Funciones Elípticas

Ing. Esteban di Tada*

Introducción

Las funciones elípticas son conocidas desde hace mucho. Sin embargo en este último tiempo han recibido una gran atención por parte de muchos matemáticos. Han sido el origen de importantes descubrimientos sobre todo en la teoría de números. El último teorema de Fermat es un ejemplo de ello así como nuevos métodos de factorización de números en sus factores primos. Una función elíptica no es una elipse. Esta vinculada con la noción de integrales elípticas que recibieron este nombre porque aparecen naturalmente cuando se quiere encontrar la longitud de un arco de una elipse. Así como el estudio de la longitud de la circunferencia da origen a las funciones trigonométricas, el cálculo de la longitud de los arcos de la elipse da origen a las integrales elípticas y sus funciones inversas las funciones elípticas. El estudio de las funciones elípticas empieza con Wallis en 1655[1] . Newton y Wallis publicaron una expansión infinita para calcular la longitud de un arco de elipse.

La definición formal de una función elíptica se establece a partir de la siguiente integral:

$$\int r\left(x,\sqrt{p(x)}\right)dx \quad (1)$$

donde **r(x,y)** es una función racional y **p(x)** es un polinomio de orden 3 o 4 sin raíces múltiples. En 1679, Jacob Bernoulli encontró una integral elíptica tratando de calcular la longitud de una espiral. En 1694 dio un paso importante en la teoría de las funciones elípticas analizando la forma de una varilla elástica comprimida en ambos extremos. Demostró que la curva satisfacía una integral de la forma

$$\frac{ds}{dt} = \frac{1}{\sqrt{1-t^4}} \quad (2)$$

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

cuyo arco tiene una longitud entre **0** y **x** dada por la siguiente integral $\int_0^x \frac{dt}{\sqrt{1-t^4}}$

En el gráfico adjunto se representa en forma gráfica la lemniscata

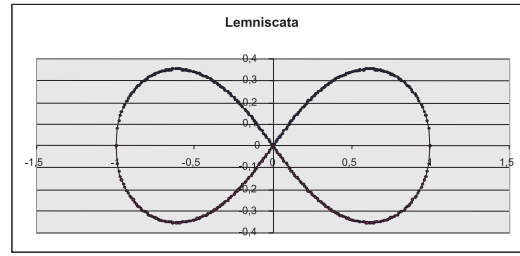
---

* Decano de la Facultad de Ingeniería. Universidad de Palermo.

1. John Wallis, hijo del reverendo John Wallis que fue ministro en Ashford en 1602, nació en 1617. A los 13 años de edad se consideró a sí mismo con suficiente madurez como para cursar la Universidad. El 1631 tomó sus primeros contactos con las matemáticas. En 1637 recibió su diploma de BA y en 1640 su Master. Se hizo famoso por su capacidad de descifrar mensajes. Un de sus libros más famosos fue *Arithmetica infinitorum.* En su libro *Tract on Conic Sections* describe las curvas que se obtienen cortando un cono con un plano.

La longitud de un arco de la curva representada por la función f(x) esta dada por la integral

$$\int_{x_0}^{x_1}\sqrt{1+\left(\frac{df}{dx}\right)^2}\,dx \qquad (3)$$



En el caso de una elipse cuya ecuación es

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1 \qquad (4)$$

se obtiene que

$$\frac{dy}{dx}=-\left(\frac{b}{a}\right)^2\frac{x}{y} \qquad (5)$$

reemplazando (5) en 3 se obtiene

$$\int_{x_0}^{x_1}\sqrt{1+\left(\left(\frac{b}{a}\right)^2\frac{x}{y}\right)^2}\,dx=\int_{x_0}^{x_1}\sqrt{1+\left(\frac{b}{a}\right)^4\left(\frac{x}{y}\right)^2}\,dx \qquad (6)$$

Reemplazando (4) en (6) se obtiene finalmente

$$\int_{x_0}^{x_1}\sqrt{\frac{a^2-\left(1-\frac{b^2}{a^2}\right)x^2}{a^2-x^2}}\,dx \qquad (7)$$

Para el caso particular de **a = b = r** (circunferencia) se obtienen las ecuaciones conocidas de la longitud de un arco de circunferencia.

La definición que usaremos para una función elíptica es mucho más sencilla aunque no por eso menos rica en sus resultados. Una función elíptica es un conjunto de puntos en el plano **xy** que satisfacen la siguiente ecuación

$$\mathbf{y^2 = Ax^3 + Bx^2 + Cx + D} \quad (7)$$

Esta definición[2] es vaga ya que no se especifica nada sobre los coeficientes y las variables x e y. Pueden ser números que pertenezcan a los reales ($\Re$), o a los complejos

2. Esta definición no es aplicable para ciertos casos en donde el dominio de definición sea un cuerpo de característica igual a 2 o igual a 3.

(**C**) (que tienen la propiedad de ser algebraicamente cerrados ya que todo polinomio cuyos coeficientes pertenezcan a *C* tiene sus ceros pertenecientes a los complejos) o pueden ser pertenecientes a los racionales (**Q**) o a un cuerpo finito (**F**) o, más precisamente, a un cuerpo de Galois **GF(p^n)** [3].

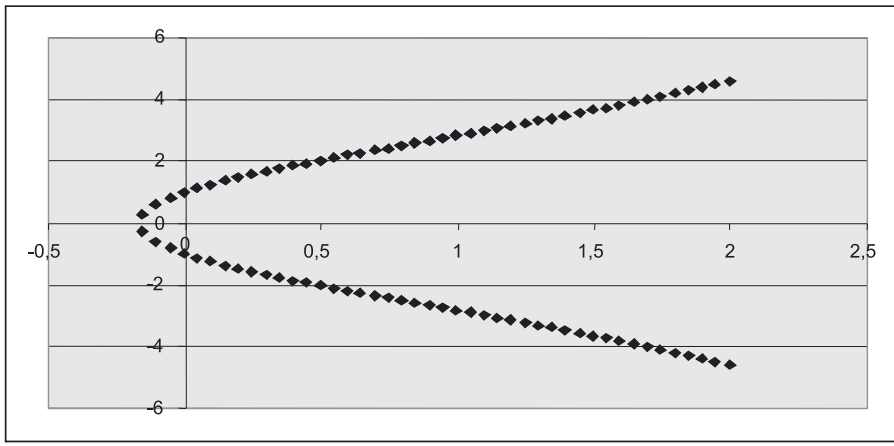
Por medio de un simple cambio de variables la ecuación (7) puede transformarse en la siguiente

$$\mathbf{y^2 = x^3 + ax + b} \quad (8)$$

Si se emplearan los siguientes valores

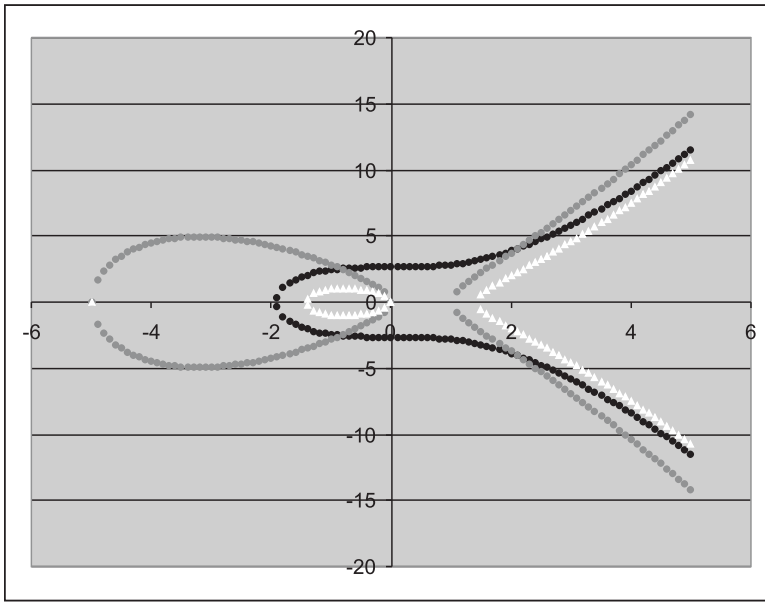
$$\mathbf{y^2 = x^3 + 6x + 1}$$

se obtendría la función que se representa en el siguiente gráfico. Cambiando los valores de a y b podrían generarse diferentes curvas.

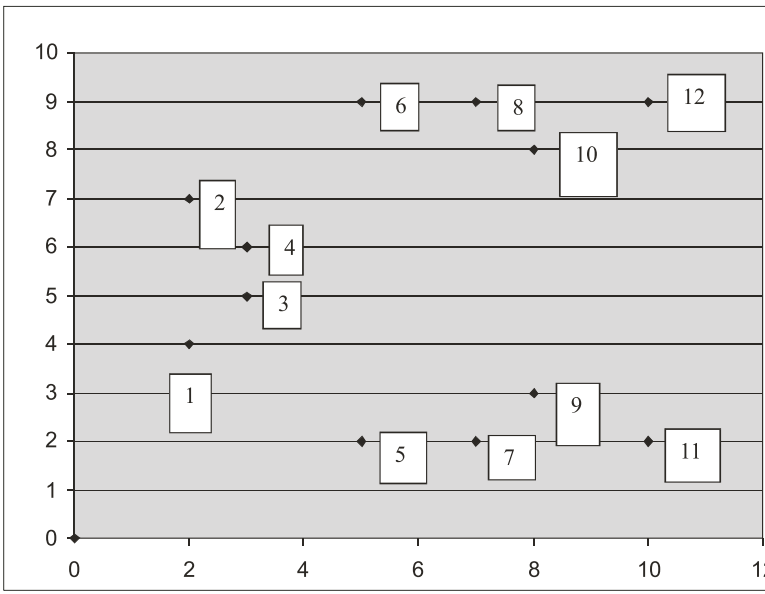


Siempre dentro de los reales se puede, variando los coeficientes, obtener otras formas de gráficos como los siguientes:

3. **p** es un número primo y **n** un entero mayor que **0**



La misma función calculada en GF(11) tiene la siguiente representación gráfica (La cantidad de puntos es finita)



Lo interesante es que sobre los puntos de la curva elíptica se puede definir una estructura de grupo, que en el ejemplo previo se representa por medio de la siguiente tabla:

X	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

Los números del gráfico corresponden al índice de las filas y columnas de la tabla de operaciones.

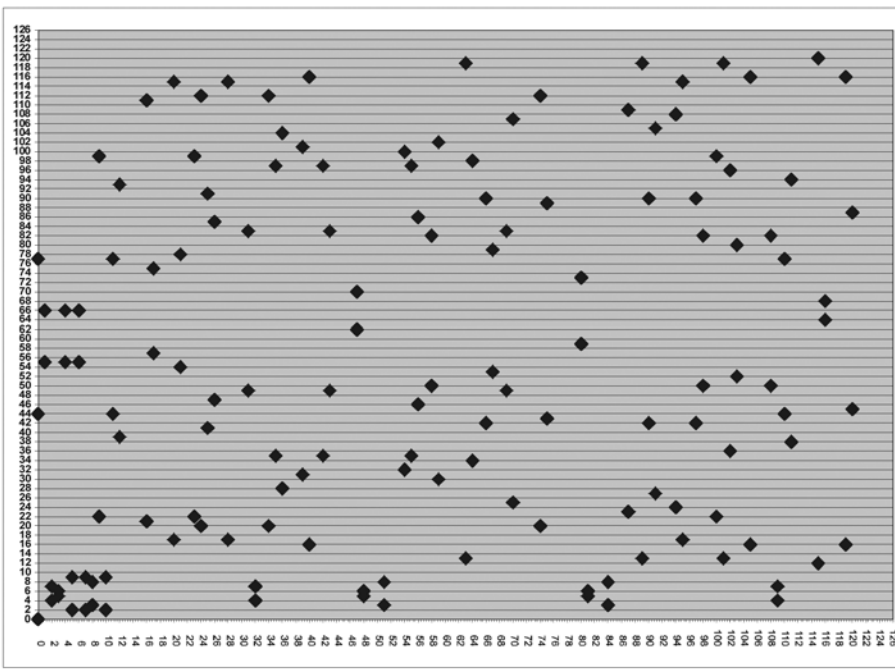
Es de hacer notar que si se renumeran los puntos de la curva elíptica de la siguiente manera

Valor actual	Nuevo valor
0	0
1	8
2	5
3	1
4	12
5	10
6	3
7	9
8	4
9	2
10	11
11	7
12	6

Y luego reordenando se obtiene la siguiente tabla[4]

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

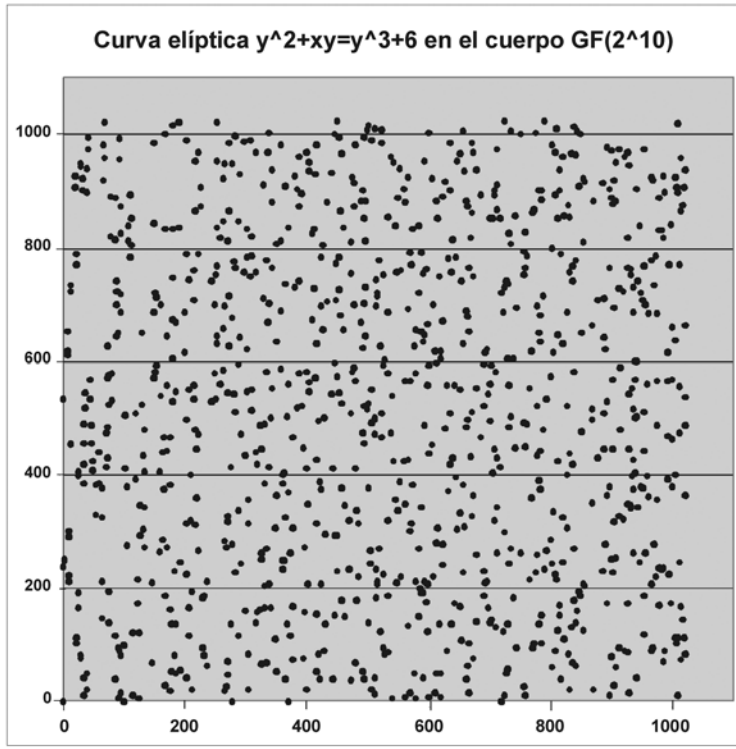
En cambio en GF(11^2) su representación gráfica es



4. La operación que se realizó es un isomorfismo (función biyectiva que conserva la estructura del grupo) entre los puntos de la función elíptica y el grupo de la clase residual de enteros módulo 13. Esta tabla se obtuvo a partir de las sumas sucesivas del punto **3=(3,5)** de la curva elíptica con 0 y consigo misma.

Si bien los puntos parecerían estar distribuidos al azar, se notan una serie de patrones. Ello se debe a la relación que existe entre los mismos y que permite definir operaciones entre los pares ordenados de coordenadas que definen cada punto.

Para el cuerpo GF(2^{10}) se obtendría el siguiente gráfico:



Las aplicaciones de las funciones elípticas cubren un amplio espectro que va desde la demostración del último teorema de Fermat hasta sus usos en criptografía.

Se obtuvo la tabla

$$n * 3 = \underbrace{3 + 3 + \ldots 3}_{\text{n veces}} = \sum_{j=1}^{j=n} 3$$

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

y se definió la correspondencia entre **n** y **n*3**. Los productos sucesivos de **3** generan todos los elementos del grupo, dado que es un grupo cíclico.

Las funciones elípticas y la criptografía

Las funciones elípticas han sido y son el origen de numerosas investigaciones en diversos aspectos de la Matemática teórica y aplicada. Entre las áreas en las que se las aplica se pueden mencionar:

Factorización de enteros. Se ha desarrollado un algoritmo para la factorización de números enteros basado en las curvas elípticas que es, en muchos sentidos, mejor que los empleados usando las técnicas convencionales de la teoría de números. Si bien la factorización de enteros ha atraído la atención de los matemáticos desde hace muchos siglos, en la actualidad el interés en su estudio ha aumentado considerablemente debido a su uso en problemas de seguridad en las comunicaciones, en las redes de computadoras y, particularmente, en Internet. En efecto, la seguridad de los métodos de firma electrónica basados en la tecnología RSA estriba en el hecho de la imposibilidad práctica de que, conocido un número que es el producto de dos números primos (de centenares de dígitos de longitud), sea posible realizar su factorización en tiempos razonables.

Números congruentes. Un número natural es llamado congruente si es el área de un triángulo rectángulo cuyos lados son números racionales. Si se denota como **x, y** y **z** los lados del triángulo, **n** será congruente si y sólo si el sistema de ecuaciones

$$x^2 + y^2 = z^2 , \quad n = \frac{1}{2} xy$$

tiene solución en **Q**. Este problema fue de mucho interés para los griegos y fue discutido por los árabes eruditos durante el siglo X. Fibonacci[5] probó que los números 5 y 6 son congruentes. Euler[6] probó que 7 es congruente. En 1983 Tunnell, de la Universidad de Rutgers, New Jersey, vinculó este problema con las funciones elípticas.

El último teorema de Fermat.[7] 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 $p \neq 3$ no existe una curva elíptica sobre **Q** cuya ecuación tenga la forma

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

5. Leonardo Pisano Fibonachi nació probablemente en la ciudad de Pisa en 1170 y murió en la misma ciudad en 1250. Recibió su educación en África del Norte donde su padre era embajador, representando los intereses comerciales de la República de Pisa.

6. Leonhard Euler nació en Basilea en 1707 y murió en San Petersburgo en 1783

7. Pierre de Fermat nació en Montauban en 1601 y murió en Castres en 1665. Fermat casi no escribió sus investigaciones en Matemática. Después de su muerte se encontraron hojas en las que él había esbozado sus descubrimientos.

con **a,b,a+b** todos números naturales que sean una potencia p de un entero. Por, lo tanto no existe una solución en **Z** de la ecuación

$$x^p + y^p = z^p$$

Su empleo en el cifrado es una de las aplicaciones que más ha coadyuvado al desarrollo de la teoría de las funciones elípticas.

La criptografía basada en grupos tiene gran utilidad en el desarrollo de mecanismos de firma digital. Existen muchos criptosistemas basados en el uso de los grupos definidos sobre curvas elípticas. Supóngase que se dispone de un grupo cíclico **G**[8] 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 $\alpha \in G$ que es su clave privada y publica su clave pública que es $\beta=\alpha^{-1}$ conjuntamente con G. Sea $\gamma \in G$ 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

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

el mensaje original. 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.

Se describirá el algoritmo de firma digital por curvas elípticas ***(ECDSA: Elliptic Curve Digital Signature Algorithm).***

Parámetros de dominio

Los parámetros de dominio para **ECDSA** consisten en una curva elíptica ***"aceptable"*** **E** definida sobre el cuerpo **GF(q)** de característica **p** y un elemento generador **P∈E(GF(q)).** Los parámetros de dominio pueden ser compartidos por un grupo de entidades o por un usuario simple[9].

Para facilitar la interoperabilidad y evitar ciertos ataques conocidos existen restricciones sobre la forma de seleccionar la curva elíptica y elegir el elemento generador.

Requerimientos del cuerpo

El orden del cuerpo finito es o bien un número primo o bien una potencia entera de 2. En el caso de ser un número primo es la clase residual **Z/pZ**. En el caso de ser $\mathbf{2^m}$ es el cuerpo generado por un polinomio irreducible de grado $\mathbf{2^m}$.

Requerimientos de la curva elíptica: Para evitar el método de factorización de Pollard y los ataques de Pong-Hellman[10], es necesario que la cantidad de puntos **Q-racionales**

---

8. Un grupo cíclico **C** es un grupo en el que existe un elemento tal que sus potencias sucesivas generan todos los elementos del mismo. Si $\alpha \in \mathbf{C}$ luego la función $\alpha^n \rightarrow \boldsymbol{n}$ es un isomorfismo entre el grupo **C** y **Z/nZ** (la clase residual modulo n).

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

10. J. Pollard, "*Montecarlo Computation for index computation mod p*", Mathematics of Computation, 32, (1978), 918-924

S. Pohlig and M. Hellman, "*An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*", IEEE transactions on Information Theory, 24(1978) 106-110.

de E, sea divisible por un número primo **n** suficientemente grande. La norma **ANSI X.969** requiere $\mathbf{n>2^{160}}$. Una vez elegido un cuerpo $\mathbf{F^q}$, **n** debe elegirse tan grande como sea posible y prácticamente debe ser **n≈q**. El orden del cuerpo que se denota $\mathbf{\#E(F_q)}$ es un número cuasi primo. En general se asume que $\mathbf{n > 2^{160}}$ y $\mathbf{n > 4\sqrt{q}}$. El cofactor **h** se define como $\mathbf{h = \#E(F_q)/n}$.

Algunas otras consideraciones se deben tener en cuenta tales como:

Que **p** no divida a $\mathbf{q^k-1}$ para $\mathbf{1 \leq k \leq C}$ donde **C** sea lo suficientemente grande como para hacer imposible el calcular el logaritmo discreto de un número (El valor de **C=20** es en general suficiente).

Resumiendo los parámetros de dominio son:

1. Un cuerpo de orden **q** (ya sea **q=p** o $\mathbf{q=2^n}$)
2. Un descriptor que defina la forma de representar los elementos del cuerpo $\mathbf{F_q}$.
3. Dos elementos $\mathbf{\alpha, \beta \in F_q}$ que definen la ecuación de la curva **E** sobre $\mathbf{F_q}$ [11].
4. Los valores $\mathbf{x_G, y_G \in F_q}$ que definen el elemento generador $\mathbf{G(x_G,y_G) \in E(F_q)}$.
5. El orden n del punto G con $n > 2^{160}$ y $n > 4\sqrt{q}$.
6. El cofactor $\mathbf{h = \#E(F_q)/n}$

Generación del par de llaves

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

1. Se selecciona un entero random (o seudo random) **d** tal que $\mathbf{1 \leq d \leq n - 1}$.
2. Se calcula **Q=[d]G** [12]
3. **Q** es la clave pública de **A** y **d** su clave privada

Generación y verificación de la firma

Generación de la 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 $\mathbf{1 \leq k \leq n - 1.}$
2. Calcula $\mathbf{[k]G=(x_1,y_1)}$
3. Calcula $\mathbf{r=x_1 \bmod n}$. Si **r** es nulo continua con el paso 1
4. Calcula $\mathbf{k^{-1}} \bmod \mathbf{n}$.

---

11. Por razones que se verán más adelante la ecuación será $\mathbf{y^2 = x^3+ax+b}$ para $\mathbf{F_p}$ **con p>3** y $\mathbf{y^2 + xy = x^3 + ax^2+b}$ para cuerpos F_{2^m}.

12. Se emplea la siguiente notación $[d] = \sum_{j=1}^{j=d} G$ donde la operación de suma es la del grupo definido en la función elíptica.

5. Crea **e** que es el compendio del documento **m**
6. Calcula $\mathbf{s=k^{-1}(e+dr) \bmod n}$. 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:

1. Verifica que $\mathbf{1 \leq r \leq n-1}$ y $\mathbf{1 \leq s \leq n-1}$
2. Calcula **e** como el compendio del mensaje **m**
3. Calcula $\mathbf{w = s^{-1} \bmod n}$.
4. Calcula $\mathbf{u_1 = ew \bmod n}$ y $\mathbf{u_2 = rw \bmod n}$
5. Calcula $\mathbf{X = [u_1]G + [u_2]Q}$
6. Si **X=O** rechaza la firma
7. Calcula $\mathbf{v = x_1 \bmod n}$ donde $\mathbf{X = X(x_1, y_1)}$
8. Acepta la firma si y solo si **v=r**

Prueba:

$$k \equiv s^{-1}(e + dr) \equiv s^{-1}e + s^{-1}dr \equiv we + wdr \equiv u_1 + u_2 d \pmod{n}$$

$$u_1 G + u_2 Q = (u_1 + u_2 d)G = kG$$

Por lo que **v=r**.

Comparación entre el método de funciones elípticas y otros métodos de firma digital

Seguridad

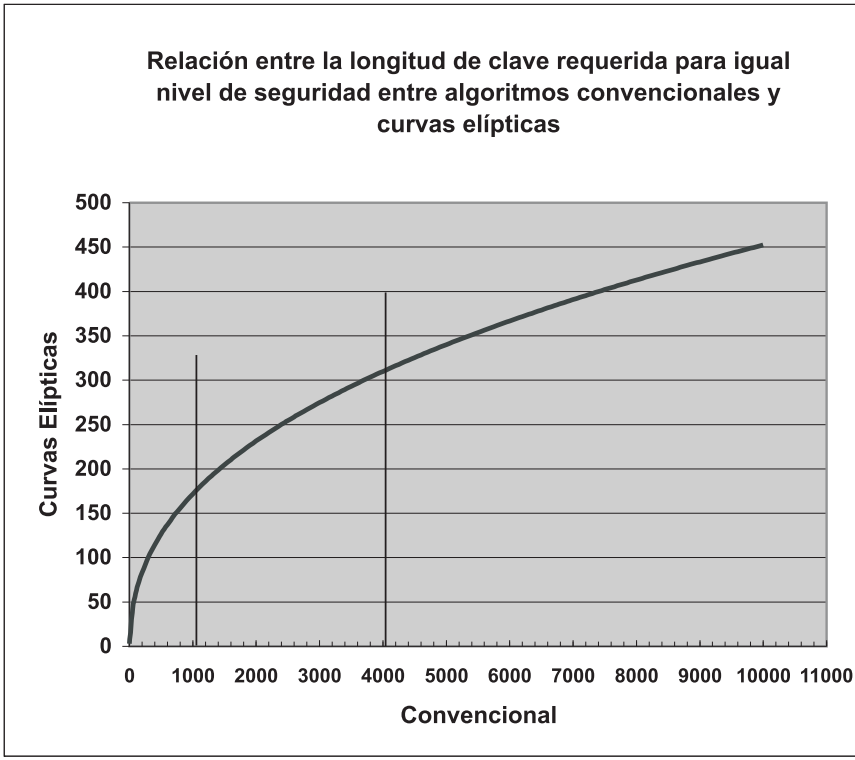
Este tema se desarrollará desde el punto de vista teórico. Es importante recalcar que la mayoría de los ataques a la seguridad son de carácter físico tales como sobornos a empleados para obtener las claves de acceso, pérdida por descuido de información confidencial, etc.

Desde un punto de vista teórico la relación entre la longitud de la clave en RSA y ECC está dada por la siguiente ecuación

$$\eta = \beta n^{1/3} \left(\log(n \log(2)) \right)^{2/3} \text{ donde } \beta \approx 4{,}91$$

En el siguiente gráfico se representa dicha curva[13]

13. Elliptic Curves in Cryptography, London Mathematical Society, Lecture Notes Series 265, Ian Blake, Gadiel Seroussi y Nigel Smart, Cambridge Press, 1999



Del análisis de la curva se deduce que a igual nivel de seguridad una clave de 1024 bits en RSA equivale a una de 160 bits usando curvas elípticas en tanto que una de 4000 es equivalente a una de 315 bits en ECC.

La otra pregunta que es lógico realizar es cuál es la complejidad de cálculo requerida En ECC una gran cantidad de cálculo puede ser realizado a priori. Además bases especiales para cuerpos de Gallois $\mathbf{F}_{2\mathbf{m}}$ pueden ser empleadas para acelerar el cálculo de operaciones módulo. Teniendo en cuenta el actual estado del arte se puede decir que ECC es un orden de magnitud (10 veces) superior que RSA y DSA[14].

14. The Elliptic Curve Cryptosystem, Certicon, 1977

Cuerpos

Un cuerpo es un ideal en el existe una inversa multiplicativa para cada elemento, excepto el cero. Un cuerpo es un triple $< \mathbf{K},+,* >$ con las siguientes propiedades:

1. $< \mathbf{K},+ >$ es un grupo abeliano con elemento neutro $\mathbf{0} \in \mathbf{K}$
2. $< \mathbf{K}-\{\mathbf{0}\},* >$ es un grupo abeliano con elemento neutro $\mathbf{1} \in \mathbf{K}-\{\mathbf{0}\}$
3. $\forall \mathbf{x,y,z} \in \mathbf{K}: \mathbf{x} * (\mathbf{z} + \mathbf{y}) = \mathbf{x} * \mathbf{z} + \mathbf{x} * \mathbf{y}$

Por ejemplo los números reales forman un cuerpo con respecto a la suma y producto habituales. En cambio los números enteros no forman cuerpo con respecto a la suma y la multiplicación dado que la inversa del producto no existe (La inversa de un entero no es un entero). Los racionales forman un cuerpo con respecto a la suma y multiplicación debido a que la inversa de un racional es un número racional.

Un subcuerpo es un subconjunto **S** de **K**, $\mathbf{S} \subseteq \mathbf{K}$ tal que $<\mathbf{S},+,*>$ satisface las propiedades definidas para el cuerpo **K**.

Existen cuerpos sobre conjuntos diferentes de los conjuntos de números. Supongamos por ejemplo el conjunto de los polinomios de la forma $\mathbf{x} + \mathbf{jy}$ donde $\mathbf{x,y} \in \mathbf{R}$ y **j** es un símbolo indeterminado por el momento. Definamos las siguientes operaciones:

1. $(x_1 + j\, y_1) + (x_2 + j\, y_2) = (x_1 + x_2) + j\, (y_1 + y_2)$

2. $(\mathbf{x}_1 + \mathbf{j}\mathbf{y}_1) * (\mathbf{x}_2 + \mathbf{j}\mathbf{y}_2)$ es el resto de dividir el polinomio producto por el polinomio $\mathbf{1} + \mathbf{j}^2$. El producto dará el polinomio siguiente

$$x_1\, x_2 - y_1\, y_2 + j\, (x_1 y_2 + x_2 y_1).$$

Nótese que de esta manera hemos definido el cuerpo de los complejos a partir de los polinomios definidos sobre los reales. Si $\mathbf{y}_1 = \mathbf{y}_2 = \mathbf{0}$ la suma y el producto quedarían definidos como en los números reales. Es decir que existe un subcuerpo de los complejos que es isomórfico a los reales[15]. Por extensión se dice que los reales son un subconjunto de los complejos o que los complejos son una extensión de los reales. Nótese que el polinomio $\mathbf{1} + \mathbf{j}^2$ no tiene ninguna raiz en los reales pero si la tiene en los complejos ya que $\mathbf{(0+j)*(0+j)} = \mathbf{-1+j0}$

Todos los ejemplos vistos son cuerpos infinitos. La clase residual módulo un número primo es un cuerpo con respecto a la suma y multiplicación módulo dicho número

15. La función $\mathbf{C} \rightarrow \mathbf{R}$ se define como $\mathbf{x} + \mathbf{j0} \rightarrow \mathbf{x}$

primo. Las operaciones de suma y producto de la clase residual módulo 11 se representan en las siguientes tablas:

*	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

+	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Es de hacer notar que en tanto que en los reales no existe ningún **n** tal que sumado el neutro de la multiplicación **(1) n** veces dé como resultado el neutro de la suma **(0)**, en este cuerpo si se suma **1** once veces el resultado es cero. La cantidad de veces que hay que sumar la unidad para obtener cero se llama la característica de un cuerpo. Si ese número no existe la característica se define como cero. Esta diferencia en el valor de la característica es la causa de ciertas diferencias entre los algoritmos que se expondrán en este trabajo.

Se considerará ahora cuerpos definidos sobre los binarios. De manera análoga a como fueron definidos los complejos, definiremos el cuerpo sobre los polinomios con coeficientes en el cuerpo de los binarios módulo el polinomio irreducible $\mathbf{p(x) = x^4 + x + 1}$. Para una mayor facilidad de representación gráfica se han codificado por el valor decimal que representan cuando el indeterminado se reemplaza por 2.

0	0	1	1	2	x	3	x + 1
4	x^2	5	$x^2 + 1$	6	$x^2 + x$	7	$x^2 + x + 1$
8	x^3	9	$x^3 + 1$	10	$x^3 + x$	11	$x^3 + x + 1$
12	$x^3 + x^2$	13	$x^3 + x^2 + 1$	14	$x^3 + x^2 + x$	15	$x^3 + x^2 + x + 1$

Este cuerpo se denomina **GF (2^4)** porque el polinomio que se emplea es de cuarto grado y los coeficientes pertenecen al cuerpo modulo 2^{16}.

16. GF son las iniciales de Galois Field. Evarist Galois fue el matemático francés que creó la teoría de los cuerpos finitos. Nació en 1811 y murió en un duelo en 1832 por razones que aun hoy no son claras.

Las operaciones quedan definidas por las siguientes tablas:

Tabla de producto

Esta es la tabla de multiplicación. Si se deseara multiplicar 5 por 9 ello equivaldría a multiplicar los polinomios $\mathbf{x^2 + 1}$ por $\mathbf{x^3 + 1}$ que da por resultado $\mathbf{x^5 + x^3 + x^2 + 1}$ y que dividido por $\mathbf{x^4 + x + 1}$ da como resto $\mathbf{x^3 + x + 1}$ que corresponde al polinomio 11.

Producto	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	2	4	6	8	10	12	14	3	1	7	5	11	9	15	13
3	3	6	5	12	15	10	9	11	8	13	14	7	4	1	2
4	4	8	12	3	7	11	15	6	2	14	10	5	1	13	9
5	5	10	15	7	2	13	8	14	11	4	1	9	12	3	6
6	6	12	10	11	13	7	1	5	3	9	15	14	8	2	4
7	7	14	9	15	8	1	6	13	10	3	4	2	5	12	11
8	8	3	11	6	14	5	13	12	4	15	7	10	2	9	1
9	9	1	8	2	11	3	10	4	13	5	12	6	15	7	14
10	10	7	13	14	4	9	3	15	5	8	2	1	11	6	12
11	11	5	14	10	1	15	4	7	12	2	9	13	6	8	3
12	12	11	7	5	9	14	2	10	6	1	13	15	3	4	8
13	13	9	4	1	12	8	5	2	15	11	6	3	14	10	7
14	14	15	1	13	3	2	12	9	7	6	8	4	10	11	5
15	15	13	2	9	6	4	11	1	14	12	3	8	7	5	10

Tabla de suma

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

En este caso la característica del cuerpo es **2** ya que **1+1=0.** Por otro lado todo elemento del cuerpo sumado consigo mismo da cero. Esto genera un inconveniente ya que la solución de ecuaciones cuadráticas $\mathbf{x^2 + ax + b = 0}$ se basa en la igualdad $\mathbf{(x + a)^2 = x^2 + 2ax + a^2}$. Esta igualdad no es válida en **GF** $\mathbf{(2^4)}$ y en todas las extensiones de cuerpos binarios, ya que $\mathbf{(x + a)^2 = x^2 + 2ax + a^2 = x^2 + a^2}$.

Por ejemplo $\mathbf{(3 + 12) = 15^2 = 10}$ **y** $\mathbf{3^2 + 12^2 = 5 + 15 = 10}$

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

Tabla de Potencias

En la tabla adjunta se han representado las sucesivas potencias de cada uno de los elementos del cuerpo (la potencia cero da la unidad para cualquier elemento) como es lógico suponer (debido a que la cantidad de elementos es finita) existe una potencia que da como resultado 1 (por ejemplo $\mathbf{2^{15} = 1}$) El valor de n tal que $\mathbf{x^n = 1}$ se llama orden del elemento y las potencias sucesivas conforman un subcuerpo con una cantidad de elementos igual al orden[17] (más el elemento neutro aditivo). En el caso en que exista un elemento que genera todo el cuerpo se dirá que el cuerpo es cíclico. En el ejemplo puesto **2**, es decir el polinomio **x**, es un elemento generador.

Las potencias sucesivas se muestran en la siguiente tabla:

17. El orden de un elemento debe dividir a la cantidad de elementos del grupo multiplicativo que en el ejemplo es $\mathbf{2^4 - 1 = 15}$

Potencias sucesivas	Resto de dividir por $x^4 + x + 1$	Código
x^0	1	1
x^1	x	2
x^2	x^2	4
x^3	x^3	8
x^4	x + 1	3
x^5	x^2 + x	6
x^6	$x^3 + x^2$	12
x^7	x^3 + x + 1	11
x^8	x^2 + 1	5
x^9	x^3 + x	10
x^{10}	x^2 + x + 1	7
x^{11}	$x^3 + x^2 + x$	14
x^{12}	$x^3 + x^2 + x + 1$	15
x^{13}	$x^3 + x^2 + 1$	13
x^{14}	x^3 + 1	9
x^{15}	1	1

Bases Normales

La operación de elevación al cuadrado es una operación lineal en los cuerpos de característica **2** como en el caso de **GF(2ⁿ)**. En efecto si **$\alpha, \beta \in$ GF(2ⁿ)**, será

$(\alpha+\beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2 = \alpha^2 + \beta^2$ ya que $2\alpha\beta = \alpha\beta + \alpha\beta = \alpha\beta(1+1) = \alpha\beta 0 = 0$

Por inducción completa puede demostrarse que

$$\left(\sum_{j=1}^{n}\alpha_j\right)^2 = \sum_{j=1}^{n}\alpha_j^{\,2} \quad \alpha \in FG(2^n)$$

En efecto si se supone que la propiedad es cierta para n $\left(\sum_{j=1}^{n}\alpha_j\right)^2 = \sum_{j=1}^{n}\alpha_j^{\,2}$, luego para **n+1** será

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

Una base normal sobre GF(2ⁿ) se define como el conjunto de elementos

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

donde $\alpha \in GF(2^n)$. Para que este conjunto constituya una base todos los α^{2k} deben ser linealmente independientes. En ese caso todo elemento $\beta \in GF(2^n)$ puede rescribirse de la siguiente manera $\beta = \sum_{j=0}^{n-1} \nu_j \alpha^{2^j}$ donde $\nu_j \in \{0,1\}$. Por lo tanto

$$\beta^2 = \left(\sum_{j=0}^{n-1} \nu_j \alpha^{2^j}\right)^2 = \sum_{j=0}^{n-1} \nu_j^2 \left(\alpha^{2^j}\right)^2 = \sum_{j=0}^{n-1} \nu_j \alpha^{2^{j+1}}$$

Reemplazando el índice de sumatoria **j** por **k-1** se obtiene

$$\beta^2 = \sum_{j=0}^{n-1} \nu_j \alpha^{2^{j+1}} = \nu_0 \alpha^{2^1} + \nu_1 \alpha^{2^2} + \nu_2 \alpha^{2^3} + ... + \nu_{n-1} \alpha^{2^n} \text{ pero } \alpha^{2^n} = \alpha \text{ de donde}$$

$$\beta^2 = \nu_{n-1} \alpha^{2^0} + \nu_0 \alpha^{2^1} + \nu_1 \alpha^{2^2} + \nu_2 \alpha^{2^3} + ... + \nu_{n-2} \alpha^{2^{n-1}}$$

De la ecuación anterior se deduce que el efecto de elevar al cuadrado es el de rotar circularmente los coeficientes ν_j hacia la derecha.

La siguiente tabla muestra la base generada por el elemento **8** del cuerpo que equivale al polinomio x^3 (representado por el valor de sus coeficientes como **1,0,0,0**).En las tablas adjuntas se incluyen las representaciones en dicha base de todos los elementos del cuerpo así como también las tablas de potencias de todos los elementos. Es conveniente recordar que cada elemento del cuerpo **GF(2^n)** es en realidad un polinomio pero que, para simplificar este texto, se lo representa por el valor decimal que tiene su representación binaria. Es así que el elemento 12 representa al polinomio $1x^3+1x^2+0x+0$ que se escribirá en forma binaria **1100**. Si se elige $\alpha = 8$ las sucesivas potencias serán $\alpha^1 = \alpha$, $\alpha^2 = 1\ 2$, $\alpha^4=15$ y $\alpha^8=10$. En este espacio vectorial el elemento **11** sería igual a $\alpha+\alpha^2+\alpha^4=11$ que representado sólo por sus coeficientes resulta **1110**. Su cuadrado **($11^2=9$)** se puede calcular rotando los coeficientes hacia la derecha con lo que se obtiene **0111** que corresponde al elemento **9**.

Base: 8 Polinomio: "1,0,0,0"

8	12	15	10	
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

Tabla de Potencias

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Tabla de Ordenes
1	1															1
2	2	4	8	3	6	12	11	5	10	7	14	15	13	9	1	15
3	3	5	15	2	6	10	13	4	12	7	9	8	11	14	1	15
4	4	3	12	5	7	15	9	2	8	6	11	10	14	13	1	15
5	5	2	10	4	7	8	14	3	15	6	13	12	9	11	1	15
6	6	7	1													3
7	7	6	1													3
8	8	12	10	15	1											5
9	9	13	15	14	7	10	5	11	12	6	3	8	4	2	1	15
10	10	8	15	12	1											5
11	11	9	12	13	6	15	3	14	8	7	4	10	2	5	1	15
12	12	15	8	10	1											5
13	13	14	10	11	6	8	2	9	15	7	5	12	3	4	1	15
14	14	11	8	9	7	12	4	13	10	6	2	15	5	3	1	15
15	15	10	12	8	1											5

Esta metodología resulta muy útil para obtener grandes potencias. Supongamos que se desea calcular $\mathbf{9^{20}}$. Esta expresión es igual $\mathbf{9^{16}9^{4}}$ que resulta $9^{24}\,9^{22}$. Pero 9^{24} se obtiene rotando 4 veces la cadena de coeficientes (como los coeficientes son solamente 4 ello significa que no se rotan) y $\mathbf{9^{22}}$ se obtiene rotando dos puestos los coeficientes. Por lo tanto $\mathbf{9^{20} = 9^{*}14=7}$. Ello implica que elevar a la potencia 20 se ha realizado con 2 rotaciones y un producto en lugar de 20 productos.

Tabla de Producto

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

Si se quisiera calcular $\mathbf{9^{1300} = 9^{1024}9^{276} = 9^{1024}9^{256}9^{20} = 9^{1024}9^{256}9^{16}9^{4}}$ que se puede rescribir de la siguiente manera $\mathbf{9^{2^{10}}\,9^{2^{8}}\,9^{2^{4}}\,9^{2^{2}}}$. Por lo tanto el proceso es el siguiente

1. Rotar los coeficientes de **9 (0111) 10** veces a la derecha. Pero dado que cada cuatro rotaciones se obtiene el mismo valor, el resultado es rotar solo dos veces hacia la derecha obteniéndose **1101** que corresponde al elemento **14**.
2. Rotar los coeficientes de **9 (0111) 8** veces a la derecha. Pero dado que cada cuatro rotaciones se obtiene el mismo valor, el resultado es no rotar obteniéndose **0111** que corresponde al elemento **9**.
3. Rotar los coeficientes de **9 (0111) 4** veces a la derecha. Pero dado que cada cuatro rotaciones se obtiene el mismo valor, el resultado es no rotar obteniéndose **0111** que corresponde al elemento **9**.
4. Rotar los coeficientes de **9 (0111) 2** con lo que se obtiene el valor **1101** que corresponde al elemento **14**.

El resultado final será $\mathbf{9^{1300}=14*9*9*14=6.}$ En este caso **1300** multiplicaciones se han reemplazado por **4** rotaciones y **4** productos.[18]

Se puede demostrar que las bases normales existen para $\mathbf{n \geq 1}$[19]. Las bases normales son de suma utilidad para la implementación de las operaciones por hardware.

Otro empleo interesante de la definición de una base es el cálculo de las inversas de un dado elemento[20]. En efecto si $\boldsymbol{\alpha \in GF(2^n)}$ puede demostrarse que $\alpha^{2^n-1}=1$. Por lo tanto será $\alpha^{2^n-2}=\alpha^{-1}$. En el anterior se ve que $\alpha^{14}=\alpha^{-1}$. Pero α^{14} puede escribirse como $\alpha^8\alpha^4\alpha^2$. La expresión anterior puede rescribirse como $\alpha^{2^3}\alpha^{2^2}\alpha^{2^1}$. Es decir que α-1 es igual **(010110100101)=6**x**7**x**6=6**. Dejamos al lector obtener el algoritmo general de cálculo de la inversa. (Será $\alpha^{-1} = \alpha^{2^{n-1}}\alpha^{2^{n-2}}\ldots\alpha^{2^1}$)

18. En realidad se ha omitido en lo expuesto como se calculan los exponentes por lo que en este caso hay que agregar una serie de operaciones que hay que realizar para determinar la forma de separar el producto (para ello hay que calcular una serie de logaritmo base 2 y operaciones de suma y resta). El logaritmo base 2 se puede determinar en base a tablas(Si se desean hacer operaciones de hasta 4000 bits, las tablas tendrían a lo sumo 4000 entradas)

19. Ver Emil Artin, Galois Theory, Dover Publications, Inc., New Cork, Pag. 66

20. Recuérdese que la inversa de α que se la denota como α^{-1}es un elemento β tal que $\alpha\beta=1$.

Funciones Elípticas

Definición:

Para todo $A,B \in K$ se define una curva elíptica **E** como el conjunto de puntos $(x,y) \in K \times K$ que satisfacen la ecuación

$$y^2=x^3+Ax+B$$

conjuntamente con un punto ideal **O**. Por motivos que se aclararán más adelante, el punto O se llamará ***identidad***. El resto de los puntos (excepto la identidad) se llamarán puntos finitos.

Definición:

Si **k** es un subcuerpo de **K** y $A,B \in k$ se definen los puntos **k-racionales** de **E** como los puntos de **E** que pertenecen a k^2. El conjunto de puntos k-racionales se lo denota con **E(k)**. Formalmente

$$(a,b) \in E(k) \Leftrightarrow (a,b) \in E(K) \text{ y } a,b \in k$$

Definición:

Una curva elíptica **E** definida por la ecuación $y^2=x^3+Ax+B$ se llamará no singular si y sólo si el polinomio $Y^2=X^3+AX+B$ tiene tres raíces distintas (Ver anexo B).

Si la característica del cuerpo fuera 2 ó 3 la definición de una función elíptica deberá ser realizada por una función más compleja que la empleada, como se vera más adelante para el caso de cuerpos de característica 2.

Polinomios

Recordemos que una función elíptica **E** es el conjunto de pares de valores **x**, **y** que satisfacen la ecuación $y^2=x^3+ax+b$ [21].

La herramienta básica empleada para el estudio de las funciones elípticas se basa en la definición de un espacio de polinomios sobre las funciones elípticas para luego obtener conclusiones analizando las propiedades de dichos polinomios. Notaremos como **K[X,Y]** [22] el conjunto de polinomios definidos sobre el conjunto de pares de puntos **x** e **y** que definen una función elíptica y que se denotará como **E**. Dos elementos de **K[X,Y]** que difieren en un múltiplo de Y^2-X^3-AX-B definirán la misma función sobre **E**, ya que dicha expresión será nula. Si se deseara ser estrictamente formal se debería definir el anillo cociente

$K[X,Y]/(Y^2-X^3-AX-B)$

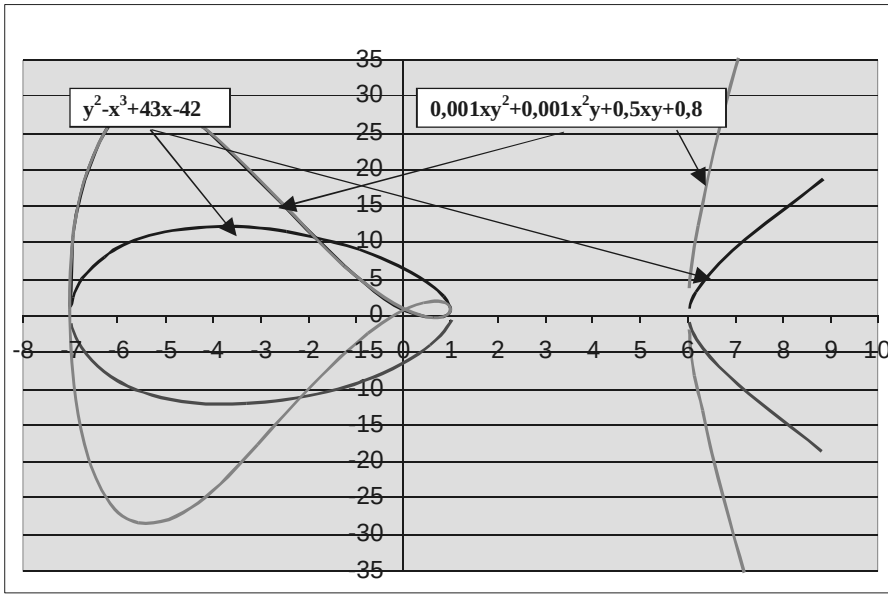
---

21. La eliminación del término cuadrático en **x** no quita generalidad al planteo dado que mediante un desplazamiento del eje de las **x** se puede obtener una función con el coeficiente del término cuadrático diferente de cero. La suma de los ceros de esta ecuación es cero. Como se verá, la definición de una función elíptica dependerá de la característica del cuerpo sobre la que se defina.

22. K[X,Y] es un polinomio en x cuyos coeficientes son polinomios en Y

donde
(Y^2-X^3-AX-B)
es el ideal generado por
Y^2-X^3-AX-B

En el gráfico siguiente se ha representado la función elíptica **$y^2 - x^3 + 43x - 42$** y el polinomio **$0{,}001xy^2 + 0{,}001x^2y + 0{,}5xy + 2$**



Del gráfico se desprende que el polinomio tiene cinco ceros. Se estudiarán las propiedades de los polinomios y de las funciones racionales por la ubicación de sus ceros y polos. Se demostrará que si dos polinomios tienen sus ceros y polos iguales y un valor común, entonces son iguales.

La realidad es que los polinomios están definidos sobre **E** (Es decir los pares de valores satisfacen la ecuación de la función elíptica), por lo que se puede emplear esta relación para reemplazar toda aparición de una potencia de **Y** mayor que 1. Por ejemplo el polinomio **$xy + x^2y^2 + x^3$** se reduce a **$x^2(x^3 + Ax + B) + x^3 + xy = x^5+(A+1)x^3+B+yx$.**

Un polinomio sobre **E** es un elemento de **K[x, y]** que denotaremos como **K[E]**.

Una importante consecuencia de esta definición es que todo polinomio sobre **E** se puede escribir como **$f(x,y) = v(x) + yw(x)$**[23]

23. Un polinomio con dos indeterminantes puede definirse como un polinomio de un indeterminante en **x** con coeficientes pertenecientes a un anillo de polinomios en **y**. Y dado que satisface la ecuación elíptica (**$y^2=x^3+ax+b$**), toda aparición de una potencia de **y** mayor que **1** puede ser reemplazada por un polinomio en **x** multiplicado por **y** elevado a una potencia menor que **2**.

Se definirá como el conjugado del polinomio $\mathbf{f(x)=v(x)+yw(x)}$ al polinomio $\overline{\mathbf{f(x)}} = \mathbf{v(x)-yw(x)}$ y su norma $\mathbf{N(f)} = \mathbf{f}\,\bar{\mathbf{f}}$ [24]

Es de remarcar que la norma de un polinomio es una función de **x** exclusivamente. En efecto $\mathbf{N(f)} = \big(\mathbf{v(x)+yw(x)}\big)\big(\mathbf{v(x)-yw(x)}\big) = \mathbf{v(x)^2 - y^2\, w(x)^2}$ y empleando la definición de la función elíptica se obtendría $\mathbf{v(x)^2 - s(x)\, w(x)^2}$ donde $\mathbf{s(x) = x^3 + ax + b}$. Luego $\mathbf{N(f) \in K[x]}$, es decir que la norma de un polinomio es un polinomio sólo de la indeterminada **x**. Adicionalmente se puede demostrar que **N(fg)=N(f)N(g).**

Funciones Racionales

Una función racional sobre **E** es una clase de equivalencia de cocientes formales de polinomios $\mathbf{r = f/g}$ [25] (con **g** no idénticamente nulo) en donde la igualdad entre **f/g** y **h/k** se define por medio de la igualdad de los productos **fk=gh**. La manera de verificar si dos funciones racionales son iguales es la de escribir **f, g, h** y **k** en su forma canónica **(f(x,y) = v(x) + yw(x))**, efectuar el producto y volver a transformarlo en su forma canónica y luego probar que los polinomios en **x** son iguales. Dado $\mathbf{r_1=f_1/g_1}$ y $\mathbf{r_2=f_2/g_2}$ estarán en relación $\mathbf{r_1 \approx r_2}$ si y sólo si $\mathbf{f_1g_2 = g_1f_2}$. El conjunto de funciones racionales es un cuerpo que se denota como **K(E)**. En efecto, la suma y el producto de dos funciones racionales da por resultado una función racional, existe un elemento neutro para la suma y el producto ($\frac{\mathbf{0}}{\mathbf{1}}$ y $\frac{\mathbf{1}}{\mathbf{1}}$) respectivamente, la suma es distributiva con respecto al producto y para toda función racional $\frac{\mathbf{f}}{\mathbf{g}}$ existe el inverso $\frac{\mathbf{g}}{\mathbf{f}}$ si **f** no es idénticamente nulo. Es de hacer notar la similitud que existe entre las funciones racionales y los números racionales. Ambos están definidos como pares ordenados de elementos pertenecientes a anillos (las funciones racionales pertenecientes al anillo de los polinomios en dos indeterminadas y los números racionales perteneciente a los números enteros). Por otro lado las funciones racionales definidas sobre el anillo de polinomios de grado cero es isomórfica con el conjunto de los números racionales.

Pero, mientras los polinomios pueden evaluarse a un valor finito en todo punto finito, las funciones racionales pueden no tener valores finitos en todos los puntos finitos de **E** (debido a la posibilidad que el denominador se anule) y pueden tener un valor que se lo notará como **O** [26]. Los puntos para los cuales el denominador se anula se llamarán polos. Nótese que si $\mathbf{r = f/g}$ multiplicando numerador y denominador por $\bar{\mathbf{g}}$ se puede demostrar que **r(x,y)=a(x)+yb(x)** donde **a** y **b** son funciones racionales de **x**

24. Nótese la similitud con el conjugado de los números complejos

25. En realidad definirlo como un cociente es una forma de representación de un par ordenado. Nótese la analogía con los números racionales

26. El punto **O** recibe el nombre de la identidad y no se encuentra dentro del conjunto de los puntos finitos. Es el punto en el infinito de la geometría proyectiva.

solamente. La demostración es muy sencilla teniendo en cuenta la definición del conjugado de un polinomio.

Definición:

Si **r** es una función racional sobre **E** y **P∈ E** es un punto finito se dirá que **r** es finita en **P** si existe una representación de **r = f/g** donde **f** y **g** son polinomios sobre **E** y **g(P) ≠ 0**. Si **r** es finita en **P** se pondrá **r(P) = f(P)/g(P).**

Más complicado es definir una función racional en el punto **O** aún cuando dicho valor exista. El método normal en Análisis para encontrar el valor (o el límite) de una función racional en el infinito es comparar los grados de denominador y numerador. En el caso de las funciones elípticas el problema es más complicado debido a la existencia de dos variables, **x** e **y**. Aún cuando parecería razonable asignar grado **1** a **x** e **y**, esto no sería consistente con la relación fundamental $y^2=x^3+ax+b$, en donde el grado **3** de **x** se ***"equipara"*** al grado **2** de **y**. Esta relación llevaría a pensar que el grado de **y** debería ser **3/2** del de **x**, ya que al reemplazar y^2 por su equivalente $x^3 + ax + b$, un exponente de **2** de **y** se transforma en un exponente de **3** de **x**. Dado que no es conveniente emplear grados fraccionales, se asignará el exponente **3** a **y** y **2** a **x**. Con el fin de evitar confusiones, se usará denotar el grado del polinomio f en x solamente por medio de la notación $\mathbf{grd_x(f)}$.

Definición:

Sea **f(x,y) = v(x) + yw(x)** un polinomio sobre **E** no idénticamente cero. El grado de **f** se define como

$$\mathbf{grd(f) = max[2\times grd_x(v),3+2\times grd_x(w)]}$$

Si **f** fuera una función sólo de **x**, su grado sería el doble del grado de acuerdo con la definición convencional.

Lema:

Este lema vincula al grado con la definición de norma y justifica la definición de grado empleada. Si **f** es un polinomio sobre **E** luego

$$\mathbf{grd(f) = grd_x(N(f))}$$

Demostración: f(x,y) = v(x) + y×w(x) luego

$$\mathbf{N(f)(x) = v^2(x) - s(x)w^2(x) \Rightarrow grd(N(f)) = max\ [2\times grd_x(v),3 + 2\times grd_x(w)]}$$

dado que el grado de **s(x)** es **3**.

Proposición: Si f y g son polinomios, entonces grd(fg) = grd(f)+grd(g).

Demostración:

$$\mathbf{grd(fg) = grd_x(N(fg)) = grd_x(N(f)\ N(g)) = grd_x(N(f)) + grd_x(N(g)) = grd(f) + grd(g)}$$

La demostración que $\mathbf{grd_x(N(f)\ N(g)) = grd_x(N(f)) + grd_x(N(g))}$ es inmediata ya que se trata de polinomios de una sola indeterminada.

Es de hacer notar que la definición de grado dada no tiene sentido de manera individual. Por lo tanto no se puede referir al grado del denominador ni del denominador de una función racional en forma individual. Sin embargo es posible referirse a la diferencia de grados entre el numerador y el denominador que si está bien definida. Por ejemplo si **r=f/g, r** puede ser igual a **h/k** pero **grd(f)** $\neq$ **grd(h)**. Pero dado que la igualdad se define por medio de la expresión **fk = gh** por lo demostrado anteriormente resulta que
grd(f) + grd(k) = grd(g) + grd(h) $\Rightarrow$ **grd(f) - grd(g) = grd(h) - grd(k)**

Con lo que se demuestra que la diferencia de grado entre el numerador y el denominador de una función racional es un invariante para todas las funciones racionales pertenecientes a la misma clase de equivalencia y por lo tanto su definición es coherente. Es decir la diferencia entre el grado del numerador y el denominador es una función de la clase de equivalencia y no de la función racional.
Supóngase que r = f/g es una función racional sobre E. Si grd(f)<grd(g) luego r(O)=0.
Si **grd(f)>grd(g)** luego **r(O)** no es finita y se lo representará por medio de la notación **r(O)** = ∞.
Si **grd(f)=grd(g)** se deberán distinguir dos casos diferentes:
Si **grd(f)** es par, entonces en la definición de grado el máximo corresponde a $2\times\mathbf{grd}_x\mathbf{(v)}$, y por tanto los términos de mayor exponente serán del tipo $\mathbf{ax^d}$ **y** $\mathbf{bx^d}$ para **f** y **g** respectivamente. Luego será **r(O)=a/b.**
Si **grd(f)** es impar, entonces en la definición de grado el máximo corresponde a $3+2\times\mathbf{grd}_x\mathbf{(w)}$ y por tanto los términos de mayor exponente serán del tipo $\mathbf{ayx^d}$ **y** $\mathbf{byx^d}$ para **f** y **g** respectivamente. Luego será **r(O)=a/b** [27].
Si **r** y **s** son dos funciones racionales con **r(O)** y **s(O)** finitos luego **rs(O)=r(V)s(O)** y **(r+s)(O)=r(O)+s(O)** [28].

Ceros y Polos

Resulta sencillo definir qué es un cero y qué es un polo. Sea **r=f/q** una función racional sobre **E** y **P(x,y)**$\in$ **E** un punto de la función. Si **r(P)=0** se dirá que **r** tiene un cero en **P** y si **r(P)=**∞ [29] se dirá que **r** tiene un polo en **P**.

Lo que no resulta fácil es definir la multiplicidad de dicho cero. Antes de enunciar el teorema que permitirá definir las multiplicidades de los ceros, se debe recordar que se asume que **E** es no singular lo que implica que el polinomio $\mathbf{X^3 + AX + B}$ tiene sus tres raíces ω_1, ω_2 y ω_3 diferentes. Luego los puntos $(\omega_1,0)$, $(\omega_2,0)$ y $(\omega_3,0)$ [30] pertenecen a **E** y serán llamados puntos de orden **2**. Como se demostrará posteriormente, al definir la

---

27. Demostrar como ejercicio que si **r** y **s** son funciones racionales con **r(O)** y **s(O)** finitos, entonces **rs(O) = r(O)s(O) y (r + s)(O)=r(O)+s(O)**
28. La función **r+s** se define de la siguiente manera **P**$\in$**(r+s)(Q)** $\leftrightarrow$**P=r(Q)+s(Q)**
29. Un polo puede existir debido a que **f** vale infinito o a que **q** es nulo.
30. La notación **(**ω**,0)** representa un punto donde **x** es igual a ω e **y** es igual a **0**. Esto es valido para ω_1, ω_2 y ω_3 dado que son las raíces del polinomio $\mathbf{X^3 + AX + B}$

estructura de grupo sobre los puntos de la curva elíptica, la suma de dichos puntos con sigo mismo, da por resultado el punto neutro del grupo.

Teorema:

Para cada punto **P∈ E** existe una función racional **u** tal que **u(P)=0** con la siguiente propiedad: Si **r** es cualquier función racional no idénticamente nula, luego $\mathbf{r = u^d s}$ para un entero **d** y una función racional **s** que es finita y diferente de cero en **P**. El valor de **d** no depende de la elección de la función **u**.

En términos menos formales, si una función racional tiene un cero en **P**, se puede representar por el producto de dos factores. El primero es una función racional **u** que se anula en **P** elevada a un exponente **d** (que no depende de la elección de **u**) y el segundo una función racional **s** diferente de cero en **P.**

La demostración de este teorema no es compleja pero es engorrosa y se incluye en el **anexo A.**

Una función **u** que satisface el teorema anterior recibe el nombre de ***variable uniformizadora*** o ***uniformizador*** en **P**. Si **r** es una función racional y $\mathbf{r = u^d s}$ donde **u** es una variable uniformizadora en **P**, el orden de **P** se define

ord(P) = d [31]

Se define la multiplicidad de un cero como el orden de la función y la multiplicidad de un polo como el negativo del orden de la función. Si un cero o uno polo tienen una multiplicidad de uno, dos, tres,…, etc. se dirá que se trata de un cero o de un polo simple, doble, triple,… respectivamente.

Ejemplos:

1. Sea el punto **P∈ E** y supóngase que **P=(k,n)** donde **k, n∈ K** y **n ≠ 0**. Sea **u = x - k** una función uniformizadora en **P**. Dado que **u** es un uniformizador en **P**, se ve que $\mathbf{ord_P (u) = 1}$. Considérese el punto **P'= (k, -n)** que también pertenece a **E** (Puesto que $\mathbf{y^2=(-y)^2}$) para el que $\mathbf{ord_{P'} = 1}$. Todo otro punto de **E** tiene orden cero. La función **u** tiene un polo en **O** y dado que **grd (u)= 2**, se deduce que $\mathbf{ord_O(u) = -2}$. En resumen **u** tiene dos ceros simples y un solo polo doble.

2. Considérese la función **y**. Esta función es uniformizante en los puntos $\mathbf{(\omega_1,0)}$, $\mathbf{(\omega_2,0)}$ y $\mathbf{(\omega_3,0)}$. Por lo tanto tiene ceros simples en dichos puntos. Además todos los otros puntos excepto **O** son de orden cero. Dado que **y** es de grado **3**, tiene un polo triple en **O**.

3. Considérese la función racional **u=x/y**. Esta función tiene un cero simple en **O** [32] como así también en los puntos $\mathbf{(0,\sqrt{B})}$ y $\mathbf{(0, -\sqrt{B})}$[33] y polos simples en los tres puntos $\mathbf{(\omega_1,0)}$, $\mathbf{(\omega_2,0)}$ y $\mathbf{(\omega_3,0)}$ de orden **2**

31. Esta definición es similar a la empleada en las funciones racionales definidas sobre los complejos.
32. El grado de **x** es **2** y el de **y** es **3**. Luego su diferencia es 1
33. $\mathbf{F(x, y)= y^2 - x^3 + Ax + B}$ de donde $\mathbf{F(x,\sqrt{B}) = F(x, -\sqrt{B}) = 0}$

Los ejemplos anteriores sugieren el siguiente teorema:
Sea **r** una función racional sobre **E**, luego $\sum_{P \in E} \mathbf{ord_P(r) = 0}$

Lema: La siguiente es una propiedad de los polinomios sobre **E**. Sea **f** un polinomio sobre **E**. La suma de las multiplicidades de los ceros de **f** iguala su grado.

Sea **n** el grado de **f**. Se demostró que $\mathbf{grad_x(N(f)) = n}$ [34] por lo que **N(f)** será, dado que es un polinomio de **x** exclusivamente

$\mathbf{N(f) = (x - a_1)\,(x - a_2)\,(x - a_3)\ldots..\,(x - a_n)}$

donde $\mathbf{a_i \in K}$ no obligatoriamente todos distintos. Ahora bien, si $\mathbf{a_i \neq \omega}$ luego $\mathbf{x\text{-}a_i}$ tiene dos ceros sobre **E** ya que $\mathbf{P(a_i, y)}$ y $\mathbf{P(a_i, -y)}$ pertenecen a la curva. Si $\mathbf{a_i = \omega}$ tendrá un solo cero pero doble ya que $\mathbf{s(\omega) = 0}$ y por tanto $\mathbf{N(f)(\omega) = v^2(\omega)}$. Por lo tanto **N(f)** tiene **2n** raíces contando multiplicidades. Pero **f** y $\bar{\mathbf{f}}$ tienen la misma cantidad de ceros ya que la función elíptica es simétrica con respecto al eje de las x. Con esto queda demostrado el lema.

Resulta simple demostrar que $\sum_{P \in E} \mathbf{ord_p(r) = 0}$. En el párrafo anterior se demostró que $\sum_{P \in E - O} \mathbf{ord_p(r)}$ es la suma de las multiplicidades de los ceros de **f**. Por el otro lado, por definición, $\mathbf{ord_O(f)}$ es el negativo del grado de **f**, con lo que queda demostrado el lema.

Del concepto de multiplicidad se deducen las siguientes propiedades:

Sea **f** un polinomio sobre **E**. La suma de las multiplicidades de los ceros de **f** es igual al grado de **f**.

Sea **f** un polinomio no constante. Luego **f** debe tener por lo menos dos ceros simples o uno doble en puntos finitos. Esto se deduce ya que el grado mínimo de un polinomio es 2 (si solamente tiene una **x**) o 3 (si solamente tiene una **y**) y la cantidad de ceros de un polinomio es igual a la cantidad de raices que tiene.

Una función racional sin polos finitos es un polinomio.

Sea $\mathbf{r(x, y) = a(x) + y\,b(x)}$ donde **a** y **b** son funciones racionales en **x** solamente. Si **r** no tiene polos entonces $\mathbf{\bar{r}(x, y) = a(x) - y b(x)}$ tampoco tiene. Por lo tanto $\mathbf{r + \bar{r} = 2a\,(x)}$ no tiene polos finitos. Por lo tanto **a(x)** no tiene polos como función de **x** y por lo tanto no puede tener polos como función sobre **E**. Por lo tanto **a(x)** es un polinomio. Esto implica que **yb(x)=r(x,y)-a(x)** no tiene polos finitos (**r** no los tiene y **a** tampoco). Por lo tanto $\mathbf{(yb)^2 = b^2 s}$ donde $\mathbf{s = x^3 + Ax + B}$ no tiene polos finitos. Si **b**, que es una función racional, tuviera un polo finito podría escribirse como $\mathbf{b\,(x) = \frac{f}{g}}$ donde **g(x) = 0** para algún $\mathbf{x \in K}$. En este caso sería $\mathbf{b^2 = \frac{f^2}{g^2}}$ con lo que $\mathbf{g^2}$ tendría una raíz doble para un valor de **x**. La única manera de que $\mathbf{sb^2}$ no tenga un polo en **P** es que **s** tenga un cero doble en **x** lo que

34. $\mathbf{N(f) = \bar{f} f = v^2\,(x) - y^2\,w^2\,(x) = v^2\,(x) - s(x)w^2\,(x)}$ **donde** $\mathbf{s(x) = x^3 + Ax + B}$

no es posible dado que **E** es no singular. Por lo tanto **b** no tiene polos finitos. Luego **b** es también un polinomio por lo que **r** resulta ser un polinomio también.

La siguiente definición resultará de utilidad: Un mapa racional **F** sobre **E** es un par **(r,s)** en el que **r** y **s** son funciones racionales sobre **E** tal que $\mathbf{s^2 = r^3 + Ar + B}$ [35].

Esta definición es coherente dado que las funciones racionales constituyen un cuerpo debido a que [36]:

1. Existen dos operaciones cerradas que son la adición y el producto
2. Existe un elemento nulo para la suma **(0/1)** y otro para el producto **(1/1)**
3. Las operaciones de producto son distributivas con respecto a la suma
4. Cada elemento tiene un inverso $\frac{\mathbf{f}}{\mathbf{g}} \times \frac{\mathbf{g}}{\mathbf{f}} = \frac{\mathbf{1}}{\mathbf{1}} \Longrightarrow \mathbf{f} \times \mathbf{g} = \mathbf{g} \times \mathbf{f}$

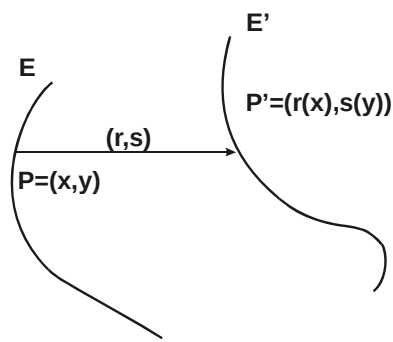
Si se acepta la convención que **F(P)=O** si **r** y **s** no son finitos en **P**, puede verse que **F** define una función de **E** en **E** por medio de **F(P)=(r(P),s(P))** dado que **r** y **s** deben tener polos en los mismos puntos[37] ya que satisfacen la ecuación $\mathbf{s^2 = r^3 + Ar + B.}$

En efecto consideremos dos funciones elípticas E y E' definidas por las siguientes ecuaciones

$$\mathbf{E: Y^2 = X^3 + AX + B}$$

$$\mathbf{E': Y^2 = X^3 + A'X + B'}$$

y sea el mapa racional $\mathbf{r^2 = s^3 + A's + B'}$ y sea un elemento del mapa racional **(r,s)**. A cada punto **P=(x,y)** de **E** le corresponderá un punto de **P'∈ E'** igual a **(x',y')**. Esto es válido por la definición de **O' (r(O),s(O))** y por el hecho que **r** y **s** satisfacen la ecuación de **E'**. En el siguiente gráfico se demuestra este hecho.



35. Nótese que esta es la ecuación de una función elíptica en donde se han reemplazado formalmente **y** por **r** y **s** por **x.**

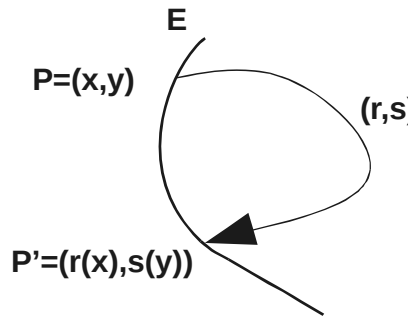
36. Si se deseara hacer un planteo completamente formal debería referirse a las clases de equivalencia de las funciones racionales. La función racional **r** representa la clase de equivalencia que lo contiene. Por supuesto se acepta la validez del axioma de la elección.

37. Por eso el requerimiento que tanto **r** como **s** sean infinitos simultáneamente

Existe una forma interesante de interpretar los mapas racionales. Dado el cuerpo **K**, los puntos de la función elíptica se obtienen por medio de la ecuación

$$\mathbf{Y^2 = X^3 + AX + B}$$

Considérese el cuerpo de las funciones racionales **K(E)**. Se puede emplear la misma ecuación para obtener una nueva curva elíptica que puede denotarse por la expresión **E(K(E))**. Pero **K(E)** puede no ser algebraicamente cerrado[38] y por nuestra convención **E(K(E))** tiene coordenadas en la clausura algebraica de **K(E)**. Los puntos finitos cuyas coordenadas caen en **K(E)** (los puntos racionales de **K(E)**) son precisamente los mapas racionales.



En el gráfico anterior se representa esta transformación. Se puede pensar que la identidad de esta curva, llamada $\mathbf{O_M}$, como el mapping con el valor constante **O**.

Divisores y líneas

Resulta conveniente definir un mecanismo para registrar los ceros y los polos de una función racional. Esto es similar a lo que ocurre con las funciones analíticas en donde los ceros y los polos de una función de variable compleja determinan las características de la misma. Una idea sería la de emplear una expresión del tipo

$$\mathbf{[(P_1,m_1), (P_2,m_2), \ldots,(P_i,m_i),\ldots, (P_n,m_n)]}$$

en donde el punto $\mathbf{P_i}$ de la función racional **r** tiene orden $\mathbf{m_i}$. Más que una enumeración explícita, resulta más práctico considerar una suma formal del tipo

$$\mathbf{m_1 < P_1> + \ldots + m_n < P_n> = \sum_{i=1}^{n} m_i < P_i >}$$ [39]

38. Los polinomios con coeficientes en K(E) pueden no tener sus raíces en dicho cuerpo.

39. El símbolo **<P>** es equivalente a la indeterminada de los polinomios y se lo utiliza para que cuando se defina la suma el resultado de dicha operación sea coherente.

La manera más práctica de definir esta suma formal es emplear el concepto de un grupo abeliano libre que esta constituido por el conjunto de combinaciones lineales formales finitas del tipo

$$\sum_{s \in S} \mathbf{m(s)s}$$

donde $\mathbf{m(s) \in Z}$ y $\mathbf{m(s)=0}$ excepto para un conjunto finito de $\mathbf{s \in S}$. La suma es también formal, por ejemplo

$$\mathbf{(m_1 s_1 + m_2 s_2)+(n_1 s_1 + n_3 s_3) = (m_1 + n_1)\, s_1 + (m_2 s_2 + n_3 s_3)}$$

No es difícil demostrar que se trata de un grupo abeliano ya que la suma es cerrada de acuerdo con la definición dada, existe un cero que es la combinación $\mathbf{0 s_0}$ y la inversa de

$$\sum_{j=1}^{n} \mathbf{m}_{s_j} \text{ es } \sum_{j=1}^{n} \mathbf{-m}_{s_j}$$

La siguiente definición será empleada para la construcción de la estructura de grupo de la curva elíptica definida sobre el cuerpo **K** cerrado algebraicamente. El grupo de divisores de **E** en el grupo abeliano libre generado por los puntos de **E** y que se denotará como **div(E)**. Para distinguir un punto **P** del divisor trivial cuya única entrada es **P** con el coeficiente **1,** se empleará, para identificar al divisor, la expresión **<P>.** Si $\mathbf{\Delta = \sum_{P \in E} m(P) < P >}$ es un divisor, se define su grado

$$\mathit{grad}(\Delta) = \sum_{P \in E} \mathit{m(P)\ para\ m\ (P)} \in \mathbf{Z}$$

Si **r** es una función racional no nula se le asocia un divisor por medio de la siguiente expresión

$$\mathbf{div(r)} = \sum_{P \in E} \mathbf{ord_P\,(r) < P >}$$

Dos observaciones pueden hacerse como consecuencia de lo expuesto anteriormente

1. Una función racional tiene una cantidad finita de ceros y polos
2. Si dos funciones racionales tienen el mismo divisor ello implica que su cociente es constante. Por lo tanto una forma de demostrar que dos funciones racionales son iguales es demostrar que tienen el mismo divisor y que por lo tanto coinciden en todo punto de **E**. En general el único punto de **E** que se conoce a priori es **O** donde frecuentemente tiene polo. En este caso se pueden comparar los coeficientes de mayor peso.

Definición:

Sea **r** una función racional y supongamos que $\mathbf{ord_O(r)=d}$, luego se define como el coeficiente principal de **r**

$$\left[\left(\frac{x}{y}\right)^{d} . r\right](O)$$

Se puede demostrar que dos funciones racionales que tienen los mismos divisores y los mismos coeficientes principales son iguales.

Es conveniente dar algunos ejemplos para consolidar los conceptos sobre funciones racionales.

Ejemplo 1:

Sea $\mathbf{P=(a,b)}\in \mathbf{E}$ donde $\mathbf{b\neq 0}$ y sea la función racional $\mathbf{r_1=(x-a)}$. Esta función racional tendrá ceros simples en **P=(a,b) y P=(a,-b)** que son los dos puntos de la curva elíptica que tiene **a** como valor de $\mathbf{x}$[40] y un polo de multiplicidad **2** en **O** (dado que **x** tiene orden **2**). Por lo tanto $\mathbf{div(r_1)=<P>+<P'>-2<O>}$

Ejemplo 2:

Sea $\mathbf{r_2=y}$ y sean ω_1, ω_2 y ω_3 las raíces de $\mathbf{x^3+Ax+B}$ que se llaman puntos de orden **2**. Sean los puntos $\mathbf{P_1(\omega_1,0)}$, $\mathbf{P_2=(\omega_2,0)}$ y $\mathbf{P_3=(\omega_3,0)}$ entonces será

$$\mathbf{div(r_2)=<P_1>+<P_2>+<P_3>-3<O>}$$

ya que el orden de **y** es **3**.

Ejemplo 3:

Sea $\mathbf{r_3=x/y}$. Esta función racional tendrá polos simple en $\mathbf{P_1(\omega_1,0)}$, $\mathbf{P_2=(\omega_2,0)}$ y $\mathbf{P_3=(\omega_3,0)}$ donde $\boldsymbol{\omega_1}$, $\boldsymbol{\omega_2}$ y $\boldsymbol{\omega_3}$ son las raíces de $\mathbf{x^3+Ax+B}$ (puntos de orden **2**). En O tendrá un cero simple ya que el orden de **y** es **3** en tanto que el de **x** es **2**. En los puntos $Q_1=(0,\sqrt{B})$ y $Q_2=(0,-\sqrt{B})$ tendrá ceros simples. Por lo tanto

$$\mathbf{div(r_3)=<Q_1>+<Q_2>-<P_1>-<P_2>-<P_3>+<O>}$$

Definición:

Un divisor[41] $\boldsymbol{\Delta}$ se llamará principal si $\boldsymbol{\Delta=div(r)}$ para alguna función racional **r**. Si $\boldsymbol{\Delta_1-\Delta_2}$ es principal se dirá que $\boldsymbol{\Delta_1}$ y $\boldsymbol{\Delta_2}$ son ***linealmente equivalentes*** o ***que pertenecen a la misma clase de divisores*** y se notará $\boldsymbol{\Delta_1\sim\Delta_2}$. En otras palabras dos divisores son linealmente equivalentes si su diferencia es divisor de una función racional.

Proposición:

Si $\mathbf{r_1}$ y $\mathbf{r_2}$ son funciones racionales sobre **E**, entonces $\mathbf{div(r_1r_2)=div(r_1)+div(r_2)}$. Dado que $\mathbf{ord_P(r_1r_2)=ord_P(r_1)+ord_P(r_2)}$ la demostración es una consecuencia inmediata de ello. Intuitivamente si $\mathbf{r_1}$ y $\mathbf{r_2}$ son funciones racionales sus ceros se deben a los ceros de los polinomios numeradores y sus polos a los ceros de los polinomios denominadores. Puede que en algunos puntos ellos coincidan. En ese caso dado en el que el orden de un polo es negativo, al realizarse la suma de los divisores el cero y el polo se anularán si sus órdenes son iguales o quedarán con un orden igual a la suma algebraica de sus respectivos órdenes.

---

40. Dada la definición de la curva elíptica $(\mathbf{y^2=x^3+Ax+B})$en los reales si **(a,b)** es una solución también lo será **(a,-b)**

41. Es de recordar que el conjunto de los divisores se define sobre todos los puntos de **E**

Teniendo en cuenta esta propiedad se puede demostrar que el conjunto de divisores principales que se denota como **Prin(E)**, es decir aquellos que son divisores de funciones racionales, constituyen un subgrupo del grupo de los divisores de **E,** debido a que las funciones racionales forman un grupo multiplicativo. En efecto la suma de divisores principales es cerrada dado que es un divisor principal correspondiente a la función racional producto de las respectivas funciones racionales. Por otro lado existe un divisor principal que es la unidad del grupo y que corresponde a la función racional unitaria multiplicativa (**r=1/1**). Finalmente para cada divisor principal existe un inverso aditivo ya que si Δ_1 es el divisor de $\mathbf{r_1=f/g}$ y Δ_2, es el divisor principal correspondiente a la función racional inversa **g/f**, entonces $\Delta_1 + \Delta_2$ corresponderá a $\mathbf{f/g \times g/f = 1}$ y por lo tanto será el elemento neutro aditivo de los divisores principales. Dentro del grupo de los divisores principales se define como $\mathbf{Div^0(E)}$ al subgrupo de los divisores de grado **0**.

El objetivo es analizar qué divisores son principales, es decir cuales son los ceros y los polos que una función racional puede tener. Esto es equivalente a estudiar los divisores que no son principales. Los mismos están representados por los elementos del grupo

$$\mathbf{Pic(E)= div(E)/Prin(E)}$$

A **Pic(E)** se lo conoce como grupo de **Picard** de **E** o grupo de la clase de divisores. Puede estudiarse un grupo más pequeño para analizar cuales son los divisores principales. El teorema que establece que si **r** es una función racional entonces

$\sum_{P \in E} \mathbf{ord_P\,(r)} = \mathbf{0}$ implica que $\mathbf{Prin(E) \subseteq Div^0(E)}$**.** Por lo tanto se tendrían que estudiar los divisores de grado cero que no son principales, es decir el grupo

$$\mathbf{Pic^0(E) = Div^0(E)/Prin(E)}$$

$\mathbf{Pic^0(E)}$ recibe el nombre de la ***parte de grado cero del grupo de Picard de E***.

Para continuar con el análisis de los ceros y polos de las funciones racionales serán de utilidad las siguientes definiciones:

Norma de un divisor. Si $\Delta = \sum_{P \in E} \mathbf{m(P)} < \mathbf{P} >$ es un divisor, su norma se definirá como

$$|\Delta| = \sum_{P \in E-O} |\mathbf{m(P)}|$$

De la definición surge que si **Δ** es el divisor de un polinomio **f** su norma **|Δ|** es la suma de las multiplicidades de los ceros de **f** que, a su vez, es el grado de **f**.

Líneas: Una línea sobre E es un polinomio de la forma

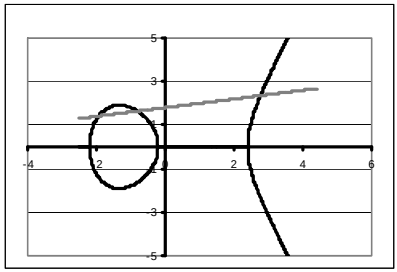
$$\ell\,\mathbf{(x, y)=\alpha\, x + \beta y + \gamma}$$

para $\boldsymbol{\alpha, \beta}$ y $\boldsymbol{\gamma \in K}$ donde $\boldsymbol{\alpha}$ y $\boldsymbol{\beta}$ no pueden ser nulos simultáneamente.

Si un punto **P(a,b)** es un cero de la línea $\mathbf{(\alpha\, a + \beta\, b + \gamma = 0)}$ se dirá que la línea ℓ pasa por **P** y que **P** está sobre la línea.

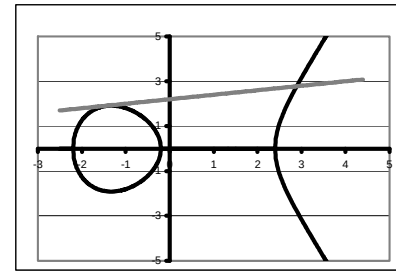
La siguiente es una propiedad importante de las líneas: Si ℓ es una línea con divisor **Δ**, luego **|Δ|** es igual a **2** o **3**. La demostración es sencilla. Dado que una línea es un polinomio su grado será **2** si $\boldsymbol{\beta=0}$ y **3** si $\boldsymbol{\beta \neq 0}$.

Los siguientes son los posibles divisores de las líneas:



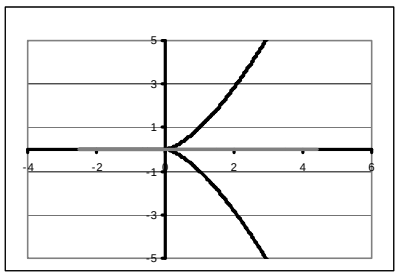
div(l) = <P> + <Q> + <R> - 3<O>

P, Q y R son los ceros de la línea en **E** (Puntos de intersección de la línea con E). Existen tres soluciones diferentes.



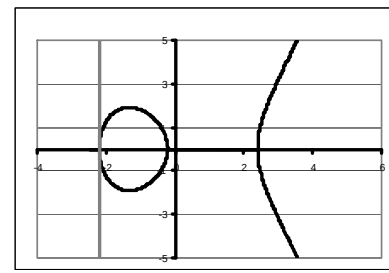
div(l) = 2<P> + <Q> - 3<O>

La línea es tangente a **E** en el punto **P.** Existe una solución doble y una simple.



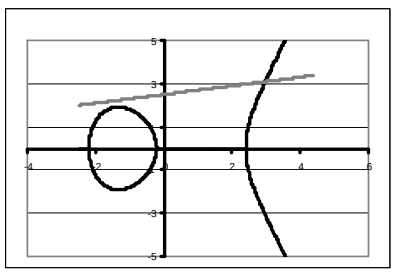
div(l) = 3<P> - 3<O>

La línea pasa por un punto deinflexión de **E**



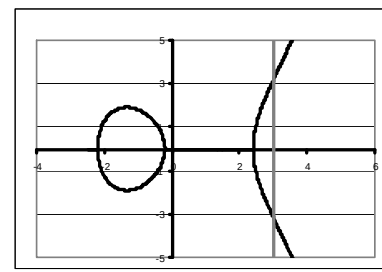
div(l) = 2<P> - 2<O>

La línea es paralela al eje de las **y** y tangente a **E.** Existe una solución doble dado que siendo x constante la ecuación final es cuadrática



div(l) = <P> - <O>

Existe una sola solución real y dos complejas. Este caso se presenta porque los reales no constituyen un cuerpo algebraicamente cerrado.



div(l) = <P> + <Q> - 2<O>

La línea es paralela al eje de las **y.** Existe una solución doble dado que siendo x constante la ecuación final es cuadrática

El siguiente teorema es uno de los resultados más importantes. En general, y por razones que se comprenderán más adelante, si **P** es el punto **(a, b)** se empleará la notación **-P** para referirse al punto **(a,-b).**

Teorema de Reducción lineal

Sea $\Delta \in$ **div(P).** Luego existe $\tilde{\Delta} \in$ **div(E)** tal que $\Delta \approx \tilde{\Delta}$ y **grad(Δ) = grad** $(\tilde{\Delta})$ y $|\tilde{\Delta}| \leq 1$

Demostración:

Supóngase que $\Delta = \sum_{P \in E} n(P) < P >$ y que los puntos **Q, R**$\in$ **E** están incluídos en **Δ** con coeficientes no nulos y del mismo signo (**Q** y **R** ambos son simultáneamente o ceros o polos). Sea ℓ una línea que pasa por los puntos **Q** y **R**. Luego dependiendo del signo del coeficiente de **Q** (o **R**) el nuevo divisor

$$\Delta + div(\ell) \qquad o \quad \Delta - div(\ell)$$

tendrá:

- Si ℓ tuviera tres ceros diferentes **|n(Q)|** y **|n(R)|** disminuidos en una unidad y, en el peor de los casos, haberse aumentado en una unidad el coeficiente correspondiente a la tercer raíz de la línea. En efecto supongamos que $\Delta = n_1 <Q> + n_2 <R> + \ldots + n_m <R_m>$ con $n_1 > 0$ y $n_2 > 0$ y que $\Delta_l = <P> + <Q> + <R> - 3<O>$, luego será $\Delta - \Delta_\ell = (n_1 - 1)<Q> + (n_2 - 1)<R> - <P> + 3<O> + n_3 <R_3> + \ldots + n_m <R_m>$
  Ahora bien el grado ($\sum_{P \in E} m(P)$) de **Δ** y Δ_ℓ son iguales dado que el grado de Δ_ℓ es cero pero $|\Delta - \Delta_\ell|$ disminuyó en **3** o **1** unidad según que **P** pertenezca o no a **Δ**

- Si ℓ hubiera tenido solamente dos ceros diferentes, se hubieran hecho decrecer **|n(Q)|** o **|n(R)|** en una unidad y no se hubiera incrementado ningún otro coeficiente.

Mediante este procedimiento se ha creado un nuevo divisor Δ_1 tal que $\Delta_1 \sim \Delta$, **grad(**Δ_1**)=grad(Δ) y** $|\Delta_1| < |\Delta|$

Después de realizar este procedimiento una cantidad finita de veces, se ha logrado crear un nuevo divisor linealmente equivalente a **Δ** y del mismo grado que **Δ** de la forma

$$\Delta' = n_1 <P> - n_2 <Q> + n<O>$$

donde n_1 y n_2 son enteros no negativos y **n** un entero arbitrario cuyo valor no interesa.

Supóngase ahora que $n_1 > 1$ y considérese la línea definida por la siguiente ecuación

$$\ell(x, y) = m(x - a) - (y - b)$$

donde **P=(a, b). P** está en ℓ si a es un cero del polinomio

$$f(x) = [m(x - a) + b]^2 - x^3 - Ax - B$$

debido a que **P** debe satisfacer simultáneamente la ecuación de la línea y la ecuación fundamental de la ecuación elíptica. Si se computa la derivada **f'(a)**[42], se comprueba que **P** tiene multiplicidad **2** si

$$\mathbf{m} = \frac{\mathbf{3a^2 + A}}{\mathbf{2b}}$$

Si **b≠0**, esta línea tendrá un divisor **2<P> + <S> - 3<O>**. Restando esta línea de **Δ'** se puede reducir $\mathbf{n_1}$ y por lo tanto **|Δ'|**. Si **P** fuera de orden **2** (una línea vertical tangente a la curva) la ecuación de la línea sería ℓ **(x, y)= x - ω** que tiene como divisor

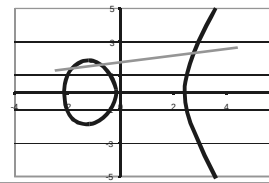
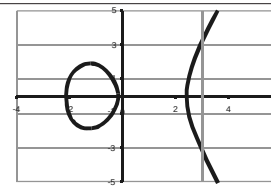
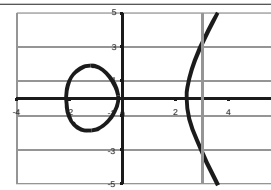
2<P> - 2<O> que puede restarse de $\mathbf{n_1}$. Similarmente se podría reducir $\mathbf{n_2}$.

Eventualmente se llega a un resultado que demuestra el teorema o a una expresión del tipo

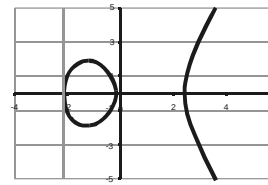
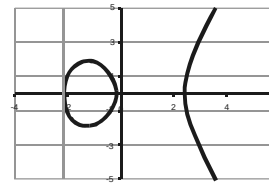
<P> + <Q> + n<O>

La línea ℓ **(x, y)= x - a** tiene los divisores **<P> + <R> - 2<O> o 2<P> - 2<O>** con lo que restando la misma se reduce al caso anterior.

En el ejemplo siguiente se muestra como el divisor **4<P>-3<Q>+3<R>-4<O>** puede reducirse al divisor **<P> - <O>** por medio de una serie de sumas y restas de líneas.

4<P>-3<Q>+3<R>-4<O>		
<P>+ <Q>+ <R>- 3<O>	-	
3<P> - 4<Q> +2<R> - <O>		
<P> + <R> -2<O>	-	
2<P> - 4<Q> + <R> +<O>		
<P>+ <R>-2<O>	-	

42. La ecuación elíptica es $\mathbf{y^2=x^3 + A\,x + B}$, por lo que $\mathbf{2yy'=3x^2+A}$ de donde resulta $\mathbf{y'=(3x^2+A)/2y}$. La pendiente de la recta es **m** y pasa por el punto **(a, b)** por lo que para que **P** tenga multiplicidad **2** deberá ser $\mathbf{m = (3a^2+A)/2b}$. Este razonamiento es válido si la característica del cuerpo **K** es diferente de **2** ó **3**. Para ser estrictamente formales se tendría que usar el concepto de derivada formal de polinomios.

<P> - 4<Q> +3<O>		
2<Q> - 2<O>	**+**	
<P> - 2<Q> + <O>		
2<Q> - 2<O>	**+**	
<P> - <O>		

Del anterior teorema surge un corolario muy importante que establece que para cada **Δ∈ div⁰(E)**, es decir $\sum_{P\in E} \mathbf{m(P)} = \mathbf{0}$, existe un único punto P de la curva elíptica tal que

$$\Delta \sim \langle P\rangle - \langle O\rangle$$

lo que equivale a que **Δ-<P>+<O>** es el divisor de una función racional.

Lo que el teorema establece es que el divisor es equivalente a un divisor de norma 1 del tipo **±<P> + n<O>**. Si el signo de **<P>** no fuera positivo, es decir que la expresión fuera **- <P> + n<O>**, basta sumarle la línea con divisor **2<P>-2<O>**. Dada la suposición que el grado de **Δ** es cero, el coeficiente de **<O>** debe ser **-1**. Para verificar que el punto es único supóngase que existe otro punto **Q** tal que **Δ ~ <Q> - <O>**. Luego será

$$\langle Q\rangle \sim \Delta + \langle O\rangle \sim \langle P\rangle$$

por lo tanto debe existir una función racional **r** donde su divisor sea [43] **div(r) = <P> - <Q>**. Usando los mismos métodos que en la demostración del teorema anterior [44], se podría concluir que debe existir una función racional t cuyo divisor es

$$\mathbf{div(t) = \langle S\rangle - \langle O\rangle \text{ para un } S \in E}$$

Pero **t** no puede tener polos finitos por lo que se trata de un polinomio. Pero siendo un polinomio debe tener como mínimo dos ceros[45] lo que contradice el hecho que

$$\mathbf{div(t) = \langle S\rangle - \langle O\rangle}$$

por lo que debe ser **<Q> = <P>**.

43. Por la definición de la relación ~

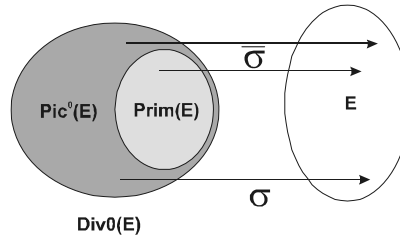
44. Sumando y restando las líneas apropiadas

45. El polinomio de menor grado sería **x** que tiene grado **2** de acuerdo con la definición dada y que tiene dos ceros.

Se puede ahora crear una aplicación

$$\bar{\sigma} : \mathbf{div^0(E)} \rightarrow \mathbf{E}$$

mediante la definición $\bar{\sigma}\,(\Lambda) = \mathbf{P}$ donde **P** es el único punto tal que $\mathbf{\Delta} \sim \langle \mathbf{P} \rangle - \langle \mathbf{O} \rangle$. Dado que si **P = O** será **div(r) ~ 0** luego $\bar{\sigma}\,(\text{div}\,(r)) = \mathbf{O}$ lo que permite deducir que $\bar{\sigma}$ induce una aplicación $\boldsymbol{\sigma}\mathbf{:pic^0 \rightarrow E}$ como se representa en el siguiente gráfico

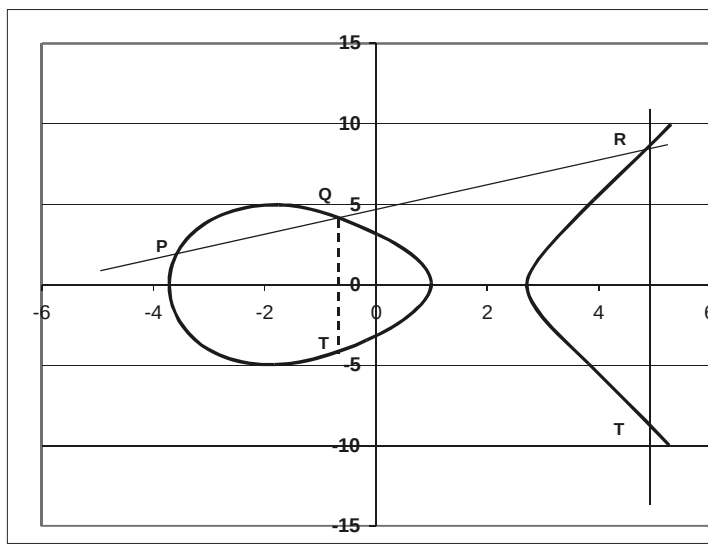


La Estructura de Grupo

La definición de la estructura de grupo sobre los puntos de una función elíptica por su formulación algebraica tiene dos dificultades: La primera, que no es intuitiva y la segunda, que la demostración de la asociatividad es engorrosa.

Otra aproximación es emplear métodos geométricos. La definición de las operaciones es más intuitiva pero la demostración de la asociatividad resulta dificultosa.

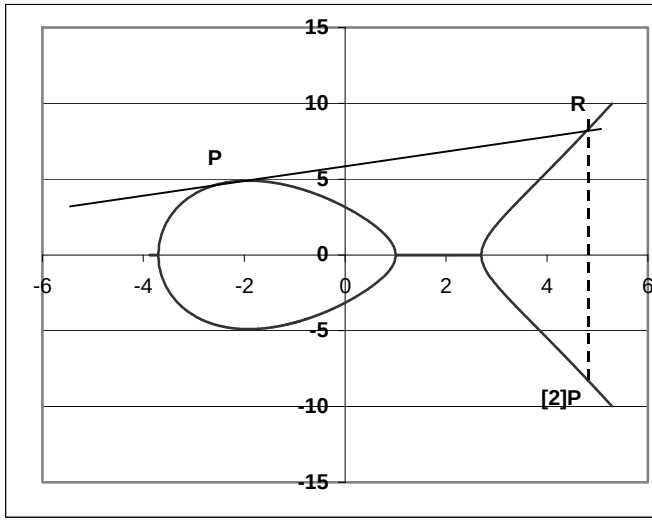
La idea básica que subyace sobre la definición de la operación de suma de los puntos de una curva elíptica es el hecho que una línea corta a una curva elíptica en no más de tres puntos[46]. En el gráfico siguiente se ejemplifica esta aseveración. La línea ℓ corta a la curva



46. Un polinomio de grado tres tiene tres raíces.

elíptica $\mathbf{y^2 = x^3 - 11x + 10}$ en los puntos **P, Q** y **R**. La operación se define por medio de la siguiente igualdad **P+Q+R=O**, donde **O** es el punto que representa el elemento neutro del grupo y que recibe el nombre de punto en el infinito (Se lo considera posicionado para valores infinitos de **y** y su nombre proviene de la geometría proyectiva). Dado que **P(x,y) + P(x,-y) = O** será **P+Q = T**. Cuando **P** y **Q** coinciden, la recta que intercepta ambos puntos se convierte en tangente a la curva y el punto se considerará doble.

El siguiente gráfico muestra esta situación[47].

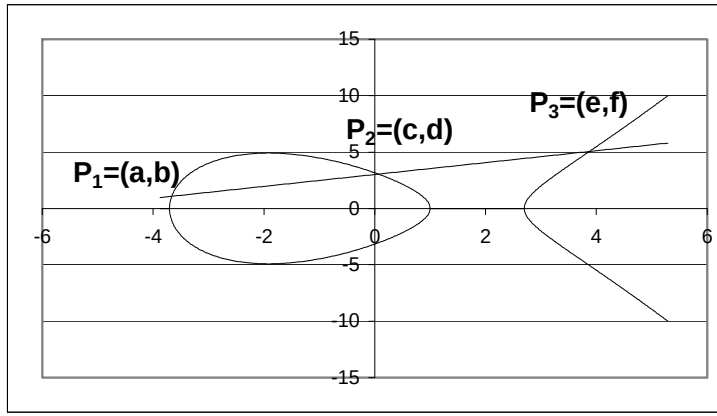


Este razonamiento es válido para el caso en el que el cuerpo admita una medida como por ejemplo en los complejos. Pero no lo es cuando se trate de cuerpos finitos en los que el concepto de límite y por lo tanto de derivada no existe.

Supóngase que $\mathbf{P \neq Q}$ y $\mathbf{P \neq -Q}$ y que $\mathbf{\Lambda}$ es la línea que pasa por **P** y **Q** y que **R** es el tercer punto de intersección de la línea con la curva elíptica. Sean las coordenadas de **P a** y **b** y las de **Q c** y **d**.

Sea la ecuación de la recta $\mathbf{\Lambda(x,y) = m(x-a) - (y-b)}$ donde $\mathbf{m = (d-b)/(c-a)}$

47. La notación [n]P con $n \in Z$ significa $\overbrace{P+P+\ldots+P}^{\text{n veces}} = \sum_{j=1}^{n} P$



Reemplazando la ecuación de la recta en el polinomio $\mathbf{y^2=x^3+Ax+B}$ se obtiene finalmente $\mathbf{f(x)=[m(x-a)+b)]^2-x^3-Ax-B}$. No es difícil demostrar que a y c son ceros de **f(x)**. Se necesita calcular cual es el tercer cero. El polinomio **f(x)** puede escribirse de la siguiente manera $\mathbf{f(x)=(x-a)(x-b)(x-e)}$ en donde **a, b** y **e** son los ceros del polinomio. Expandiendo esta expresión se obtiene que el coeficiente de $\mathbf{x^2}$ es **a+b+e** en tanto que expandiendo la expresión original se obtiene que el coeficiente de **x** es $\mathbf{m^2}$. De ambas igualdades se obtiene finalmente que $\mathbf{e = m^2 - a - b}$. Para obtener la coordenada **y** se emplea la ecuación de la recta. Finalmente las coordenadas del tercer punto son

$$\mathbf{e = m^2 - a - b}$$
$$\mathbf{f = m\,(x - a) + b}$$
$$\mathbf{m = (d - b) / (c - a)}$$

Se analizará con más detalle la estructura antes definida. Sea el cuerpo **K** y la curva elíptica $\mathbf{y^2 = x^3 + ax + b}$ donde $\mathbf{a, b \in K}$.

Sean tres puntos de la recta $\mathbf{P_1}$, $\mathbf{P_2}$ y $\mathbf{P_3}$ de coordenadas $\mathbf{(x_1, y_1)}$, $\mathbf{(x_2, y_2)}$ y $\mathbf{(x_3, y_3)}$ respectivamente. La recta que pasa por los puntos $\mathbf{P_1}$ y $\mathbf{P_2}$ tendrá por ecuación $\mathbf{y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}\,(x - x_1)}$. Si se define la pendiente como $\mathbf{m = \frac{y_2 - y_1}{x_2 - x_1}}$ la ecuación anterior puede rescribirse de la siguiente manera: $\mathbf{y = y_1 - mx_1 + mx}$.

Pero

$$\mathbf{y_1 - mx_1 = y_1 - \frac{y_2 - y_1}{x_2 - x_1}\,x_1 = \frac{y_1 x_2 - x_2 y_1}{x_2 - x_1} = \mu}$$

Finalmente la ecuación de la recta será $\mathbf{y = \mu + mx}$

Las operaciones del grupo se definirán tal que $\mathbf{P_1 + P_2 + P_3 = O}$ donde **O** es el elemento neutro del grupo. Por lo tanto será $\mathbf{P_1 + P_2 = -P_3}$

Analizaremos los tres casos siguientes:

1. Las coordenadas $\mathbf{x_1}$ y $\mathbf{x_2}$ son iguales pero $\mathbf{y_2}$ es diferente de $\mathbf{y_1}$. En este caso será $\mathbf{P_3 = O}$. De la ecuación elíptica se deduce que $\mathbf{y_1^2 - y_2^2 = (y_1 + y_2)(y_1 - y_2) = 0}$ de donde, dada la condición que las ordenadas de los puntos son diferentes, deberá verificarse que $\mathbf{y_1 + y_2 = 0}$ de donde $\mathbf{y_2 = -y_1}$. Finalmente se obtiene que $\mathbf{-P(x, y) = P(x, -y)}$.

2. Las coordenadas $\mathbf{x_1}$ y $\mathbf{x_2}$ son diferentes. En este caso deberán existir tres puntos de intersección entre la recta que pasa por los puntos $\mathbf{P_1}$ y $\mathbf{P_2}$ y la curva elíptica ya que si una ecuación cúbica tiene dos soluciones reales la tercera deberá ser también ser real, llamemos $\mathbf{x_1}$, $\mathbf{x_2}$ y $\mathbf{x_3}$ a los tres ceros de la ecuación cúbica. Luego
$\mathbf{(x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x + x_1x_2x_3}$

   El coeficiente del término cuadrático cambiado de signo es la suma de las raíces del polinomio. Reemplazando la ecuación de la recta $\mathbf{y = \mu + mx}$ en la ecuación elíptica

$$\mathbf{y^2 = x^3 + ax + b}$$

   se obtiene
$\mathbf{x^3 + ax + b - \mu^2 - 2\mu mx - m^2x^2 = x^3 - m^2x^2 + (a - 2\mu m)x + b - \mu^2}$

   de donde se deduce que $\mathbf{m^2 = x_1 + x_2 + x_3}$ y por lo tanto será $\mathbf{x_3 = m^2 - x_1 - x_2}$. Utilizando la ecuación de la recta se obtienen las siguientes ecuaciones para calcular las coordenadas del punto de la curva suma de $\mathbf{P_1}$ y $\mathbf{P_2}$

$$\mathbf{x = m^2 - x_1 - x_2}$$
$$\mathbf{y = -\mu - mx}$$

   donde

$$\mathbf{m} = \frac{\mathbf{y_2 - y_1}}{\mathbf{x_2 - x_1}} \quad \text{y} \quad \boldsymbol{\mu} = \frac{\mathbf{x_2y_1 - x_1y_2}}{\mathbf{x_2 - x_1}}$$

3. Los dos puntos $\mathbf{P_1}$ y $\mathbf{P_2}$ son iguales.
   Desde un punto de vista geométrico se podría calcular la ecuación de la recta empleando la tangente a la curva en dicho punto. Ésta se puede obtener fácilmente por medio de la derivada que resultaría ser $\mathbf{y' = \frac{x^2 + a}{2y}}$. Ello sólo sería válido en el caso de que el cuerpo tuviera una métrica como por ejemplo en el caso de los reales o los complejos. Si bien los resultados son iguales se considera que el camino de deducción que se propone es más general.
   Aplicando la ecuación elíptica en los puntos $\mathbf{P_1}$ y $\mathbf{P_2}$ se obtiene
$\mathbf{y_1^2 - y_2^2 = (y_1 + y_2)(y_1 - y_2) = x_1^3 - x_2^3 + a(x_1 - x_2)}$

de donde se deduce que $(y_1 + y_2)\frac{y_1 - y_2}{x_1 - x_2} = \frac{x_1^3 - x_2^3}{x_1 - x_2} + a$. Pero

$x_1^3 - x_2^3 = (x_1 - x_2)(x_1^2 + x_1 x_2 + x_2^2)$.

Reemplazando esta expresión en la anterior se obtiene

$m = \frac{y_1 - y_2}{x_1 - x_2} = \frac{x_1^2 + x_1 x_2 + x_2^2 + a}{y_1 + y_2}$. En el caso en el que P_1 fuera igual a P_2 será

$$m = \frac{3x_1^2 + a}{2y_1} .$$

El valor de μ se calcula como $\mu = y_1 - mx_1$ que para el caso en que $P_1 = P_2$ resulta

$$\mu = \frac{-x_1^3 + ax_1 + 2x}{2y_1}$$

Es de hacer notar que estas expresiones no son válidas para cuerpos con característica **2**[48] ya que $2y_1 = y_1 + y_1 = 1y_1 + 1y_1 = (1 + 1)\, y_1 = 0y_1 = 0$. Pero dado que los cuerpos más empleados en las computadoras digitales son los basados en el cuerpo de los binarios, este problema invalidaría el uso de curvas elípticas en las computadoras. Para cuerpos de característica 2 la ecuación elíptica se define $y^2 + xy = x^3 + ax^2 + b$

Con un razonamiento análogo al anterior los puntos de intersección de la recta $y = \mu + mx$ con la curva elíptica deberán satisfacer la ecuación

$x^3 + ax^2 + b - (\mu + mx)^2 - (\mu + mx)\, x = 0$ de donde

$x^3 + (a - m^2 - m)\, x^2 + (2\mu m - \mu)\, x + b - \mu^2 = 0$ y para cuerpos de característica **2** será

$x^3 + (a - m^2 - m)\, x^2 - \mu x + b - \mu^2 = 0$

La expansión de $(x - x_1)(x - x_2)(x - x_3) = 0$ es

$x^3 - (x_1 + x_2 + x_3)\, x^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3)\, x + x_1 x_2 x_3 = 0$

que para $x_1 = x_2$ se simplifica

$x^3 + x_3 x^2 + x_1 x_3 x + x_1^2 x_3 = 0$ [49]

---

48. La característica de un cuerpo es el menor número natural **n** que existe tal que $\sum_{j=1}^{n} 1 = 0$ donde **1** es el elemento neutro del grupo multiplicativo y **0** el del grupo aditivo. Si dicho número no existe (como en el caso de los reales, por ejemplo) se dice que la característica es cero.

49. Estos resultados se logran porque en cuerpos de característica **2** $\forall x, y \in K: x + y = 0$

Se obtendrían lo siguientes resultados.

1. Para iguales valores de **x** constantes , **-P(x,y)=P(x,x+y)**
2. Para valores de x diferentes

$$x_3 = m^2 + m + a + x_1 + x_2$$
$$y_3 = \mu + mx_3$$

donde

$$\mathbf{m} = \frac{y_2 + y_1}{x_2 + x_1} \text{ y } \mu = \frac{x_2 y_1 + x_1 y_2}{x_2 + x_1}$$

3. Para valores de x iguales:

De $x^3 + x_3 x^2 + x_1 x_3 x + x_1^2 x_3 = 0$ y $x^3 + (a - m^2 - m) x^2 - \mu x + b - \mu^2 = 0$ se deduce que $x_1^2 = \mu$ y $x_3 = a + m^2 + m$. Pero $x_1^2 + mx_1 = \mu + mx_1 = y_1$ de donde

$$\mathbf{m} = \frac{y_1 + x_1^2}{x_1}$$

En la siguiente tabla se resumen los resultados anteriores

P(x,y)	$x_1 \neq x_2$ $P(x_1,y_1)+P(x_2,y_2) = Q(x_3,y_3)$		$x_1 = x_2 \neq 0$ $[2]P(x_1,y_1) = Q(x_3,y_3)$	
	$\mathbf{m} = \frac{y_2 + y_1}{x_2 + x_1}$	$\mu = \frac{x_2 y_1 + x_1 y_2}{x_2 + x_1}$	$\mathbf{m} = \frac{y_1 + x_1^2}{x_1}$	$\mu = x_1^2$
-P(x,y) = P(x,x+y)	$Q(x,y) = Q(m2 + m + a, \mu + (m + 1) x)$			

Para demostrar que la operación entre puntos antes definida induce una estructura de grupo abeliano sobre los puntos de una curva elíptica, hay que probar que

1. La operación es cerrada y conmutativa
2. Existe un elemento neutro
3. Cada punto tiene un inverso
4. La operación es asociativa

Las propiedades **1, 2** y **3** son fácilmente demostrables a partir de las definiciones pero la demostración que la operación definida es asociativa es más compleja de demostrar. Para ello se empleará el concepto de divisores y líneas antes definido.

Se empleará la siguiente nomenclatura: dado el punto **P(x, y)** se definirá **-P** al punto con coordenadas **P(x, -y).**

Sea la aplicación biyectiva definida previamente

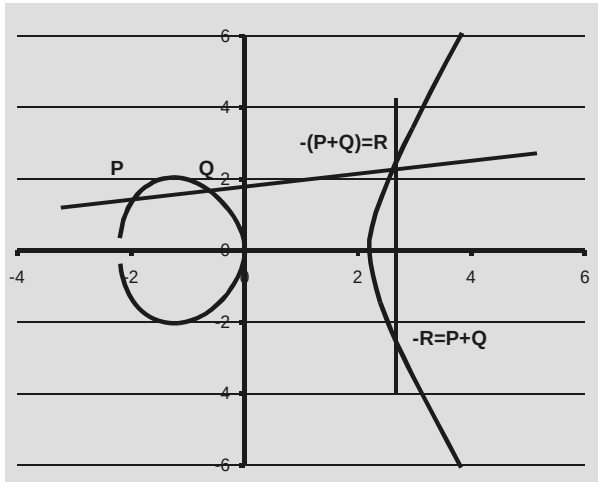
$$\sigma: Pic^0(E) \rightarrow E$$

Se definirá la aplicación inversa $\kappa = \sigma^{-1}$ por lo que $\kappa(P)$ es la clase de equivalencia lineal del divisor $<P> - <O>$. De la definición de κ surge que $\kappa(O)=0$, es decir que $\kappa(O)$ es la clase lineal de equivalencia de cero

Proposición: $\kappa(P + Q) = \kappa(P) + \kappa(Q)$

Supóngase que $Q = O$. Por lo tanto $\kappa(P + O) = \kappa(P) = \kappa(P) + 0 = \kappa(P) + \kappa(O)$, con lo que queda demostrada la tesis

Supóngase que ni **P** ni **Q** son iguales a **O**. En este caso se considerará la línea ℓ que pasa por los puntos **P** y **Q**.



El divisor de la misma será

$$\mathbf{div}(\ell) = <P> + <Q> + <R> - 3<O>$$

Sea ℓ' la línea que pasa por **R** y **-R** cuyo divisor será

$$\mathbf{div}(\ell') = <R> + <-R> - 2<O>$$

Luego el divisor de ℓ' / ℓ será

$$\mathbf{div}(\ell' / \ell) = - <P> - <Q> + <-R> + <O> = - <P> - <Q> + <P + Q> + <O> \sim 0$$

Reescribiendo la expresión anterior se obtiene

$$[<P + Q> - <O>] - [<P> - <Q>] - [<Q> - <O>] =$$
$$[<P + Q> - <O>] - [<P> - <Q>] - [<Q> - <O>] \sim 0$$

que corresponde de acuerdo con la definición de κ a

$$\kappa(P + Q) - \kappa(P) - \kappa(Q) = 0$$

de donde se deduce que

$$\boldsymbol{\kappa(P + Q) = \kappa(P) + \kappa(Q)}$$

Dado que la adición en $\mathbf{Pic^0(E)}$ es asociativa también lo serán las operaciones antes definidas de donde se demuestra el punto **4** con lo que las operaciones establecidas sobre los puntos de la curva elíptica inducen una estructura de grupo.

En base a los resultados anteriores se puede definir una aplicación **suma** de **div(E)** sobre **E** de la siguiente manera:

$$\mathbf{suma}\left(\sum \mathbf{n(P) < P >}\right) = \sum \mathbf{n(P)\, P}$$

en donde la sumatoria de la izquierda se realiza sobre los divisores mientras que la suma de la derecha se realiza sobre los puntos de la curva elíptica.

Un resultado muy importante que se obtiene de lo expuesto anteriormente es el siguiente:

Sea $\Delta = \sum_{P \in E} n(P) < P >$ un divisor. Luego **Δ** es principal si y sólo si

$$\mathbf{grad(\Delta)} = \sum_{\mathbf{P \in E}} \mathbf{n(P) = 0} \quad \mathbf{y} \quad \mathbf{suma}\left(\sum_{\mathbf{P \in E}} \mathbf{n(P) < P >}\right) = \mathbf{O}$$

Anexo A

Sea la curva elíptica **E** definida por la ecuación $\mathbf{y^2=x^3+Ax+B}$. Para cada punto $\mathbf{P \in E}$ existe una función racional **u**, tal que **P(u)=0**, con la propiedad que si **r** es una función racional no idénticamente nula, entonces

$\mathbf{r = u^d s}$

para un entero **d** y una función racional **s** que es finita y diferente de cero en **P**. Además el número **d** no depende de la elección de **u**.

Para probar el teorema se analizarán los siguientes tres casos

1. **P** no es de orden **2** y $\mathbf{P \neq O}$
2. **P** es de orden **2** y $\mathbf{P \neq O}$
3. **P = O**

Caso 1 (P no es de orden **2** y $\mathbf{P \neq O}$)

Se demostrará que para **P = (a,b)** se puede elegir **u(x,y) = x - a.** Supóngase que $\mathbf{r(P) = \frac{f(P)}{g(P)} = 0}$. Luego será **f(P)=0 y g(P)=0** ya que **g(P)** no puede tener un polo en **P** por ser un polinomio y $\mathbf{P \neq O}$. Si se puede descomponer $\mathbf{f=u^d t}$, entonces dividiendo por **g** se obtiene $\mathbf{r = \frac{f}{g} = \frac{u^d t}{g} = u^d \left(\frac{t}{g}\right) = u^d s}$.

Dado que **f(x, y) = v(x) + yw(x) y** $\mathbf{\bar{f}(x,y) = v(x) - yw(x)}$. Se analizarán aquí dos casos:

1. $\mathbf{\bar{f}(P) = 0}$

En este caso y dado que la característica del cuerpo es diferente de dos y $\mathbf{y(P)=b \neq 0}$ será

$$\mathbf{v(a) + bw(a) = 0}$$
$$\mathbf{v(a) - bw(a) = 0}$$

El determinante de este sistema de ecuaciones es **-2b** por lo que su solución es

$$\mathbf{v(a) = w(a) = 0}$$

Dado que **v** y **w** son polinomios en **x** exclusivamente se puede reescribir **f** como

$$\mathbf{f(x,y) = v(x) + yw(x) = (x - a)v_1(x) + y\,(x-a)\,w_1(x) =}$$
$$\mathbf{(x - a)[v_1(x)+yw_1(x)] = (x - a)\,s_1(x)}$$

2. $\mathbf{\bar{f}(P) \neq 0}$

En este caso se puede multiplicar **f** por $\bar{f}/\bar{f}$ obteniéndose

$$\mathbf{f(x, y) = \frac{v^2(x) - s(x)w^2(x)}{\bar{f}(x, y)}}$$

donde $\mathbf{s(x) = x^3 + Ax + B}$. Dado que $\mathbf{f(P) = 0}$ y $\mathbf{\bar{f}(P) \neq 0}$ el numerador debe ser nulo, es decir que $\mathbf{v^2(x) - s(x)w^2(x) = 0}$ para $\mathbf{x = a.}$ Por lo tanto se puede escribir, dado que se trata de un polinomio solamente en x

$$\mathbf{v^2(x) - s(x)w^2(x) = (x - a)d(x)}$$

de donde resulta

$$\mathbf{f(x, y) = (x - a)\frac{d(x)}{\bar{f}(x, y)} = (x - a)s_1(x)}$$

donde $\mathbf{s_1(x, y) = \frac{d(x)}{\bar{f}(x, y)}}$ es una función racional.

En el caso en el que $\mathbf{s_1(P) = 0}$ se puede continuar este proceso. Para comprobar que el proceso no entra en un ciclo infinito se debe tener en cuenta que si $\mathbf{f(x,y) = (x - a)^d s_1(x,y),}$ luego $\mathbf{N(f)(x) = (x - a)^{2d}N(s_1)(x)}$. Pero $\mathbf{N(s_1)(x)}$ no tiene polos en **a** (Dado que $\mathbf{\bar{f}(x, y)}$ no es nulo en **P**) por lo que **2d** debe ser menor que el grado de **N(P)**.

Por lo tanto si **r** tiene un cero en P=(a,b), se puede emplear
$\mathbf{u(x,y) = x - a}$

Si **r** tiene un polo en **P**, entonces $\mathbf{1/r}$ tiene un cero y en este caso **d** será negativo. Si **r** no tiene ni un cero ni un polo entonces será $\mathbf{d = 0}$. Por lo tanto en el caso genérico se puede usar $\mathbf{u = x - a.}$

Caso 2 (P es de orden 2 y P≠O)

En este caso será $\mathbf{P=(\omega_1,0)}$ (ω_1, ω_2,ω_3 son las raíces de $\mathbf{x_3+Ax+B}$). Se demostrará que $\mathbf{u(x,y) = y}$ es aplicable. Se puede asumir que $\mathbf{r=f/g}$ tiene un cero en $\mathbf{P(\omega_1,0)}$ y que f(P)=0. Dado que $\mathbf{f(x,y) = v(x)+yw(x)}$ resultará que $\mathbf{f(P) = 0 = v(\omega_1).}$ Por lo tanto se puede escribir, dado que v es un polinomio en **x**,

$$\mathbf{v(x)=(x - \omega_1)v_1(x)}$$

Dado que las raíces de $\mathbf{s_1(x)}$ son diferentes (La curva no es singular) se obtiene, multiplicando por $\mathbf{(x - \omega_2)(x - \omega_3)}$, la siguiente expresión:

$$\mathbf{f(x, y) = (x - \omega_1)v_1(x) + yw(x) = \frac{(x - \omega_1)(x - \omega_2)(x - \omega_3)v_1(x) + yw_1(x)}{(x - \omega_2)(x - \omega_3)} =}$$

donde

$$\mathbf{\frac{y^2 v_1(x) + yw_1(x)}{(x - \omega_2)(x - \omega_3)} = y\left[\frac{yv_1(x) + w_1(x)}{(x - \omega_2)(x - \omega_3)}\right]}$$

$\mathbf{w_1(x)= (x - \omega_2)(x - \omega_3)w(x).}$

Si la función $\frac{yv_1(x) + w_1(x)}{(x - \omega_2)(x - \omega_3)}$ se anula en **P** el proceso puede continuar con $\mathbf{f_1(x) = w_1(x) + yv_1(x)}$. Por razones análogas a la expuesta anteriormente este proceso debe terminar luego de una cantidad finita de ciclos.

Caso 3 P=O

Se demostrará que **u(x,y) = x/y** es correcto. Supóngase que **r = f/g** y que **r(O) = 0.** Esto significa que **grad(f) < grad(g) = d < 0.** Por la definición de grado será

$$\mathbf{grad(y) - grad(x) = 1}$$

ya que $\mathbf{grad(y^d f)=grad(x^d g)}$ y que $\mathbf{(y/x)^d r}$ es finito y diferente de cero en **O**. Dado la identidad

$$\mathbf{r} = \left(\frac{\mathbf{x}}{\mathbf{y}}\right)^{\mathbf{d}} \left[\left(\frac{\mathbf{y}}{\mathbf{x}}\right)^{\mathbf{d}} \mathbf{r}\right]$$

queda demostrado que **u=x/y** es correcto.

Anexo B

Transformación de la ecuación de tercer grado

Sea la ecuación $x^3 + ax^2 + bx + c = 0$. Haciendo la transformación de variables $x = y + d$ se obtiene:

$$(y + d)^3 + a(y + d)^2 + b(y + d) + c = y^3 + 3dy^2 + 3d^2y + d^3 + ay^2 + 2ady + ad^2 + by + bd + c =$$

$$y^3 + (3d + a)y^2 + (3d^2 + 2ad + b)y + d^3 + ad^2 + bd + c$$

Si se define $d = -\frac{a}{3}$ la expresión anterior se reduce a

$$y^3 + \left(b - \frac{a^2}{3}\right)y + \left(\frac{2}{27}a^3 - \frac{1}{3}ab + c\right)$$

Si se define $A = b - \frac{a^2}{3}$ y $b = \frac{2}{27}a^3 - \frac{1}{3}ab + c$ la ecuación original se transforma en $x^3 + Ax + B = 0$

Haciendo la transformación $x = y + \frac{w}{y}$ se obtiene

$\left(y + \frac{w}{y}\right)^3 + A\left(y + \frac{w}{y}\right) + B$ de donde se deduce que

$$y^3 + 3y^2\frac{w}{y} + 3y\left(\frac{w}{y}\right)^2 + \left(\frac{w}{y}\right)^3 + Ay + A\frac{w}{y} + B = y^3 + 3yw + 3\frac{w^2}{y} + \frac{w^3}{y^3} + Ay + A\frac{w}{y} + B$$

Multiplicando ambos miembros por y^3 queda la siguiente expresión

$$y^6 + 3wy^4 + 3w^2y^2 + w^3 + Ay^4 + Awy^2 + By^3 =$$

$$y^6 + (3w + A)y^4 + By^3 + w(3w + A)y^2 + w^3$$

Haciendo el cambio de parámetro $w = -\frac{A}{3}$ se obtiene

$$y^6 + By^3 + \frac{A^3}{27} = 0$$

Finalmente reemplazando $y^3 = x$ se obtiene $x^2 + Bx - \frac{A^3}{27} = 0$

Resolviendo esta ecuación de segundo [50] orden la solución queda

50. Este método es válido para cuerpos de característica diferente de 2 y 3, ya que en dichos cuerpos 2 es el cero aditivo (característica 2) y 27 es el cero aditivo (característica 3)

$$x = -\frac{A}{2} \pm \sqrt{\frac{B^2}{4} + \frac{A^3}{27}}$$

Para que no existan raíces múltiples es necesario que

$$\boxed{\Delta = 27B^2 + 4A^3 \neq 0}$$