$$i \equiv j \pmod{N} \tag{3.58}$$

lo cual es una contradicción. Por tanto $\vec{a}$ genera A_M.

Este mismo razonamiento permite demostrar que, si α es el menor entero positivo tal que $M|\alpha\vec{a}$ (recordar que, entonces, $(M,\vec{a}) = N/\alpha$) los vectores $\vec{a}$, $2\vec{a}$,..., $\alpha\vec{a}$ son distintos módulo M. Además $(\alpha+1)\vec{a} \equiv \vec{a} \pmod{M}$, por tanto α es, en realidad, el *orden* del elemento $\vec{a}$.

Según el teorema anterior y la definición de m.c.d. dada en (3.36), es inmediato que una condición necesaria para que $\vec{a}$ sea generador de A_M es

$$(N, (\vec{a})) = 1 \tag{3.59}$$

o sea

$$(\vec{a},M) = 1 \Longrightarrow ((\vec{a}), N) = 1 \tag{3.60}$$

Hemos visto que, si $(\vec{a},M) = 1$, el conjunto $S=\{\vec{a},2\vec{a},..,N\vec{a}\}$ es un sistema completo de residuos módulo M. Además, en la sección 3.3.2 se vió que $\phi(N)$ de estos vectores, los que son de la forma $\alpha\vec{a}$ con $(\alpha,N) = 1$, cumplen $(\alpha\vec{a},M) = 1$.

Que no existen otros vectores de S con estas características se deduce de un resultado que puede considerarse como generalización del teorema 3.2.5, y que se demuestra de la misma forma[5]. Esto es:

$$(\vec{a},M) = 1 \text{ y } (\alpha,N) = g \in Z^+ \Longrightarrow (\alpha\vec{a},M) = g \tag{3.61}$$

Teorema 3.3.6:

Si el grupo A_M es cíclico, tiene $\phi(N)$ generadores.

---

(5) Basándose en el hecho de que, si $a,b,m \in Z$, $(a,m) = 1$, $(b,m) = g$, entonces $(ab,m) = g$. Ver |NZ1|.

Siguiendo con nuestro ejemplo, en primer lugar se comprueba fácilmente que el vector $\vec{a} = (2,1)$ de la figura 3.3.1 es un generador de A_M; bien sea viendo que $(\vec{a},M) = 1$ (aplicando (3.35)) o bien, como se muestra en dicha figura, comprobando que los vectores $\vec{a}$, $2\vec{a}$,..., $N\vec{a}$ (puntos situados en linea recta) son todos distintos módulo $M = \begin{pmatrix} 3 & 1 \\ -2 & 4 \end{pmatrix}$.

Por tanto, en este caso, el grupo es cíclico y además, como los números primos con N=14 son 1, 3, 5, 9, 11 y 13, los $\phi(N) = 6$ generadores de A_M son $\vec{a}$, $3\vec{a}$, $5\vec{a}$, $9\vec{a}$, $11\vec{a}$ y $13\vec{a}$ mod. M. Estos puntos vienen indicados con un pequeño círculo en la figura 3.3.1 y, según el sistema completo de residuos escogido en ella, corresponden a los vectores mostrados en la figura 3.3.2.

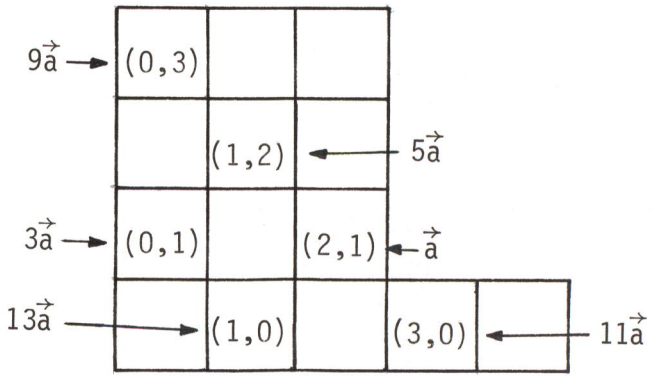

Fig. 3.3.2

El hecho de que el grupo A_M tenga tantos generadores como el grupo multiplicativo M_N en Z (en el cual el conjunto de elementos es el conjunto de enteros módulo N y primos con N, y la operación es la multiplicación mod. N), induce a pensar en la posibilidad de definir un producto entre los vectores de A_M. Esto será posible gracias al concepto de "generador lineal" que introduciremos en el apartado siguiente.

3.3.5 Generadores lineales

Diremos que el vector $\vec{p} = (p_1,\ldots,p_n) \varepsilon Z^n$ es un *generador lineal* de A_M si se cumple

$$\forall \vec{x},\vec{y} \varepsilon Z^n, \quad \vec{x} \equiv \vec{y} \pmod{M} \Longleftrightarrow \vec{x}\cdot\vec{p} \equiv \vec{y}\cdot\vec{p} \pmod{N} \tag{3.62}$$

donde el punto entre vectores indica producto escalar.

Notar que el vector $\vec{p}$ permite establecer un isomorfismo, ψ, entre el grupo A_M y el grupo de las N clases de restos mod. N que denotaremos por A_N o, equivalentemente, entre los sistemas completos de residuos mod. M, $S = \{\vec{r}_1,\ldots,\vec{r}_N\}$, y mod. N, $T = \{0,..,N-1\}$ de manera que

$$\psi : S \longrightarrow T, \quad \psi(\vec{r}_i) = \vec{p}\cdot\vec{r}_i \pmod{N} \tag{3.63}$$

En particular, existe $\vec{r}_j \varepsilon S$ tal que

$$\vec{p}\cdot\vec{r}_j \equiv 1 \pmod{N} \tag{3.64}$$

es decir

$$\vec{p}\cdot\vec{r}_j + \alpha N = 1, \ \alpha \varepsilon Z \tag{3.65}$$

por tanto, una condición necesaria para que $\vec{p}$ sea generador lineal de A_M es

$$(p_1,\ldots,p_n,N) = ((\vec{p}),N) = 1 \tag{3.66}$$

Notar la analogía con (3.59).

Siguiendo con (3.63), sabemos por el teorema 3.3.4 que, si α_i denota cualquiera de los $\phi(N)$ enteros tales que $0<\alpha<N$ y $(\alpha_i,N) = 1$, los conjuntos $\alpha_i S = \{\alpha_i\vec{r}_1,\ldots,\alpha_i\vec{r}_N\}$, i = 1,..., (N), también son sistemas completos de residuos mod. M; e igualmente los conjuntos $\alpha_i T = \{\alpha_i\vec{p}\cdot\vec{r}_1,\ldots,\alpha_i\vec{p}\cdot\vec{r}_N\}$ mod. N |NZ1|. Por tanto

los $\phi(N)$ vectores $\alpha_i\vec{p}$, $i = 1,\ldots,\phi(N)$ son generadores lineales. Veamos que todos ellos son distintos módulo N, es decir, dados dos vectores cualesquiera, no todas sus componentes son iguales mod. N.

En efecto, si

$$\alpha_i\vec{p} \equiv \alpha_j\vec{p} \pmod{N} \text{ (componente a comp.)}, \quad i \neq j \tag{3.67}$$

multiplicando escalarmente ambos miembros por el vector $\vec{r}_j \in Z^n$ dado por la relación (3.64), obtenemos[6]

$$\alpha_i\vec{p}\cdot\vec{r}_j \equiv \alpha_j\vec{p}\cdot\vec{r}_j \pmod{N} \tag{3.68}$$

de donde

$$\alpha_i \equiv \alpha_j \pmod{N} \tag{3.69}$$

en contradicción con la hipótesis.

Supongamos como antes que la matriz M está formada por los vectores $\vec{m}_1,\ldots,\vec{m}_n$. Si en (3.6.2) hacemos $\vec{x} = \vec{m}_i$ y $\vec{y} = \vec{0}$, $i = 1,\ldots,n$, (recordar el teorema 3.3.1(a)) obtenemos otra condición necesaria para que $\vec{p}$ sea generador lineal, a saber: $\vec{p}\cdot\vec{m}_i \equiv 0 \pmod{N}$ $\forall i$. Esta condición, junto con la dada en (3.66), son también suficientes, es decir que una definición equivalente a (3.62) es:

$\vec{p}$ es generador lineal de A_M si y sólo si cumple

(a) $\vec{p}\cdot\vec{m}_i \equiv 0 \pmod{N}$ $\forall i = 1,\ldots,n$ (3.70a)

(b) $((\vec{p}), N) = 1$ (3.70b)

En efecto, nos basta demostrar, a partir de estas condiciones, que *los vectores de la forma $\vec{z} = \vec{\lambda}M \equiv \vec{0} \pmod{M}$, $\vec{\lambda} \in Z^n$, y sólo ellos, satisfacen $\vec{p}\cdot\vec{z} \equiv 0 \pmod{N}$*, ya que esto es lo que afirma (3.62) si hacemos $\vec{z} = \vec{x} - \vec{y}$.

---

(6) Recordar el teorema homólogo al teor. 3.3.1(c) en Z, o sea si $a \equiv b$ y $c \equiv d \pmod{m}$ entonces $\alpha a+\beta c \equiv \alpha b+\beta d \pmod{m}$ siendo todos los números enteros.

Según (3.70a)

$$\vec{p}\cdot\vec{z} = \vec{p}\cdot(\lambda_1\vec{m}_1 + \ldots + \lambda_n\vec{m}_n) \equiv 0 \pmod{N} \qquad (3.71)$$

Además, según (3.70b), existe $\vec{x}_1 \in Z^n$ tal que $\vec{x}_1\cdot\vec{p} \equiv 1 \pmod{N}$, por tanto $\forall i = 1,\ldots,N$ existe $\vec{x}_i \in Z^n$ tal que

$$\vec{x}_i\cdot\vec{p} \equiv i \pmod{N} \qquad (3.72)$$

Entonces, si aparecen todas las clases de restos en Z, debemos tener igualmente N clases residuales en Z^n. En particular

$$\vec{z}\cdot\vec{p} \equiv 0 \pmod{N} \Longrightarrow \vec{z} \equiv \vec{0} \pmod{M} \qquad (3.73)$$

El siguiente resultado caracteriza a los grupos A_M que poseen generadores lineales.

Teorema 3.3.7:

A_M es cíclico si y sólo si tiene un generador lineal

Demostración:

Si A_M es cíclico, sea $\vec{a}$ un generador. Entonces construimos el generador lineal $\vec{p}$ de la siguiente forma: $\forall i = 1,\ldots,n$, sea p_i, $0 < p_i < N$, el menor entero positivo tal que

$$\vec{e}_i \equiv p_i\vec{a} \pmod{M} \qquad (3.74)$$

donde $\vec{e}_i = (0,\ldots,1,\overset{(i}{\ldots},0)$. Demostraremos que $\vec{p}$ cumple (3.62).

Supongamos que $\vec{x} \equiv \vec{y} \pmod{M}$. Por una parte

$$\vec{x} = (x_1,\ldots,x_n) = x_1\vec{e}_1+\ldots+x_n\vec{e}_n \equiv x_1p_1\vec{a}+\ldots+x_np_n\vec{a} = (\vec{x}\cdot\vec{p})\vec{a} \pmod{M} \qquad (3.75)$$

Análogamente

$$\vec{y} \equiv (\vec{y}\cdot\vec{p})\vec{a} \pmod{M} \qquad (3.76)$$

Por tanto

$$(\vec{x}\cdot\vec{p})\vec{a} \equiv (\vec{y}\cdot\vec{p})\vec{a} \pmod{M} \qquad (3.77)$$

de donde, según el corolario 3.3.2(b) y por ser $\vec{a}$ generador de A_M, o sea $(\vec{a},M) = 1$, obtenemos

$$\vec{x}\cdot\vec{p} \equiv \vec{y}\cdot\vec{p} \pmod{N} \tag{3.78}$$

Recíprocamente, si se satisface (3.78), aplicando el teorema 3.3.1(b) podemos escribir:

$$(\vec{x}\cdot\vec{p})\vec{a} \equiv (\vec{y}\cdot\vec{p})\vec{a} \pmod{M} \tag{3.79}$$

Desarrollando ambos miembros

$$x_1p_1\vec{a}+\ldots+x_np_n\vec{a} \equiv y_1p_1\vec{a}+\ldots+y_np_n\vec{a} \pmod{M} \tag{3.80}$$

pero, según (3.74), esto implica

$$x_1\vec{e}_1 +\ldots+ x_n\vec{e}_n \equiv y_1\vec{e}_1 +\ldots+ y_n\vec{e}_n \pmod{M} \tag{3.81}$$

que equivale a

$$\vec{x} \equiv \vec{y} \pmod{M} \tag{3.82}$$

En cuanto a la condición suficiente, si $\vec{p}$ es un generador lineal de A_M, escogemos $\vec{a}$ de manera que

$$\vec{a}\cdot\vec{p} \equiv \alpha \pmod{N} \tag{3.83}$$

siendo α cualquier entero tal que $(\alpha,N) = 1$, lo cual siempre es posible ya que $\vec{p}$ satisface (3.66).

Entonces, como los números $\vec{a}\cdot\vec{p}$, $2\vec{a}\cdot\vec{p}$,..., $N\vec{a}\cdot\vec{p}$ forman un sistema completo de restos mod. N, según (3.62), los vectores $\vec{a}$, $2\vec{a}$, ..., $N\vec{a}$ forman asimismo un sistema completo de residuos mod. M.

Según la demostración del teorema anterior, cada generador de A_M da lugar a un generador lineal. Además, según hemos visto, si existe uno, $\vec{p}$, existen $\phi(N)$ generadores lineales distintos módulo N de la forma $\alpha_i p$, $(\alpha_i,N) = 1$, por tanto, al resolver (3.73), generadores distintos darán lugar a generadores lineales distintos.

Así, el teorema 3.3.7 podría reenunciarse diciendo que

A_M es cíclico si y sólo si tiene $\phi(N)$ generadores lineales.

En el ejemplo que venimos considerando, y tomando el generador $\vec{a} = (2,1)$, las ecuaciones diofánticas derivadas de (3.73) son

$$(1,0) \equiv p_1(2,1) \pmod{M} \qquad (3.84a)$$

$$(0,1) \equiv p_2(2,1) \pmod{M} \qquad (3.84b)$$

con $M = \begin{pmatrix} 3 & 1 \\ -2 & 4 \end{pmatrix}$, y se obtienen las soluciones $p_1 = 13$ y $p_2 = 3$ (mod N). En la figura 3.3.1 se muestra como obtener este resultado geométricamente.

Procediendo análogamente con los otros 5 generadores de la figura 3.3.2, se obtienen otros tantos generadores lineales. Todos ellos se muestran en la figura 3.3.3 ocupando el mismo lugar que los generadores de los cuales proceden.

Otra forma más sencilla de obtener todos los generadores lineales es, como hemos dicho, multiplicando (mod 14) el primero, (13,3), por los números α_i, $1<\alpha_i<14$, $(\alpha_i,14) = 1$, según se muestra en el gráfico de la figura 3.3.4.

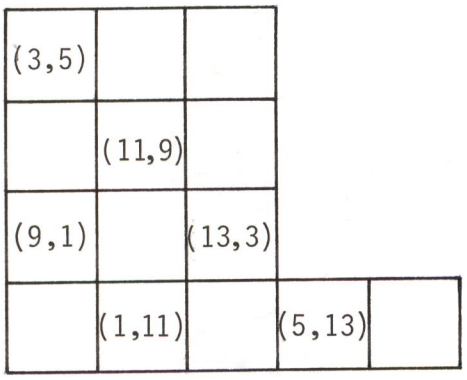

Fig. 3.3.3

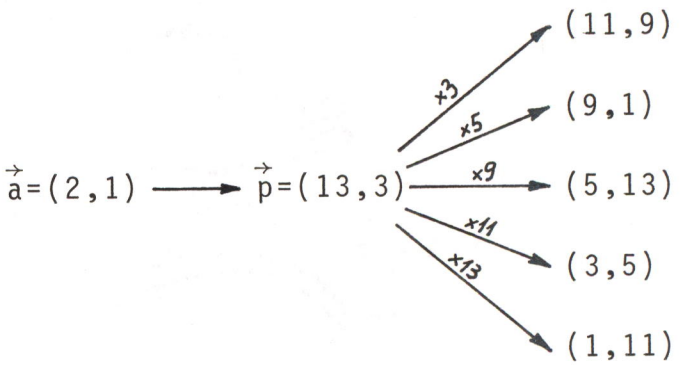

Fig. 3.3.4

Como comentamos al final del apartado 3.3.4, a través de los generadores lineales se puede definir un producto entre los vectores del grupo A_M.

En efecto, si $\vec{x}$ e $\vec{y}$ son elementos del grupo y $\vec{p}$ es un generador lineal de A_M, diremos que $\vec{z}$ es el *producto de* $\vec{x}$ *por* $\vec{y}$ *módulo M*, denotándolo por $\vec{z} = \vec{x} \otimes \vec{y}$, si y sólo si

$$\vec{z}\cdot\vec{p} \equiv (\vec{x}\cdot\vec{p})(\vec{y}\cdot\vec{p}) \pmod{N} \tag{3.85}$$

Es inmediato demostrar que esta operación está bien definida en el sentido de que si $\vec{a} \equiv \vec{b} \pmod{M}$ y $\vec{c} \equiv \vec{d} \pmod{M}$ entonces $\vec{a} \otimes \vec{b} \equiv \vec{c} \otimes \vec{d} \pmod{M}$.

Además el producto así definido permite establecer un grupo multiplicativo, M_M, en Z^n, en el cual el conjunto de elementos es el conjunto de vectores mod. M generadores de A_M (es decir, cuyo m.c.d. con M es 1). Dicho grupo es isomorfo con el grupo M_N en Z citado anteriormente.

Dada M, otro procedimiento para hallar un generador lineal $\vec{p}$ de A_M es resolver las n ecuaciones diofánticas que se derivan de (3.70a) imponiendo además la condición (3.70b). Ver |FVY2| y |FYV1|. Así, (3.70a), en forma matricial, equivale a

$$\vec{p}M^T = \vec{\mu}N \tag{3.86}$$

donde M^T denota la transpuesta de M y $\vec{\mu} \in Z^n$.
Despejando

$$\vec{p} = N\vec{\mu}(M^T)^{-1} \tag{3.87}$$

solución que será válida si cumple (3.70b), o sea

$$(N, N\vec{\mu}(M^T)^{-1}) = 1 \tag{3.88}$$

lo que, recordando la definición (3.36), equivale a

$$(\vec{\mu}, M^T) = 1 \tag{3.89}$$

luego existe un generador lineal de A_M si A_{MT} es cíclico.

Esto justifica el siguiente teorema:

Teorema 3.3.8:

Dada M, A_M es cíclico si y sólo si A_{MT} es cíclico.

La doble implicación es consecuencia de $(M^T)^T = M$.

En el ejemplo anterior, la matriz transpuesta de M es $M^T = \begin{pmatrix} 3 & -2 \\ 1 & 4 \end{pmatrix}$ que genera el retículo mostrado en la figura 3.3.5.

Los generadores , indicados con una "o" en dicha figura, son los vectores $\vec{\mu}_1 = (3,-1)$, $\vec{\mu}_2 = (1,1)$, $\vec{\mu}_3 = (3,1)$, $\vec{\mu}_4 = (1,3)$, $\vec{\mu}_5 = (2,3)$ u $\vec{\mu}_6 = (2,-1)$. Entonces, según (3.87) y (3.89), cada uno de los generadores lineales de A_M, $\vec{p}_i$, mostrados en las figuras 3.3.3 y 3.3.4, vienen dados por

$$\vec{p}_i = (p_{i1}, p_{i2}) = N\vec{\mu}_i(M^T)^{-1} = (\mu_{i1},\mu_{i2})\begin{pmatrix} 4 & 2 \\ -1 & 3 \end{pmatrix} \qquad (3.90)$$

para todo i = 1,...,6.

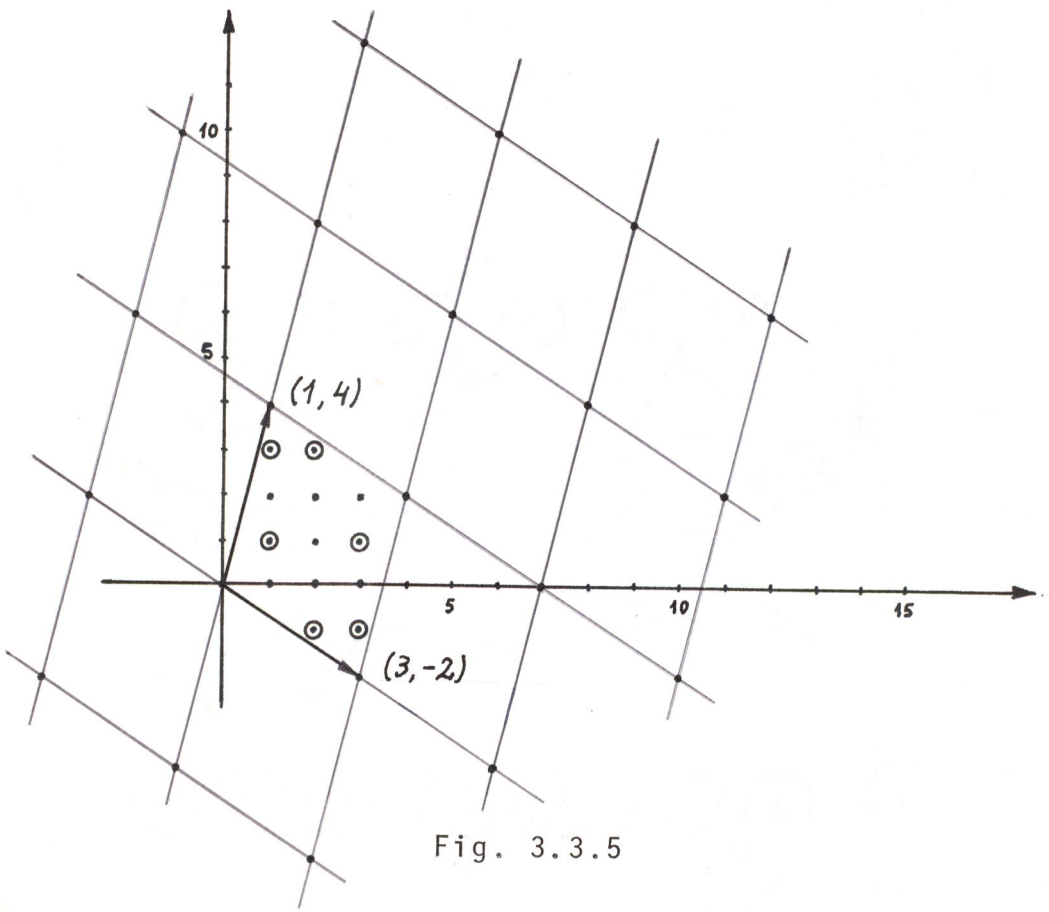

Fig. 3.3.5

3.3.6 Grupos cíclicos en Z^2

Para el caso n=2, hemos hallado una caracterización muy sencilla de los grupos A_M cíclicos y es la siguiente:

Teorema 3.3.9:

Sea M la matriz 2x2 formada por los vectores del plano $\vec{m}_1=(m_{11},m_{12})$ y $\vec{m}_2 = (m_{21},m_{22})$. Entonces el grupo A_M es cíclico y, por tanto, tiene un generador lineal, si y sólo si

$$\text{m.c.d. } \{m_{11}, m_{12}, m_{21}, m_{22}\} = (M) = 1 \qquad (3.91)$$

Demostración:

En primer lugar, pasaremos a la notación empleada en |FVY2| y |FYV1| y que quedará justificada en la sección 3.4. Sean $\vec{m}_1=(l,-y)$ y $\vec{m}_2 = (-x, h)$, de donde N = lh - xy.

Como hemos dicho, una matriz equivalente a M es la matriz M" formada por los vectores $\rho\vec{m}_1 + \sigma\vec{m}_2$ y $\tau\vec{m}_1 + \nu\vec{m}_2$, ρ, σ, τ, $\nu \in Z$, si det(M") = ±det(M). Mediante un cálculo sencillo es posible determinar estos coeficientes para que M" sea de la forma $\begin{pmatrix} L & 0 \\ -X & H \end{pmatrix}$ y resulta: ρ = h/(y,h), σ = y/(y,h), y τ y ν son cualquier par de enteros que cumplan $-\tau y + \nu h = (y,h)$ (sabemos que esta ecuación tiene infinitas soluciones). En efecto, con estos valores, se obtiene:

$$\rho\vec{m}_1 + \sigma\vec{m}_2 = (\rho l-\sigma x, -\rho y+\tau h) = \left(\frac{N}{(y,h)}, 0\right) \qquad (3.92)$$

$$\tau\vec{m}_1 + \nu\vec{m}_2 = (\tau l-\nu x, -\tau y+\nu h) = (\tau l-\nu x, (y,h)) \qquad (3.93)$$

de donde det(M") = N y, por tanto, M" ≡ M.

Además, y debido a que los elementos de M" se pueden expresar como combinación lineal de los de M y viceversa, es inmediato demostrar que

$$(M") = (M) \qquad (3.94)$$

Pasemos ahora a la demostración propiamente dicha. Por ser $M'' \equiv M$, A_M es cíclico si y sólo si lo es $A_{M''}$. Según el teorema 3.3.5, y aplicando la definición de m.c.d. dada en (3.35), sabemos que $A_{M''}$ es cíclico sii existe $\vec{a} = (a_1, a_2) \in Z^2$ tal que

$$(\vec{a}, M'') = (LH, a_1H+a_2X, a_2L) = 1 \qquad (3.95)$$

Si $(M) = (M'') = (L, X, H) = f \neq 1$ entonces, según (3.95), $(\vec{a}, M'') \geq f \quad \forall \vec{a} \in Z^2$, luego $A_{M''}$ no es cíclico y queda demostrada la condición necesaria.

Recíprocamente, si $(L, X, H) = 1$, sea $(L, X) = g$ con lo cual $(g, H) = 1$. Esto supone que $(L/g, X/g) = 1$, por tanto, según el conocido "teorema de Dirichlet"[7], en la sucesión $\{\frac{X}{g} + \xi\frac{L}{g}\}$, $\xi \in Z$, existen infinitos primos. En particular

$$\frac{X}{g} + \xi_i\frac{L}{g} = p_i \Longrightarrow \quad X + \xi_i L = gp_i \qquad (3.96)$$

siendo p_i un primo que podemos escoger tan grande como queramos.

Por otra parte, a partir de la matriz M'' y sumando al segundo vector una combinación lineal del primero, podemos obtener la matriz $M' \equiv M''$ siguiente:

$$M'' = \begin{pmatrix} L & 0 \\ -X & H \end{pmatrix} \equiv M' = \begin{pmatrix} L & 0 \\ -(x+\xi_i L) & H \end{pmatrix} = \begin{pmatrix} L' & 0 \\ -X' & H' \end{pmatrix} \qquad (3.97)$$

donde escogeremos ξ_i de forma que p_i, dado por (3.96), cumpla $(p_i, H) = 1$ de donde, al ser $(g, H) = 1$, se implica $(p_i g, H) = 1$, es decir

$$(X+\xi_i L, H) = (X', H') = 1 \qquad (3.98)$$

---

(7) El teorema de Dirichlet afirma que si $(a_o, r) = 1$, la progresión aritmética $a_o + nr$, $n = 0,1,\ldots$ contiene infinitos primos. Ver p.e. |A2, cap.7|.

pero, como antes, $A_{M''}$ es cíclico si y sólo si lo es $A_{M'}$, o sea, si existe $\vec{a} \in Z^2$ tal que

$$(\vec{a}, M') = (L'H', a_1H'+a_2X', a_2L') = 1 \qquad (3.99)$$

pero, por (3.98), existen enteros a_1 y a_2 tales que $a_1H'+a_2X' = 1$, lo que asegura el cumplimiento de (3.99) y completa la demostración.

A partir de la matriz M', y aplicando las condiciones (3.70a y b) se puede obtener también muy fácilmente un generador lineal p de $A_{M'}$, y por tanto de A_M. Resulta

$$\vec{p} = (H', X') = (H, X+\xi_i L) \qquad (3.100)$$

3.4 REDES DE PASOS CONMUTATIVOS

3.4.1 Consideraciones generales

En esta sección usaremos la relación de equivalencia entre vectores de Z^n, establecida en la sección 3.3, para construir redes de camino dedicado unidireccional tales como las estudiadas en la sección 3.1.

Como sabemos, este tipo de grafos son especialmente aptos para modelar las estructuras de interconexión en redes locales.

Una *red de pasos conmutativos* con N nudos y grado d = n queda completamente especificada por la matriz nxn M formada por los vectores $\vec{m}_1,\ldots,\vec{m}_n \in Z^n$ y con det(M) = N. Al grafo d-diregular generado de esta forma lo denotaremos por $D_M = (V, A)$.

En efecto, cada vértice de D_M se corresponde con un elemento del grupo A_M, de manera que, para identificar los elementos de V, escogeremos un sistema completo de residuos módulo M,

$S = \{\vec{r}_1,\ldots,\vec{r}_N\}$.

Así, V = S y las funciones de la sección 3.1 (recordar el punto 2 al final de ella) son de la forma:

$$f_i: S \longrightarrow S \ , \ f_i(\vec{r}_j) = \vec{r}_j + \vec{e}_i \ (\text{mod. } M) \qquad (3.101)$$
$$\forall i = 1,\ldots,n \text{ y } \forall j = 1,\ldots,N$$

Las funciones f_i son *conmutativas* y, según el teor. 3.3.1c, *biyectivas*. Por tanto, la red D_M satisface las propiedades estudiadas en la sección 3.1.

La simetría de la estructura obtenida (D_M es un *digrafo simétrico* |H1|) permite estudiar sus características a partir de cualquier vértice. Por comodidad elegimos el vértice $\vec{0}$.

Además, y debido a que los principales parámetros a estudiar son *diámetro* y *distancia media*, tomaremos los demás vectores de $S = \{(r_{j1},\ldots,r_{jn}) \mid j = 1,\ldots,N\}$ de manera que $r_{ji} \geq 0 \ \forall i,j$ y las sumas de sus componentes $r_{j1}+\ldots+r_{jn}$ sean mínimas $\forall j = 1,..,N$. Así, cada una de dichas sumas representa la distancia desde el vértice $\vec{0}$ hacia el vértice $\vec{r}_j$, es decir

$$\forall j=1,..,N \qquad d(\vec{0}, \vec{r}_j) = \sum_{i=1}^{n} r_{ji} \qquad (3.102)$$

Resumiendo, S es el conjunto de N puntos de Z^n distintos mod. M, con coordenadas no negativas y cuya *distancia ortogonal* al origen es mínima.

Entonces, el diámetro k y la distancia media entre vértices $\bar{k}$ de D_M vienen dados por

$$k = \max\{\sum_{i=1}^{n} r_{ji}, \ j=1,\ldots,N\} \qquad (3.103)$$

$$\bar{k} = \frac{1}{N} \sum_{j=1}^{N} \sum_{i=1}^{n} r_{ji} \qquad (3.104)$$

Todo ello justifica la elección del conjunto $C_{\vec{0}}$ que hemos hecho en el apartado 3.3.3.

Para minimizar el diámetro y/o la distancia media, deseamos que todos los vértices estén tan cerca del $\vec{0}$ como sea posible. Por tanto, dados k y d, la red óptima D_M sería aquella cuyo conjunto de vértices fuese

$$V = S^* = \{(m_1,\ldots,m_d) \mid 0 \leq m_i,\ \Sigma m_i \leq k\} \qquad (3.105)$$

lo que, según (3.3), implica

$$|V| = \det(M) = \binom{d+k}{d} \qquad (3.3')$$

vértices.

Demostrar que no existe tal red para k>1 equivale a ver que, para tal k, no existe M cuyo sistema completo de residuos sea S^* o también, según el apartado 3.3.3, que el conjunto $C^*_{\vec{0}}$ construido a partir de S^* no tesela mediante traslaciones el espacio R^d.

Enunciamos este resultado de la forma siguiente:

Teorema 3.4.1:

En toda red D_M de pasos conmutativos, grado d y diámetro k>1, se cumple

$$N < \binom{d+k}{d} \qquad (3.106)$$

Demostración:

Supongamos que todos los elementos de S^* son distintos[8]. Demostra

---

(8) En lo sucesivo, tanto las igualdades de los vectores de Z^n como las operaciones entre ellos son módulo M.

remos que, entonces, C_0^* no tesela el espacio R^d.

Consideremos el conjunto

$$E_i = \{(m_1,\ldots,-1,\overset{(i}{\ldots},m_d) \mid 0 \leqslant m_j,\ 0 \leqslant \sum_{j\neq i} m_j \leqslant k-1\} \tag{3.107}$$

De la desigualdad

$$(m_1,\ldots,0,\overset{(i}{\ldots},m_d) \neq (m_i',\ldots,0,\overset{(i}{\ldots}m_d') \tag{3.108}$$

debida al supuesto de que los m_j y m_j' cumplen la condición impuesta en (3.107) y, por tanto, ambos puntos pertenecen a $\mathcal{S}^*$, se obtiene, sumando $-\vec{e}_i$ [9] a ambos miembros,

$$(m_1,\ldots,-1,\overset{(i}{\ldots},m_d) \neq (m_1',\ldots,-1,\overset{(i}{\ldots},m_d') \tag{3.109}$$

Es decir, todos los puntos de E_i son distintos de manera que, según el mismo razonamiento que nos condujo a (3.3), tenemos

$$|E_i| = \binom{d+k-2}{d-1} \tag{3.110}$$

Definimos ahora el conjunto $E = \bigcup_{i=1}^{d} E_i$. Veamos que, análogamente, todo par de puntos pertenecientes a distintos E_i son tambien distintos. En efecto, si fuese

$$(m_1,\ldots,-1,\overset{(i_1}{\ldots},m_{i_2},\ldots,m_d) = (m_1',\ldots,m_{i_1}',\ldots,-1,\overset{(i_2}{\ldots},m_d') \tag{3.111a}$$

$$\text{con } i_1 \neq i_2 \text{ y } \quad 0 \leqslant \sum_{j\neq i_1} m_j \leqslant k-1 \quad \text{y} \quad 0 \leqslant \sum_{j\neq i_2} m_j \leqslant k-1 \tag{3.111b}$$

y sumando $\vec{e}_{i_1} + \vec{e}_{i_2}$ [10] a ambos miembros, resultaría

---

[9] Esto equivale a aplicar f_i^{-1} cuya existencia queda asegurada al ser f_i biyectiva.

[10] Es decir, aplicar $f_{i_1} \circ f_{i_2}$.