臺北市一 OO 學年度高級中等學校電腦程式設計競賽決賽試題

(高中組)

說明：

1. 本試卷共有四題，每題 25 分。
2. 請記得隨時備份自己的程式。

試題：

1. 合影隊型

問題敘述

酷酷鯊是一支新成立的棒球隊，共有 N 位球員。球隊裡原本氣氛融洽，大家都是好麻吉，同心協力爭取年度總冠軍。然而，最近一連串的比賽不順利，球員間開始出現摩擦。今天，棒球聯盟邀請了總統夫人到場開球。總統夫人是酷酷鯊隊的球迷，因此她希望能和全體球員合影留念。拍照時，球員們會站成一列。為了避免尷尬，球隊經理希望在安排拍照的隊型時，不要讓彼此有芥蒂的球員站在一起。

舉例來說，如果有五位球員 A, B, C, D, E，其中 A 和 B 不願意站在一起，C 和 D 不願意站在一起，那麼 ABCDE 和 ABCED 不是適當的隊型，而 ACBDE 和 CADEB 則都是適當的隊型。

現在請你撰寫一個程式，協助球隊經理在總統夫人蒞臨之前，排出一個適當的合影隊型吧！

輸入說明

第一行為球員人數 (N)，$N \le 15$。(球員代號從 A 開始編起。)

第二行為有摩擦的球員配對數 (M)，$M \le 50$。

第三行開始，每一行有兩個字元，代表有摩擦的兩個球員代號。兩個字元間以一個空格隔開。

輸出說明

請輸出以字典遞增排序方式的第一個適合隊型。如果沒有任何適合隊型，請輸出 No Solution。計算時間不得超過 2 秒鐘。

輸入範例一	**輸入範例二**
5 2 A B C D **輸出範例一** ACBDE	4 4 A B C D C A C B **輸出範例二** No Solution

2. Knapsack 解密問題

在一個基於 subset sum 問題的實驗性公開金鑰密碼系統中，某甲想要加密一些文字資料給某乙，甲取得乙的公開金鑰如右圖共有 29 個 32 位元的整數，其中第一個整數 p 為質數，連同第二個到第二十九個整數 $a_0 \sim a_{27}$ 可以用來加密四個 ASCII 文字資料，由於每一個 ASCII 編碼的位元組只有 7 個位元是有意義的，我們將四個文字資料以 28 個位元 $m_{27} \sim m_0$ 表示，其中 $m_i \in \{0,1\}$ 且 $m_{27} \sim m_{21}$ 代表第一個字元, …, $m_6 \sim m_0$ 代表第四個字元，密文 $c_j = \sum_{i=0}^{27} m_i * a_i \bmod p$，其中 $x \bmod p$ 代表整數 x 除以 p 的餘數，這個系統中加密鑰匙 a_i 是以下列方法計算的:

```
p=3019271449
a[0]= 965341323
a[1]=2896023969
a[2]=1807435166
   …
a[25]=    2235759
a[26]= 969812841
a[27]= 974284359
```

$a_i = s * b_i \bmod p$，$b_0 = 1$，$b_i = (\sum_{j=0}^{i-1} b_j) + 1 + k_i \bmod p$, i=1,2,…,27，其中 $k_0 \sim k_{27} \in \{0,1\}$ 及 s 為祕密參數，請設計一個演算法將右圖中密文 c_j 對應的訊息解出，以上例而言(test2.txt)，解回的 ASCII 文字為“Biometrics (or biometric authentic cation) .... under surveillance.”，測試檔案 test1.txt 解回的文字為“HelloWorld”。

```
c[0]= 629263857
c[1]= 636887368
c[2]= 525742329
   …
c[85]=   78690518
c[86]=1997428695
c[87]=1128693140
```

已知 a_i 及 p，由 c_i 解出 m_i 是一個已知的 NP 問題，雖然在此例子中只有 28 個 a_i，暴力破解困難度還不算太高,一般實際應用中至少有 1024 個 a_i，當然所使用的質數 p 也就至少有 1024 個位元，本題中不希望你使用暴力破解，所以要求你的程式能夠在 1 秒內解回至少 1000 個文字。測試資料檔案中每一列的資料依序為 $p, a_0, a_1, \ldots, a_{27}, c_0, c_1, \cdots, c_n$，請解出密文 $c_0, c_1, \cdots$ 所對應的訊息 $m_0, m_1, \ldots$。

注意:如果你沒有解出 m_i 但是計算出 $b_0, b_1,\ldots, b_{27}$ 的話也可以得到部份分數:

1. 基本上如果你求出 $b_0, b_1,\ldots, b_{27}$, 就可以很快地解密 $c_0, c_1, \ldots, c_n$; 也就是需要由 s, a_i, 及 $a_i = s*b_i \mod p$ 解出 b_i。
2. 這個工作在一般整數群中可以很容易地修改求最大公因數 gcd(s,p) 的演算法, 找到 t 滿足 $t*s=1 \mod p$, 將上式左右兩側乘上 t 可得 $t*a_i = t*s*b_i = b_i \mod p$, 即可由此式計算 b_i。
3. 例如: p=23, s=5 可用右圖的輾轉相除法求 gcd(23, 5)=1, 如右圖所示, 進一步可以求出 t=14, 滿足 14*5=1 mod 23

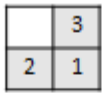
```
23 = 4 * 5 + 3    … ①
 5 = 1 * 3 + 2    … ②
 3 = 1 * 2 + 1    … ③
 2 = 2 * 1 + 0
最後整除時的除數即
為最大公因數
```

```
②*(-1)+③可得到
 -5 = -2 * 3 + 1    … ④
①*2+④可得到
2 * 23 = 9 * 5 + 1  移項可得
-9 * 5 = 1 - 2 * 23  亦即
(23-9) * 5 = 1 + 3 * 23 亦即
14 * 5 = 1 + 3 * 23
```

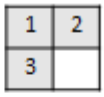
4. 注意兩個 32 位元整數的乘積需要 64 位元才能表示
5. 因為目前使用的質數 p 太小, 使得目前這個系統的設計幾乎沒有安全性, 由 a_0, $a_1,\ldots, a_{27}$ 中就可以很快地推得 s, 所以你不需要知道任何祕密就可以解出訊息, 請注意每一組測試資料使用的 s 是不一樣的。

3. 資訊不完全之數字盤遊戲

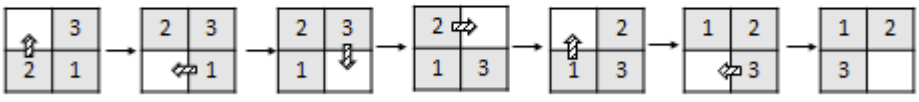
數字盤是一個流傳很久也很受歡迎的遊戲，在方形盤裡通常會有一些標有數字的方塊及一個空格，與空格上下或左右相鄰的方塊可以移到空格處，而原來位置會變成空格，也就是說方塊移動規則是只能上下或左右移動。例如在 2x2 的數字盤遊戲我們若要將圖(i)中的數字盤變成圖(ii)中的數字盤的一種方式之一是經由圖(iii)中的 6 次移動而達成：



圖(i)

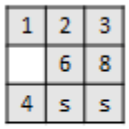


圖(ii)



圖(iii)

數學老師明斯基別出心裁地設計了一個 NxN 數字盤玩法是：例如當 N=4 時，在原本應該要有編號 1 至 15 的 15 個方塊在其中，明斯基老師會任意地將其中的幾個數字方塊用星號方塊取代(每個星號方塊變成都是一模一樣的)，要學生莫菲將一個隨意給定的數字盤初始盤面(如圖(iv)所示，其中數字方塊 2 與 10 分別由星號方塊取代)移動到另一個指定的目標盤面(如圖(v)所示)。



圖(iv)

圖(v)

請來幫莫菲找出，當隨意給定一個 *N*x*N* 數字盤初始盤面，同時其中的幾個數字方塊是用星號方塊取代時，移到另一個指定的目標盤面所需的最少移動次數。

程式輸入

程式輸入為一個隨意給定 *N*x*N* (*N*≤5)數字盤初始盤面(例如圖(iv))與指定的目標盤面(例如圖(v))：

1 2 3 b 6 8 4 s s

1 2 3 4 s 6 s 8 b

上述第一行代表初始盤面(圖(iv))，第二行代表目標盤面。其中字母 s 代表星號方塊、字母 b 代表盤面上的空格，輸入數字或字母字時以空白鍵隔開。

程式輸出

程式輸出為一整數，代表由初始盤面到目標盤面所需最少移動次數；若無法移動至目標盤面則程式輸出-1。程式必須在 30 秒內執行完成。

【範例 一】

輸入資料

1 2 3 b 6 8 4 s s

1 2 3 4 s 6 s 8 b

輸出資料

7

【範例二】

輸入資料

b 1 3 4 5 2 6 8 9 10 7 12 13 14 11 15

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 b

輸出資料

6

4. 因式分解

給任一個整數，將之因式分解是很常見的問題，但是不是可以將任一個整數 a 因式分解成一個整數 b 的連乘積(意即 b 連乘 m 次後等於 a)，就成為另一個更有趣的問題。例如：(1) 若 a=1024，那可能 b=4, m=5 也有可能 b=2, m=10;(2) 若 a=99，那 b=99, m=1。針對這樣的問題，一個遊戲規則如下：給定一個絕對值不為 1 的整數 a，將 a 因式分解成 b 的 m 次方，m 越大獎金越高，為了拿最高獎金，需要找到最大的 m 值，請你寫個程式來達成這個目標。(請注意：a, b 可以為負整數)

Input：
一個測試檔(檔名為 in.txt)，內每一列有 1 個整數(即 a)，0 代表輸入資料結束。

Output：
對每筆測試資料依上述的說明求得 $a=b^m$，並使得 m 為最大，然後產生一輸出檔(檔名為 out.txt)，輸出檔中每一列對應一筆輸入檔的資料，格式為：先產生編號(如範例所示，依序為(1) (2) (3) …)，再輸出兩個數字，其第一個數是 b，第二個數是 m(b 與 m 中間以逗點隔開)。

Sample Input file:
21
34359738368
-25
0

Sample output file:
(1) 21, 1
(2) 2, 35
(3) -25, 1