$。經由質因數分解 :$649 \div 11 = 59$。故$p = 11, q = 59$。

求 d:

1. 計算 $\phi(n) = (p-1)(q-1) = 10 \times 58 = 580$ 。
2. 解同餘方程式 $ed \equiv 1 \pmod{\phi(n)}$ ，即 $387d \equiv 1 \pmod{580}$。
3. 使用輾轉相除法求逆元：
   $580 = 1 \times 387 + 193$ $387 = 2 \times 193 + 1$ $1 = 387 - 2(580 - 387) = 3 \times 387 - 2 \times 580$ 故

$d = 3$。

解密 Ciphertext 10:

$Plaintext = 10^d \pmod{n} = 10^3 \pmod{649} = 1000 \pmod{649} = \mathbf{351}$ 。

加密 Plaintext 351：

$Ciphertext = 351^{387} \pmod{649}$。由上題可知$351 \equiv 10^3 \pmod{649}$。

$351^{387} \equiv (10^3)^{387} = 10^{1161} \pmod{649}$。

根據歐拉定理，$10^{\phi(649)} = 10^{580} \equiv 1 \pmod{649}$。

$10^{1161} = (10^{580})^2 \times 10^1 \equiv 1^2 \times 10 = \mathbf{10}$ 。

d 是否唯一： NO。

證明： 在 $0 < d < \phi(n)$ 的範圍內，d 是乘法群 $\mathbb{Z}_{\phi(n)}^*$ 中的元素。因為
$\gcd(e, \phi(n)) = \gcd(387, 580) = 1$ ，根據群論性質，模逆元 d 在該範圍內是唯一的。