Geometrías Finitas con Cuerpos Finitos y Cuadrados Latinos

Orlando Galdames Bravo

6 de abril de 2010

1. Un poco de historia
   - Orígenes
   - Geometría con cuadrados Latinos
   - Más cosas con cuadrados Latinos
2. Cuadrados Latinos
   - Propiedades de los cuadrados Latinos
   - Cuerpos de Galois
   - Cuadrados Latinos mutuamente ortogonales
3. Geometrías finitas
   - Introducción
   - Planos finitos
   - Geometrías finitas y cuadrados Latinos
   - Ejemplo de geometría finitas
4. Bibliografía

Cuadrados Latinos
Definición

Definición (Euler, 1776)

Un cuadrado Latino es una tabla $n \times n$ de n elementos, en la que estos aparecen una vez en cada fila y una vez en cada columna.

Cuadrados Latinos

Euler

Adivinanza (Euler, 1779/1782)

¿Es posible ordenar 6 compañías, cada una con 6 oficiales de distinto rango en una formación 6×6 de manera que no se repitan rangos o compañías en una columna o en una fila?

Solución: $^{\cdot o}N$

Conjetura

Euler responde que no es posible y además dice que tampoco lo es para ningún cuadrado de orden n si $n \equiv 2 (mod\ 4)$.

Cuadrados Latinos

Euler

Definición (Cuadrado Latino (Euler, 1782))

Dos cuadrados Latinos son ortogonales si al superponerlos generan una tabla con todos sus elementos distintos.

Ejemplo (Cuadrados Latinos ortogonales)

Dados dos cuadrados Latinos

$$\begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \quad y \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \quad \text{superponiéndolos:} \quad \begin{pmatrix} a1 & b2 & c3 \\ c2 & a3 & b1 \\ b3 & c1 & a2 \end{pmatrix}$$

No se repite ningún elemeno en la superposición por tanto son ortogonales

Adivinanza de Euler: ¿existen cuadrados Latinos ortogonales de orden 6?

Geometría con cuadrados Latinos

Algunos resultados destacados

- En 1890, A. Cayley demuestra que la tabla de multiplicar de un grupo es un cuadrado Latino.
- En 1901, G. Tarry responde, mediante un eshaustivo trabajo combinatorio sobre de cuadrados Latinos de orden 6, que Euler tenía razón en su adivinanza.
- En 1906, O. Veblen y W. Bussey demuestran, usando cuerpos finitos de Galois, que existen planos proyectivos de orden potencia de un primo.
- En 1938, R. C. Bose muestra cómo construir cuadrados Latinos de orden potencia de un primo usando también cuerpos de Galois. Además relaciona los cuadrados Latinos con las geometrías finitas.
- En 1959, R. C. Bose y S. S. Shrikhande demuestran que es posible construir cuadrados Latinos de orden $4t + 2$ para $t \geq 5$.
- Finalmente en 1960 R. C. Bose, S. S. Shrikhande y E. T. Parker demuestran que existen cuadrados Latinos ortogonales de orden $n > 6$.

Cuadrados Latinos
Aplicaciones

Hoy en día los cuadrados Latinos se utilizan en diversas áreas de la matemática.

- Para el diseño de experimentos en estadística.
- Ayuda a demostrar la coloración de ciertos tipos de grafos.
- En el estudio de grupos y otras estructuras como casi-grupos, semigrupos y grupoides.
- Generación de códigos de corrección de errores en ciencias de la información y la computación.
- Rompecabezas matemáticos: Sudoku, Kenken, Futoshiki, Cuadrados Mágicos. . .
- Demuestran la existencia de geometrías finitas como veremos.
- La generalización a hipercubos latinos se utiliza en estadística y en métodos numéricos.

Cuadrados Latinos
Propiedades

Propiedad (1)

La tabla de multiplicar de un grupo es un cuadrado Latino.

Demostración:
Supongamos que

$$x_i x_j = x_i x_k,$$

multiplicando por a izquierda

$$-x_i,$$

tenemos que

$$x_j = x_k.$$

□

Cuadrados Latinos
Propiedades

Propiedad (2)

Existen cuadrados Latinos de cualquier orden natural.

Demostración:
Tomando como conjunto base $(\mathbb{Z}_n, +)$ que es grupo, luego su tabla de Cayley es un cuadrado Latino. □

Cuadrados Latinos
Propiedades

Propiedad (3)

Si permutamos filas o columnas seguimos obteniendo un cuadrado Latino.

Demostración:
Sea σ_f una permutación de sus filas y σ_c de sus columnas,

permutando filas y columnas de (L_{ij}) obtenemos

$$(L_{\sigma_f(i)\sigma_c(j)}),$$

si tenemos que

$$L_{\sigma_f(i)\sigma_c(j)} = L_{\sigma_f(i)\sigma_c(k)},$$

Cuadrados Latinos
Propiedades

σ_f está bien definida, luego podemos tomar $p = \sigma_f(i)$,

$$L_{p\sigma_c(j)} = L_{p\sigma_c(k)}$$

como (L_{ij}) es cuadrado Latino tenemos que

$$\sigma_c(j) = \sigma_c(k).$$

□

Observación: Dado el conjunto de cuadrados latinos de orden n, se puede definir la acción del grupo de permutaciones sobre este conjunto. Recientemente los autores Hulpke, Kaski y Östergärd han usado esta propiedad para el cálculo del número de Cuadrados Latinos de orden 11.

Cuerpos de Galois
Algunas propiedades

Teorema (Galois)

Un cuerpo finito tiene q elementos, donde q es la potencia de un primo.

Demostración:
Sea K el cuerpo finito de orden q.

Sea el homomorfismo de anillos $f : \mathbb{Z} \to K$ definido como $f(n) := n\varepsilon$, donde ε es la unidad de K.

Por el teorema de isomorfía tenemos que $\mathbb{Z}/m\mathbb{Z} \cong \text{Im}f \subseteq K$ para algún m entero,

por otro lado $\text{Im}f$ es un dominio, luego m debe ser un primo p.

Cuerpos de Galois
Algunas propiedades

Por tanto

$$\mathrm{Im} f = \{0, 1\varepsilon, \ldots, (p-1)\varepsilon\} \cong \mathbb{Z}_p\,,$$

y $p = |\,\mathrm{Im} f|$, luego $\mathrm{Im} f$ no puede tener subcuerpos, luego debe ser primo.

Veamos que el orden es $|K| = p^n$.

Supongamos que hay dos primos p y q que dividen a $|K|$.

Por el teorema de Cauchy para grupos abelianos existen dos elementos a y b de órdenes p y q respectivamente.

Cuerpos de Galois
Algunas propiedades

Luego $(p\varepsilon)a = 0 = (q\varepsilon)b$,

y como K es cuerpo

$$p\varepsilon = q\varepsilon = 0\,.$$

Por otro lado $(p, q) = 1$, luego por Bézout tenemos que $rp + sq = 1$ para $r, s \in \mathbb{Z}$,

y así $\varepsilon = r(p\varepsilon) + s(q\varepsilon) = 0$, lo que es una contradicción. $\square$

NOTA: El cuerpo de orden p^n es único y se denota por $\mathrm{GF}(q)$.

Cuerpos de Galois
Algunas propiedades

Otras propiedades útiles:

- Para todo punto $x \in \mathrm{GF}(q)$ tenemos que $x^q = x$.
- Si p es primo $\mathrm{GF}(p) \cong \mathbb{Z}/\mathbb{Z}_p$.
- El cuerpo finito $\mathrm{GF}(p^m) \cong \mathrm{GF}(p)[x]/(f(x))$ donde $f \in \mathrm{GF}(p)[x]$ es un polinomio de grado m irreducible sobre $\mathrm{GF}(p)$.
- El primo p es la caracterísitica del cuerpo $\mathrm{GF}(p^h)$.
- $\mathrm{GF}(p^r)$ es subcuerpo de $\mathrm{GF}(p^h)$ si y sólo si r divide a h.

Para demostrarlas se puede consultar el libro de Robert B. Ash o el de Joseph J. Rotman.

Cuadrados Latinos
Más propiedades

Definición (Cuadrados mutuamente ortogonales)

Si $L_1, \ldots, L_r$ son cuadrados Latinos de orden n tales que L_i es ortogonal a L_j para todo $i \neq j$, entonces se llama conjunto de r cuadrados Latinos mutuamente ortogonales de orden n, o en inglés MOLS.

Teorema (Existencia de cuadrados mutuamente ortogonales)

Existe un conjunto de $n-1$ cuadrados Latinos mutuamente ortogonales de orden n, donde n es potencia de un primo.

Demostración:
Definimos nuestro conjunto base: GF(n) con $n = p^m$, p primo y m natural no cero.

GF(n) $= \{x_0, \ldots, x_{n-1}\}$ donde $x_0 = 0$ y $x_1 = 1$.

Cuadrados Latinos
Más propiedades

Definimos $L_k = (L_{ij}^k) = (x_k x_i + x_j)$ para $k = 1, \ldots, n-1$.

Pregunta: ¿ $L_{ij}^k - L_{il}^k = (x_k x_i + x_j) - (x_k x_i + x_l) = 0$?

sumando $x_k x_i$ a la izquierda

La pregunta queda: ¿ $x_j - x_l = 0$?

que se cumple sii $x_j = x_l$, es decir sii $j = l$.

Luego sii son cuadrados latinos.

Veamos que $\{L_1, \ldots, L_{n-1}\}$ es un conjunto de MOLS:

Supongamos $(L_{ij}^k, L_{ij}^l) = (L_{pq}^k, L_{pq}^l)$, con $k \neq l$, entonces planteamos la siguiente ecuación

Cuadrados Latinos
Más propiedades

$$\begin{cases} x_k x_i + x_j &= x_k x_p + x_q \\ x_l x_i + x_j &= x_l x_p + x_q \end{cases} \quad (1)$$

Restandolas

$$(x_k - x_l)(x_i - x_p) = 0,$$

Como GF(n) es cuerpo, no tiene divisores de 0 así que:

$$x_k = x_l \text{ o } x_i = x_p,$$

es decir

$$k = l \text{ o } i = p.$$

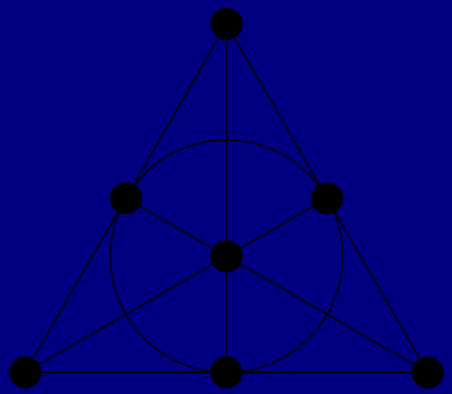
Como $k \neq l$, $i = p$ entonces $j = q$ por ser L^k y L^l cuadrados latinos o también por las ecuaciones (1). □

Geometrías Finitas

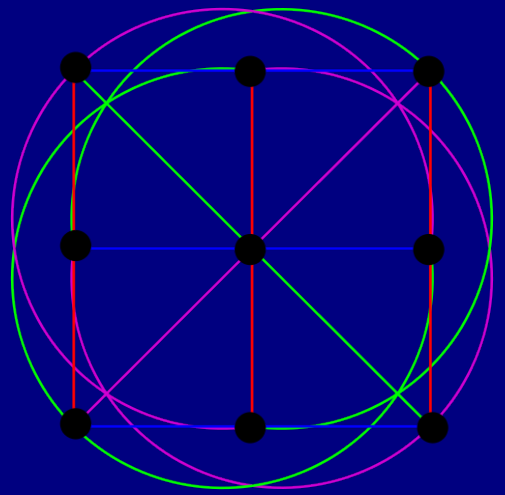
Introducción

Geometría para un conjunto finito que se define axiomáticamente.

Existencia:	Cuadrados Latinos.	Cuerpos de Galois.
Construcción:	Cuerpos de Galois.	Sistemas de Steiner.



Plano de Fano (1892). PG(2,2)



Plano afín de 9 puntos. AG(2,3)

El plano proyectivo
Definición

Definición

Un plano proyectivo es un conjunto de puntos $\mathcal{P}$, con un conjunto $\mathcal{L}$ de subconjuntos de $\mathcal{P}$, llamadas lineas. Cumpliendo los siguientes axiomas:

1. *Dos puntos inciden en una única linea.*
2. *Dos lineas inciden en un único punto.*
3. *Hay al menos cuatro puntos, de los cuales tres son no colineales.*

Propiedad

Todos los elementos de $\mathcal{L}$ tienen el mismo cardinal.

Si a este cardinal le restamos 1 lo llamamos orden del plano proyectivo. El plano proyectivo de orden q se denota por $\mathrm{PG}(2, q)$.

Geometrías finitas
Propiedades

Demostración. (Propiedad)
Sean P un punto y l una linea del plano proyectivo,

por los dos primeros axiomas P incide con tantas lineas como l incide con puntos.

Si P' está en l, por el primer axioma P' y P inciden en una única linea.

Si l' pasa por P, por el segundo axioma l' y l inciden en un único punto.

Por el tercer axioma existe $Q \neq P$ que no está en l,

por lo mismo tenemos que l tiene tantos puntos como lineas que inciden con Q,

que coincide con el número de lineas que inciden en P. $\square$

Geometrías finitas
Propiedades

Propiedad

El plano proyectivo de orden n tiene $n^2 + n + 1$ lineas y puntos.

Demostración:
Por definición de orden, sabemos que para un punto tenemos $n + 1$ lineas incidentes,

y como cada una tiene $n + 1$ puntos, éstas incidirán en otros n puntos.

Por tanto en el plano proyectivo tenemos $n(n + 1) + 1 = n^2 + n + 1$ puntos,

que ya hemos visto que coincide con el número de lineas. □

El plano afín
Definición

Definición

Un plano afín es un conjunto de puntos $\mathcal{P}$, con un conjunto $\mathcal{L}$ de subconjuntos de $\mathcal{P}$, llamadas lineas. Cumpliendo los siguientes axiomas:

1. *Dos puntos inciden en una única linea.*
2. *Para cada linea l y un punto no incidente a ella, existe una única linea l' que contiene al punto y tal que $l \cap l' = \emptyset$.*
3. *Hay al menos tres puntos no colineales.*

El plano afín de orden q se denota por $\mathrm{AG}(2, q)$.

Definición

Sean m y l lineas de un $AG(2, q)$, diremos que son paralelas si $m \cap l = \emptyset$ o si $m = l$. La relación de paralelismo es de equivalencia.

Geometrías finitas

Relación entre el plano proyectivo y el afín

Dado el plano afín $\mathrm{AG}(2, q)$ podemos construir el proyectivo $\mathrm{PG}(2, q)$.

- $\mathcal{P}$ puntos de $\mathrm{AG}(2, q)$.
- $\mathcal{L}$ lineas de $\mathrm{AG}(2, q)$.
- $\mathcal{E}$ clases de equivalencia paralelas.

Definimos $l_+ = l \cup [l]$ y $l_\infty = \{[l] : [l] \in \mathcal{E}\}$.

Donde el conjunto de puntos es

$$\mathcal{P} \cup \mathcal{E}$$

y el de lineas

$$\{l_+ : l \in \mathcal{L}\} \cup \{l_\infty\}$$

es un plano proyectivo.

Geometrías finitas

Relación entre el plano proyectivo y el afín

Demostración:

1. - Si $x, y \in \mathcal{P}$, entonces $\exists!$ l tal que $x, y \in l$, por tanto $x, y \in l_+$.
   - Si $x \in \mathcal{P}$ y $[l] \in \mathcal{E}$, $\exists!$ l' tal que $l \cap l' = \emptyset$, es decir, son paralelas, y por tanto $[l] = [l']$, luego $x, [l] \in l'_+$.
   - Si $[l], [l'] \in \mathcal{E}$ entonces $[l], [l'] \in l_\infty$.
   La unicidad se deduce de la unicidad de l y l'.
2. Sean l_+ y l'_+ tales que $l_+ \neq l'_+$. Puede ocurrir que l y l' sean paralelas, entonces l_+ y l'_+ se cortan en $[l] \in \mathcal{E} \subset {}_+$, si no son paralelas, entonces $\exists\, x \in l \cap l'$, luego $x \in l_+ \cap l'_+$.
   Veamos la unicidad: denotamos α al punto de corte, si $\exists\, \beta \in l_+ \cap l'_+$ con $\alpha \neq \beta$, entonces $\exists!$ l''_+ tal que $\alpha, \beta \in l''_+$, es decir $\alpha, \beta \in l''_+ \cap l'_+ \cap l_+$, por unicidad $l'_+ = l_+$, lo que es una contradicción. Por otro lado l_+ y l_∞ sólo se pueden cortar en $[l]$.
3. Sabemos que hay tres puntos no colineales, y hemos añadido las clases de lineas paralelas, como hay más de una linea, hay más de una clase, luego tenemos más de tres puntos en $\mathcal{P} \cup \mathcal{E}$.

Geometrías finitas

Relación entre el plano afín y el proyectivo

Recíprocamente:

Si al plano proyectivo $\mathrm{PG}(2, q)$ le quitamos una linea y todos los puntos incidentes en ella, obtenemos un plano afin.

Habitualmente la linea eliminada se le llama línea del infinito.

Propiedad

El plano afín de orden n tiene $n^2 + n$ lineas y n^2 puntos.

Sabemos que el plano proyectivo tiene $n^2 + n + 1$ lineas y puntos,
luego si quitamos una linea nos quedan $n^2 + n$,
y si quitamos los $n + 1$ puntos de esta linea nos quedan n^2.

Geometrías finitas
Existencia

Teorema

Existe un plano afín de orden n si y sólo si existen $n-1$ cuadrados Latinos de orden n mutuamente ortogonales.

Esquema para la demostración:

- La idea es configurar un sistema de coordenadas.
- Se toman dos rectas que se cruzan en un punto que llamamos origen.
- El resto de puntos se etiquetan de 1 a $n-1$ en ambas rectas.
- Cada punto del sistema será un punto del plano afín y viceversa.
- En total hay n^2 puntos todos con distintas coordenadas.
- Tenemos una malla con dos cuadrados latinos superpuestos.
- Como los puntos son distintos, además son ortogonales.
- Hay $n-1$ clases paralelas, luego hay $n-1$ cuadrados ortogonales.

Geometrías finitas
Existencia

Corolario

Existe un plano proyectivo de orden n si y sólo si existen n cuadrados Latinos de orden $n+1$

Corolario

Existen planos afines de orden n para n potencia de un primo.

Geometrías finitas

Ejemplo

Veamos cómo construir un plano afín de orden finito utilizando cuerpos finitos.

El conjunto base será el de GF(7), es decir, las siguiente clases:

$$\{0, 1, x, x^2, x^3, x^4, x^5\}$$

Busquemos las lineas.

Por la teoría sabemos que deben ser lineas de 7 puntos.

Resolvemos la ecuación lineal con incógnitas y y x

$$y \equiv \alpha x + \beta (\text{mod } 7)$$

donde $\alpha, \beta \in$ GF(7). Veamos cómo resolverla.

Geometrías finitas

Ejemplo

Algoritmo de Euclides para la división y p primo

$$y = cp + r \ ,$$

donde c es el cociente, p el módulo y r el resto.

Entonces

$$\alpha x + \beta = cp + r \ ,$$

la solución nos la dará el resto.

Despejando:

$$r = \alpha x + \beta - cp \ .$$

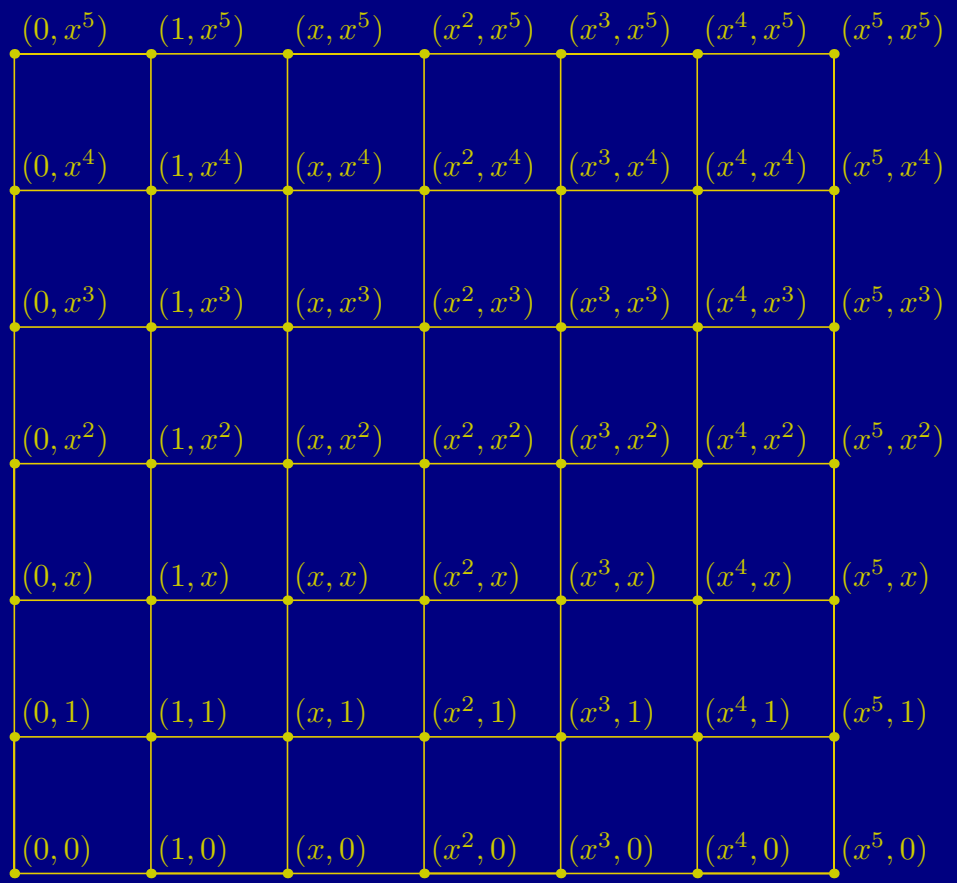
Los puntos que buscamos son los

$$(x, r) \quad \text{para} \quad x = 0, \ldots, p-1 \ .$$

Geometrías finitas

Ejemplo

Disponemos los puntos de GF(7) en una tabla como en el teorema



Geometrías finitas
Ejemplo

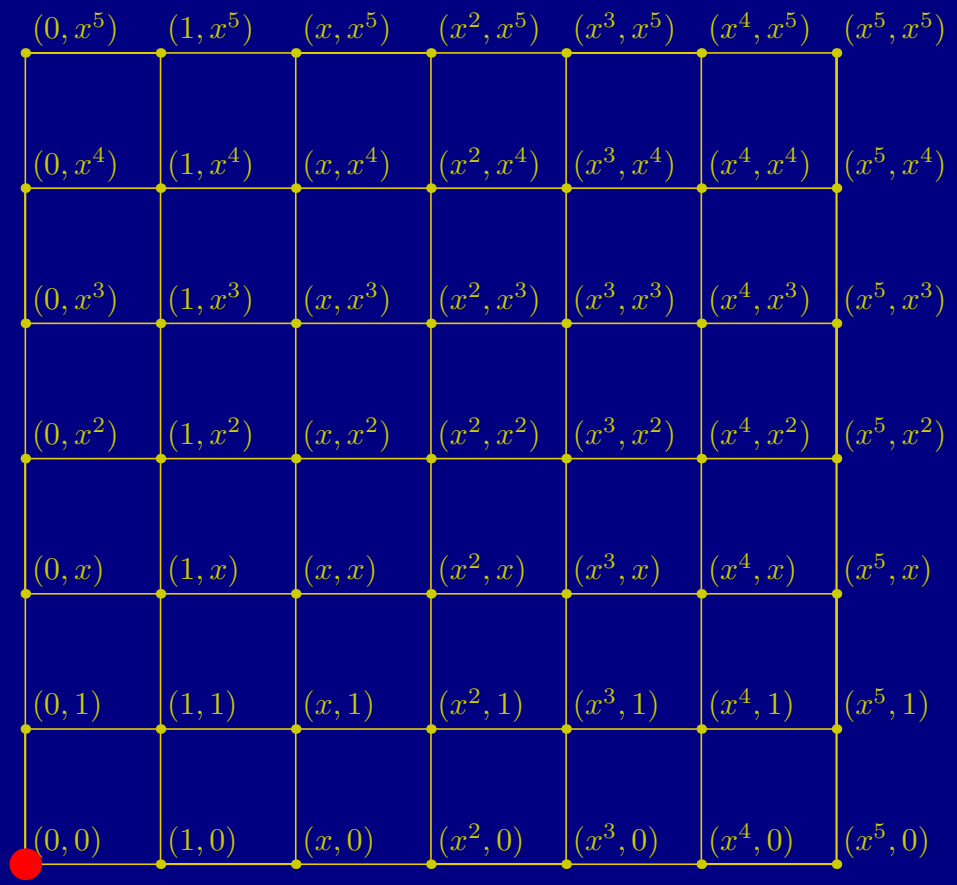
Aplicando el algoritmo en metapost:

```
for i=0 upto n-1:

    resto:=0;
    j:=a*i+b;
    restaux:=j;

    if j<n:
        if j>=0:
            resto:=j;
        else:
            co:=0;
            forever: exitunless restaux<0;  ----> %equivale a un "do while"
                co:=co-1;
                restaux:=j-co*n; ---> %Algortimo de Euclides
                resto:=restaux;
            endfor
        fi
    else:
        co:=0;
        forever: exitunless restaux>n-1;
            co:=co+1;
            restaux:=j-co*n; ---> %Algortimo de Euclides
            resto:=restaux;
        endfor
    fi

    draw (i*u,resto*u) withpen pencircle scaled 6pt withcolor(0,0,1);
endfor;
```

Geometrías finitas

Ejemplo

$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

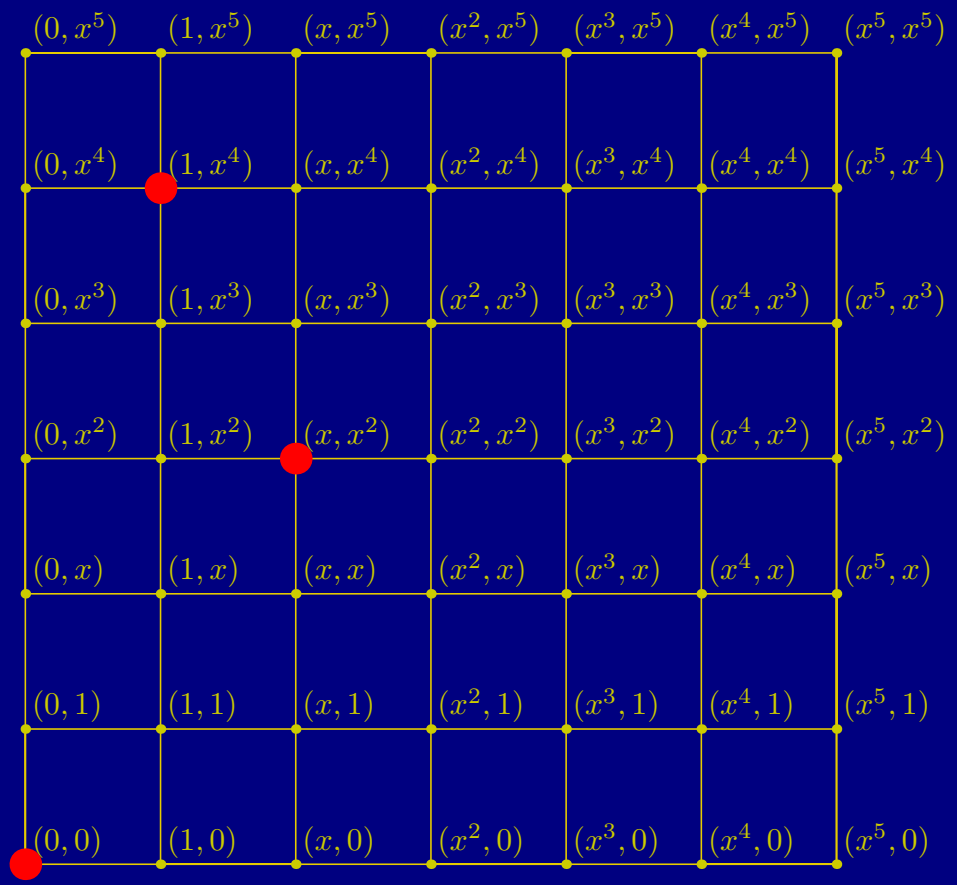
Ejemplo

$$p \equiv 5q + 56 (\text{mod } 7)$$

Geometrías finitas

Ejemplo

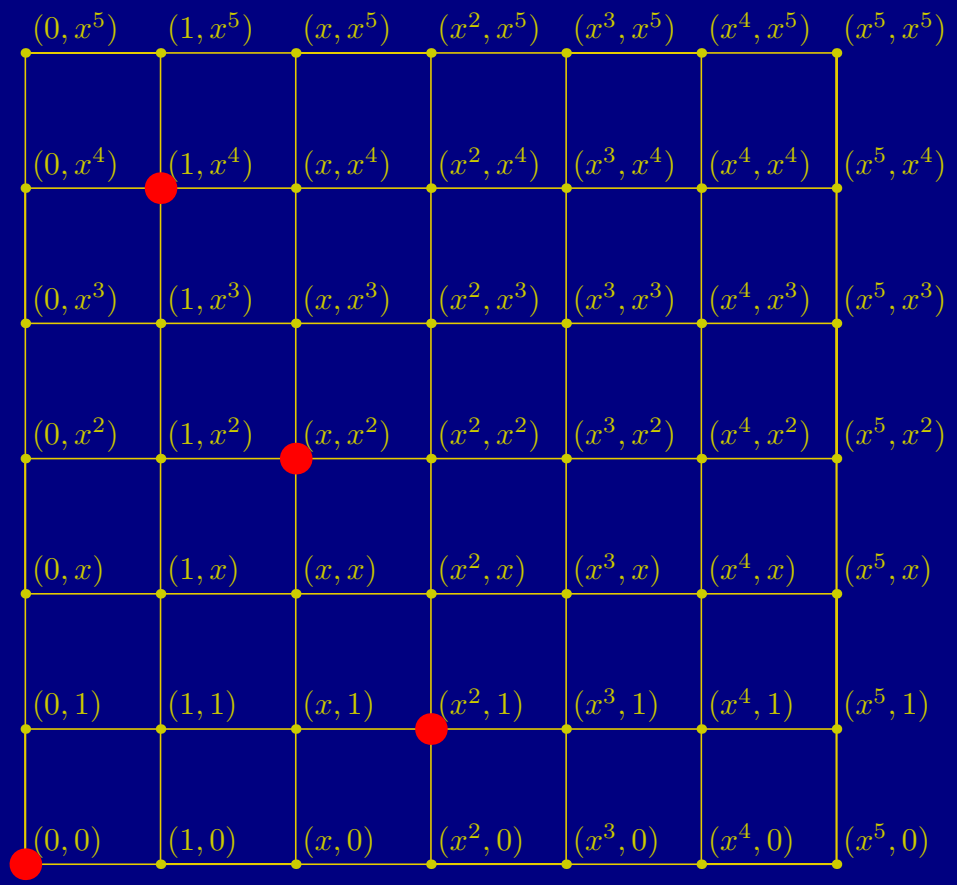
$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

Ejemplo

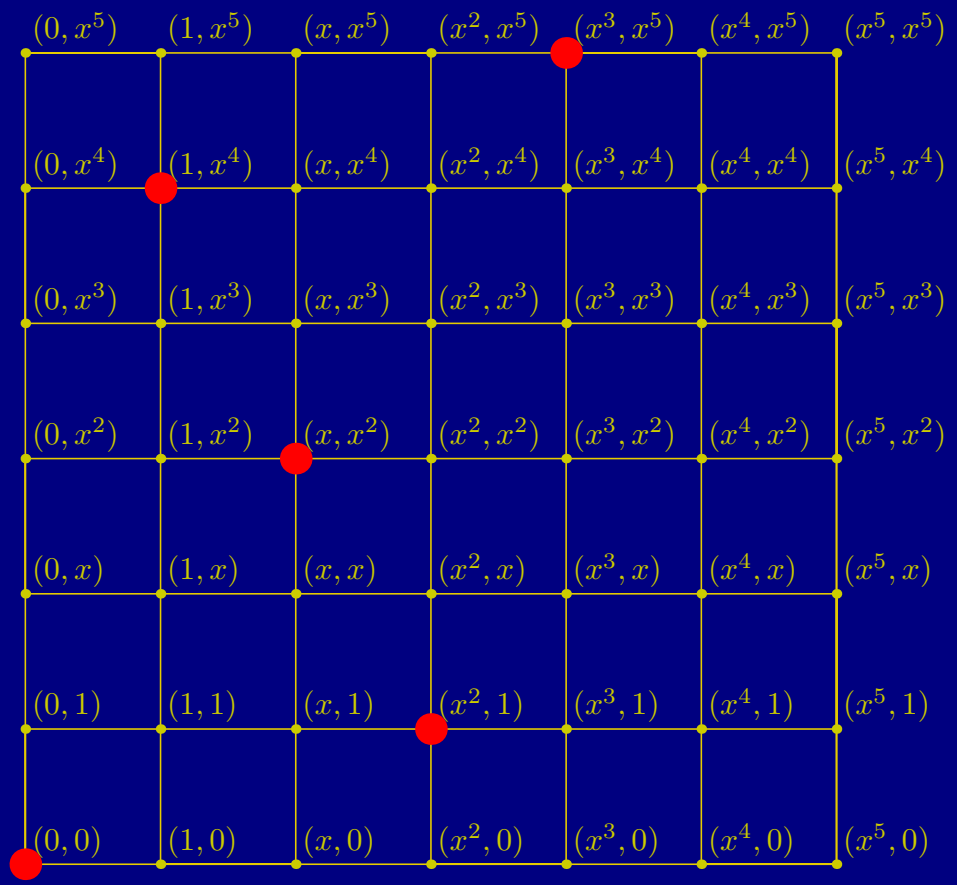
$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

Ejemplo

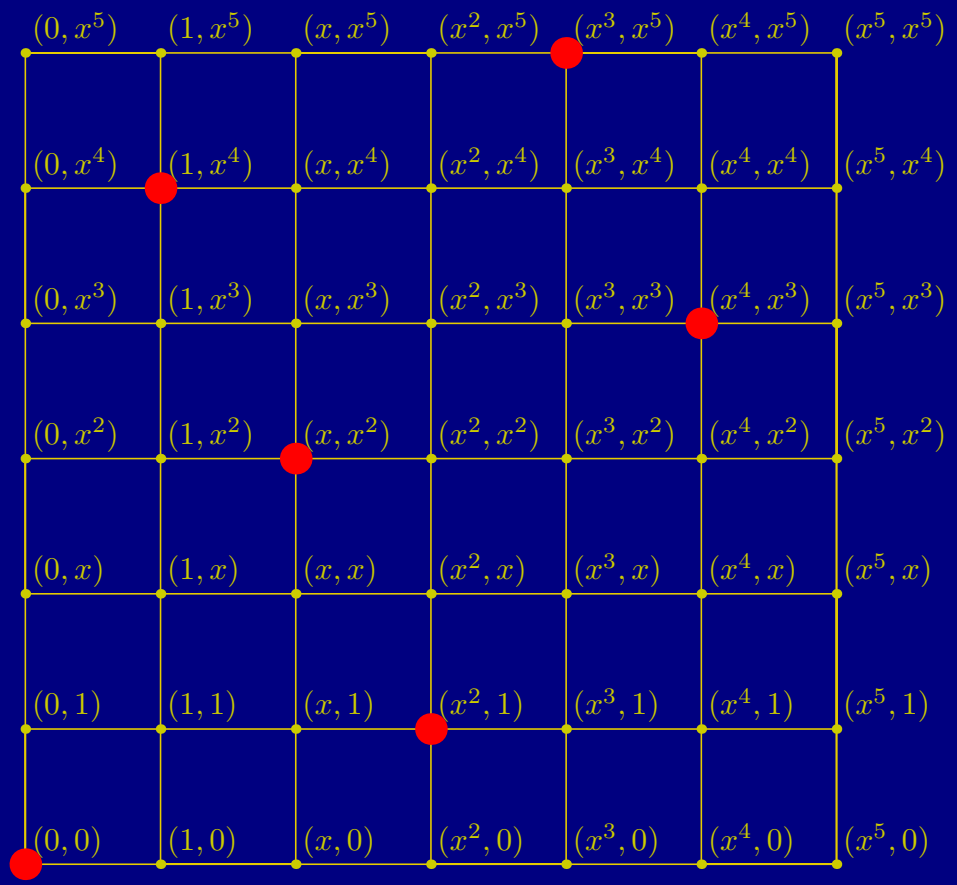
$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

Ejemplo

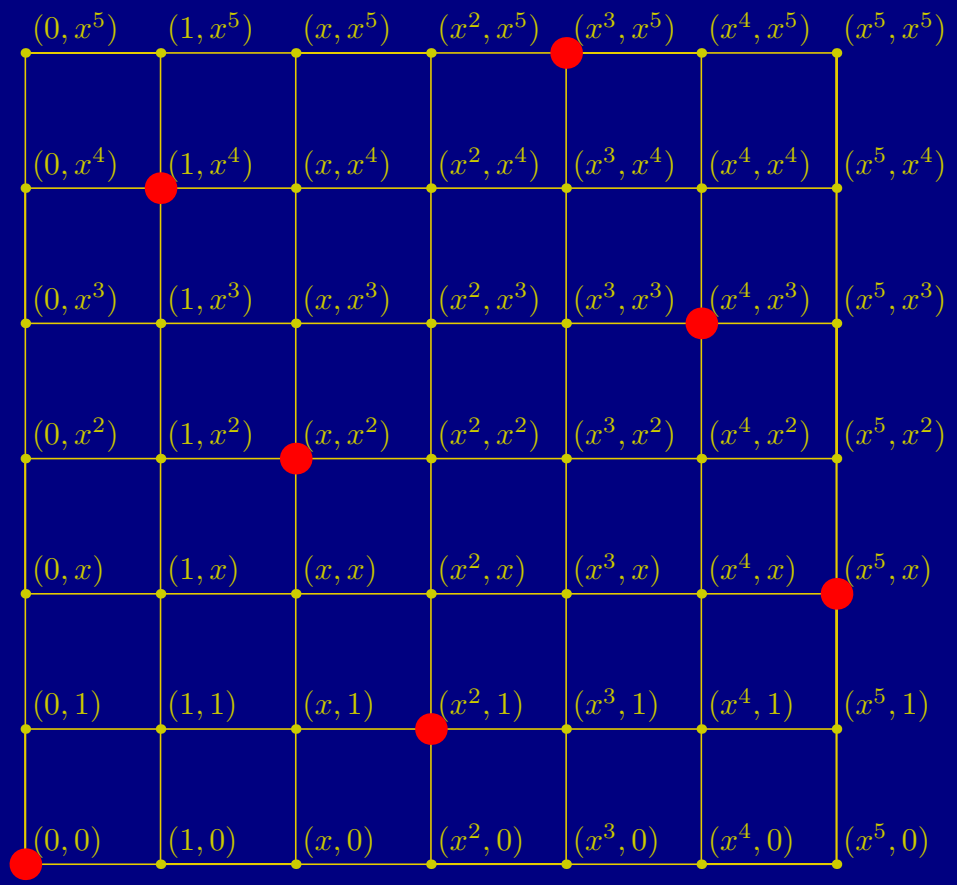
$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

Ejemplo

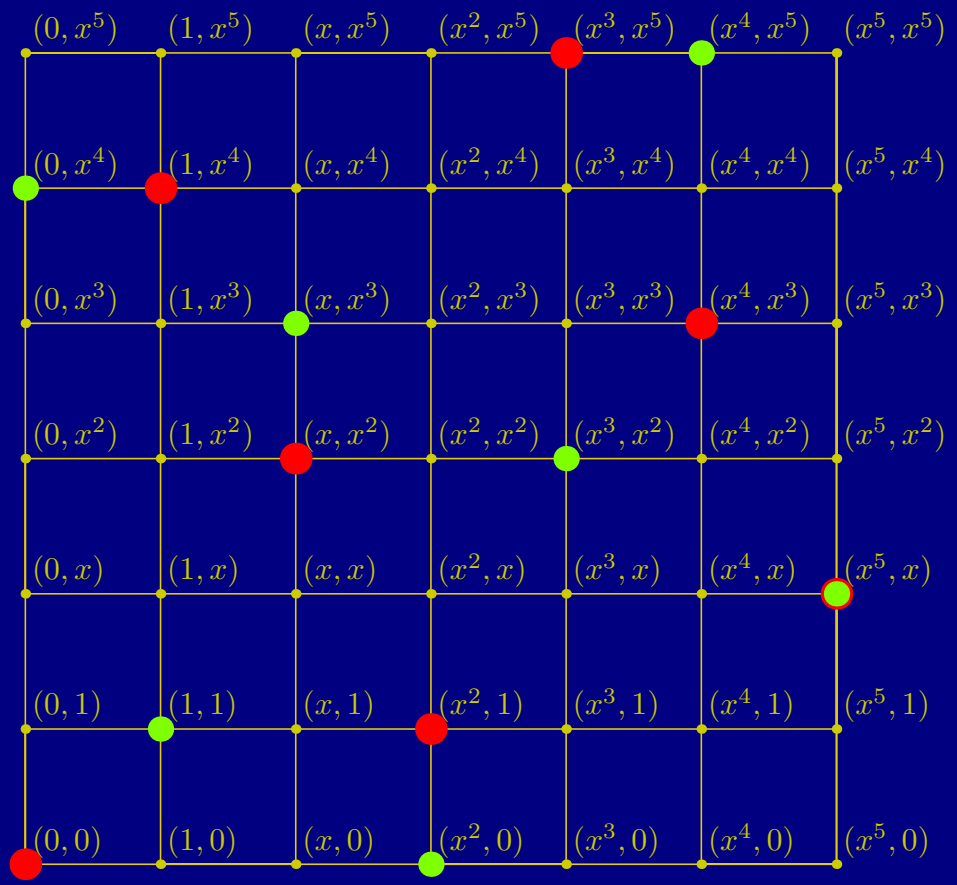
$$p \equiv 5q + 56 (\text{mod } 7)$$



Geometrías finitas

Ejemplo

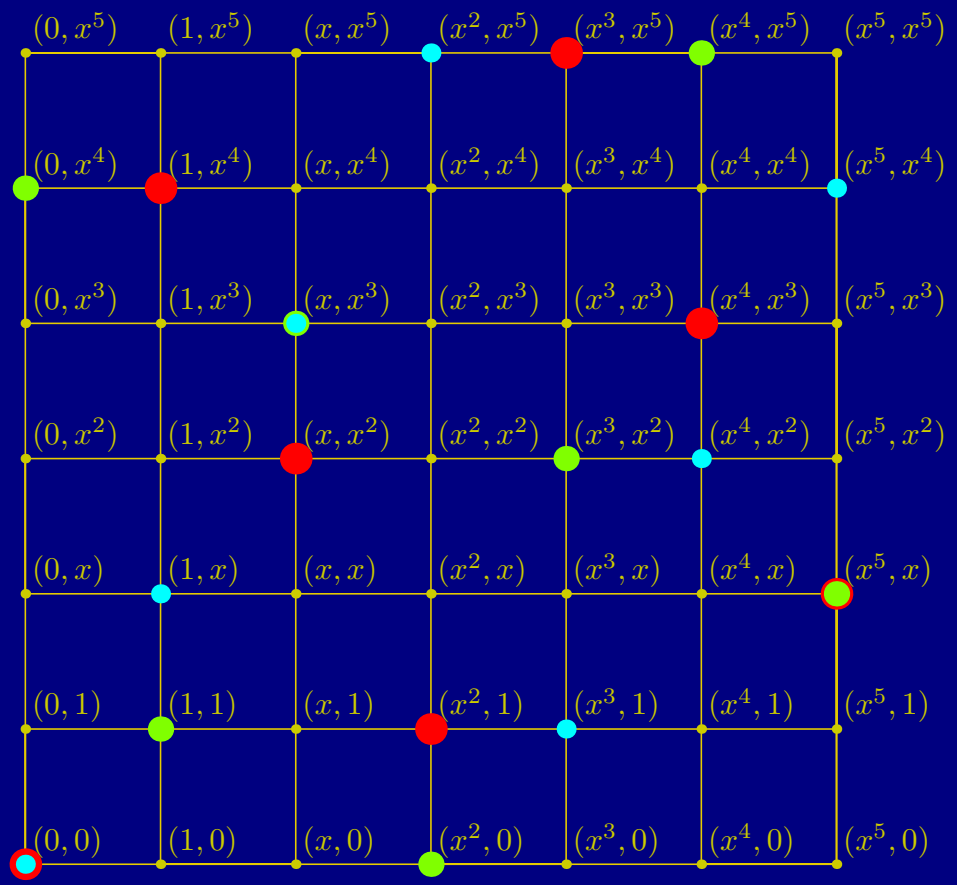
$p \equiv 5q + 56 (\text{mod } 7)$ $\quad$ $p \equiv -81q - 23 (\text{mod } 7)$



Geometrías finitas

Ejemplo

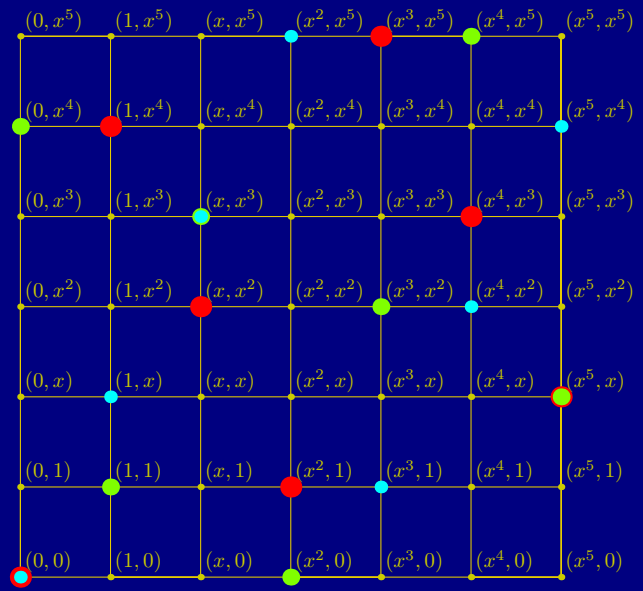
$p \equiv 5q + 56 (\text{mod } 7)$ $p \equiv -81q - 23 (\text{mod } 7)$ $p \equiv 37q - 21 (\text{mod } 7)$



Geometrías finitas

Ejemplo

$p \equiv 5q + 56 (\text{mod } 7)$ $p \equiv -81q - 23 (\text{mod } 7)$ $p \equiv 37q - 21 (\text{mod } 7)$



- Ninguna de las lineas es paralela.
- Todas se cortan en un único punto.
- Si unimos los puntos con rectas paralelas obtenemos diversas rectas con pendientes iguales módulo 7.
- Hemos dibujado un triángulo.

Geometrías finitas

Ejemplo

Consideraciones para un algoritmo en base a $\mathrm{GF}(p^n)$.

En el caso de orden primo hemos usado que $\mathrm{GF}(p) \cong \mathbb{Z}_p$.

Ahora debemos utilizar que $\mathrm{GF}(p^n) \cong \mathbb{Z}[x]/(f(x))$, donde $f(x)$ es irreducible en $\mathbb{Z}[x]$.

Lo más complicado es idear las tablas de sumar y de multiplicar, existe amplia documentación para construir los cuerpos $\mathrm{GF}(p^n)$.

Se sabe que el cuerpo que resulta no depende del polinomio $f(x)$, pero la complejidad para el cálculo sí depende de la elección de $f(x)$.

Una vez tenemos las tablas aplicamos el algoritmo que conocemos para estas tablas módulo p.

Para la construcción de $\mathrm{GF}(p^n)$ consultar el libro de Ash o el de Rotman.

Geometrías Finitas

Introducción

Ejemplo de tablas para GF(3^2).

×	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

+	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Bibliografía

Para realizar este trabajo

- Modern Algebra with Applications
  W. Gilbert, Wiley, New York, 1976.
- Mathematicas Recreations and Essays
  W. W. Rouse Ball and H. S. M. Coxeter, Dover Publications, Inc., New York, 1987.
- Advanced Modern Algebra
  Joseph J. Rotman, Prentice Hall, 2003.
- Abstract Algebra: The Basic Graduate Year
  Robert B. Ash, University of Illinois, 2000.
- An Introduction to Finite Geometry
  Simeon Ball and Zsuzsa Weiner, Universitat Politècnica de Catalunya, 2003.

Referencias
Artículos


Finite Geometry
Chris Godsil, Combinatorics & Optimization, University of Waterloo, 2004.


De quadratis magicis
Leonhard Euler, Charla impartida en la Academia de Ciencias de San Petersburgo en octubre de 1776, Leonhardi Euleri Commentationes arithmeticae collectae, auspiciis Academiae imperialis scientiarum petropolitanae, Vol. 2, p. 593-602, 1849.


Recherches sur une Nouvelle Espece de Quarres Magiques
Leonhard Euler, Lectura en la Academia de Ciencias de San Petersburgo en marzo de 1779, Verhandelingen Zeeuwsch Genootschap der Wetenschappen, Vol. 10, p. 85-239, 1782.


On Latin Squares
Arthur Cayley, Oxford Cambridge Dublin Messenger Mathematics, Vol. 19, p. 135-137, 1890.

Referencias
Artículos


Le Problème de 36 Officiers
G. Tarry, Comptes Rendu de l'Association Française pour l'Avancement de Science Naturel, Vol. 1, p. 122-123, 1900 and Vol. 2, p. 170-203, 1901.


Finite Projective Geometries
Oswald Veblen y W. H. Bussey, Transactions of the American Mathematical Society, Vol. 7, p. 241-259, 1906.


On the Falsity of Euler's Conjecture About the Nonexistence of Two Orthogonal Latin Squares of Order 4t + 2
R. C. Bose y S. S. Shrikhande, Proceedings of the National Academy of Science, Vol. 45, p. 734-737, 1959.

Referencias

Artículos

On the Construction of Sets of Mutually Orthogonal Latin Squares and the Falsity of a conjecture of Euler
R. C. Bose y S. S. Shrikhande, Transactions of the American Mathematical Society, Vol. 95, nº 2, p. 191-209, 1960.

Further Results on the Construction of Mututally Orthogonal Latin Squares and the Falsity of Euler's Conjecture
R. C. Bose, S. S. Shrikhande y E. T. Parker, Canadian Journal of Mathematics, Vol. 12, p. 189-203, 1960.

The Number of Latin Squares of Order 11
Alexander Hulpke, Petteri Kaski y Patric R. J. Östergärd, preprint, arXiv:0909.3402v2 [math.CO], febrero 2010.

On the Number of Latin Squares
Brendan D. Mc Kay y Ian M. Wanless, Annals of Combinatorics, Vol. 9, p. 335-344, 2005.

Referencias
Artículos

Orthogonal Latin Squares
E. T. Parker, Proceedings of the National Academy of Science, Vol. 45, p. 859-862, 1959.

Geometrías finitas y espacios discretos finitos
Jesús García López, XI Encuentros de Geometría Computacional, Santander, p. 199-202, junio de 2005.

Some Comments on Philatelic Latin Squares from Pakistan
Ka Lok Chu, Simo Puntanen y George P. H. Styan, Pakistan Journal of Statistics, Vol. 25, nº 4, p. 427-471, 2009.

Latin Squares and their Partial Transversals
Nikolaos Rapanos, Harvard College Mathematics Review, Vol. 2, nº 1, p. 4-12, 2008.

Bibliografía
Ampliación Cuadrados Latinos

- Latin squares: new developments in the theory and applications
  J. Dénes y A. D. Keedwell, Ed. Elsevier Science Publishers, 1991.
- Discrete mathematics using Latin squares
  C. F. Laywine, G. L. Mullen, John Wiley & Sons, Inc., 1998.
- Latin squares and their applications
  J. Dénes y A. D. Keedwell, Akadémiai Kiadó, 1974.

Bibliografía
Ampliación Geometrías Finitas

- Finite Geometries
  Dembowski, Combinatorics & Optimization, University of Waterloo, 2004.
- Finite projective spaces of three dimensions
  J. W. P. Hirschfeld, Oxford University Press, New York, 1998.
- General Galois geometries
  J. W. P. Hirschfeld and J. A. Thas, Oxford University Press, New York, 1991.