Universidad de La Habana

FACULTAD DE MATEMÁTICA Y COMPUTACIÓN

Proyecto de Diseño de Análisis y Algoritmos

Raudel Alejandro Gómez Molina C-411

$\mathbf{\acute{I}ndice}$

1.	\mathbf{Red}	lucción de Emparejamiento
	1.1.	Ejercicio
	1.2.	Etiquetas
	1.3.	Solución
		1.3.1. Fuerza bruta
		1.3.2. Teorema Kőnig
		1.3.3. Obtener el cubrimiento mínimo
		1.3.4. Utilizando Kőnig y el cubrimiento mínimo
2.	Núr	mero de subarreglos k-buenos
	2.1.	Ejercicio
	2.2.	Etiquetas
	2.3.	Solución
		2.3.1. Fuerza bruta
		2.3.2. Mejorando la fuerza bruta
		2.3.3. Divide y Vencerás
		2.3.4. Programación Dinámica
3.	Dist	tribución Justa
	3.1.	Ejercicio
	3.2.	Etiquetas
	3.3.	Solución
		2.2.1 Taoyie de Números

1. Reducción de Emparejamiento

1.1. Ejercicio

Link del problema en la plataforma Codeforces

■ límite de tiempo por test: 8 segundos

• límite de memoria por test: 512 megabytes

Te dan un grafo bipartito con n_1 vértices en la primera parte, n_2 vértices en la segunda parte, y m aristas. El emparejamiento máximo en este grafo es el subconjunto máximo posible (en tamaño) de aristas de este grafo tal que ningún vértice está incidente a más de una arista elegida.

Debes procesar dos tipos de consultas en este grafo:

- 1 elimina el número mínimo posible de vértices de este grafo para que el tamaño del emparejamiento máximo se reduzca exactamente en 1, e imprime los vértices que has eliminado. Luego, encuentra un emparejamiento máximo en este grafo e imprime la suma de los índices de las aristas que pertenecen a este emparejamiento;
- 2 este tipo de consulta se realizará solo después de una consulta de tipo 1. Como respuesta a esta consulta, debes imprimir las aristas que forman el emparejamiento máximo que has elegido en la consulta anterior. Ten en cuenta que debes resolver el problema en modo en línea. Esto significa que no puedes leer toda la entrada de una vez. Solo puedes leer cada consulta después de escribir la respuesta a la consulta anterior. Usa las funciones fflush en C++ y BufferedWriter.flush en Java después de cada escritura en tu programa.

Entrada

La primera línea contiene cuatro enteros n_1 , n_2 , m y q $(1 \le n_1, n_2 \le 2 \cdot 10^5; 1 \le m \le \min(n_1 \cdot n_2, 2 \cdot 10^5); 1 \le q \le 2 \cdot 10^5)$.

Luego siguen m líneas. La i-ésima contiene dos enteros x_i y y_i $(1 \le x_i \le n_1; 1 \le y_i \le n_2)$, lo que significa que la i-ésima arista conecta el vértice x_i en la primera parte y el vértice y_i en la segunda parte. No hay pares de vértices que estén conectados por más de una arista.

Luego siguen q líneas. La i-ésima contiene un entero, 1 o 2, indicando la consulta i-ésima. Restricciones adicionales sobre las consultas:

- el número de consultas de tipo 1 no superará el tamaño del emparejamiento máximo en el grafo inicial;
- el número de consultas de tipo 2 no superará 3;
- cada consulta de tipo 2 será precedida por una consulta de tipo 1;
- tu solución solo puede leer la *i*-ésima consulta después de imprimir la respuesta a la consulta (i-1)-ésima y vaciar el búfer de salida.

Salida

Para una consulta de tipo 1, imprime la respuesta en tres líneas de la siguiente manera:

- la primera línea debe contener el número de vértices que eliminas;
- la segunda línea debe contener los índices de los vértices que eliminas, de la siguiente manera: si eliminas el vértice x de la parte izquierda, imprime x; si eliminas el vértice y de la parte derecha, imprime -y (índice negativo);
- la tercera línea debe contener la suma de los índices de las aristas en algún emparejamiento máximo en el grafo resultante. Las aristas están numeradas del 1 al m.

Para una consulta de tipo 2, imprime la respuesta en dos líneas de la siguiente manera:

- la primera línea debe contener el tamaño del emparejamiento máximo;
- la segunda línea debe contener los índices de las aristas que pertenecen al emparejamiento máximo. Ten en cuenta que la suma de estos índices debe ser igual al número que imprimiste al final de la consulta de tipo 1 anterior.

Después de imprimir la respuesta a una consulta, no olvides vaciar el búfer de salida.

1.2. Etiquetas

- Flujo
- Emparejamientos
- Cobertura de vértices

1.3. Solución

En el ejercicio se tiene un grafo **bipartito** en el que se debe responder a dos tipos de consultas, en la primera se debe eliminar la mínima cantidad de vértices para que el emparejamiento máximo del grafo se reduzca exactamente en 1 y en la segunda se debe informar las aristas que pertenecen al emparejamiento máximo en el grafo que se tiene actualmente. Una observación importante es que la interactividad del ejercicio no permite responder las consultas de forma **offline** (recibir todas las consultas hacer algún tipo de preprocesamiento conociendo todas las posibles consultas y luego responder cada una de forma individual), por lo que es necesario responder las consultas de forma individual sin conocer las demás e ir manteniendo el estado del grafo.

Definiciones:

- Se define un emparejamiento máximo de un grafo G como M(G).
- Se define un cubrimiento mínimo de un grafo G como C(G).
- Se define el grafo inducido de G = V, E, por V' tal que $V' \subset V$ como I(G, V').

1.3.1. Fuerza bruta

El primer acercamiento para resolver este problema es primeramente encontrar un emparejamiento máximo en el grafo de entrada, para esto ya que dicho grafo es **bipartito** se puede usar el algoritmo de **Khun** (basado en el teorema de **Khun**) o **Flujo Máximo**, estos dos algoritmos funcionan en una complejidad de O(VE).

Luego cuando se necesite analizar una consulta del tipo 1, se puede iterar por todos los posibles conjuntos de vértices V' tal que $V' \subset V$ y |M(I(G, V'))| = |M(G)| - 1 y elegir el conjunto de mayor cardinalidad, este algoritmo es algo lento ya que su complejidad es de $O(2^{|V|}VE)$.

Para las consultas de tipo 2 solo se debe guardar el emparejamiento encontrado en la consulta de tipo 1 anterior e informar las aristas que pertenecen a dicho emparejamiento, en una complejidad de O(q) donde q es la cardinalidad del emparejamiento máximo del grafo actual.

1.3.2. Teorema Kőnig

El teorema de **Kőnig** plantea que dado un grafo **bipartito** G se cumple que |C(G)| = |M(G)|, además plantea una equivalencia entre estos 2 conjuntos es decir como dado un emparejamiento máximo encontrar un cubrimiento mínimo y viceversa.

Demostración:

Sea un grafo **bipartito** G = V, E, con A y B los conjuntos de vértices que representan la bipartición, definamos Q = M(G) y $A_q = \{x \in A \mid \exists y \text{ tal que } \langle x, y \rangle \in Q\}$ y $B_q = \{y \in B \mid \exists x \text{ tal que } \langle x, y \rangle \in Q\}$.

En primer lugar si se tiene un cubrimiento de vértices W se cumple que 2 aristas de Q no inciden sobre un mismo vértice de W porque de lo contrario Q no sería un emparejamiento, por otro lado cada arista en Q debe ser cubierta por un vértice de W ya que de lo contrario W no sería un cubrimiento de vértices. Por tanto si |Q| = |W| entonces se puede decir que W es un cubrimiento mínimo.

Sea Z el conjunto de formado por la unión de $A \setminus A_q$ y el conjunto de vértices que a los que se puede llegar usando caminos Q alternantes partiendo de los vértices de $A \setminus A_q$.

Ahora si se define $K = (A_q \setminus Z) \cup (B_q \cap Z)$ se puede demostrar que K es un cubrimiento de vértices. Observe que para cada arista $\langle x,y \rangle \in E$ con $x \in A$ y $y \in B$ se cumple que $x \in A_q \vee y \in B_q$ porque si no Q no sería máximo: si $\langle x,y \rangle$ pertenece a uno de los caminos Q alternantes entonces $y \in B_q \cap Z$ porque todas las aristas que pertenecen a un camino Q alternante tienen un vértice en B_q , de lo contrario tendríamos un camino Q aumentativo; ahora si $\langle x,y \rangle$ no pertenece a ninguno de los caminos Q alternantes entonces $x \in A_q \setminus Z$ porque si $x \notin A_q$ se cumple que $\langle x,y \rangle$ pertenece a un camino Q alternante.

Solo resta demostrar que |K| = |Q|. Observe que para toda arista $\langle x, y \rangle \in Q$ con $x \in A$ y $y \in B$ se cumple que: si $\langle x, y \rangle$ pertenece a uno de los caminos Q alternantes entonces $y \in B_q \cap Z \land x \notin A_q \setminus Z$ porque $x \in Z$; ahora si $\langle x, y \rangle$ no pertenece a ninguno de los caminos Q alternantes entonces $x \in A_q \setminus Z \land y \notin B_q \cap Z$ porque $x \notin Z$. Entonces como $(A_q \setminus Z) \cap (B_q \cap Z) = \emptyset$ por lo enunciado anteriormente se cumple que |K| = |Q|.

1.3.3. Obtener el cubrimiento mínimo

Como se demostró anteriormente en el teorema de **Kőnig** existe una equivalencia entre el emparejamiento máximo y el cubrimiento mínimo en un grafo **bipartito**.

Si se toma la demostración anterior para encontrar un cubrimiento mínimo es necesario primeramente encontrar un emparejamiento máximo, para esto se puede usar el algoritmo de **Khun** (basado en el teorema de **Khun**) o **Flujo Máximo**, ambos en una complejidad de O(VE).

Luego se puede encontrar el conjunto de vértices Z mediante un **DFS** restringiendo el uso de caminos que no sean Q alternantes, en una complejidad de O(V + E).

Solo resta formar el conjunto K, lo cual se puede lograr mediante los conjuntos A, B, A_q , B_q y Z, en una complejidad de O(V).

1.3.4. Utilizando Kőnig y el cubrimiento mínimo

Si se emplea el teorema de **Kőnig** demostrado anteriormente se puede pasar a analizar el problema de forma diferente, es decir existe una equivalencia entre M(G) y C(G) donde G es un grafo **bipartito** ahora se puede buscar la menor candad de vértices tal que al eliminarlos la cardinalidad del cubrimiento mínimo disminuya exactamente en 1 y dicho conjunto cumplirá con las restricciones del problema original.

Se puede realizar la siguiente observación si V_c es un cubrimiento de vértices de G = V, E entonces para cualquier vértice $v \in V_c$, sea $V'_c = V_c - v$ y V' = V - v, se cumple que V'_c es un cubrimiento de vértices del grafo I(G, V'). Para demostrar el anterior enunciado observe que para toda arista $e \in E$ se cumple que e incide sobre alguno de los vértices de V_c , por tanto las únicas aristas de E que no inciden sobre V'_c son las que únicamente incidían sobre v y dichas aristas no pertenecen a I(G, V'), por lo que como las aristas de I(G, V') son subconjunto de E entonces se cumple que V'_c cubre todas las aristas de I(G, V').

Ahora dado el razonamiento anterior si V_c es un cubrimiento mínimo de vértices de G = V, E entonces para cualquier vértice $v \in V_c$, sea $V'_c = V_c - v$ y V' = V - v, se cumple que V'_c es un cubrimiento mínimo de vértices del grafo I(G, V'). Como ya se demostró que V'_c es un cubrimiento de vértices solo falta demostrar que V_c es mínimo. Para ello suponga que existe un cubrimiento menor V''_c del grafo I(G, V'), entonces si se añade v a dicho cubrimiento se obtiene un cubrimiento de G, ya que todas las aristas que estaban en G y no en I(G, V') incidían sobre v lo cual contradice el hecho de que V_c sea mínimo.

Luego si se elimina cualquier vértice v de G que participe en un cubrimiento mínimo obtenemos un grafo que cuya cardinalidad del cubrimiento mínimo disminuye en 1 con respecto a la cardinalidad del cubrimiento mínimo en el grafo original.

Ahora se puede utilizar el resultado demostrado anteriormente para responder eficientemente las consultas de tipo 1. Para ello es necesario primeramente obtener un cubrimiento mínimo en el grafo de entrada (esto se puede lograr mediante el algoritmo descrito anteriormente) y cada vez que se proporcione una consulta de este tipo seleccionar un vértice de dicho conjunto.

Para las consultas de tipo 2, es necesario mantener un emparejamiento que se corresponda con el cubrimiento mínimo de vértices del grafo actual. Para ello se puede emplear el algoritmo descrito anteriormente para encontrar el cubrimiento mínimo en el grafo inicial y cuando se procese una consulta del tipo 1 eliminar la arista del emparejamiento que incide sobre el vértice que se va a eliminar (esto siempre es posible porque para todo vértice del cubrimiento mínimo inicial existe una arista del emparejamiento que incide sobre dicho vértice y para cada arista del emparejamiento inicial exactamente uno de sus 2 vértices pertenece al cubrimiento mínimo), por tanto al eliminar dicha arista se obtiene un emparejamiento con cardinalidad igual al cubrimiento mínimo de vértices y por el teorema de **Kőnig** se puede asegurar que este emparejamiento es máximo.

Entonces para resolver el ejercicio primero es necesario encontrar un cubrimiento mínimo y el emparejamiento máximo asociado a dicho cubrimiento esto tiene una complejidad de O(VE) empleando el algoritmo descrito anteriormente, las consultas de tipo 1 se pueden responder en una complejidad de O(1) y las de tipo 2 en una complejidad de O(q) donde q es la cardinalidad del emparejamiento máximo del grafo actual.

2. Número de subarreglos k-buenos

2.1. Ejercicio

Link del problema en la plataforma Codeforces

- límite de tiempo por prueba: 2 segundos
- límite de memoria por prueba: 256 megabytes

Sea bit(x) el número de unos en la representación binaria de un número entero no negativo x.

Un subarreglo de un arreglo se llama k-bueno si consiste solo en números que no tienen más de k unos en su representación binaria. Es decir, un subarreglo (l,r) del arreglo a es bueno si para cualquier i tal que $l \le i \le r$ se cumple la condición bit $(a_i) \le k$.

Se te da un arreglo a de longitud n, que consiste en enteros no negativos consecutivos que comienzan desde 0, es decir, $a_i = i$ para $0 \le i \le n-1$ (en indexación basada en 0). Necesitas contar el número de subarreglos k-buenos en este arreglo.

Dado que la respuesta puede ser muy grande, imprime el resultado módulo $10^9 + 7$.

Entrada

Cada prueba consiste en múltiples casos de prueba. La primera línea contiene un número entero t $(1 \le t \le 10^4)$ —el número de casos de prueba. Las siguientes líneas describen los casos de prueba.

La única línea de cada caso de prueba contiene dos enteros n, k $(1 \le n \le 10^{18}, 1 \le k \le 60)$.

Salida

Para cada caso de prueba, imprime un solo número entero: el número de subarreglos k-buenos módulo $10^9 + 7$.

2.2. Etiquetas

- Máscara de bits
- Divide y Vencerás
- Programación Dinámica

2.3. Solución

En el ejercicio se tiene un arreglo de los números de 0 a n-1 en orden creciente y se debe responder el número de subarreglos k-buenos. La principal dificultad para el ejercicio es contar eficientemente el número de estos subarreglos así que primeramente se puede abordar un algoritmo de fuerza bruta para resolver el ejercicio.

Nota: En la solución del ejercicio se usarán números soportados por la aritmética de la computadora (hasta 64 bits), por lo que las operaciones con los bits de los números se consideran constantes. Para llevar esta solución a otro modelo de cómputo puede considerar las operaciones de bits sobre n en una complejidad de $O(\log(n))$.

2.3.1. Fuerza bruta

Para resolver este ejercicio observe que se pueden probar con todos los posibles subarreglos y determinar por cada subarreglo si este es k-bueno o no. Para ello se puede encontrar todos los subarreglos en una complejidad de $O(n^2)$ y comprobar si un subarreglo es k-bueno tiene una complejidad de O(n), para una complejidad total de $O(n^3)$.

2.3.2. Mejorando la fuerza bruta

Observe que se puede mejorar el algoritmo anterior haciendo la siguiente observación: si se tiene que un subarreglo (l,r) es k-bueno entonces se puede asegurar que para todo x tal que $l < x \le r$ se cumple que el subarreglo (l,x) es k-bueno, por otro lado si se tiene que un subarreglo (l,r) no es k-bueno entonces se puede asegurar que para todo x tal que $r \le x \le n$ se cumple que el subarreglo (l,x) no es k-bueno.

Ahora si para cada índice l se calcula el mayor r tal que (l,r) es k-bueno se puede obtener el número de subarreglos k-buenos que comienzan en l. Para esto se puede iterar por todos los índices x de 1 hasta n en una complejidad de O(n) y para cada índice x, iterar y desde x hasta que se cumpla que y > n o $bit(a_y) > k$ con una complejidad de O(n), para una complejidad total de $O(n^2)$.

2.3.3. Divide y Vencerás

Ahora para continuar mejorando la solución del ejercicio se puede utilizar un enfoque se divide y vencerás. Para ello se puede buscar la mayor potencia de 2 que es menor que n o simplemente el último bit activo de n y elegir esta potencia como pivote, observe que en la parte izquierda del pivote solo se deben buscar subarreglos k-buenos de 0 a $2^q - 1$ (q es el último bit activo de n) mientras en la parte derecha del pivote todos los números tienen activado el bit q (q es el último bit activo para cada uno de estos números) por lo que se puede buscar subarreglos de (k-1)-buenos de 0 a $n-2^q-1$ (aquí el truco radica en restar 2^q a todos los números en la parte izquierda del pivote y trabajar desde 0 a $n-2^q-1$).

Entonces resta resolver la parte de la conquista eficientemente, es decir buscar los arreglos k-buenos que tengan el extremo izquierdo de a la izquierda del pivote y el extremo derecho a la derecha del del pivote. Para ello se define la

función f(n,k) = (c,l,r), la función f(n,k) retorna el número de subarreglos k-buenos de 0 a n-1, la longitud de del subarreglo k-bueno más grande que termina en n-1, respectivamente, observe que l y r pueden ser igual a 0. Ahora la cantidad de subarreglos pertenecientes a la conquista simplemente es la multiplicación del tamaño del subarreglo más grande que termina en 2^q y el tamaño del subarreglo más grande que comienza en 2^q . El resto de la solución usando este método consiste en el mantenimiento de las invariantes descritas, a continuación se presenta un pseudocódigo:

```
f(n, k) {
    q <-- último bit activo de n

    if(k < 0)
        return 0, 0, 0

    if(n == 0)
        return 1, 1, 1

    if(2**q == n)
        q--

    c1, l1, r1 = f(2**q, k)
    c2, l2, r2 = f(n - 2**q, k - 1)

    l = l1 == 2**q ? l1 + l2 : l1
    r = r2 == n - 2**q ? r2 + r1 : r2

    return c1 + c2 + r1 * l2, l, r
}</pre>
```

Solo falta analizar la complejidad temporal, en cada llamado recursivo dividimos la entrada en 2 y hacemos 2 llamadas recursivas, la conquista tiene una complejidad de O(1) por lo que el T(n) recursivo quedaría de la siguiente manera: T(n) = 2T(n/2) + c, por lo que la complejidad final es O(n).

2.3.4. Programación Dinámica

Si se observa el algoritmo descrito en la sección anterior, cuando se divide el tamaño de la entrada en la parte izquierda del pivote siempre se hace buscan los subarreglos de 0 a n-1, donde n siempre es una potencia de 2, por lo que si se memoriza los valores de f(n,k) cuando n es una potencia de 2, la suma de todos los llamados que se realizan en la parte izquierda tiene una complejidad total de $O(\log(n)k)$.

```
f(n, k) {
    q <-- último bit activo de n

if(k < 0)
    return 0, 0, 0

if(n == 0)
    return 1, 1, 1

if(dp[q][k] and n == 2**q)
    return dp[q][k]</pre>
```

```
if(2**q == n)
    q--

c1, l1, r1 = f(2**q, k)
 c2, l2, r2 = f(n - 2**q, k - 1)

l = l1 == 2**q ? l1 + l2 : l1
 r = r2 == n - 2**q ? r2 + r1 : r2

if(2**q == n)
    dp[q][k] = c1 + c2 + r1 * l2, l, r

return c1 + c2 + r1 * l2, l, r
}
```

Entonces con esta modificación el T(n) recursivo quedaría de la siguiente manera: T(n) = T(n/2) + c, por lo que la complejidad del T(n) es $O(\log(n))$ y la complejidad final es $O(\log(n)k)$.

3. Distribución Justa

3.1. Ejercicio

- límite de tiempo por prueba: 0.35 segundos
- límite de memoria por prueba: 1024 megabytes

Un empresario tiene N planos, cada uno describiendo un tipo de edificio. Cada plano especifica la altura del edificio mediante dos enteros G y R.

- G: Altura del piso de planta baja. Puede ser cero, lo que indica que el edificio no tiene planta baja.
- R: Altura de cada piso residencial. Cada edificio tiene al menos un piso residencial.

El empresario quiere distribuir todos estos planos entre sus dos hijos, Alicia y Bob. Cada hijo construirá exactamente un edificio de cada plano que se le asigne, eligiendo el número de pisos residenciales para cada edificio.

El empresario quiere evitar mostrar favoritismo hacia cualquiera de los hijos, por lo que busca una distribución justa de los planos. Decidió que una distribución justa es aquella en la que es posible construir los edificios de tal manera que la suma de las alturas de los edificios construidos por cada hijo sea la misma. ¿Puedes decir si existe una distribución justa?

Considera el siguiente ejemplo con N=3 planos:

- G = 1 y R = 1 (las alturas posibles son 2, 3, 4,...);
- G = 0 y R = 3 (sin planta baja, las alturas posibles son 3, 6, 9,...);
- G = 2 y R = 1 (las alturas posibles son 3, 4, 5,...).

En este caso, una distribución justa posible es asignar el segundo plano a Alicia y el resto a Bob. Aunque Alicia recibe un solo plano mientras que Bob recibe dos, pueden construir dos pisos residenciales en el primer tipo de edificio (altura 3), dos pisos residenciales en el segundo (altura 6) y un piso residencial en el tercero (altura 3). De esta manera, la suma de las alturas de los edificios construidos por cada hijo sería 6.

Entrada

La primera línea contiene un número entero N $(1 \le N \le 2 \cdot 10^5)$ que indica el número de planos.

Cada una de las siguientes N líneas contiene dos enteros G ($0 \le G \le 2 \cdot 10^5$) y R ($1 \le R \le 10^9$), que denotan respectivamente la altura de la planta baja y la altura de cada piso residencial especificada por el plano correspondiente. La suma de las alturas de las plantas bajas de todos los planos es como máximo $2 \cdot 10^5$.

Salida

Imprime una sola línea con la letra mayúscula \mathbf{Y} si existe una distribución justa de los planos, y la letra mayúscula \mathbf{N} en caso contrario.

3.2. Etiquetas

- Suma de subconjunto
- Teoría de Números
- Mochila DP

3.3. Solución

Para este problema se deben particionar el conjunto de los planos de los edificios en 2 subconjuntos, para asignar a Alice y a Bbb respectivamente de tal manera que exista una configuración en la que la suma de los edificios construidos por cada uno sea igual.

Para la solución de este problema primero se eliminará la restricción de la suma de las alturas de las plantas bajas y luego se resolverá el ejercicio usando esta restricción.

3.3.1. Teoría de Números

Se define los conjuntos A y B como el conjunto de índices de los edificios que construye Alice y Bob respectivamente. Entonces se cumple que $|A|=p, |B|=q, p+q=n, A=\{a_1,a_2,\ldots a_p\}, B=\{b_1,b_2,\ldots b_q\}, p>0$ y q>0.

Luego el ejercicio se reduce a encontrar si existe una solución de a la siguiente ecuación:

$$g_{a_1} + r_{a_1}x_{a_1} + g_{a_2} + r_{a_2}x_{a_2} + \dots + g_{a_p} + r_{a_p}x_{a_p} = g_{b_1} + r_{b_1}x_{b_1} + g_{b_2} + r_{b_2}x_{b_2} + \dots + g_{b_q} + r_{b_q}x_{b_q}$$
(1)

donde $x_i > 0, \forall i : 1 \leq i \leq n$. Transformando la ecuación anterior:

$$r_{a_1}x_{a_1} + r_{a_2}x_{a_2} + \ldots + r_{a_p}x_{a_p} - r_{b_1}x_{b_1} - r_{b_2}x_{b_2} - \ldots - r_{b_q}x_{b_q} = g_{b_1} + g_{b_2} + \ldots + g_{b_q} - g_{a_1} - g_{a_2} - \ldots - g_{a_p}$$
 (2)

$$r_{a_1}x_{a_1} + r_{a_2}x_{a_2} + \ldots + r_{a_p}x_{a_p} - r_{b_1}x_{b_1} - r_{b_2}x_{b_2} - \ldots - r_{b_q}x_{b_q} = k$$
(3)

entonces una condición necesaria para que la ecuación tenga solución es que:

$$\operatorname{mcd}(r_1, r_2, \dots, r_n) \mid k \tag{4}$$

Sea la ecuación de ax + by = c, con $a > 0 \land b > 0$ por el teorema de **Bezout** se tiene que:

$$x = x_0 - k\frac{b}{d} \wedge y = y_0 + k\frac{a}{d} \tag{5}$$

donde x_0 y y_0 son soluciones particulares de la ecuación y d = mcd(a, b). Observe que siempre podemos garantizar que exista una solución x = x' y y = y', con $x' > 0 \land y' < 0$, ya que independientemente del signo de x_0 y y_0 se puede seleccionar un k negativo con módulo lo suficientemente grande para encontrar x' y y'

Ahora volviendo al ejercicio, por la observación anterior se puede asegurar que existe una solución mayor que 0 para x_{a_1} la ecuación:

$$r_{a_1}x_{a_1} + w_1 \operatorname{mcd}(r_{a_2}, r_{a_3}, \dots, r_{a_n}, r_{b_1}, r_{b_2}, \dots, r_{b_n}) = k$$
 (6)

y siguiendo misma idea se puede asegurar que existe una solución positiva para cada uno de los x_{a_i} $\forall i: 2 \le i \le p-1$ en las siguientes ecuaciones:

$$r_{a_2}x_{a_2} + w_2 \operatorname{mcd}(r_{a_3}, \dots, r_{a_p}, r_{b_1}, r_{b_2}, \dots, r_{b_q}) = w_1 \operatorname{mcd}(r_{a_2}, \dots, r_{a_p}, r_{b_1}, r_{b_2}, \dots, r_{b_q})$$

$$(7)$$

$$r_{a_3}x_{a_3} + w_3 \operatorname{mcd}(r_{a_4}, \dots, r_{a_n}, r_{b_1}, r_{b_2}, \dots, r_{b_n}) = w_2 \operatorname{mcd}(r_{a_3}, \dots, r_{a_n}, r_{b_1}, r_{b_2}, \dots, r_{b_n})$$
(8)

:

$$r_{a_{p-1}}x_{a_{p-1}} + w_{p-1}\operatorname{mcd}(r_{a_p}, r_{b_1}, r_{b_2}, \dots, r_{b_q}) = w_{p-2}\operatorname{mcd}(r_{a_{p-1}}, r_{a_p}, r_{b_1}, r_{b_2}, \dots, r_{b_q})$$

$$(9)$$

Ahora se debe probar que la siguiente ecuación tiene soluciones con las restricciones anteriores:

$$r_{a_n}x_{a_n} - r_{b_1}x_{b_1} - r_{b_2}x_{b_2} - \dots - r_{b_n}x_{b_n} = w_{p-1}\operatorname{mcd}(r_{a_n}, r_{b_1}, r_{b_2}, \dots, r_{b_n})$$
 (10)

Usando el enfoque anterior se puede asegurar que existe una solución mayor que 0 para cada uno de los $x_{b_i} \forall i : 2 \le i \le q$ en las siguientes ecuaciones:

$$e_q \operatorname{mcd}(a_p, r_{b_1}, \dots, r_{b_q-1}) - r_{b_q} x_{b_q} = w_{p-1} \operatorname{mcd}(r_{a_p}, r_{b_1}, r_{b_2}, \dots, r_{b_q})$$
(11)

$$e_{q-1}\operatorname{mcd}(a_p, r_{b_1}, \dots, r_{b_q-2}) - r_{b_{q-1}}x_{b_{q-1}} = e_q\operatorname{mcd}(a_p, r_{b_1}, \dots, r_{b_q-1})$$
(12)

:

$$e_2 \operatorname{mcd}(a_p, r_{b_1}) - r_{b_2} x_{b_2} = e_3 \operatorname{mcd}(a_p, r_{b_1}, r_{b_2})$$
(13)

Finalmente se puede asegurar una solución mayor que 0 para x_n y b_1 :

$$r_{a_p} x_{a_p} - r_{b_1} x_{b_1} = e_2 \operatorname{mcd}(a_p, r_{b_1}) \tag{14}$$

Por tanto se puede asegurar (4) es una condición necesaria y suficiente para que (3) tenga solución. Además de esto la demostración anterior proporciona un algoritmo para encontrar dichas soluciones (las soluciones particulares de la ecuación de **Bezout** se pueden encontrar usando el algoritmo **Extendido de Euclides**).

Entonces se ha demostrado que el ejercicio es equivalente a encontrar dos conjuntos P y Q tales que, $P \cup Q = \{g_1, g_2, \ldots, g_n\}, P \neq \emptyset, Q \neq \emptyset, P \cap Q = \emptyset$ y además debe cumplirse que:

$$\operatorname{mcd}(r_1, r_2, \dots, r_n) \mid \sum_{i=0}^{|P|} p_i - \sum_{i=0}^{|Q|} q_i$$
 (15)

donde los p_i y q_i son los elementos que de los conjuntos P y Q respectivamente.