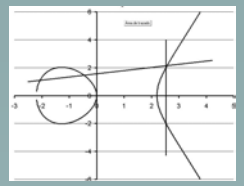
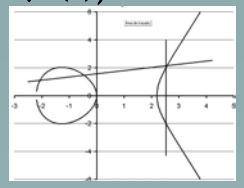


Funciones Elípticas

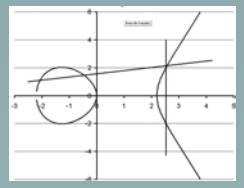
$\int r\left(x, \sqrt{p(x)}\right)dx$



Un poco de Historia

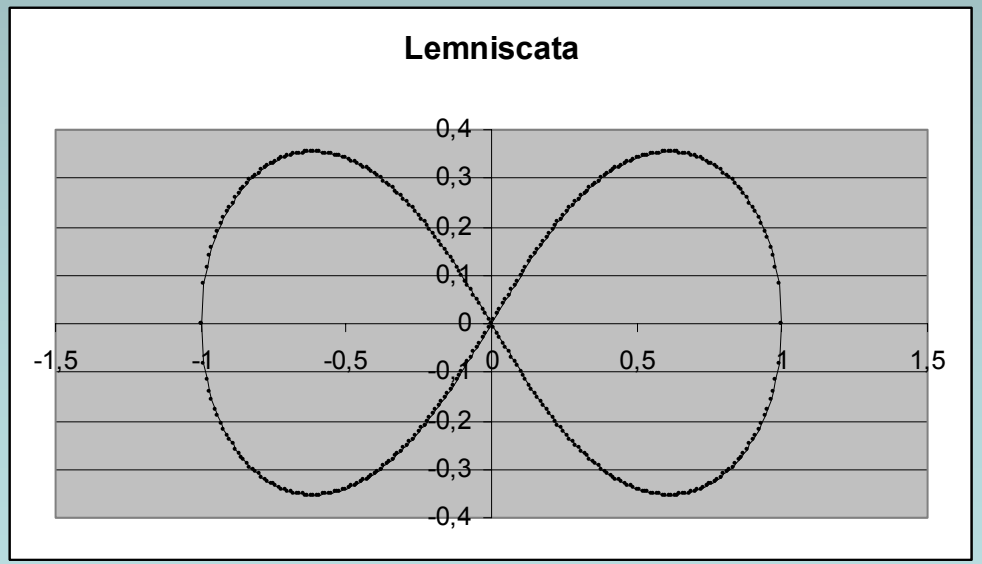
- [John Wallis, hijo del reverendo John Wallis ministro en Ashford en 1602, nació en 1617. Se hizo famoso por su capacidad de descifrar mensajes. En su libro *Tract on Conic Sections* describe las curvas que se obtienen cortando un cono con un plano.

$$\int r\left(x, \sqrt{p(x)}\right)dx$$

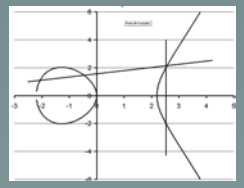


La lemniscata

Bernoulli introdujo el concepto de la lemniscata cuya ecuación es $\left(x^2+y^2\right)^2 = x^2 - y^2$



$$\int_0^x \frac{dt}{\sqrt{1-t^4}}$$



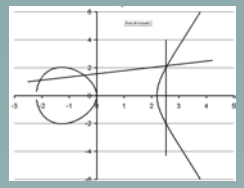
Funciones Elípticas

Forma afín de Weierstrass

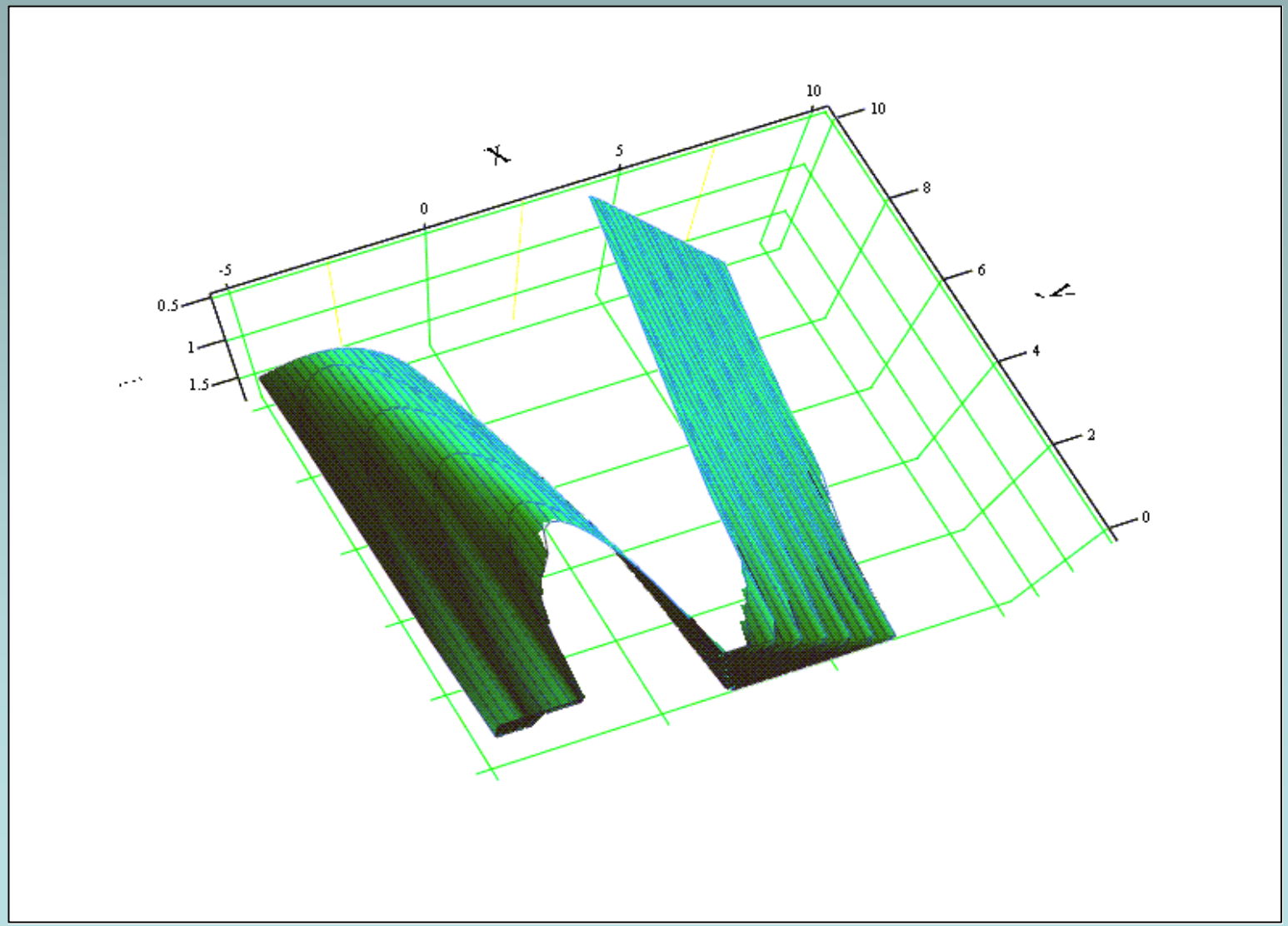
$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

Forma proyectiva

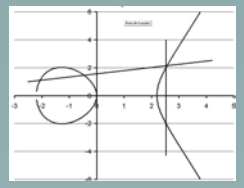
$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$



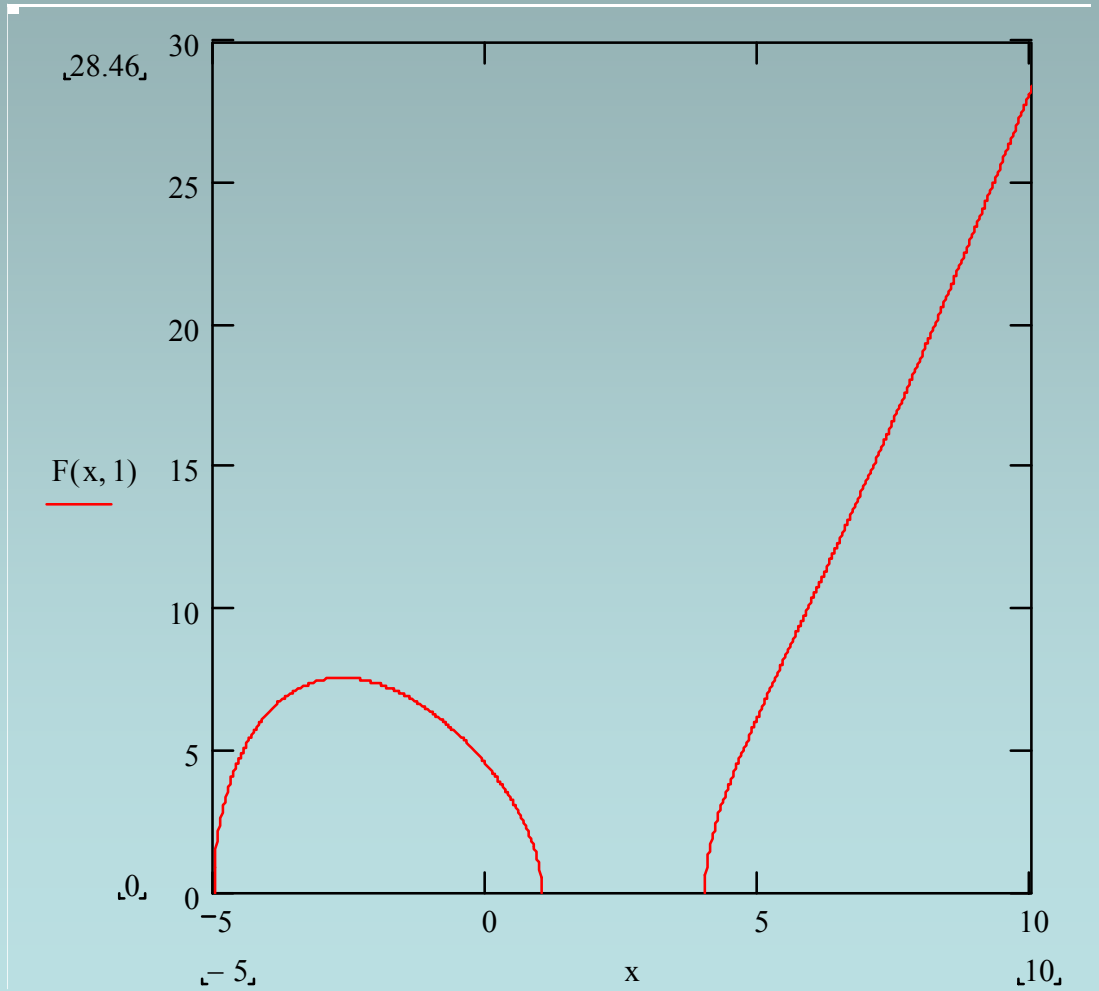
Representación proyectiva

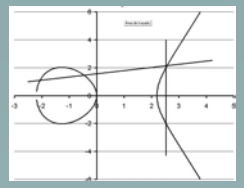


RF



Representación afín





Cambio de variables

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

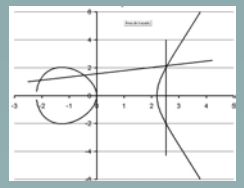
$$\downarrow$$

$$y^2 = Ax^3 + Bx^2 + Cx + D$$

$$\downarrow$$

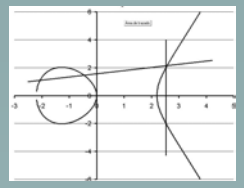
$$y^2 = x^3 + ax + b$$

$a, b, x, y \in \Re, C, Q, GF(p^n)$



Definiciones

- **C Son los complejos de la forma z = x + j y Que son algebraicamente cerrados**
- **$\Re$ Son los números reales que no son algebraicamente cerrados**
- **Q son los racionales de la forma x/y done x e y son enteros**
- **GF(p^n) Es un cuerpo finito de $q=p^n$ elementos donde p es un número primo y n un entero positivo mayor que 0**



Complejos

- Son pares ordenados (x,y) que se escriben

$$x + j\,y$$

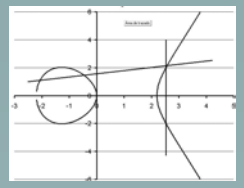
- La suma se define

$$(x_1,y_1)+(x_2,y_2)=(x_1+x_2,x_1+y_2)=x_1+x_2+j(y_1+y_2)$$

- El producto se define

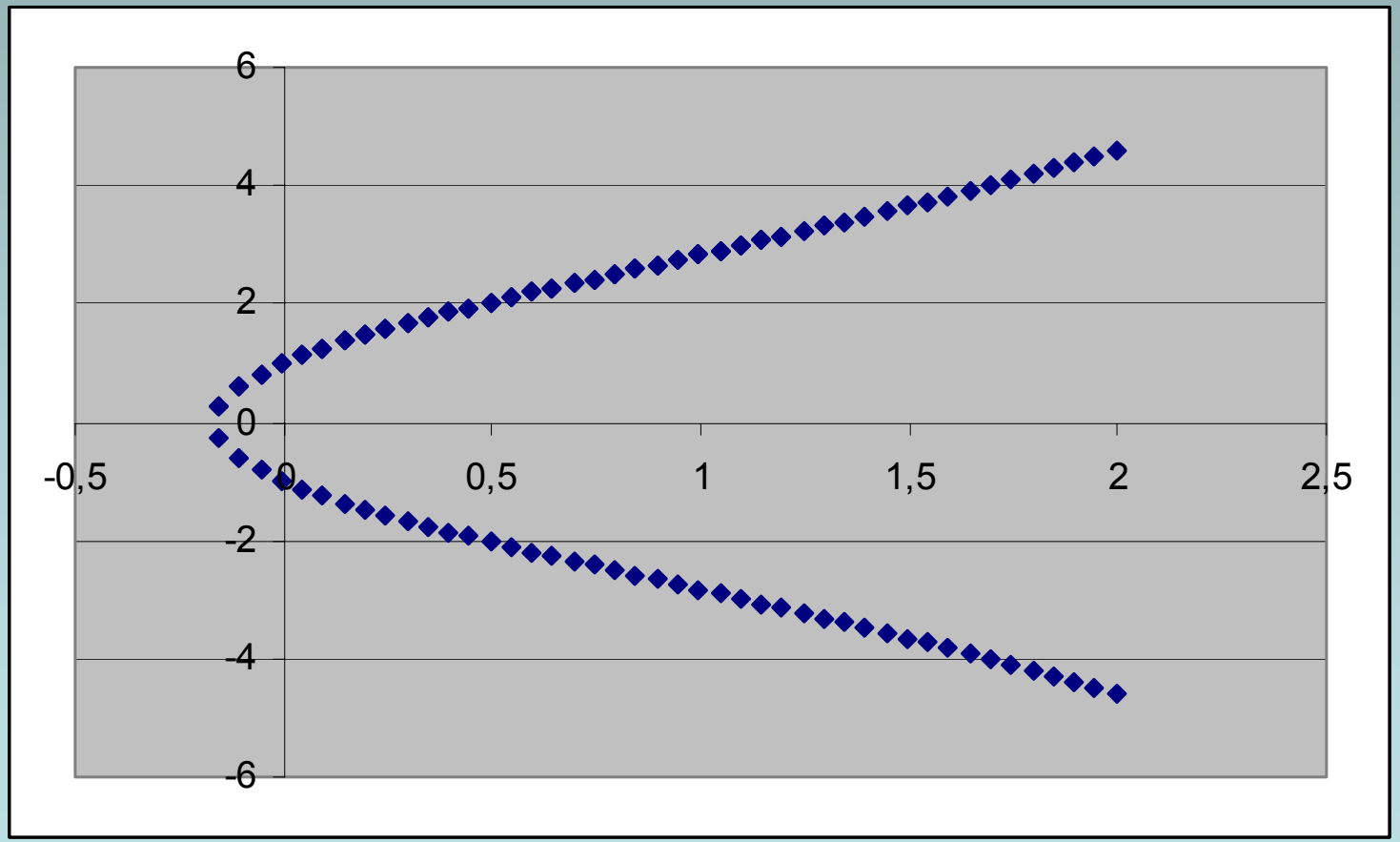
$$(x_1,y_1)\,(x_2,y_2)=(x_1x_2-y_1y_2,x_1y_2+x_2y_1)=$$
$$x_1x_2-y_1y_2+j(x_1y_2+x_2y_1)$$

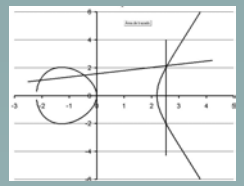
- Neutro para la suma (0,0)
- Neutro para el producto (1,0)
- Ejemplo (0,1)(0,1)=(-1,0)



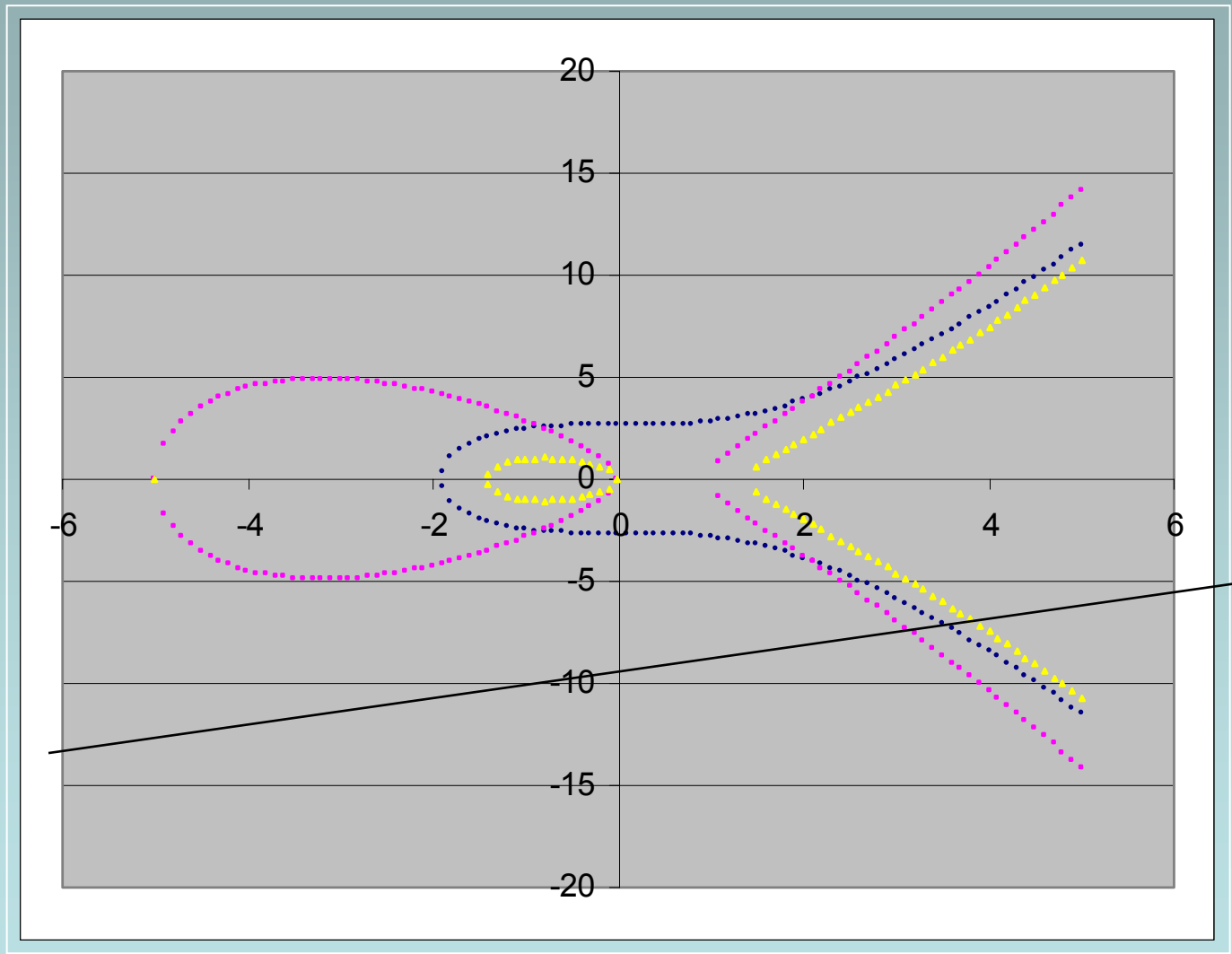
Ejemplo curva elíptica

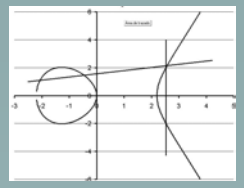
$$y^2 = x^3 + 6x + 1$$



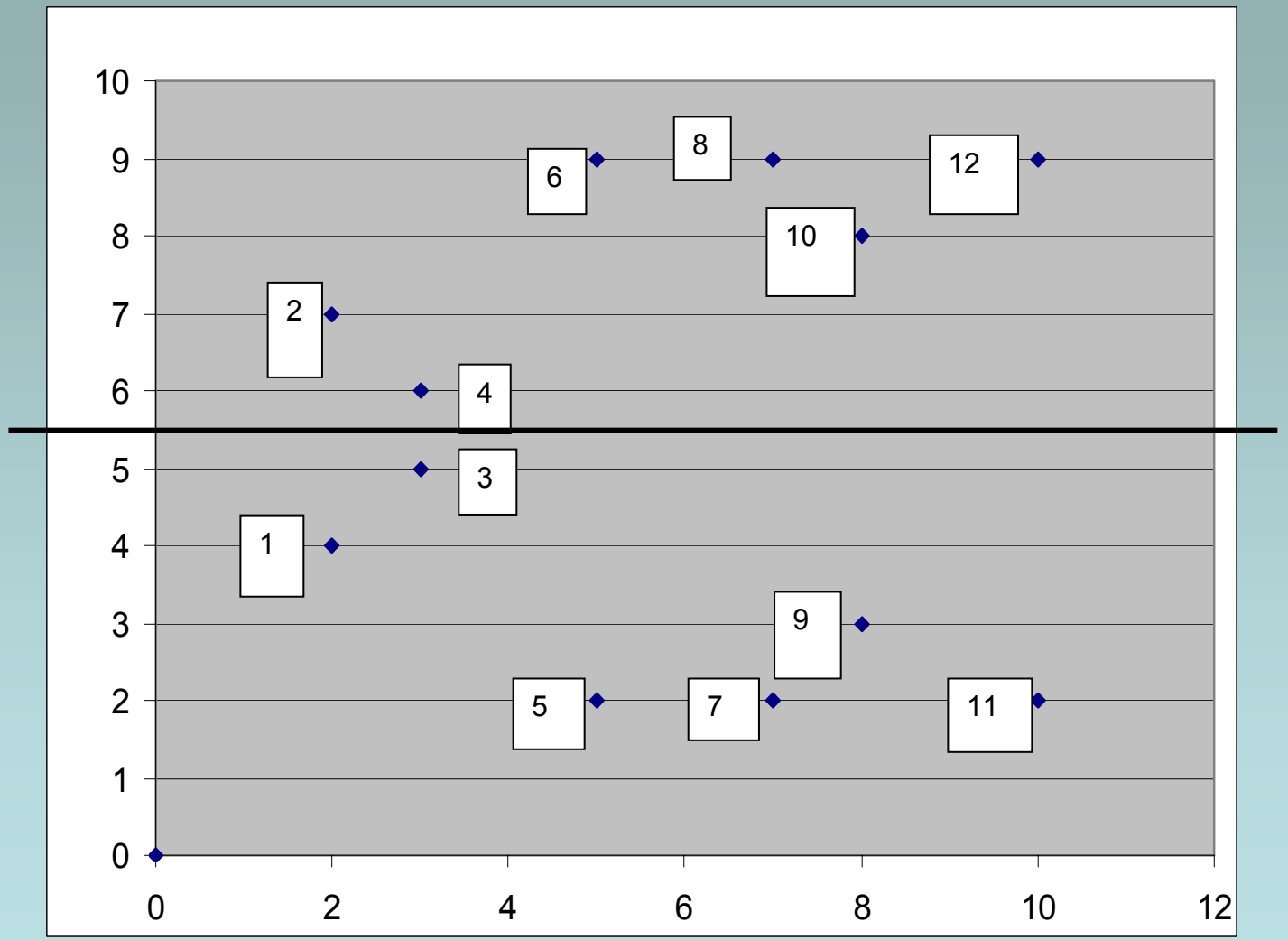


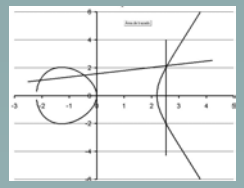
Diferentes Formas





GF(11)



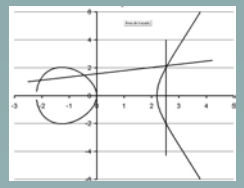


Estructura de grupo

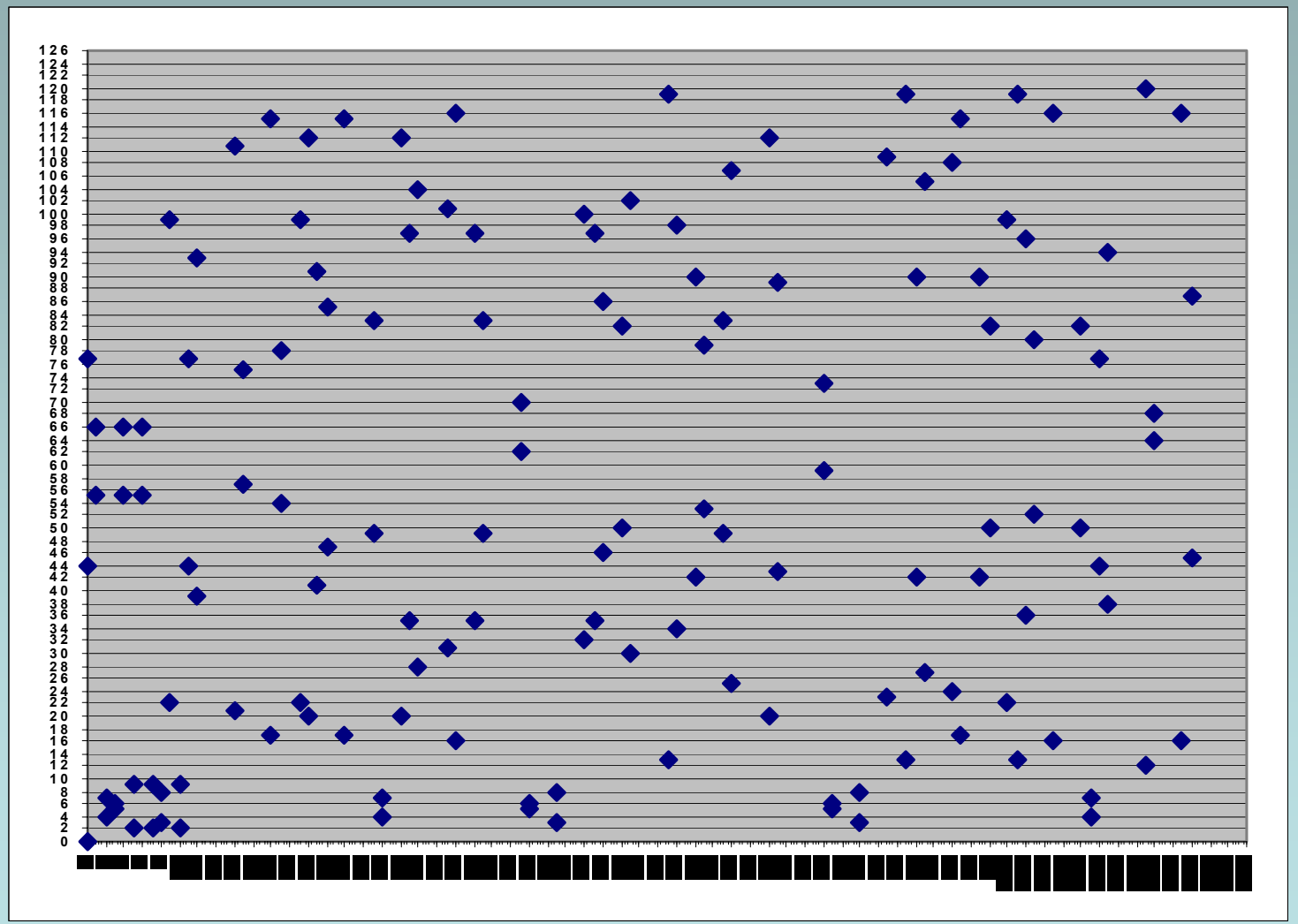
×	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	6	0	7	11	2	10	8	4	5	12	9	3
2	2	0	5	12	8	9	1	3	7	11	6	4	10
3	3	7	12	9	0	10	8	5	2	6	4	1	11
4	4	11	8	0	10	7	9	1	6	3	5	12	2
5	5	2	9	10	7	11	0	12	3	4	1	8	6
6	6	10	1	8	9	0	12	4	11	2	3	5	7
7	7	8	3	5	1	12	4	2	0	10	11	6	9
8	8	4	7	2	6	3	11	0	1	12	9	10	5
9	9	5	11	6	3	4	2	10	12	8	0	7	1
10	10	12	6	4	5	1	3	11	9	0	7	2	8
11	11	9	4	1	12	8	5	6	10	7	2	3	0
12	12	3	10	11	2	6	7	9	5	1	8	0	4

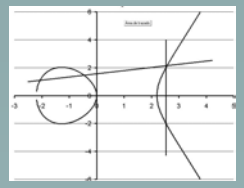
$$\underbrace{\underbrace{(5+4)}_{7}+2}_{3}$$

$$\underbrace{5+\underbrace{(4+2)}_{8}}_{3}$$

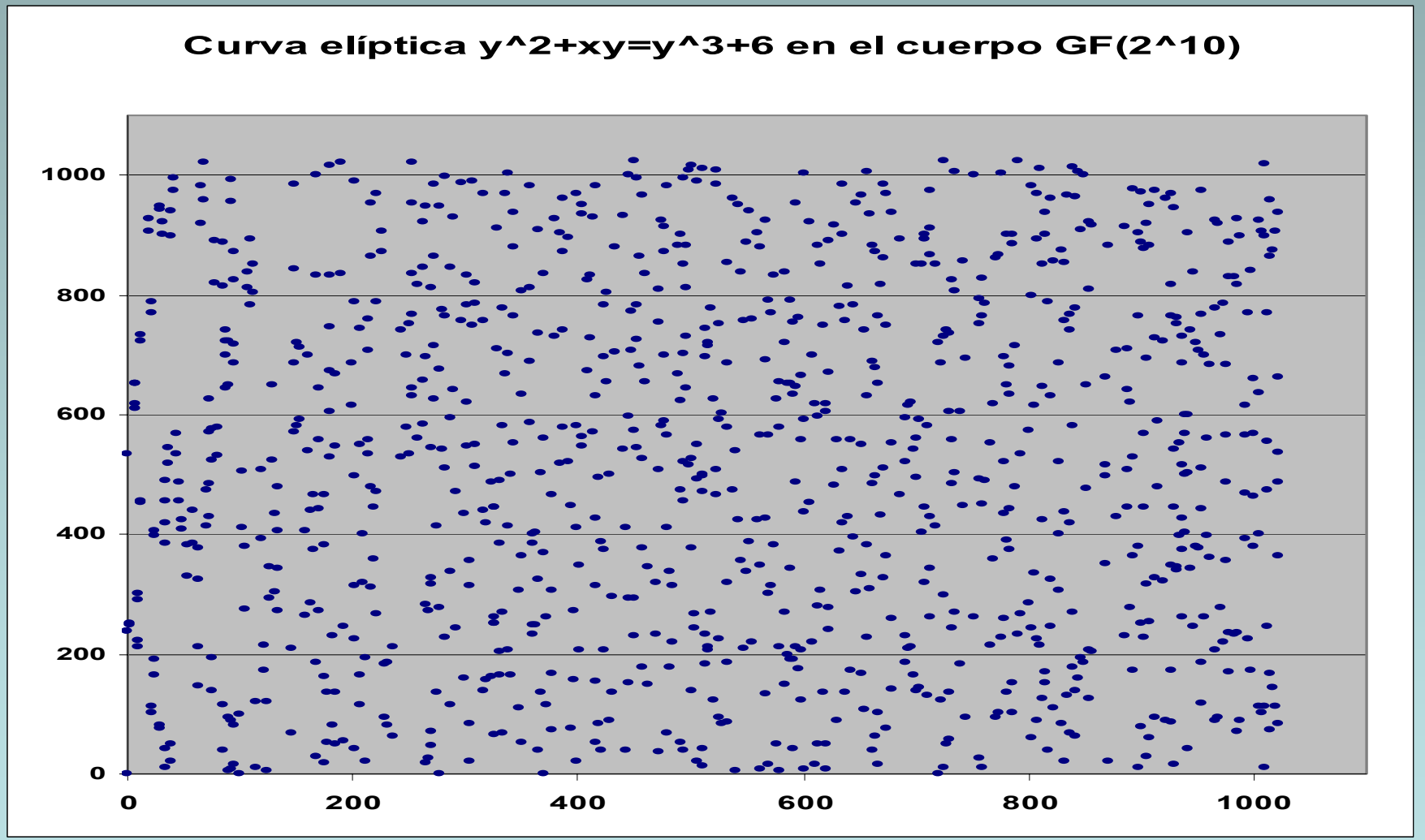


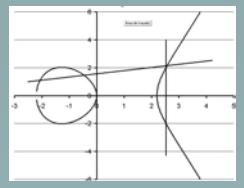
Ejemplo en GF(11^2)





Otro ejemplo en FG(2^{10})

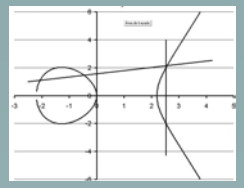




Las curvas elípticas en la criptografía

- ***Factorización de enteros.*** El método RSA de firma digital se basa en la imposibilidad práctica de descomponer en sus factores primos números enteros muy grandes (de más de 300 cifras)
- ***Números congruentes.*** Un número natural es llamado congruente si es el área de un triángulo rectángulo cuyos lados son números racionales.
- ***Firma Digital***. La estructura de grupo de los puntos de una curva elíptica se emplea en reemplazo del método RSA para la firma digital
- ***El último teorema de Fermat***. Recientemente Wiles demostró que todas las curvas elípticas sobre los racionales **Q** (con una pequeña restricción) están vinculadas con las formas modulares. A partir de este teorema se deduce que para un número primo impar $\mathbf{p \neq 3}$ no existe una curva elíptica sobre **Q** cuya ecuación tenga la forma

$$y^2 = x(x+a)(x-b)$$

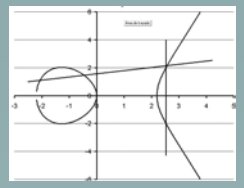


Uso en Firma Digital

- Supóngase que se dispone de un grupo **G** de orden **#G.** El grupo que se emplea es el grupo definido sobre los puntos de una curva elíptica. El principio se basa en lo siguiente: Un usuario elige un $\alpha \in \mathbf{G}$ que es su clave privada y publica su clave pública que es $\beta = \alpha^{-1}$ conjuntamente **G**. Sea $\gamma \in \mathbf{G}$ el mensaje a transmitir. El usuario 1 transmite $\delta = \gamma\alpha$ (multiplica el mensaje por su clave privada). El usuario 2 recibe dicho mensaje δ y lo multiplica por la clave pública del usuario 1, obteniendo

$$\delta\beta = (\gamma\alpha)\alpha^{-1} = \gamma(\alpha\alpha^{-1}) = \gamma 1 = \gamma$$

- Este sistema será seguro en la medida en que no sea posible conocer α a partir de β. Los protocolos que se emplean son un poco más complejos que el ejemplo puesto.

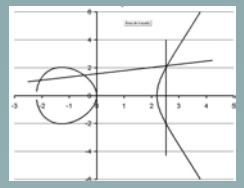


Ejemplo

×	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	6	0	7	11	2	10	8	4	5	12	9	3
2	2	0	5	12	8	9	1	3	7	11	6	4	10
3	3	7	12	9	0	10	8	5	2	6	4	1	11
4	4	11	8	0	10	7	9	1	6	3	5	12	2
5	5	2	9	10	7	11	0	12	3	4	1	8	6
6	6	10	1	8	9	0	12	4	11	2	3	5	7
7	7	8	3	5	1	12	4	2	0	10	11	6	9
8	8	4	7	2	6	3	11	0	1	12	9	10	5
9	9	5	11	6	3	4	2	10	12	8	0	7	1
10	10	12	6	4	5	1	3	11	9	0	7	2	8
11	11	9	4	1	12	8	5	6	10	7	2	3	0
12	12	3	10	11	2	6	7	9	5	1	8	0	4

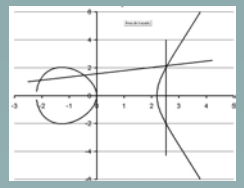
- ***Alicia*** **tiene clave privada 3. Su clave publica es 4 que es el inverso de 3 y quiere mandar el mensaje 9 a *Roberto*. Multiplica 3 por nueve y manda 6 a *Roberto*.**
- ***Roberto*** **recibe el 6 y sabe que la clave pública de Alicia es 4. Multiplica 6 por 4 y obtiene 9 que es el mensaje enviado por Alicia**

El sistema es seguro siempre y cuando no sea posible calcular la clave privada a partir de la clave pública



ECDSA: Elliptic Curve Digital Signature Algorithm

- ***Parámetros de dominio***
  - Un cuerpo de orden **q** (ya sea **q=p** o **$q=2^n$**)
  - Un descriptor que defina la forma de representar los elementos del cuerpo **F_q**.
  - Dos elementos $\alpha,\beta \in \mathbf{F_q}$ que definen la ecuación de la curva **E** sobre **F_q**
  - Los valores $\mathbf{x_G,y_G} \in \mathbf{F_q}$ que definen el elemento generador $\mathbf{G(x_G,y_G)} \in \mathbf{E(F_q)}$.
  - El orden n del punto G con $n > 2^{160}$ y
  - El cofactor $\mathbf{h = \#E(F_q)/n}$.

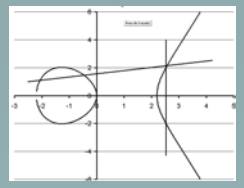


Algunos datos

La curva elíptica **E** debe ser "***aceptable***" definida sobre el cuerpo **GF(q)** de característica **p** y un elemento generador **P**$\in$**E(GF(q))**. Si **q=2^n n >160 =**

$2^{160}\approx$1461500000000000000000000000000000000000000

Para obtener más detalles consultar IEEE P1363. Standard specifications for public-key cryptography, Septiembre 1998



Protocolo

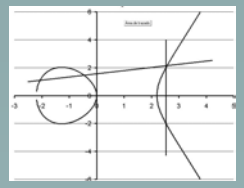
- ***Generación del par de llaves***

  La llaves de una entidad A asociadas con el dominio **D=(q,a,b,G,n,h)** se realiza de la siguiente manera:

  – Se selecciona un entero random (o seudo random) **d** tal que **.1≤d ≤n-1**

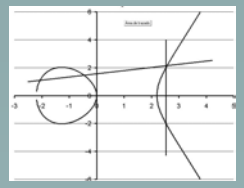
  – Se calcula **Q=[d]G**

  – **Q** es la clave pública de A y **d** de su clave privada



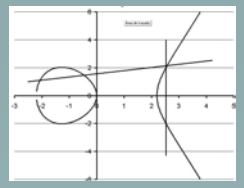
Firma

- Para firmar un mensaje **m**, una entidad con parámetros de dominio **D=(q,a,b,G,n,h)** y con el par de claves **(d,Q)** procede de la siguiente manera:
  1. Genera un numero random (o seudo random) **k** tal que **$1 \leq k \leq n-1$**.
  2. Calcula **$[k]G=(x_1,y_1)$**
  3. Calcula **$r=x_1 \bmod n$**. Si **r** es nulo sigue con el paso 1
  4. Calcula **$k^{-1} \bmod n$**.
  5. Crea **e** que es el compendio del documento **m**
  6. Calcula **$s = k^{-1}(e+dr) \bmod n$**. Si **s** es nulo sigue con el paso 1.
  7. La firma de **A** para el mensaje **m** es **(r,s)**



Verificación de la Firma

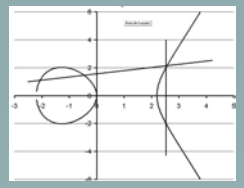
- Para verificar la firma (r,s) de m calculada por A, B debe obtener una copia autenticada de los parámetros de dominio **D=(q,a,b,G,n,h)** y de la clave pública Q.
- El proceso es el siguiente:
- Verifica que **$1 \leq r \leq n-1$** y **$1 \leq s \leq n-1$**
  1. Calcula **e** como el compendio del mensaje **m**
  2. Calcula $w = s^{-1} \bmod n$.
  3. Calcula $u^1 = ew \bmod n$ y $u^2 = rw \bmod n$
  4. Calcula $X = [u_1]G + [u_2]Q$
  5. Si **$X = \mathcal{O}$** rechaza la firma
  6. Calcula **$v = x_1 \bmod n$** donde **$X = X(x_1, y_1)$**
  7. Acepta la firma si y solo si **v=r**



Demostración

El símbolo ≡ indica que las operaciones son módulo n

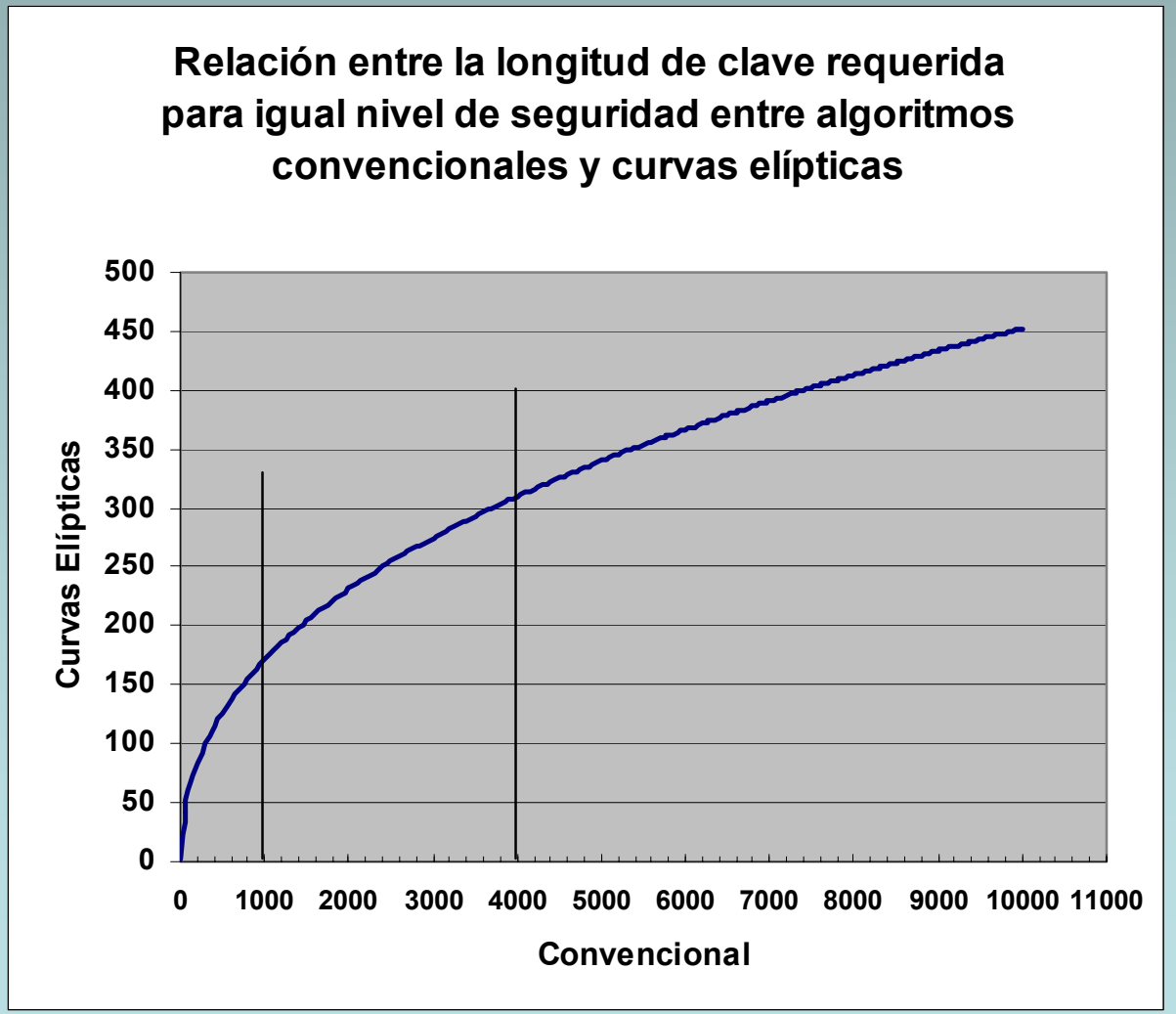
$k \equiv s^{-1}(e+dr)$	Por que el que generó la firma calculó $s \equiv k^{-1}(e+dr)$
$\equiv s^{-1}e+s^{-1}dr$	Propiedad distributiva
$\equiv we+wdr$	Porque así se definió w
$\equiv u_1+u_2d$	Porque así se definió
$k \equiv u_1+u_2d$	
$X=[u_1]G+[u_2]Q$	
$X=[u_1]G+[u_2][d]G$	Porque la clave pública $Q=[k]G$
$X=[u_1+u_2d]G$	
$[k]G$	

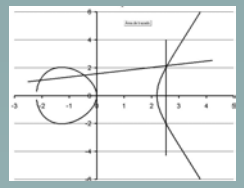


Comparación RSA, CE

$$\eta = \beta n^{1/3}\left(\log(n\log(2))^{2/3}\right)$$

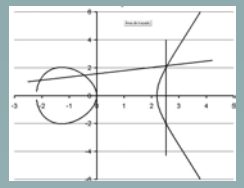
$$\beta \approx 4{,}91$$





Matemáticas

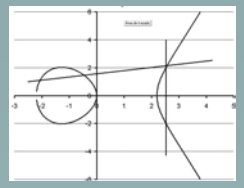
- Conjuntos y Relaciones
- Semigrupos
- Grupos
- Anillos
- Cuerpos



Conjuntos y Relaciones

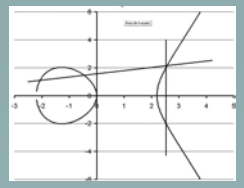
- Los conjuntos se representarán con letras mayúsculas ya sea por una propiedad que los elementos deben satisfacer (conjunto de los números pares) o por enumeración de los elementos que lo constituyen (A={1,2,5,7}). Para indicar que el elemento α pertenece al conjunto A se empleará la notación $\alpha \in A$.
- Dado los conjuntos A y B se definirá el conjunto $A \times B$ al conjunto de todos los pares ordenados del tipo (α,β) donde $\alpha \in A$ $\beta \in B$. Por ejemplo si A={a,b,c} y B={1,2} seria

  $A \times B$={(a,1),(b,1),(c,1), (a,2),(b,2),(c,2)
- Una relación R entre A y B es $R \subseteq A \times B$ (Un subconjunto del producto cartesiano de A por B)
- Se definen dos operaciones fundamentales que son la unión y la intersección



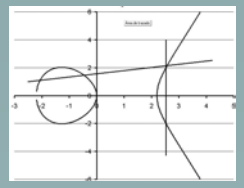
Subgrupos

- Dado un conjunto S y una operación (+) entre los elementos de S que satisfaga las siguientes propiedades
  - $s_1, s_2 \in S$ luego $s_1 + s_2 \in S$ (Cerrada)
  - Existe $e \in S$ tal que para todo $s \in S$ $s+e=s$ (Existencia del elemento neutro)
  - Si $s_1, s_2, s_3 \in S$ luego $(s_1+s_2)+,s_3 = s_1+(s_2+s_3)$ (asociatividad)



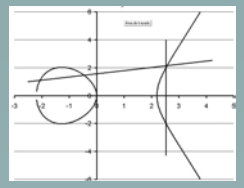
Ejemplo

- Los enteros con respecto al producto
- Sea $\Sigma_n=\{\sigma_1, \sigma_2, .., \sigma_n\}$ un conjunto llamado alfabeto cuyos elementos se llamarán letras. Lamaremos Σ^*_n al conjunto de todas las secuencias (palabras) que se pueden formar con las letras del alfabeto más la secuencia nula (λ) que es la secuencia que no tiene niugún caracter. Por ejemplo si n=4, un elemento de Σ^*_4 sería $\sigma_4\,\sigma_2\,\sigma_2\,\sigma_3$
- Definamos la operación de concatenación de la siguiente manera: dadas dos palabras, a y b, la concatenación de ambas es una nueva palabra que se obtiene poniendo los caracteres de b a continuación de los de a. Refiriéndonos al ejemplo anterior si $\mathbf{a=}\sigma_4\,\sigma_2\,\sigma_2\,\sigma_3$ y $\mathbf{b} = \sigma_3\,\sigma_1$ luego $\mathbf{ab=}_4\,\sigma_2\,\sigma_2\,\sigma_3\,\sigma_3\,\sigma_1$
- El elemento unidad es λ, ya que concatenar a cualquier palabra una palabra sin letras no la altera, es decir que a $\lambda = \lambda a = a$



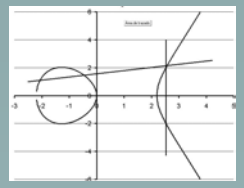
Grupos

- Un grupo es un subgrupo que tiene además de las propiedades enunciadas la siguiente propiedad: para todo elemento $\mathbf{g} \in \mathbf{G}$ existe un elemento **h** tal que **gh=e** (existencia del inverso). Generalmente **h** se lo denota como $\mathbf{g^{-1}}$
- Ejemplo los enteros con respecto a la suma, los racionales con respecto a la suma y al producto, los reales con respecto a la suma y al producto



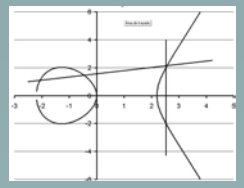
Anillos

- Un anillo es un conjunto S con dos operaciones + y $\times$ tal que;
  - es un grupo con respecto a la suma
  - los elementos de S sin el elemento neutro de la suma forman subgrupo grupo respecto al producto
  - la suma es distributiva con respecto al producto
- Al grupo con respecto a la suma se lo llama grupo aditivo y al grupo con respecto al producto de lo llama grupo multiplicativo



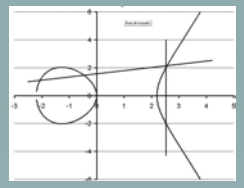
Ejemplos de anillo

- Los enteros con respecto a la suma y el producto. La inversa multiplicativa no esta definida ya que el cociente entre dos enteros puede no existir



Polinomios

- Sea un anillo S y sean $\alpha_i \in S$ elementos del anillo. Un polinomio de la indeterminada X es un objeto de la forma
- $p(X)=\alpha_0+ \alpha_1X+ \alpha_2X^2+....+ \alpha_nX^n$
- Suma Si $p(X)=\alpha_0+ \alpha_1X+ \alpha_2X^2+....+ \alpha_nX^n$ y
- $q(x)= \beta_0+ \beta_1X+ \beta_2X^2+....+ \beta_nX^n$
- $p(X)+q(x)=(\alpha_0+\beta_{0)}+(\alpha_0+\beta_0)X+...+(\alpha_n+ \beta_n)X^n$
- Producto



Polinomios

Producto

$$P(X)=\sum_{j=1}^{n_1}\alpha_j x^j \quad y \quad Q(X)=\sum_{j=1}^{n_2}\beta_j x^j \quad \text{luego}$$

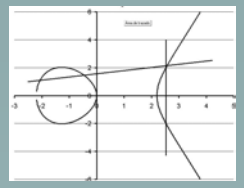
$$P(X)Q(X)=\sum_{j=0}^{n_1}\alpha_j x^j\sum_{k=0}^{n_2}\beta_k x^k=\sum_{j=0}^{n_1}\sum_{k=0}^{n_2}\alpha_j\beta_k x^k x^j=\sum_{j=0}^{n_1}\sum_{k=0}^{n_2}\alpha_j\beta_k x^{k+j}$$

Ejemplo

$(2 + 3x + 2x^2)(1 + x) =$

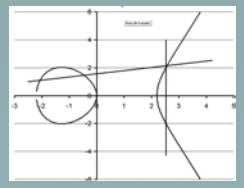
$2 + 3x + 2x^2 + 2x + 3x^2 + 2x^3 =$

$2 + 5x + 5x^2 + 2x^3$



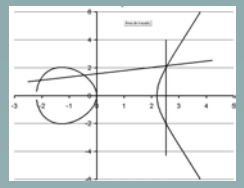
Polinomios

- Los polinomios forman un anillo
  - La suma y producto son cerradas
  - La suma forma grupo
  - El producto forma un subgrupo (La operación inversa no esta definida)
  - Suma es distributiva con respecto al producto



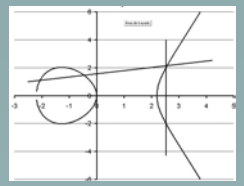
Cuerpos

- Un cuerpo es un anillo que forma grupo multiplicativo
- Como ejemplo
  - Los raciónales con respecto al la suma y el producto
  - Los reales con respecto al la suma y el producto
  - Los complejos con respecto al la suma y el producto



Cuerpos finitos

- Los ejemplos anteriores se refieren a cuerpos con una infinita cantidad de elementos. Existen cuerpos que tienen una cantidad finita de elementos
- Sea p un número primo
- Sea GF el conjunto de números naturales menores que p
- Si $a,b \in GF$ la suma será el resto de dividir a+b por p
- Si $a,b \in GF$ el producto será el resto de dividir a*b por p
- El cuerpo se denota GF(p)



Ejemplo FG(7)

Tabla de la suma

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tabla del producto

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$$\underbrace{1+1+1+1+1+1+1}_{7 \text{ veces}} = 0$$

$$4 * (3 + 2) = 4 * 3 + 4 * 2 = 5 + 1 = 6 \qquad 4 * 5 = 6$$

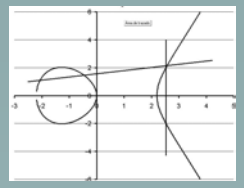
$$3x + 2y = 6$$

$$5x + 6y = 4$$

$$\begin{vmatrix} 3 & 2 \\ 5 & 6 \end{vmatrix} = 3 * 6 - 5 * 2 = 4 - 3 = 4 + 4 = 1$$

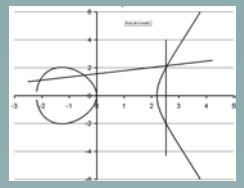
$$x = \frac{\begin{vmatrix} 6 & 2 \\ 4 & 6 \end{vmatrix}}{1} = 6 * 6 - 4 * 2 = 1 - 1 = 0$$

$$y = \frac{\begin{vmatrix} 3 & 6 \\ 5 & 4 \end{vmatrix}}{1} = 3 * 4 - 6 * 5 = 5 - 2 = 5 + 5 = 3$$



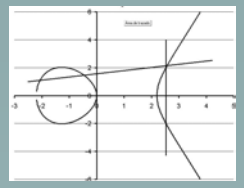
Más cuerpos finitos

- Sea el conjunto de objetos de la forma (x,y) donde $x,y \in \Re$
- Sean las operaciones
  - $(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$
  - $(x_1,y_1)*(x_2,y_2)=(x_1*x_2 - y_1*y_2 , x_1*y_2 + x_2*y_1)$
- Otra representación $x + jy$ $j^2 = -1$



Otra forma

- Sean los polinomios de la forma $X^2 + 1$
- En los reales este polinomio no tiene solución
- Sea el anillo de los polinomios de grado 1 de la forma $aX + b \quad a,b \in \Re$
- Sea la suma $(a_1X+b_1)+(a_2X+b_2)=(a_1+a_2)X+(b_1+b_2)$
- Sea el producto
- $(a_1X+b_1)*(a_2X+b_2)=a_1a_2X_2+(a_1b_2+a_2b_1)X+b_1b_2$



Dividido por X^2+1

$$a_1a_2X^2+(a_1b_2+a_2b_1)X+b_1b_2 \quad \Big| \quad X^2+1$$

$$a^1a^2X^2 \qquad +a^1a^2 \qquad\qquad a1a2$$

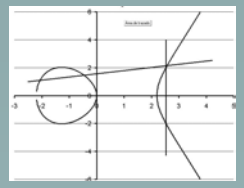
$$(a_1b_2+a_2b_1)X + b_1b_2- a_1a_2$$

El polinomio que queda es

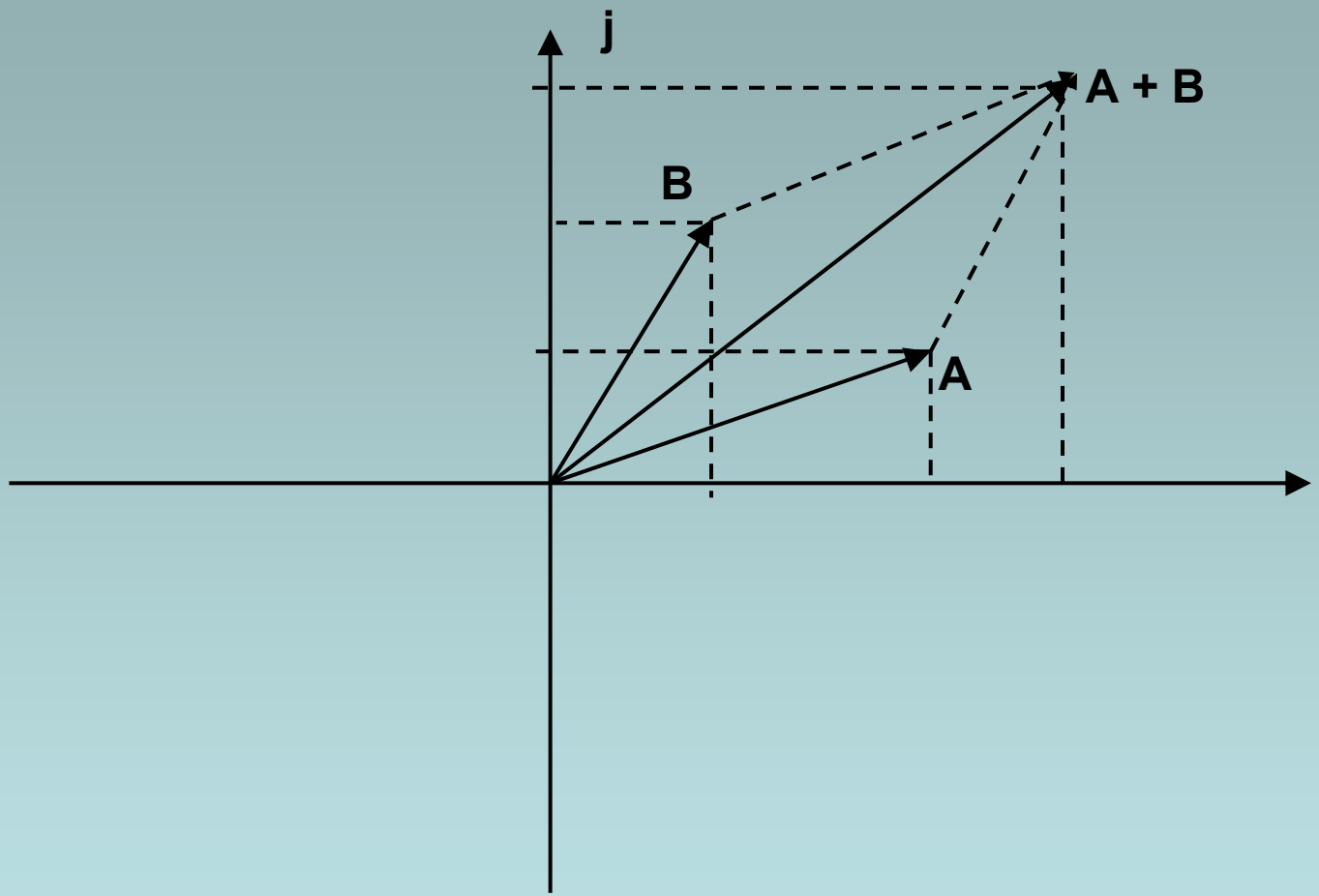
$$(a_1b_2+a_2b_1)X + b_1b_2- a_1a_2$$

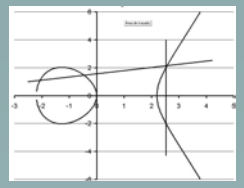
Por lo tanto en la clase residual x^2+1 será

$$(a_1X+b_1)*(a_2X+b_2)=(a_1b_2+a_2b_1)X + b_1b_2- a_1a_2$$



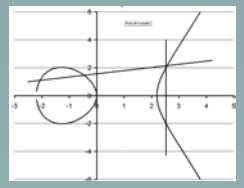
Como vectores





Cuerpos de Galois GF(p^n)

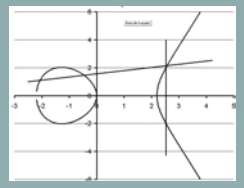
- Se busca un polinomio irreducible (que no tenga solución de orden n)
- Para todos los polinomios de orden inferior a n se definen las operaciones
  - Suma como la suma de polinomios
  - Producto como el resto de dividir por el polinomio irreducible el producto de los dos polinomios



Ejemplo

- Sea en base 2 el polinomio x^3+x+1 que es irreducible (si x=0 da 1 y si x=1 da 1)
- Sean los polinomios identificados por su valor binario

0	0
1	1
2	x
3	x+1
4	x^2
5	x^2+1
6	x^2+x
7	x^2+x+1



Tablas de Operaciones

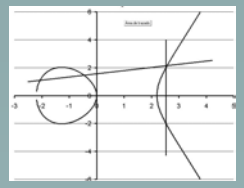
+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

x	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	3	1	7	5
3	3	6	5	7	4	1	2
4	4	3	7	6	2	5	1
5	5	1	4	2	7	3	6
6	6	7	1	5	3	2	4
7	7	5	2	1	6	4	3

Observaciones 1 + 1 = 0

Característica del cuerpo 2

$$(x + y)^2 = x^2 + y^2$$



Espacios vectoriales en GF(2^n)

- **Bases normales**
  - **$(\alpha+\beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2 = \alpha^2 + \beta^2$ ya que**

  $2\alpha\beta = \alpha\beta + \alpha\beta = \alpha\beta(1 + 1) = \alpha\beta 0 = 0$
- **Se puede demostrar por inducción completa que para $\alpha \in$ GF(2^n)**

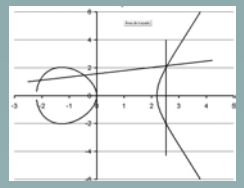
$$\left(\sum_{j=1}^{n}\alpha_j\right)^2 = \sum_{j=1}^{n}\alpha_j^2$$

Base Normal $\alpha \in$ GF(2n)

$$\left(\alpha^{2^0}\alpha^{2^1}, \alpha^{2^2}, ..., \alpha^{2^{n-1}}\right)$$

$$\beta = \nu_0\alpha^{2^0} + \nu_1\alpha^{2^1} + ... + \nu_{n-1}\alpha^{2^{n-1}}$$

$$\beta^2 = \nu_{n-1}\alpha^{2^0} + \nu_0\alpha^{2^1} + \nu_1\alpha^{2^2} + ... + \nu_{n-2}\alpha^{2^{n-1}}$$



Ejemplo

Base Polinomio x^3

8	12	15	10	N°
0	0	0	0	0
1	0	0	0	8
0	1	0	0	12
1	1	0	0	4
0	0	1	0	15
1	0	1	0	7
0	1	1	0	3
1	1	1	0	11
0	0	0	1	10
1	0	0	1	2
0	1	0	1	6
1	1	0	1	14
0	0	1	1	5
1	0	1	1	13
0	1	1	1	9
1	1	1	1	1

Sea el polinomio 12 x^3+x^2

En la base normal es 0100. Luego su cuadrado será 0010 que corresponde al polinomio 15.

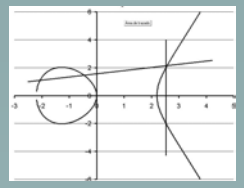
$(x^3+x^2)^2=x^6+x^4$. El resto de dividir por el polinomio irreducible x^4+x+1 da

$$x^6 + x^4 \quad \Big| \; x^4+x+1$$

$$x^6 \quad x^3 \; x^2 \qquad x^2+1$$

$$x^4 \; x^3 \quad x \; 1$$

$$x^3 \; x^2 \; x \; 1$$



Ejemplo

- Calcular $\alpha=(x^3+x^2+1)^{9345}$ que en la base normal es 1011

$$\alpha^{9345} = \alpha^{2^{13}+2^{10}+2^7+2^0} = \alpha^{2^{13}}\alpha^{2^{10}}\alpha^{2^7}\alpha^{2^0}$$

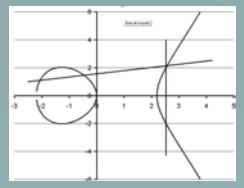
Rotar 13 veces a la derecha es decir 1 1101 = 14

Rotar 10 veces a la derecha es decir 2 1110 = 11

Rotar 7 veces a la derecha es decir 3 0111= 9

Rotar 0 ves a la derecha 1011 =13

Luego $(x^3+x^2+1)^{9345}=14*11*9*13=1$

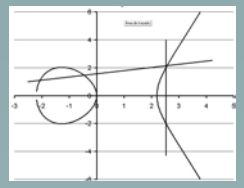


Funciones Elípticas

- Para cuerpos de característica >3
  - $f(X,Y)=Y^2 - X^3 - AX - B \qquad A,B \in K$
  - $f(X,Y,Z)=Y^2Z - X^3 - AXZ^2 - BZ^3 \quad A,B \in K$
  - Tres raíces diferentes

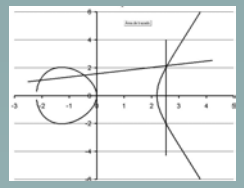
$$\frac{\partial F(X,Y,Z)}{\partial X} \neq 0, \quad \frac{\partial F(X,Y,Z)}{\partial Y} \neq 0, \quad \frac{\partial F(X,Y,Z)}{\partial Z} \neq 0$$

- Para cuerpos de característica = 2
  - $Y^2+XY=X^3+AX^2+B \quad A,B \in K$



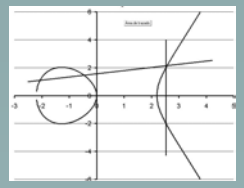
Polinomios

- Expresiones formales del tipo
  - $a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \quad a_j \in I \;\; 0 \leq j \leq k$
- I puede ser otro idel como el de los polinomios definidos sobre un Ideal K
- Ejemplo
  - $(Y^2+3)X^3+(y^3+2^Y+4)X^2+XY+3$

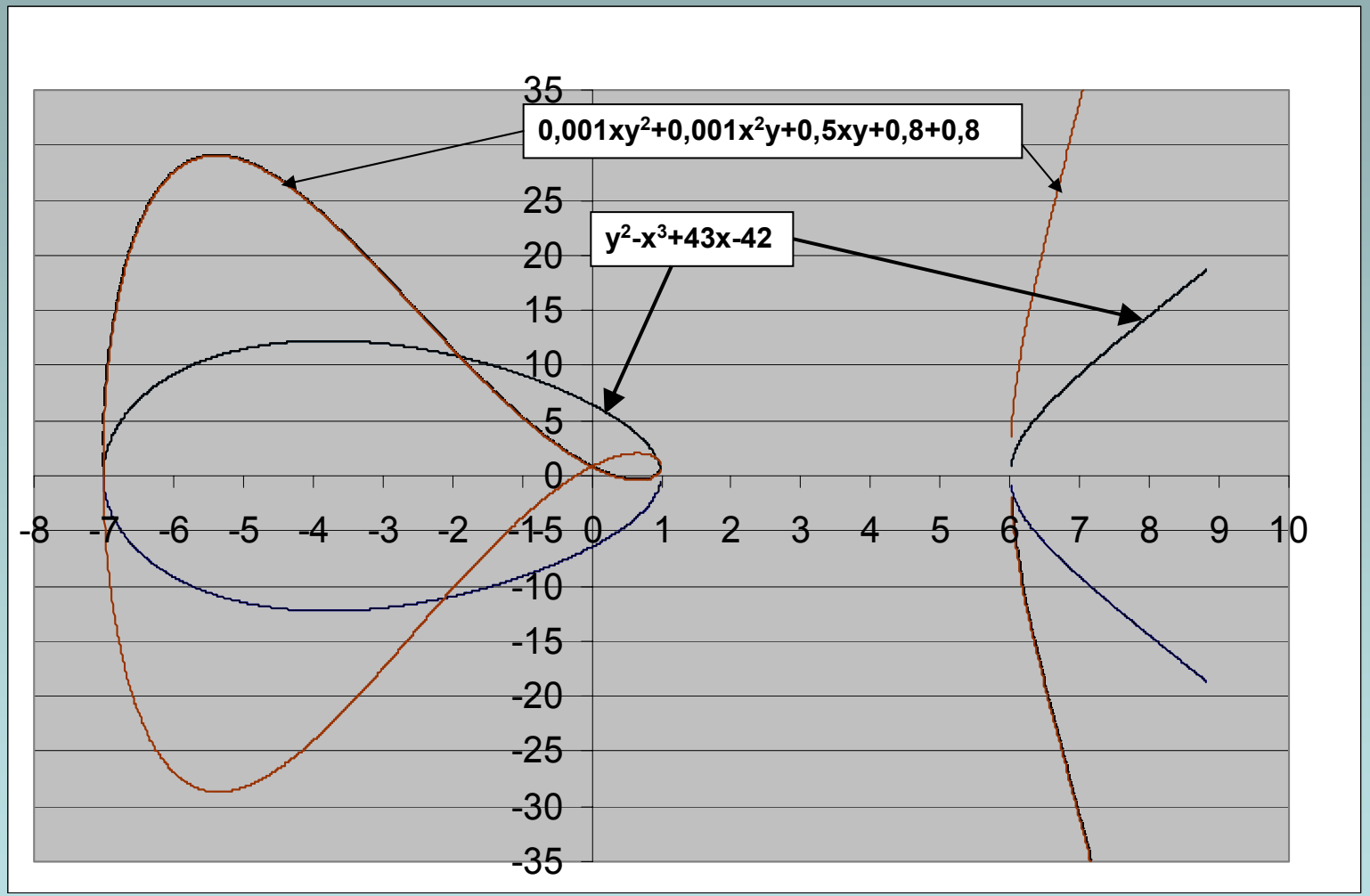


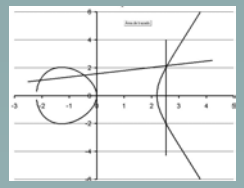
Polinomios sobre las funciones elípticas

- Dado f(x,y) para los pares de valores de un función elíptica
  - Cada aparición de un término con y^k k>1 puede reemplazarse por $y^2=x^3+Ax+B$
  - Todo polinomio f(x,y) puede expresarse como
    - $f(x,y)=v(x) + yw(x)$
    - $xy + x^2y^2 + x^3$ se reduce a
    - $x^2(x^3 + Ax + B) + x^3 + xy = x^5+(A+1)x^3+B+yx$
  - Conjugado $\bar{f}(x,y)=x(x) – y\ w(x)$
  - Norma f $\bar{f}$ $=(v+yw)(v-yw)=v^2-y^2w^2= v^2-sw^2$ donde $s=x^3+Ax+B$. La Norma solo depende de x



Ejemplo


0,001xy²+0,001x²y+0,5xy+0,8+0,8
y²-x³+43x-42
35
25
20
15
10
5
0
-10
-15
-20
-25
-30
-35
-8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10

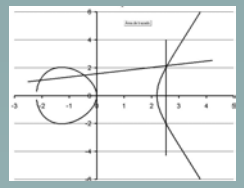


Funciones Racionales

- r(x,y)=f(x,y)/g(x,y) es una relación de equivalencia f/g=h/k sii fk=gh

$$\frac{\mathbf{f(x,y)}}{\mathbf{g(x,y)}} = \frac{\mathbf{f(x,y)} * \overline{\mathbf{g}}\mathbf{(x,y)}}{\mathbf{g(x,y)} * \overline{\mathbf{g}}\mathbf{(x,y)}} = \mathbf{r(x)} + \mathbf{yt(x)}$$

Donde r y t son funciones racionales de x solamente



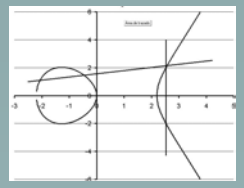
Ejemplo

Sea la función racional

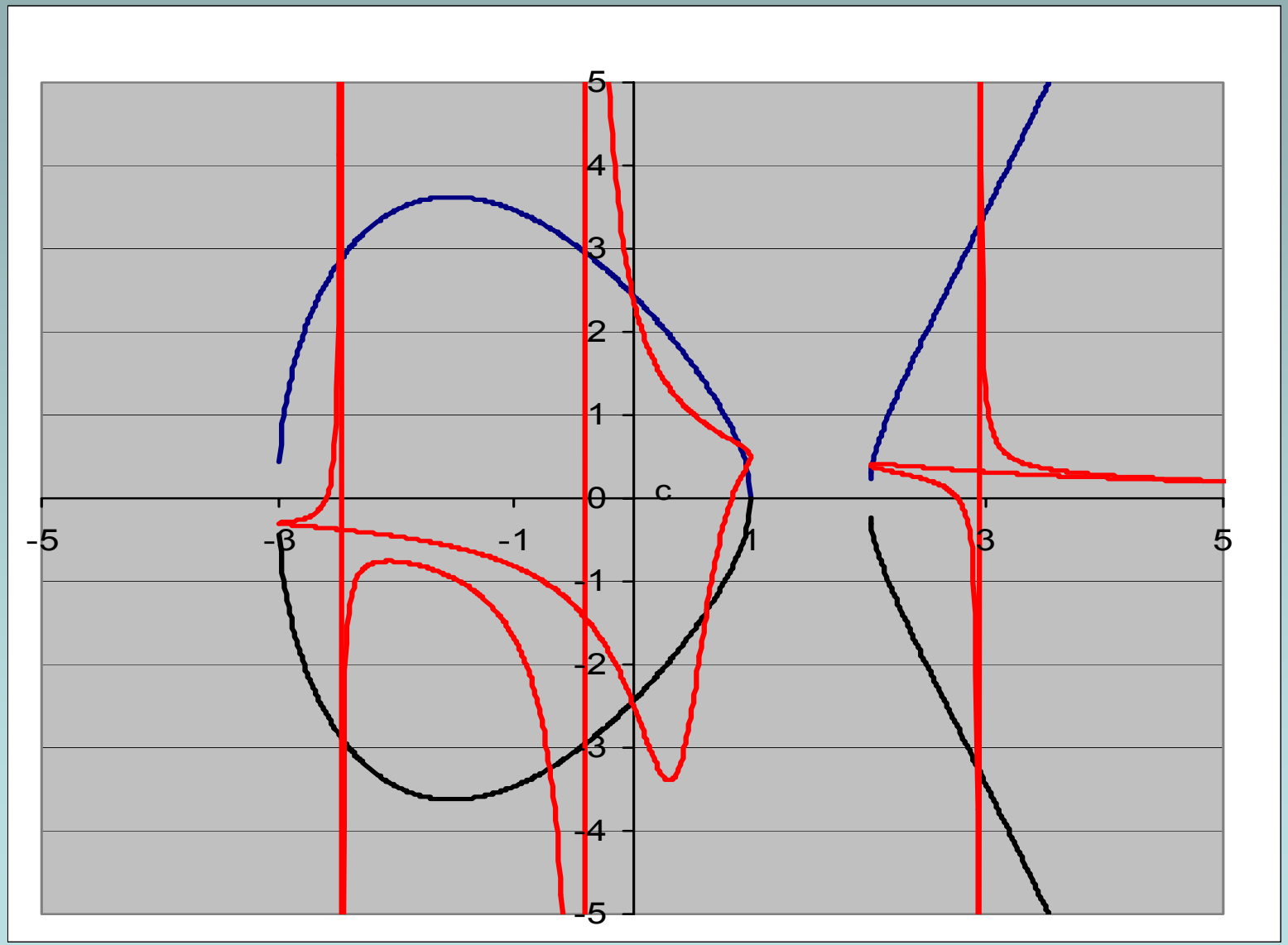
$$\frac{x+y}{x^2+1+yx} = \frac{(x+y)(x^2+1-yx)}{(x^2+1+yx)(x^2+1-yx)}$$

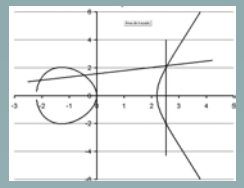
$$= \frac{-x^4+x^3+7x^2+7x}{-x^5+x^4+7x^3-4x^2+1} + y\frac{1}{-x^5+x^4+7x^3-4x^2+1}$$

sobre la curva elíptica $y^2=x^3-7x+6$

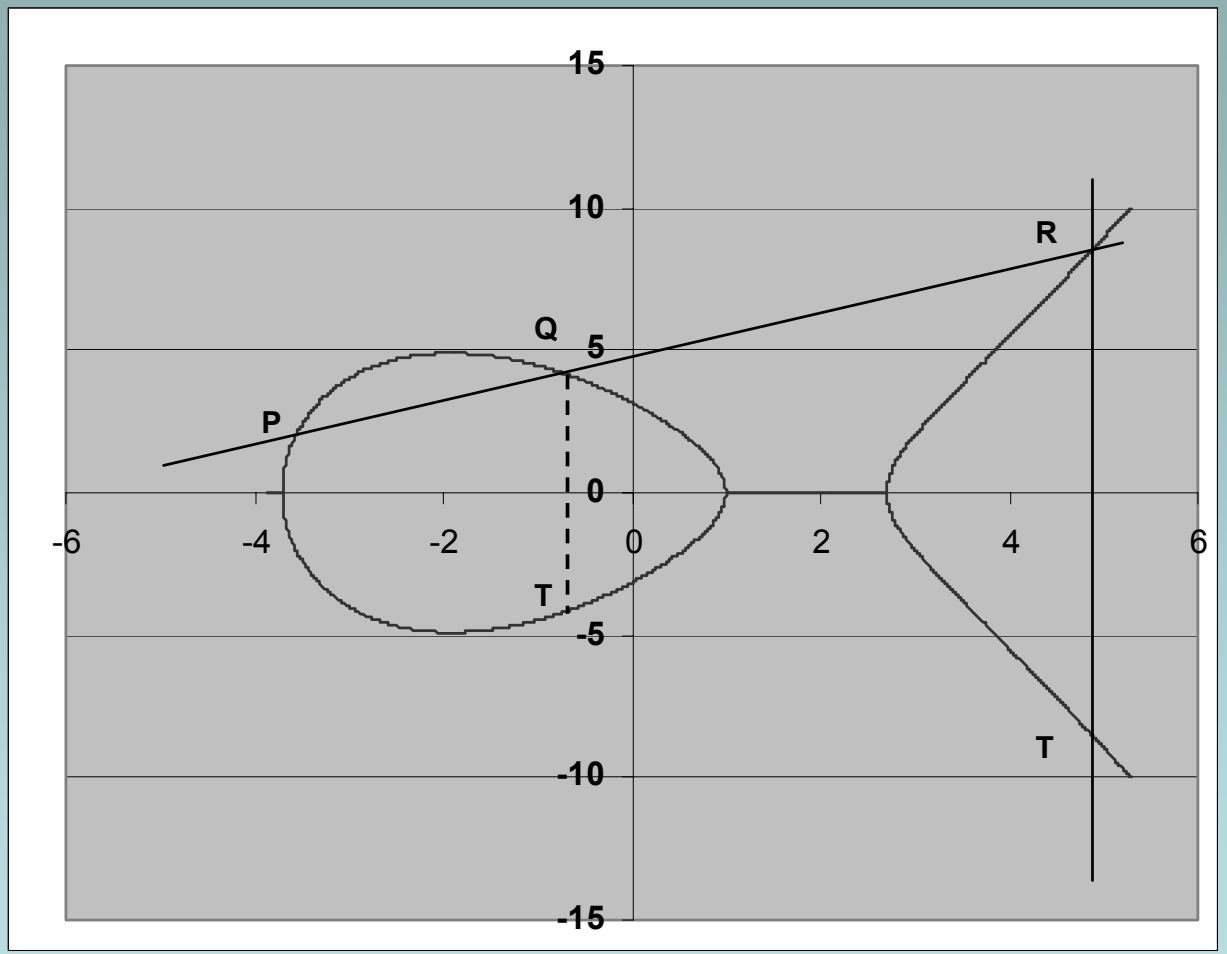


Ejemplo$(x+y)/(x^2+1+yx)$



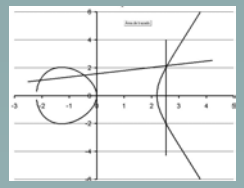


La estructura de grupo

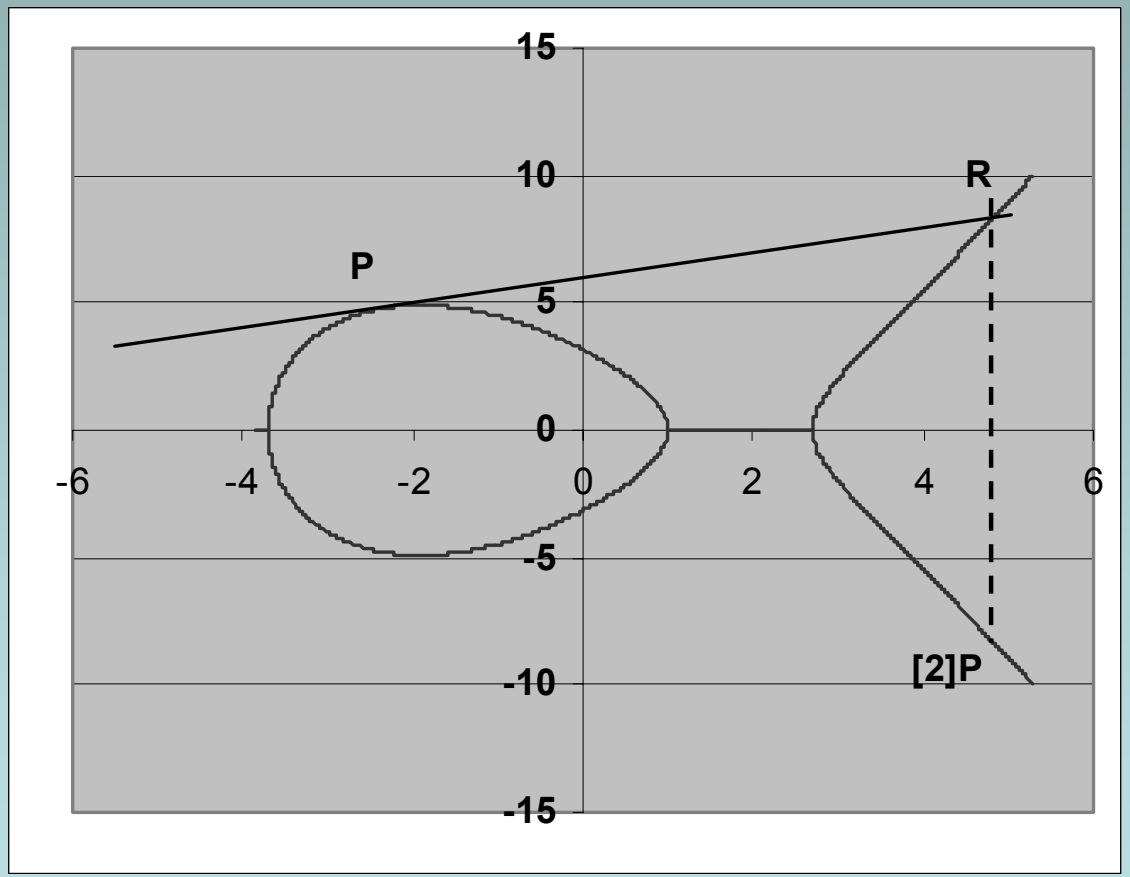


P+Q+R=𝒪

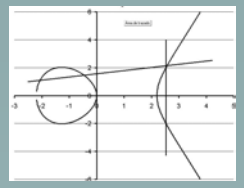
R+T=𝒪



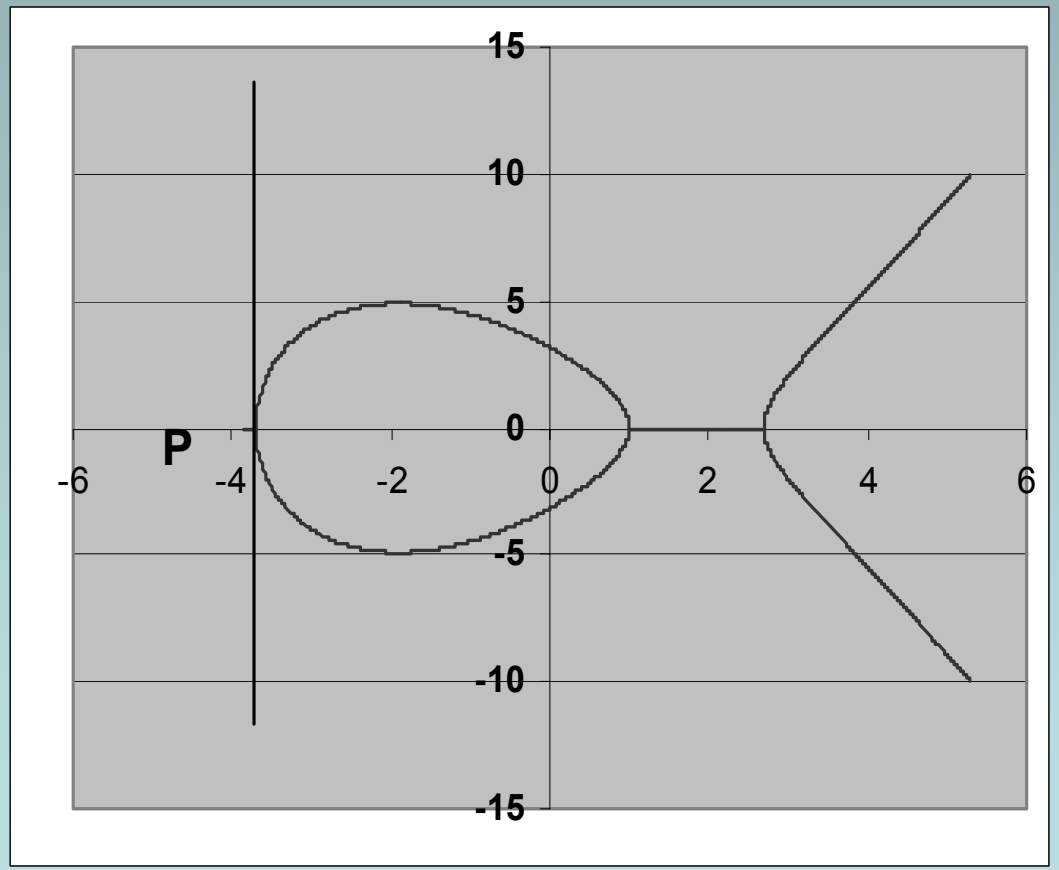
La Estructura ee Grupo



[2]P + R = ∅

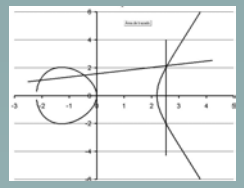


Estructura de grupo



P + P = $\mathcal{O}$

Puntos de orden 2



Algunas Ecuaciones para cuerpos con característica mayor que 3

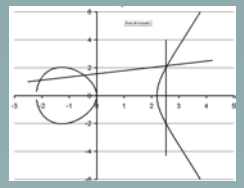
1. **-P(x,y)=P(x,-y)**

2. **$P(x_1,y_1)+Q(x_2,y_2)=R(x,y)$ con $x_1 \neq x_2$**

$$m = \frac{y_2 - y_1}{x_2 - x_1} \qquad \mu = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} \qquad x = m^2 - x_1 - x_2 \qquad y = -u - mx$$

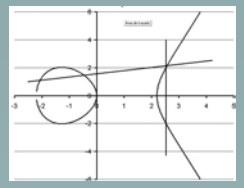
3. **Los puntos son iguales**

$$m = \frac{[3]x_1^2 + a}{[2]y_1} \qquad \mu = \frac{-x_1^3 + ax_1 + [2]x}{[2]y_1} \qquad x = m^2 - x_1 - x_2 \qquad y = -u - mx$$

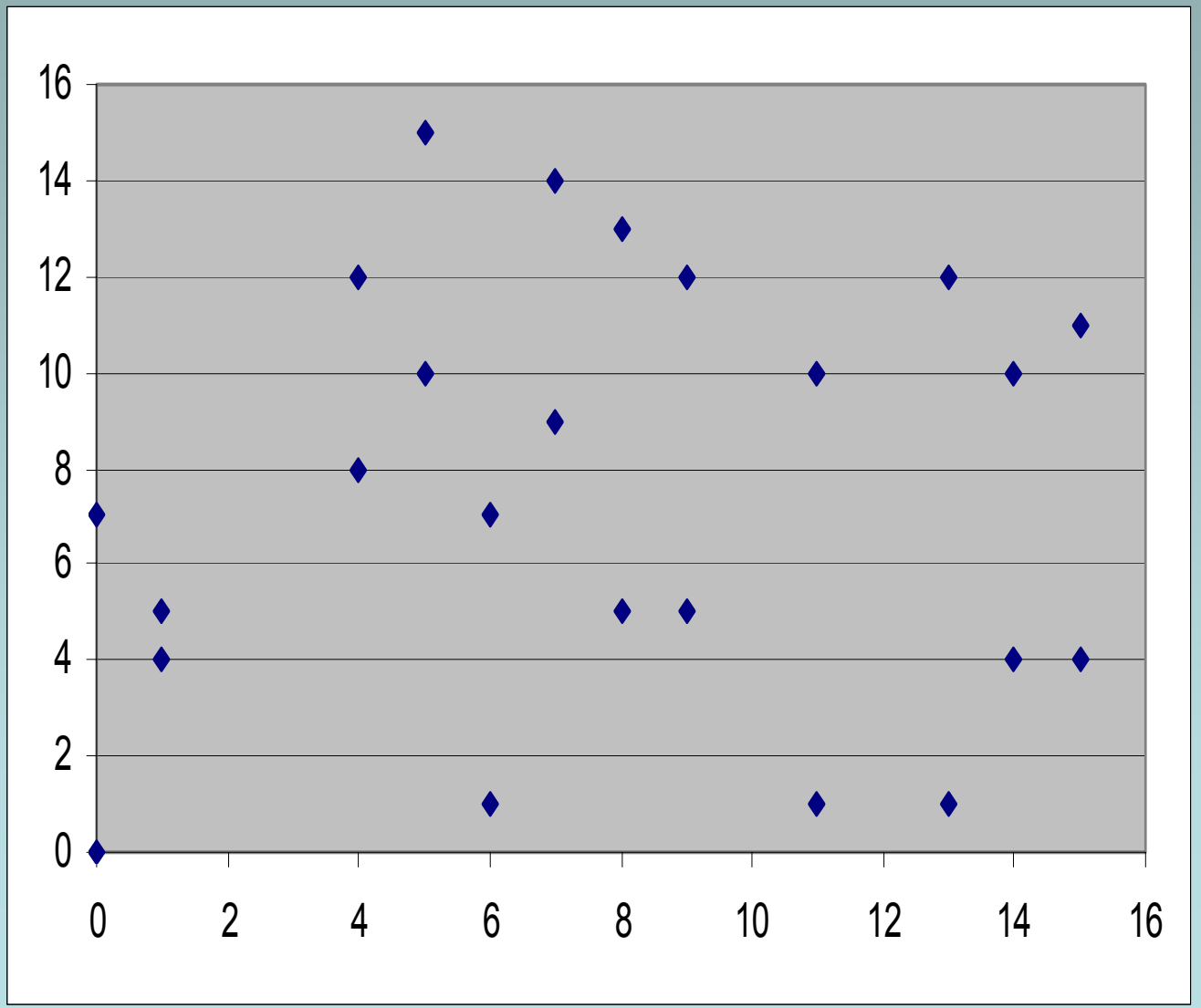


Para cuerpos con característica 2. $y^2+xy=x^3+ax^2+b$

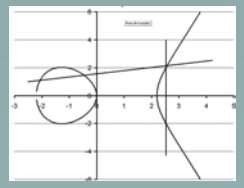
P(x,y)	$x_1 \neq x_2$ $P(x_1,y_1)+P(x_2,y_2)=Q(x_3,y_3)$		$x_1=x_2$ $[2]P(x_1,y_1)=Q(x_3,y_3)$	
	$m=\frac{y_2+y_1}{x_2+x_1}$	$\mu=\frac{x_2y_1+x_1y_2}{x_2+x_1}$	$m=\frac{y_1+x_1^2}{x_1}$	$\mu=x_1^2$
$-P(x,y)=P(x,x+y)$	$Q(x,y) = Q(m^2+m+a, \mu+(m+1)x)$			



Ejemplo en GF(2^4)

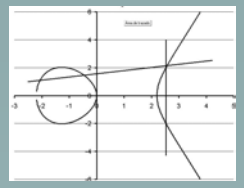


0	0	0
1	0	7
2	1	4
3	1	5
4	4	8
5	4	12
6	5	10
7	5	15
8	6	1
9	6	7
10	7	9
11	7	14
12	8	5
13	8	13
14	9	5
15	9	12
16	11	1
17	11	10
18	13	1
19	13	12
20	14	4
21	14	10
22	15	4
23	15	11

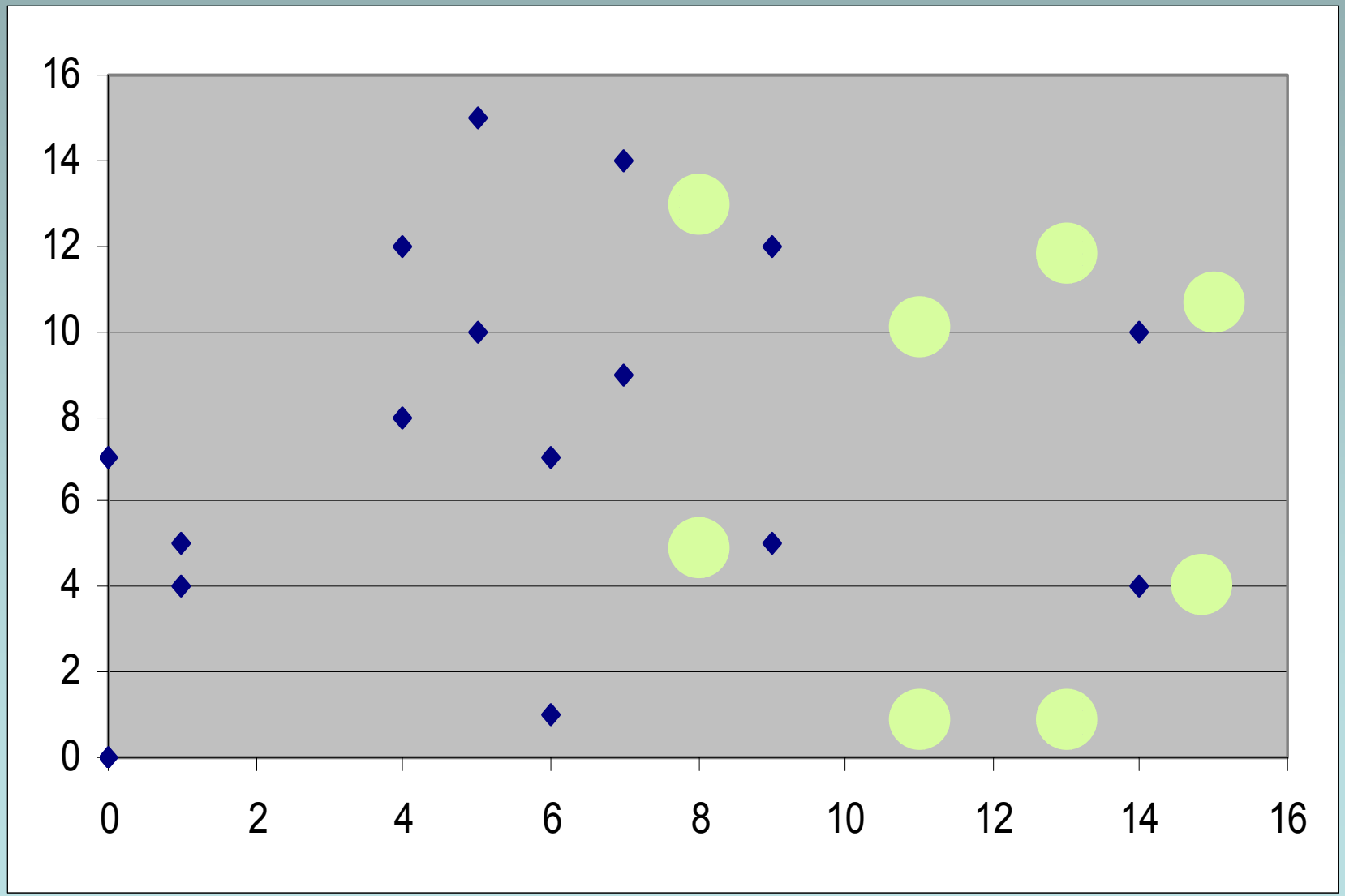


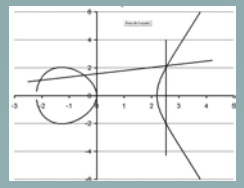
Continuación

Grupo eliptico																								
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	1	0	10	11	6	7	4	5	9	8	2	3	17	16	20	21	13	12	23	22	14	15	19	18
2	2	10	11	0	9	4	8	6	5	7	3	1	22	14	18	12	20	19	16	15	23	17	21	13
3	3	11	0	10	5	8	7	9	6	4	1	2	15	23	13	19	18	21	14	17	16	22	12	20
4	4	6	9	5	2	0	10	1	3	11	8	7	20	17	19	16	12	14	15	18	22	13	23	21
5	5	7	4	8	0	3	1	11	10	2	6	9	16	21	17	18	15	13	19	14	12	23	20	22
6	6	4	8	7	10	1	2	0	11	3	9	5	14	12	22	13	17	20	21	23	19	16	18	15
7	7	5	6	9	1	11	0	3	2	10	4	8	13	15	12	23	21	16	22	20	17	18	14	19
8	8	9	5	6	3	10	11	2	1	0	7	4	18	22	21	14	19	23	17	13	15	20	16	12
9	9	8	7	4	11	2	3	10	0	1	5	6	23	19	15	20	22	18	12	16	21	14	13	17
10	10	2	3	1	8	6	9	4	7	5	11	0	19	20	23	17	14	22	13	21	18	12	15	16
11	11	3	1	2	7	9	5	8	4	6	0	10	21	18	16	22	23	15	20	12	13	19	17	14
12	12	17	22	15	20	16	14	13	18	23	19	21	6	0	2	7	1	4	11	9	10	5	8	3
13	13	16	14	23	17	21	12	15	22	19	20	18	0	7	6	3	5	1	8	10	4	11	2	9
14	14	20	18	13	19	17	22	12	21	15	23	16	2	6	8	0	4	10	5	3	9	1	11	7
15	15	21	12	19	16	18	13	23	14	20	17	22	7	3	0	9	11	5	2	4	1	8	6	10
16	16	13	20	18	12	15	17	21	19	22	14	23	1	5	4	11	7	0	9	2	6	3	10	8
17	17	12	19	21	14	13	20	16	23	18	22	15	4	1	10	5	0	6	3	8	2	7	9	11
18	18	23	16	14	15	19	21	22	17	12	13	20	11	8	5	2	9	3	4	0	7	10	1	6
19	19	22	15	17	18	14	23	20	13	16	21	12	9	10	3	4	2	8	0	5	11	6	7	1
20	20	14	23	16	22	12	19	17	15	21	18	13	10	4	9	1	6	2	7	11	8	0	3	5
21	21	15	17	22	13	23	16	18	20	14	12	19	5	11	1	8	3	7	10	6	0	9	4	2
22	22	19	21	12	23	20	18	14	16	13	15	17	8	2	11	6	10	9	1	7	3	4	5	0
23	23	18	13	20	21	22	15	19	12	17	16	14	3	9	7	10	8	11	6	1	5	2	0	4



Ejemplo en GF(2^4)

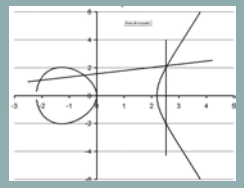




Generación con α=13

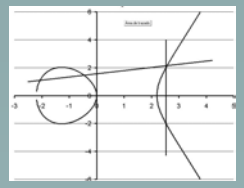
n	[n]α
0	0
1	13
2	7
3	15
4	3
5	23
6	9
7	19
8	10
9	20
10	4
11	17
12	1

n	[n]α
13	16
14	5
15	21
16	11
17	18
18	8
19	22
20	2
21	14
22	6
23	12
24	0



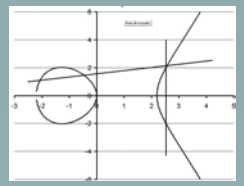
¿Y qué sigue?

- Funciones súper elípticas de género g
  - $y^2 + h(x)\, y = f(x)$ en $K(x,y)$
  - $h(x) \in K[x]$ es un polinomio de grado g a lo sumo
  - $f(x) \in K[x]$ es un polinomio de grado $2g+1$
  - K es un cuerpo y $\overline{K}$ su clausura transitiva
  - Ejemplo
    - $y^2 = x^5 - 5x^3 + 4x$

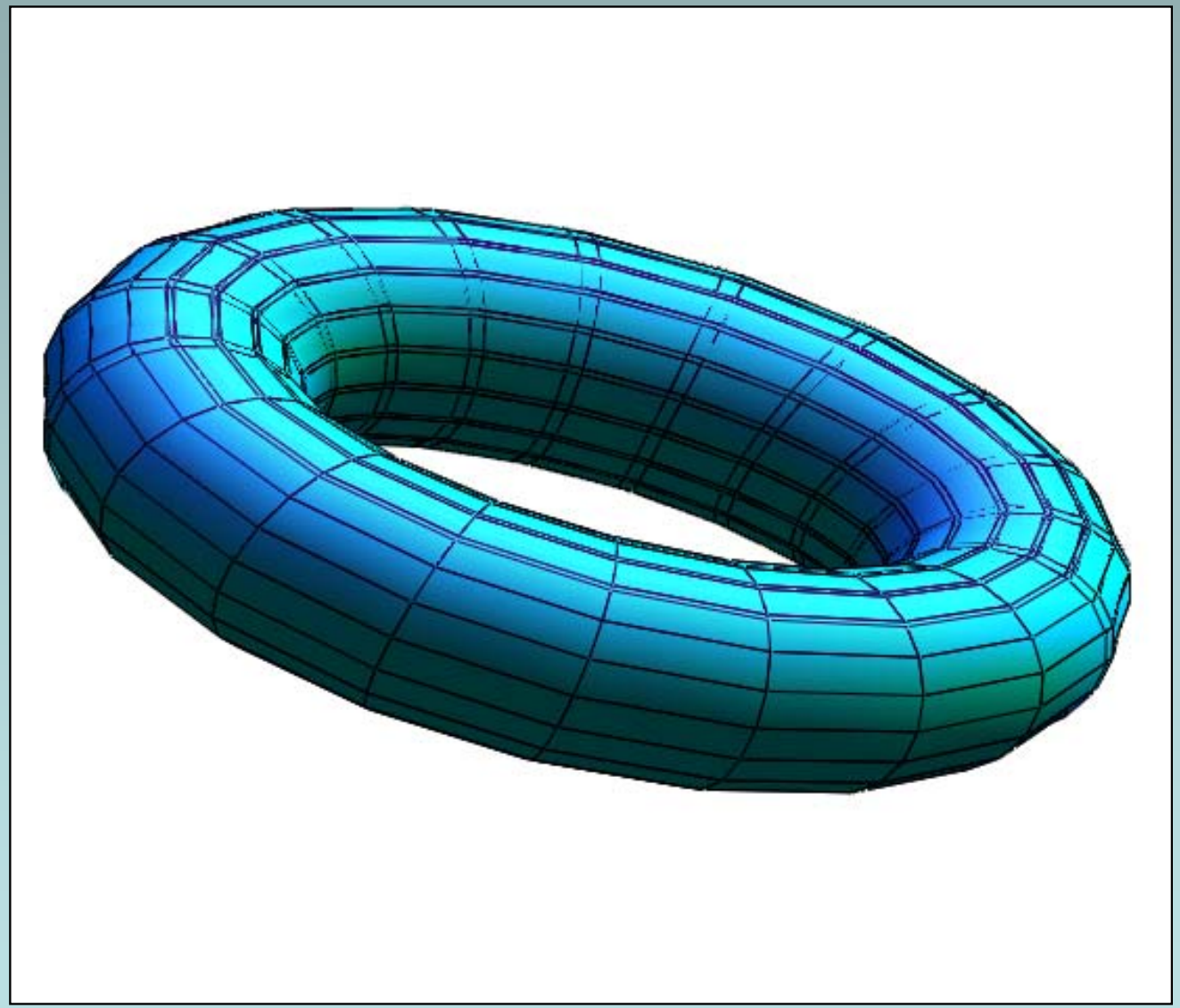


Ejemplo

$y^2 = x^5 - 5x^3 + 4x$



Toros



Q