Pro Mathematica: Vol. II, No. 3, 1988

PLANOS PROYECTIVOS FINITOS Y EL TEOREMA DE BRUCK Y RYSER

Enzo R. GENTILE (*)

Este trabajo, de naturaleza expositiva, tiene por objeto mostrar curiosas y estrechas relaciones entre la existencia de planos proyectivos, formas cuadráticas y cuadrados latinos.

La cuestión se centra en un problema geométrico: la existencia de planos proyectivos finitos de cierto orden.

Recordemos que un **plano proyectivo** es una estructura de incidencia

$$\mathcal{P} = (P, R, I),\ P = puntos, R = rectas,\ I = incidencia$$

de puntos y rectas sometidas a las siguientes relaciones:

(*) Profesor Titular de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires.

p1. Con todo par de puntos distintos existe una única recta incidente a ambos puntos.

p2. Con todo par de rectas distintas hay un único punto incidente con ambas rectas.

p3. Existen cuatro puntos tales que ninguna terna de los mismos es incidente a una misma recta. (O sea, existen cuatro puntos, de a 3 no alineados).

Si el plano es finito, o sea consiste de sólo un número finito de puntos, entonces existe n natural que satisface:

$$|P| = n^2 + n + 1$$
$$|R| = n^2 + n + 1$$
$$|r| = n + 1, \text{ cualquiera sea } r \in R.$$

Se dice entonces que el plano proyectivo tiene **orden n.** Uno de los problemas fundamentales de lo que se ha dado en llamar **Geometrías Finitas,** es saber para qué $n \in N$ existen planos proyectivos de orden n. Copiando los planos proyectivos reales o complejos es posible construir planos proyectivos sobre cuerpos finitos cuyo orden es el cardinal del cuerpo, o sea una potencia de un primo. En 1949 los matemáticos R. H. Bruck y H. J. Ryser publicaron un trabajo sobre la inexistencia de planos proyectivos de cierto orden. Por ejemplo se sigue de este resultado que no hay planos proyectivos de orden 6. No obstante es un problema abierto la existencia de planos proyectivos de orden 10.

La demostración del teorema de Bruck y Ryser se puede obtener como sencilla aplicación de la teoría de formas cuadráticas sobre cuerpos p-ádicos y esto lo haremos en detalle en este trabajo.

La noción de plano proyectivo está naturalmente ligada a la noción de **plano afin.** Un plano afin es una estructura de incidencia

$\mathcal{A} = (P, R, I)$, $P = puntos$, $R = rectas$, $I = incidencia$

sometida a las siguientes condiciones:

a1. Con todo par de puntos distintos existe una única recta incidente con ambos puntos.

a2. Dados una recta r y un punto p no incidentes, existe una única recta incidente con p pero no incidente con r.

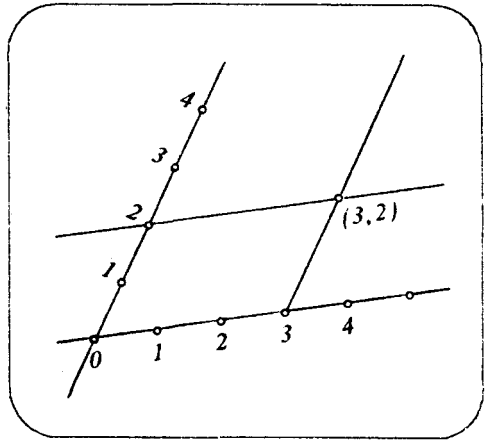
a3. Existen tres puntos, no incidentes con ninguna recta.

Si el plano afín es finito existe un entero positivo n tal que:

$|P| = n^2$
$|R| = n(n+1)$
$|r| = n$, para toda $r \in R$.

Se dice entonces que el plano afín tiene **orden n.** Por supuesto que el problema de existencia de planos proyectivos de orden n es equivalente a la existencia de planos proyectivos de orden n. En efecto, el plano proyectivo se obtiene adjuntando al plano afín una recta, la recta "en el infinito".

Dado un plano afín de orden n podemos coordenar sus puntos de la manera siguiente. Se toma una recta. Sus n puntos los llamamos: *0, 1, ..., n–1.* Por 0 tomamos otra recta y denominamos sus puntos por *0, 1, ..., n–1,* siendo el punto 0 común a ambas rectas. Utilizando esas rectas como



ejes coordenados, podemos representar en la forma habitual los n^2 puntos por pares (a, b), con a y b recorriendo el conjunto *0, 1, ..., n–1.*

Tomemos una recta no paralela a ninguna de las rectas coordenadas. Con ella tomamos sus n rectas paralelas. Numeremos las mismas de *0* a *n–1* en forma arbitraria. Definimos ahora una matriz de nxn cuyos coeficientes son *0* a *n–1*, en la forma siguiente: en el lugar (a,b) colocamos el entero de *0* a *n–1* que corresponde a la única recta que pasa por (a, b). Obtenemos una matriz que es un **cuadrado latino,** o sea es una matriz de nxn con coeficientes *0, ..., n-1* y con la propiedad que cada coeficiente i, $0 \leq i \leq n-1$ aparece una y sólo una vez en cada columna y fila.

Puesto que hay *n–1* haces de rectas paralelas incidentes con los ejes coordenados y distintos de estos, podemos construir por el proceso descrito exactamente *n–1* matrices que son cuadrados latinos. El hecho relevante es que estos *n-1* cuadrados latinos son **ortogonales** dos a dos. Digamos que dos cuadrados latinos (a_{ij}), (b_{ij}) del mismo orden con $a_{ij} \in \{t_1, ..., t_n\}$, $b_{ij} \in \{s_1, ..., s_n\}$, se dicen **ortogonales** y anotamos $(a_{ij}) \perp (b_{ij})$, si los n^2 pares ordenados (t_i, s_j), $1 \leq i, j \leq n$, ocurren exactamente una sola vez en los n^2 pares ordenados (a_{ij}, b_{ij}).

Por ejemplo los cuadrados latinos

$$\begin{matrix} 1 & 2 \\ 2 & 1 \end{matrix} \quad y \quad \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$$

no son ortogonales pues al formar la matriz: $\begin{matrix} 10 & 21 \\ 21 & 10 \end{matrix}$ se repiten elementos.

En cambio los cuadrados latinos de orden 3,

$$\begin{matrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 2 & 0 & 1 \end{matrix} \qquad \begin{matrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 0 & 2 \end{matrix}$$

son ortogonales dado que la matriz

$$\begin{matrix} 10 & 22 & 01 \\ 02 & 11 & 20 \\ 21 & 00 & 12 \end{matrix}$$

no tiene elementos repetidos
Análogamente

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{matrix} \perp \begin{matrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{matrix}$$

Hemos observado entonces que la existencia de un plano proyectivo (o afin) de orden n implica la existencia de un conjunto de $n-1$ cuadrados latinos ortogonales. Mostraremos luego que, recíprocamente, la existencia de un conjunto de $n-1$ cuadrados latinos ortogonales implica la existencia de un plano proyectivo (o afin) de orden n.

La cuestión de existencia de cuadrados latinos se remonta al matemático Leonhard Euler (1707–1783) quien en 1782 planteó el célebre **Problema de los 36 Oficiales.** Se trata de saber si 36 oficiales, de 6 grados diferentes y de 6 cuarteles diferentes pueden disponerse en un cuadrado de 6 filas por 6 columnas de manera tal que cada grado y cada cuartel este representado por un oficial, en cada fila y en cada columna. Es claro que si disponemos de dos cuadrados latinos de orden 6 ortogonales sabemos como lograr esa disposición. La conjetura de Euler establecía la imposi-

bilidad de responder afirmativamente este problema.

En el año 1900, el matemático francés G. Tarry, vía una enumeración exhaustiva, probó la imposibilidad de resolver afirmativamente el problema de los 36 oficiales.

Llamemos $N(n)$ al número máximo de cuadrados latinos de orden n ortogonales entre si. Euler demostró que $N(n) > 1$ si $n \neq 2 \pmod 4$ y conjeturó que para $n \equiv 2 \pmod 4$ era $N(n) = 1$. Esta última conjetura resultó incorrecta dado que en 1960, R.C. Bose, S.S. Shrikhande y E.T. Parker probaron que $N(n) > 1$ para todo $n \neq 1, 2, 6$.

(Referencia: P. Dembowski, **Finite Geometries,** Springer-Verlag, 1968). Notar que se sigue del resultado de Tarry de la solución negativa del problema de los 36 oficiales, que no existen planos proyectivos de orden 6, resultado éste incluido en el Teorema de Bruck y Ryser.

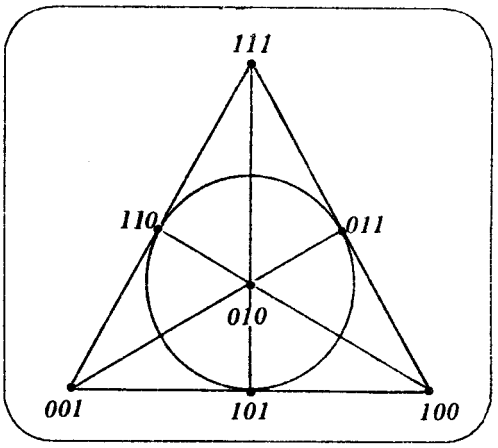
PLANOS PROYECTIVOS FINITOS Y EL TEOREMA DE BRUCK Y RYSER

Ya definimos en la introducción la noción de plano proyectivo de orden n. Si el lector quiere hacer algún tipo de ejercitación le proponemos demostrar a partir de las condiciones p1., p2., p3. las siguientes afirmaciones:

i. Todo plano proyectivo contiene al menos 7 puntos.
ii. Si P es un plano proyectivo de orden n, entonces:

a. **Toda recta** de P es incidente a exactamente $n+1$ puntos.
b. **Todo punto** de P es incidente a exactamente $n+1$ rectas.
c. $|P| = n^2 + n + 1$
d. $|R| = n^2 + n + 1$

Notemos la existencia de un plano proyectivo de orden 2, o sea formado por $7 = 2^2 + 2 + 1$ puntos. Es el famoso **plano de Fano.**



Notemos que si p es un número primo positivo y $r \in N$ entonces existe un plano proyectivo de orden p^r. En efecto, será suficiente probar la existencia de un plano afín de orden p^r. Sea $K = GF(p^r)$ el cuerpo finito de orden p^r (cuerpo de Galois). Formamos el plano $K^2 = \{(a, b) \mid a, b \in K\}$. Los *puntos* son los elementos de K^2, las *rectas* son las soluciones de las ecuaciones:

$$aX + bY + c = 0, \quad a, b, c \in k, \quad (a, b) \neq (0, 0)$$

Este plano se denomina afín sobre K, se denota por $A_2(p^r)$. El plano proyectivo asociado se denota por $P_2(p^r)$.

El teorema de Bruck y Ryser es un teorema de *no existencia* de planos proyectivos de ciertos órdenes.

Teorema: (Bruck y Ryser, 1949) Sea $n \in N$ tal que $n \equiv 1$ ó $2 \pmod 4$ y además n **no** es suma de dos cuadrados en Z. Entonces no existe ningún plano proyectivo de orden n.

Una aplicación nítida resulta para $n = 6$, que satisface ambas condiciones. No obstante para $n = 10$, se tiene $10 \equiv 2 \pmod 4$ pero $10 = 1^2 + 3^2$ y el teorema no se aplica. Veamos en una tabla la existencia de planos proyectivos.

Orden	¿Plano Proyectivo?	Razón
2	Si, P_2 (2)	
3	Si, P_2 (3)	
4	Si, P_2 (2^2)	
5	Si, P_2 (5)	
6	No,	por Teorema B y R
7	Si, P_2 (7)	
8	Si, P_2 (2^3)	
9	Si, P_2 (3^2)	
10	?	$10 = 1^2 + 3^2$
11	Si, P_2 (11)	
12	?	$12 \equiv 0 \pmod 4$

Nota: Existen planos proyectivos de orden > 9 que no son de la forma P_2 (p^r), son los planos proyectivos **no-desarguianos,** o sea no satisfacen el clásico Teorema de Desargues.

Vamos a la demostración del Teorema de Bruck y Ryser. Primeramente recordamos de la teoría elemental de números que la condición de ser suma de dos cuadrados es equivalente a que en la factorización de n en producto de factores primos, todo factor primo p impar, que aparezca con exponente máximo impar, debe ser de la forma $p \equiv 1 \pmod 4$.

O sea también que si p es un número primo impar y p^s divide exactamente a n entonces s es par ó $p \equiv 1 \pmod 4$. Por ejemplo:

$$n = 2 \cdot 3^2 \cdot 5 \cdot 7^4 \cdot 11^e$$

es suma de dos cuadrados si e es par, no lo es si e es impar.

El teorema establece entonces que si $\mathcal{P}$ es un plano proyectivo

de orden n y si $n \equiv 1$ ó $2 \pmod 4$ entonces todo primo p **impar** que divide a n en exactamente una potencia impar debe satisfacer $p \equiv 1 \pmod 4$.

Sea $N = n^2 + n + 1$. Sea $(p_j)_{1 \le j \le N}$ un sistema de P. Sea $(X_j)_{1 \le j \le N}$ un sistema de N indeterminadas sobre el cuerpo racional Q. Identifiquemos cada Xj con un punto p_j del plano proyectivo. Cada recta determina una forma lineal

$$L_k = \sum_j X_j \qquad\qquad k \in R \ (= rectas)$$

donde j recorre los índices de los puntos p_j de la recta k. Hay pues N funciones lineales de este tipo.

Consideremos la forma cuadrática

$$q = \sum L_k^2 = (n+1) \sum_{i=1}^{N} X_i^2 + \sum_{i \neq j} X_i X_j$$

El hecho relevante de la demostración es hallar una diagonalización inteligente de la forma cuadrática q. Se tiene:

$$q = (n+1) \sum_{i=1}^{N} X_i^2 + 2 \sum_{i<j} X_i X_j$$

$$q = (n+1) X_1^2 + n X_2^2 + \ldots + n X_N^2 + 2(X_1 X_2 + \ldots + X_1 X_N) + (X_2 + \ldots + X_N)^2$$

$$= (X_2 + \ldots X_N)^2 + n(X_2 + (X_1/n))^2 + n(X_3 + (X_1/n))^2 + \ldots + n\,(X_N + (X_1/n))^2$$

Por lo tanto si escribimos:

$$Y_1 = X_2 + \ldots + X_N$$
$$Y_j = X_j + n^{-1} . X_1, \quad j > 1$$

Resulta la diagonalización

$$q = Y_1^2 + n. \sum_{j>1} Y_j^2$$

Utilizando la notación diagonal para denotar formas cuadráticas se tiene la isometría, sobre Q ,

$$q = \langle 1, 1, \ldots, 1 \rangle \text{ (N unos)}$$
$$\cong \langle 1, n, \ldots, n \rangle \text{ (N-1 enes)}$$

Analicemos esta forma cuadrática sobre el cuerpo p-ádico Q_p. Siendo el primo p impar, la forma <1, 1, 1, 1> es isótropa y por lo tanto asi lo es la forma $\langle n, n, n, n \rangle$ de manera que se tiene la isometría

$$\langle 1, 1, 1, 1 \rangle \cong \langle 1, -1, 1, -1 \rangle \cong \langle n\, n, n, n \rangle$$

Se sigue entonces del teorema de cancelación de Witt y de la propiedad aritmética

$$n \equiv 1 \text{ ó } 2 \pmod 4 \Rightarrow N \equiv 3 \pmod 4,$$

la isometría de las formas cuadráticas.

$$\langle 1, 1, 1 \rangle \cong \langle 1, n, n \rangle$$

y también $\langle 1, 1 \rangle \cong \langle n, n \rangle$, *sobre* Q_p

Escribiendo $n = p^e . u$, con e impar y u unidad en Q_p se tiene la isometría.

$$\langle 1, 1 \rangle \cong \langle p.u, p.u \rangle$$

Por lo tanto $p.u$ es suma de dos cuadrados en Q_p: $p.u = r^2 + s^2$

con r, s en Q_p. Multiplicando eventualmente por una potencia par de p podemos suponer que r y s son unidades en Q_p. Por lo tanto pasando al cuerpo residual ($= Z_p$) resulta $r^2 + s^2 = 0$ en Z_p con $r \neq 0, s \neq 0$.

Se sigue entonces que la ecuación $x^2 = -1$ es resoluble en Z_p. Esto ocurre si y sólo si p es de la forma $4m + 1$. El Teorema queda completamente demostrado.

En un Apéndice resumimos las propiedades relativas a números p–ádicos requeridos en esta demostración. Para profundizar el tema recomendamos: **Neal Koblitz,** p–adic Numbers, p–adic Analysis, and Zeta –Functions, Springer–Verlag, (1977), **Z. I. Borevich–I. R. Shafarevich,** Number Theory, Academic Press, (1966). Para la parte de Formas Cuadráticas puede consultarse la Monografía de la OEA, Estructuras Algebraicas VI, Formas Cuadráticas de **F. Piscoya** (1981).

CUADRADOS LATINOS ORTOGONALES Y PLANOS PROYECTIVOS FINITOS

Retomemos nuestra discusión anterior. Sea para cada n natural, $N(n)$ = número máximo de cuadrados latinos de orden n ortogonales dos a dos.

Proposición: $N(n) \leq n - 1$, para $n > 1$.

Demostración: Notemos primeramente que si A es un cuadrado latino, $A = (a_{ij})$ de orden n con coeficientes 1, 2, ..., n y t una permutación de {1, 2, ..., n}, la matriz $A' = (b_{ij})$ con $b_{ij} = t(a_{ij})$, es un cuadrado latino y además si $A \perp M$, entonces $A' \perp M$.

Decimos entonces que A y A' son cuadrados latinos **equivalentes.** Sean dados (a^k_{ij}), i, j = *1, ..., n* ; k = *1, ..., n, n* cuadrados latinos ortogonales dos a dos. Supongamos que en todos los cuadrados latinos los coeficientes son *1, 2, ..., n.* Podemos suponer,

sin pérdida de generalidad, que la primera fila de todos los cuadrados latinos es la sucesión 1, 2, ..., n. Esto es posible por la posibilidad de tomar cuadrados latinos equivalentes. Por ejemplo si n = 3 se tendrían los cuadrados,

1	2	3	1	2	3	1	2	3
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.

Observemos ahora la segunda fila de los cuadrados. En el lugar 21 no está permitido el 1, para ninguna de las n matrices. Se sigue que existen dos cuadrados (a_{ij}^{k}), (a_{ij}^{r}), $k \neq r$ con $a_{21}^{k} = a_{21}^{r}$

Pero también se verifica que $a_{1i}^{k} = a_{1i}^{r} = a_{21}^{k} = a_{21}^{r} = d$, de manera que el apareamiento de la matriz k con la matriz r repite el par (d, d). Por lo tanto los cuadrados k y r no son ortogonales, una contradicción. Esto muestra que $N(n) \leq n - 1$. Para ilustrar el razonamiento usando los cuadrados de orden 3 escritos anteriormente, escribamos las segundas filas de esos cuadrados:

1	2	3	1	2	3	1	2	3
2	.	.	2	.	.	.	.	.
.	.	.	.	.	.	.	.	.

ó

1	2	3	1	2	3	1	2	3
3	.	.	3	.	.	.	.	.
.	.	.	.	.	.	.	.	.

Se ve claramente que el apareamiento de las dos primeras matrices repite el par 22 en un caso y el par 33 en el segundo.

Notar que N(2) = 1 lo cual es obvio dado que el apareamiento de los cuadrados latinos,

1	2	2	1	da lugar a	12	21
2	1	1	2		21	12

Veamos ahora el siguiente resultado fundamental.

Teorema: Sea $n > 1$. Entonces $N(n) = n - 1$ si y sólo si existe un plano proyectivo finito de orden n.

Demostración: Supongamos dados $n - 1$ cuadrados latinos ortogonales $A^{(k)} = (a^k_{ij})$, $k = 1, 2, \ldots, n$. Supongamos además que los coeficientes a^k_{ij} se toman en el conjunto $S = \{0, 1, \ldots, n-1\}$. Vamos a definir un **plano afín** de orden n. **Los puntos** serán los elementos del conjunto $S^2 = S \times S$.

Diremos que un subconjunto $r \subset S^2$ de n elementos es una **recta** si y sólo si existe un cuadrado latino $A^{(j)}$ tal que:

$$(u,v) \in r, (s,t) \in r \Rightarrow a^j_{uv} = a^j_{st}$$

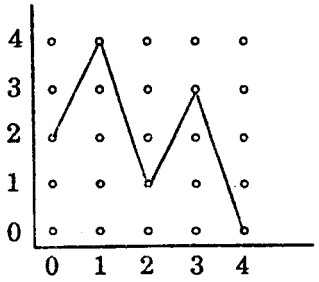
Es decir, todos los elementos del cuadrado $A^{(j)}$ ubicados en las coordenadas $(u, v) \in r$, tienen el mismo valor. Incluiremos también como rectas a los subconjuntos de S^2 que tienen una misma coordenada (tales como (0, 1), (0, 2), ..., (0, $n-1$). La relación de incidencia es obvia. Debemos verificar la validez de los axiomas de plano afín. A ese fin notemos que por cada punto pasan $n+1$ rectas distintas. Si excluimos las dos rectas "vertical" y "horizontal" nos quedan $n - 1$ rectas que llamaremos propias. Estas $n - 1$ corresponden a los $n - 1$ cuadrados latinos ortogonales. El axioma que requiere atención es el que se asegura que por dos puntos distintos pasa una única recta. Para fijar las ideas consideremos el punto (1, 1). La existencia de $n - 1$ cuadrados latinos ortogonales asegura que hay exactamente $n - 1$ rectas que unen (1, 1) con (2, 2), (1, 1) con (2, 3), ..., (1, 1) con (2, $n-1$). Repitiendo este razonamiento para los elementos de la segunda fila, luego tercera, etc. probamos que el punto (1, 1) está unido a

todo otro punto de S^2. Repitiendo esto para todos los elementos, se concluye la verificación de la propiedad.

Ilustraremos esta parte del Teorema considerando 4 cuadrados latinos ortogonales de orden 5:

01234	02413	03142	04321
12340	13024	14203	10432
23401	24130	20314	21043
34012	30241	31420	32104
40123	41302	42031	43210

El plano afín será:



El subconjunto $(0,2),(1,4),(2,1),(3,3)$ constituye una recta pues en el segundo cuadrado latino los lugares con esas coordenadas tienen todos el valor común 4. Suponiendo que los elementos 0, 1, 2, 3, 4 pertenecen a Z_5, esta recta es la recta de $A_2(5)$ dada por $y = 2x + 2$.

La demostración de la recíproca, o sea de la existencia de $n - 1$ cuadrados latinos ortogonales, dada la existencia de un plano proyectivo de orden n, la hemos bosquejado anteriormente y en lugar de dar los detalles, proponemos al lector retomar el ejemplo del plano afín $A_2(5)$ sobre el cuerpo Z_5 y construir en ese caso los cuadrados latinos. Estos son exactamente los que hemos enumerados más arriba. Por cada recta $y = m.x$, con $m = 1, 2, 3, 4$ consi-

deramos la líneas de nivel.

$$y = m.x + k\,,\ k = 0, 1, 2, 3, 4$$

Obtenemos las 4 cuadrados latinos anteriores. Por ejemplo para las rectas y = x + k, k = 0, 1, 2, 3, 4, los valores de y cuando x recorre 0, 1, 2, 3, 4 da la matriz (cuadrado latino)

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

Ejercicio: Utilizando un cuerpo de 4 elementos y el plano afín $A_2(4)$ construir 3 cuadrados latinos de orden 4 ortogonales.

Una aplicación

Cuadrados latinos ortogonales permiten hacer "diseños" de experimentos. Supongamos se dispone de tres tipos de una droga para la fiebre y tres tipos de una droga para el dolor de cabeza. Se trata de experimentar con estas drogas sobre tres individuos en un período de tres días. Para el caso de una droga, por ejemplo para la fiebre, un diseño razonable es mediante un cuadrado latino de orden 3, por ejemplo (A, B, C denotan los individuos y 1, 2, 3 los tipos de droga)

	Días		
	L	M	Mi
A	1	2	3
B	2	3	1
C	3	1	2

Análogamente podemos diseñar el mismo experimento con

la droga para el dolor de cabeza.

	Días		
	L	M	Mi
A	1	2	3
B	3	1	2
C	2	3	1

Puesto que cada individuo toma una droga para la fiebre y una para el dolor de cabeza cada día, se puede estudiar el efecto combinado de la administración de ambas drogas. Por un período de 9 días el diseño sería simplemente que cada individuo ingiera las 9 posibles combinaciones de estos dos tipos de medicamentos.

Ahora para un período de tres días un diseño natural es tomar los dos cuadrados latinos ortogonales y formar el apareamiento.

	Días		
	L	M	Mi
A	11	22	33
B	23	31	12
C	32	13	21

Por ejemplo el individuo B ingiere el Lunes la droga 2 para la fiebre y la droga 3 para el dolor de cabeza, el martes la droga 3 para la fiebre y la droga 1 para el dolor de cabeza, ... (pobre tipo!).

Apéndice:Números p-ádicos

En la demostración del Teorema de Bruck y Ryser hemos utilizado la teoría de formas cuadráticas sobre cuerpos p-ádicos. Insistamos en que todo el material allí usado es elemental. De la

teoría de formas cuadráticas lo más que usamos es el teorema de cancelación de Witt. De números p–ádicos requerimos algunos hechos elementales que vamos a detallar aqui a fin de hacer autocontenida nuestra exposición. Sea p un primo positivo. Un **número p–ádico** es una serie formal.

$$a = a_m p^m + a_{m+1}\ p^{m+1} + \ldots$$

donde los coeficientes a_i son enteros, $0 \leq a_i < p$, $a_m \neq 0$ y $m \in Z$. Números p–ádicos se suman y multiplican en forma habitual efectuando la reducción módulo p. La totalidad de números p–ádicos se denota por Q_p y constituye un cuerpo: el **cuerpo de números p–ádicos.** Los número racionales forman un subcuerpo de Q_p. Los números p–ádicos de la forma:

$$a_0 + a_1 p + a_2 p^2 + \ldots \quad , 0 \leq a_i < p$$

se denominan **enteros p–ádicos.** La totalidad de enteros p–adicos denotada por O_p, constituye un subanillo de Q_p, el **anillo de enteros p–ádicos.** Este anillo es **local,** es decir, con un único ideal maximal denotado por P y formado por todos los múltiplos del número p, o sea.

$$P = (a_0 + a_1 p + a_2 p^2 + \ldots \mid a_0 = 0)$$

Los enteros p–ádicos con $a_0 \neq 0$ constituyen el **grupo de unidades** de O_p que denotamos con U_p. Decimos también que son las unidades de Q_p. El anillo cociente O_p/P llamado el **cuerpo residual** coincide con el cuerpo finito Z_p de enteros módulo p.

El resultado relevante a nuestro fin es el siguiente. El mismo constituye un teorema de levantamiento de cuadrados de Z_p a O_p y permite determinar las clases de cuadrados de Q_p^* que a su vez permite estudiar las formas cuadráticas sobre Q_p.

Teorema: Sea p, primo impar. Una unidad $u = u_0 + u_1 p + u_2 p^2 + \cdots$ es un cuadrado en O_p si y sólo si u es un cuadrado módulo el ideal maximal P, o equivalentemente si y sólo si u_0 es un cuadrado como elemento de Z_p.

El grupo multiplicativo Q_p^*/Q_p^{*2} contiene 4 elementos representados por $1, e, p, pe$, donde e es un entero, $1 < e < p$, que no es residuo cuadrático módulo p.

Notemos que al tomar una unidad $u \in U_p$ y al pasar al cociente módulo el ideal P, estamos en Z_p. El hecho notable de esta proposición es que si $u = u_0 + u_1 p + u_2 p^2 + \ldots$ es una unidad, es un cuadrado en Q_p si y sólo si u_0 (pensado en Z_p) es un cuadrado. Por ejemplo si $p = 5$ las unidades $u_0 + u_1 5 + \ldots$ que son cuadrados en Q_5 son exactamente aquellas en que $u_0 = 1$ ó 4. Este resultado en un caso muy particular de un célebre resultado, el **Lema de Hensel** (Kurt Hensel (1861–1941) introdujo ó inventó los números p–ádicos a fines del siglo pasado revolucionando la matemática y gestando la llamada matemática moderna). Veamos un bosquejo de la demostración del Teorema.

Sea $u = u_0 + u_1 p + u_2 p^2 + \ldots$ tal que $u \equiv a_0 \pmod{P}$ o lo que es lo mismo (mod p) dado que P es el ideal generado por p.

Tenemos que encontrar un número p–ádico a tal que $a^2 = u$.
Vamos a determinar inductivamente los a_i tales que:

$$a = a_0 + a_1 p + a_2 p^2 + \ldots \text{ y } a^2 = u$$

Es equivalente a determinar $a_0, a_1, \ldots$ tales que para todo $k \in N$,

$$(a_0 + a_1 p + \ldots + a_k p^k)^2 \equiv u \pmod{p^{k+1}} \qquad 0 \leq a_i < p$$

La hipótesis del Teorema asegura la existencia de a_0, $0 < a_0$

$< p$ tal que $a_0^2 \equiv u_0 \pmod p$, de manera que la elección de a_0 está garantizada.

Supongamos entonces determinados $a_0, a_1, \ldots, a_k$, $k \geq 0$ con esas propiedades. Vamos a determinar a_{k+1}.

Sea $c = a_0 + \ldots + a_k p^k$, $c^2 \equiv u \pmod{p^{k+1}}$.

Se tiene que satisfacer

$$(c + a_{k+1}p^{k+1})^2 \equiv u \,(mod\, p^{k+2}),$$

operando y usando la hipótesis inductiva:

$$c^2 + 2ca_{k+1}p^{k+1} + a_{k+1}p^{2(k+1)} \equiv u \,(mod\, p^{k+2})$$

o sea:

$$2ca_{k+1} \equiv \frac{u - c^2}{p^{k+1}} \qquad (mod\, p)$$

Puesto que $2 \not\equiv 0 \pmod p$ y $c \equiv a_0 \not\equiv 0 \pmod p$, se puede despejar el valor a_{k+1}. Esto prueba entonces la parte relativa a "levantamiento de cuadrados".

Sea $x \neq 0$ un elemento de Q_p^*. Multiplicando eventualmente por una potencia **par** de p podemos suponer que x es de la forma,

$$x = a_0 + a_1 p + \ldots, a_0 \neq 0 \quad \acute{o} \quad x = p^i(a_0 + a_1 p + \ldots) \; con \; a_0 \neq 0.$$

Entonces es claro que x es un cuadrado en Q_p si y sólo si a_0 es un cuadrado en Z_p e i es par. Puesto que en Z_p^* hay sólo dos clases de cuadrados, digamos representadas por 1, e, $1 < e < p$, las clases de cuadrados en Q_p^* están representadas por 1, e, p, pe, como queríamos probar. Otro hecho elemental utilizado fue que la forma cuadrática $x_1^2 + x_2^2 + x_3^2 + x_4^2$ abreviada $\langle 1, 1, 1, 1 \rangle$, es isótropa. Para

ver esto usamos el hecho que dicha forma es isótropa sobre Z_p. Por lo tanto existen enteros x_1, x_2, x_3, x_4 no todo ceros tales que la suma $x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{p}$. Supongamos $x_1 \neq 0$. Pensemos ahora a $x_1, \ldots, x_4$ en Q_p. La ecuación : $x_1 = -(x_1^2 + x_2^2 + x_3^2)$ es resoluble módulo p, por lo tanto es resoluble en Q_p y esto muestra que la forma $\langle 1,1,1,1 \rangle$ es isótropa. Se sigue de la teoría elemental de formas cuadráticas que podemos escribir la isometría.

$$\langle 1,1,1,1 \rangle \cong \langle 1,-1,1,-1 \rangle$$

y dado que para cualquier escalar $a \neq 0$ es $\langle a, -a \rangle \cong \langle 1, -1 \rangle$, resulta la isometría utilizada en la demostración del Teorema de Bruck y Ryser, a saber $\langle 1,1,1,1 \rangle \cong \langle n,n,n,n \rangle$.

Nota Bibliográfica: El tema de Geometrías Finitas se puede consultar en el libro ya citado de Dembowski. Esta es una obra de índole enciclopédico. También aconsejamos el clásico libro de **Marshall Hall,** Jr. Combinatorial Theory, Balisdell Pub. (1967). El libro Projective Planes de **D. R. Hughes y F. C. Pipes** constituye una buena introducción a la teoría moderna de planos no–desarguianos. Para leer sobre cuadrados latinos consultar **J. Denes y A. D. Keedwell** Latin Squares and their applications, Academic Press (1974). Consultar también, **W. W. Rouse Ball,** Mathematical Recreations and Essays, Macmillan, Londres (1939).