9
2 ej.

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CIENCIAS

Acerca de la Construcción de Soluciones para el Problema Modular de las n Damas

Tesis

que para obtener el título de

matemático

presenta

Carlos Castaño Bernard

Septiembre de 1992

Contenido

Notación y terminología

Sea **P** el plano euclideano, sea ***G*** el grupo de sus simetrías. Un *mosaico* en **P** es una cubierta **Φ** de subconjuntos compactos de **P** tal que

a. Sea **int** el operador interior (topológico). Para cada c, $c' \in \mathbf{\Phi}$ se tiene que $\mathbf{int}(c) \cap \mathbf{int}(c') \neq \varnothing$ implica $c = c'$.

b. Existe ***H***, subgrupo de ***G***, tal que $H(c) = \mathbf{\Phi}$, con $c \in \mathbf{\Phi}$.

Los elementos de **Φ** son llamados las *figuras* de **P**, la clase de las figuras de **P** módulo ***G*** es llamada la *figura generadora* del mosaico **Φ**.

Sea ***J*** un grupo. Dado un ***J***-conjunto S, sea **T*J*** el conjunto de los elementos $g \in J$ tales que $gx = x$, para algún x en S, implique $g = 1$. Llamemos a **T*J*** el conjunto de las *traslaciones* del ***J***-conjunto S . En los casos en los que estamos interesados en esta tesis, **T*J*** es un grupo.

1. Introducción

1.1. Un *tablero universal* es un mosaico χ en el plano euclideano **P** tal que su figura generadora sea la clase de congruencia de un cuadrado sólido. Una *casilla* es una figura de χ. Sea G el grupo de las simetrías del plano **P**. Para cada H subgrupo de G sea $H(\chi)$ el subgrupo de los elementos h en H tales que para cada casilla c el conjunto $h(c)$ sea una casilla de χ. Notemos que el grupo $G(\chi)$ es el grupo de simetrías de χ.

Sea T un subgrupo de $\mathbf{T}G(\chi)$. Entonces T es un grupo abeliano cuyo rango es 0, 1, ó 2, actuando de manera propiamente discontínua en **P**, correspondiendo **P** módulo T a un plano, a un cilindro, ó a un toro, respectivamente. Además vemos que **P** módulo T está provisto de un mosaico (i.e. el inducido por χ) que denotamos χ_T . Sea $G(\chi_T)$ el grupo de las simetrías de χ_T , que vemos naturalmente incluido en $G(\chi)$.

1.2. Vemos que para cada $T' \leq T \leq \mathbf{T}G(\chi)$ hay un triángulo conmutativo de proyecciones naturales

$$\begin{tikzcd}
\chi_{T'} \arrow[dr] \arrow[dd] & \\
& \chi_T \arrow[dl] \\
\chi_{\mathbf{T}G(\chi)} &
\end{tikzcd}$$

Notemos que podemos ver el conjunto de los mosaicos χ_T , con $T \leq \mathbf{T}G(\chi)$, como objetos de una categoría C en la que , si $T' \leq T \leq \mathbf{T}G(\chi)$, hacemos $C(\chi_{T'}, \chi_T) := \{\pi\}$, donde π es la proyección natural de $\chi_{T'}$ a $\chi_{T'}$, y $C(\chi_T , \chi_{T'})$ es el conjunto de las funciones z que van del conjunto de las casillas de χ_T al conjunto de las casillas de $\chi_{T'}$ tales que $\pi z = 1$, donde 1 es la identidad en χ_T; nos referiremos a $C(\chi_T , \chi_{T'})$ como el conjunto de las *secciones* de la proyección π. No volveremos a tocar la Teoría de las Categorias, salvo en la siguiente

Observación El mosaico χ es un objeto universalmente repelente en C.

1.3. Identifiquemos a $\mathbf{T}G(\chi)$ con el grupo abeliano subyacente a la $\mathbf{Z}$-álgebra de los enteros gaussianos $A := \mathbf{Z}[\, i \,]$ extendiendo

$$\textit{desplazar cada casilla una casilla a la derecha} \longmapsto 1,$$

$$\textit{desplazar cada casilla una casilla hacia arriba} \longmapsto i,$$

a un (único) isomorfismo de grupos. Vemos que esto induce una identificación de $\mathbf{T}G(\chi_T)$ con el grupo A/T.

Formemos el espacio punteado (χ_T, c), donde c es una casilla de χ_T. Para cada e existe un v en $\mathbf{T}G(\chi)$ tal que $e = v + c$. Tal v es único módulo T'. A través de la identificación de arriba podemos dotar al mosaico punteado (χ_T, c) de coordenadas en el Z-módulo cociente A/T'.

1.4. El grupo de las simetrías de (χ_T, c), que denotamos $G(\chi_T, c)$, es por definición el conjunto de los elementos g en $G(\chi_{T'})$ tales que $gc = c$. Podemos ver a $G(\chi, c)$ como el grupos de las simetrías de la casilla c. Consecuentemente $G(\chi, c)$ es (en un sentido geométrico) canónicamente isomorfo al grupo diédrico D_4. En coordenadas podemos ver a D_4 generado por los siguientes 2 Z-automorfismos de A:

$$a + bi \longmapsto a - bi,$$

$$a + bi \longmapsto b + ai,$$

que denotamos κ y λ, respectivamente. El grupo $R := \langle r \rangle$, donde $r := \lambda\kappa$, es llamado el grupo de las *rotaciones* del mosaico punteado (χ, c). Notemos que la función que asocia a cada u en el grupo multiplicativo de las unidades del anillo A el automorfismo Z-lineal de A dado por

$$w \longmapsto uw,$$

se restringe a un isomorfismo sobre R. Vemos además que bajo este isomorfismo i corresponde al generador r.

1.5. La inclusión natural de $G(\chi_T)$ en $G(\chi)$ se restringe a una inclusión natural de $G(\chi_T, c_T)$ en $G(\chi, c)$. Un *tablero* es un mosaico χ_T tal que $G(\chi_T, c_T) = G(\chi, c)$, para alguna casilla c de χ. Un *tablero punteado* es un mosaico punteado (χ_T, c_T) en el cual χ_T es un tablero para alguna casilla c de χ.

Observación Si el mosaico punteado (χ_T, c_T), con c casilla de χ, se ve en coordenadas como $A/\alpha A$, con $\alpha \in A$, entonces $\chi_\alpha := \chi_T$ es un tablero.

Proposición Si el mosaico χ_T es un tablero entonces $\chi_\alpha = \chi_T$, para algún $\alpha \in A$ definido de manera única módulo R.

Demostración
En particular tenemos que $iT = T$. Pero $ZT = T$, entonces $AT = T$, es decir, T es un ideal de A. Recordando que A es un dominio de ideales principales, vemos que existe $\alpha \in A$, definido de manera única salvo unidades, tal que $\alpha A = T$. Entonces podemos concluir que (χ_T, c) se ve en coordenadas como $A/\alpha A$, para $\alpha \in A$ definido de manera única módulo R.

Decimos que el tablero χ_α es *real* si el ideal αA puede ser generado por un elemento en Z.

1.6. Sea $m \in A$. Una *pieza* en χ_m es un subconjunto $p \subseteq \mathbf{T}G(\chi_m)\backslash\{0_m\}$, un *movimiento* de p es cualquier $v \in p$. Si $d\,|\,m$ entonces la proyección de la pieza p al tablero χ_d es el conjunto $\pi(p)\backslash\{0_d\}$, donde π es la proyección de χ_m a χ_d ; si q es una pieza en χ denotamos q_m la proyección de q en el tablero χ_m. Decimos que una pieza p es *cíclica* si $p = Zv\backslash\{0_m\}$, con $v \in \mathbf{T}G(\chi_m)$; decimos que p es una *estrella* si

$$p = \Big(\bigcup_{v \in S} Zv\Big)\backslash 0_m,$$

para algún $S \subseteq \mathbf{T}G(\chi_m)$; en caso de que para cada $v \in S$ se tenga que $|Zv| = |m|$ entonces decimos que la estrella es brillante. Definiendo en términos de las coordenadas usuales las siguientes piezas en χ:

$$torre := (Zi \cup Z)\backslash\{0\},$$

$$alfil := (Z(1+i) \cup Z(1-i))\backslash\{0\},$$

$$dama := torre \cup alfil,$$

Observación Para cada $m \in \mathbf{N}$ tenemos que la $torre_m$, el $alfil_m$, y la $dama_m$ son estrellas brillantes.

1.7. Una posición en χ_m es una función f del conjunto del las casillas de χ_m al conjunto potencia $P(\mathbf{T}G(\chi_m)\backslash\{0_m\})$. Decimos que la casilla c de χ_m es una *colocación* de la pieza p en la posición f si $f(c) = p$. Supongamos que tenemos colocaciones de piezas p y q en las casillas c y e, respectivamente. Decimos que la colocación c de p *ataca* a una colocación e de q si $v + c = e$, para algún movimiento v de p. Decimos que la posición f es *p-pacífica* si no hay colocación c de la pieza p en la posición f que ataque a una colocación de una pieza no vacía.

1.8. *Desde este momento hasta el final de esta tesis nos restringiremos al caso de las posiciones f en las que, a lo más, hay una colocación de una pieza no vacía.* Identifiquemos pues cada posición f con el conjunto de las casillas c de χ_m tales que $f(c) \neq \emptyset$. Definimos la *proyección* de una posición **C** del tablero χ_m al tablero χ_d , es la posición $\pi(\mathbf{C})$ en χ_d , donde π es la proyección de χ_m a χ_d. Una *sección* de una posición **C** del tablero χ_d al tablero χ_m es la posición $z(\mathbf{C})$, donde z es una sección de la proyección π.

Observación Sea p una estrella brillante de un tablero real χ_m . Si **C** es una posición p-pacífica en el tablero χ_m entonces $|\mathbf{C}| \leq m$.

Decimos que la posición **C** del tablero χ_m es una *solución al problema de la pieza p en el tablero χ_m* si **C** es p-pacífica y $|\mathbf{C}| = m$.

2. El teorema de Euler-Hurwitz y la existencia de soluciones al problema de las damas.

2.1. Sea m un entero positivo. Sea **C** una solución al problema de las **torres** en χ_m. Notemos que podemos ver a (χ_m, c) en coordenadas como $Z_m \times Z_m$. Entonces la solución **C** puede verse como la gráfica de una función τ del primer factor al segundo factor del producto $Z_m \times Z_m$.

Proposición La posición **C** es una solución al problema de las damas en χ_m si y sólo si las ecuaciones

$$x - y = \tau(x) - \tau(y),$$

$$x - y = \tau(y) - \tau(x),$$

con $x, y \in \boldsymbol{Z}_m$ sólo se satisfacen trivialmente (i.e. $x - y = 0_m$).

Demostración

La posición **C** no es solución al problema de las damas si y sólo si existen c, e en **C** tales que $v = c - e$, con $v \in alfil_m$. En coordenadas $c = (x, \tau(x))$, $e = (y, \tau(y))$, y $v = (l, (+/-)l)$ esto se traduce a

$$(l, +/-l) = (x, \tau(x)) - (y, \tau(y)),$$

con $l \in \boldsymbol{Z}_m$ no nulo. Esto equivale a que la ecuación

$$x - y = (+/-)(\tau(y) - \tau(x)),$$

tiene una solución no trivial.

El hecho de que las ecuaciones de la proposición de arriba no tengan una solución no trivial equivale a que cada una de las ecuaciones

$$x - \tau(x) = y - \tau(y),$$

$$x + \tau(x) = y + \tau(y),$$

implique $x = y$. En otras palabras, tenemos el siguiente

Corolario La posición **C** es una solución al problema de las damas en χ_m si y sólo si el conjunto

$$\{x - \tau(x) \mid x \in \boldsymbol{Z}_m\}$$

y el conjunto

$$\{x + \tau(x) \mid x \in \boldsymbol{Z}_m\}$$

tienen cardinalidad m.

Teorema(Euler) Si **C** es solución al problema de las damas en χ_m entonces 2 no divide a m.

Demostración

Si suponemos que $2 \mid m$ tendríamos que $\Sigma x = (m/2)_m$, y consecuentemente llegaríamos a que

$$(m/2)_m = \Sigma(x + \tau(x)) = \Sigma x + \Sigma\tau(x) = (m/2)_m + (m/2)_m = 0_m,$$

que es un absurdo. Así concluimos que 2 no divide a m.

Teorema(Hurwitz) Si **C** es solución al problema de las damas en χ_m entonces 3 no divide a m.

Demostración

1. Consideremos que

$$\Sigma(x - \tau(x))^2 = \Sigma x^2$$

$$\Sigma(x^2 - 2\tau(x)x + \tau(x)^2) = \Sigma x^2$$

$$\Sigma x^2 - 2\Sigma\tau(x)x + \Sigma\tau(x)^2 = \Sigma x^2$$

$$\Sigma x^2 = 2\Sigma\tau(x)x \ ,$$

pero

$$\Sigma(x - \tau(x))^2 = \Sigma(x + \tau(x))^2 \ ,$$

$$\Sigma(x^2 - 2\tau(x)x + \tau(x)^2) = \Sigma(x^2 + 2\tau(x)x + \tau(x)^2) \ ,$$

$$\Sigma x^2 - 2\Sigma\tau(x)x + \Sigma\tau(x)^2 = \Sigma x^2 + 2\Sigma\tau(x)x + \Sigma\tau(x)^2 ,$$

$$4\Sigma\tau(x)x = 0_m,$$

entonces

$$2\Sigma x^2 = 0_m,$$

pero

$$1^2 + 2^2 + 3^2 + \ldots + m^2 = m(m+1)(2m+1)/6,$$

entonces

$$(m+1)_3(2m+1)_3 = 0_3 .$$

Si suponemos que $3 \mid m$ tendríamos que $m_3 = 0_3$ y consecuentemente

$$(m_3 + 1_3)(2_3 m_3 + 1_3) = 0_3 ,$$

$$(0_3 + 1_3)(2_3 0_3 + 1_3) = 0_3 ,$$

y llegaríamos a que $1_3 = 0_3$, que es un absurdo. Así concluimos que 3 no divide a m.

2.2. Consideremos el tablero punteado $(\boldsymbol{\chi}_m, c)$. Decimos que una posición es *cíclica* si $\mathbf{C} = \boldsymbol{Z}v$, para algún $v \in \mathbf{T}G(\boldsymbol{\chi}_m)$.

Supongamos que $\mathbf{C}$ una solución cíclica al problema de las torres en $(\boldsymbol{\chi}_m, c)$. Entonces la permutación asociada a $\mathbf{C}$ es de la forma $\tau(x) = kx$, con $k \in \boldsymbol{Z}_m$. Además tenemos la siguiente

Proposición La posición cíclica $\mathbf{C}$ dada por $\tau(x) = kx$ es una solución al problema de las damas en $\boldsymbol{\chi}_m$ si y sólo si tanto $1 + k$ como $1 - k$ son elementos invertibles en el anillo $\boldsymbol{Z}_m$.

Demostración

Notemos que $1 +/- k$ es unidad en $\boldsymbol{Z}_m$ si y sólo si $x \longmapsto (1 +/- k)x$ es una biyección, que es lo mismo que decir que el conjunto $\{x +/- kx \mid x \in \boldsymbol{Z}_m\}$ tenga cardinalidad m. Dado el corolario a la proposición en (2.1) esto equivale a decir que **C** sea solución al problema de las damas en χ_m.

Supongamos que ni 2 ni 3 divide a m. Vemos que para el caso en que $k := 2_m$ la solución cíclica es una solución al problema de las damas en χ_m ya que tanto $(1 + 2)_m$ como $(1 - 2)_m$ son unidades en χ_m. Así llegamos al recíproco del teorema de Euler-Hurwitz en el siguiente

Corolario Si ni 2 ni 3 dividen a m entonces existe una solución al problema de las damas en χ_m.

Sin embargo no todas las soluciones al problema de las damas son cíclicas como podemos verlo en la siguiente

Proposición La permutación τ en el conjunto $\boldsymbol{Z}_{13}$ dada por

$$\begin{gathered}
\tau(13_{13}) = 13_{13},\\
\tau(1_{13}) = 6_{13},\\
\tau(2_{13}) = 10_{13},\\
\tau(3_{13}) = 2_{13},\\
\tau(4_{13}) = 7_{13},\\
\tau(5_{13}) = 12_{13},\\
\tau(6_{13}) = 4_{13},\\
\tau(7_{13}) = 19_{13},\\
\tau(8_{13}) = 1_{13},\\
\\
\tau(9_{13}) = 5_{13},\\
\tau(10_{13}) = 11_{13},\\
\tau(11_{13}) = 8_{13},\\
\tau(12_{13}) = 3_{13},
\end{gathered}$$

representa una solución no-cíclica al problema de las damas en χ_m .

Demostración
Para ver que τ representa una solución al problema de las damas en χ_m basta checar que los miembros izquierdos de cada una de las siguientes columnas sean distintos dos a dos:

$$\begin{array}{rr}
13_{13}+13_{13}=13_{13}, & 13_{13}-13_{13}=13_{13},\\
1_{13}+6_{13}=7_{13}, & 1_{13}-6_{13}=8_{13},\\
2_{13}+10_{13}=12_{13}, & 2_{13}-10_{13}=5_{13},\\
3_{13}+2_{13}=5_{13}, & 3_{13}-2_{13}=1_{13},\\
4_{13}+7_{13}=11_{13}, & 4_{13}-7_{13}=10_{13},\\
5_{13}+12_{13}=4_{13}, & 5_{13}-12_{13}=6_{13},\\
6_{13}+4_{13}=10_{13}, & 6_{13}-4_{13}=2_{13},\\
7_{13}+9_{13}=3_{13}, & 7_{13}-9_{13}=11_{13},\\
8_{13}+1_{13}=9_{13}, & 8_{13}-1_{13}=7_{13},\\
9_{13}+5_{13}=1_{13}, & 9_{13}-5_{13}=4_{13},\\
10_{13}+11_{13}=8_{13}, & 10_{13}-10_{13}=12_{13},\\
11_{13}+8_{13}=6_{13}, & 11_{13}-8_{13}=3_{13},\\
12_{13}+3_{13}=2_{13}, & 12_{13}-3_{13}=9_{13}.
\end{array}$$

Si suponemos que es cíclica, tendríamos que como Z_{13} es un campo, C corresponde al lugar geométrico de una línea cuya pendiente μ esta dada por $\mu = \sigma(x)/x$, para cualquier $x \in Z_m$ no nula, digamos $\mu = \sigma(1_{13}) = 6_{13}$. De esta manera tendríamos que $\sigma(2_{13}) = 12_{13}$, pero de la definición de σ vemos que $\sigma(2_{13}) = 10_{13}$, llegando así a una contradicción.

Observación Se puede ver por ensayo y error que la solución de la proposición de arriba, entre las soluciones no-cíclicas, tiene cardinalidad mínima.

3. El producto de Polya

3.1 Sean

$$z_1 : (\chi_m, c) \longrightarrow (\chi_{mn}, c').$$

$$z_2 : \chi_n \longrightarrow \chi_{mn}$$

secciones . El *producto de Polya* de z_1 con z_2 , que denotamos $z_1 \otimes z_2$, es la composición:

$$\chi_m \times \chi_n \xrightarrow{z_1 \times z_2} \chi_{mn} \times \chi_{mn} \xrightarrow{\lambda} \chi_{mn},$$

donde $z_1 \times z_2$ está definido por $(x, y) \mapsto (z_1(x), z_2(y))$, y λ está dado por

$$(x, y) \mapsto nx + y.$$

A cada pareja $(\mathbf{C}_1, \mathbf{C}_2)$, donde $\mathbf{C}_1$ es una posición en (χ_m, c) y $\mathbf{C}_2$ es una posición en χ_n, el *producto de Polya de* $\mathbf{C}_1$ *con* $\mathbf{C}_1$, *respecto a* (z_1, z_2), es la posición en χ_{mn} definida por:

$$\mathbf{C}_1 \otimes \mathbf{C}_2 := (z_1 \otimes z_1)(\mathbf{C}_1 \times \mathbf{C}_2) = nz_1(\mathbf{C}_1) + z_2(\mathbf{C}_2).$$

[Limitándonos a secciones z de (χ_k, c_k) a (χ, c) tales que en coordenadas
$$z_2(\chi_k) = \{1, \ldots, k\} \times \{1, \ldots, k\},$$
vemos que el producto de Polya corresponde así al producto de Kronecker de matrices.]

Observación Para cada $d \in nz_1(\mathbf{C}_1)$ tenemos que $d + z_2(\mathbf{C}_2)$ es una sección de $\mathbf{C}_2$.

Proposición El producto de Polya $\mathbf{C}_1 \otimes \mathbf{C}_2$ se descompone como unión ajena de secciones de C_2 de la siguiente manera

$$\dot{\mathbf{C}}_1 \otimes \mathbf{C}_2 = \bigcup_{d \in n\, z_1(\mathbf{C}_1)} (d + z_2(\mathbf{C}_2))$$

Demostración

Supongamos que existen $d', d'' \in nz_1(\mathbf{C}_1)$, diferentes, tales que

$$(d' + z_2(\mathbf{C}_2)) \cap (d'' + z_2(\mathbf{C}_2)) \neq \emptyset.$$

Entonces existirían $c, c' \in \mathbf{C}_2$ tales que

$$z_2(c) + d = z_2(c'),$$

donde $d := d' - d''$. Entonces, si π denota la proyección de χ_{mn} a χ_n, tendríamos que

$$\pi(z_2(c) + d) = \pi(z_2(c')),$$

$$\pi z_2(c) + \pi(d) = \pi(z_2(c')),$$

$$c + \pi(d) = c',$$

pero $d \in n\,\mathbf{T}G(\chi_{mn})$, entonces

$$c + 0_n = c',$$

$$c = c',$$

$$z_2(c) = z_2(c').$$

concluyéndose así que $d' = d''$, que es absurdo. Entonces los uniendos son ajenos dos a dos.

Corolario Tenemos la identidad

$$|\mathbf{C}_1 \otimes \mathbf{C}_2| = |\mathbf{C}_1|\,|\mathbf{C}_2|.$$

Demostración

Claramente para cada $d \in n\, z_1(\mathbf{C}_1)$ tenemos que

$$|\mathbf{C}| = |z_2(\mathbf{C}_2)| = |d + z_2(\mathbf{C}_2)|.$$

Entonces basta demostrar que

$$|nz_1(\mathbf{C}_1)| = |z_1(\mathbf{C}_1)|.$$

Para este fin, si consideramos $z_1(c')$, $z_1(c'') \in z_1(\mathbf{C}_1)$, con c', $c'' \in \mathbf{C}_1$ tales que $c := z_1(c') - z_1(c'') \neq 0_{mn}$, basta que demostremos que $nc \neq 0_{mn}$. Si fuera cierto que $nc = \mathbf{0}_{mn}$ tendríamos que

$$nc \in mn\mathbf{T}G(\chi),$$

entonces

$$c \in m\mathbf{T}G(\chi),$$

Si π es la proyección de χ_{mn} a χ_m entonces

$$0_m = \pi(c) = \pi(z_1(c') - z_1(c'')) = \pi z_1(c') - \pi z_1(c'') = c' - c''$$

entonces

$$c' = c'',$$

$$z_1(c') = z_1(c''),$$

y concluiríamos que $c = 0_m$, que es absurdo.

3.2 Sea p una pieza en χ.

Lema Sea z una sección de χ_m a χ_{mn}. Si $\mathbf{C}$ es una posición p_m–pacífica en χ_m entonces $z(\mathbf{C})$ es una posición p_{mn}–pacífica en χ_{mn}.

Demostración

Supongamos que $z(\mathbf{C})$ no es p_{mn}–pacífica. Entonces existen $z(c)$, $z(c') \in z(\mathbf{C})$, con c, $c' \in \mathbf{C}$ tales que

$$v + z(c) = z(c'),$$

para algún $v \in p_{mn}$. Sea π la proyección de χ_{mn} a χ_m.

Entonces

$$\pi(v + z(c)) = z(c'),$$

$$\pi(v) + \pi z(c) = \pi z(c'),$$

$$\pi(v) + c = c'$$

Como $\pi(v) \notin p_m$ ($\mathbf{C}$ es por hipótesis p_m–pacífica) tendríamos que $\pi(v) \in 0_m$, que implica que

$$c = c',$$

$$z(c) = z(c'),,$$

y concluiríamos así que $v \notin p_{mn}$, que es absurdo. Entonces $z(c)$ es p_{mn}–pacífica.

Decimos que la pieza p_{mn} tiene la *propiedad de Polya*, que denotamos $\mathbf{P}_n$, si para cada $v \in \mathbf{T}G(\chi_{mn})$ se tiene que $nv \in p_{mn}$ implica $v \in p_{mn}$. Así llegamos al siguiente

Lema Si la pieza p_{mn} tiene la propiedad $\mathbf{P}_n$, entonces $nz(\mathbf{C})$ es p_{mn}–pacífica.

Teorema Supongamos que la pieza p_{mn} tiene la propiedad $\mathbf{P}_n$. Entonces, si $\mathbf{C}_1$ es p_m–pacífica y $\mathbf{C}_2$ es p_n–pacífica entonces $\mathbf{C}_1 \otimes \mathbf{C}_2$ es p_{mn}–pacífica.

Demostración
Supongamos que $\mathbf{C}_1 \otimes \mathbf{C}_2$ no es p_{mn}–pacífica. Entonces habrían k y k' $\in \mathbf{C}_1 \otimes \mathbf{C}_2$ tales que $v := k - k' \in p_{mn}$. Entonces existen $d, d' \in nz_1(\mathbf{C}_1)$ tales que

$$k \in d + z_2(\mathbf{C}_2),$$

$$k' \in d' + z_2(\mathbf{C}_2).$$

En otras palabras $k = d + z_2(c)$ y $k' = d' + z_2(c')$, con $c, c' \in \mathbf{C}_2$. Entonces

$$* \qquad v = d - d' + z_2(c) - z_2(c').$$

Si π es la proyección de χ_{mn} a χ_n entonces

$$\pi(v) = \pi(d - d') + \pi z_2(c) - \pi z_2(c').$$

Viendo que $d - d' \in n\mathbf{T}G(\chi_{mn})$ y simplificando, obtenemos

$$\pi(v) = c - c'.$$

Como por hipótesis $\mathbf{C}_1$ es una posición p_m–pacífica, necesariamente $c = c'$. De manera que la ecuación (*) se reduce a

$$v = d - d',$$

que significa que $nz_1(\mathbf{C}_1)$ no es p_n–pacífica, lo cual a la luz del lema anterior, es un absurdo. Así concluímos que $\mathbf{C}_1 \otimes \mathbf{C}_2$ es p_{mn}–pacífica.

Proposición Si p_{mn} es brillante entonces tiene la propiedad $\mathbf{P}_n$.

Demostración
Sea $w \in \mathbf{T}G(\chi_{mn})$ y supongamos que $nw \in p_{mn}$. Entonces existe $v \in S$ tal que $nw \in \mathbf{Z}v$. El hecho de que $\mathbf{T}G(\chi_{mn})$ sea un Z_{mn}-módulo libre implica que $\mathbf{Z}v$ es maximal en la familia de las Z_{mn}-módulos cíclicos. Así concluimos que $w \in \mathbf{Z}v$.

Teorema Si $\mathbf{C}_1$ es una solución al problema de las damas en χ_m y $\mathbf{C}_2$ es una solución al problema de las damas en χ_n, entonces $\mathbf{C}_1 \otimes \mathbf{C}_2$ es solución al problema de las damas en χ_{mn}.

Demostración
Se sigue del corolario en (3.1) que la cardinalidad de $\mathbf{C}_1 \otimes \mathbf{C}_2$ es la requerida. Por otro lado, el hecho de que $\mathbf{C}_1 \otimes \mathbf{C}_2$ sea $dama_{mn}$-pacífica se desprende del teorema en (3.2), y la proposición de arriba, al observar que la dama es una estrella brillante.

4. Conexión con la aritmética de la forma cuadrática $x^2 + y^2$

4.1 Sea **C** una solución al problema de las m damas en (χ_m, c), es decir una solución para el tablero χ_m tal que $c \in \mathbf{C}$. El grupo de las simetrías de **C**, que denotamos $G(\mathbf{C})$, es el conjunto de los elementos $g \in G(\chi_m, c)$ tales que $g\mathbf{C} = \mathbf{C}$.

Proposición Para el caso $m = 1$ tenemos $G(\mathbf{C}) = D_4$, en los demas casos $G(\mathbf{C}) \subseteq R$.

Demostración
Basta con que demostremos que **C** no es ni κ-invariante ni λ-invariante. Como $m > 1$ hay una dama colocada en una casilla $x + yi_m := c \neq 0_m$. Si **C** fuera κ-invariante tendríamos que $d := x - yi_m \in \mathbf{C}$. Veamos que $d - c = 2x$ y notemos que $2x \neq 0_m$ (El teorema de Euler implica que 2 no divide a m, entonces suponer $2x = 0_m$ conduciría a que $x = 0_m$ y así concluiríamos que $c = y$ atacaría a la dama colocada en 0_m), de manera que $d - c$ es un movimiento de torre, contradiciendo el hecho de que **C** sea solución. Consecuentemente **C** no es κ-invariante. Si **C** fuera λ- simétrica tendríamos que $d: = y + xi \in \mathbf{C}$. Veamos que $c - d = x - y + (y - x)i \neq 0_m$ (suponer que $c - d = 0_m$ nos conduce a $x = y$, $x + y = 0_m$, y obtendríamos $2x = 0_m$, $2y = 0_m$ y, por el teorema de Euler, concluiríamos que $x = 0$, $y = 0$), de manera que $c - d$ es un movimiento de alfil, contradiciendo el hecho de que **C** sea solución. Consecuentemente **C** tampoco es λ-simétrica.

Corolario Si **C** tiene la propiedad adicional de ser cíclica entonces la única simetría no trivial de **C** es la $\boldsymbol{R}$-invariancia.

Teorema Supongamos que **C** es cíclica y R-invariante. Entonces existe ρ en A, determinado de manera única módulo $\boldsymbol{R}$, que satisface las siguientes 2 propiedades:

I. Si $\rho = a + bi$, con a, b en $\boldsymbol{Z}$, entonces $a^2 + b^2 = m$,

II. $\boldsymbol{Z}\,\rho_m = \mathbf{C}$.

Demostración

Veamos que $\boldsymbol{Z}_m\mathbf{C} = \mathbf{C}$ y que $i_m\mathbf{C} = \mathbf{C}$, entonces $\boldsymbol{Z}_m[i_m]\mathbf{C} = \mathbf{C}$, pero $\boldsymbol{Z}_m[i_m] = A/mA$, entonces **C** es ideal de A/mA. Por uno de los teoremas de isomorfismo de Noether llegamos a que $\pi^{-1}(\mathbf{C})$ es un ideal de A. Pero A es un dominio de ideales principales (ver el apéndice 1), entonces existe ρ en $\pi^{-1}(\mathbf{C})$ tal que $\rho A = \pi^{-1}(\mathbf{C})$. Sea $\rho = a + bi$, con a, b en **Z**. Recordemos que la norma N de la $\boldsymbol{Z}$-álgebra A tiene la propiedad

$$a^2 + b^2 = N(\,a + bi) \;=\; |A/\rho A|$$

Por otro lado recordemos que hay un isomorfismo canónico de $\boldsymbol{Z}$-módulos entre $A/\rho A$ y $(A/mA)\,/\,\mathbf{C}$, y además tenemos que

$$|(A/mA)\,/\,\mathbf{C}| = |(A/mA)| \;/\; |\mathbf{C}| = m^2/m = m.$$

Consecuentemente

$$a^2 + b^2 = m,$$

demostrando así que ρ satisface la propiedad (**I**). Por otro lado notemos que como $\boldsymbol{Z}+\boldsymbol{Z}i = A$ entonces $\boldsymbol{Z}\rho+\boldsymbol{Z}\rho i = \rho A$, así es que $\boldsymbol{Z}\rho_m+\boldsymbol{Z}\rho_m i_m = \mathbf{C}$. Como i es una unidad en A tenemos que i_m es unidad en A/mA, así es que ρ_m tiene el mismo orden que $\rho_m i_m$. Como **C** es cíclico esto implica que $\boldsymbol{Z}\rho_m = \boldsymbol{Z}\rho_m i_m$, entonces concluimos que $\boldsymbol{Z}\rho_m = \mathbf{C}$, demostrando así que ρ satisface la propiedad (**II**). Finalmente, si suponemos que existe otro ρ' que satisface la propiedad (**I**), tendríamos que $A/\rho' A = m$. Entonces el epimorfismo canónico de $A/\rho' A$ sobre $A/\rho A$ es un isomorfismo, es decir, $\rho' A = \rho A$. Entoinces existe u en A invertible tal que $\rho' = u\rho$. Así concluímos que ρ' y ρ están en la misma clase módulo $\boldsymbol{R}$.

Teorema Para cada ρ en A que satisface (**I**) y (**II**) tenemos que $\mathbf{C} := \mathbf{Z}\rho_m$ es $\boldsymbol{R}$-simétrica.

Demostración
Escribamos $\rho = a + bi$, con a, b en **Z**. Notemos que como **C** es en particular solución al problema de las torres en (χ_m, o) tenemos que a_m y b_m son unidades en **Z**/m**Z**. Entonces $r := a_m (b_m)^{-1}$ está bien definido. Veamos que

$$r\,\rho_m = r^2 b_m + a_m i_m,$$

pero vemos que $r^2 = -1_m$. Entonces

$$r\,\rho_m = i_m \rho_m,$$

que, como **C** es cíclica, nos permite concluir que $i_m\rho_m$ pertenece a $\boldsymbol{Z}\rho_m$, es decir **C** es ***R***-simétrica.

Apéndice 1: El anillo de los enteros gaussianos.

1. Dada una extensión finita de campos E/F, la *norma* de la extensión E/F es una función de E a F, que denotamos $N_{E/F}$, definida para cada $\alpha \in A$ como el determinante de la transformación F-lineal

$$\alpha : E \longrightarrow E,\ x \longmapsto \alpha x\,.$$

Teorema Sea ι el grado de inseparabilidad de la extensión E/F. Sea $\{\sigma_1\ , \ .\ .\ .\ ,\sigma_n\}$ el conjunto de todos los morfismos de campos (i.e. encajes) de F a E. Tenemos la fórmula

$$N_{E/F}(\alpha) = (\sigma_1 \cdot \ .\ .\ .\ \cdot \sigma_n)^{\iota}.$$

Demostración

Primero se demuestra para el caso en que $E = F(\alpha)$, considerando que la matríz de α relativa a la base $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$, donde d es el grado del polinomio mínimo de α sobre F, es una matriz 'compañera'. El caso general se obtiene factorizando E/F a través de $F(\alpha)$.

Denotando $K^{\times}$ al grupo multiplictivo de sus elementos invertibles de K, vemos que para cada inclusión $E \supseteq F$, tal que E/F sea finita, la norma $N_{E/F}$ restringida de $E^{\times}$ a $F^{\times}$ es un morfismo de grupos. Tenemos a un paso tenemos el siguiente

Corolario Sea K la categoria en la que los objetos son todos los campos, y donde los morfismos son las inclusiones $E \supseteq F$ tales que E/F es finita. Se puede demostrar que el asignar a cada campo K el grupo $K^{\times}$, y a cada inclusión $E \supseteq F$ tal que E/F es finita, el morfismo de grupos $N_{E/F}$, es un functor, que denotamos N, de K a la categoria de los grupos.

2. Un anillo *euclidiano* es una pareja (A, d), donde A es un dominio entero y d es una función que va de $A^{\times}$ a los enteros, que satisface los siguientes dos axiomas:

a. Para cada a, b en $A^{\times}$ se tiene $d(a) \leq d(ab)$.

b. Para cada a, b en $A^{\times}$ existen t, r en A tales que $a = tb + r$, donde $r = 0$ ó $d(r) < d(b)$.

Proposición Un anillo euclideano (A, d) es un anillo de ideales principales.

Demostración

Sea I un ideal de A. Sin pérdida de generalidad podemos suponer que $I \neq \{0\}$. Así es que existe $g \in I$ con $d(g)$ mínimo. Escribamos cada $x \in I$ en la forma $x = tg + r$, con t , $r \in A$ tales que $d(r) < d(g)$ ó $r = 0$. Notemos que $tg \in I$, consecuentemente $r \in I$. Necesariamente $r = 0$ ya que g tiene la propiedad de minimizar d en I. Así concluimos que $x \in gA$.

3. El *anillo de los enteros gaussianos* el la Z-álgebra A que se obtiene al adjuntar al anillo de los enteros Z el número complejo i. La norma $N_{C/R}$, del campo de los números complejos C al campo de los números reales R, se restringe a un morfismo de monoides de $A^{\times}$ a Z, que denotamos por simplicidad N, y lo llamamos la *norma* de los enteros gaussianos. Notemos que para cada $\alpha \in A$ tenemos que $N(\alpha) = \alpha\sigma(\alpha)$, donde σ es la conocida conjugación compleja $a + bi \longmapsto a - bi$.

Teorema La pareja (A, N) es un anillo euclideano.

Demostración

Claramente sólo falta demostrar que N satisface la propiedad (b). Necesitaremos un

Lema Sea n entero positivo, sea $y \in A$. Entonces existen t, $r \in A$ tales que $y = tn + r$, con $d(r) < d(n)$ ó $r = 0$.

Demostración del lema

Escribamos $y = a + bi$. Recordando que Z es un anillo euclideano, vemos que existen enteros u, u' tales que

$$a = un + u',$$

con $2|u'| \leq |n|$. Análogamente, existen enteros v, v' tales que

$$b = vn + v',$$

con $2|v'| \leq |n|$. Haciendo $t := u + vi$, $r := u' + v'i$, primero vemos que $y = tn + r$, y luego vemos que, como

$$N(r) = u'^2 + v'^2 \leq n^2/4 + n^2/4 < n^2 = N(n),$$

podemos concluir que $\boldsymbol{d}(r) < \boldsymbol{d}(n)$ ó $r = 0$, quedando demostrado así el lema.

Sea $y \in A$ y sea $x \in A^{\times}$. Aplicando el lema para el entero positivo $N(x)$ y el gaussiano $y\sigma(x)$, vemos que hay $t, r \in A$ tales que $y\sigma(x) = tn + r$, con $\boldsymbol{d}(r) < \boldsymbol{d}(n)$ ó $r = 0$. Entonces tenemos que

$$N(y - tx)N(\sigma(x)) < N(x)N(\sigma(x)),$$

entonces

$$y = tx - r',$$

con $r' := y - tx$ tal que $r' = 0$ ó $N(r') = N(y - tx) < N(x)$, quedando así demostrado el teorema.

Apéndice 2: Sobre las soluciones "doblemente periódicas" del problema de las n-damas.

por G. Pólya en Zurich.

1. Se supone que el tablero de n^2 casillas tiene un sistema de coordenadas rectangular en el cuadrante positivo, que las orillas [del tablero] son paralelas a los ejes coordenados. y los puntos medios de todas las casillas tienen coordenadas con números enteros lo más pequeños posible. En este arreglo de los números enteros de todas las coordenadas de los puntos medios, se tiene que el lugar de la casilla del tablero cuadrático funciona, ya sea como una unidad propia de longitud, o es un componente múltiple de éste, así las coordenadas de todos los puntos medios de las casillas deben ser números enteros lo más pequeños posibles, para que sólo ocurra lo primero. Bajo estas condiciones los siguientes bordes del tablero, de sus ejes de coordenadas paralelos tienen el intervalo 1/2 y cuando conocemos como x y y las coordenas del punto medio de cualquier casilla del tablero, entonces son constantes estos números de la hilera 1, 2, 3, . . . , n. El problema de las n-damas requiere ahora la solución de n-casillas similares a éste, cuyas coordenadas del punto medio:

$$(x_1, y_1), \ (x_2, y_2), \ (x_3, y_3), \ \ldots, \ (x_n, y_n),$$

satisfacen las siguientes 2n(n-1) desigualdades:

$$(1) \quad x_k \neq x_l \ , \ y_k \neq y_l \ , \ x_k - x_l \neq y_k - y_l \ , \ x_k - x_l \neq -(y_k - y_l),$$

para $k \neq l$.

Ahora defino una solución "doblemente periódica", cuando no solamente estas desigualdades (1), sino también las muchas otras incongruencias mod. n:

$$(2)\quad x_k \equiv x_l\ ,\ y_k \equiv y_l\ ,\ x_k - x_l \equiv y_k - y_l\ ,\ x_k - x_l \equiv -(y_k - y_l),$$

son satisfechas.

Tales soluciones tienen también un significado geométrico singular [2]: se piensa no solamente en el dominio de nuestro tablero, sino también en el plano completo con una red del campo cuadrático, cubierto por la misma cantidad y se piensa además que la misma solución propuesta se repite periódicamente en ambas direcciones, es decir, se piensa que así como con una casilla (x_k , y_k), también están ocupados con damas todas aquellas casillas, (x'_k , y'_k) para los que:

$$x'_k \equiv x_k\ ,\ y'_k \equiv y_k \quad (\text{mod } n)$$

son satisfechas. El "tablero infinito" cubierto con figuras de este modo tiene entonces, como consecuencia de las incongruencias (2), la siguiente propiedad: si en cualquier dirección se separa del tablero infinito un tablero cuadrático infinito de n^2 campos, los bordes paralelos a los ejes de las coordenas, entonces se encuentran exactamente n damas en el tablero separado, las cuales no pueden atacar en lados opuestos y así representan una solución del problema de las n-damas.

Según esto, la expresión "doblemente periódica" no necesita otra explicación. En consideración de este significado de nuestro tipo particular de solución, no se comprenden con ventaja, bajo $x_1 , \dots , x_k , \dots , x_n$, $y_1 , \dots , y_k , \dots , y_n$, números determinados sino sistemas de residuos mod. n. Correspondientemente, no siempre convierte el índice k en pares en los números 1, 2, 3, . . . ,n, sino que perimito que pase cualquier sistema completo de residuos mod. n, en el que encuentro la siguiente condición: cuando k'=k, tambien $x_{k'} \equiv x_k$, $y_{k'} \equiv y_k$ mod. n.

La consideración de la solución doblemente periódica mod. n, lleva hacia una interpretación muy clara y atrayente de muchos enunciados sencillos, pero importantes, de la Teoría de los Números. Yo creo que podría ser de utilidad para los estudiosos de matemáticas que lo requieran, hacer más clara la siguiente descomposición en un tablero o en un pizarrón cuadriculado, por medio de la exposición o el dibujo.

2. El contenido de la incongruencia (2) se puede explicar así: cada una de las cuatro hileras de números siguientes
(3)

$$x_1, \quad x_2, \quad x_3, \quad \ldots, x_n$$

$$y_1, \quad y_2, \quad y_3, \quad \ldots, y_n$$

$$x_1 + y_1, \; x_2 + y_2, \; x_3 + y_3, \; \ldots, x_n + y_n$$

$$x_1 - y_1, \; x_2 - y_2, \; x_3 - y_3, \; \ldots, x_n - y_n$$

pueden representar un sistema completo de residuos mod. n. De esta condición se puede deducir el enunciado:
Las soluciones doblemente periódicas del problema de las n damas existen si y sólo si n no es divisible ni entre 2 ni entre 3.

Primero demostraré lo siguiente:

Sea n par y que ambas hileras de números

$$x_1, x_2, x_3, \ldots, x_n,$$

$$y_1, y_2, y_3, \ldots, y_n,$$

representen sistemas completos de residuos mod. n, así los n números

(4) $x_1 + y_1, \; x_2 + y_2, \; x_3 + y_3, \; \ldots, x_n + y_n$

no pueden constituir un sistema completo de residuos mod. n.

En realidad se tiene

(5) $1 + 2 + 3 + 4 + \ldots + n = n(n + 1)/2 \equiv n/2 \pmod{n}$,

y por lo tanto, también:

$\Sigma x_k \equiv n/2$, $\Sigma y_k \equiv n/2$,

debe ser mod. n. Pero de ahí sigue

$\Sigma (x_k + y_k) \equiv 0$,

que si (5) no fuera posible, entones los números (4) constituirían un sistema completo de residuos mod. n.-- Esta demostración se debe a Euler [1].
Si n es divisible entre 3, entonces no pueden ser los cuatro sistemas (3), sistemas completos de residuo mod. n.
En realidad, se tiene

$1^2 + 2^2 + 3^2 + 4^2 + \ldots + n^2 = n(n + 1)(2n + 1)/6$,

y $2(1^2 + 2^2 + 3^2 + 4^2 + \ldots + n^2) \equiv n/3 \pmod{n}$.

Si los cuatro sistemas (3) fueran ahora sistemas de residuo completos, entonces tendrían lugar las siguientes congruencias:

$$2\Sigma\,(x_k + y_k) \equiv n/3\ ,\ 2\Sigma\,(x_k + y_k) \equiv n/3\ ,$$

$$4\Sigma\ x_k^2 \equiv 2n/3\ ,\ 4\Sigma\ y_k^2 \equiv 2n/3\ ,$$

Súmense las dos primeras congruencias y réstense ahí las dos últimas y así se demuestra claramente la insostenibilidad de la suposición; entonces se obtiene que:

$$0 = -2\ n/3 \quad (\text{mod. } n).$$

Agradezco esta demostración al Sr. Profesor Hurwitz [2].

Queda por demostrar que siempre existe, por otro lado, la solución doblemente periódica cuando "n" no es divisible ni entre 2 ni entre 3. En este caso se proporcionan siempre r números enteros, tales que los 3 números $r - 1$, r y $r + 1$, son primos relativos. Por ejemplo, se pueden tomar $r = 2$ ó $r = 3$. Se elije cualquier valor fijo a y se establece:

$$x_k = k, \quad y_k = a + kr,$$

entonces el sistema (3) de cuatro, toma la forma:

$$\begin{array}{ccccc} 1, & 2, & 3, & \ldots, & n \\ a + r, & a + 2r, & a + 3r, & \ldots, & a + nr \end{array}$$

$$a + (r+1), \quad a + 2(r+1), \quad a + 3(r+1), \quad \ldots, \quad a + n(r+1)$$

$$-a - (r-1), \quad -a - 2(r-1), -a - 3(r-1), \quad \ldots, -a - n(r-1),$$

Todos los sistemas de cuatro construyen así hileras aritméticas, cuyas diferencias, a saber 1, r, r + 1, –(r – 1) respectivamente, son divisibles por números diferentes a n. Será suficiente demostrar con dos hileras aproximadamente, que los n números mod. n comprendidos son incongruentes.

Si se tuviera

$$a + rk = a + rl \quad (\text{mod. } n)$$

se seguiría

$$r(k - l) = 0 \quad (\text{mod. } n)$$

$$k - l = 0 \quad (\text{mod. } n)$$

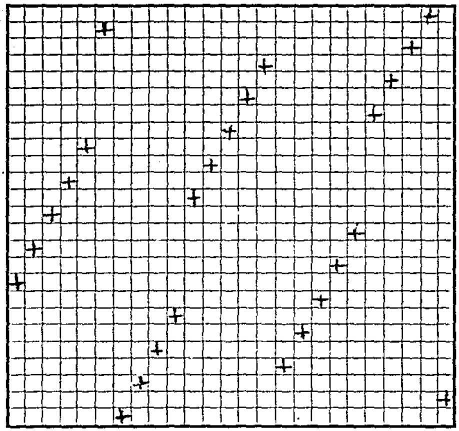

fig 1

En la hilera no hay dos miembros contiguos diferentes a + rk y a + rl, para cada $k \equiv l$. Estas soluciones doblemente periódicas ya han sido proporcionadas en el tomo I por Lucas [1].

3. Sería erróneo creer ahora quye todas las soluciones doblemente periódicas deben mostrar un arreglo similar sencillo de una hilera aritmética. La siguiente solución para n = 13 es un ejemplo:

$x = 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13$

$y = 1,\ 7,\ 11,\ 3,\ 8,\ 13,\ 5,\ 10,\ 2,\ 6,\ 12,\ 9,\ 4$

(mod. 13)

como es convincente a través de la construcción del sistema doblemente periódico (3), solamente que avace cada uno de los alores de las coordenadas por una hilera aritmética.

A continuación quisiera resaltar en particular que el 13 es número primo. Cuando n es un número compuesto (que no comparte divisores con 2 y 3), se puede dar un gran número de soluciones doblemente periódicas, las cuales no avanzan hacia hileras aritméticas sencillas, como ahora deseo explicar.

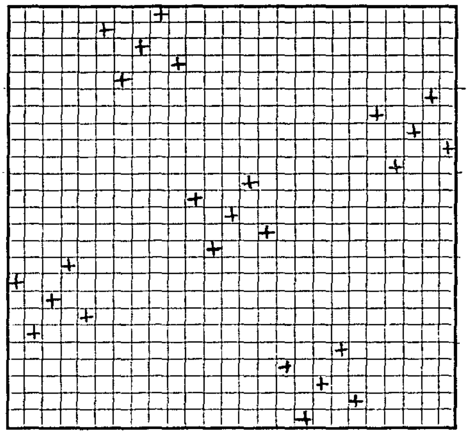

fig 2

Con este fin considero ahora, en lugar de nuestro otro tablero de n^2 casillas, uno similar de $(mn)^2$ casillas, donde ni m ni n son divisibles entre 2 ó entre 3. Sean r y s tales que:

$r - 1, r, r + 1$ no comparten divisores con m

y $s - 1, s, s + 1$ no comparten divisores con n.

Posteriormente sean a y

$s_1, s_2, s_3, \ldots, s_n,$

números tales que:

(6) $s_l = a + sl \pmod{n}$

Defino luego:

(7) $s_l - s_{l'}$ cuando $l' = l \pmod{n}$

Finalmente sea b un número cualquiera, pero bien determinado.
Ahora establezco:

$x_{nk+l} = nk + l \pmod{mn}$, $y_{nk+l} = nrk + s_l + b \pmod{mn}$.
y afirmo que (x_{nk+l}, y_{nk+l}) da por resultado una solución doblemente periódica del problema de las mn damas, cuando k recorre un sistema completo de residuos mod. m y l recorre un sistema completo de residuos mod. n.
En realidad se obtienen de este modo, mn parejas de residuos:

$(x_{nk+l}, y_{nk+l}),$

y debe demostrarse que aquellos sistemas (3) análogos a los sistemas de cuatro, cuyos miembros reciben ahora mn, construyen sistemas completos de residuos mod. mn. Finalmente se da como ejemplo para el segundo sistema lo siguiente: sea

(8) $y_{nk'+l'} = y_{nk+l} \pmod{mn}$

ó, lo que es lo mismo,

(9) $nrk' + s_{l'} + b = nrk + s_l + b \pmod{mn}$

de lo que sigue:

$s_l - s_{l'} \quad$ (mod n.),

y según (6)

$sl' = sl \pmod{n}$

(10) $l' = l \pmod{n}$

Luego se tiene según (7):

$s_l = s_{l'}$,

y, cuando esto se sustituye en (9), entonces se obtiene:

$nrk' \equiv nrk \pmod{mn}$

$rk' \equiv rk \pmod{m}$

(11) $k' \equiv k \pmod{m}$.

El resultado del análisis es por consiguiente: la congruencia (8) solamente puede mantenerse bajo ambas condiciones (10) y (11) Q.E.D.
La construcción cuya verdad fue demostrada ahora mismo, se explicará también por medio de un ejemplo. Los números más pequeños, los cuales no son divisibles ni entre 2 ni entre 3 y vienen a consideración, son: $m = 5$, $n = 5$. Posteriormente elijo:

$r = 3 \qquad s = 2$

$b = 5 \qquad a = 2$

Entonces se tiene:

$s_n \equiv 2 + 2n$ (mod. 5),

pero de ese modo el s_n no queda bien establecido. Debo elegir de ahí un primer ejemplo (Fig 1)

$s_1 = 4, \quad s_2 = 6, \quad s_3 = 8, \quad s_4 = 10, \quad s_5 = 12$

y para un segundo ejemplo (Fig. 2)

$s_1 = 4, \quad s_2 = 1, \quad s_3 = 3. \quad s_4 = 5, \quad s_5 = 2.$

Se separa del tablero infinito, un tablero cuadrático de 25^2 casillas por medio de las desigualdades:

$$1 \leq x_{5k+1} \leq 25, \qquad 1 \leq y_{5k+1} \leq 25$$

y así se obtienen la Fig. 1 y la Fig. 2.- Es evidente que se pueden encontrar aún más exposiciones compuestas para números que están compuestos por 3 o más factores.

4. En el tomo I se encuentra una discusión detallada de las soluciones "doblemente simétricas" [1], es decir, de aquellas soluciones que giran sobre sí mismas por giro del tablero sobre un ángulo recto. Como ahí se demostró, es necesario que para la existencia de soluciones similares, n sea de la forma 4m o de la forma 4 m + 1.

No carece de interés examinar [2], si existen soluciones doblemente simétricas también para n mayores. Demostraré lo siguiente:

Si no solamente el número n por sí mismo, sino también todos sus factores primos son de la forma 4m + 1, entonces el problema de las n damas tiene soluciones, las cuales son simultáneamente doblemente simétricas y doblemente periódicas.

Si todos los factores primos de n son de la forma 4m + 1, entonces hay un número r, que como se sabe [1], tienen la propiedad que:

(12) $r^2 \equiv -1 \pmod{n}$

Como puede observarse, es necesario que r no tenga divisores comunes con n. De:

$(r-1)(r+1) \equiv r^2 - 1 \equiv -2 \pmod{n}$

resulta posteriormente que tampoco $r-1$ y $r+1$ comparten divisores comunes con n.

Ahora establezco:

(13) $x_l \equiv l, \quad y_l \equiv rl \pmod{n}$.

Cuando l pasa por un sistema completo de residuos mod. n, entonces (13) representa una solución doblemente periódica de las n damas, como si fuera expuesto bajo 2.

Así como l, tambien rl pasa por un sistema completo de residuos mod. n. Según (12) y (13) se tiene:

$x_{rl} \equiv rl \equiv y_l \;,\quad y_{rl} \equiv r^2 l \equiv -x_l \pmod{n}$.

Eso significa, sin embargo, que por medio de un giro de 90° en el sentido de las manecillas del reloj, los puntos congruentes con $(x_l \;, \; y_l)$ recorren el punto y son congruentes con $(x_{rl} \;, \; y_{rl})$ es decir, que por medio de un giro similar del tablero infinito completo, la solución doblemente periódica (13) se recorre a sí misma. Se separa del tablero infinito, por medio de las desigualdades:

$-(n-1)/2 \le x_i \le (n-1)/2 \quad , \quad -(n-1)/2 \le y_i \le (n-1)/2 \quad ,$

un tablero infinito de n^2 casillas, con el punto (0, 0) como punto medio y así las n figuras (números) situadas se recorren por medio del giro mencionado, Q.E.D.

El lector encuentra la solución que se encontró arriba para n = 5 y para n = 13, en el tomo I, representada con figuras: Fig. 7 (pag. 216) y Fig. 28 (pág. 258). En estas exposiciones se debe observar lo siguiente: hay 4 reinas, las cuales tienen el intervalo más pequeño posible de la reina parada en el punto medio (0, 0) del tablero. Si a y b son las dos coordenadas de la casilla que ocupa cualquiera de esas 4 reinas, entonces se tiene:

$$(14) \quad n = a^2 + b^2 ,$$

donde los dos números a y b no comparten divisores entre sí, ni con n. Se observa una conducta similar en el caso siguiente de n = 17, 25 y éste sirve para encontrar lo más rápidamente posible estas exposiciones delicadas.

Esta observación tiene un valor sólo general. Para examinar esto y para conocer en suma el significado teórico -numérico de estas exposiciones, son necesarios por supuesto, conocimientos profundos [1].
La congruencia (12) tiene el mismo significado que una igualdad:

$$r^2 = -1 + mn,$$

donde m representa un número entero. La forma cuadrática

$$nx^2 + 2rxy + my^2$$

tiene el determinante $r^2 = -mn = -1$ y debe ser equivalente por consecuencia, a la única forma reducida $x^2 + y^2$ del determinante -1. Eso significa que existen 4 números a, b, α y β de un tipo tal, que:

$$(15) \quad a\beta - b\alpha = 1$$

$$(16)\ (ax + \alpha y)^2 + (bx + \beta y)^2 = nx^2 + 2rxy + my^2,$$

Por medio de la comparación de los coeficientes en (16), se obtiene:

$$n = a^2 + b^2,$$

$$a\alpha + b\beta = r$$

y estas dos últimas igualdades dan, combinadas con (15):

$$\begin{aligned} ar &= a^2\alpha + b\alpha\beta \\ &= a^2\alpha + b\,(b\alpha + 1) \\ &= n\alpha + b \end{aligned}$$

$$ar = b \pmod{n}$$

De este modo, la solución (13) para $l \equiv a$, $x_1 \equiv a$, $y_1 \equiv ra \equiv b$, da realmente como resultado una descomposición del tipo (14).
Si se considera nuestro tablero infinito como el plano de números complejos, entonces los puntos medios de los distintos campos son los números enteros Gaussianos [2]. Obsérvese que al igual que con n, también an pasa por un sistema completo de residuos mod. n, de tal modo que nuestra solución también puede tomar la forma

(13)'

$$\begin{aligned} x_{al} + iy_{al} &\equiv al\,(1 + ir) \pmod{n} \\ &\equiv l\,(a + ib) \pmod{(a + ib)(a - ib)} \\ &\equiv 0 \pmod{a + ib} \end{aligned}$$

La solución (13) se obtendrá así, cuando cada una de las casillas del tablero infinito sea cubierto con figuras (números) cuyos puntos medios son especies de múltiplos complejos de un número entero Gaussiano a + ib, donde a y b no comparten divisores y (a + ib)(a − ib) = n. Este sistema de puntos se ordena en cuadrantes del plano $n = a^2 + b^2$ y así aclara que la conducta observada con el ejemplo n = 5, 13, 17, 25, es cierta en general.

5. El precedente da motivo a diferentes observaciones, las cuales también conciernen a las soluciones no doblemente periódicas del problema de las n damas. Deseo, sin embargo, proponer aquí brevemente por que estas exposiciones no ofrecen ningún interés teórico-numérico, no se dirigen hacia ningún resultado definitivo y también por qué el hacer una presentación detallada sería demasiado fastidioso.

La Fig. 2 nos da una solución cercana al siguiente ejercicio:

Construir una solución del problema de las mn-reinas, a partir de cualquier solución del problema de las m reinas y a partir de una solución doblemente periódica del problema de las n reinas. - La construcción se desarrolla de la siguiente manera: se divide cada casilla del tablero de m^2 casillas, en n^2 cuadrantes iguales. Si la casilla de interés del tablero de m^2 casillas estaba descubierta, todas las n casillas resultantes quedan igualmente descubiertas; si por el contrario, aquella estaba cubierta, se compone la solución concedida doblemente periódica del problema de las n reinas a partir de las n^2 casillas resultantes, de tal modo que el último de los tableros resultantes se compondrá exactamente de mn hileras horizontales y verticales, m veces. Está claro que las mn reinas así divididas no pueden practicar ningún ataque de torre una tras otra. Se puede examinar que éstas no pueden realizar ningún ataque de alfil tampoco: trasládense igualmente las n reinas correspondientes (las cuales se originan de la justificaicón de uno y de su propia casilla del tablero de m hileras), en una dirección diagonal hacia las casillas n ó 2n ó 3n . . . y entonces la solución doblemente periódica para n trasladada puede ciertamente llegar junto a otra solución doblemente periódica, pero nunca coincide, y ahí carecemos de una solución correcta del problema de las n damas. Ahora se tiene fácilmente, a partir del concepto de la solución doblemente periódica (véase 1), que las 2n reinas, las cuales se componen de dos tableros de n^2 casillas, separados exactamente de la misma solución doblemente periódica, que no se pueden atacar como alfiles (pero cada una de las dos reinas paradas en tableros distintos, podrán atacarse como torres, desde la distancia n). Cuando las reinas no pueden atacarse nunca como alfiles, después de un desplazamiento similar hacia la casilla n ó 2n ó 3n . . . en la dirección diagonal, entonces pudieron hacerlo ante un desplazamiento más pequeño, Q.E.D.

El giro del tablero infinito, el cual examinamos en (4) dá motivo a la siguiente observación: si se separan n – 1 figuras de la solución (13) a través de la desigualdad

(17) $1 \leq x_i \leq n - 1, \quad 1 \leq y_i \leq n - 1$

entonces construyen una solución para el tablero de $(n - 1)^2$ casillas. Si se añade entonces la figura en la casilla (0, 0) enconces construyen siempre una solución, naturalmente de un tablero de n^2 casillas. La solución (17) es idéntica a la solución:

(18) $-n + 1 \leq x_i \leq -1, \quad 1 \leq y_i \leq n - 1$

donde el tablero infinito fue hecho doblemente periódico. Por medio del giro del tablero infinito, sobre un ángulo recto en el sentido de las manecillas del reloj, se cubren las n – 1 figuras (18) con las de (17). También se puede afirmar lo siguiente en una expresión distinta:

Si todos los factores primos de n + 1 son de la forma 4m + 1, entonces el problema de las n reinas tiene seguramente soluciones doblemente simétricas.

La composición particularmente sencilla para n = 16 en el tomo I, sirve como ejemplo.

La construcción bajo 4 que se nombró, no provee ninguna solución doblemente simétrica para el caso de n = 9. Entonces el número 9 = 3·3 es realmente la forma 4m + 1, sin embargo, no se compone de factores primos de la misma forma. Por la misma razón, el método que se expuso arriba no ofrece ninguna solución doblemente simétrica, para n = 8 = 9 – 1. Esto aclara en cierto modo, el hecho mencionado en el Capítulo IX, que en suma no hay ninguna solución doblemente simétrica para n = 8 y n = 9.