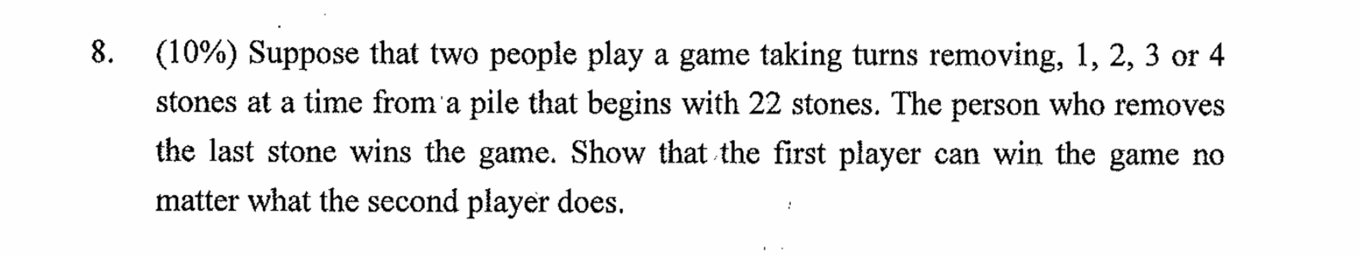
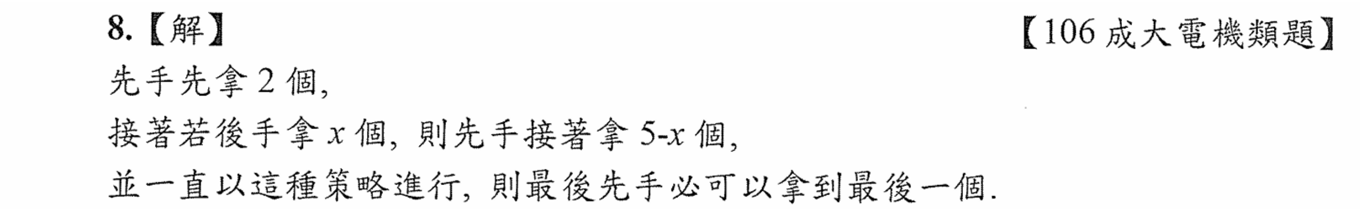
winning strategy-subtraction game



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：

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

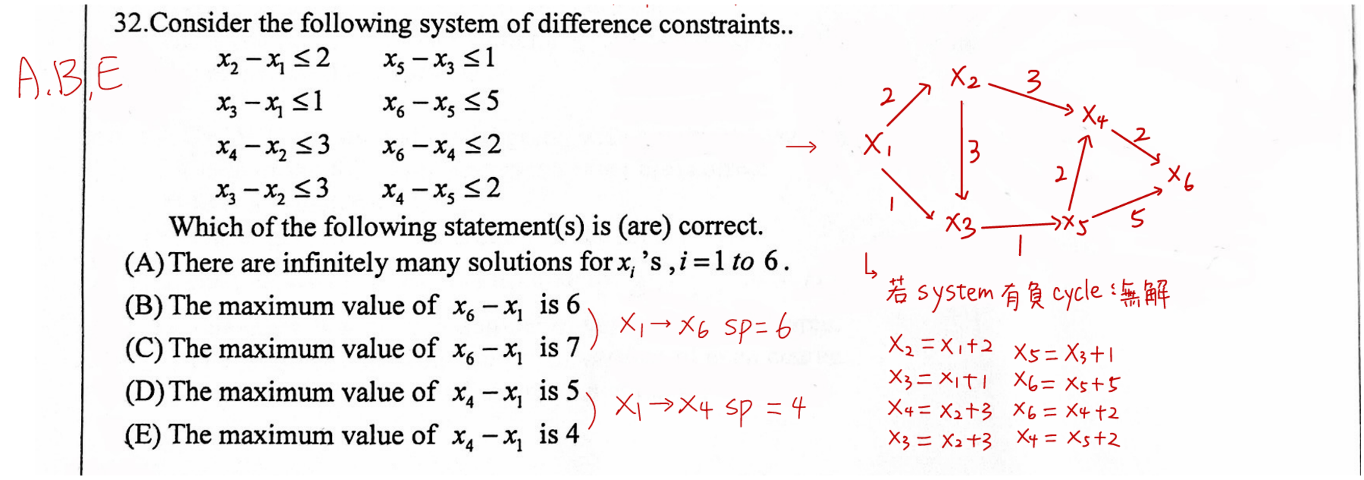
👉 每一輪都把石頭數拉回到：

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

最後：

- 對手面對 5
- 對手拿完後，你一定能拿到最後一顆

difference constraints



A.B,E

32.Consider the following system of difference constraints..

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

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

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

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

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

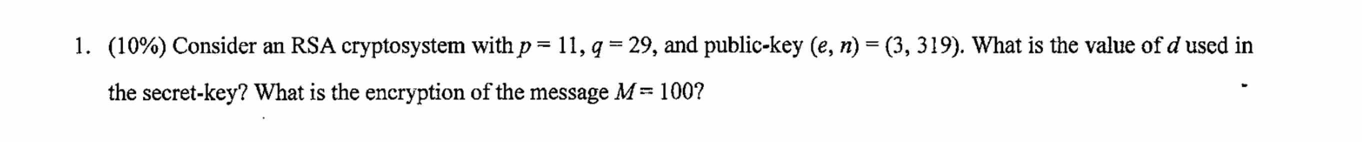
$X_2 = X_1 + 2$ $\quad$ $X_5 = X_3 + 1$

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

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

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

RSA



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：$C = 254$