Trabajo Monográfico

Teorema de Hasse y Conjetura de Sato-Tate

Gustavo Rama

Orientador: Gonzalo Tornaría (CMAT-FCIEN)

Licenciatura en Matemáticas
Facultad de Ciencias
Universidad de la República
Uruguay

12 de octubre de 2010

Índice general

Introducción

El tema a tratar en esta monografía serán las curvas elípticas y algunos tópicos en particular referentes a ellas. Una curva elíptica es una ecuación del tipo

$$y^2 = x^3 + ax + b \tag{1}$$

con a, b en algún cuerpo K. Lo que realmente nos interesa son las soluciones de (1). Al conjunto de pares (x, y) en K^2 que satisfacen (1), junto a un elemento $\mathcal{O}$ que llamamos identidad y lo pensamos que como un punto en infinito, le llamamos conjunto de puntos K-racionales, y lo denotamos por $E(K)$

$$E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

A este conjunto se le puede dar una estructura de grupo abeliano luego de desarrollar cierta cantidad de teoría, siendo la parte mas difícil de probar en general la asociatividad.

Para sumar dos puntos P y Q en $E(K)$ hacemos lo siguiente: primero trazamos la recta que los une. Esa recta cortara a un tercer punto R' de la curva elíptica que será el opuesto de esa suma. Definimos $P + Q$ simetrizando R' con respecto del eje Ox obteniendo asi el punto $R = P + Q$. Además suponemos que $\mathcal{O}$ será el neutro de la suma. En la figura 1 se puede ver un ejemplo sencillo.

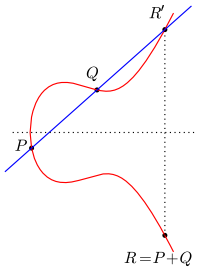


Figura 1: Ejemplo de suma en una curva elíptica. $P + Q + R = \mathcal{O}$.

Una vez definida la estructura de grupo de la curva elíptica, fijamos el cuerpo $K = \mathbb{F}_p$, o sea un cuerpo finito de p elementos, siendo p primo. Nos preguntamos

que cantidad de elementos tendrá el grupo finito $E(\mathbb{F}_p)$. El siguiente teorema fue conjeturado por Artin y demostrado por Hasse.

Teorema de Hasse: *Sea E una curva elíptica definida sobre $K = \mathbb{F}_p$. Entonces*

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}$$

Es interesante calcular el error de que $|E(\mathbb{F}_p)|$ sea $p + 1$, que es a_p

$$a_p = p + 1 - |E(\mathbb{F}_p)|$$

Las cotas dadas por el teorema de Hasse sirvieron para diseñar un algoritmo debido a Shanks y a Mestre, utilizando la estrategia baby-step giant-step de Shanks para encontrar el orden del grupo de la curva elíptica. Que nos da un algoritmo de orden $O(p^{1/4+\varepsilon})$.

Hay un algoritmo debido a Schoof que usa un refinamiento del teorema de Hasse que corre en $O(\log(p)^9)$, y uno mejorado con aportes de Elkies y Atkins que corre en $O(\log(p)^4)$.

Una vez que podemos calcular los a_p nos interesa estudiar la sucesión

$$(a_p/2\sqrt{p})_{p \text{ primo}} \subset [-1, 1]$$

Hay una interesante conjetura sobre la distribución de esta sucesión debido a Sato y a Tate que nos dice que la distribución de esta sucesión converge a la de un semicirculo en $[-1, 1]$. Un ejemplo del histograma para una curva elíptica se puede ver en la figura 2.

Conjetura de Sato-Tate: *Para todo subintervalo $[a, b] \subset [-1, 1]$,*

$$\lim_{X\to\infty} \frac{\#\left\{\frac{a_p}{2\sqrt{p}} \in [a, b] : p < X\right\}}{\#\{\text{primos } p < X\}} = \frac{2}{\pi}\int_a^b \sqrt{1 - x^2}dx$$

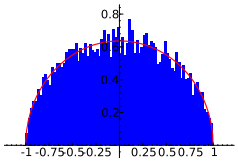


Figura 2: Histograma de distribución de $a_p/2\sqrt{p}$ de una curva elíptica.

La conjetura ha sido probada para una familia grande de curvas elípticas. En 2006 Taylor probo que la conjetura es cierta si E es una curva elíptica sobre un cuerpo totalmente real con reducción multiplicativa para algún primo[Tay].

En el primer capitulo definimos los conceptos básicos de una curva elíptica. Definimos los polinomios y funciones racionales en E, los primeros como polinomios en dos variables en K sobre la ecuación (1), y las funciones racionales

como cocientes de polinomios definidas formalmente. Probamos luego que la suma de los ordenes de los puntos de $E(K)$ es 0.

Necesitamos llevar registro de los ceros y polos de una función racional, para lo que definimos el grupo de divisores de E, que es el grupo libre con base $E(K)$, y denotamos $\mathrm{Div}(E)$. Encontramos una biyección entre $K(E)$ y cierto subgrupo de $\mathrm{Div}(E)$, que nos será de mucha importancia para definir una estructura de grupo abeliano en $E(K)$.

La suma la podemos definir de la siguiente manera, si dos puntos están en $E(K)$ sabemos que la recta que pasa por ellos cortara en un solo punto mas de $E(K)$ que lo definimos como el opuesto de la suma de esos dos puntos. En resumen, si una recta pasa por los puntos P, Q, R entonces $P + Q + R$ será el neutro del grupo. La biyección mencionada sirve para probar que esta operación es asociativa. Probarla de otra manera, por ejemplo de manera algebraica es mucho mas engorroso.

Una vez definida la suma investigamos las funciones racionales g_n y h_n dadas por

$$nP = (g_n(P), h_n(P))$$

Junto a la información que obtenemos con la definición de derivación en $E(K)$, podemos entre otras cosas calcular la cantidad de puntos de n-torsión de $E(K)$

$$E[n] = \{P \in E(K) : nP = \mathcal{O}\}$$

que es n^2 y usando la estructura propia de la curva vemos que

$$E[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Por ultimo calculamos polinomios ψ_n asociados a las funciones g_n y h_n, que entre otras propiedades cumplen que

$$\begin{aligned} g_n &= x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2} \\ h_n &= \frac{\psi_{n+1}\psi_n^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \end{aligned}$$

Y nos permiten probar que el grupo de p-torsión es $\mathbb{Z}/p\mathbb{Z}$ o el grupo trivial, siendo p la característica de K.

El capitulo segundo esta dedicado a la demostración del teorema de Hasse

Para demostrarlo desarrollamos conceptos como el índice de ramificación de mapas racionales, que son pares de funciones racionales que satisfacen (1).

Definimos los Endomorfismos en E como mapas racionales que a su vez sean homomorfismo de grupo.

Luego definimos el Pairing de Weil, una herramienta importante para la demostración del teorema, que es un mapa que devuelve una raíz de la unidad en K, dados dos puntos de $E(K)$. Probamos algunas propiedades básicas del Pairing de Weil, una de las cuales tiene demostración nada trivial, y sumando

propiedades básicas de Endomorfismos y matrices sobre anillos llegamos a la demostración del teorema.

En el capitulo tercero presentamos algoritmos para calcular, dado un primo p, el entero a_p que cumple

$$|E(\mathbb{F}_p)| = p + 1 - a_p$$

donde $\mathbb{F}_p$ es el cuerpo finito de p elementos.

El primer algoritmo, que es el mas directo, calculamos a_p como la suma de ciertos símbolos de Legendre. Lo cual nos da un algoritmo bueno para p pequeño.

Usando la cota de la primera parte del teorema de Hasse podemos usar la estrategia baby-step giant-step de Shanks, que presentamos en su forma mas general, para hallar $|E(\mathbb{F}_p)|$ y por lo tanto a_p.

Finalizamos el capitulo presentando escuetos comentarios sin demostración de otros algoritmos mas rápidos que el de Shanks, como es el de Schoof y SEA. También calculamos la velocidad del algoritmo de Shanks contra el algoritmo SEA en ciertas curvas, ambos algoritmos implementados en los programas de matemática Sage y Pari/GP[Pari][Sage].

Hablamos en el cuarto capitulo de la conjetura de Sato-Tate, como de otras dos conjeturas que la refinan en cierto sentido.

Presentamos también calculos que hicimos para ajustar curvas con la que se puede definir la conjetura. Buscábamos una dependencia entre el rango de la curva y ciertas constantes que hallamos experimentalmente. La dependencia quedo sin responder, con vistas a investigaciones futuras.

Seguimos en esta parte una presentacion de William Stein en “Sage Days 5, Clay Math Institute, 2007” [Ste1], sobre un trabajo con Barry Mazur.

En el apéndice presentamos todos los calculos hechos en el capitulo anterior.

Capítulo 1

Curvas Elípticas

1.1. Curvas Elípticas

Definición 1.1.1. Una *curva elíptica* sobre un cuerpo K es una curva definida por una ecuación de la forma

$$Y^2 = X^3 + AX + B \tag{1.1}$$

donde $A, B \in K$ y $-16(4A^3 + 27B^2) \neq 0$.

El conjunto de puntos *K-racionales* de E es

$$E(K) = \{(a, b) \in K^2 : b^2 = a^3 + Aa + B\} \cup \{\mathcal{O}\}$$

Al elemento $\mathcal{O}$ le llamamos *identidad*, y a el resto de los puntos les llamamos *puntos finitos*.

Definición 1.1.2. Dada una curva elíptica E como en (1.1) definimos el *discriminante* de E como

$$\Delta(E) = -16(4A^3 + 27B^2)$$

Observación 1.1.1.

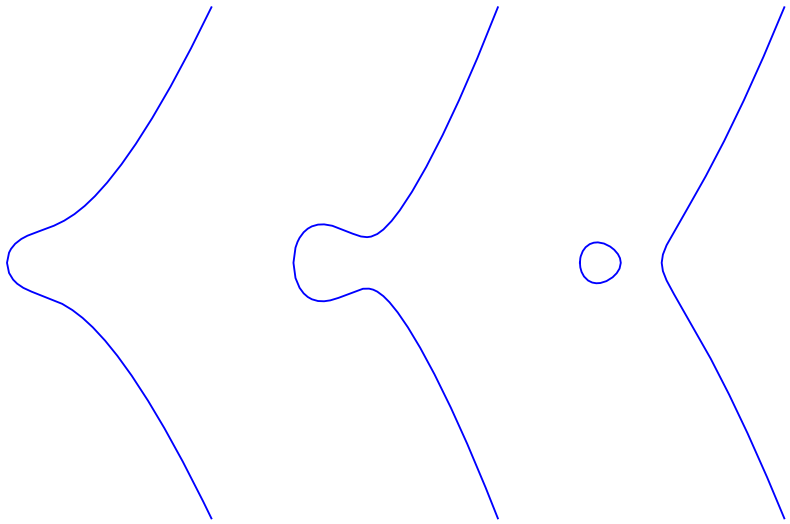
i. Al pedir que el discriminante sea no nulo estamos pidiendo que el polinomio $F(X, Y) = Y^2 - X^3 - AX - B$ no tenga raíces múltiples. Es equivalente a pedir que las derivadas parciales de F no se anulen simultaneamente en un punto que anula F.

ii. Si K tiene característica 2, entonces para $A, B \in K$ $\Delta(E) = -16(4A^3 + 27B^2) = 0$, por lo que no existirían curvas elípticas con nuestra definición. Existe un problema similar cuando la característica es 3.

Si consideramos ecuaciones de la forma

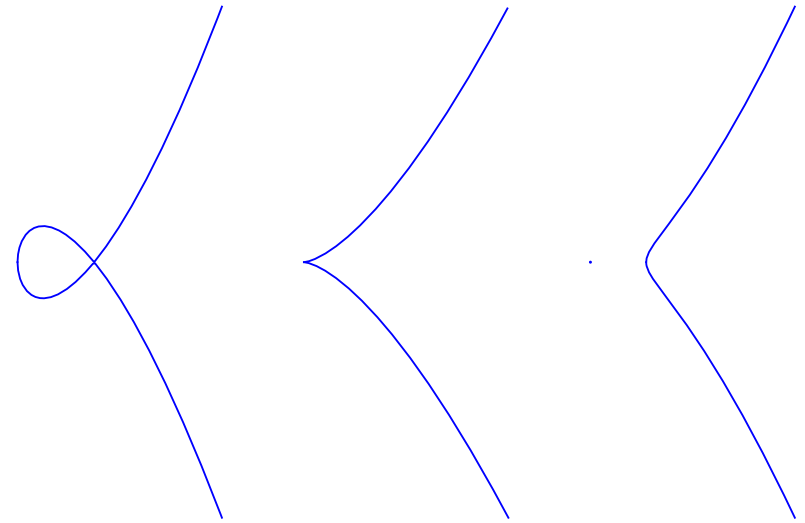
$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

obtenemos una noción más general de curvas elípticas, que nos permite definir correctamente curvas en características 2 y 3.



(a) $Y^2 = X^3 + X + 1$ (b) $Y^2 = X^3 - X + 1$ (c) $Y^2 = X^3 - X$

Figura 1.1: Curvas elípticas sobre $K = \mathbb{R}$.



(a) $Y^2 = X^3 - 3X + 2$ (b) $Y^2 = X^3$ (c) $Y^2 = X^3 - 3X - 2$

Figura 1.2: Curvas en $\mathbb{R}$ que no son elípticas.

iii. Los símbolos "x" e "y" los usaremos como las funciones coordenadas en $E(K)$, definidas como $x(a,b) = a$ y $y(a,b) = b$

iv. Pensaremos al punto $\mathcal{O}$ como un punto "en infinito". Y denotaremos $x(\mathcal{O}) = y(\mathcal{O}) = \infty$

En la figura 1.1 damos tres ejemplos de los puntos finitos de curvas elípticas cuando $K = \mathbb{R}$.

En la figura 1.2 damos ejemplos de curvas cubicas que no son elípticas ya que su discriminante es nulo.

1.2. Polinomios y funciones racionales

Definición 1.2.1. Un *polinomio en* E es un elemento de $K[x,y]$, donde

$$K[x,y] = \{f(x,y) : f \in K[X,Y]\}$$

con x e y las funciones coordenadas definidas en 1.1.1.

Observación 1.2.1. A $K[x,y]$ lo podemos pensar como el anillo de polinomios en las variables X, Y módulo el ideal generado por el polinomio $Y^2 - X^3 - AX - B$.

O sea

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

Observación 1.2.2. Todo polinomio en E lo podemos escribir como

$$f(x,y) = v(x) + yw(x) \tag{1.2}$$

donde $v, w \in K[X]$. Escribimos $f(x,y) = a_{n,m}x^n y^m + \cdots + a_{1,0}x + a_{0,1}y + a_{0,0}$ con $a_{i,j} \in K \ \forall \ i = 0,1,\ldots,n, \ j = 0,1,\ldots,m$. Como se cumple $y^2 = x^3 + Ax^2 + B$ cambiamos toda potencia de y mayor que 1 por $x^3 + Ax + B$.

Decimos que f escrito como en (1.2) está escrito en *forma canónica*.

Definición 1.2.2. Si $f(x,y) = v(x) + yw(x)$ es un polinomio en E, su *conjugado* $\bar{f}$ es el polinomio $\bar{f}(x,y) = v(x) - yw(x)$ y su *norma* es el polinomio $N(f) = f\bar{f}$.

Observación 1.2.3. Si $f(x,y) = v(x) + yw(x)$ entonces $N(f)(x,y) = v(x)^2 - s(x)w(x)^2$, donde $s(x) = x^3 + Ax + B$. De modo que podemos ver a $N(f)$ como una función en una variable, o sea un elemento de $K[x]$.

Esto nos sirve para probar, por ejemplo, que la elección de v y w es única. Si suponemos que $f(x,y)$ es la función nula, entonces $N(f)$ también es la función nula. Por lo tanto, como el grado de s es impar y los grados de v^2 y w^2 son pares, el polinomio v^2 tiene que ser nulo ya que $v(x)^2 = s(x)w(x)^2$, donde el grado de sw^2 es impar.

Concluimos que v es el polinomio nulo, por lo que w también ya que s es no nulo.

De la misma manera se prueba que $K[x,y]$ no tiene divisores del cero.

Definición 1.2.3. Una *función racional* en E es una clase de equivalencia del cociente formal de polinomios f/g, con $g \neq 0$, donde identificamos f/g con h/k si $fk = gh$ como polinomios en E.

Es fácil de ver que el conjunto de funciones racionales en E forman un cuerpo que donotamos $K(E)$

Observación 1.2.4. Mientras que los polinomios en E tienen valores para todo punto finito de la curva elíptica, las funciones racionales pueden no tener, y pueden tener en $\mathcal{O}$.

Notar que si $r = f/g$ es una función racional en E, multiplicando por $\bar{g}/\bar{g}$, podemos escribir $r(x, y) = a(x) + yb(x)$, donde a y b son funciones racionales sólo en x.

Definición 1.2.4. Si r es una función racional en E y P es un punto finito de $E(K)$, decimos que r es *finita* en P si existen polinomios f y g en E tal que $r = f/g$ y $g(P) \neq 0$. Si r es finita en P definimos $r(p) = f(P)/g(P)$ que no depende de f y g.

Queremos calcular el valor de una función racional en $\mathcal{O}$, si es posible. La manera usual en cálculo para hallar el valor de una función racional en infinito es comparando los grados del numerador y el denominador. En nuestro caso, la situación es más complicada ya que estamos trabajando con dos variables, x e y.

Mientras, sería natural asignarle grado 1 a x e y, pero esto no sería consistente con nuestra relación fundamental $y^2 = x^3 + Ax + B$. Esta relación nos sugiere que el grado de y sería $3/2$ el grado de x.

Como no queremos trabajar con grados fraccionales vamos a asignarle grado 3 a y y grado 2 a x.

Para evitar confusiones, denotaremos el grado usual de un polinomio f en la variable x como $\mathrm{gr}_x(f)$.

Definición 1.2.5. Sea $f(x, y) = v(x) + yw(x)$ un polinomio no nulo en E. Definimos el *grado* de de f como:

$$\mathrm{gr}(f) = max\{2 \cdot \mathrm{gr}_x(v), 3 + 2 \cdot \mathrm{gr}_x(w)\} \tag{1.3}$$

Lema 1.2.1. *Si f es un polinomio en E entonces*

$$\mathrm{gr}(f) = \mathrm{gr}_x(N(f))$$

Demostración: Si escribimos $f(x, y) = v(x) + yw(x)$, $N(f)(x) = v^2(x) - s(x)w^2(x)$, donde $s(x) = x^3 + Ax + B$. Por lo tanto, el lema se desprende de la definición de grado. □

Para ver que la definición de grado es útil, debemos probar el siguiente resultado.

Proposición 1.2.2. *Si f y g son dos polinomios en E entonces* $\mathrm{gr}(f \cdot g) = \mathrm{gr}(f) + \mathrm{gr}(g)$

Demostración: Usando el lema anterior, obtenemos

$$\begin{aligned} \mathrm{gr}(fg) &= \mathrm{gr}_x(N(fg)) = \mathrm{gr}_x(N(f)N(g)) \\ &= \mathrm{gr}_x(N(f)) + \mathrm{gr}_x(N(g)) = \mathrm{gr}(f) + \mathrm{gr}(g) \end{aligned}$$

ya que conocemos la proposición para gr_x. □

Observemos que no podemos definir del grado del denominador o el numerador de una función racional, pero si podemos ver que la diferencia entre ellos es constante. Si $r = f/g = h/k \Rightarrow \mathrm{gr}(f) + \mathrm{gr}(k) = \mathrm{gr}(h) + \mathrm{gr}(g)$, ya que $fk = hg$ $\Rightarrow \mathrm{gr}(f) - \mathrm{gr}(g) = \mathrm{gr}(h) - \mathrm{gr}(k)$.

Podemos entonces hacer las siguientes definiciones:

Definición 1.2.6. Sea $r = f/g$ función racional en E.

- Si $\mathrm{gr}(f) < \mathrm{gr}(g)$ definimos $r(\mathcal{O}) = 0$.
- Si $\mathrm{gr}(f) > \mathrm{gr}(g)$ decimos que r no es finita en $\mathcal{O}$ y denotamos $r(\mathcal{O}) = \infty$.
- Si $\mathrm{gr}(f) = \mathrm{gr}(g)$
  - Si el grado de f es par, escribiendo a f y g en forma canónica, tendrían sus términos de grado mas alto de la forma ax^d y bx^d respectivamente (para algunos $a, b \in K$ y un entero d). Definimos $r(\mathcal{O}) = a/b$.
  - Si f es de grado impar, los términos de grado más alto serán ayx^d y byx^d, y definimos $r(\mathcal{O}) = a/b$.

1.3. Ceros y Polos

Definición 1.3.1. Sea r una función racional en E, r tiene un *cero* en $P \in E(K)$ si $r(P) = 0$, r tiene un *polo* en P si $r(P) = \infty$.

Antes de demostrar el siguiente teorema necesitamos estudiar ciertos puntos de la curva.

Recordemos que $X^3 + AX + B$ tiene tres raíces diferentes en $\bar{K}$, que les llamaremos ω_1, ω_2 y ω_3. Denotamos ω cuando nos referimos a una cualquiera de ellas.

Entonces E puede tener sólo tres puntos con coordenada y nula, $(\omega_1, 0)$, $(\omega_2, 0)$ y $(\omega_3, 0)$. Estos puntos son llamados *puntos de orden* 2. Quedará más claro el nombre cuando definamos la ley de grupo para E.

Teorema 1.3.1. *Sea $P \in E$, entonces existe una función racional u, cero en P con la siguiente propiedad:*

Si r es una función racional no nula, entonces

$$r = u^d t \tag{1.4}$$

para algún $d \in \mathbb{Z}$ y t una función racional que no se anula en P. Es más, el entero d no depende de la elección de la función u.

Demostración: Hay que diferenciar tres casos para la demostración.

- En el primer caso, asumimos que P no es $\mathcal{O}$ ni es un punto de orden 2. Sea entonces $P = (a, b)$ con $a, b \in K$, vamos a probar que podemos tomar $u(x, y) = x - a$. Supongamos que $r(P) = 0$. Entonces $r = f/g$ con $f(P) = 0$ y $g(P) \neq 0$. Si podemos descomponer $f = u^d s$ como en (1.4), dividiendo por g llegamos al resultado deseado para r.

  Escribimos $f(x, y) = v(x)+yw(x)$, $\bar{f} = v(x)-yw(x)$. Si $\bar{f}(P) = 0$, entonces como la característica de K no es 2 y $b = y(P) \neq 0$, sumando $f(a, b)$ y $\bar{f}(a, b)$, obtenemos que $v(a) = 0$ y $w(a) = 0$. Como v y w son polinomios en una variable $v(x) = (x - a)v_1(x)$ y $w(x) = (x - a)w_1(x)$ con v_1 y w_1 polinomios en una variable. Entonces

  $$f(x, y) = (x - a)t_1(x, y)$$

  para algún polinomio t_1 en E.

  Si $\bar{f}(P) \neq 0$, podemos multiplicar f por $\bar{f}/\bar{f}$ y obtenemos

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

  con $s(x) = x^3 + Ax + B$. Que $f(P) = 0$ y $\bar{f}(P) \neq 0$ implica $v^2(x) - s(x)w^2(x) = 0$ para $x = a$, siendo éste un polinomio en una variable. Por lo tanto, como en el caso anterior,

  $$f(x, y) = (x - a)t_1(x, y)$$

  pero aquí t_1 es una función racional finita en P. En ambos casos podemos, si $t_1(P) = 0$, seguir con el proceso.

  Para ver que este proceso debe terminar observamos que si $f(x, y) = (x - a)^d t_1(x, y)$, entonces $N(f)(x) = (x - a)^{2d} N(t_1)(x)$. Y sabemos que $N(t_1)(x)$ no tiene un polo en a por lo tanto $2d$ debe ser menor que el orden de $N(f)$ como una función sólo de x.

  Luego si r tiene un cero en P podemos tomar u como $x - a$. Si r tiene un polo en P, entonces $1/r$ tiene un cero en P, y $x - a$ sigue sirviendo, pero con $d < 0$. Si r no tiene un polo ni un cero en P podemos tomar $d = 0$ y $t = u$.

- Ahora asumimos que P es un punto de orden dos y $P = (\omega_1, 0)$. Vamos a probar que podemos tomar u como la función y.

  Como antes, si $r(P) = 0$ asumimos que $r = f/g$ y $f(P) = 0$, lo que implica que $v(\omega_1) = 0$ donde $f(x, y) = v(x) + yw(x)$.

  Luego $v(x) = (x-\omega_1)v_1(x)$ con v_1 un polinomio en x. Como $s(x)$ no tiene

raíces dobles, podemos escribir $s(x) = (x - \omega_1)s_1(x)$ con $s_1(\omega_1) \neq 0$,

$$\begin{aligned} f(x,y) &= (x-\omega_1)v_1(x) + yw(x) \\ &= \frac{(x-\omega_1)s_1(x)v_1(x) + yw_1(x)}{s_1(x)} \\ &= \frac{s(x)v_1(x) + yw_1(x)}{s_1(x)} \\ &= \frac{y^2v_1(x) + yw_1(x)}{s_1(x)} \\ &= y\left[\frac{yv_1(x) + w_1(x)}{s_1(x)}\right] \end{aligned}$$

donde $w_1(x) = s_1(x)w(x)$. Si la función entre paréntesis se anula en P repetimos el proceso para $w_1(x) + yv_1(x)$. Este proceso debe terminar porque factorizamos $(x - \omega_1)$ de v o w, que pueden tener una cantidad finita de estos factores. Por lo tanto podemos tomar $u(x, y) = y$.

- Como último caso debemos probar el teorema para $P = \mathcal{O}$, para esto demostraremos que $u(x, y) = x/y$ cumple la tesis.

  Supongamos que $r = f/g$ con $r(\mathcal{O}) = 0$. Esto es lo mismo que $\text{gr}(f) - \text{gr}(g) = d < 0$. Como $\text{gr}(y) - \text{gr}(x) = 1$, $\text{gr}(y^d f) = \text{gr}(x^d g)$ y $(y/x)^d r = \frac{y^d f}{x^d g}$ por definición es finita y no nula en $\mathcal{O}$.

  Luego, puesto que

  $$r = (x/y)^d \left[(y/x)^d r\right]$$

  probamos que podemos tomar $u(x, y) = x/y$ en $\mathcal{O}$.

Para ver que el número d es único, supongamos que u y u' son dos funciones racionales que cumplen las condiciones del teorema. Esto implica que podemos escribir $u = (u')^e s$ y $u' = u^f t$, entonces

$$u = u^{ef}(t^e s) \tag{1.5}$$

Si $ef \neq 1$ dividiendo en (1.5) por u y evaluando en P, obtenemos el absurdo $1 = 0$ si $ef > 1$. Y si $ef < 1$ dividimos por u^{ef} para llegar a $0 = t(P)^e s(P) \neq 0$. Si $e = -1$ entonces $uu' = s$ y evaluando en P se vuelve a presentar el absurdo $0 = 1$.

Por lo que concluimos $e = f = 1$. Entonces si r es una función racional no nula que se anula en P, podemos escribir $r = u^d s = (u')^d t$. □

El teorema anterior nos permite definir los siguientes conceptos:

Definición 1.3.2. Una función que cumple las condiciones del teorema 1.3.1 es llamada *variable de uniformización* en P.

Si r es una función racional y $r = u^d s$ donde u es una variable de uniformización en P decimos que el *orden* de r en P es d y escribimos

$$\text{ord}_P(r) = d$$

Definimos la *multiplicidad* de un cero como el orden de la función en el punto, la *multiplicidad* de un polo como el opuesto del orden de la función en el punto.

Decimos que un polo o un cero es simple, doble o triple si tiene multiplicidad uno, dos o tres respectivamente.

Proposición 1.3.2. *Sean $P \in E(K)$, r y s funciones racionales en E, entonces se cumple:*

1. $\mathrm{ord}_P(rs) = \mathrm{ord}_P(r) + \mathrm{ord}_P(s)$
2. $\mathrm{ord}_P(1/r) = -\mathrm{ord}_P(r)$
3. $\mathrm{ord}_P(r/s) = \mathrm{ord}_P(r) - \mathrm{ord}_P(s)$

Demostración: Sea u una variable de uniformización en P,

$$r = u^{d_1} s_1$$
$$s = u^{d_2} s_2$$

siendo s_i funciones racionales finitas y no nulas en P y $d_i \in \mathbb{Z}$.

1. Ocurre que $rs = u^{d_1} s_1 u^{d_2} s_2 = u^{(d_1+d_2)} s_1 s_2$ y $s_1 s_1$ es no nula y finita en P. Entonces $\mathrm{ord}_P(rs) = \mathrm{ord}_P(r) + \mathrm{ord}_P(s)$.
2. Se verifica que $1/r = \frac{1}{u^{d_1} s_1} = u^{-d_1} \frac{1}{s_1}$ y $\frac{1}{s_1}$ es no nula y finita en P porque s_1 lo es.
3. Se deduce de las partes anteriores.

□

Mostraremos cuatro ejemplos de variables de uniformización.

Ejemplo 1.3.1.

1. Sea f un polinomio en E. Si $\mathrm{gr}(f) = n$

   $$f(x,y) = \left(\frac{x}{y}\right)^{-n} \frac{x^n f(x,y)}{y^n}$$

   y $\mathrm{gr}(x^n f) = \mathrm{gr}(x^n) + \mathrm{gr}(f) = 2n + n = 3n = \mathrm{gr}(y^n)$, entonces $\frac{x^n f(x,y)}{y^n}$ es no nula y finita en $\mathcal{O}$. Por lo tanto f tiene un polo en $\mathcal{O}$ con multiplicidad $gr(f)$.

2. Sean $P \in E(K)$ con $P = (k,l)$, $k, l \in K$ y $l \neq 0$, $u(x,y) = x - k$.

   Como u es una variable de uniformización en P $\mathrm{ord}_P(u) = 1$. Claramente, $P' = (k, -l)$ es un punto de E y $\mathrm{ord}_{P'}(u) = 1$ ya que $u(P') = 0$.

   Para el resto de los puntos finitos de E, u no se anula, por lo tanto u tiene orden 0 en ellos. También sabemos que u tiene un polo en $\mathcal{O}$ y tiene grado 2, entonces $\mathrm{ord}_{\mathcal{O}}(u) = -2$.

   Concluimos que u tiene dos ceros con multiplicidad 1 y un polo con multiplicidad 2.

3. Consideramos ahora la función y y K algebraicamente cerrado. Vimos que y es una variable de uniformización en los tres puntos de orden 2 que son $(\omega_1, 0)$, $(\omega_2, 0)$ y $(\omega_3, 0)$, por lo tanto y tiene tres ceros con multiplicidad uno en esos puntos.

   Además y tiene orden 0 en el resto de los puntos finitos.

   Como $\mathrm{gr}(y) = 3$ llegamos a la conclusión de que $\mathrm{ord}_{\mathcal{O}}(y) = -3$. Entonces y tiene tres ceros con multiplicidad uno y un polo con multiplicidad tres.

4. Si K es algebraicamente cerrado. La función $u(x, y) = x/y$ tiene un cero de orden uno en $\mathcal{O}$ y luego hay que diferenciar dos casos. Si $B \neq 0$, u tiene ceros de orden uno en los puntos $(0, \sqrt{B})$ y $(0, -\sqrt{B})$ ya que

$$u(x, y) = (x - 0)^1 \frac{1}{y}$$

   además tiene polos de orden uno en los puntos de orden dos porque

$$u(x, y) = y^{-1} x$$

   entonces u tiene tres ceros de orden uno y tres polos de orden uno.

   Si $B = 0$, u tiene un cero simple en $(0, 0)$ ya que

$$\frac{x}{y} = \frac{xy}{y^2} = \frac{xy}{x^3 + Ax} = y^1 \frac{1}{x^2 + A}$$

   y $A \neq 0$. Tiene además polos en $(\pm\sqrt{-A}, 0)$ con multiplicidad uno, ya que

$$\frac{x}{y} = \frac{1}{y} x$$

   y $\sqrt{-A} \neq 0$, ya que si no $A = 0$ y seria $\Delta(E) = 0$.

Los ejemplos anteriores dan pie al siguiente teorema:

Teorema 1.3.3. *Sea r una función racional en E. Si K es algebraicamente cerrado entonces*

$$\sum_{P \in E} \mathrm{ord}_P(r) = 0$$

Necesitamos el siguiente lema para poder probar el teorema.

Lema 1.3.4. *Sea un polinomio f en E y K algebraicamente cerrado. La suma de las multiplicidades de los ceros de f es igual al grado de f, o sea*

$$\sum_{P \in E/\ f(P)=0} \mathrm{ord}_P(f) = \mathrm{gr}(f)$$

Demostración: Sea $n = \mathrm{gr}(f)$. Por el lema 1.2.1, $\mathrm{gr}_x(N(f)) = n$, escribimos

$$N(f)(x) = f\bar{f}(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$$

donde los $a_i \in K$, que pueden no ser diferentes.

Si $a_i \neq \omega$, entonces $(x - a_i)$ tiene dos raíces en E, $(a_i, \sqrt{a_i^3 + Aa_i + B})$ y $(a_i, -\sqrt{a_i^3 + Aa_i + B})$.

Si $a_i = \omega$ entonces $(x - a_i)$ tiene una sola raíz en E pero de multiplicidad dos.

Concluimos que $f\bar{f}$ tiene exactamente $2n$ raíces contadas con multiplicidad.

Ahora, como f y $\bar{f}$ tienen la misma cantidad de raíces, ya que si escribimos $f(x, y) = v(x) + yw(x)$ entonces $f(a, b) = v(a) + bw(a) = \bar{f}(a, -b)$ y (a, b) es raíz de f si y sólo si $(a, -b)$ es raíz de $\bar{f}$.

Podemos concluir entonces que la suma de las multiplicidades de los ceros de f es n. □

Demostración del Teorema 1.3.3: Alcanza con probar el teorema para un polinomio ya que si $r = f/g$ entonces en virtud de la proposición 1.3.2, $\mathrm{ord}_P(r) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)\ \forall\ P \in E$. Entonces

$$\sum_{P \in E} \mathrm{ord}_P(r) = \sum_{P \in E} \mathrm{ord}_P(f) - \sum_{P \in E} \mathrm{ord}_P(g)$$

Sea entonces f un polinomio en E, por el lema 1.3.4

$$\sum_{P \in E - \{\mathcal{O}\}} \mathrm{ord}_P(f) = \mathrm{gr}(f)$$

y como vimos en el ejemplo 1.3.1.1 f tiene un polo de multiplicidad $\mathrm{gr}(f)$ en $\mathcal{O}$. Por lo tanto

$$\sum_{P \in E} \mathrm{ord}_P(f) = \sum_{P \in E - \{\mathcal{O}\}} \mathrm{ord}_P(f) + \mathrm{ord}_{\mathcal{O}}(f) = \mathrm{gr}(f) - \mathrm{gr}(f) = 0$$

con lo que queda demostrado el teorema. □

Lema 1.3.5. *Sea f un polinomio no constante en E, con K algebraicamente cerrado. Entonces f tiene al menos dos ceros simples o uno doble en puntos finitos de E.*

Demostración: Como f es no constante $\mathrm{gr}(f) \geq 2$ ya que $\mathrm{gr}(x) = 2$ y $\mathrm{gr}(y) = 3$ y f debe tener una x o una y. El resultado entonces se deduce del lema 1.3.4. □

Observación 1.3.1. Si K es algebraicamente cerrado E tiene infinitos puntos, ya que si $x_0 \in K$ entonces $\sqrt{x_0^3 + Ax_0 + B} \in K$, y K tiene infinitos elementos.

Proposición 1.3.6. *Si dos funciones racionales sobre E coinciden en infinitos puntos entonces son iguales cuando K es algebraicamente cerrado.*

Demostración: Si r y s coinciden en infinitos puntos finitos $r - s$ tiene infinitos ceros y si no es constante debe tener infinitos polos por el teorema 1.3.3, de otra manera r y s también tendría infinitos polos.

Probaremos que una función racional r no constante no puede tener infinitos polos. Si $r = f/g$ tiene infinitos polos, g debe de tener infinitos ceros, g tiene que ser constante cero por el lema 1.3.4, luego r debe ser constante nula. □

Lema 1.3.7. *Una función racional sin polos finitos es un polinomio.*

Demostración: Sea r una función racional sin polos finitos. Si escribimos $r(x, y) = a(x) + yb(x)$ con a y b funciones racionales, como r no tiene polos finitos, $\bar{r} = a - yb$ tampoco. Luego $r + \bar{r} = 2a$ no tiene polos finitos.

Si a tiene un polo como función de una variable entonces tiene como función en E. Entonces a es un polinomio. Esto implica que $yb = r - a$ no tiene polos finitos. Por lo tanto $(yb)^2 = sb^2$ tampoco tiene polos finitos, donde $s(x) = x^3+Ax+B$. Si b tiene un polo en un punto finito entonces escribiendo $b = f/g$, f y g polinomios, $g(x) = 0$ para algún $x \in K$, $P = (x, y)$. En ese caso, $b^2 = f^2/g^2$y g^2 tiene un cero con multiplicidad al menos dos. La única manera entonces de que sb^2 tenga un polo en P es que s tenga un cero con multiplicidad mayor a dos, pero s tiene sólo raíces simples. Por lo tanto b no tiene polos finitos, y r,b son polinomios. □

Definición 1.3.3. Un *mapa racional* F en E es un par (r, s), donde r y s son funciones racionales en E que cumplen la condición

$$s^2 = r^3 + Ar + B$$

Si definimos $F(P) = \mathcal{O}$ cuando r y s no son finitos en P, vemos que $F : E \to E$ $F(P) = (r(P), s(P))$, define una función ya que r y s tienen polos en los mismos puntos.

Observación 1.3.2. Una manera interesante de ver los mapas racionales en E es la siguiente. Si E está definida por la ecuación

$$Y^2 = X^3 + AX + B \tag{1.6}$$

Sea $H = K(E)$ el cuerpo de funciones racionales en E. Entonces los mapas racionales son los puntos $E(K)$-racionales en la curva E definida por la ecuación (1.6) sobre H. La identidad de $E(K)$ lo podemos pensar como el mapa $\mathcal{O}_M$ con valor constante $\mathcal{O}$.

1.4. Divisores y Rectas

Necesitamos un método para llevar cuenta de los polos y ceros de una función racional r. La manera que haremos será la de las sumas formales de elementos de E.

Definición 1.4.1. Sea $S \neq \emptyset$. El *grupo abeliano libre generado por* S es el conjunto de combinaciones lineales formales de elementos de S

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

donde $m(s) \in \mathbb{Z}$ y $m(s) = 0$ salvo para una cantidad finita o vacía de elementos de S.

Definición 1.4.2. Sea E una curva elíptica sobre K cuerpo algebraicamente cerrado. El *grupo de divisores* de E es el grupo abeliano libre generado por los puntos de E, y lo denotamos $\mathrm{Div}(E)$. Dado $P \in E$ denotamos $\langle P \rangle$ al divisor tal que $m(P) = 1$ y $m(P') = 0$ para todo $P' \in E - \{P\}$.

Si $\Delta = \sum_{P \in E} m(P)\langle P \rangle \in \mathrm{Div}(E)$ definimos su *grado* como:

$$\mathrm{gr}(\Delta) = \sum_{P \in E} m(P) \in \mathbb{Z}$$

Si r es una función racional sobre E le asociamos un divisor por la siguiente ecuación

$$\mathrm{div}(r) = \sum_{P \in E} \mathrm{ord}_P(P)\langle P \rangle$$

Observación 1.4.1.

- Observamos que una función racional tiene una cantidad finita de ceros y polos. Esto fue demostrado en el Lema 1.3.4 si K es algebraicamente cerrado.

  Si no lo es, el conjunto de ceros o de polos de r es un subconjunto del conjunto de ceros o polos de r definida en E sobre la clausura algebraica de K.

- Si dos funciones racionales tienen el mismo divisor entonces, por la Proposición 1.3.2 y el Lema 1.3.7, su cociente es constante. Entonces, una manera de probar que dos funciones racionales son iguales es probar que tienen el mismo divisor y concuerdan en un punto. En general el único punto al que podemos acceder es $\mathcal{O}$, y usualmente las funciones tienen polos en $\mathcal{O}$. En ese caso, podemos comparar los coeficientes principales, que definiremos a continuación.

Definición 1.4.3. Sea una función racional r con $\mathrm{ord}_{\mathcal{O}}(r) = d$. El *coeficiente principal* de r es:

$$[(y/x)^d r](\mathcal{O})$$

Proposición 1.4.1. *Dos funciones racionales r y s que tienen igual divisor y sus coeficientes principales coinciden son iguales.*

Demostración: Ya vimos que $r/s = C$ constante. Sea $n = \mathrm{ord}_{\mathcal{O}}(r) = \mathrm{ord}_{\mathcal{O}}(s)$ entonces

$$C = \frac{(y/x)^n r}{(y/x)^n s}(\mathcal{O}) = \frac{((y/x)^n r)(\mathcal{O})}{((y/x)^n s)(\mathcal{O})}$$

entonces r y s son iguales si y solo si $C = 1$ si y solo si los coeficientes principales de r y s son iguales. □

Ejemplo 1.4.1.

1. Sea $P = (a, b) \in E$ con $b \neq 0$, y $r_1 = (x - a)$. Ya vimos en el ejemplo 1.3.1 que r_1 tiene ceros simples en P y $P' = (a, -b)$ y un polo doble en $\mathcal{O}$. Entonces $\mathrm{div}(r_1) = \langle P \rangle + \langle P' \rangle - 2\langle \mathcal{O} \rangle$

2. Si K es algebraicamente cerrado. Sea $r_2 = y$. Si P_i $(i = 1, 2, 3)$ son los puntos de orden 2, entonces

$$\operatorname{div}(r_2) = \langle P_1 \rangle + \langle P_2 \rangle + \langle P_3 \rangle - 3\langle \mathcal{O} \rangle$$

3. Si $r_3 = x/y$ y K algebraicamente cerrado, $Q = (0, \sqrt{B})$ y $Q' = (0, -\sqrt{B})$, con $B \neq 0$, entonces

$$\operatorname{div}(r_3) = \langle Q \rangle + \langle Q' \rangle - \langle P_1 \rangle - \langle P_2 \rangle - \langle P_3 \rangle + \langle \mathcal{O} \rangle$$

Definición 1.4.4. Decimos que un divisor Δ es *principal* si $\Delta = \operatorname{div}(r)$ para alguna función racional r.

Si $\Delta_1 - \Delta_2$ es principal, con $\Delta_1, \Delta_2 \in \operatorname{Div}(E)$, Δ_1 y Δ_2 son *linealmente equivalentes* y escribimos $\Delta_1 \sim \Delta_2$.

Proposición 1.4.2. *Si r_1 y r_2 son funciones racionales en E, entonces*

$$\operatorname{div}(r_1 r_2) = \operatorname{div}(r_1) + \operatorname{div}(r_2) \tag{1.7}$$

y el conjunto de divisores principales forma un subgrupo de $\operatorname{Div}(E)$.

Demostración: El resultado (1.7) se deduce inmediatamente de la Proposición 1.3.2.

Sean ahora $\Delta_1 = \operatorname{div}(r_1)$ y $\Delta_2 = \operatorname{div}(r_2)$, con r_1, r_2 funciones racionales. Entonces $\Delta_1 + \Delta_2 = \operatorname{div}(r_1 r_2)$. Además el divisor que tiene todas sus entradas cero es $\operatorname{div}(r)$ donde r es la función racional nula. □

De aca al final de la sección asumimos que K es algebraicamente cerrado.

Definición 1.4.5. Por la Proposición anterior el conjunto de los divisores principales es un subgrupo que denotaremos por $\operatorname{Prin}(E)$.

Definimos también $\operatorname{Div}^0(E)$ como los divisores en E tal que su grado es cero, que es trivialmente un subgrupo de $\operatorname{Div}(E)$.

Uno de los objetivos de esta sección es estudiar cuáles divisores son principales, o sea ver qué ceros y polos una función racional puede tener. Esto es equivalente a estudiar qué divisores no son principales. Esos divisores están representados por el grupo

$$\operatorname{Pic}(E) = \operatorname{Div}(E)/\operatorname{Prin}(E)$$

$\operatorname{Pic}(E)$ es llamado el *grupo de Picard*. En realidad podemos investigar un grupo más pequeño para estudiar qué divisores son principales. El teorema 1.3.3 implica que $\operatorname{Prin}(E) \subset \operatorname{Div}^0(E)$, por lo que podemos estudiar los divisores de grado cero que no son principales, o sea el grupo

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

que llamamos *parte de grado cero del grupo de Picard*.

Vamos a probar que $\operatorname{Pic}^0(E)$ está en correspondencia biunívoca con los puntos de E. Necesitaremos las siguientes definiciones.

Definición 1.4.6. Si $\Delta = \sum_{P \in E} m(P)\langle P \rangle$ es un divisor, su *norma* es:

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

Observación 1.4.2. Un divisor de norma uno es de la forma $\pm\langle P \rangle + n\langle \mathcal{O} \rangle$ con $n \in \mathbb{Z}$. Además si $\Delta = \text{div}(f)$ con f un polinomio en E, $|\Delta|$ es la suma de las multiplicidades de los ceros de f, que es el grado de f.

Definición 1.4.7. Una *recta* en $E(K)$ es un polinomio de la forma

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

con α, β, $\gamma \in K$ y α, β no simultáneamente nulos.

Si un punto P es cero de una recta ℓ, decimos que ℓ es una recta que pasa por P, y que P está en ℓ.

Lema 1.4.3. *Si ℓ es una recta con divisor Δ, luego $|\Delta| = 2$ o 3.*

Demostración: El polinomio ℓ tiene grado 2 si $\beta = 0$ o 3 si $\beta \neq 0$. Entonces, por el lema 1.3.4, la suma de las multiplicidades de los ceros de ℓ es 2 o 3, y esta suma es exactamente $|\Delta|$. □

Proposición 1.4.4. *Los posibles divisores de una recta ℓ son los siguientes:*

i. $\text{div}(\ell) = \langle P \rangle + \langle Q \rangle + \langle R \rangle - 3\langle \mathcal{O} \rangle$.

ii. $\text{div}(\ell) = 2\langle P \rangle + \langle Q \rangle - 3\langle \mathcal{O} \rangle$.

iii. $\text{div}(\ell) = 3\langle P \rangle - 3\langle \mathcal{O} \rangle$.

iv. $\text{div}(\ell) = \langle P \rangle + \langle Q \rangle - 2\langle \mathcal{O} \rangle$.

v. $\text{div}(\ell) = 2\langle P \rangle - 2\langle \mathcal{O} \rangle$.

donde P, Q y R son puntos diferentes de E.

Demostración: Supongamos que $\ell(x, y) = \alpha x + \beta y + \gamma$ con α, β, $\gamma \in K$, si $l(x, y) = 0$

$$\begin{aligned} (-\beta y)^2 &= (\alpha x + \gamma)^2 \\ \beta^2 y^2 &= \alpha^2 x^2 + 2\alpha\gamma x + \gamma^2 \\ \beta^2(x^3 + Ax + B) &= \alpha^2 x^2 + 2\alpha\gamma x + \gamma^2 \end{aligned}$$

Por lo que $f(x) = \beta x^3 - \alpha^2 x^2 + (\beta A - 2\alpha\gamma)x + \beta B - \gamma^2 = 0$. Si $\beta \neq 0$, entonces f es un polinomio de grado tres, por lo que debe de tener tres raíces.

- Si tiene tres raíces diferentes es el caso *i.*, ya que ℓ tendrá tres raíces diferentes.

- Si tiene una raíz doble y otra simple es el caso *ii.*.
- Si tiene una raíz triple es el caso *iii.*
- Falta ver qué pasa cuando $\beta = 0$, en ese caso f será un polinomio de grado dos, por lo que tenemos las opciones de que tenga dos raíces simples o una doble que corresponden a los casos *iv.* y *v.* respectivamente.

□

Ejemplo 1.4.2. Daremos ejemplos de los casos de la Proposición 1.4.4. Sea E la curva dada por la ecuación

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

y $K = \mathbb{C}$.

i. Si $\ell(x, y) = 2x - y + 1$ entonces $\operatorname{div}(\ell) = \langle(0, 1)\rangle + \langle(-1, -1)\rangle + \langle(5, 11)\rangle - 3\mathcal{O}$.

ii. Si $\ell(x, y) = x - y$ entonces $\operatorname{div}(\ell) = 2\langle(1, 1)\rangle + \langle(-1, -1)\rangle - 3\mathcal{O}$.

iii. Si $\ell(x, y) = -x/2 - y + 1$ entonces $\operatorname{div}(\ell) = 3\langle(0, 1)\rangle - 3\mathcal{O}$.

iv. Si $\ell(x, y) = x$ entonces $\operatorname{div}(\ell) = \langle(0, 1)\rangle + \langle(0, -1)\rangle - 2\mathcal{O}$.

v. Si $\ell(x, y) = x - x_0$, con $x_0 = -\frac{\sqrt[3]{108-12\sqrt{69}}}{6} - \frac{\sqrt[3]{108+12\sqrt{69}}}{6}$ entonces $\operatorname{div}(\ell) = 2\langle(x_0, 0)\rangle - 2\mathcal{O}$.

Teorema 1.4.5 (Reducción Lineal)**.** *Sea* $\Delta \in \operatorname{Div}(E)$*, entonces existe* $\tilde{\Delta} \in \operatorname{Div}(E)$ *tal que* $\Delta \sim \tilde{\Delta}$*,* $\operatorname{gr}(\Delta) = \operatorname{gr}(\tilde{\Delta})$ *y* $|\tilde{\Delta}| \leq 1$

Demostración: Supongamos que $\Delta = \sum_{P \in E} n(P)\langle P\rangle$ y Q, $R \in E(K)$ tal que $n(Q)$ y $n(R)$ tienen el mismo signo y son no nulos. Sea ℓ la recta que pasa por Q y R. Dependiendo del signo de $n(Q)$, $\Delta + \operatorname{div}(\ell)$ o $\Delta - \operatorname{div}(\ell)$ tendrá $|n(Q)|$ y $|n(R)|$ reducidos una unidad si ℓ tiene tres raíces diferentes. Por la Proposición 1.4.4 habremos, como mucho, aumentado en uno el coeficiente de otro punto.

Si ℓ tiene sólo dos raíces diferentes, habremos reducido en uno $|n(Q)|$ o $|n(R)|$ sin aumentar ningún otro coeficiente. Entonces, obtenemos un divisor Δ_1 tal que $\Delta_1 \sim \Delta$, $\operatorname{gr}(\Delta_1) = \operatorname{gr}(\Delta)$, ya que $\operatorname{gr}(\ell) = 0$, y $|\Delta_1| < |\Delta|$.

Luego de hacer esta reducción lineal una cantidad finita de veces, obtenemos un divisor Δ' linealmente equivalente a Δ de igual grado tal que

$$\Delta' = n_1\langle P\rangle - n_2\langle Q\rangle + n\langle\mathcal{O}\rangle$$

donde n_1 y n_2 son enteros no negativos y n entero.

Supongamos que $n_1 > 1$. Consideremos la recta

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

con $P = (a, b)$. P está en ℓ si a es cero del siguiente polinomio

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

ya que P tiene que cumplir la ecuaciones de la recta y de la curva elíptica. Calculando $f'(a)$ vemos que P tiene multiplicidad dos si

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

Cuando $b \neq 0$, la recta tiene divisor $2\langle P\rangle + \langle S\rangle - 3\langle\mathcal{O}\rangle$. Entonces substrayéndolo podemos reducir $|\Delta'|$, pero como introducimos $\langle S\rangle$ debemos aplicar el primer método de vuelta.

Si P es un punto de orden dos, la recta $\ell(x, y) = x - \omega$ tiene divisor $2\langle P\rangle - 2\langle\mathcal{O}\rangle$ y substrayéndolo podemos reducir n_1. De la misma manera podemos reducir n_2.

Luego de aplicar los dos métodos anteriores, si no terminamos, llegamos a:

$$\langle P\rangle - \langle Q\rangle + n\langle\mathcal{O}\rangle$$

La recta $\ell(x, y) = x - a$ tiene divisor $\langle P\rangle + \langle R\rangle - 2\langle\mathcal{O}\rangle$ o $2\langle P\rangle - 2\langle\mathcal{O}\rangle$ y substrayéndolo podemos aplicar el primer método y obtendríamos el resultado buscado. □

Corolario 1.4.6. *Para cada $\Delta \in \mathrm{Div}^0(E)$, existe un único punto $P \in E$ tal que*

$$\Delta \sim \langle P\rangle - \langle\mathcal{O}\rangle$$

Demostración: El Teorema 1.4.5 nos dice que Δ es equivalente a un divisor de norma 1, o sea un divisor de la forma $\pm\langle P\rangle + n\langle\mathcal{O}\rangle$.

Si el signo del coeficiente de P es -1 entonces substrayéndole la recta con divisor $\langle P\rangle + \langle Q\rangle - 2\langle\mathcal{O}\rangle$, podemos cambiar el signo. Como $\mathrm{gr}(\Delta) = 0$ vemos que el coeficiente de $\mathcal{O}$ tiene que ser -1, entonces sólo nos falta probar que P es único. Supongamos que $\Delta \sim \langle Q\rangle - \langle\mathcal{O}\rangle$ también. Entonces $\langle Q\rangle \sim \Delta + \langle\mathcal{O}\rangle \sim \langle P\rangle$, por lo que debería de haber una función racional r tal que $\mathrm{div}(r) = \langle P\rangle - \langle Q\rangle$.

Usando los métodos de la prueba del Teorema anterior vemos que existe una función racional t con divisor $\langle R\rangle - \langle\mathcal{O}\rangle$ para algún $R \in E$. Claramente t no tiene polos finitos, por lo que por el Lema 1.3.7 t debe de ser un polinomio. Entonces t sería un polinomio con un solo cero y además simple, lo que contradice el Lema 1.3.5, por lo que $P = Q$. □

Definamos un mapa $\bar{\sigma} : \mathrm{Div}^0(E) \to E$ como $\bar{\sigma}(\Delta) = P$ donde P es el único punto P tal que $\Delta \sim \langle P\rangle - \langle\mathcal{O}\rangle$. $\bar{\sigma}$ induce un mapa

$$\sigma : \mathrm{Pic}^0(E) \to E$$

de la siguiente manera, $\sigma(\Delta + \mathrm{Prin}(E)) = \bar{\sigma}(\Delta)$ donde $\Delta \in \mathrm{Div}^0(E)$.

Corolario 1.4.7. *El mapa σ es una biyección.*

Demostración: σ es sobreyectiva porque

$$\sigma((\langle P\rangle - \langle\mathcal{O}\rangle) + \mathrm{Prin}(E)) = P$$

Es inyectiva porque si $\sigma(\Delta+\text{Prin}(E)) = \sigma(\Delta'+\text{Prin}(E))$ con $\Delta \sim \langle P\rangle - \langle\mathcal{O}\rangle$ y $\Delta' \sim \langle P'\rangle - \langle\mathcal{O}\rangle$, entonces $\bar{\sigma}(\Delta + \text{div}(r)) = \bar{\sigma}(\Delta' + \text{div}(r'))$, con r y r' funciones racionales. Como $\text{div}(r) \sim \mathcal{O}$ para cualquier función racional r, tenemos que $P = \bar{\sigma}(\Delta+\text{div}(r)) = \bar{\sigma}(\Delta'+\text{div}(r')) = P'$, entonces $\Delta+\text{Prin}(E) = \Delta'+\text{Prin}(E)$. □

1.5. La Ley de Grupo

Daremos ahora una estructura de grupo abeliano al conjunto de los puntos K-racionales de una curva elíptica.

Hay varias maneras de hacer esto. Daremos la definición en su formulación algebraica, que tiene dos desventajas: no es clara su motivación y la demostración de la asociatividad es muy complicada. Otro enfoque es el geométrico en el cual es más obvia la motivación pero la asociatividad sigue siendo complicada. Por lo que usaremos el enfoque geométrico como motivación, la definición algebraica y usaremos los divisores tratados en la sección anterior para demostrar la asociatividad.

La idea detrás de la suma en una curva elíptica es que una recta no cortará más de tres veces la curva. Describimos escuetamente cómo funciona antes de dar la definición formal.

Primero, definimos a $\mathcal{O}$ como la identidad o cero del grupo y lo identificamos con la dirección vertical. Luego, si el punto $P \in E(k)$ es tal que $P = (a, b)$ definimos $-P = (a, -b)$. Finalmente si P, Q y R están en una misma recta, definimos la suma como para que se cumpla que $P + Q + R = \mathcal{O}$. En la figura 1.3 mostramos como sumar en una curva elíptica.

Supongamos que tenemos que $P \neq Q, -Q$ y sea la recta ℓ que pasa por P y Q, y R el tercer punto de corte que es fácil de verificar que es finito. Escribimos $P = (a, b)$ y $Q = (c, d)$ tal que ℓ se puede escribir como

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

donde $m = \frac{d-b}{c-a}$. Ya hemos visto que, como (a, b) es raíz de ℓ y está en la curva, tenemos que a es raíz del polinomio

$$f(x) = [m(x - a) + b]^2 - x^3 - Ax - B \tag{1.8}$$

Es trivial verificar que a y c son raíces de f. Sea e su tercer raíz. Escribiendo

$$f(x) = (x - a)(x - c)(x - e)$$

vemos que el coeficiente en x^2 de f es $a+c+e$. Usando la ecuación (1.8), vemos que el coeficiente en x^2 es m^2, por lo que $m^2 = a + c + e$ o $e = m^2 - a - c$. Para conseguir la coordenada en y de R, simplemente introducimos m^2 en la ecuación de la recta y despejamos, por lo que $R = (m^2 - a - c, m(e - a) + b)$.

Si $P = Q$, entonces usamos la recta tangente a P, o sea la recta con doble cero en P. Vimos que esa recta tiene la ecuación usual con $m = \frac{3a^2+A}{2b}$.

Resumiendo, para sumar dos puntos finitos diferentes que no son opuestos intersectamos la recta que pasa por ellos con la curva y luego simetrizamos con respecto al eje de las x. Si los puntos a sumar son iguales, usamos la recta tangente para conseguir el punto a simetrizar.

Definición 1.5.1. Sea E una curva elíptica sobre el cuerpo k. Definimos

$$+ : E(k) \times E(k) \to E(k)$$

de la siguiente manera:

- $\mathcal{O} + P = P + \mathcal{O} = P$ para todo $P \in E(k)$.
- Si $P = (a, b)$ definimos $-P = (a, -b)$ y $P + (-P) = (-P) + P = \mathcal{O}$.
- Supongamos ahora que P_1 y P_2 no son $\mathcal{O}$, y que $P_1 \neq -P_2$. Si $P_1 = (a_1, b_1)$ y $P_2 = (a_2, b_2)$. Si $a_1 \neq a_2$ (entonces $P_1 \neq P_2$), definimos

  $$\lambda = \frac{b_2 - b_1}{a_2 - a_1}$$

  mientras que si $a_1 = a_2$ (por lo que $P_1 = P_2$, ya que habíamos asumido que $P_1 \neq -P_2$), definimos

  $$\lambda = \frac{3a_1^2 + A}{2b_1}$$

  Definimos $P_1 + P_2 = P_3 = (a_3, b_3)$ por

  $$a_3 = -a_1 - a_2 + \lambda^2$$

  y

  $$b_3 = -b_1 - \lambda(a_3 - a_1)$$

Llamaremos la fórmula de la suma en el caso $P_1 \neq P_2, -P_2, \mathcal{O}$ (o sea $\lambda = (b_2 - b_1)/(a_2 - a_1)$ la fórmula *general* de la suma ya que es la que mas se usa para casi todos los pares de puntos.

Observación 1.5.1. Si P y Q son puntos no ambos $\mathcal{O}$, entonces podemos encontrar una recta ℓ tal que su divisor es

$$\langle P \rangle + \langle Q \rangle + \langle R \rangle - 3\langle \mathcal{O} \rangle$$

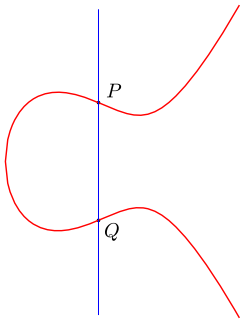
entonces R es $-P - Q$. Lo anterior es cierto aunque $Q = \pm P$ o $\mathcal{O}$.

Teorema 1.5.1. *Una curva elíptica con la suma definida en 1.5.1 es un grupo abeliano.*

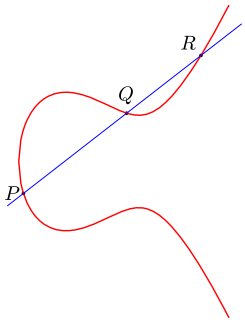
Todos los axiomas de grupo son triviales de demostrar menos la asociatividad, que se desprenderá de la siguiente proposición.

Recodemos la biyección

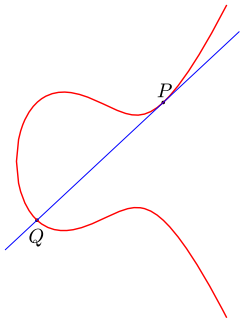
$$\sigma : \mathrm{Pic}^0 \to E(K)$$



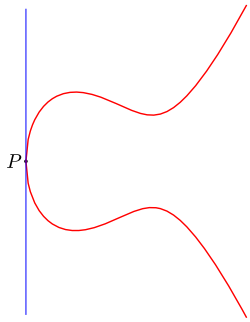
(a) $P + Q + \mathcal{O} = \mathcal{O}$



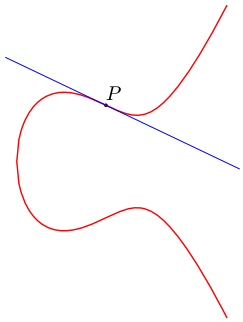
(b) $P + Q + R = \mathcal{O}$



(c) $P + P + Q = \mathcal{O}$



(d) $P + P + \mathcal{O} = \mathcal{O}$



(e) $P + P + P = \mathcal{O}$

Figura 1.3: Suma en una curva elíptica.

definida en la sección anterior, cuando K es algebraicamente cerrado. Denotemos $\kappa = \sigma^{-1}$, entonces $\kappa(P)$ es la clase lineal de equivalencia del divisor $\langle P\rangle - \langle\mathcal{O}\rangle$, o sea

$$\kappa(P) = \langle P\rangle - \langle\mathcal{O}\rangle + \mathrm{Prin}(E)$$

Claramente $\kappa(\mathcal{O})$ es la clase lineal de equivalencia nula.

Proposición 1.5.2. $\kappa(P+Q) = \kappa(P) + \kappa(Q)$

Demostración: El resultado es trivial si $P = Q = \mathcal{O}$, por lo que asumimos que P y Q no son ambos $\mathcal{O}$. Sea ℓ la recta que pasa por P y Q. Como observamos en 1.5.1 el divisor de la recta ℓ lo podemos escribir como

$$\mathrm{div}(\ell) = \langle P\rangle + \langle Q\rangle + \langle R\rangle - 3\langle\mathcal{O}\rangle$$

Sea ℓ' la recta que pasa por R y $-R$, entonces

$$\mathrm{div}(\ell') = \langle R\rangle + \langle -R\rangle - 2\langle\mathcal{O}\rangle$$

Hemos visto que $R = -P - Q$, $-R = P + Q$ y

$$\mathrm{div}(\ell'/\ell) = \mathrm{div}(\ell') - \mathrm{div}(\ell) = \langle P+Q\rangle - \langle P\rangle - \langle Q\rangle + \langle\mathcal{O}\rangle \sim 0$$

ya que ℓ'/ℓ es una función racional. Reescribiendo llegamos a que

$$(\langle P+Q\rangle - \langle\mathcal{O}\rangle) - (\langle P\rangle - \langle\mathcal{O}\rangle) - (\langle Q\rangle - \langle\mathcal{O}\rangle) \sim 0$$

que es lo mismo que $\kappa(P+Q) - \kappa(P) - \kappa(Q) = 0$. □

Corolario 1.5.3. *La suma en una curva elíptica es asociativa.*

Demostración: Esto se debe a que $E(K)$ es isomorfo como grupo a Pic^0, cuando K es algebraicamente cerrado, que es claramente asociativo.

Si K no es algebraicamente cerrado, vemos que $E(K)$ es un subgrupo de $E(\bar{K})$, donde $\bar{K}$ es la clausura algebraica de K. □

Hemos probado que κ es un homomorfismo de grupos, por lo que claramente σ también lo es. Como $\bar{\sigma}$ es la composición de σ con la proyección de $\mathrm{Div}^0(E)$ a $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E)$, es también un homomorfismo. Hay una manera mas simple de ver a $\bar{\sigma}$.

Definición 1.5.2. Definimos el mapa *suma* de $\mathrm{Div}(E)$ en $E(K)$ como

$$\mathrm{suma}\left(\sum_{P\in E(K)} n(P)\langle P\rangle\right) = \sum_{P\in E(K)} n(P)P$$

Proposición 1.5.4. *La función $\bar{\sigma}$ es la restricción de* suma *a* $\mathrm{Div}^0(E)$*, o sea*

$$\bar{\sigma} = \mathrm{suma}\,|_{\mathrm{Div}^0(E)}$$

Demostración: Sea $\Delta \in \mathrm{Div}^0(E)$, por la demostración del Teorema 1.4.5 y el Corolario 1.4.6

$$\Delta = \langle P \rangle - \langle \mathcal{O} \rangle + \sum_{i=1}^{m} \mathrm{div}(\ell_i)$$

donde ℓ_i son rectas y $P \in E(K)$. Es inmediato que la función suma es aditiva por lo que

$$\begin{aligned} \mathrm{suma}(\Delta) &= \mathrm{suma}(\langle P \rangle) - \mathrm{suma}(\langle \mathcal{O} \rangle) + \sum_{i=1}^{m} \mathrm{suma}(\mathrm{div}(\ell_i)) \\ &= P - \mathcal{O} + \sum_{i=1}^{m} \mathcal{O} \\ &= P \end{aligned}$$

ya que $\mathrm{suma}(\mathrm{div}(\ell_i)) = \mathcal{O}$ por la definición de la ley de grupo. □

Proposición 1.5.5. *Sea* $\Delta = \sum_{P \in E(K)} n(P)\langle P \rangle$ *un divisor con* K *algebraicamente cerrado. Entonces* Δ *es principal si y solo si* $\mathrm{gr}(\Delta) = \sum_{P \in E(K)} n(P) = 0$ *y* $\mathrm{suma}(\Delta) = \sum_{P \in E(K)} n(P)P = \mathcal{O}$.

Demostración: Ya hemos probado que si Δ es principal entonces $\mathrm{gr}(\Delta) = 0$. Supongamos entonces que $\mathrm{gr}(\Delta) = 0$. Recordemos que $\Delta \sim \langle P \rangle - \langle \mathcal{O} \rangle$ para un único $P \in E(K)$. Luego Δ es principal $\Leftrightarrow$ $\Delta \sim 0 \Leftrightarrow \langle P \rangle - \langle \mathcal{O} \rangle \sim 0 \Leftrightarrow \mathrm{suma}(\Delta) = \mathcal{O}$. □

1.6. Multiplicación por n

Estamos interesados en la función $[n] : P \to n \cdot P$, el punto P sumado a si mismo n veces. Mas particularmente en las funciones $g_n(P) = x(n \cdot P)$ y $h_n(P) = y(n \cdot P)$, o sea

$$n \cdot P = (g_n(P), h_n(P))$$

El próximo teorema es una demostración de que la suma es racional. Cuando escribimos la suma de dos mapas racionales nos referimos a la suma en la curva elíptica E definida sobre $K(E)$, definido en 1.3.2. Recordemos también que $\mathcal{O}_M$ es el mapa racional constante $\mathcal{O}$, que es la identidad de $E(K(E))$.

En esta sección asumimos que K es algebraicamente cerrado.

Teorema 1.6.1. *Sean* F *y* G *mapas racionales en* E. *Si* $L = F + G$ *entonces* $L(P) = F(P) + G(P)$ *para todo* P *en* $E(K)$.

Demostración: La no trivialidad del teorema radica en que aunque F no es $G, -G$, o $\mathcal{O}_M$, $F(P)$ puede ser $G(P), -G(P)$, o $\mathcal{O}$.

Si F, G o $F+G$ son $\mathcal{O}_M$ entonces el resultado es trivial, por lo que suponemos excluidos esos casos.

Supongamos que $F = (r, s)$ y $G = (t, v)$. Hay dos casos de estudio, cuando $r \neq t$ y cuando $r = t$. Supongamos que $L = (w, z)$ entonces

$$w = -(t + r) + \lambda^2 \tag{1.9}$$

y

$$z = -v - \lambda(w - t) \tag{1.10}$$

donde en el primer caso

$$\lambda = \frac{s - v}{r - t} \tag{1.11}$$

y en el segundo

$$\lambda = \frac{3r^2 + A}{2s} \tag{1.12}$$

I. Asumamos que estamos en el caso que λ es como en (1.11).

A. Si $r(P)$ y $t(P)$ son finitos y diferentes, $L(P) = F(P) + G(P)$ es simplemente la formula genérica de la suma en una curva elíptica.

B. Si $r(P) = t(P)$ y son finitos, puede pasar $s(P) = -v(P)$, o $s(P) = v(P)$.

1. Si $s(P) = -v(P)$ y son finitos tenemos que $F(P) = -G(P)$. Vemos entonces que λ tiene un polo en P, por lo que se cumple la tesis ya que

$$F(P) + G(P) = F(P) + (-F(P)) = \mathcal{O}$$

y $L(P) = \mathcal{O}$.

2. Si $s(P) = v(P)$, sabemos que son finitos, las formulas de $F(P) + G(P)$ y $L(P)$ solo difieren en la definición de λ. Como $v \neq -s$, porque $r \neq t$, tenemos que

$$\begin{aligned} \lambda &= \frac{v - s}{t - r} \cdot \frac{v + s}{v + s} \\ &= \frac{[t^3 - r^3] - A(t - r)}{(t - r)(v + s} \\ &= \frac{t^2 + rt + r^2 + A}{s + v} \end{aligned}$$

En el caso en que $r(P) = t(P)$ y $s(P) = v(P) \neq 0$, resulta que

$$\lambda(P) = \frac{3r(P)^2 + A}{2s(P)}$$

que es justamente el λ de la formula de duplicación y es justo lo que precisamos para que $F(P) + G(P) = 2F(P) = L(P)$ ya que $F(P) = G(P)$.
Si $s(P) = v(P) = 0$, estamos en un punto $F(P)$ de orden dos. Vemos de la expresión de λ que tiene un polo en P por lo que las componentes de $L(P)$ son no finitas. Pero esto es lo que precisamos ya que $F(P) = G(P)$ es un punto de orden dos y $F(P) + G(P) = \mathcal{O} = L(P)$.

C. Pasamos a estudiar el caso en que solo uno de los dos puntos es $\mathcal{O}$, digamos que es $F(P)$.

En este caso tenemos que $r = r_1/u^d$ y $s = s_1/u^e$, donde u es una variable de uniformización en P, r_1,s_1 son funciones racionales finitas

y no nulas en P y d, e son enteros positivos. Como $s^2 = r^3 + Ar + B$, se desprende que $2e = 3d$, ya que $2d = \mathrm{gr}(s^2) = \mathrm{gr}(r^3 + Ar + B) = 3d$ y $s_1^2(P) = r_1^3(P)$. La ultima afirmación se debe a que

$$\frac{s_1^2}{r_1^3} = 1 + \frac{Au^{2e}r_1 + Bu^{3e}}{r_1}$$

y también recordando que $u(P) = 0$. Usando las ecuaciones (1.9), (1.10) y (1.11), calculamos w,

$$\begin{aligned}
w &= -(t+r) + \left(\frac{s-v}{r-t}\right)^2 \\
&= \frac{-(r^3 - t^2r - tr^2 + t^3) + (s^2 - 2vs + v^2)}{(r-t)^2} \\
&= \frac{-r^3 + t^2r + tr^2 - t^3 + (r^3 + Ar + B) - 2vs + v^2}{(r-t)^2} \\
&= \frac{tr^2 + (t^2 + A)r + (v^2 - t^3 + B - 2vs)}{r^2 - 2rt + t^2} \\
&= \frac{tr_1^2u^{-2d} + (t^2 + A)r_1 + u^{-d}(v^2 - t^3 + B - 2vs_1u^{-e})}{r_1^2u^{-2d} - 2r_1u^{-d}t + t^2} \\
&= \frac{tr_1^2 + u^dR_1 - 2vu^{2d-e}s_1}{r_1^2 + u^dR_2}
\end{aligned}$$

donde $R_1 = (t^2 + A)r_1 + (v^2 - t^3 + B)u^d$ y $R_2 = u^dt^2 - 2tr_1$ son funciones racionales finitas en P. Como $2e = 3d$ tenemos que $2d - e > 0$ ya que $2d - e = \frac{1}{2}(4d - 2e) = \frac{1}{2}(4d - 3d) = \frac{d}{2} > 0$, y esto implica que $w(P) = t(P)$. Esto es lo que queremos ya que $F(P) + G(P) = G(P)$ cuando $F(P) = \mathcal{O}$.

Podríamos calcular la coordenada y de una manera similar pero vamos a evitarlo usando la asociatividad de la suma en la curva elíptica de mapas racionales.

Como $L = F + G$ sabemos que $L - G = F$. Por el calculo de la coordenada x arriba vemos que $L(P) \neq \mathcal{O}$, por lo que $(G - L)(P) = G(P) - L(P) = F(P) = \mathcal{O}$ basado en uno de los casos anteriores. Lo que demuestra que $G(P) = L(P)$.

D. El próximo caso a estudiar es cuando F y G tienen ambos el valor $\mathcal{O}$ en P.

Nuevamente podemos usar la asociatividad de la curva elíptica de mapas racionales. Como $L = F + G$, $(F + G) - L = \mathcal{O}_M$ y por la asociatividad $F + (G - L) = \mathcal{O}_M$. Supongamos que $L(P) = Q \neq \mathcal{O}$. Entonces como $G(P) = \mathcal{O}$, podemos ver $G(P) - L(P) = -Q$ por el caso anterior.

Similarmente vemos que $F(P) + (G - L)(P) = -Q$, pero $(F + (G - L))(P) = \mathcal{O}$ por lo que $L(P) = \mathcal{O}$ como necesitábamos.

II. Supongamos ahora que $r = t$.

Si $s = -v$, entonces $F = -G$, por lo que $L = \mathcal{O}_M$. Pero claramente $F(P) = -G(P)$, por lo que $F(P) + G(P) = \mathcal{O}$ para todo $P \in E(K)$.

Podemos asumir entonces que $s \neq -v$. Claramente, $s(P)$ puede ser igual a $-v(P)$ para algún P. Como $s \neq -v$, $F \neq -G$, consecuentemente podemos asumir que $F = G$.

Si $r(P)$ es finito, entonces $L(P) = F(P) + G(P)$ porque están igualmente definidas. En el caso que $r(P)$ no sea finito, observamos que la formula de duplicación implica

$$\begin{aligned} w &= -t - r + \frac{9r^4 + 6r^2A + A^2}{4s^2} \\ &= \frac{-8rs^2 + 9r^4 + 6r^A + A^2}{4s^2} \\ &= \frac{-8r^4 - 8r^2A - 8r^2B + 9r^4 + 6r^rA + A^2}{4s^2} \\ &= \frac{r^4 - (2A + 8B)r^2 + A^2}{4r^3 + 4Ar + 4B} \end{aligned}$$

por lo que w tiene un polo en P. Luego z tiene un polo en P, y podemos concluir que $L(P) = \mathcal{O} = \mathcal{O} + \mathcal{O} = F(P) + G(P)$.

□

Definición 1.6.1.

$$E(K)[n] = \{P \in E(K) : n \cdot P = \mathcal{O}\}$$

y escribimos $E[n]$ cuando es claro que usamos el cuerpo K.

Observemos que $\mathcal{O} \in E[n]$ para todo n, y además $E[n]$ es un subgrupo de $E(K)$. Los puntos de $E[n]$ los llamaremos puntos de *n-torsión* de E.

Recordar que g_n y h_n están definidas por $n \cdot P = (g_n(P), h_n(P))$.

Teorema 1.6.2. *g_n y h_n son funciones racionales en E con polos exactamente en los puntos de $E[n]$, y $E[n]$ es un conjunto finito.*

Demostración: La prueba es por inducción en n. Claramente las funciones $g_1(x, y) = x$ y $h_1(x, y) = y$ son racionales, ambas con un único polo en $\mathcal{O}$. Suponemos ahora que g_n y h_n son funciones racionales, $E[n]$ es finito, y g_n y h_n tienen sus polos exactamente en los puntos de $E[n]$ para $n < q$.

La idea de la inducción es usar

$$qP = P + (q - 1)P \tag{1.13}$$

Por inducción podemos asumir que g_{q-1} y h_{q-1}, las componentes de $(q-1)P$, son funciones racionales. Nuestro resultado entonces se debe al teorema anterior si sabemos que $P \to qP$ no es el mapa racional $\mathcal{O}_M$, o sea, si sabemos que $(q - 1)P \neq -P$ para algún P. Pero $(q - 1)P = -P$ para todo P implica que $E[q] = E(K)$.

Supongamos que $E[q] = E(K)$ y $k > 1$ divide a q, y escribimos $q/k = l$. Luego $E[k]$ es un subgrupo de $E[q]$, y si $P \in E[q]$, $lP \in E[k]$ y $kP \in E[l]$, por

lo tanto si $E[q]$ tiene cardinal infinito $E[k]$ y $E[l]$ también. Pero como k y l son menores que q entonces $E[k]$ y $E[l]$ son finitos, por lo que si q tiene un divisor no trivial $E[q]$ es finito.

Asumimos que q es primo. Observemos que $E[2]$ es finito porque solo hay cuatro puntos P con $2P = \mathcal{O}$, que son los puntos de orden dos y $\mathcal{O}$. Además $E[q] = E(K)$ implica que $E[2] \subset E[q]$ por lo que q es par. Como q es primo deducimos que $q = 2$, que contradice la afirmación de que $E[q]$ es infinito. Entonces $E[q] \neq E(K)$ y (g_q, h_q) no es el mapa $\mathcal{O}_M$, por lo que $E[q]$ es finito porque es el conjunto de polos de una función racional. □

Corolario 1.6.3. *La función racional $g_n - x$ no es idénticamente nula para $n > 1$.*

Demostración: Si $(g_n - x)(P) = 0$ para todo $P \in E(K)$ tendríamos que $n \cdot P = \pm P$, o $(n \pm 1) \cdot P = \mathcal{O}$ para todo P. Entonces tendríamos que $E[n-1]$ o $E[n+1]$ tendría infinitos elementos, contradiciendo el teorema anterior. □

Escribimos las formulas de g_2 y h_2 ya que nos van a ser de utilidad. Recordando que $s(x) = x^3 + Ax + B$, tenemos

$$g_2(P) = x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4s(x)} \tag{1.14}$$

$$h_2(P) = y(2P) = y \cdot \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3}{8s(x)^2} \tag{1.15}$$

Proposición 1.6.4. *Existen funciones $\tilde{g}_n$ y $\tilde{h}_n$ racionales en x, con la propiedad $g_n(P) = \tilde{g}_n(x(P))$ y $h_n(P) = y(P)\tilde{h}_n(x(P))$*

Demostración: Sea el mapa racional $F(P) = nP$, $F = (g_n, h_n)$. Es claro que $F(-P) = (-F)(P)$.

Si $g_n(x, y) = a(x) + yb(x)$, $h_n(x, y) = c(x) + yd(x)$, con a, c, d, c funciones racionales en x, tenemos

$$\begin{aligned} (g_n(x,-y), h_n(x,-y)) &= (g_n(x,y), -h_n(x,y)) \\ (a(x) - yb(x), c(x) - yd(x)) &= (a(x) + yb(x), -c(x) - yd(x)) \end{aligned}$$

Luego $g_n(x, y) = a(x)$ y $h_n(x, y) = yd(x)$. □

Sea p la característica de K. Decimos que dos enteros no nulos son coprimos si no tienen factores primos en común. También decimos que dos enteros con alguno de ellos 0 son coprimos si el otro es no nulo.

Proposición 1.6.5. *Si n y p son coprimos entonces*

$$\frac{g_n}{x}(\mathcal{O}) = \frac{1}{n^2}$$

y

$$\frac{h_n}{y}(\mathcal{O}) = \frac{1}{n^3}$$

Demostración: La prueba es por inducción en n. Primero asumamos que $n < p$. Nuestro resultado es claramente cierto si $n = 2$ por las ecuaciones (1.14) y (1.15).

Usando la ecuación $nP = (n-1)P + P$ y como por el Corolario 1.6.3 $g_n - x$ no es idénticamente nula, por la formula de suma en la curva elíptica de mapas racionales obtenemos

$$g_n = -g_{n-1} - x + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2$$

$$h_n = -h_{n-1} - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right) \cdot (g_n - g_{n-1})$$

Dividiendo las ecuaciones por x e y respectivamente obtenemos

$$\frac{g_n}{x} = -\frac{g_{n-1}}{x} - 1 + \frac{y^2}{x^3} \cdot \left(\frac{\frac{h_{n-1}}{y} - 1}{\frac{g_{n-1}}{x} - 1}\right)^2 \tag{1.16}$$

$$\frac{h_n}{y} = -\frac{h_{n-1}}{y} - \left(\frac{\frac{h_{n-1}}{y} - 1}{\frac{g_{n-1}}{x} - 1}\right) \cdot (g_n - g_{n-1}) \tag{1.17}$$

Evaluando (1.16) y (1.17) en $\mathcal{O}$, usando la hipotesis de inducción y suponiendo que $m = n - 1$

$$\begin{aligned}
\frac{g_n}{x}(\mathcal{O}) &= -\frac{1}{m^2} - 1 + \left(\frac{\frac{1}{m^3} - 1}{\frac{1}{m^2} - 1}\right)^2 = -\frac{1}{m^2} - 1 + \left(\frac{1 - m^3}{m - m^3}\right)^2 \\
&= -\frac{1}{m^2} - 1 + \left(\frac{1 + m + m^2}{m + m^2}\right)^2 = -\frac{1}{m^2} - 1 + \left(\frac{1}{m + m^2} + 1\right)^2 \\
&= -\frac{1}{m^2} - 1 + \frac{1}{m^2(m+1)^2} + \frac{2}{m(m+1)} + 1 \\
&= \frac{2m^2 + 2m - m^2 - 2m - 1 + 1}{m^2(m+1)^2} = \frac{m^2}{m^2(m+1)^2} \\
&= \frac{1}{n^2}
\end{aligned}$$

$$\begin{aligned}
\frac{h_n}{y}(\mathcal{O}) &= -\frac{1}{m^3} - \left(\frac{\frac{1}{m^3} - 1}{\frac{1}{m^2} - 1}\right) \cdot \left(\frac{1}{(m+1)^2} - \frac{1}{m^2}\right) \\
&= -\frac{1}{m^3} + \left(\frac{1 + m + m^2}{m + m^2}\right)\left(\frac{2m+1}{m^2(m+1)^2}\right) \\
&= \frac{2m^3 + 3m^2 + 3m + 1 - (m+1)^3}{m^3(m+1)^3} = \frac{m^3}{m^3(m+1)^3} \\
&= \frac{1}{n^3}
\end{aligned}$$

De esta manera queda probado para todo $n < p$. Para probarlo para $n = p+1$ debemos utilizar un método parecido al anterior. Sabemos que

$$n \cdot P = 2 \cdot P + (n-2) \cdot P$$

por lo que

$$(g_n, h_n) = (g_{n-2}, h_{n-2}) + (g_2, h_2)$$

entonces si $n = kp + 1$ para algún $k \in \mathbb{Z}^+$ y $m = n - 2$

$$\begin{aligned}
\frac{g_n}{x}(\mathcal{O}) = &= -\frac{1}{m^2} - \frac{1}{4} + \left(\frac{\frac{1}{m^3} - \frac{1}{8}}{\frac{1}{m^2} - \frac{1}{4}}\right)^2 = -\frac{1}{m^2} - \frac{1}{4} + \left(\frac{8 - m^3}{8m - 2m^3}\right)^2 \\
&= -\frac{1}{m^2} - \frac{1}{4} + \left(\frac{4 + 2m + m^2}{4m + 2m^2}\right)^2 \\
&= -\frac{1}{m^2} - \frac{1}{4} + \left(\frac{2}{2m + m^2} + \frac{1}{2}\right)^2 \\
&= -\frac{1}{m^2} - \frac{1}{4} + \frac{2}{m^2(m+2)^2} + \frac{4}{m(m+2)} + \frac{1}{4} \\
&= \frac{m^2}{m^2(m+2)^2} \\
&= \frac{1}{n^2}
\end{aligned}$$

y de una manera similar se prueba que $\frac{h_n}{y}(\mathcal{O}) = \frac{1}{n^3}$. □

Corolario 1.6.6. *Si n y p son coprimos el coeficiente principal de g_n es $1/n^2$ y el de h_n es $1/n^3$.*

Demostración: El orden de g_n en $\mathcal{O}$ es -2 ya que

$$g_n = \left(\frac{x}{y}\right)^{-2} \frac{g_n}{x} \frac{x^3}{y^2}$$

y $\frac{g_n}{x}\frac{x^3}{y^2}$ es no nulo y finito en $\mathcal{O}$, además su valor es $1/n^2$ por la proposición anterior. Luego por definición el coeficiente principal de g_n es $1/n^2$.

De la misma manera se ve que el orden de h_n en $\mathcal{O}$ es -3 ya que

$$h_n = \left(\frac{x}{y}\right)^{-3} \frac{h_n}{y} \frac{x^3}{y^2}$$

y $\frac{h_n}{y}\frac{x^3}{y^2}$ tiene valor $1/n^3$ en $\mathcal{O}$, por lo que el coeficiente principal de h_n es $1/n^3$. □

1.7. El divisor de $g_m - g_n$

Queremos calcular el divisor de $g_m - g_n$ y encontrar una relación con los puntos de $E[k]$ para un k apropiado. Para poder calcular las multiplicidades de los ceros y los polos de $g_m - g_n$, debemos estudiar la noción de derivación. Queremos definir una derivación de una función racional cualquiera en E, pero debemos tener en cuenta que la derivación en el polinomio $y^2 - x^3 - Ax - B$ tiene que ser cero. Si tomamos formalmente una derivación, obtenemos

$$2yDy = (3x^2 + A)Dx$$

que nos induce a definir una derivación de la siguiente manera.

Definición 1.7.1. Dado un cuerpo k una *k-derivación* o mas simplemente *derivación* es un mapa lineal $d : k \to k$ que cumple la regla de Leibniz, o sea

$$d(ab) = d(a)b + ad(b)$$

para todo $a, b \in k$.

Definición 1.7.2. Definimos una derivación D en el cuerpo $K(E)$, de funciones racionales sobre E, de la siguiente manera: primero definimos D para x e y

$$D(x) = 2y$$

$$D(y) = 3x^2 + A$$

y finalmente para una función racional $a(x) + yb(x)$ cualquiera

$$D(a + yb) = D(a) + D(y)b + yD(b)$$

Proposición 1.7.1.

1. *D esta bien definida y es una derivación.*
2. *D cumple, si r y s son funciones racionales con s no nula,*

$$D\left(\frac{r}{s}\right) = \frac{D(r)s - rD(s)}{s^2}$$

3. $D(r^n) = nr^{n-1}D(r)$.
4. *Sea r una función racional tal que es finita en P entonces $D(r)$ también es finita en P.*

Demostración:

1. Esta bien definida porque la representacion de una función racional como $a(x) + yb(x)$ es única. Y es una derivación por la manera en que la definimos.
2. $$\begin{aligned} D\left(\frac{r}{s}\right) &= D\left(\frac{rs}{s^2}\right) = \frac{D(rs)}{s^2} + D\left(\frac{1}{s^2}\right)rs \\ &= \frac{D(r)s + D(s)r}{s^2} + \frac{2rsD\left(\frac{1}{s}\right)}{s} \\ &= \frac{2D(r)}{s} + 2rD\left(\frac{1}{s}\right) + \frac{-D(r)s + D(s)r}{s^2} \\ &= 2D\left(\frac{r}{s}\right) + \frac{-D(r)s + D(s)r}{s^2} \end{aligned}$$

   entonces $D\left(\frac{r}{s}\right) = \frac{D(r)s - rD(s)}{s^2}$.

3. Si $n = 1$ es claro. Si el resultado es cierto para $n-1$

$$\begin{aligned} D(r^n) &= D(r^{n-1})r + D(r)r^{n-1} \\ &= (n-1)r^{n-2}D(r)r + D(r)r^{n-1} \\ &= nr^{n-1}D(r) \end{aligned}$$

4. Si $P \neq \mathcal{O}$ y $r = f/g$ es finita en P, $g(P) \neq 0$. Luego

$$Dr = \frac{Dfg - fDg}{g^2}$$

y Dr es finita en P ya que $g^2(P) \neq 0$.

Si $P = \mathcal{O}$, podemos escribir

$$r = \frac{u + yv}{w + yz} = \frac{(u + yv)(w + yz)}{w^2 - sz^2}$$

donde u, v, w, z son funciones en x y $s(x) = x^3 + Ax + B$. Podemos suponer que $r = f/w$ donde f es un polinomio en x, y y w un polinomio en x y $\text{gr}(f) \leq \text{gr}(w)$. Si escribimos $f = u + yv$ con u, v polinomios en x y

$$\begin{aligned} u(x) &= a_n x^n + \cdots + a_1 x + a_0 \\ v(x) &= b_m x^m + \cdots + b_1 x + b_0 \\ w(x) &= c_k x^k + \cdots + c_1 x + c_0 \end{aligned}$$

sabemos que

$$\begin{aligned} Dr &= \frac{2yu_x w + s_x vw + 2yv_x w - 2yw_x u - 2sw_x v}{w^2} \\ &= \frac{(s_x vw - 2sw_x v) + y(2u_x w + 2v_x w - 2w_x u)}{w^2} \\ &= \frac{g}{w^2} \end{aligned}$$

donde u_x indica la derivada usual. Luego

$$\begin{aligned} \text{gr}(g) &= \text{máx}\{2\,\text{gr}_x(s_x vw - 2sw_x v), 3 + 2\,\text{gr}_x(2u_x w + 2v_x w - 2w_x u)\} \\ &= \text{máx}\{2\,\text{gr}_x((3b_m c_k - 2kc_k b_m)x^{m+k+2} + l(x)), \\ &\quad 3 + 2\,\text{gr}_x((2na_n c_k - 2ka_n c_k)x^{n+k-1} + d(x) + 2mb_m c_k x^{k+m-1} + e(x))\} \end{aligned}$$

donde $\text{gr}_x(l) < m + k + 2$, $\text{gr}_x(d) < n + k - 1$, $\text{gr}_x(e) < k + m - 1$.

Sabemos que $n \leq k$ y que $3 + 2m < 2k$, la ultima desigualdad se debe a que uno es impar y el otro par. Si el grado de g es par

$$\text{gr}(g) = 2m + 2k + 4 \leq 4k = \text{gr}(w^2)$$

y Dr es finita en $\mathcal{O}$. Si $\text{gr}(g)$ es impar y $n = k$

$$\text{gr}(g) \leq \text{máx}\{4k - 1, 2k + 2m - 1\}$$

porque $(2na_n c_k - 2ka_n c_k) = 0$, y claramente es menor que $4k$. Si $n < k$ se cumple también que $\text{gr}(g) \leq \text{gr}(w^2)$ por lo que también Dr será finita en $\mathcal{O}$.

□

Proposición 1.7.2. *Sea r una función racional. Si $\mathrm{ord}_P(r) = d \neq 0$ es coprimo con p, entonces $\mathrm{ord}_P(Dr) = d - 1$.*

Demostración: Sea u una variable uniformizadora en P, y $r = u^d r_1$ donde $r_1(P)$ finito y no cero. Entonces

$$Dr = du^{d-1}Dur_1 + u^d Dr_1$$

Si probamos que Du es finito y no nulo en P, $Dr = u^{d-1}r_2$ con r_2 finita y no nula en P, ya que Dr_1 es finita en P.

Si P no es $\mathcal{O}$ ni de orden 2, $u(x, y) = x - x(P)$, por lo que $Du = 2y$, que es finita y no nula en P.

Si P es de orden 2, tomamos $u = y$, y $Du = 3x^2 + A$. Como E es elíptica, sabemos que la derivada de $f(x) = x^3 + Ax + B$ es no nula en los ceros de f. Como $f_x(x) = 3x^2 + A$ y $y(P) = \omega$, cero de f. Entonces Du es finita y no nula en P si es de orden 2.

Si $P = \mathcal{O}$, tomamos $u = x/y$, y

$$Du = d(x/y) = \frac{2y^2 - 3x^3 - Ax}{y^2} = \frac{-y^2 + 2Ax + 3B}{y^2}$$

que es -1 en $\mathcal{O}$. □

Proposición 1.7.3. *Se cumple que $Dg_n = 2nh_n$ y $Dh_n = n(3g_n^2 + A)$.*

Demostración: Si $n = 1$ se deduce de la definición de D.

Cuando $n = 2$, derivando la ecuación (1.14) y multiplicando por 4 vemos que da la ecuación (1.15).

Suponemos que se cumple para $n - 1$ entonces se cumplen las siguientes ecuaciones:

$$\begin{aligned}
g_n &= -g_{n-1} - x + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2 && (1.18)\\
h_n &= -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)(g_n - x) && (1.19)\\
(h_{n-1})^2 &= (g_{n-1})^3 + Ag_{n-1} + B && (1.20)\\
Dg_{n-1} &= 2(n-1)h_{n-1} && (1.21)\\
Dh_{n-1} &= (n-1)(3g_{n-1}^2 + A) && (1.22)
\end{aligned}$$

Las ecuaciones (1.18) y (1.19) se deducen de la formula de adición a $nP = (n-1)P + P$. La ecuación (1.20) expresa que $(g_{n-1}, h_{n-1})(P)$ esta en la curva para todo P. Y, por ultimo, las ecuaciones (1.21) y (1.22) son la hipotesis de inducción.

Si aplicamos D a (1.18)

$$\begin{aligned} Dg_n &= -Dg_{n-1} - 2y + 2\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) \\ &= -2(n-1)h_{n-1} - 2y + 2\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) \\ &= -2(n-1)(h_{n-1}-y) - 2ny + 2\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) \\ &= -2ny - 2\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right)\left[(n-1)(g_{n-1}-x) - D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right)\right] \end{aligned}$$

Multiplicando (1.19) por $2n$ vemos que alcanza con probar que

$$(n-1)(g_{n-1}-x) - D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) = n(g_n - x)$$

o que

$$\begin{aligned} ng_n &= (n-1)g_{n-1} + x - D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) \\ &= -ng_{n-1} - nx + (2n-1)g_{n-1} + (n+1)x - D\left(\frac{h_{n-1}-y}{g_{n-1}-x}\right) \end{aligned}$$

para esto, viendo n(1.18) podemos probar que

$((2n-1)g_{n-1}+(n+1)x)(g_{n-1}-x)^2-(D(h_{n-1}-y)(g_{n-1}-x)-D(g_{n-1}-x)(h_{n-1}-y))$

es igual a

$$\begin{aligned} n(h_{n-1}-y)^2 &= nh_{n-1}^2 - 2nh_{n-1}y + ny^2 \\ &= ng_{n-1}^3 + Ang_{n-1} + 2Bn + nx^3 + Anx - 2nh_{n-1}y \end{aligned}$$

Ahora

$$\begin{aligned} & ((2n-1)g_{n-1} + (n+1)x)(g_{n-1}-x)^2 \\ = \; & (2n-1)g_{n-1}^3 - 3(n-1)g_{n-1}^2 x - 3g_{n-1}x^2 + (n+1)x^3 \end{aligned}$$

y aplicando (1.20), (1.21) y (1.22)

$$\begin{aligned} & D(h_{n-1}-y)(g_{n-1}-x) - D(g_{n-1}-x)(h_{n-1}-y) \\ = \; & (3(n-1)g_{n-1}^3 + A(n-1)g_{n-1} - 3g_{n-1}x^2 - Ag_{n-1} - A)(g_{n-1}-x) \\ & -2((n-1)h_{n-1}-y)(h_{n-1}-y) \\ = \; & 3(n-1)g_{n-1}^3 + A(n-1)g_{n-1} - 3g_{n-1}x^2 - Ag_{n-1} - 3(n-1)g_{n-1}^2 x \\ & -A(n-1)x + 3x^3 + Ax - 2(n-1)h_{n-1}^2 + 2(n-1)h_{n-1}y + 2h_{n-1}y - y^2 \\ = \; & (n-1)g_{n-1}^3 - 3(n-1)g_{n-1}^2 x - 3g_{n-1}x^2 - Ang_{n-1} \\ & +x^3 - Anx - 2Bn + 2nh_{n-1}y \end{aligned}$$

Y restando las dos ultimas ecuaciones vemos que claramente es igual

$$n(h_{n-1}-y)^2$$

Lo que muestra que $Dg_n = 2nh_n$.

Falta verificar que $Dh_n = n(3g_n + A)$, pero es fácil de verificar derivando

$$h_n^2 = g_n^3 + Ag_n + B$$

y usando que $Dg_n = 2nh_n$. □

Antes de presentar el teorema sobre el divisor de $g_m - g_n$, necesitamos un lema sobre traslaciones. El lema nos permitirá usar información sobre el orden de g_n en un punto de $E[n]$ para obtener información sobre el orden de g_n en todos los puntos de $E[n]$.

Lema 1.7.4. *Sean $P, Q \in E(K)$ y u una variable uniformizadora en P. Entonces la función $T_Q(u)$ definida por*

$$T_Q(u)(R) = u(R + Q) \tag{1.23}$$

es una variable uniformizadora en $P - Q$.

Demostración: Si definimos $T_Q : E(K) \to E(K)$ de la misma manera que en (1.23), vemos que es un automorfismo de cuerpos, donde su inversa es T_{-Q}.

Supongamos entonces que $T_Q(u)$ no es una variable uniformizadora en $P-Q$. Como $T_Q(u)(P-Q) = u(P-Q+Q) = 0$, $\mathrm{ord}_{P-Q}(T_Q(u)) = m > 1$. Por lo que $T_Q(u) = v^m v_1$ donde v es una variable uniformizadora en $P - Q$ y v_1 es finita y no nula en $P - Q$.

Ahora, si $\mathrm{ord}_P(r) = d$ entonces $r = u^d r_1$ con $d \in \mathbb{Z}$ y r_1 finita y no nula en P, y $T_Q(r) = T_Q(u)^d T_Q(r_1) = v^{md} s_1^d T_Q(r_1)$ por lo que $\mathrm{ord}_{P-Q}(T_Q(r)) = dm$ ya que $(s_1^d T_Q(r_1))(P - Q) = s_1^d(P - Q)r_1(P)$ que es finito y no nulo.

Si $r = T_{-Q}(v)$ entonces $1 = \mathrm{ord}_{P-Q}(v) = \mathrm{ord}_{P-Q}(T_Q(r)) = m\,\mathrm{ord}_P(r)$, llegando así a un absurdo ya que tendríamos que $\mathrm{ord}_P(r) = 1/m \notin \mathbb{Z}$. Podemos afirmar entonces que $T_Q(u)$ es una variable de uniformización en $P - Q$. □

Es inmediato a partir del lema que si una función racional r tiene divisor $\sum_{P \in E(K)} n(P)\langle P\rangle$ el divisor de $T_Q(r)$ será $\sum_{P \in E(K)} n(P)\langle P - Q\rangle$ Recordemos que

$$E[n] = \{P \in E(K) : n \cdot P = 0\}$$

Denotamos $\langle E[n]\rangle$ como el divisor que tiene entradas con valor uno en los puntos de $E[n]$ y cero en el resto.

Suponemos de aca en mas que la característica de K no es 3, ya que presenta dificultades.

Teorema 1.7.5. *Supongamos que $m > n > 0$ y que $m, n, m - n$ y $m + n$ son coprimos con p. Entonces*

$$\mathrm{div}(g_m - g_n) = \langle E[m + n]\rangle + \langle E[m - n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle \tag{1.24}$$

Demostración: Hay varios casos para demostrar.

• Primero consideramos los puntos de $E[m] \cap E[n]$. Por definición esos puntos también están en $E[m+n]$ y $E[m-n]$. Por lo que debemos probar que $g_m - g_n$

tiene orden $1+1-2-2=-2$ en esos puntos. Uno de esos puntos es $\mathcal{O}$. La Proposición 1.6.5 nos dice que g_m y g_n tienen polos dobles en $\mathcal{O}$. Además el Corolario 1.6.6 nos dice que g_m tiene coeficiente principal $1/m^2$ y g_n tiene coeficiente principal $1/n^2$. Por lo que podemos escribir

$$g_m = \left(\frac{x}{y}\right)^2 r_1 \quad g_n = \left(\frac{x}{y}\right)^2 r_2$$

con $r_1(\mathcal{O}) = 1/m^2$ y $r_2(\mathcal{O}) = 1/n^2$, por el Corolario 1.6.6 nuestras hipotesis implican que

$$m^2 \not\equiv n^2 \mod p$$

ya que si no $1 \equiv \frac{m^2}{n^2} \equiv \left(\frac{m}{n}\right)^2 \mod p$ entonces $m-n \equiv 0 \mod p$ o $m+n \equiv 0$ mód p contradiciendo las hipotesis. Luego $g_m - g_n$ tiene orden -2 en $\mathcal{O}$.

Si $P \in E[n]$, entonces $T_P(g_n) = g_n$ ya que $n(Q+P) = nQ$. Por el Lema 1.7.4, el orden de g_n es el mismo en todos los puntos de $E[n]$. Vemos que $g_m - g_n$ tienen orden -2 en $E[m] \cap E[n]$, ya que $T_P(g_m - g_n) = T_P(g_m) - T_P(g_n) = g_m - g_n$.

- Consideramos ahora los puntos que están en $E[m] \backslash E[n]$.

Esos puntos no pueden estar en $E[m+n]$ ni en $E[m-n]$ por nuestras hipotesis. Debemos mostrar que $g_m - g_n$ tienen orden -2 en estos puntos. Mostramos en el caso anterior que g_m tiene orden -2 y como g_n tiene orden positivo, podemos escribir $g_m = u^{-2} r_1$ y $g_n = u^d r_2$ donde u es una variable uniformización en un punto $P \in E[m] \backslash E[n]$, $d \in \mathbb{N}$, y r_1, r_2 son funciones racionales finitas que no se anulan en P. Luego $g_m - g_n = u^{-2}(r_1 - u^{d+2} r_2)$, con $r_1 - u^{d+2} r_2$ finita y no nula en P.

- El tercer caso es el de los puntos que no están en $E[m]$ ni en $E[m]$.

Hay tres subcasos, $P \in E[m-n] \backslash E[m+n]$, $P \in E[m+n] \backslash E[m-n]$ y $P \in E[m-n] \cup E[m+n]$. En los tres subcasos $g_m - g_n$ tiene un cero en P, ya que si $mP = nP$ o $mP = -nP$ esto implica que $(g_m(P), h_m(P)) = (g_n(P), h_n(P))$ o $(g_m(P), h_m(P)) = -(g_n(P), h_n(P)) = (g_n(P), -h_n(P))$. Entonces el problema esta en hallar la multiplicidad de ese cero. Usaremos la derivación en E para esto. Por la Proposición 1.7.3, $D(g_m - g_n) = 2m h_m - 2n h_n$.

- Si $P \in E[m-n] \backslash E[m+n]$, tenemos que $mP = nP \neq -nP$ y como $P \notin E[m] \cup E[n]$, $mP \neq \mathcal{O}$ y $nP \neq \mathcal{O}$. En este caso $h_m(P) = h_n(P)$ por lo que $D(g_m - g_n)(P) = 2(m-n) h_n(P)$. Como $nP \neq -nP$, nP no es un punto de orden dos, entonces $h_n(P) \neq 0$, y además $m-n$ es coprimo con p por lo que $D(g_m - g_n)(P) \neq 0$. Probamos que $g_m - g_n$ tiene un cero de orden uno.

- El caso $P \in E[m+n] \backslash E[m-n]$ es simétrico al caso anterior.

- En el caso en que $P \in E[m-n] \cup E[m+n]$, tenemos que $mP = -nP$, $mP = nP$, $nP \neq \mathcal{O}$ y $mP \neq \mathcal{O}$. Todo esto implica que $2mP = 2nP = \mathcal{O}$ por lo que $D(g_m - g_n)(P) = 0$ lo que implica que la multiplicidad es al menos dos. Debemos estudiar $DD(g_m - g_n)(P)$. La Proposición 1.7.3 nos dice que

$$Dh_n = n(3g_n^2 + A)$$

Como $2nP = \mathcal{O}$, nP es un punto de orden dos. Luego $g_n(P) = \omega$ y $h_n(P) = 0$. Entonces

$$DD(g_m - g_n)(P) = 2(m^2 - n^2)(3\omega^2 + A)$$

que es no nulo ya que $m-n$ y $m+n$ son coprimos con p, y E es una curva elíptica. Luego $g_m - g_n$ tiene un cero doble. □

Corolario 1.7.6. *Si n es coprimo con p, $E[n]$ tiene n^2 puntos.*

Demostración: Sea d_n la cantidad de puntos en $E[n]$. Usando la ecuación (1.24) y tomando grados obtenemos

$$d_m + d_n - d_{m+n} - d_{m-n} = 0 \tag{1.25}$$

Sabemos que $d_1 = 1$ y que $d_2 = 4$. Podemos ver que $d_n = n^2$ cumple (1.25) ya que

$$(m+n)^2+(m-n)^2-2m^2-2n^2 = m^2+2mn+n^2+m^2-2mn+n^2-2m^2-2n^2 = 0$$

Para ver que la solución es única alcanza con tomar $\bar{d}_1 = \bar{d}_2 = 0$ y mostrar que si $\bar{d}_n$ cumple (1.25) para n coprimo con p entonces $\bar{d}_n = 0$. Sea k coprimo con p y supongamos que $\bar{d}_n = 0$ para $n < k$ y coprimo con p. Si tomamos $m = k-1$ y $n = 1$, vemos que $\bar{d}_k = 2\bar{d}_{k-1} - \bar{d}_{k-2}$. Por lo tanto $\bar{d}_k = 0$ si $k-1$ y $k-2$ son coprimos con p. Si tomamos $m = k-2$ y $n = 2$ vemos que $\bar{d}_k = 2\bar{d}_{k-2} - \bar{d}_{k-4}$, por lo que $\bar{d}_k = 0$ si $k-2$ y $k-4$ son coprimos con p. De la misma manera vemos que $\bar{d}_k = 0$ si $k-3$ y $k-6$ son coprimos con p

Si $k-1$ no es coprimo con p. Entonces $k-2$ si lo es, y si $k-4$ es coprimo con p, por lo que $p = 3$ que lo habíamos excluido.

Si $k-2$ no es coprimo con p, entonces $k-3$ tiene que serlo, y si $k-6$ no lo es, 4 es múltiplo de 2, por lo que $p = 2$ caso que también habíamos excluido.

Concluimos que siempre hay un caso que hace que $\bar{d}_k = 0$. □

Corolario 1.7.7. *Si n es coprimo con p, $E[n]$ es isomorfo a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Demostración: Primero lo demostramos para $n = l$ primo.

Por el Teorema Fundamental de Grupos Abelianos, sabemos que $E[l]$ es isomorfo a $\mathbb{Z}/l^2\mathbb{Z}$ o a $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, ya que $E[l]$ tiene l^2 elementos, pero como todos los elementos de $E[l]$ son puntos de l-torsión, no puede ser $\mathbb{Z}/l^2\mathbb{Z}$ que contiene elementos que no lo son. Entonces $E[l]$ es isomorfo a $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$.

Ahora si $n = l^e$ con l primo y $e \geq 0$, $E[n]$ es isomorfo a

$$\mathbb{Z}/l^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/l^{a_r}\mathbb{Z}$$

con $a_i \geq 0$ y $a_1+a_2+\cdots+a_r = 2e$. Luego $(\mathbb{Z}/l\mathbb{Z})^r$ es isomorfo a un subgrupo de $E[n]$, y como solo hay l^2 puntos de l-torsión tiene que ser $1 \leq r \leq 2$. Claramente no puede ser $E[l^e]$ isomorfo a $\mathbb{Z}/l^{2e}\mathbb{Z}$, así que es isomorfo a $\mathbb{Z}/l^a\mathbb{Z} \times \mathbb{Z}/l^b\mathbb{Z}$ con $a+b = 2e$. Si a o b es mayor que e entonces tendríamos en $E[l^e]$ puntos de orden mayor que l^e. Entonces $E[l^e]$ es isomorfo a $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$.

Ahora, si n es coprimo con p y $l^e||n$ con l primo, $\mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z}$ es isomorfo a un subgrupo de $E[n]$ y es el mas grande que contiene elementos de orden l, luego $E[n]$ es isomorfo a

$$\prod_{l \ / \ l^e||n} \mathbb{Z}/l^e\mathbb{Z} \times \mathbb{Z}/l^e\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

□

1.8. Los Polinomios de División

Queremos definir polinomios ψ_n con divisor $\langle E[n]\rangle$. Si $P \in E[n]$, $-P \in E[n]$, y si son diferentes suman $\mathcal{O}$. Si no lo son luego es un punto de orden dos por lo que todos los puntos de orden dos están en $E[n]$ y suman $\mathcal{O}$. Por lo tanto suma($\langle E[n]\rangle$) $= \mathcal{O}$. Sabemos además que gr($\langle E[n]\rangle$) $= n^2$. Ahora si tomamos el divisor $\Delta = \langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$, por la Proposición 1.5.5 existe una función racional r tal que div$(r) = \langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$. Pero r no tiene polos finitos porque todos los coeficientes de $\langle E[n]\rangle$ son 0 o 1. Entonces por el Lema 1.3.7 r es un polinomio. El único problema es que no es necesariamente único. Pero si fijamos su coeficiente principal si.

Todo esto funciona bien cuando n y p son coprimos. Queremos calcular los ψ_n de manera inductiva, así que precisamos definirlos también en los múltiplos de p . Para eso vamos a definirlos primero en característica 0, probar lo que necesitamos, despues dar una definición diferente para característica positiva y ver que los resultados con característica 0 implican los resultados con característica positiva. **Asumimos entonces que la característica de K es 0.**

Definición 1.8.1. Sea ψ_n el único polinomio con divisor $\Delta = \langle E[n]\rangle - n^2\mathcal{O}$ y con coeficiente principal n.

Observación 1.8.1. Como el coeficiente en $\mathcal{O}$ del divisor Δ es $1 - n^2$ sabemos por el Ejemplo 1.3.1 que el grado de ψ_n es $n^2 - 1$.

Proposición 1.8.1.

1. $$\psi_n^2(P) = n^2 \prod_{P' \in E[n]\setminus\mathcal{O}} [x(P) - x(P')]$$

2. *Si n es impar, ψ_n es una función que solo depende x y su grado como función en x es $(n^2 - 1)/2$.*

3. *Si n es par, ψ_n es el producto de y por una función que depende solo de x y el grado en x de esa función es $(n^2 - 4)/2$.*

Demostración:

1. Vamos a probar que el divisor de $f(P) = n^2 \prod_{P' \in E[n]\setminus\mathcal{O}}[x(P) - x(P')]$ es 2Δ y que f tiene coeficiente principal n^2, que es el coeficiente principal de ψ_n. Claramente $f(P') = 0$ para todo $P' \in E[n]\setminus\mathcal{O}$, además tiene orden dos porque en el producto de f aparecen $x(P)-x(P')$ y $x(P)-x(-P')$ que son iguales. El orden de f en $\mathcal{O}$ es $\mathrm{gr}(f) = \prod_{P' \in E[n]\setminus\mathcal{O}} \mathrm{gr}([x(P) - x(P')]) = \prod_{P' \in E[n]\setminus\mathcal{O}} 2 = 2(n^2 - 1)$. Entonces $\mathrm{div}(f) = 2\Delta = 2\,\mathrm{div}(\psi_n) = \mathrm{div}(\psi_n^2)$ y claramente el coeficiente principal de ψ_n^2 y f coinciden.

2. Podemos escribir $\psi_n = v + yw$, donde v y w son polinomios que solo dependen de x. Entonces $\psi_n^2 = v^2 + 2yvw + sw^2$, y como vimos en la parte anterior ψ_n^2 no tiene términos que dependan de y, entonces v o w tienen que ser nulos. Como $\mathrm{gr}(\psi_n) = n^2 - 1$ es par debe ser $\psi = v$. Y por la definición de grado se cumple que $n^2 - 1 = \mathrm{gr}(v) = 2\,\mathrm{gr}_x(v)$.

3. Por la parte anterior sabemos que $\psi = yw$ porque el grado de ψ es impar. Además $n^2 - 1 = \mathrm{gr}(\psi_n^2) = 3 + 2\,\mathrm{gr}_x(w)$, $\mathrm{gr}_x(w) = (n^2-4)/2$.

Teorema 1.8.2. *Si $m > n > 0$ se cumple que*

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} \tag{1.26}$$

Demostración: Por el Teorema 1.7.5 sabemos que

$$\mathrm{div}(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle$$

Por definición,

$$\mathrm{div}\left(-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}\right) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle$$

Las dos ecuaciones anteriores nos dicen que $g_m - g_n$ y $-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$ tienen igual divisor. Sabemos que g_n tiene coeficiente principal $1/n^2$ y ψ_n tiene n. Entonces el coeficiente principal de $-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$ es $-\frac{(m+n)(m-n)}{m^2n^2} = -\frac{m^2-n^2}{m^2n^2} = \frac{1}{m^2} - \frac{1}{n^2}$ que es el coeficiente principal de $g_m - g_n$. Por lo tanto son la misma función. □

Corolario 1.8.3. *Para todo $P \in E(K)$ se cumple*

$$g_n(P) = x(nP) = x(P) - \frac{\psi_{n+1}(P)\psi_{n-1}(P)}{\psi_n(P)^2} \tag{1.27}$$

Demostración: Como $g_1 = x$ la prueba es trivial a partir del Teorema anterior. □

El próximo teorema nos da las propiedad básicas de los polinomios ψ_n, que usaremos luego para definirlos en característica positiva.

Teorema 1.8.4. *Los polinomios ψ_n cumplen*

o. $\psi_0 = 0$

i. $\psi_1 = 1$

ii. $\psi_2(P) = 2y$

iii. $\psi_3(P) = 3x^4 + 6Ax^2 + 12Bx - A^2$

iv. $\psi_4(P) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABX - 8B^2 - A^3)$

v. para $m > n > 0$

$$\psi_n^2\psi_{m+n}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1} = \psi_{m+n}\psi_{m-n} \tag{1.28}$$

Demostración: *o.* y *i.* se deducen de la definición.

Para demostrar *ii.* sabemos que ψ_2 es y por una función que depende solo de x y que tiene grado $(4-4)/2 = 0$ como función en x, además ψ_2 debe tener coeficiente principal 2. Por lo tanto $\psi_2(P) = 2y$.

Para *iii.*, observamos por el Corolario 1.8.3 que

$$g_2(P) = x(2P) = x(P) - \frac{\psi_3(P)\psi_1(P)}{\psi_2(P)^2}$$

conocemos todos los elementos de la ecuación salvo ψ_3. Despejando

$$\begin{aligned}
\psi_3(P) &= x\psi_2^2(P) - g_2(P)\psi_2^2(P) \\
&= 4y^2x - 4y^2\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} \\
&= 4x^4 + 4Ax^2 + 4Bx - x^4 + 2Ax^2 + 8Bx - A^2 \\
&= 3x^4 + 6Ax^2 + 12Bx - A^2
\end{aligned}$$

Podríamos hacer una cuenta similar para calcular ψ_4. Pero podemos hacerlo de otra manera que nos evita calcular g_3. Si P es un punto de torsión 4 entonces tiene orden 2 o 4. Si tiene orden 2 entonces $y(P) = 0$ y si tiene orden 4 entonces $2P$ es de orden 2 por lo que $h_2(P) = 0$. Sabemos que $h_2(P) = y \cdot \frac{x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-8B^2-A^3}{8s(x)^2}$ entonces claramente $\psi_3(P) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$.

Para probar *v.* escribimos $g_m - g_n = (g_m - g_1) - (g_n - g_1)$ y usando la ecuación (1.26) obtenemos

$$-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} = x - \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} - x + \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}$$

y se deduce inmediatamente de la ecuación. □

Corolario 1.8.5.

i. Para $k > 2$

$$\psi_{2k} = \frac{\psi_k}{2y}(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2)$$

ii. Para $k \geq 2$

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k+1}^3\psi_{k-1}$$

Demostración: Para demostrar *i.* usamos la ecuación (1.28) con $m = k+1$ y $n = k-1$. Para *ii.* $m = k+1$ y $n = k$. □

Proposición 1.8.6. *Si* $P \in E(K)$ *y* $n \geq 2$

$$h_n(P) = y(nP) = \frac{\psi_{n+2}(P)\psi_{n-1}(P)^2 - \psi_{n-2}(P)\psi_{n+1}(P)^2}{4y\psi_n(P)^3} \tag{1.29}$$

Demostración: La prueba es por inducción.

Si $n = 2$, ya habíamos visto en 1.8.4 iv. que $h_2(P) = \psi_4/64y^4$ y

$$\frac{\psi_4(P)\psi_1(P)^2 - \psi_0(P)\psi_3(P)^2}{4y\psi_2(P)^3} = \frac{\psi_4(P)}{4y(2y)^3} = h_2(P)$$

Para el paso inductivo usamos

$$\begin{aligned} h_n &= -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)(g_n - x) \\ &= -y - \left(\frac{\psi_{n-1}^3\psi_{n+1}}{\psi_n^3\psi_{n-2}}\right)\left(\frac{\psi_{n+1}\psi_{n-2}^2 - \psi_{n-3}\psi_n^2}{4y\psi_{n-1}^3} - y\right) \\ &= \frac{\psi_{n-1}^3\psi_2^2\psi_{n+1} - \psi_n^3\psi_2^2\psi_{n-2} - \psi_{n+1}^2\psi_{n-2}^2 + \psi_{n-3}\psi_n^3\psi_{n+1}}{4y\psi_n^3\psi_{n-2}} \end{aligned}$$

Por la ecuación (1.28) sabemos que

$$\psi_{n-1}^3\psi_2^2\psi_{n+1} = \psi_{n-1}^2(\psi_2^2\psi_{n-1}\psi_{n+1}) = \psi_{n-1}^2\psi_{n+2}\psi_{n-2} + \psi_{n-1}^2\psi_n^2\psi_3$$

$$\psi_n^3\psi_2^2\psi_{n-2} = \psi_n^2(\psi_2^2\psi_n\psi_{n-2}) = \psi_n^2\psi_{n-3}\psi_{n+1} + \psi_{n-1}^2\psi_n^2\psi_3$$

y poniendo estas dos ecuaciones en la anterior se deduce el resultado. □

Queremos extender los resultados de esta sección a cuerpos de característica positiva. La idea es observar que las igualdades que queremos probar son en realidad igualdades polinomiales en el anillo $\mathbb{Z}[A, B, x, y]$, entonces se cumplen cuando reducimos módulo un primo p.

De ahora en mas asumimos que la característica de K es arbitraria.

Definición 1.8.2. Los polinomios ψ_n son los únicos polinomios que cumplen las siguientes condiciones:

o. $\psi_0 = 0$

i. $\psi_1 = 1$

ii. $\psi_2(P) = 2y$

iii. $\psi_3(P) = 3x^4 + 6Ax^2 + 12Bx - A^2$

iv. $\psi_4(P) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABX - 8B^2 - A^3)$

v. Para $k > 2$

$$\psi_{2k} = \frac{\psi_k}{2y}(\psi_{k+2}\psi_{k-1}^2 - \psi_{k-2}\psi_{k+1}^2) \tag{1.30}$$

vi. Para $k \geq 2$

$$\psi_{2k+1} = \psi_{k+2}\psi_k^3 - \psi_{k+1}^3\psi_{k-1}$$

Por el Teorema 1.8.2 y el Corolario 1.8.5, esta definición coincide con la dada en característica 0.

Consideremos ahora el cuerpo $\mathcal{K} = \mathbb{Q}(\mathcal{A}, \mathcal{B})$ de funciones racionales en las indeterminadas $\mathcal{A}$ y $\mathcal{B}$ sobre $\mathbb{Q}$. Sea la curva elíptica definida por

$$Y^2 = X^3 + \mathcal{A}X + \mathcal{B}$$

En este caso podemos identificar el cuerpo de funciones racionales de E sobre $\mathcal{K}$ con el cuerpo de fracciones del anillo $\mathcal{R} = \mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]/(Y^2 - X^3 - \mathcal{A}X - \mathcal{B})$. Claramente los polinomios ψ_n están en el anillo $\mathcal{R}$. Si consideramos entonces una igualdad polinomial como (1.28), que es una igualdad de los ψ_n con coeficientes enteros. Probamos hasta ahora que se cumple en característica 0, sin embargo vamos a deducir que se cumple la igualdad para los ψ_n en una curva elíptica cualquiera sobre un cuerpo arbitrario.

El anillo $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]$ tiene la propiedad de que existe un único homomorfismo de anillos de el en R que manda $\mathcal{A}, \mathcal{B}, X, Y$ en elementos cualquiera de R. Si mandamos esas indeterminadas en A, B, x, y en el cuerpo de funciones racionales de una curva cualquiera, entonces el homomorfismo induce un mapa de $\mathcal{R}$ en el cuerpo de funciones racionales de esa curva. Este mapa claramente manda los polinomios ψ_n de una curva en los ψ_n de la otra. Por lo que cualquier igualdad que involucre los ψ_n que se cumpla en característica 0 se tiene que cumplir para cualquier curva sobre cualquier cuerpo.

Demostraremos el Corolario 1.8.3 y la Proposición 1.8.6. O sea, las expresiones de g_n y h_n en función de los ψ_n en característica p.

Teorema 1.8.7. *i. ψ_n es no nulo para $n > 0$.*

ii. g_n cumple

$$g_n = x - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2} \tag{1.31}$$

iii. h_n cumple, para $n > 1$

$$h_n = \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3} \tag{1.32}$$

Demostración: Es claro que ψ_n es no nulo si $0 < n \leq 4$.

Asumamos ahora (1.31) y (1.32) para $n < m$, y que ψ_n es no nulo para $n < m + 1$.

Asumamos también que estamos en característica 0.

Si tomamos la expresión de g_m dada por (1.31), y notamos que

$$g_m = -g_{m-1} - x + \left(\frac{h_{m-1} - y}{g_{m-1} - x}\right)^2$$

podemos usar las ecuaciones (1.31) y (1.32) para $n = m - 1$, que sabemos ciertas para característica 0, para eliminar g_{m-1} y h_{m-1}. Obtenemos entonces una identidades en los polinomios ψ_n.

De la misma manera podemos usar la ecuación (1.32) y

$$h_m = -y - \left(\frac{h_{m-1} - y}{g_{m-1} - x}\right)(g_m - x)$$

para obtener otra identidades en los ψ_n.

Que son estas identidades no es importante, lo importante es que son identidades en $\mathbb{Z}[\mathcal{A}, \mathcal{B}, X, Y]/(Y^2 - X^3 - \mathcal{A}X - \mathcal{B})$. Entonces por el argumento anterior son identidades que se cumplen también en característica p. Queremos convertir esas identidades en característica p de vuelta en las ecuaciones a demostrar. Para hacer esto debemos dividir por ψ_{m-2}, ψ_{m-1} y ψ_m, que son no nulos por la hipotesis inductiva. Luego las ecuaciones (1.31) y (1.32) para $n = m$ se cumplen en característica arbitraria.

Sabemos entonces que

$$g_m - x = -\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2}$$

Por el Corolario 1.6.3 $g_m - x$ es no nulo. Entonces ψ_{m+1} tampoco, lo que nos permite seguir con la inducción. □

Casi lo único que nos falta probar de los ψ_n es que su divisor es $\langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$, que solo se cumple si n y p son coprimos.

Proposición 1.8.8. *Si n es coprimo con p,* $\mathrm{div}(\psi_n) = \langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$ *incluso en característica positiva. Además, si n no es necesariamente comprimo con p, ψ_n tiene todos sus ceros en $E[n]$.*

Demostración: Hemos probado que

$$g_n - x = -\frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}$$

Como sabemos que $g_n - x$ tiene solo polos en $E[n]$, ψ_n tiene ceros en $E[n]$. Hay que ver que estos ceros son simples y que no hay otros.

Si n es coprimo con p ,$\mathrm{gr}(\psi_n) = n^2 - 1$ ya que lo es en característica cero, y su coeficiente principal no se reduce a cero módulo p porque es n. Como ψ_n tiene un polo en $\mathcal{O}$ y ceros en $E[n]$, no puede tener otros ceros porque $E[n]$ tiene n^2 puntos. Como los polos de $g_n - x$ en $E[n]$ tienen multiplicidad dos, la ecuación (1.31) muestra que los ceros de ψ_n tienen que ser simples. Esto prueba que $\mathrm{div}(\psi_n) = \langle E[n]\rangle - n^2\langle\mathcal{O}\rangle$.

Si n es múltiplo de p, podemos observar la ecuación (1.30) para $k = n$:

$$\psi_{2n+1} = \psi_{n+1}\psi_n^3 - \psi_{n+1}^3\psi_{n-1} \tag{1.33}$$

ψ_n debe de ser coprimo con ψ_{n+1} porque si no ψ_{2n+1} tendría una raíz triple. Como $2n+1$ es coprimo con p esto no seria posible por el argumento anterior. Si miramos nuevamente la ecuación (1.30) con $k = n - 1$, vemos que ψ_n tiene que ser coprimo con ψ_{n-1}. Entonces la ecuación (1.31) implica que ψ_n tiene todos sus ceros en $E[n]$, pero no sabemos si son simples. □

Observación 1.8.2. $E[p]$ es isomorfo a $\mathbb{Z}/p\mathbb{Z}$ o a el grupo trivial.

Demostración: En característica cero el coeficiente principal de ψ_n es n. Por lo que en característica p el grado de ψ_p es menor que $p^2 - 1$. Como los elementos de $E[p]$ son todos ceros de ψ_p, esto dice que $E[p]$ no puede tener p^2 elementos. Como $E[p]$ es un grupo tal que todos sus elementos son de p-torsión, $E[p]$ tiene que ser $\mathbb{Z}/p\mathbb{Z}$ o el grupo trivial. □

Capítulo 2

Teorema de Hasse

2.1. Introducción

Sean p un primo, n un entero positivo, $q = p^n$, y $k = \mathrm{GF}(q)$, el cuerpo finito de q elementos. Sea K la clausura algebraica de k. En este capitulo estamos interesados en la curva elíptica definida sobre k definida por

$$Y^2 = X^3 + AX + B \tag{2.1}$$

para $A, B \in k$. Una pregunta natural es cuantos elementos tiene $E(k)$, que denotamos por E_q.

Una herramienta importante en el estudio de esta problema es el mapa racional φ, llamado el mapa de Frobenius. Necesitamos un resultado trivial antes de definir φ.

Proposición 2.1.1. *Si* $(a, b) \in E(K)$, $(a^q, b^q) \in E(K)$.

Demostración: Si $(a, b) \in E(K)$, $b^2 = a^3 + aA + B$

$$b^{2q} = (a^3 + aA + B)^q = a^{3q} + a^q A^q + B^q$$

ya que por el Pequeño Teorema de Fermat y la formula del binomio de Newton $(c+d)^q = c^q + d^q$. Además, como A y B están en k por el Teorema mencionado $A^q = A$ y $B^q = B$, por lo que $(a^q, b^q) \in E(K)$. □

Definición 2.1.1. El *mapa de Frobenius* es el mapa $\varphi : E(K) \to E(K)$ definido por $\varphi(a, b) = (a^q, b^q)$ y $\varphi(\mathcal{O}) = \mathcal{O}$.

Proposición 2.1.2. *Sea* $P = (a, b) \in E(K)$, $P \in E(k)$ *si y solo si* $\varphi(P) = P$.

Demostración: $(a, b) = \varphi(a, b)$ si y solo si $a = a^q$ y $b = b^q$. Ahora observamos que el polinomio $f(X) = X^q - X$ en $K[X]$ tiene grado q y si $a \in k$ $f(a) = 0$, por lo que tiene q raíces. Por lo tanto si a o b no estuvieran en k el polinomio f tendría mas de q raíces. □

Presentamos ahora el Teorema a probar en el curso de este capitulo que fue conjeturado por Emil Artin y demostrado por Helmut Hasse.

Teorema de Hasse: *Sea E una curva elíptica definida sobre $k = \mathrm{GF}(q)$, y $t = q + 1 - E_q$. Entonces*

i. $\varphi \circ \varphi - [t] \circ \varphi + [q] = \mathcal{O}_M$ *y*

ii. $|t| \leq 2\sqrt{q}$

donde $[m]$ es el mapa racional $P \mapsto mP$.

A pesar de que el Teorema Principal trata sobre curvas elípticas sobre cuerpos finitos, muchos de los resultados que llevan a el son validos para cualquier cuerpo. Solo los resultados sobre el mapa de Frobenius requieren a k ser finito. Por lo tanto por el resto de esta parte, al menos que explicitemos su finitud, k será un cuerpo arbitrario de característica $\neq 2$ o 3 y K su clausura algebraica.

2.2. El Índice De Ramificación

Lema 2.2.1. *Si r es una función racional no constante en E, r toma todos los valores de K y ∞.*

Demostración: Por el Lema 1.3.5 y el Teorema 1.3.3 sabemos que r tiene al menos un cero y un polo. El lema queda probado si consideramos $r - a$ para todo $a \in K$. □

Proposición 2.2.2. *Un mapa racional $F : E(K) \to E(K)$ no constante es sobreyectivo.*

Demostración: Si $F = (r, s)$ donde r y s son funciones racionales. Si r fuese constante s tomaría una cantidad finita de valores y por el lema anterior seria constante por lo que F también lo seria. Lo mismo pasa si suponemos que s fuese constante. Podemos afirmar que r y s son no constantes.

Por el lema anterior deducimos que r y s tienen polos y además en los mismos puntos porque $(r(P), s(P))$ son puntos de la curva. Entonces F toma el valor $\mathcal{O}$, y llegamos al resultado buscado tomando la función racional $Q \mapsto F(Q) - P$ para todo P en la curva. □

Vamos ahora a definir el índice de ramificación de un mapa racional no constante en un punto dado P. Si tomamos u una variable uniformizadora en $F(P)$ podemos ver que $u \circ F$ es no constante nula, ya que si así lo fuese, como F es sobreyectiva, u seria constante, lo que es absurdo. Concluimos que $u \circ F$ es cero en $F(P)$ pero no constante nula.

Definición 2.2.1. El *índice de ramificación de F en P* es definido por

$$e_F(P) = \mathrm{ord}_P(u \circ F)$$

donde u es una variable uniformizadora en $F(P)$.

Observación 2.2.1. $e_F(P)$ es independiente de u

Demostración: Si u' es otra variable de uniformización en $F(P)$ y $u \circ F = v^{d_1} r_1$, $u' \circ F = v^{d_2} r_2$ con $d_1, d_2 \in \mathbb{Z}$, r_1, r_2 funciones racionales finitas y no nulas en P y v una variable de uniformización en P. Si r es una función racional entonces $r = u^d r_3 = u'^d r_4$ con r_3, r_4 finitas y no nulas en $F(P)$. Luego $r \circ F = v^{dd_1} r_1 r_3 \circ F = v^{dd_2} r_2 r_4 \circ F$. Sabemos que $dd_1 = dd_2$, y alcanza con tomar una función r con orden positivo en $F(P)$.

Proposición 2.2.3. *Si r es una función racional no nula en E y F un mapa racional no contante. Sea $P \in E(K)$, se cumple*

$$\mathrm{ord}_P(r \circ F) = [\mathrm{ord}_{F(P)}(r)][e_F(P)]$$

Demostración: Sean u y v variables uniformizadoras en $F(P)$ y P respectivamente. Podemos escribir $r \circ F = v^d r_1$, $u \circ F = v^f r_2$ y $r = u^e r_3$ con r_1, r_2 finitas no nulas en P y r_3 finita n nula en $F(P)$. Ocurre

$$r \circ F = (u^e r_3) \circ F = (u \circ F)^e (r_3 \circ F) = (v^{ef})(r_2^e (r_3 \circ F))$$

por lo que $d = ef$ y se deduce el resultado. □

Usamos ahora el índice de ramificación para investigar el efecto de los mapas racionales en los divisores.

Definición 2.2.2. Supongamos que F es un mapa racional no constante. Definimos $F^* : \mathrm{Div}(E) \to \mathrm{Div}(E)$ el homomorfismo que cumple

$$F^*(\langle Q \rangle) = \sum_{F(P)=Q} e_F(P) \langle P \rangle$$

Proposición 2.2.4. *El homomorfismo F^* es inyectivo.*

Demostración: Supongamos que $F^*(\Delta) = F^*(\Delta')$ con $\Delta = \sum_P n(P)\langle P \rangle$ y $\Delta' = \sum_Q m(Q)\langle Q \rangle$,

$$\Delta'' = \sum_P n(P) F^*(P) = \sum_Q m(Q) F^*(Q)$$

Si $n(P) \neq 0$ y $F(R) = P$, existe Q con $m(Q) \neq 0$ tal que $F(R) = Q$, por lo que el coeficiente de $\langle R \rangle$ en Δ'' es por un lado $e_F(R)n(P)$, y $e_F(R)m(Q)$ y $n(P) = m(Q)$. Además $P = Q$ porque son $F(R)$, y $\Delta = \Delta'$

□

Proposición 2.2.5. *Si F es un mapa racional no constante y r es una función racional no nula. Se verifica*

$$\mathrm{div}(u \circ F) = F^*(\mathrm{div}(r))$$

Demostración:

$$\begin{aligned}
\operatorname{div}(r \circ F) &= \sum_P \operatorname{ord}_P(r \circ F)\langle P\rangle \\
&= \sum_P [\operatorname{ord}_{F(P)}(r)][e_F(P)]\langle P\rangle \\
&= \sum_Q \operatorname{ord}_Q(r) \left(\sum_{F(P)=Q} e_F(P)\langle P\rangle \right) \\
&= \sum_Q \operatorname{ord}_Q(R) F^*(\langle Q\rangle) \\
&= F^*(\operatorname{div}(r))
\end{aligned}$$

□

Lema 2.2.6. *Si F_1 y F_2 son mapas racionales no constantes $F_1 \circ F_2$ es un mapa racional no constante y para $P \in E(K)$*

$$e_{F_1 \circ F_2}(P) = e_{F_1}(F_2(P)) e_{F_2}(P)$$

Demostración: Como los mapas racionales son sobreyectivos $F_1 \circ F_2$ es no constante.

Sea u una variable unifomizadora en $F_1(F_2(P))$. Entonces

$$\begin{aligned}
e_{F_1 \circ F_2}(P) &= \operatorname{ord}_P(u \circ F_1 \circ F_2) \\
&= \operatorname{ord}_{F_2(P)}(u \circ F_1) e_{F_2}(P) \\
&= e_{F_1}(F_2(P)) e_{F_2}(P)
\end{aligned}$$

Proposición 2.2.7. *Si F_1 y F_2 son mapas racionales no constantes*

$$(F_1 \circ F_2)^* = F_2^* \circ F_1^*$$

Demostración:

$$\begin{aligned}
(F_2^* \circ F_1^*)(\langle R\rangle) &= F_2^* \left(\sum_{F_1(Q)=R} e_{F_1}(Q)\langle Q\rangle \right) \\
&= \sum_{F_1(Q)=R} e_{F_1}(Q) \cdot \sum_{F_2(P)=Q} e_{F_2}(P)\langle P\rangle \\
&= \sum_{(F_1 \circ F_2)(P)=R} e_{F_1}(F_2(P)) e_{F_2}(P)\langle P\rangle \\
&= \sum_{(F_1 \circ F_2)(P)=R} e_{F_1 \circ F_2}(P)\langle P\rangle \\
&= (F_1 \circ F_2)^*(\langle R\rangle)
\end{aligned}$$

□

2.3. Endomorfismos

Definición 2.3.1. Un mapa racional en E es una *endomorfismo* si además es un homomorfismo de grupos.

Estos mapas forman un grupo que denotamos $\mathrm{End}(E)$.

Ejemplo 2.3.1.

i. El mapa $[m]$ definido por $[m](P) = mp$ es claramente un endomorfismo.

ii. El mapa de Frobenius es también un endomorfismo. Esto se prueba igual que en 2.1, usando el binomio de Newton.

Teorema 2.3.1. *Si $\alpha : E(K) \to E(K)$ es un endomorfismo no nulo el índice de ramificación $e_\alpha(P)$ es independiente de P.*

Demostración: Sea $P \in E$, definimos $a\mathcal{T}_P$ de modo que $a\mathcal{T}_P(Q) = P + Q$. Como α es endomorfismo

$$(\alpha \circ a\mathcal{T}_P)(Q) = \alpha(P + Q) = \alpha(P) + \alpha(Q) = (a\mathcal{T}_{\alpha(P)} \circ \alpha)(Q)$$

Luego $\alpha \circ a\mathcal{T}_P = a\mathcal{T}_{\alpha(P)} \circ \alpha$. Aplicando el Lema 2.2.6 en el punto $\mathcal{O}$ obtenemos

$$e_\alpha(P) e_{\alpha \circ a\mathcal{T}_P}(\mathcal{O}) = e_{a\mathcal{T}_{\alpha(P)}}(\alpha(P)) e_\alpha(\mathcal{O})$$

Del Lema 1.7.4 vemos que el índice de ramificación de una traslación es 1 en cualquier punto. Si $P \in E(K)$ y u es una variable de uniformización en $a\mathcal{T}_P(Q) = P + Q$, $e_{a\mathcal{T}_P}(Q) = \mathrm{ord}_Q(u \circ a\mathcal{T}_P) = \mathrm{ord}_Q(T_P(u)) = 1$, ya que $T_P(u)$ es una variable de uniformización en $P + Q - P = Q$. Entonces $e_\alpha(P) = e_\alpha(\mathcal{O})$ para todo $P \in E(K)$. □

Definición 2.3.2. Si α es un endomorfismo en E, denotamos e_α como el valor constante de $e_\alpha(P)$ para $P \in E(K)$.

Lema 2.3.2. *Sean m un entero, r una función racional, y D la derivación de la sección 1.7. Se cumple que*

$$D(r \circ [m]) = (mDr) \circ [m]$$

Demostración: El lema es obvio para $m = 0$.

Si $r = x$, $r \circ [m] = g_m$, y por la Proposición 1.7.3 queda demostrado para $r = x$. Lo mismo pasa para $r = y$.

Se puede ver que las funciones racionales que cumplen la tesis del lema son cerradas por las operaciones $+, -, \times$ y división. Por lo que queda probado el lema para $m \geq 0$.

El caso $m = -1$ es fácil de verificar.

Si $m \geq 0$

$$\begin{aligned} D(f \circ [-m]) &= D(f \circ [m] \circ [-1]) \\ &= -D(f \circ [m]) \circ [-1] \\ &= (-m)Df \circ [-m] \end{aligned}$$

□

Proposición 2.3.3. *Si E esta definida sobre $k = \mathrm{GF}(q)$ y φ es el mapa de Frobenius, $e_\varphi = q$.*

Demostración: Sabemos que $e_\varphi = e_\varphi(\mathcal{O})$. Como $u = x/y$ es una variable de uniformización en $\mathcal{O}$, $u \circ \varphi = u^q$, y por la definición de grado se deduce el resultado. □

Definición 2.3.3. Sea $\alpha : E(K) \to E(K)$ un endomorfismo. Si $e_\alpha = 1$, decimos que α es *separable*. Si $e_\alpha > 1$ decimos que es *inseparable*.

Lema 2.3.4. *Si r es una función racional en x y $r_x = 0$ entonces $r(x) = \tilde{r}(x^p)$, donde $\tilde{r}$ es una función racional en x.*

Demostración: Si $r(x) = a_n x^n + \cdots + a_1 x + a_0$ es un polinomio y $r_x(x) = n a_n x^{n-1} + \cdots + a_1 = 0$, luego si $1 \leq k \leq n$, $a_k = 0$ o $k \equiv 0 \pmod{p}$, porque estamos trabajando en característica p. Por lo tanto $r(x) = a_{pm} x^{pm} + a_{p(m-1)} x^{p(m-1)} + \cdots + a_p x^p + a_0$, para algún m entero, que es un polinomio en x^p. Escribimos $r = f/g$ con f y g polinomios en x coprimos. Que $r_x = 0$ implica que $f_x g = f g_x$ y como f y g son coprimos $f | f_x$ y $g | g_x$. Claramente $f_x = g_x = 0$, y f y g son polinomios en x^p. □

Proposición 2.3.5. *Sea una función racional r en E tal que $Dr = 0$, existe una función racional $\tilde{r}$ tal que $r(x, y) = \tilde{r}(x^p, y^p)$.*

Demostración: Primero notamos que

$$y^p = y(y^2)^{\frac{p-1}{2}} = y s(x)^{\frac{p-1}{2}}$$

donde $s(x) = x^3 + Ax + B$. Por lo tanto r tiene una única representacion

$$r(x, y) = u(x) + y^p v(x)$$

donde u y v son funciones racionales en x. Si $Dr = 0$ tenemos que

$$[u_x(x) + y^p v_x(x)] 2y = 0$$

Deducimos entonces que $u_x = v_x = 0$, y el por el lema anterior se cumple la tesis. □

Proposición 2.3.6. *Si α es un endomorfismo, α es inseparable si y solo si $D(r \circ \alpha) = 0$ para toda r función racional.*

Demostración: Si $D(r \circ \alpha) = 0$ para toda r función racional, por lo que en particular lo es para u variable uniformizadora en $\alpha(P)$ para algún P. Entonces $(u \circ \alpha)(P) = 0$ y $D(u \circ \alpha) = 0 \Rightarrow \mathrm{ord}_P(u \circ \alpha) > 1 \Rightarrow e_\alpha = e_\alpha(P) > 1$.

Supongamos que ahora que existe una función racional r y un punto P tal que

$$[D(r \circ \alpha)](P) \neq 0$$

Sea $w = r - r(\alpha(P))$. Luego $(w \circ \alpha)(P) = 0$ y

$$[D(w \circ \alpha)](P) = [D(r \circ \alpha)](P) \neq 0$$

en ese caso $w \circ \alpha$ tiene un cero de multiplicidad uno en P. Se deduce que

$$1 = \operatorname{ord}_P(w \circ \alpha) = [\operatorname{ord}_{\alpha(P)} w]e_\alpha$$

y vemos que $e_\alpha = 1$. □

Corolario 2.3.7. *Un endomorfismo α es inseparable si y solo si*

$$\alpha(x, y) = (u(x^p, y^p), v(x^p, y^p))$$

con u y v funciones racionales.

Demostración: Por las proposiciones anteriores sabemos que si α es inseparable $D(x \circ \alpha) = D(y \circ \alpha) = 0$ y $(x \circ \alpha)(x, y) = u(x^p, y^p)$ $(y \circ \alpha)(x, y) = v(x^p, y^p)$. Luego $\alpha(x, y) = (x \circ \alpha, y \circ \alpha)(x, y) = (u(x^p, y^p), v(x^p, y^p))$

Si $\alpha(x, y) = (u(x^p, y^p), v(x^p, y^p))$, $D(x \circ \alpha) = 0$ y $D(y \circ \alpha) = 0$ y eso implica que $D(r \circ \alpha) = 0$ para toda función racional en E, y α es inseparable. □

Corolario 2.3.8. *Si m es un entero coprimo con p, $[m]$ es un endomorfismo separable.*

Demostración: Sea $P \in E(K)$ y u variable de uniformización en $[m](P) = mp$. Por el lema 2.3.2

$$D(u \circ [m])(P) = (mDu)(mP) \neq 0$$

y por la Proposición anterior $[m]$ es separable □

Proposición 2.3.9. *Si α y β son dos Endomorfismos inseparables, también lo es $\alpha + \beta$.*

Demostración: Es inmediato a partir del Corolario 2.3.7. □

Proposición 2.3.10. *Si E esta definida sobre $k = \mathrm{GF}(q)$ y m, n son enteros con m coprimo con p, el endomorfismo $[m] + [n] \circ \varphi$ es separable, donde φ es el mapa de Frobenius.*

Demostración: Sea $\alpha = [m] + [n] \circ \varphi$, si α es inseparable $[m] = \alpha - [n] \circ \varphi$. Como $[m]$ es la suma de dos Endomorfismos, el segundo porque $e_\varphi = q$ y $e_{[n]\circ\varphi} = e_{[n]}e_\varphi > 0$, por la Proposición anterior será inseparable contradiciendo el Corolario 2.3.8. □

Definición 2.3.4. Supongamos que α en un morfismo no nulo. Sea $|\ker \alpha|$ la cantidad de elementos en el núcleo de α. Definimos el *grado* de α como

$$\mathrm{gr}(\alpha) = |\ker \alpha| e_\alpha$$

Proposición 2.3.11.

i. Si m y p son coprimos, $\mathrm{gr}([m]) = m^2$.

ii. Si E esta definida sobre $\mathrm{GF}(q)$ *el grado del mapa de Frobenius es q.*

iii. Si α y β son dos Endomorfismos no nulos,

$$\mathrm{gr}(\alpha \circ \beta) = \mathrm{gr}(\alpha)\,\mathrm{gr}(\beta)$$

iv. Si α es un endomorfismo no nulo y $\Delta \in \mathrm{Div}(E)$,

$$\mathrm{gr}(\alpha^*(\Delta)) = \mathrm{gr}(\alpha)\,\mathrm{gr}(\Delta)$$

Demostración:

i. Sabemos que $e_{[m]} = 1$ porque $[m]$ es separable, y $|ker[m]| = m^2$ como vimos en 1.7.6. Entonces $\mathrm{gr}([m]) = 1 \cdot m^2 = m^2$.

ii. Por la Proposición 2.3.3 $e_\varphi = q$, y claramente $\ker\varphi = \{\mathcal{O}\}$ por lo tanto $|ker\varphi| = 1$.

iii. Por definición $\mathrm{gr}(\alpha\circ\beta) = |ker(\alpha\circ\beta)|e_{\alpha\circ\beta} = |ker(\alpha\circ\beta)|e_\alpha e_\beta$, falta probar que $|ker(\alpha\circ\beta)| = |ker\alpha||ker\beta|$.

Primero probaremos que dado $Q \in E(K)$ la cantidad de elementos de $L = \{P : \gamma(P) = Q\}$ es $|\ker\gamma|$ donde γ es un endomorfismo en E. Para probarlo sabemos que existe $R \in E(K)$ tal que $\gamma(R) = Q$ ya que γ es sobreyectivo. Entonces $\gamma(P) = Q$ si y solo si $\gamma(P - R) = \gamma(P) - Q = \mathcal{O}$. Encontramos una biyección entre L y $|\ker\gamma|$. Si $\ker\alpha = \{P_1, P_2, \cdots, P_n\}$ y $\ker\beta = \{Q_1, Q_2, \cdots, Q_m\}$. Sabemos que existen R_i tales que $\beta(R_i) = P_i$ por la sobreyectividad de β. Por lo visto anteriormente $\ker(\alpha\circ\beta) = \{Q_i + R_j : i = 1,\ldots,m \;\; j = 1,\ldots,n\}$, ya que si $(\alpha\circ\beta)(P) = \mathcal{O} \Rightarrow \beta(P) = P_{i_0}$ $\Rightarrow P = R_{i_0} + Q_j$ por la biyección vista anteriormente.

iv. Primero lo probamos para $\Delta = \langle P\rangle$.

$$\begin{aligned}\mathrm{gr}(\alpha^*\langle P\rangle) &= \mathrm{gr}\left(\sum_{\alpha(Q)=P} e_\alpha(Q)\langle Q\rangle\right)\\ &= e_\alpha\,\mathrm{gr}\left(\sum_{\alpha(Q)=P}\langle Q\rangle\right) = e_\alpha|\ker\alpha|\end{aligned}$$

donde la ultima igualdad la probamos en el punto anterior. Si el divisor $\Delta = \sum_P n(P)\langle P\rangle$

$$\mathrm{gr}(\alpha^*\Delta) = \mathrm{gr}\left(\sum_P n(P)\langle P\rangle\right) = \sum_P n(P)\,\mathrm{gr}(\alpha^*\langle P\rangle) = \mathrm{gr}(\alpha)\,\mathrm{gr}(\Delta)$$

□

Proposición 2.3.12. *Sea α un endomorfismo no nulo. Para $P \in E(K)$, sea P_0 tal que $\alpha(P_0) = P$,*

$$\mathrm{suma}[\alpha^*\langle P\rangle - \alpha^*\langle\mathcal{O}\rangle] = (\mathrm{gr}\,\alpha)P_0$$

Demostración: Tenemos que

$$\alpha^*\langle P\rangle = e_\alpha \sum_{\alpha(Q)=P} \langle Q\rangle = e_\alpha \sum_{\alpha(R)=\mathcal{O}} \langle P_0 + R\rangle$$

Luego

$$\begin{aligned}
\operatorname{suma}[\alpha^*\langle P\rangle - \alpha^*\langle\mathcal{O}\rangle] &= \operatorname{suma}\left[e_\alpha \sum_{\alpha(R)=\mathcal{O}} (\langle P_0 + R\rangle - \langle R\rangle)\right] \\
&= e_\alpha \sum_{\alpha(R)=\mathcal{O}} P_0 \\
&= e_\alpha |\ker\alpha| P_0 \\
&= (\operatorname{gr}\alpha) P_0
\end{aligned}$$

□

2.4. El pairing de Weil

Fijemos un entero m coprimo con p.

Lema 2.4.1. *Para $T \in E[m]$, el divisor $[m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)$ es principal.*

Demostración: Como $\operatorname{gr}(\langle T\rangle - \langle\mathcal{O}\rangle) = 0$

$$\operatorname{gr}([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)) = \operatorname{gr}[m]\operatorname{gr}(\langle T\rangle - \langle\mathcal{O}\rangle) = 0$$

por la Proposición 2.3.11 parte iv.

Sea ahora T_0 tal que $mT_0 = [m](T_0) = T$. Luego $\operatorname{suma}([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle) = gr([m])T_0 = m^2T_0$ por la Proposición 2.3.12, y $m^2T_0 = mT = \mathcal{O}$. □

Sea g_T una función racional tal que

$$\operatorname{div}(g_T) = [m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)$$

que sabemos que existe porque $\operatorname{gr}([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)) = 0$ y $\operatorname{suma}([m]^*(\langle T\rangle - \langle\mathcal{O}\rangle)) = \mathcal{O}$. A pesar de que g_T no es único, es único salvo multiplicación de escalares.

Recordemos que $a\mathcal{T}_P$ es la traslación por P. Vemos fácilmente que

$$a\mathcal{T}_P^*(\langle Q\rangle) = \sum_{a\mathcal{T}_P(R)=Q} e_a\mathcal{T}_P(R)\langle Q\rangle = \langle Q - P\rangle$$

ya que $a\mathcal{T}_P$ es una biyección y $e_{a\mathcal{T}_P}(Q) = 1$ para todo $Q \in E(K)$.

Lema 2.4.2. *Sean $S, T \in E[m]$,*

$$\operatorname{div}(g_T \circ a\mathcal{T}_S) = \operatorname{div}(g_T)$$

Demostración: Como $S \in E[m]$, $[m] \circ a\mathcal{T}_S = [m]$. Usando las Proposiciones 2.2.5 y 2.2.7

$$\begin{aligned} \operatorname{div}(g_T \circ a\mathcal{T}_S) &= a\mathcal{T}_S^*(\operatorname{div}(g_T)) \\ &= (a\mathcal{T}_S^* \circ [m]^*)(\langle T\rangle - \langle \mathcal{O}\rangle) \\ &= ([m] \circ a\mathcal{T}_S)^*(\langle T\rangle - \langle \mathcal{O}\rangle) \\ &= [m]^*(\langle T\rangle - \langle \mathcal{O}\rangle) \\ &= \operatorname{div}(g_T) \end{aligned}$$

Proposición 2.4.3. *Sean $S, T \in E[m]$. La función $(g_T \circ a\mathcal{T}_S)/g_T$ es constante, y su valor es una raíz m-esima de la unidad en K, además es independiente de la elección de la función g_T.*

Demostración: Sabemos por el lema anterior que $(g_T \circ a\mathcal{T}_S)/g_T$ es contante y $((g_T \circ a\mathcal{T}_S)/g_T)(\mathcal{O}) = g_T(P)/g_T(\mathcal{O})$ que no depende de g_T porque es único salvo multiplicación por constantes

Existe $\zeta \in E[K]$ tal que $g_T \circ a\mathcal{T}_S = \zeta g_T$. Componiendo repetidamente con $a\mathcal{T}_S$ vemos que

$$g_t \circ a\mathcal{T}_S^i = \zeta^i g_T$$

Tomando $i = m$ deducimos que $\zeta^m = i$, ya que $a\mathcal{T}_S^m$ es el mapa identidad. □

Definición 2.4.1. Sean $T, S \in E[m]$ y sea μ_m el grupo de m-raíces de la unidad en K. El mapa de $E[m] \times E[m]$ en μ_m que manda (S, T) en $(g_T \circ a\mathcal{T}_S)/g_T$ es llamado el pairing de Weil, y lo denotamos por

$$w(S, T) = \frac{g_T \circ a\mathcal{T}_S}{g_T}$$

Teorema 2.4.4. *Sean $S_1, S_2, S, T_1, T_2, T \in E[m]$. El pairing Weil satisface las siguientes propiedades:*

i. $w(S_1 + S_2, T) = w(S_1, T)w(S_2, T)$.

ii. $w(S, T_1 + T_2) = w(S, T_1)w(S, T_2)$.

iii. $w(T, T) = 1$

iv. Si $w(S, T) = 1$ para todo $S \in E[m]$ entonces $T = \mathcal{O}$.

v. Si α es un endomorfismo

$$w(\alpha(S), \alpha(T)) = w(S, T)^{\operatorname{gr}\alpha}$$

Demostración:

i. Por definición

$$\begin{aligned} w(S_1+S_2,T) &= \left(\frac{g_t\circ a\mathcal{T}_{S_1+S_2}}{g_T}\right)(P) \\ &= \frac{(g_T\circ a\mathcal{T}_{S_1})(S_2+P)}{g_T(P)} \\ &= \frac{(g_T\circ a\mathcal{T}_{S_1})(S_2+P)}{g_T(S_2+P)}\frac{g_T(S_2+P)}{g_T(P)} \\ &= w(S_1,T)\left(\frac{g_T\circ a\mathcal{T}_{S_2}}{g_T}\right)(P) \\ &= w(S_1,T)w(S_2,T) \end{aligned}$$

ii. Primero observamos que

$$\operatorname{div}\left(\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\right) = [m]^*(\langle T_1+T_2\rangle - \langle T_1\rangle - \langle T_1\rangle + \langle\mathcal{O}\rangle)$$

Claramente $\langle T_1+T_2\rangle - \langle T_1\rangle - \langle T_1\rangle + \langle\mathcal{O}\rangle$ es principal, ya que tiene grado cero y suma $\mathcal{O}$. Sea h una función con ese divisor,

$$\operatorname{div}\left(\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\right) = [m]^*(\operatorname{div}(h)) = \operatorname{div}(h\circ[m])$$

y vemos que

$$\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}} = c\cdot h\circ[m]$$

para algún $c\in K$. Luego si $S\in E[m]$,

$$\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\circ a\mathcal{T}_S(P) = (c\cdot h\circ[m])(P+S) = (c\cdot h\circ[m])(P) = \frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}(P)$$

entonces $\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}$ es invariante bajo traslación de elementos de $E[m]$. Se verifica

$$\begin{aligned} w(S,T_1+T_2) &= \frac{g_{T_1+T_2}\circ a\mathcal{T}_S}{g_{T_1+T_2}} \\ &= \frac{g_{T_1+T_2}\circ a\mathcal{T}_S}{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}\frac{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}{g_{T_1+T_2}} \\ &= \frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\circ a\mathcal{T}_S\frac{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}{g_{T_1+T_2}} \\ &= \frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\frac{(g_{T_1}\circ a\mathcal{T}_S)(g_{T_2}\circ a\mathcal{T}_S)}{g_{T_1+T_2}} \\ &= w(S,T_1)w(S,T_2) \end{aligned}$$

iii. Sea $T_0\in E(K)$ tal que $mT_0 = T$. usando las Proposiciones 2.2.5,2.2.7 y la demostración del Lema 2.4.1

$$\begin{aligned} \operatorname{div}(g_T\circ a\mathcal{T}_{iT_0}) &= a\mathcal{T}^*_{iT_0}(\operatorname{div} g_T) \\ &= a\mathcal{T}^*_{iT_0}\circ[m]^*(\langle T\rangle - \langle\mathcal{O}\rangle) \\ &= ([m]\circ a\mathcal{T}_{iT})^*(\langle T\rangle - \langle\mathcal{O}\rangle) \\ &= (a\mathcal{T}_{iT_0}\circ[m])^*(\langle T\rangle - \langle\mathcal{O}\rangle) \\ &= [m]^*\circ a\mathcal{T}^*_{iT}(\langle T\rangle - \langle\mathcal{O}\rangle) \\ &= [m]^*(\langle(1-i)T\rangle - \langle -iT\rangle) \end{aligned}$$

Deducimos que el de

$$G = g_T(g \circ a\mathcal{T}_{T_0})(g \circ a\mathcal{T}_{2T_0}) \cdots (g \circ a\mathcal{T}_{(m-1)T_0})$$

es

$$\begin{aligned}[m]^*[(\langle T\rangle - \langle \mathcal{O}\rangle) \quad &+ \quad (\langle \mathcal{O}\rangle - \langle -T\rangle) + (\langle -T\rangle - \langle -2T\rangle) \\ &+ \quad \cdots + (\langle (2-m)T\rangle - \langle (1-m)T\rangle)\end{aligned}$$

que es cero ya que $T \in E[m]$. Por lo tanto G es una constante, y si la componemos con $a\mathcal{T}_{T_0}$ obtendremos la misma constante G. Luego

$$g_T(g \circ a\mathcal{T}_{T_0}) \cdots (g \circ a\mathcal{T}_{(m-1)T_0}) = (g \circ a\mathcal{T}_{T_0})(g \circ a\mathcal{T}_{2T_0}) \cdots (g \circ a\mathcal{T}_{mT_0})$$

y despues de cancelar obtenemos

$$g_T = g_t \circ a\mathcal{T}_{mT_0} = g_T \circ a\mathcal{T}_T$$

y $w(T,T) = (g_T \circ a\mathcal{T}_T)/g_T = 1$.

iv. Supongamos que $T \in E[m]$ y que $w(S,T) = 1$ para todo $S \in E[m]$. Esto implica que $g_T \circ a\mathcal{T}_S = g_T$, o sea que g_T es invariante bajo traslaciones por elementos de $E[m]$. Usamos ahora el siguiente Lema, y su prueba la daremos luego.

Lema 2.4.5. *Supongamos que r es una función racional en E tal que es invariante bajo traslaciones por elementos de $E[m]$. Se cumple que $r = t \circ [m]$ para alguna función racional t.*

Vemos que $g_T = h \circ [m]$ para alguna función racional r. Pero

$$[m]^*(\mathrm{div}(h)) = \mathrm{div}(g_T) = [m]^*(\langle T\rangle - \langle \mathcal{O}\rangle)$$

Y por la Proposición 2.2.4, vemos que $\langle T\rangle - \langle \mathcal{O}\rangle = \mathrm{div}(h)$ que es un divisor principal. Luego T debe de ser $\mathcal{O}$ ya que $\mathcal{O} = \mathrm{suma}(\mathrm{div}(h)) = T - \mathcal{O}$.

v. Queremos probar que

$$\left(\frac{g_T \circ a\mathcal{T}_S}{g_T}\right)^{gr\alpha} = \frac{g_{\alpha(T)} \circ a\mathcal{T}_{\alpha(S)}}{g_{\alpha(T)}}$$

Pero vemos que $a\mathcal{T}_{\alpha(S)} \circ \alpha = \alpha \circ a\mathcal{T}_S$. Si componemos α en el lado derecho de la ecuación anterior, que es constante y queda igual, obtenemos

$$\frac{g_{\alpha(T)} \circ \alpha \circ a\mathcal{T}_S}{g_{\alpha(T)} \circ \alpha}$$

Reescribiendo lo que queremos demostrar, obtenemos

$$\frac{g_T^{\mathrm{gr}\,\alpha} \circ a\mathcal{T}_S}{g_T^{\mathrm{gr}\,\alpha}} = \frac{g_{\alpha(T)} \circ \alpha \circ a\mathcal{T}_S}{g_{\alpha(T)} \circ \alpha}$$

que es equivalente a probar

$$\left(\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\mathrm{gr}\,\alpha}}\right) \circ a\mathcal{T}_S = \frac{g_{\alpha(T)} \circ \alpha}{g_T^{\mathrm{gr}\,\alpha}}$$

Debemos por lo tanto probar que

$$\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\operatorname{gr}\alpha}}$$

es invariante con las traslaciones de elementos de $E[m]$.

Como α es un endomorfismo, α conmuta con $[m]$, y α^* conmuta con $[m]^*$. Luego

$$\begin{aligned}\operatorname{div}\left(\frac{g_T \circ a\mathcal{T}_S}{g_T}\right) &= \alpha^* \circ [m]^*(\langle T\rangle - \langle\mathcal{O}\rangle) - \operatorname{gr}(\alpha)[m]^*(\langle T\rangle - \langle\mathcal{O}\rangle) \\ &= [m]^*[\overbrace{\alpha^*(\langle\alpha(T)\rangle - \langle\mathcal{O}\rangle) - \operatorname{gr}(\alpha)(\langle T\rangle - \langle\mathcal{O}\rangle)}^{:=\Upsilon\in\operatorname{Div}(E)}]\end{aligned}$$

Vamos a probar que Υ es principal. Como

$$\operatorname{gr}(\alpha^*(\Delta)) = \operatorname{gr}\alpha\operatorname{gr}\Delta$$

para $\Delta \in \operatorname{Div}(E)$, el grado de Υ es cero. Por lo proposición 2.3.12,

$$\operatorname{suma}(\alpha^*(\langle\alpha(T)\rangle - \langle\mathcal{O}\rangle)) = \operatorname{gr}(\alpha)T$$

que cancela suma aplicada al segundo termino de Υ. Si $\operatorname{div}(h) = \Upsilon$ con h función racional,

$$\operatorname{div}\left(\frac{g_T \circ a\mathcal{T}_S}{g_T}\right) = [m]^*(\operatorname{div}(h)) = \operatorname{div}(h \circ [m])$$

Vemos entonces que

$$\operatorname{div}\left(\frac{g_T \circ a\mathcal{T}_S}{g_T}\right)$$

es invariante bajo traslaciones por elementos de $E[m]$.

□

Demostración Lema 2.4.5*:* Sea H el cuerpo de funciones racionales en E que son invariantes bajo traslaciones de elementos de $E[m]$. Sea también el cuerpo

$$J = \{g \circ [m] : g \in K(E)\}$$

Tenemos claramente

$$J \subset H \subset K(E)$$

H es el cuerpo fijo de $W = \{\mathcal{T}_S : S \in E[m]\}$, con $\mathcal{T}_S(g) = g \circ a\mathcal{T}_S$. Por la teoría de Galois sabemos que $[E(K) : H]$, o sea la dimensión de $E(K)$ como H-espacio vectorial, es igual a la cantidad de elementos del grupo W, que es m^2. Vamos a probar que $[E(K) : J] \leq m^2$, y como $[E(K) : J] = [E(K) : H][H : J] = m^2[H : J]$ vemos que $H = J$.

Consideremos el subcuerpo

$$J(x) = \{\phi(x)/\varphi(x) : \phi, \varphi \in J[X],\ \varphi(x) \neq 0\} \subset K(E)$$

Como $g_m = x \circ [m]$ y $h_m = y \circ [m]$ vemos que g_m y h_m están en J. Por la Proposición 1.6.4, $h_m = y\tilde{h}_m$ donde $\tilde{h}_m$ es una función es x. Entonces $y = h_m/\tilde{h}_m$ y $K(E) = J(x)$.

Si probamos que x es cero de un polinomio de $J[X]$ de grado m^2, el conjunto $\{1, x, x^2, \ldots, x^{m^2}\}$ será linealmente dependiente en $K(E) = J(x)$ como J espacio vectorial y sabemos que $\{1, x, \ldots, x^{[K(E):J]}\}$ es base, entonces $[K(E) : J] \leq m^2$. Recordemos la ecuación

$$g_m = x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}$$

o

$$x\psi_m^2 - \psi_{m-1}\psi_{m+1} - \psi_m^2 g_m = 0$$

Por la Proposición 1.8.1 ii. iii. ψ_m^2 y $\psi_{m-1}\psi_{m+1}$ son polinomios en x, de grados en x m^2-1 y m^2 respectivamente. Además, como el coeficiente principal de ψ_n es n, el coeficiente en x^{m^2} de $x\psi_m^2 - \psi_{m-1}\psi_{m+1}$ es $m^2-(m-1)(m+1) = 1$. Luego x satisface el polinomio de grado m^2

$$X\psi_m^2(X) - \psi_{m-1}(X)\psi_{m+1}(X) - g_m(X)\psi_m^2(X) = 0$$

en $J[X]$. □

Corolario 2.4.6. *Para $S, T \in E[m]$ se cumple que $w(S,T) = w(T,S)^{-1}$.*

Demostración: Sabemos que

$$1 = w(S+T, S+T) = w(S,T)w(S,S)w(T,T)w(T,S) = w(T,S)w(S,T)$$

Y se cumple la tesis. □

Observación 2.4.1. Si m no es primo entonces $\mathbb{Z}/m\mathbb{Z}$ no es un cuerpo, y $E[m]$ no es un espacio vectorial. Pero si es un módulo libre sobre $\mathbb{Z}/m\mathbb{Z}$ de rango 2 ya que por 1.7.7 $E[m]$ es isomorfo como grupo a $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Corolario 2.4.7. *Sea $\{T_1, T_2\}$ una base de $E[m]$ como $\mathbb{Z}/m\mathbb{Z}$ módulo, $w(T_1, T_2)$ es una m-raíz primitiva de la unidad en K.*

Demostración: Supongamos que $w(T_1, T_2)^n = 1$. Luego $w(nT_1, T_2) = 1$. Y si $c_1, c_2 \in \mathbb{Z}$, $w(nT_1, c_1T_1 + c_2T_2) = w(T_1, T_1)^{nc_1}w(nT_1, T_2)^{c_2} = 1$. Luego $nT_1 = \mathcal{O}$ y m divide a n. □

Teorema 2.4.8. *Sea α un endomorfismo no nulo entonces $\alpha(E[m]) \subset E[m]$. Además el discriminante de α en $E[m]$ es* $\mathrm{gr}(\alpha) \mod m$.

Demostración: Sean T_1 y T_2 una base de $E[m]$ sobre $\mathbb{Z}/m\mathbb{Z}$. Existen enteros módulo m, a_{ij} con $i, j = 1, 2$, tales que

$$\alpha(T_i) = \sum_{j=1}^{2} a_{ij}T_j$$

y $\det(\alpha) = a_{11}a_{22} - a_{12}a_{21}$.

Tenemos que

$$\begin{aligned} w(T_1,T_2)^{\operatorname{gr}\alpha} &= w(\alpha(T_1),\alpha(T_2)) \\ &= w(a_{11}T_1+a_{12}T_2, a_{21}T_1+a_{22}T_2) \\ &= w(T_1,T_1)^{a_{11}a_{12}}\cdot w(T_1,T_2)^{a_{11}a_{22}} \\ &\quad \cdot w(T_2,T_1)^{a_{12}a_{21}}\cdot w(T_2,T_2)^{a_{12}a_{22}} \\ &= w(T_1,T_2)^{a_{11}a_{22}} w(T_1,T_2)^{-a_{12}a_{21}} \\ &= w(T_1,T_2)^{a_{11}a_{22}-a_{12}a_{21}} \\ &= w(T_1,T_2)^{\det(\alpha)} \end{aligned}$$

y como $w(T_1,T_2)$ es una m-raíz primitiva de la unidad $\det(\alpha) \equiv gr(\alpha) \mod m$. □

Lema 2.4.9. *Sean A y B matrices 2×2 con entradas en un anillo conmutativo R. Para $c_1, c_2 \in R$ se cumple*

i. $\det(c_1A + c_2B) = c_1^2 \det A + c_2^2 \det B + c_1c_2[\det(A+B) - \det A - \det B]$

ii. $\operatorname{tr} A = 1 + \det A - \det(I - A)$

Demostración: Si

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

entonces

$$\begin{aligned} \det(c_1A+c_2B) &= (c_1a+c_2e)(c_1d+c_2h) - (c_1c+c_2g)(c_1b+c_2f) \\ &= c_1^2(ad-eb) + c_2^2(eh-gf) + c_1c_2(ah+ed-gb-gf) \\ &= c_1^2\det A + c_2^2 \det B + c_1c_2[\det(A+B) - \det A - \det B] \end{aligned}$$

ya que

$$\begin{aligned} \det(A+B) - \det A - \det B &= ad+ah+ed+eh-bc-bg-fc-fg \\ &\quad -ad+bc-eh+fg \\ &= ah+ed-gb-gf \end{aligned}$$

lo que prueba i.

Probamos ahora ii.

$$\begin{aligned} \det A - \det(I-A) &= ad-cb \\ &\quad -1+a+d-ad+bc \\ &= a+d-1 \\ &= \operatorname{tr} A - 1 \end{aligned}$$

Teorema 2.4.10. *Si α y β son Endomorfismos,*

$$\operatorname{gr}(c_1\alpha + c_2\beta) = c_1^2 \operatorname{gr}\alpha + c_2^2 \operatorname{gr}\beta + c_1c_2[\operatorname{gr}(\alpha+\beta) - \operatorname{gr}\alpha - \operatorname{gr}\beta]$$

Demostración: Sea m un entero comprimo con p. Si restringimos α y β a $E[m]$, por el Teorema 2.4.8 y el lema anterior

$$\begin{aligned}\operatorname{gr}(c_1\alpha + c_2\beta) &\equiv \det(c_1\alpha + c_2\beta) \\ &\equiv c_1^2 \det\alpha + c_2^2 \det\beta + c_1c_2[\det(\alpha+\beta) - \det\alpha - \det\beta] \\ &\equiv c_1^2 \operatorname{gr}\alpha + c_2^2 \operatorname{gr}\beta + c_1c_2[\operatorname{gr}(\alpha+\beta) - \operatorname{gr}\alpha - \operatorname{gr}\beta] \quad \text{mód } m\end{aligned}$$

Entonces se cumple la igualdad porque la equivalencia se cumple para todo m coprimo con p. Si $a \equiv b \mod m$, con $m > 0$, $a - b = km$, sea $q = pkm + 1$ coprimo con pkm mayor que uno si $pkm \neq 0$, $a - b = lq$. Por lo que $km = lq$ y como q no divide km l si, si $l = kms$ $qs = 1$ y $q = 1$. Por lo que $pkm = 0$ y $k = 0$, y $a = b$. □

Teorema 2.4.11. *Si α es un endomorfismo,*

$$\beta = \alpha \circ \alpha - [1 + \operatorname{gr}\alpha - \operatorname{gr}(1-\alpha)] \circ \alpha - [\operatorname{gr}\alpha] = \mathcal{O}_M$$

Demostración: Cuando nos restringimos a $E[m]$, vemos que β es

$$\alpha \circ \alpha - [1 + \operatorname{gr}\alpha - \operatorname{gr}(1-\alpha)] \circ \alpha - [\operatorname{gr}\alpha] = \alpha \circ \alpha - [tr\alpha] \circ \alpha - \det\alpha$$

Por el teorema de Cayley-Hamilton toda matriz A cumple

$$A^2 - (\operatorname{tr} A)A + \det A = 0$$

Luego β restricto a $E[m]$ es cero. Y como esto se cumple para todo m coprimo con p, β es $\mathcal{O}_M$. □

Teorema 2.4.12 (Hasse)**.** *Sea $t = q + 1 - E_q$. Se cumple*

i. $\varphi \circ \varphi - [t] \circ \varphi + [q] = \mathcal{O}_M$

ii. $|t| \leq 2\sqrt{q}$

Demostración: Primero notemos que $\ker(1-\varphi)$ es el conjunto de $(a,b) \in E(K)$ con $(a,b) = (a^q, b^q)$ y el punto $\mathcal{O}$. Por la Proposición 2.1.2 sabemos que $\ker(1-\varphi)$ es el conjunto de puntos k-racionales de E, luego $|\ker(1-q)| = E_q$.

También por la Proposición 2.3.10 sabemos que $1 - \varphi$ es separable, por la definición de grado, $\operatorname{gr}(1-\varphi) = E_q$. Como $\operatorname{gr}\varphi = q$ por 2.3.11 i., ii. es consecuencia del Teorema 2.4.11.

Para probar ii., vemos que

$$c_1^2 + c_2^2 q + c_1c_2(E_q - 1 - q) = \operatorname{gr}(c_1[1] - c_2\varphi) \geq 0$$

para todo $c_1, c_2 \in \mathbb{Z}$, por el Teorema 2.4.10, ya que $\operatorname{gr}[1] = 1$. Luego

$$\left(\frac{c_1}{c_2}\right)^2 + q + \left(\frac{c_1}{c_2}\right)(E_q - 1 - q) = \left(\frac{1}{c_2}\right)^2 \operatorname{gr}(c_1[1] - c_2\varphi) \geq 0$$

para todo racional c_1/c_2. Ahora

$$v^2 + vt + q \geq 0$$

para todo v real. El discriminante del polinomio cuadrático en la izquierda de la ecuación anterior debe ser no positivo. Por lo tanto como el discriminante es $t^2 - 4q$, tenemos que $|t| \leq 2\sqrt{q}$. □

Capítulo 3

Algoritmos para contar puntos

Presentaremos ahora algoritmos para contar la cantidad de puntos en una curva elíptica E sobre el cuerpo $\mathbb{F}_p$. O lo que es lo mismo, encontrar los números enteros a_p tales que

$$|E(\mathbb{F}_p)| = p + 1 - a_p$$

Primero mostraremos un algoritmo fácil para hallar los a_p.

Supongamos que tenemos una curva elíptica E dada por la ecuación

$$y^2 = x^3 + ax + b \text{ con } a, b \in \mathbb{Z}$$

La curva tiene siempre un punto en el infinito, $\mathcal{O}$, y luego para cada $x \in \mathbb{F}_p$ hay $1 + \left(\frac{x^3+ax+b}{p}\right)$ valores para y que son solución de la curva. Donde

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{p} \\ +1 & \text{si } a \not\equiv 0 \pmod{p} \text{ y } x^2 \equiv a \pmod{p} \text{ para algún } x \in \mathbb{Z} \\ -1 & \text{si no existe un tal } x \end{cases}$$

llamado el *Símbolo de Legendre*. Entonces $|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3+ax+b}{p}\right)$, resultando la formula

$$a_p = -\sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$

Esta formula nos da un algoritmo en $O(p^{1+o(1)})$ para calcular a_p, que es útil para p pequeño.

3.1. Algoritmo de Shanks

Daremos ahora la versión mas general del Algoritmo de Shanks.

Sea G un grupo abeliano finito, y g un elemento de el. Queremos encontrar el orden de g en G, o sea el mas pequeño n tal que g^n es el neutro de G. Una manera de hacer esto es calcular $g, g^2, g^3, \ldots$, hasta que obtengamos 1. Este algoritmo toma $O(n)$ operaciones de grupo. En algunos casos es lo mejor que podemos hacer.

Pero en muchos casos conocemos una cota superior B de n, y podemos aplicar la estrategia baby-step giant-step de Shanks para hallar n.

Procedemos de la siguiente manera. Sea $q = \left\lceil \sqrt{B} \right\rceil$. Primero calculamos $1, g, g^2, \ldots, g^{q-1}$, los llamados baby-steps y definimos $g_1 = g^{-q}$. El orden n de g es escrito como $n = aq + r$, con $0 \leq r < q$, y por la elección de q tenemos que $a \leq q$, ya que de lo contrario tendríamos que $n = aq + r > q^2 + r \geq B + r \geq n + r$ por lo que $0 > r$.

Luego, para $a = 1, \ldots, q$ calculamos g_1^a, que serian los giant-steps, y verificamos si esta en el conjunto $1, g, \ldots, g^{q-1}$. Si esta, tenemos que que $g^{aq+r} = 1$, luego n es un divisor de $aq + r$ y factorizando podremos hallar n. Este método requiere $O(B^{1/2})$ operaciones de grupo, que es menor que $O(n)$ si B es una cota razonable.

Hay que tener en cuenta que hay que buscar al menos q veces en una lista de q elementos. Si esto lo hacemos de una manera ingenua, tomara $O(q^2) = O(B)$ comparaciones, e incluso si las operaciones de grupo son mas lentas que las comparaciones, las comparaciones terminarían dominando el tiempo de ejecución del algoritmo y tornandolo en un método inútil. Una manera de evitar esto es ordenando la lista de q elementos usando un $O(q \log(q))$ método de ordenamiento como HeapSort. Luego una busqueda en un conjunto ordenado toma $O(\log(q))$ comparaciones, llevando el tiempo de ejecución a $O(q \log(q))$. Podemos también usar tablas de Hash para almacenar y buscar, que será aun mas rápido en promedio.

Una aplicación del método de Shanks requiere como mucho q giant-steps, cada uno de ellos de tamaño q. Si tenemos información adicional sobre n podemos aumentar la eficiencia del algoritmo. Daremos dos ejemplos, uno de los cuales nos será de utilidad al buscar los a_p. Asumamos que además de la cota superior B de n tenemos una cota inferior C, o sea

$$C \leq n \leq B$$

Y empezando la lista de los baby-steps en g^C en vez de $1 = g^0$, podemos disminuir el máximo de los giant-steps y el tamaño de ellos a $\sqrt{B - C}$.

Como segundo ejemplo asumamos que n cumple cierta congruencia, $n \equiv n_0 \pmod{b}$. Entonces podemos disminuir el tamaño y la cantidad de los giant-steps a $\left\lceil \sqrt{B/b} \right\rceil$.

3.2. Algoritmo de Shanks-Mestre

Podemos usar el algoritmo de Shanks para obtener un algoritmo para hallar los a_p en $O(p^{1/4+\varepsilon})$ para todo $\varepsilon > 0$. Por el Teorema de Hasse sabemos que

$$p + 1 - 2\sqrt{p} < |E(\mathbb{F}_p)| < p + 1 + 2\sqrt{p}$$

El algoritmo de Shanks nos sirve para hallar el orden de un elemento en un grupo dadas ciertas cotas, lo que no nos da necesariamente el orden del grupo. Necesitariamos refinar el algoritmo de Shanks para eso, lo que es mas difícil de implementar. Pero en el caso del grupo de una curva elíptica sobre $\mathbb{F}_p$ podemos usar la siguiente Proposición que nos ahorrara el trabajo extra.

Si uno considera todas las curvas sobre $\mathbb{F}_p$ definidas por

$$y^2 = x^3 + ad^2x + bd^3$$

con $d \neq 0$, entonces hay exactamente dos clases de isomorfismos de esas curvas. Las curvas tales que $\left(\frac{d}{p}\right) = 1$ son todas isomorfas a la curva inicial que corresponde a $d = 1$, y las curvas tales que $\left(\frac{d}{p}\right) = -1$ son todas isomorfas pero a otra curva. Llamemos E' a una de esas curvas.

Falta probar porqué son isomorfas dependiendo del símbolo de Legendre de d. Sean $d_1, d_2 \neq 0$ tales que $\left(\frac{d_1}{p}\right) = \left(\frac{d_2}{p}\right)$, luego $\left(\frac{d_1/d_2}{p}\right) = 1$ porque el símbolo de Legendre es multimplicativo en la coordenada de arriba. Sea $e \in \mathbb{Z}$ tal que $(d_1/d_2) \equiv e^2 \pmod{p}$. Finalmente el mapa $(x, y) \mapsto (x/e^2, y/e^3)$ es un isomorfismo entre las curvas $E_{d_1} : y^2 = x^3 + ad_1^2x + bd_1^3$ y $E_{d_2} : y^2 = x^3 + ad_2^2x + bd_2^3$.

Observación 3.2.1. Si E es una curva elíptica sobre un cuerpo finito $\mathbb{F}_p$, $E(\mathbb{F}_p)$ es un grupo cíclico o el producto de dos grupos cíclicos.

Esto es consecuencia del Corolario 1.7.7.

Proposición 3.2.1. *Sean*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/k_1\mathbb{Z} \times \mathbb{Z}/k_2\mathbb{Z} \quad y \quad E'(\mathbb{F}_p) \simeq \mathbb{Z}/k_1'\mathbb{Z} \times \mathbb{Z}/k_2'\mathbb{Z}$$

las estructuras abelianas de los grupos $E(\mathbb{F}_p)$ y $E'(\mathbb{F}_p)$, con $k_1|k_2$ y $k_1'|k_2'$, para $p > 457$ tenemos que

$$\text{máx}(k_2, k_2') > 4\sqrt{p}$$

Ver [Coh], Proposición 7.4.11.

La Proposición nos dice que hay un punto en E o en E' de orden mayor que $4\sqrt{p}$, y consecuentemente hay un único entero en el intervalo $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ múltiplo del orden de ese punto, y ese entero debe ser $|E(\mathbb{F}_p)|$ o $|E'(\mathbb{F}_p)|$. Además sabemos que, si $E' : y^2 = x^3 + ad_0^2x + b_0^3$

$$\begin{aligned}\left(\frac{x^3 + ax + b}{p}\right) &= \left(\frac{(d_0x)^3 + ad^2(d_0x) + bd_0^3}{p}\right)\left(\frac{1/d_0^3}{p}\right) \\ &= -\left(\frac{(d_0x)^3 + ad^2(d_0x) + bd_0^3}{p}\right)\end{aligned}$$

Y como multiplicar por d_0 es una biyección en $\mathbb{F}_p$ tenemos que si $|E(\mathbb{F}_p)| = p+1-a_p = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)$, $|E'(\mathbb{F}_p)| = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ad_0^2x+bd_0^3}{p}\right) = p+1-\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right) = p+1+a_p$, por lo que podemos hallar el a_p en cualquier curva que nos dara el a_p en la otra.

Esto lleva al siguiente algoritmo.

Algoritmo 3.2.1 (Shanks-Mestre)**.** Dada una curva elíptica E sobre $\mathbb{F}_p$ con $p > 457$ por la ecuación $y^2 = x^3 + ax + b$, el algoritmo calcula el entero a_p tal que $|E(\mathbb{F}_p)| = p + 1 - a_p$.

1. [Inicializar]
   Fijar $x \leftarrow -1$, $A \leftarrow 0$, $B \leftarrow 1$, $k_1 \leftarrow 0$.

2. [Obtener siguiente punto] (Aquí sabemos que $|E(\mathbb{F}_p)| \equiv A \pmod B$).
   Repetir $x \leftarrow x + 1$, $d \leftarrow x^3 + ax + b$, $k \leftarrow \left(\frac{d}{p}\right)$ hasta que $k \neq 0$ y $k \neq k_1$. Fijar $k_1 \leftarrow k$. Finalmente, si $k_1 = -1$ fijar $A_1 \leftarrow 2p + 2 - A \pmod B$ si no fijar $A_1 \leftarrow A$.

3. [Encontrar múltiplo del orden de un punto]
   Sea m el menor entero tal que $m > p + 1 - 2\sqrt{p}$ y $m \equiv A_1 \pmod B$. Usando el algoritmo de Shanks encontrar un entero n tal que $m \leq n < p + 1 + 2\sqrt{p}$, $n \equiv m \pmod B$ y $nP_d = \mathcal{O}$, con $P_d = (xd, d^2)$, en la curva $Y^2 = X^3 + ad^2X + bd^3$ (observemos que esta curva será isomorfa a alguna de las curvas E, E' dependiendo del signo de k_1).

4. [Encontrar orden]
   Factorizar n y deducir el orden exacto h del punto $P_d = (xd, d^2)$.

5. [Finalizado?] Usando el Teorema Chino de los Restos, encontrar el menor entero h' múltiplo de h, $h \leq h'$ y tal que $h' \equiv \pmod B$. Si $h' < 4\sqrt{p}$ fijar $B \leftarrow \text{mcm}(B, h)$, entonces $A \leftarrow h' \pmod B$ si $k_1 = 1$, $A \leftarrow 2p + 2 - h' \pmod B$ si $k_1 = -1$, y volver al paso 2.

6. [Calcular a_p]
   Sea N el único múltiplo de h' tal que $p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}$. Devolver $a_p = p + 1 - k_1N$ y terminar el algoritmo.

Explicaremos ahora el algoritmo y su correctitud.

El paso 1 es simplemente la inicialización de las variables a usar en el algoritmo.

En el paso 2 iteramos en x sumándole 1 hasta que encontramos uno tal que $\left(\frac{x^3+ax+b}{p}\right)$ es no nulo y diferente de k, o sea que cambiamos de clase de isomorfismo.

Luego como sabemos que $|E(\mathbb{F}_p)| \equiv A \pmod B$ y $|E(\mathbb{F}_p)|+|E'(\mathbb{F}_p)| = 2p+2$, y elegimos A_1 congruente a $|E(\mathbb{F}_p)|$ o $|E'(\mathbb{F}_p)|$ módulo B dependiendo de signo de k_1.

En el paso 3 buscamos un entero múltiplo del orden del punto $P_d = (dx, d^2)$ en la curva

$$Y^2 = X^3 + ad^2X + bd^3$$

ya que

$$(dx)^3 + ad^3(dx) + bd^3 = d^3(x^3 + ax + b) = d^4 = (d^2)^2$$

usando el algoritmo descripto en 3.1. Lo usamos de la siguiente manera, primero calculamos

$$S = \{\mathcal{O}, P_d, BP_d, 2BP_d, \ldots, (q-1)BP_d\}$$

con $q = \left\lceil \sqrt{\frac{4\sqrt{p}}{B}} \right\rceil$. Ahora sabemos que $n - m = B\alpha$ con $\alpha = aq + r$, $0 \leq r < q$ y se prueba como antes que $0 \leq a \leq q$. Despues para $0 \leq a \leq q$ buscamos $-(m + Baq)P_d$ en S. Una vez encontrado procedemos como en 3.1.

El paso 4 es inmediato.

En el paso 5, primero buscamos un múltiplo del orden de P_d que sea congruente a A_1 módulo B y lo podemos hacer con el algoritmo del Teorema Chino de los Restos. Luego verificamos si el orden es menor que $4\sqrt{p}$, si es así no nos alcanza para hallar a_p y volvemos al paso 2 luego de cambiar las variables para que de nuevo el orden de $E(\mathbb{F}_p)$ sea congruente a A módulo B y cambiando B por el mínimo común múltiplo entre B y el h' que habíamos hallado. O sea, el punto P_d no nos da el a_p pero nos da información sobre una congruencia del orden de $E(\mathbb{F}_p)$, que la usamos para acortar la ejecución del algoritmo. Finalmente si h' es mayor que $4\sqrt{p}$ entonces podemos hallar a_p con el, en el paso 6, que es inmediato.

Para el paso 4 podemos usar el algoritmo 1.3.11 dado en [Coh], y para el paso 5 podemos usar el algoritmo 1.4.3 dado en [Coh].

El tiempo de ejecución de este algoritmo es de $O(p^{1/4+\varepsilon})$ ya que la operación dominante del algoritmo es hallar el orden del punto (dx, d^2), aunque busquemos uno de orden mayor que $4\sqrt{p}$ sabemos que hay muchos de esos puntos en E o en E' por la Proposición 3.2.1. Y habíamos viste en 3.1 que hallar el orden con el algoritmo de Shanks tenia orden, tomando $B = p+1+2\sqrt{p}$, $C = p+1-2\sqrt{p}$, $O\left(\sqrt{B-C}\right) = O\left(\sqrt{4\sqrt{p}}\right) = O\left(\sqrt[4]{p}\right)$.

3.3. Otros Algoritmos

Daremos a continuación una escueta descripción o comentario de otros algoritmos para hallar a_p que son mas eficientes que el anterior.

3.3.1. Mejora de Shanks-Mestre

En el paso 3 del Algoritmo 3.2.1 podemos usar el hecho que hallar el opuesto de un elemento de E es trivial. Escribimos $n - m = B\alpha$ con $\alpha = aq + r$, pero en este caso tomamos $-q \leq r < q$ con $q = \left\lceil \sqrt{\frac{2\sqrt{p}}{B}} \right\rceil$ y $0 \leq a \leq 2q + 1$. El cambio es que no tenemos que hallar rP_d para todos los r, si no solo los r no negativos.

O sea $S = \{\mathcal{O}, BP_d, 2BP_d, \ldots, (q-1)BP_d\}$. Luego calculamos $-(m + Baq)P_d$ y verificamos si la coordenada en x coincide con la coordenada en x de algún elemento de S. Esta mejora nos divide el tamaño de S en $\sqrt{2}$, mejorando el uso de memoria y de tiempo de ejecución.

3.3.2. Algoritmo de Schoof

Recordemos que por la primer parte del Teorema de Hasse el endomorfismo de Frobenius satisface la siguiente relación en $E(\mathbb{Z}_p)$

$$\varphi \circ \varphi - [t] \circ \varphi + [q] = \mathcal{O}_M$$

con $t = p + 1 - |E(\mathbb{F}_p)|$. Podemos restringirnos a los puntos de $E[l]$ con l primo y considerar la ecuación

$$\varphi_l \circ \varphi_l + [m] = [\tau] \circ \varphi_l \tag{3.1}$$

donde

$$m \equiv p \pmod{l}$$

y $\tau \equiv t \pmod{l}$. El algoritmo entonces consiste en hallar τ para suficientes primos pequeños $l = 3, 5, 7, 11, \ldots, L$ tales que

$$\prod_{l \leq L \ l \neq 2,p} l > 4\sqrt{p}$$

ya que tenemos una cota para a_p. Luego usando el Teorema Chino de los Restos podemos determinar t de manera única. Por lo que solo necesitamos un método de calcular $\tau \equiv t \pmod{l}$ para un primo l diferente de 2 y p.

Sea l un primo diferente de 2 y p y $P = (x, y) \in E[l]$ diferente de $\mathcal{O}$. Por el Teorema 1.8.7, que nos daba las relaciones entre las funciones g_n, h_n y los polinomios ψ_m, la relación (3.1) se cumple si y solo si

$$\begin{aligned} \left(x^{p^2}, y^{p^2}\right) \quad + \quad & \left(x - \frac{\psi_{p-1}\psi_{p+1}}{\psi_p^2}, \frac{\psi_{p+2}\psi_{p-1}^2 - \psi_{p-2}\psi_{p+1}^2}{4y\psi_p^3}\right) \\ = \quad & \begin{cases} 0 \text{ si } \tau \equiv 0 \pmod{l}. \\ \left(x^p - \left(\frac{\psi_{\tau-1}\psi_{\tau+1}}{\psi_\tau^2}\right)^p, \left(\frac{\psi_{\tau+2}\psi_{\tau-1}^2 - \psi_{\tau-2}\psi_{\tau+1}^2}{4y\psi_\tau^3}\right)^p\right) \text{ si no.} \end{cases} \end{aligned}$$

Por la Proposición 1.8.8 el punto $P = (x, y)$ esta en $E[l]$ si y solo si $\psi_l(x, y) = 0$ si y solo si $f_l(x) = 0$ con f_l función en x, demostrada su existencia en 1.8.1. Usando la formula $y^2 = x^3 + ax + b$ y la ley de grupo de la curva elíptica, la relación anterior puede ser transformada en relaciones de la forma

$$H_1(x) = 0 \text{ y } H_2(x) = 0 \tag{3.2}$$

para algunos polinomios en $\mathbb{F}_p[X]$. Esto se deduce del hecho que $P = (x, y)$ cumple la relación si y solo si $-P = (x, -y)$ la cumple. Tenemos que verificar que se cumple

$$H_1 \equiv 0 \pmod{f_l} \text{ y } H_2 \equiv 0 \pmod{f_l}$$

en $\mathbb{F}_p[X]$. Esto se verifica para todo $\tau \in \mathbb{Z}/l\mathbb{Z}$, hasta que algún τ es encontrado que cumpla (3.2).

El tiempo de ejecución del Algoritmo de Schoof es de $O(\log^9 p)$, demostrado en [Sch], donde esta demostración completa y también un algoritmo para raíces cuadradas módulo primos.

3.3.3. Algoritmo SEA

Ciertas mejoras al Algoritmo de Schoof por Elkies y Atkins dio como resultado un algoritmo mas rápido llamado Algoritmo SEA, Schoof-Elkies-Atkins que corre en $O(\log^4 p)$, una referencia se puede encontrar en [Csi].

3.4. Algunos calculos

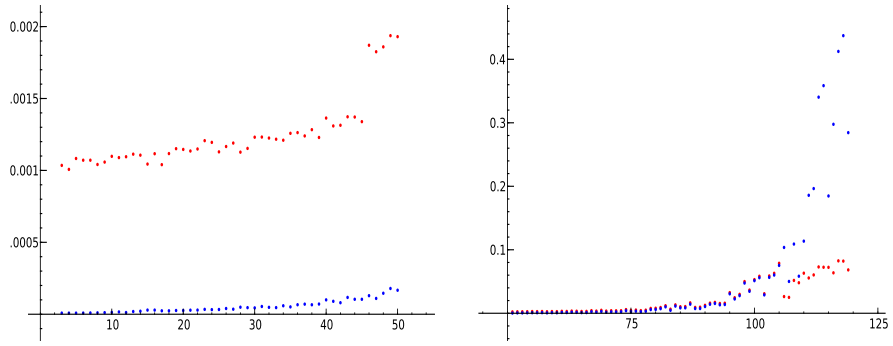
A continuación presentamos gráficas del tiempo de ejecución de los algoritmos SEA y Shanks-Mestre, para diferentes curvas elípticas. A la izquierda están graficados los tiempos de ejecución para primos de tamaño $(3/2)^n$ para n entre 3 y 50, y a la derecha para n entre 51 y 120. En rojo esta graficado el tiempo de ejecución del algoritmo SEA y en azul el algoritmo de Shanks-Mestre. El algoritmo SEA esta implementado en el sistema de computación matemática SAGE[Sage] y el algoritmo de Shanks-Mestre en el sistema PARI/GP[Pari].

Observar que para n pequeños es mas rápido el algoritmo de Shanks-Mestre y luego aumenta mas rápido que el SEA. También se puede observar como demora mas el SEA en general en las distintas curvas, la diferencia entre ellas es el rango sobre $\mathbb{Q}$. Por el teorema de Mordell sabemos que el grupo de puntos de una curva elíptica sobre $\mathbb{Q}$ es finitamente generado, y el rango es la dimensión de la parte infinita del grupo. O sea,

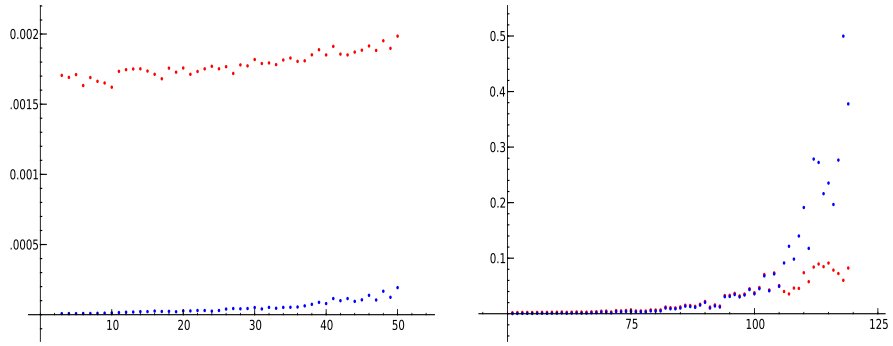
$$E(\mathbb{Q}) = E_{\text{tor}}(\mathbb{Q}) \oplus \mathbb{Z}^r$$

donde $E_{\text{tor}}(\mathbb{Q})$ es la parte de torsión de la curva que es un grupo finito, y r es el rango.

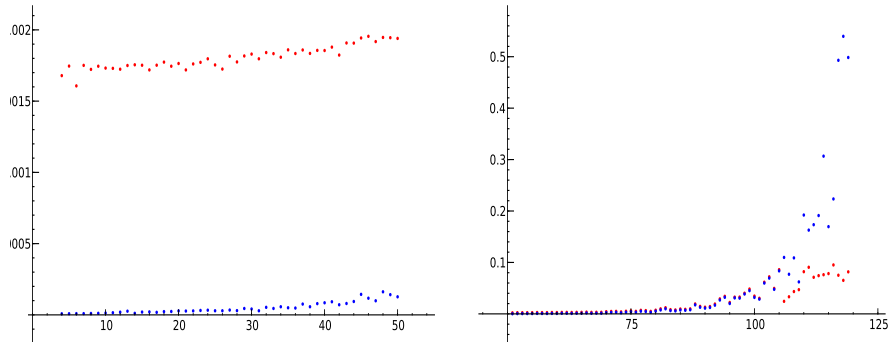
La curva de la figura **??** tiene rango 0, el de la figura **??** tiene rango al menos 12 y el de la figura 3.1 tiene rango al menos 22. Observamos entonces que, en estos casos, a mayor rango mas tiempo de ejecución del algoritmo.



(a) E: $y^2 = x^3 - 13392x - 1080432$



(b) E: $y^2 = x^3 - 101596938352x + 12361366202306320$



(c) E: $y^2 = x^3 - 12186281750382032063223179650309591 23x + 49956273142750033462337511268341097165563678362299447 8$

Figura 3.1: Tiempos de ejecución de los algoritmos de Shanks-Mestre y SEA para primos de tamaño $(3/2)^n$ con n entre 3 y 120.
- Tiempo de ejecución del algoritmo Shanks-Mestre.
- Tiempo de ejecución del algoritmo SEA.

Capítulo 4

Conjetura de Sato-Tate

4.1. Introducción

En los capítulos anteriores probamos una cota para la cantidad de puntos de una curva elíptica sobre un cuerpo finito y como hallar esa cantidad. Pero no hemos dado una formula explicita de esa cantidad, porque en general no se conoce tal formula. Pero podemos dar un ejemplo donde si se conoce. Tenemos el siguiente resultado de Gauss sobre la curva

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

que es isomorfa sobre $\mathbb{Q}$ a la curva elíptica $y^2 = x^3 - 432$.

Teorema 4.1.1 (Gauss)**.** *Sea E_p la cantidad de puntos de la curva elíptica*

$$y^2 = x^3 - 432$$

sobre el cuerpo $\mathbb{F}_p$, con p primo.

1. *Si $p \not\equiv 1 \pmod 3$, entonces $E_p = p + 1$.*
2. *Si $p \equiv 1 \pmod 3$, entonces existen enteros A y B tales que*

$$4p = A^2 + 27B^2$$

y son únicos salvo cambio de signo, y si fijamos el signo de A para que $A \equiv 1 \pmod 3$ entonces

$$E_p = p + 1 + A$$

Presentamos algunos ejemplos del teorema anterior en la tabla 4.1. Para hallar E_p alcanza con buscar un B tal que $4p - 27B^2$ sea cuadrado. Esto puede ser fácilmente hallado para p pequeño buscando uno a uno. Observar que iteramos en B ya que esta multiplicado por 27 y será un poco mas pequeño que A.

Este tipo de formulas solo son conocidas para curvas con lo que llamamos multiplicación compleja, que definimos a continuación.

p	A	B	$E_p = p + 1 + A$
7	1	1	9
13	-5	1	9
19	7	1	27
31	4	2	36
1000003	1003	333	1001007
10000000033	196417	7253	10000196451

Cuadro 4.1: Cantidad de puntos en la curva $y^2 = x^3 - 432$ sobre $\mathbb{F}_p$.

Definición 4.1.1. Sea E una curva elíptica sobre un cuerpo K. Decimos que E tiene *multiplicación compleja*, si existen Endomorfismos en E que no son multiplicación por n, sobre la clausura algebraica de K. En otras palabras $\mathbb{Z} \subsetneq \mathrm{End}(E(\bar{K}))$.

Ejemplo 4.1.1. Sea E la curva elíptica dada por la ecuación, en $\mathbb{C}$

$$y^2 = x^3 - 432$$

Un endomorfismo que no es es multiplicación por un entero es, si $(x, y) \in E(\mathbb{C})$,

$$(x, y) \longmapsto (e^{2\pi i/3}x, y)$$

ya que aplicado tres veces es la identidad.

La conjetura de Sato-Tate es una afirmación sobre la distribución de la sucesión $a_p = p+1-|E(\mathbb{F}_p)|$, de una curva elíptica E sin multiplicación compleja. En el capitulo 2 probamos cotas inferior y superior para ellos, pero no sabemos si se alcanzan o cuan cerca llegan a estar. O sea, podemos preguntarnos si las cotas de Hasse son las óptimas. En la figura 4.1 vemos que los a_p se acercan bastante a las curvas $y = \pm 2\sqrt{x}$, aunque la segunda curva elíptica es con multiplicación compleja.

Por el teorema de Hasse podemos ver que la sucesión de los a_p normalizado por $2\sqrt{p}$ esta en el intervalo $[-1, 1]$,

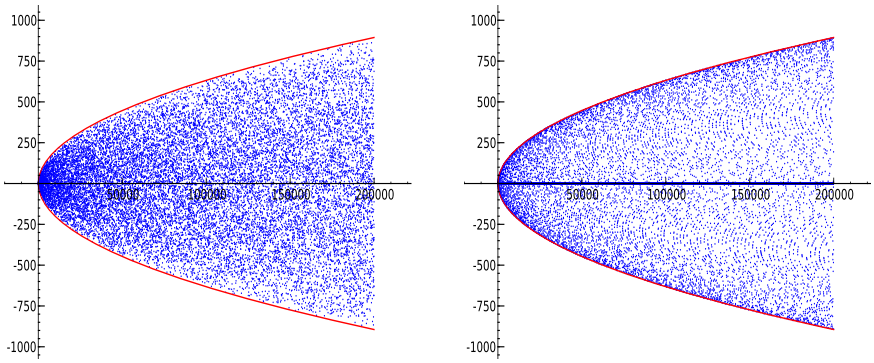
$$(a_p/2\sqrt{p})_{p \text{ primo}} \subset [-1, 1]$$

Podemos entonces preguntar como se distribuye esta sucesión en el intervalo $[-1, 1]$.

En el caso de que la curva elíptica tenga multiplicación compleja podemos hacer la siguiente heurística de la distribución mencionada. Tomamos, por ejemplo, la curva $y^2 = x^3 - 432$, de la cual tenemos una formula exacta de a_p. Primero descartamos los primos $p \not\equiv 1 \pmod 3$, de los cuales sabemos que $a_p = 0$.

Para estudiar la distribucion de $a_p/2\sqrt{p}$ estudiamos el limite

$$\lim_{X \to \infty} \frac{\#\{p \leq X : p \text{ primo},\ p \equiv 1 \ (\mathrm{mod}3),\ a_p \leq \alpha\}}{\#\{p \leq X : p \text{ primo},\ p \equiv 1 \ (\mathrm{mod}3)\}}$$



(a) $y^2 = x^3 - 13392x - 1080432$ (b) $y^2 = x^3 + 1$

Figura 4.1: Gráfica de los puntos (p, a_p), en azul, con $p \leq 200000$. En rojo las curvas $\pm 2\sqrt{x}$.

Para eso consideramos los conjuntos

$$S_{\alpha,X} = \{p \leq X : p \text{ primo}, \ p \equiv 1 \ (\text{mod}3), \ a_p \leq \alpha\} \tag{4.1}$$
$$S = \{p \leq X : p \text{ primo}, \ p \equiv 1 \ (\text{mod}3)\} \tag{4.2}$$

y sabemos por la formula dada en el Teorema 4.1.1 que, definiendo $f(A, B) = A^2 + 27B^2$,

$$S_{\alpha,X} = \left\{(A, B) \in \mathbb{Z}^2 : \frac{f(A, B)}{4} \leq X, \ \frac{f(A, B)}{4} \text{ primo con } A \equiv 1 \ (\text{mod}3), \ A \leq \alpha\right\}$$

La heurística es la siguiente. Para grandes valores de X podemos asumir

$$\frac{\#S_{\alpha,X}}{\#S} \approx \frac{\text{Área}\left\{(A, B) \in \mathbb{R}^2 : f(A, B) \leq X, \frac{A}{\sqrt{A^2+27B^2}} \leq \alpha\right\}}{\text{Área}\{(A, B) \in \mathbb{R}^2 : f(A, B) \leq X\}}$$

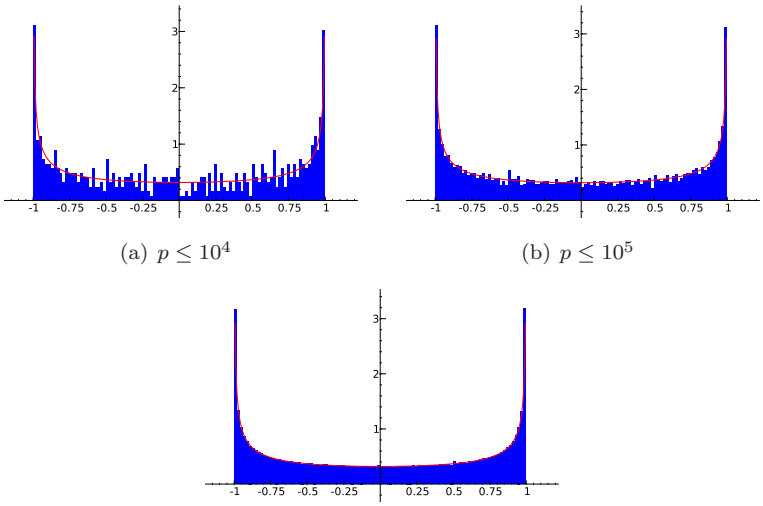
que es $-\text{Arccos}(\alpha)/\pi$. Entonces tenemos la distribución de $(a_p)_{p\equiv 1 \ (\text{mod}3), \ \text{primo}} \subset [-1, 1]$. Por lo tanto podemos predecir que

$$\lim_{X\to\infty} \frac{\#\left\{\frac{a_p}{2\sqrt{p}} \in [a, b] : p < X, \ p \equiv 1 \ (\text{mod}3)\right\}}{\#\{\text{primos } p < X, \ p \equiv 1 \ (\text{mod}3)\}} = \frac{1}{\pi}\int_a^b \frac{1}{\sqrt{1-x^2}}dx$$

En la figura 4.2 mostramos histogramas de la distribución mencionada, para distintas cotas X.

4.2. Conjetura de Sato-Tate

Para el caso en que la curva no tenga multimplicación compleja, graficamos en la figura 4.3 la distribución de las sucesiones $(a_p/2\sqrt{p})_{p<X}$ para distintas



(a) $p \leq 10^4$ (b) $p \leq 10^5$

(c) $p \leq 5 \times 10^6$

Figura 4.2: Histogramas de distribución de los $a_p \neq 0$, para la curva elíptica $y^2 = x^3 - 432$, en azul. En rojo la curva $1/\sqrt{1-x^2}$.

curvas E, con diferentes rangos, y cotas X. Usamos para calcular los a_p para poder hacer los histogramas el algoritmo de Shanks-Mestre presentado en el capitulo anterior. Lo elegimos ya que estamos calculando todos los a_p hasta un X fijo y por lo tanto será mas eficiente usar el algoritmo que es mas rápido para primos pequeños. Calculamos con cotas hasta 10^6 por dos razones, la primera es que ya era evidente que eran casi iguales los histogramas y los semicírculos, y consumía un tiempo no razonable para cotas por ejemplo de 10^8. Observando los histogramas vemos que las sucesiones toman la distribución de un semi-circulo "aplastado" en $[-1, 1]$.

Conjetura 1 (Sato-Tate)**.** *Sea E una curva elíptica sin multiplicación compleja. Entonces la distribución de la sucesión $(a_p/2\sqrt{p})$ en $[-1, 1]$ converge a la distribución semi-circular $(2/\pi)\sqrt{1-x^2}$. O sea, para todo subintervalo $[a, b] \subset [-1, 1]$,*

$$\lim_{X\to\infty} \frac{\#\left\{\frac{a_p}{2\sqrt{p}} \in [a,b] : p < X\right\}}{\#\{\text{primos } p < X\}} = \frac{2}{\pi}\int_a^b \sqrt{1-x^2}dx$$

Podemos definir las siguientes funciones para reformular la conjetura:

$$\begin{aligned} X(T) &= \frac{\int_{-1}^{T}\sqrt{1-x^2}dx}{\int_{-1}^{1}\sqrt{1-x^2}dx} = \frac{2}{\pi}\int_{-1}^{T}\sqrt{1-x^2}dx \\ Y_C(T) &= \frac{\#\left\{\text{primos } p < C : -1 < \frac{a_p}{2\sqrt{p}} < T\right\}}{\#\{\text{primos } p < C\}} \\ \Delta(C) &= \sqrt{\int_{-1}^{1}(X(T) - Y_C(T))^2 dT} \end{aligned}$$

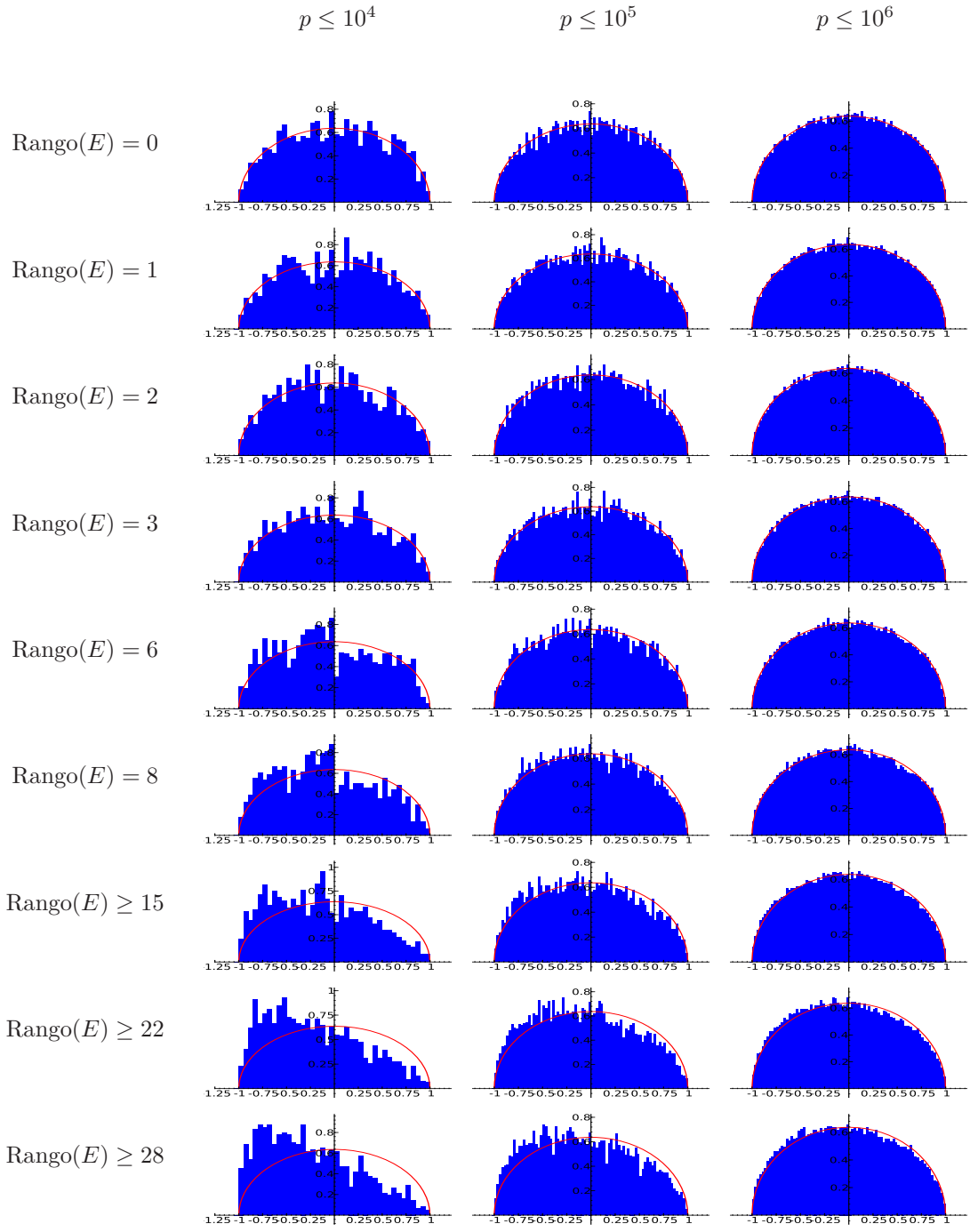
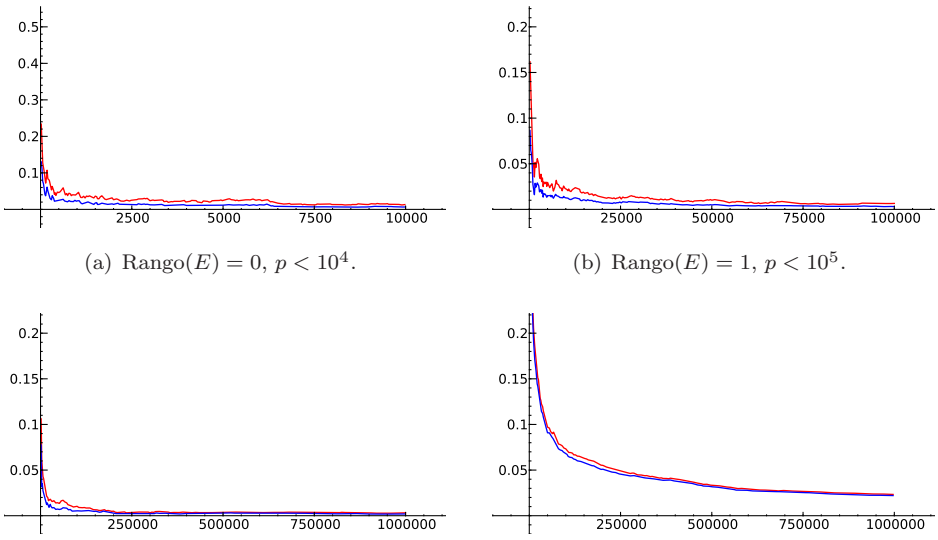


Figura 4.3: Histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$, para curvas elípticas con distinto rango y cota X.



(a) Rango$(E) = 0$, $p < 10^4$.

(b) Rango$(E) = 1$, $p < 10^5$.

(c) Rango$(E) = 2$, $p < 10^6$.

(d) Rango$(E) \geq 28$, $p < 10^6$.

Figura 4.4: Gráficas de $\Delta(C)$ y $\Delta_\infty(C)$. Por Sato-Tate convergen a 0.

Donde $X(T)$ es el área debajo del semicirculo normalizado y $\Delta(C)$ es la norma L_2 de la diferencia entre X y Y_C. Definamos también $\Delta_\infty(C)$ como la norma L_∞. Entonces la conjetura de Sato-Tate nos dice que:

$$\lim_{C\to\infty} \Delta(C) = \lim_{C\to\infty} \Delta_\infty(C) = 0$$

En la figura 4.4 mostramos gráficas de $\Delta(C)$ y $\Delta_\infty(C)$ para diferentes curvas y cotas, donde parece cierto que convergen a 0. De vuelta las cuentas las hicimos con el algoritmo de Shanks-Mestre por las mismas razones. Una vez que parece cierta la convergencia podemos preguntar con que velocidad converge. O sea, ¿como tiende $\Delta(C)$ o $\Delta_\infty(C)$ a cero?

La siguiente conjetura nos dice algo sobre la velocidad de convergencia.

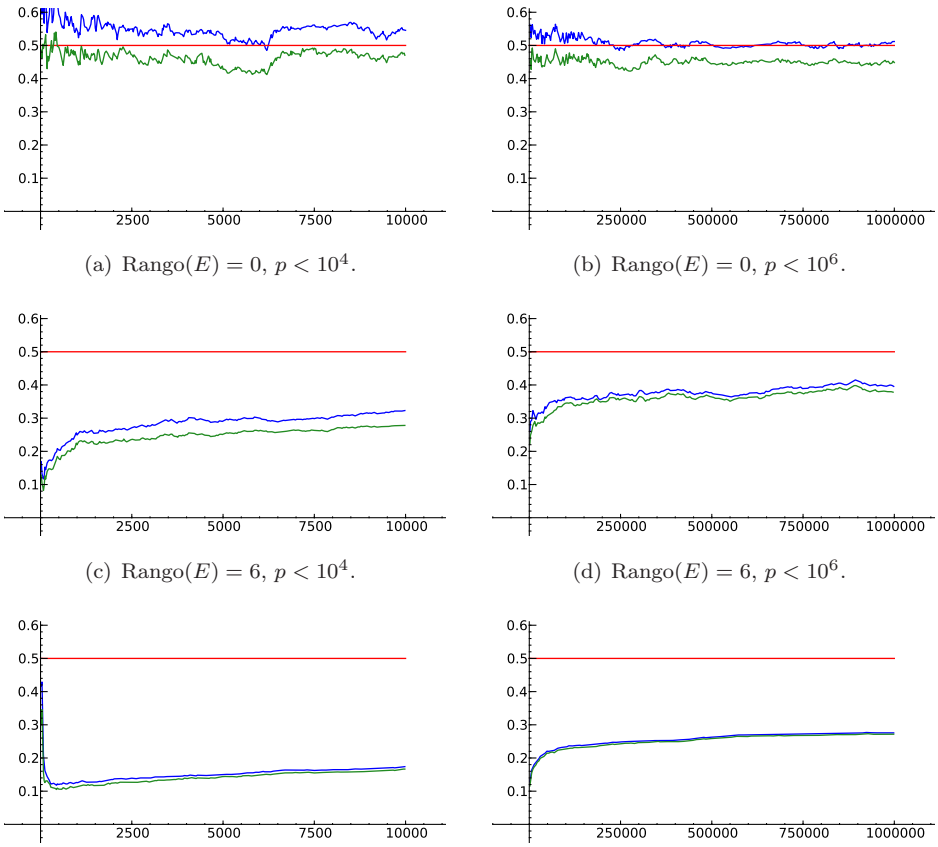
Conjetura 2 (Akiyama-Tanigawa)**.** *Para todo $\varepsilon > 0$ y para $C \gg 0$ se cumple*

$$\Delta_\infty(C) \leq \frac{1}{C^{1/2-\varepsilon}}$$

Para testear la conjetura de Akiyama-Tanigawa, podemos, en vez de graficar $\Delta(C)$, graficar $-\log_C(\Delta(C))$. Y ver como se compara esta función con $\frac{1}{2}$, y si es cierto que se acerca a ε de $\frac{1}{2}$. Esto lo podemos ver en la figura 4.5.

En las gráficas logarítmicas vemos que cuanto mas grande es el rango de la curva elíptica mas lejos esta $-\log(\Delta(C))$ de $\frac{1}{2}$. Preguntamos entonces si podemos predecir el comportamiento asintótico de de la curva $\Delta(C)$. Tratamos de aproximar la curva $\Delta(C)$ con una del tipo

$$\frac{1}{2} - \frac{\alpha}{\log(X)}$$



(a) Rango$(E) = 0$, $p < 10^4$.

(b) Rango$(E) = 0$, $p < 10^6$.

(c) Rango$(E) = 6$, $p < 10^4$.

(d) Rango$(E) = 6$, $p < 10^6$.

(e) Rango$(E) \geq 28$, $p < 10^4$.

(f) Rango$(E) \geq 28$, $p < 10^6$.

Figura 4.5: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ que parecen tender a $1/2$ para curvas elípticas E.

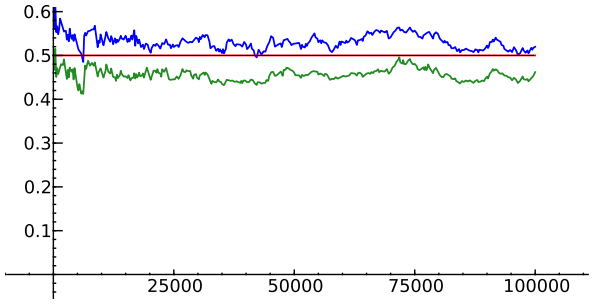
para algún α a buscar experimentalmente de la siguiente manera. Dada una cota X optimizamos la norma L_2 de la diferencia entre $\frac{1}{2} - \frac{\alpha}{\log(X)}$ y $-\log(\Delta(C))$.

Luego de hallar los α para curvas con diferentes rangos pudimos observar que cuanto mas grande es el rango mas grande es α. Aunque no hemos podido hallar una relación aritmética entre el α y el rango, que es un tema interesante para seguir investigando. Esto se puede observar mejor en el apéndice.

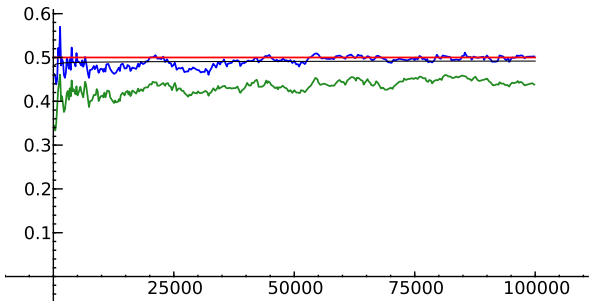
Esto lo podemos resumir en la siguiente conjetura que refina la conjetura de Akiyama-Tanigawa ya que nos dice como va a ser el ε.

Conjetura 3 (Stein)**.** *Para una curva elíptica E sin multiplicación compleja existe un α tal que*

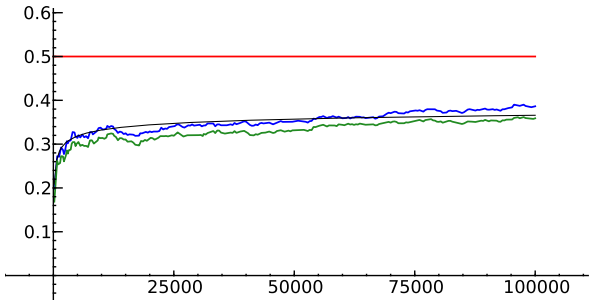
$$\frac{1}{2} - \frac{\alpha}{\log(C)} \leq -\log_C(\Delta(C))$$



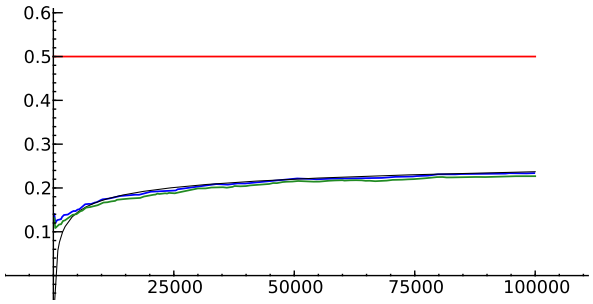
(a) Rango$(E) = 0$, $\alpha = 0$, $p < 10^5$



(b) Rango$(E) = 1$, $\alpha = 0{,}025$, $p < 10^5$



(c) Rango$(E) = 5$, $\alpha = 1{,}41$, $p < 10^5$



(d) Rango$(E) \geq 28$, $\alpha = 3{,}10$, $p < 10^5$

Figura 4.6: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas E.

Apéndice A

Apéndice

Presentamos en este apéndice todos los datos calculados, que por comodidad de lectura omitimos en los capítulos anteriores.

A.1. Las Curvas

En todos los calculos usamos curvas elípticas E con diferentes rangos. Estas son:

- Curva elíptica de rango 0:

$$y^2 = x^3 - 13392x - 1080432$$

- Curva elíptica de rango 1:

$$y^2 = x^3 - 16x + 16$$

- Curva elíptica de rango 2:

$$y^2 = x^3 - 3024x + 46224$$

- Curva elíptica de rango 3:

$$y^2 = x^3 - 112x + 400$$

- Curva elíptica de rango 4:

$$y^2 = x^3 - 1267x + 17230$$

- Curva elíptica de rango 5:

$$y^2 = x^3 - 1264x + 21904$$

- Curva elíptica de rango 6:

$$y^2 = x^3 - 3346947x + 2323281150$$

- Curva elíptica de rango 7:

$$y^2 = x^3 - 10012x + 346900$$

- Curva elíptica de rango 8:

$$y^2 = x^3 - 379792x + 61463440$$

- Curva elíptica de rango mayor o igual a 11:

$$y^2 = x^3 - 837232742021688783 72x + 2946651690639070704580403200 65$$

- Curva elíptica de rango mayor o igual a 12:

$$y^2 = x^3 - 101596938352x + 12361366202306320$$

- Curva elíptica de rango mayor o igual a 14:

$$y^2 = x^3 - 35971713708112x + 85086213848298394000$$

- Curva elíptica de rango mayor o igual a 15:

$$y^2 = x^3 - 271916280086622893057201183332587x + 1243568676486997208976444495097191363366645800166$$

- Curva elíptica de rango mayor o igual a 17:

$$y^2 = x^3 - 245693409843776913996918175860 3x + 1997378191278720059044784189699562032770792902$$

- Curva elíptica de rango mayor o igual a 18:

$$\begin{aligned} y^2 &= x^3 - 339240442801468257888199655168607602590091449044914 67x \\ &+ 2382693062150390633665411116567171551061211207873414884113814796983925669947270 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 19:

$$\begin{aligned} y^2 &= x^3 - 330201392199460219323796316 43x \\ &+ 2101673458771559496667419867471431403720758 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 20:

$$\begin{aligned} y^2 &= x^3 - 558696503073168446634037276274951163x \\ &+ 2405715655591861282320569262502949697866831965877260 38 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 21:

$$\begin{aligned} y^2 &= x^3 - 279733529059487322931660258701999146187x \\ &- 90859579977643735705517120084046778651756373828106367986 6 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 22:

$$\begin{aligned} y^2 &= x^3 - 12186281750382032063223179650309591 23x \\ &+ 49956273142750033462337511268341097165563678362299447 8 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 23:

$$\begin{aligned} y^2 &= x^3 - 24951844465641520625173490142878300472387x \\ &+ 15249747219523352507645272143625911405453781336654958684927 34 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 24:

$$\begin{aligned} y^2 &= x^3 - 15557160935994194991338086647175216810008 3x \\ &+ 23525121249375992220490683570065893549428750489751411487963982 \end{aligned}$$

- Curva elíptica de rango mayor o igual a 28:

$$\begin{aligned} y^2 &= x^3 - 32108419864920842536053133134941668401488368499486330402 7x \\ &+ 22068231548819556138901110838639219053415720136358962117716078469478004397240002754 46 \end{aligned}$$

A.2. Los Histogramas

En esta sección presentamos los histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$ para las curvas de la sección A.1. Primero presentamos los histogramas con primos hasta 10^3 y luego hasta 10^4, 10^5 y 10^6. Los histogramas estarán ordenados por rango de menor a mayor yendo de izquierda a derecha y de arriba hacia abajo.

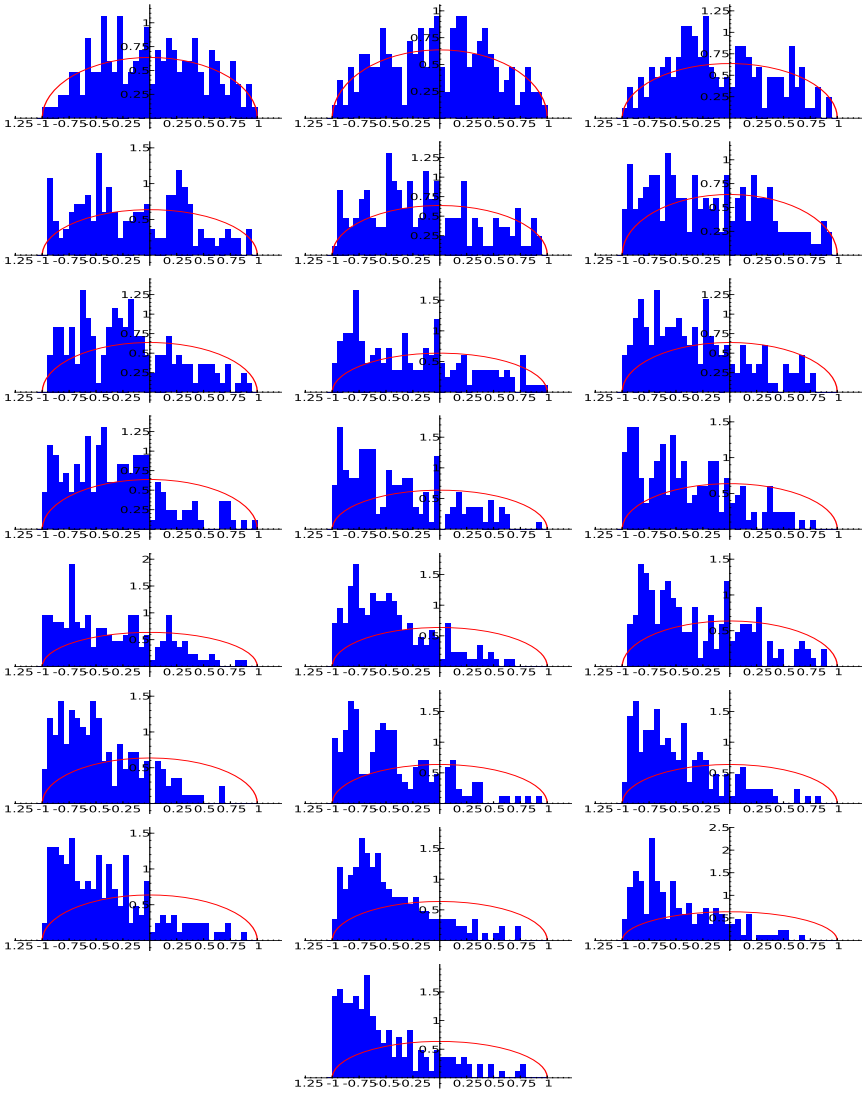


Figura A.1: Histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$, para las curvas de la sección A.1 y cota 10^3.

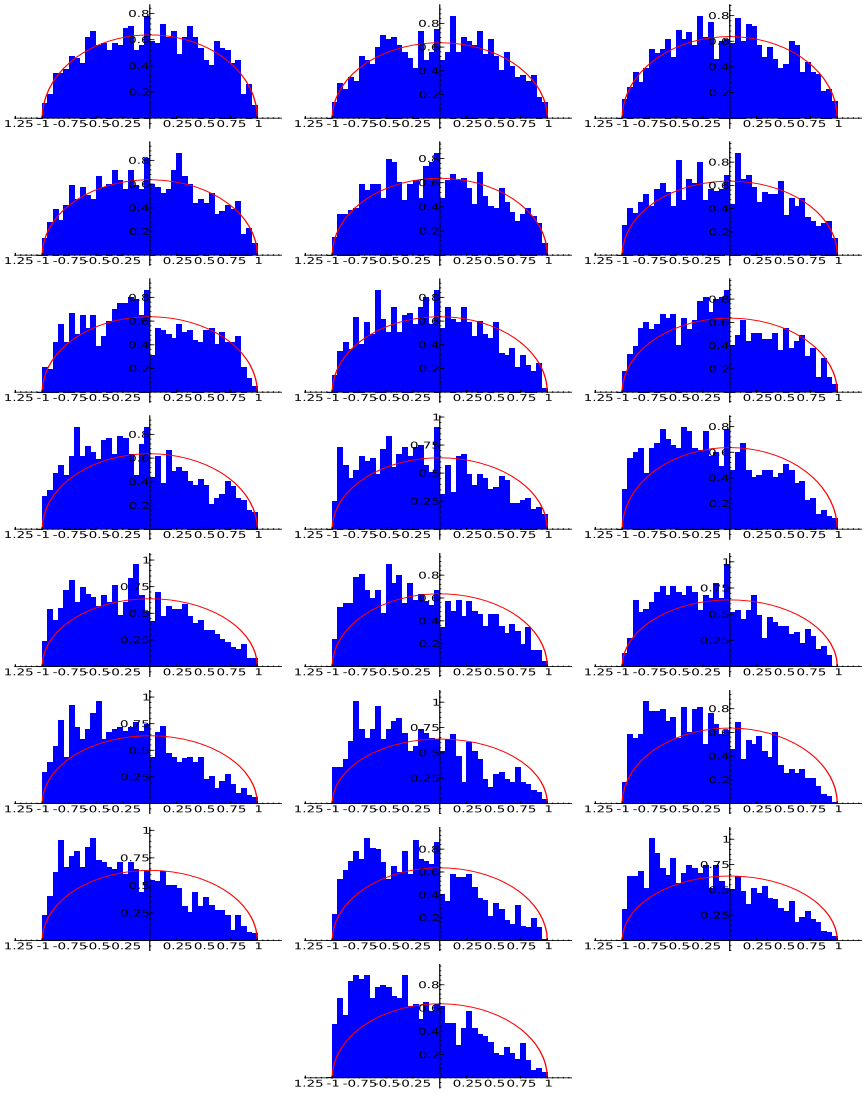


Figura A.2: Histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$, para las curvas de la sección A.1 y cota 10^4.

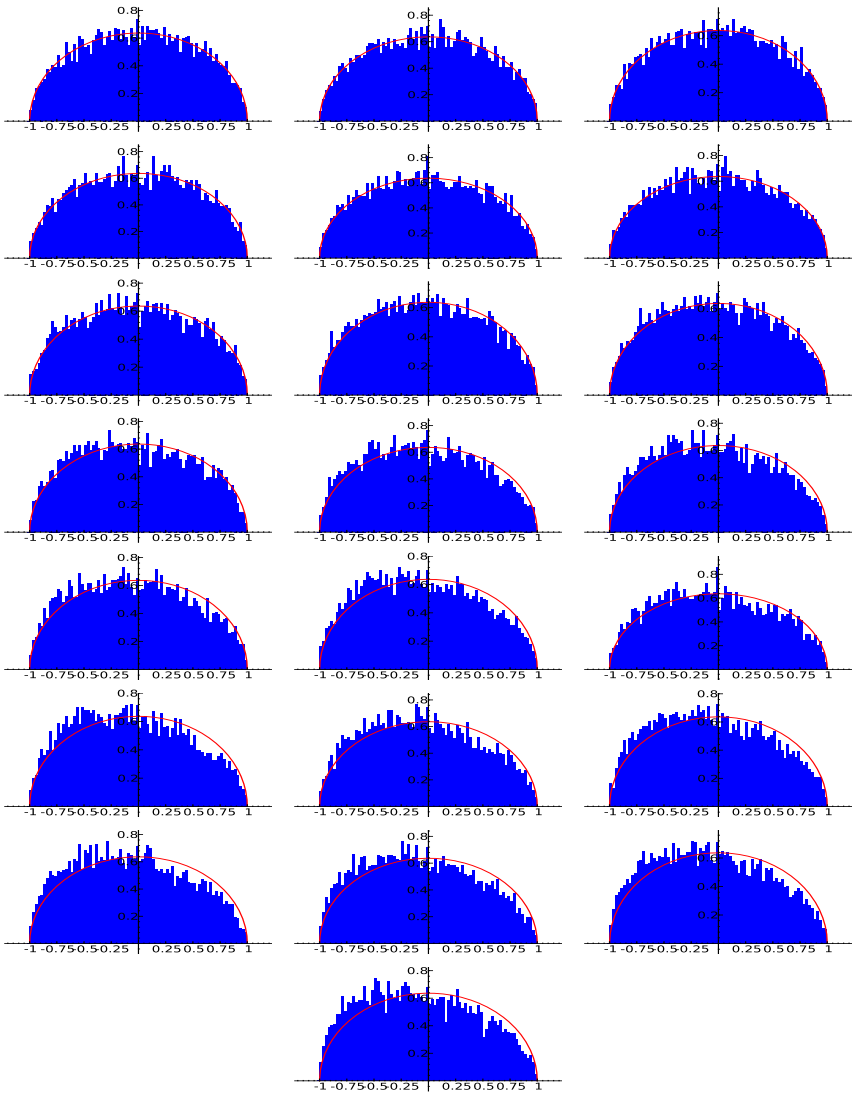


Figura A.3: Histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$, para las curvas de la sección A.1 y cota 10^5.

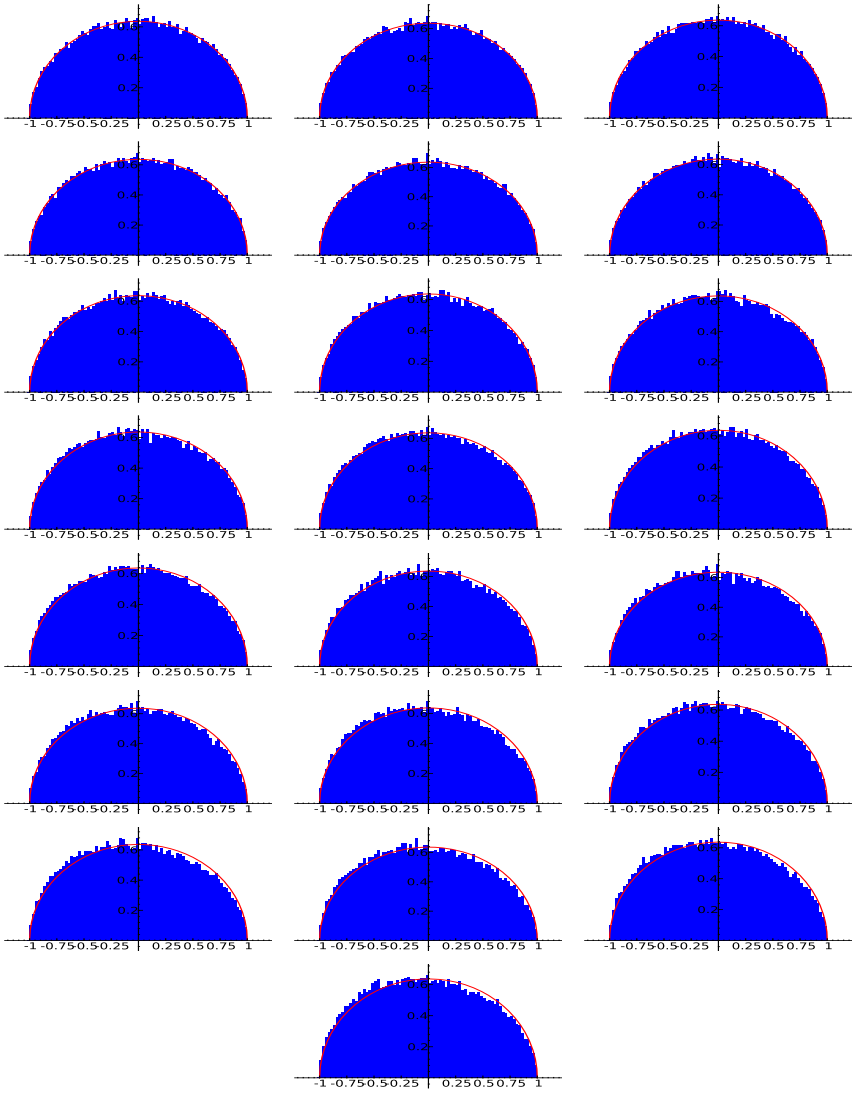
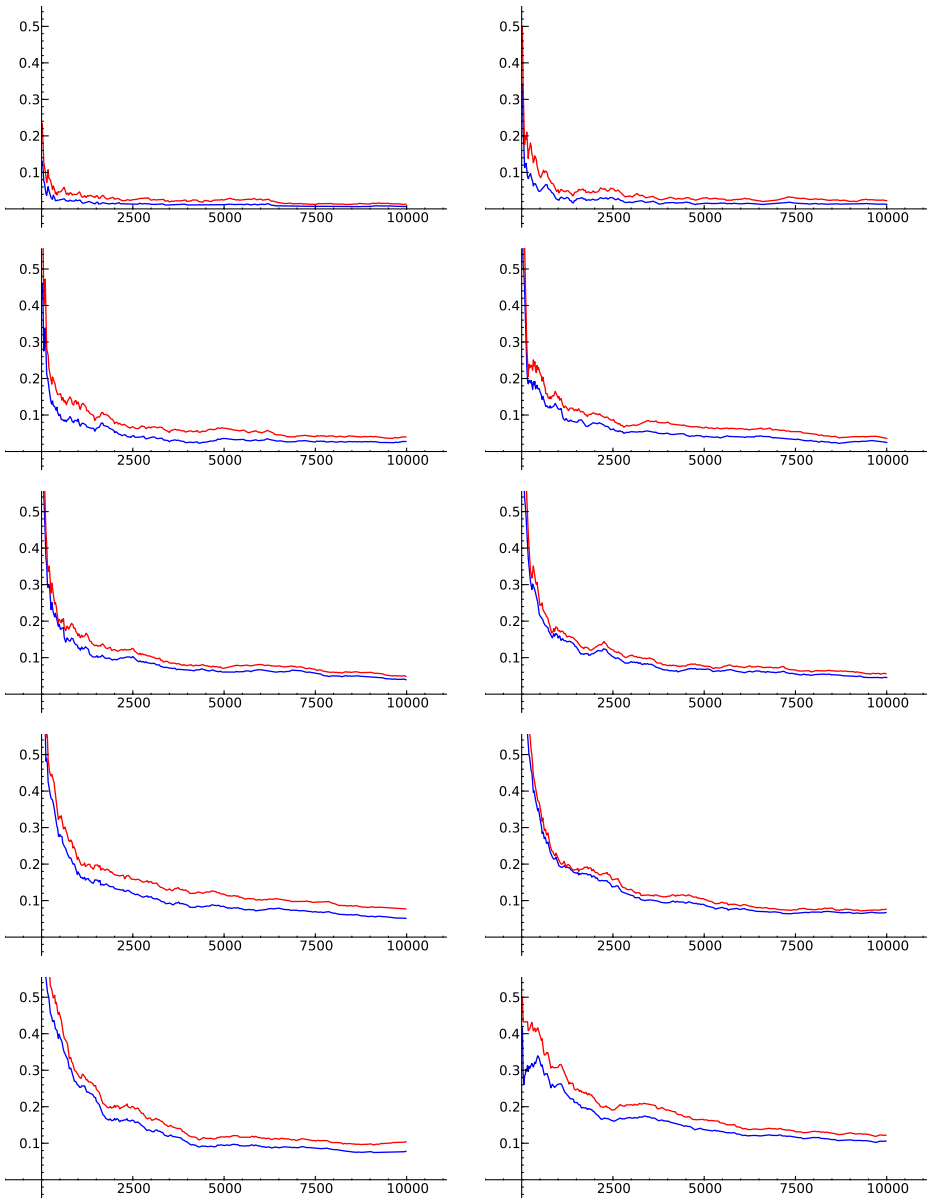


Figura A.4: Histogramas de la distribución normalizada de la sucesión $(a_p/2\sqrt{p})_{p<X}$, para las curvas de la sección A.1 y cota 10^6.

A.3. Gráficas de Δ y Δ_∞

En esta sección presentamos las gráficas de las funciones $\Delta(C)$ y $\Delta_\infty(C)$ primero para $C < 10^4$ luego para $C < 10^5$ y finalmente para $C < 10^6$. Las gráficas estarán ordenados por rango de menor a mayor yendo de izquierda a derecha y de arriba hacia abajo.



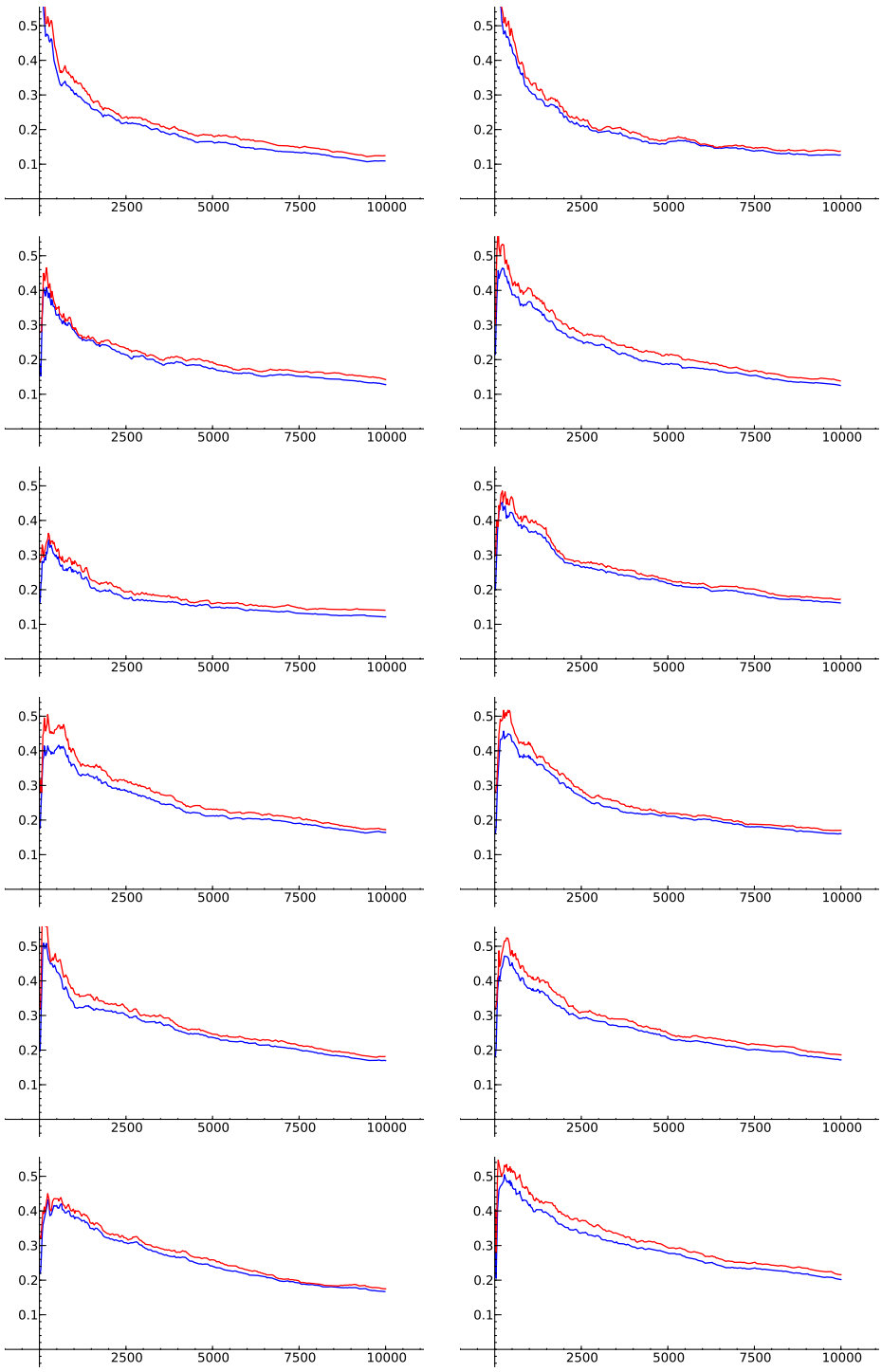
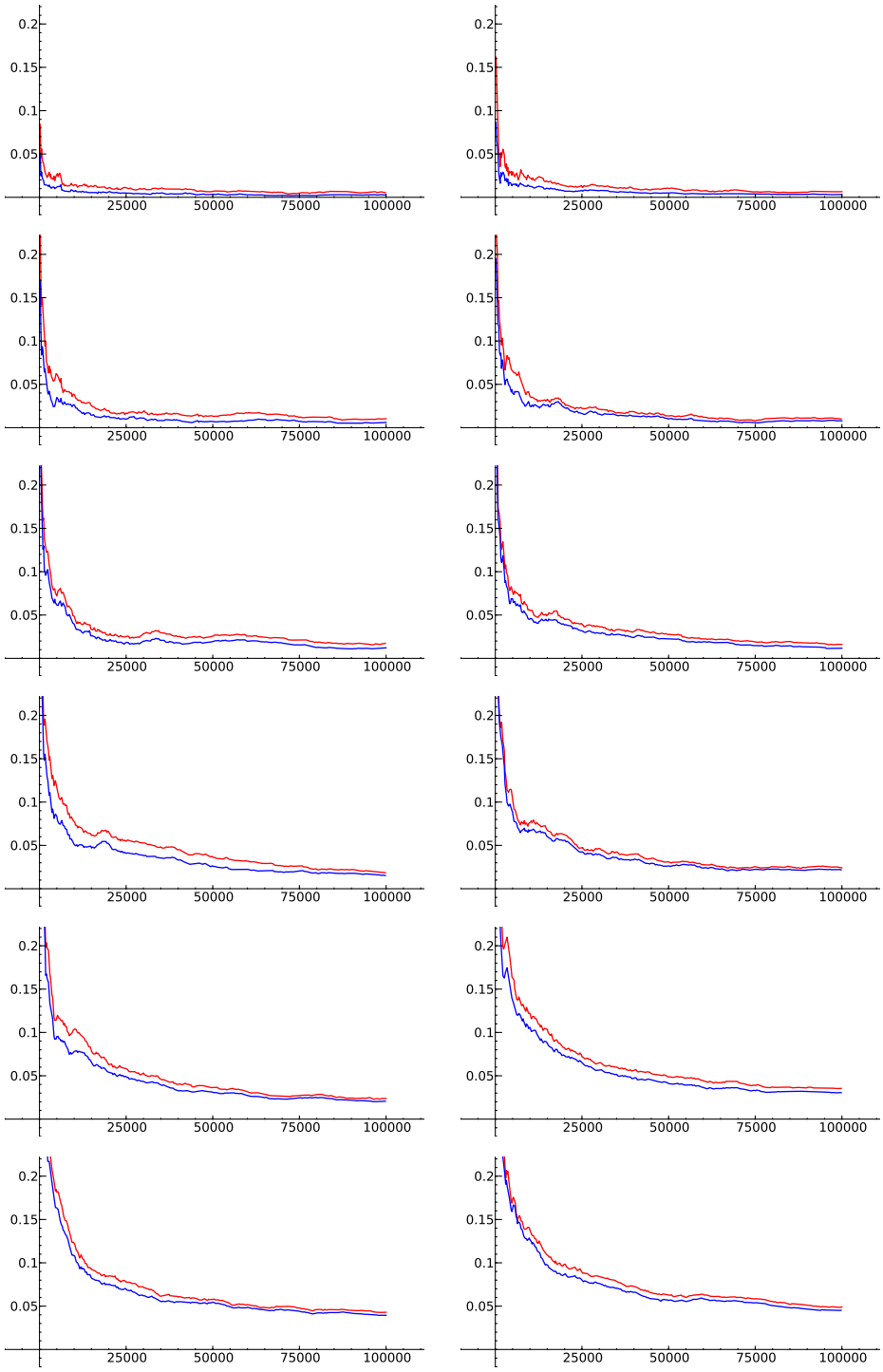


Figura A.5: Gráficas de $\Delta(C)$ y $\Delta_\infty(C)$ para las curvas de la sección A.1 y $C < 10^4$.


0.2
0.15
0.1
0.05
25000
50000
75000
100000

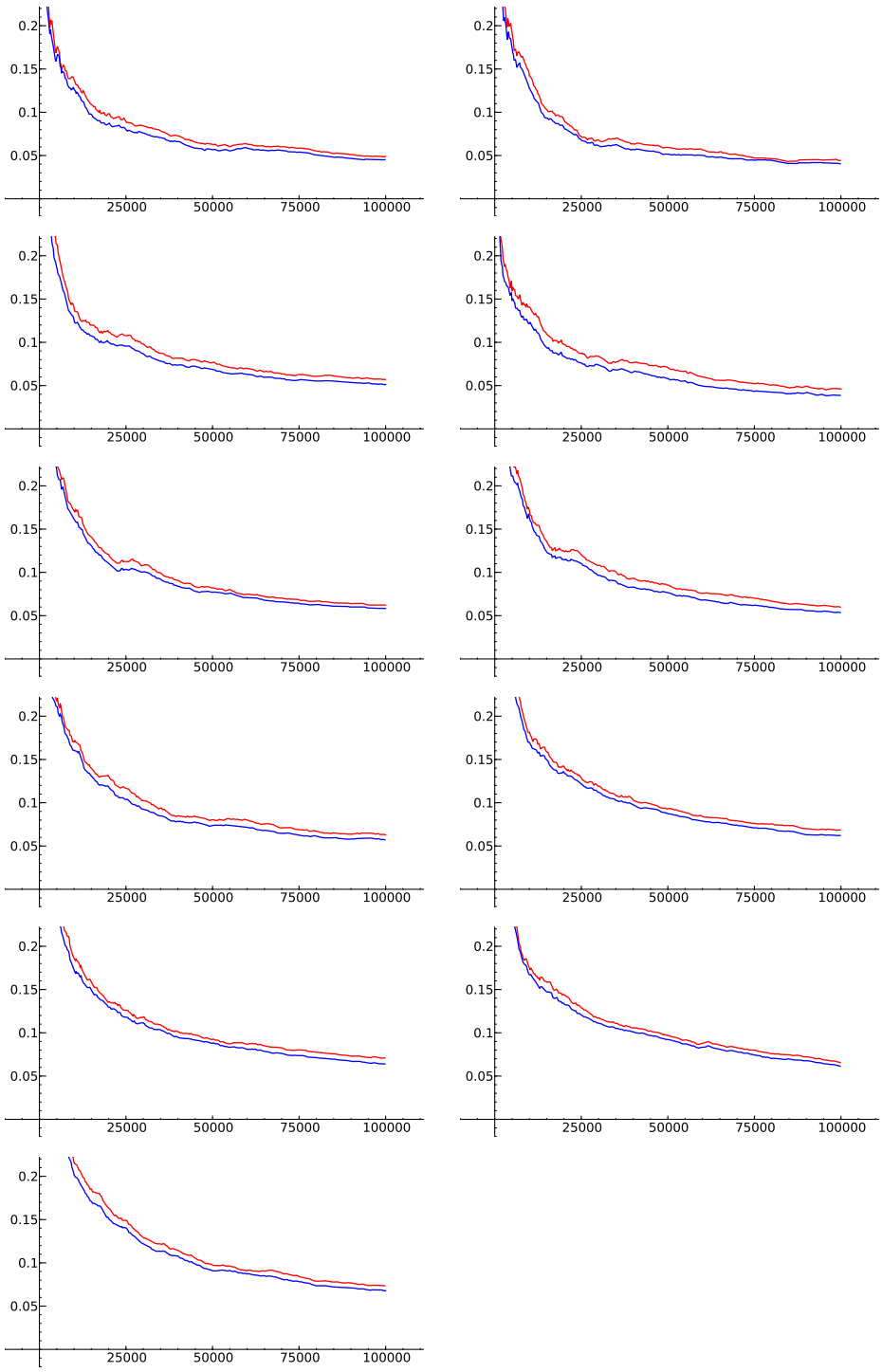
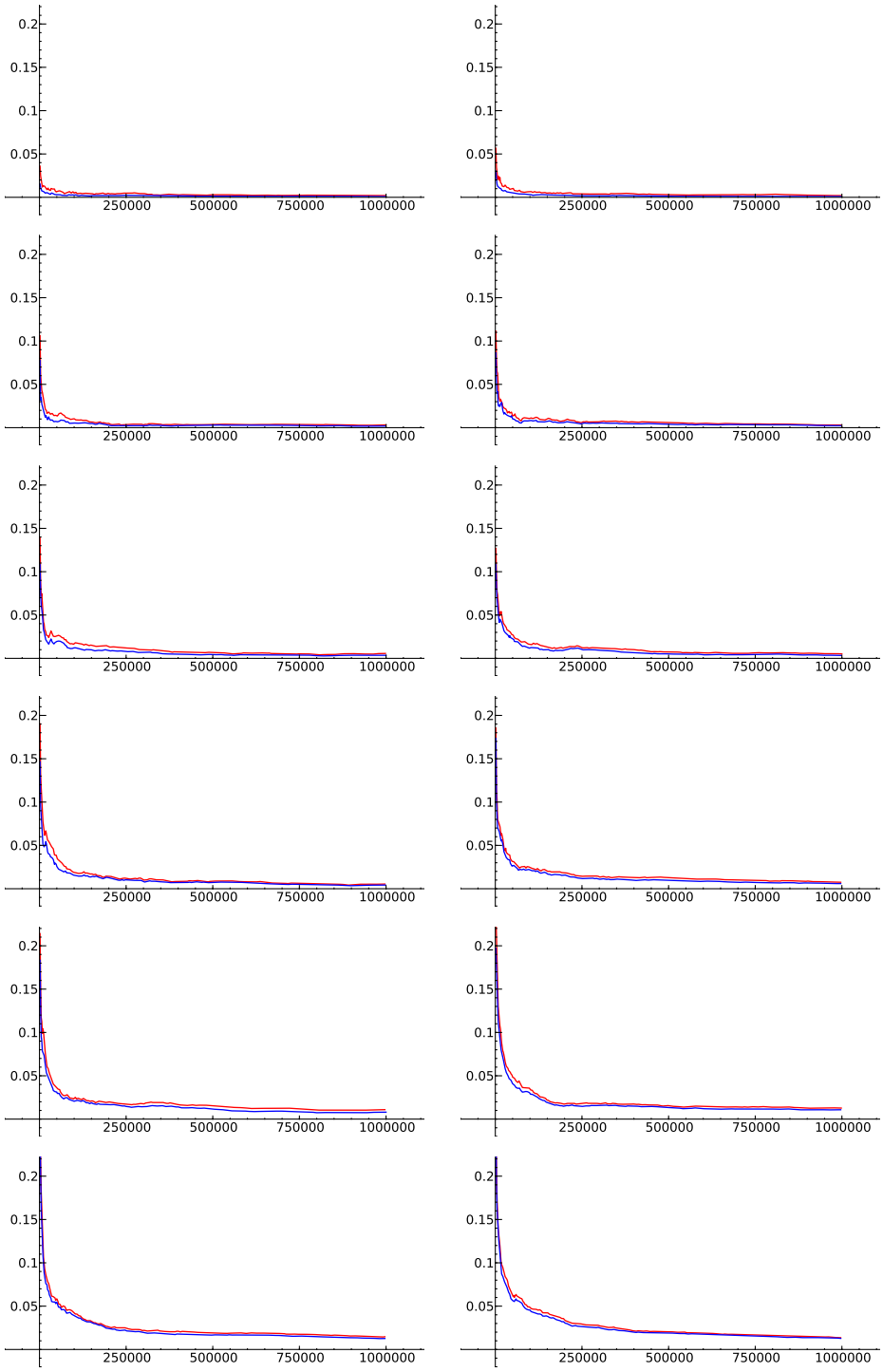


Figura A.6: Gráficas de $\Delta(C)$ y $\Delta_\infty(C)$ para las curvas de la sección A.1 y $C < 10^5$.


0.2
0.15
0.1
0.05
250000
500000
750000
1000000

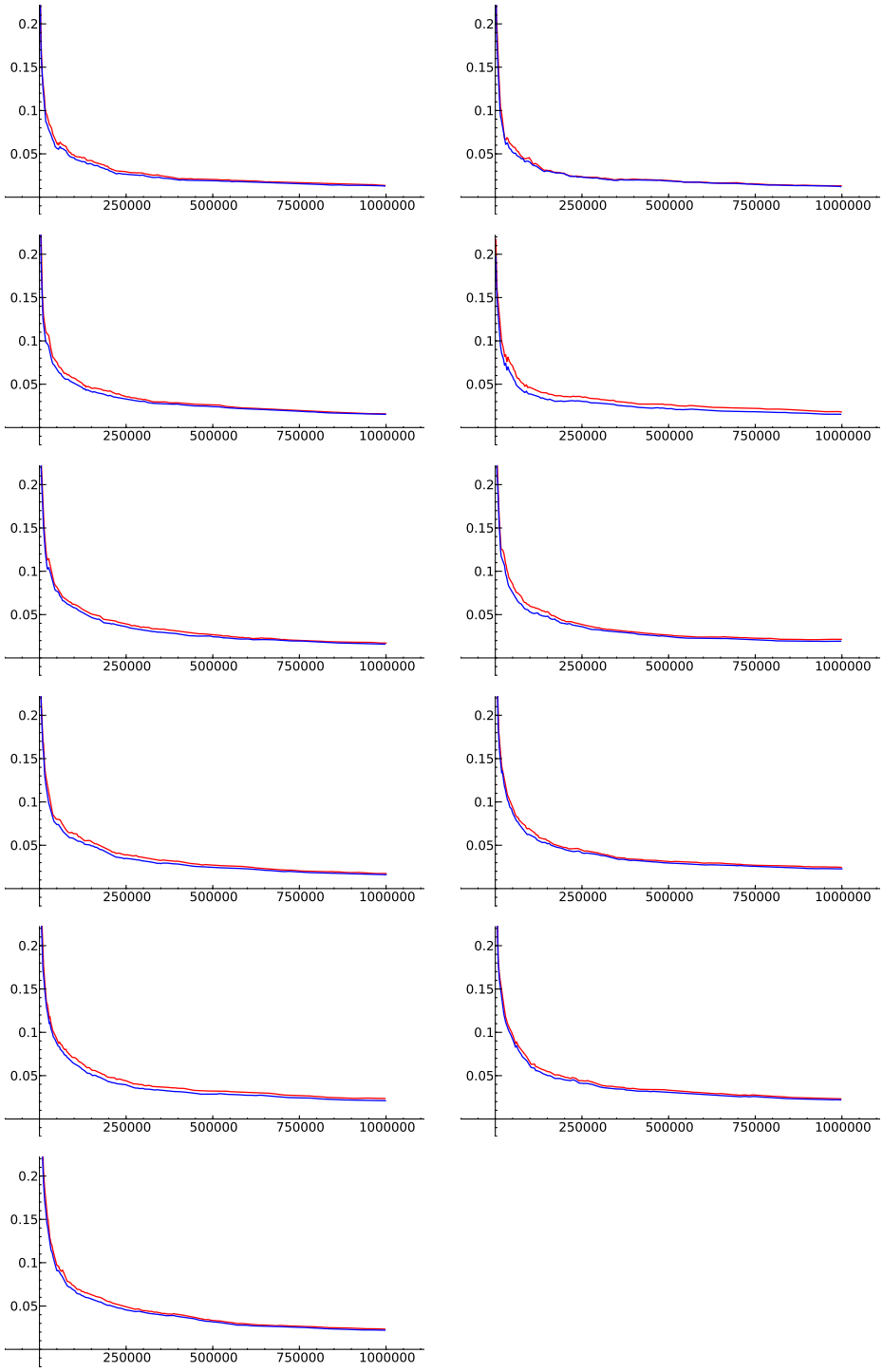
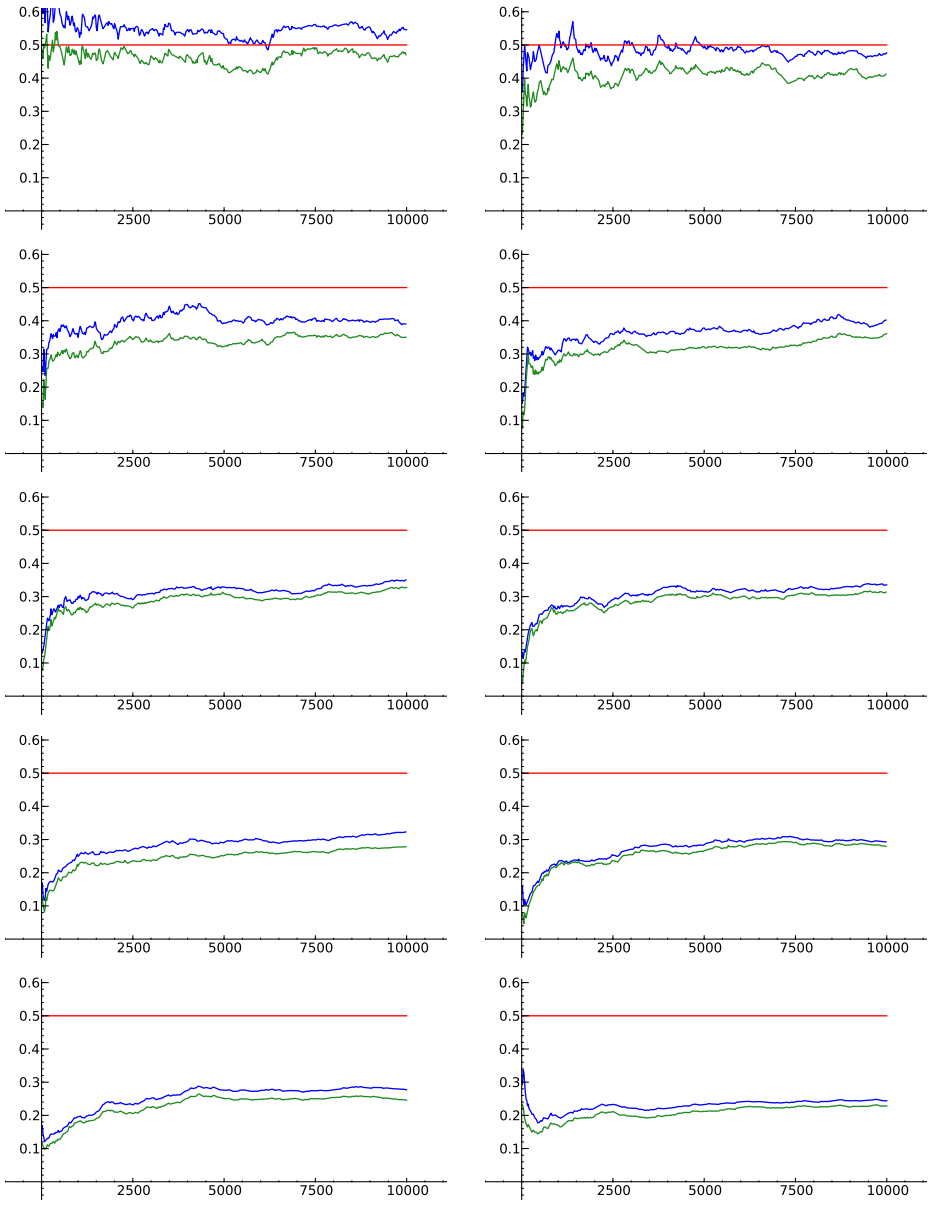


Figura A.7: Gráficas de $\Delta(C)$ y $\Delta_\infty(C)$ para las curvas de la sección A.1 y $C < 10^6$.

A.4. Gráficas logarítmicas de Δ y Δ_∞

En esta sección presentamos las gráficas de las funciones $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ primero para $C < 10^4$ luego para $C < 10^5$ y finalmente para $C < 10^6$. Las gráficas estarán ordenados por rango de menor a mayor yendo de izquierda a derecha y de arriba hacia abajo.



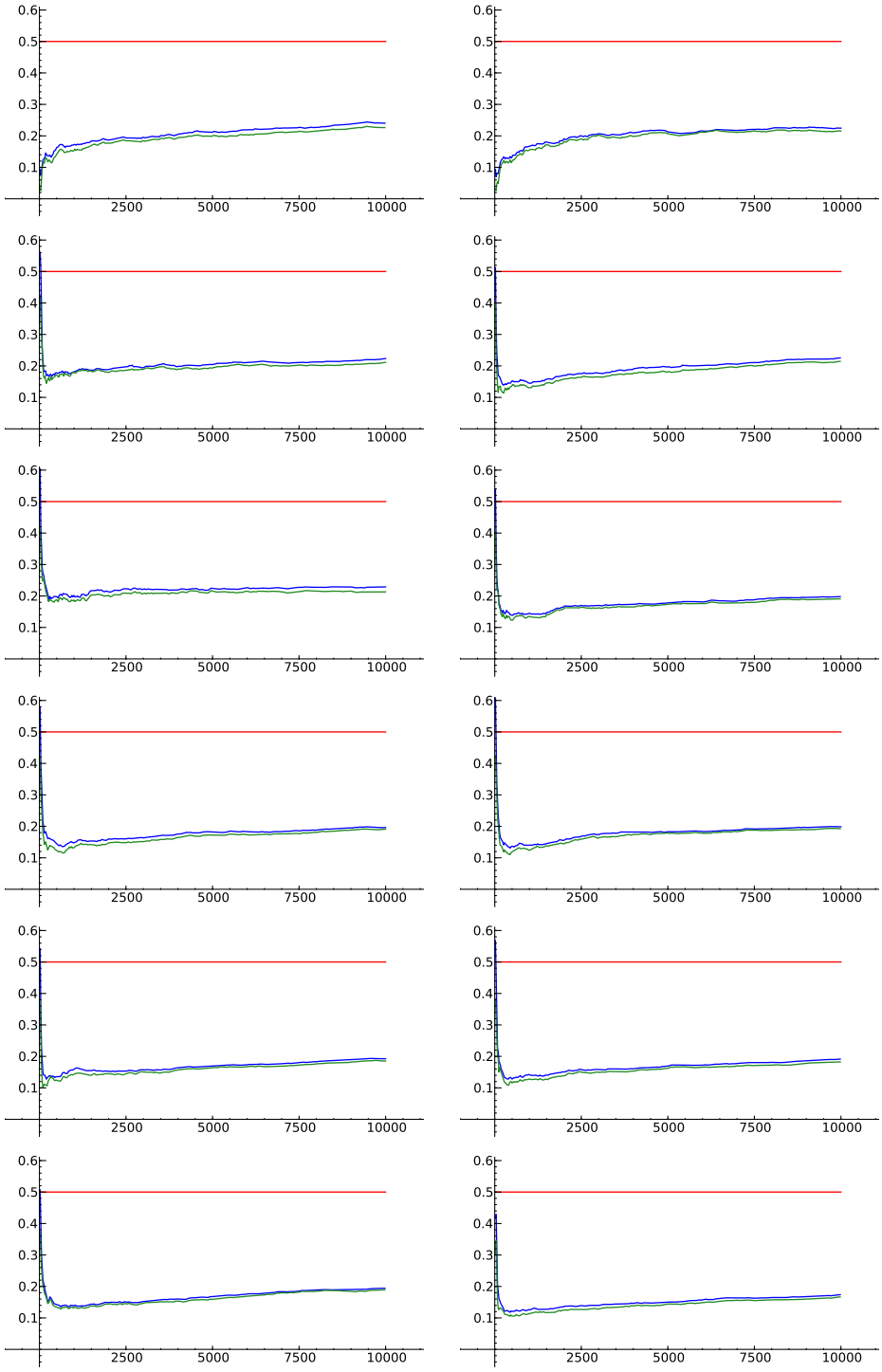
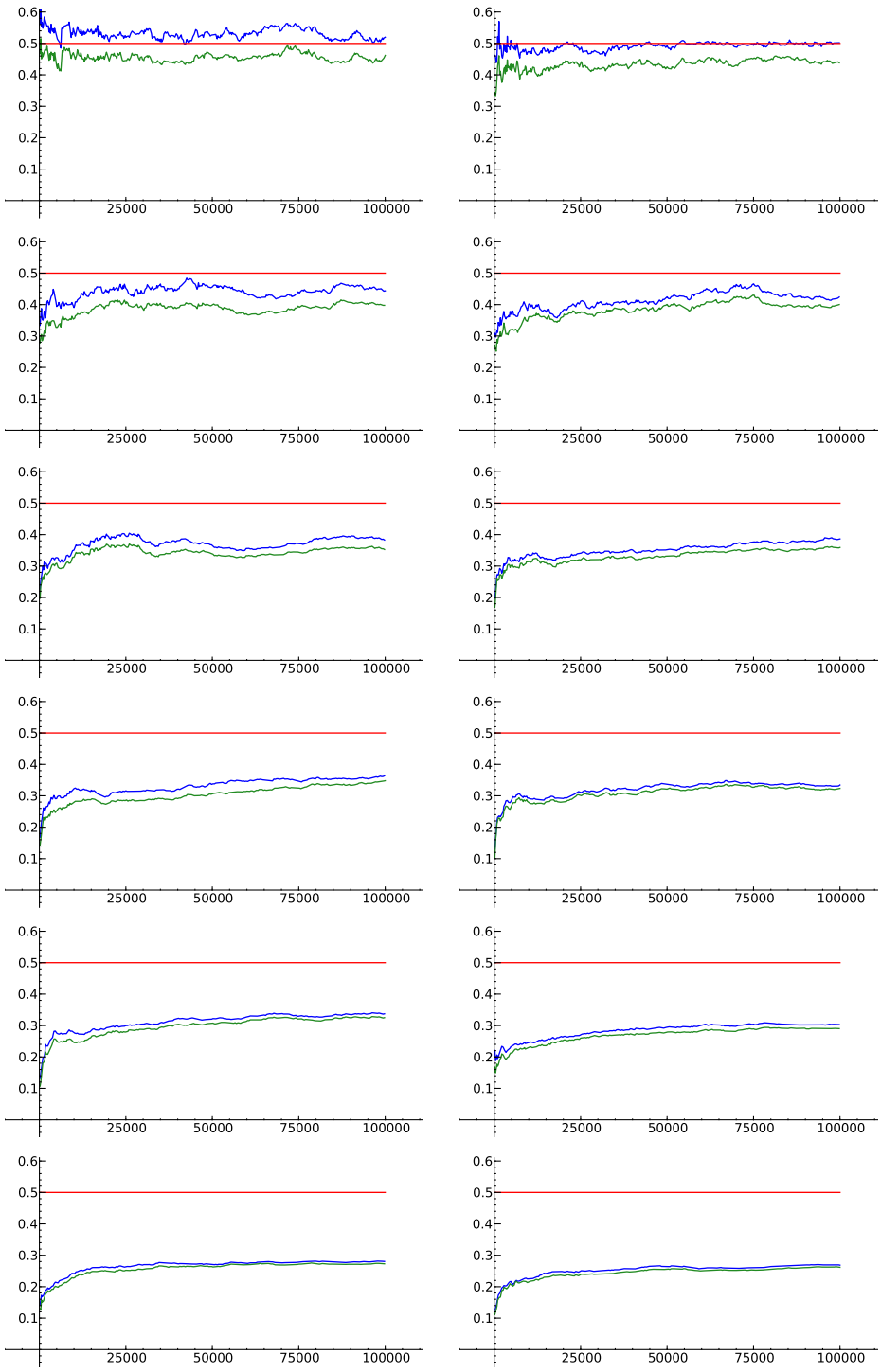


Figura A.8: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ para las curvas de la sección A.1 y $C < 10^4$.


0.6
0.5
0.4
0.3
0.2
0.1
25000
50000
75000
100000

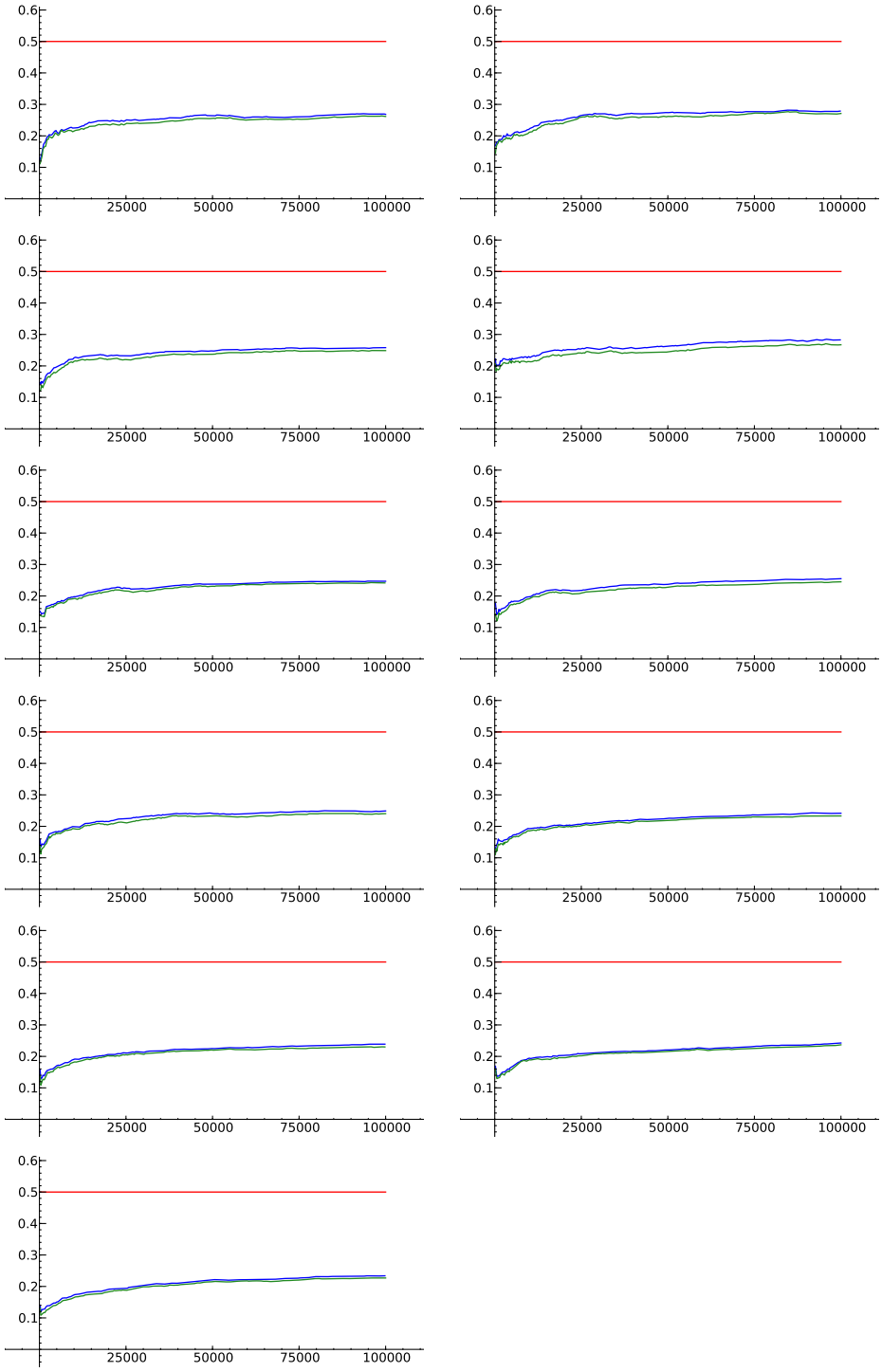
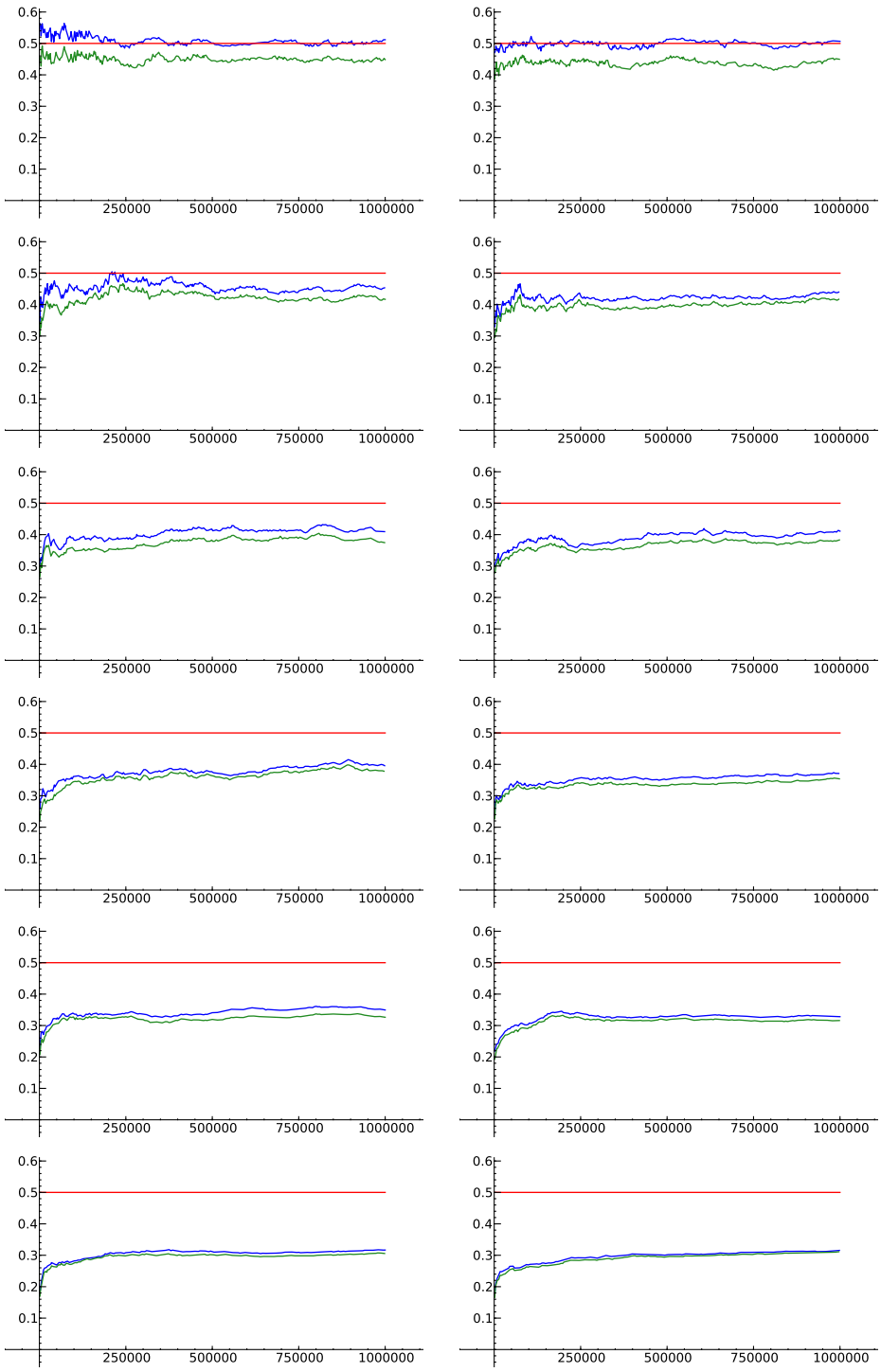


Figura A.9: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ para las curvas de la sección A.1 y $C < 10^5$.


0.6
0.5
0.4
0.3
0.2
0.1
250000
500000
750000
1000000

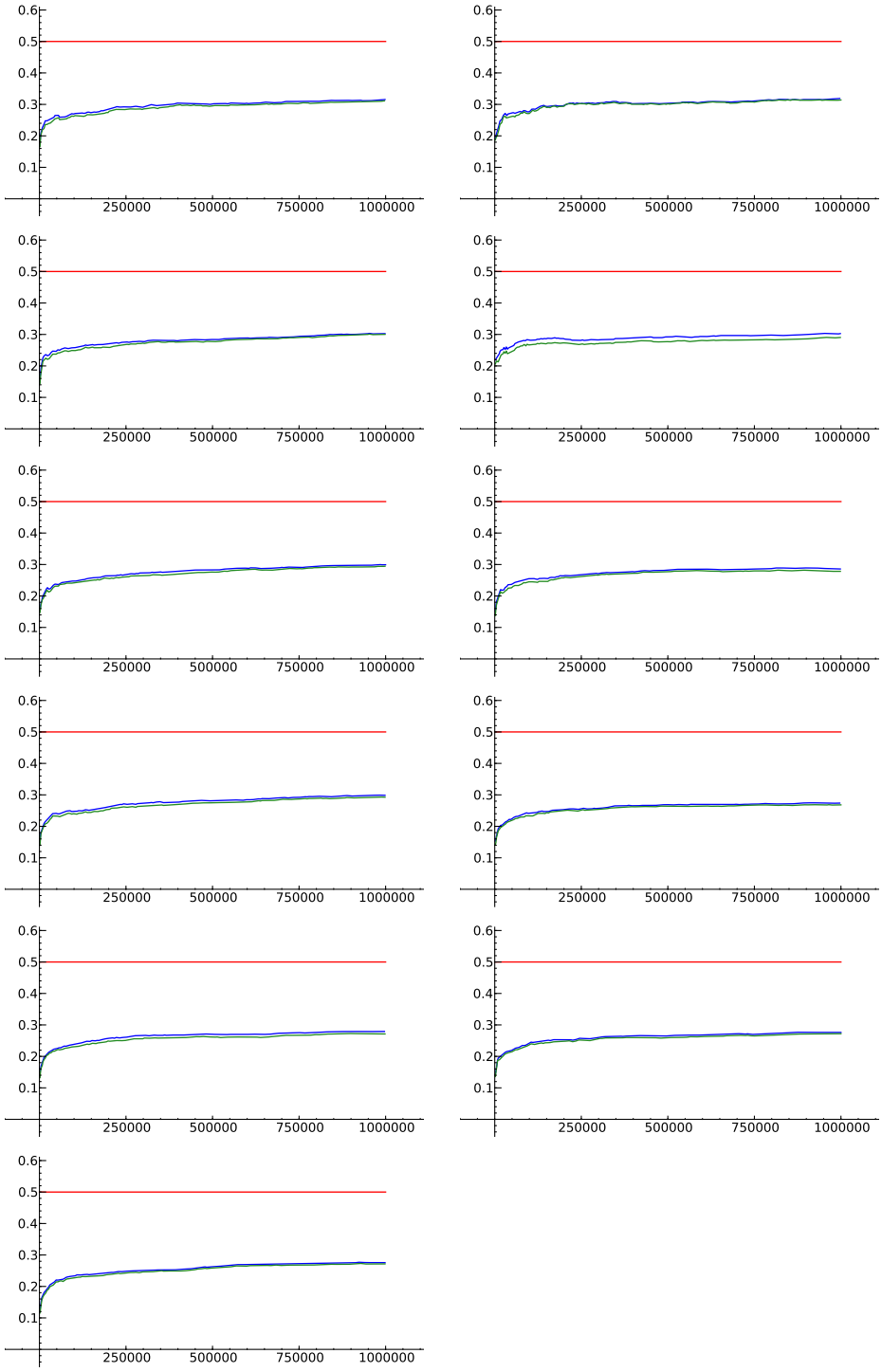
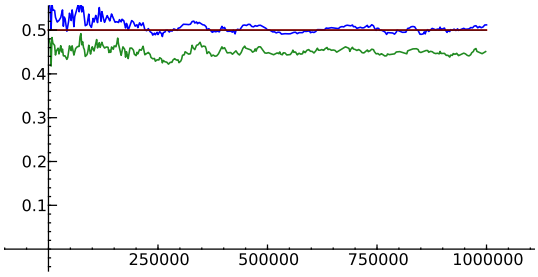


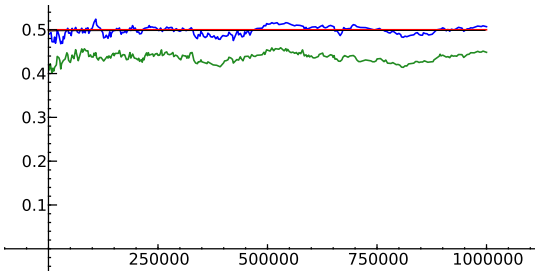
Figura A.10: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ para las curvas de la sección A.1 y $C < 10^6$.

A.5. Gráficas logarítmicas de Δ, Δ_∞ y aproximaciones

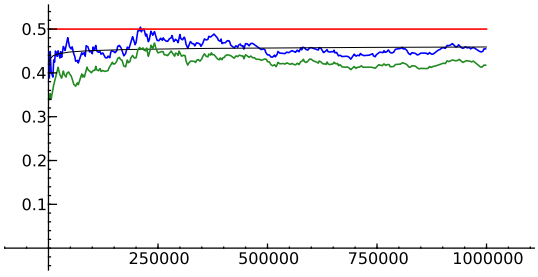
En esta sección presentamos las gráficas de las funciones $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y las aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(C)}$, con α hallado experimentalmente para ajustar la curva $-\log_C(\Delta(C))$, con $C < 10^6$. Las gráficas estarán ordenados por rango de menor a mayor yendo de arriba hacia abajo. También mostraremos los α hallados y una gráfica rango contra α.



(a) Rango$(E) = 0$, $\alpha = 0$, $p < 10^6$

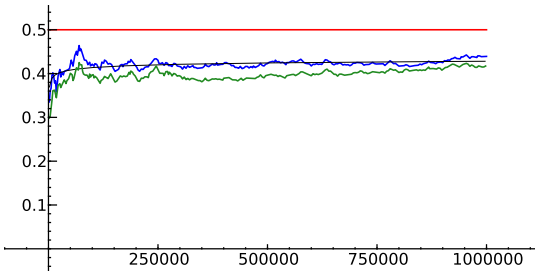


(b) Rango$(E) = 1$, $\alpha = 0{,}025$, $p < 10^6$

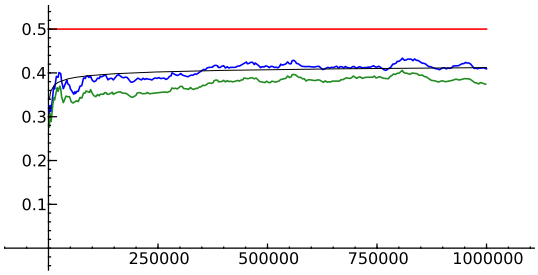


(c) Rango$(E) = 2$, $\alpha = 0{,}56$, $p < 10^6$

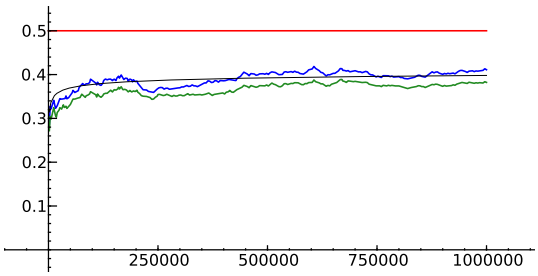
Figura A.11: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.



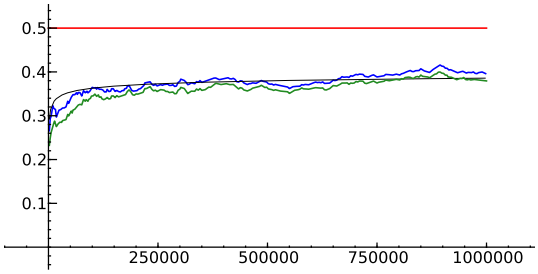
(a) Rango$(E) = 3$, $\alpha = 0{,}99$, $p < 10^6$



(b) Rango$(E) = 4$, $\alpha = 1{,}21$, $p < 10^6$

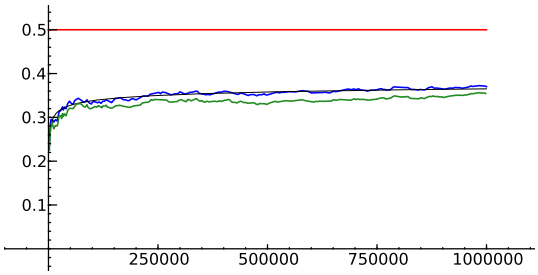


(c) Rango$(E) = 5$, $\alpha = 1{,}41$, $p < 10^6$

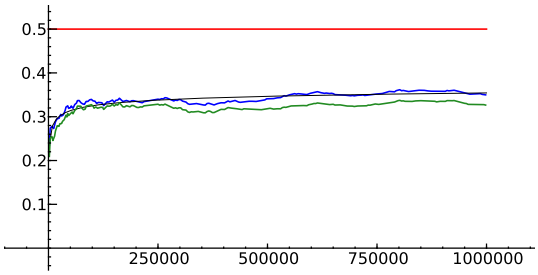


(d) Rango$(E) = 6$, $\alpha = 1{,}58$, $p < 10^6$

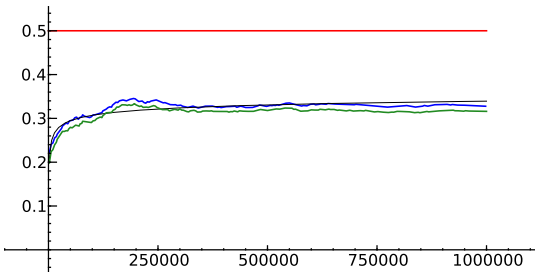
Figura A.12: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.



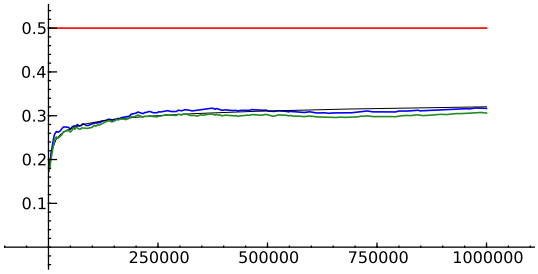
(a) Rango$(E) = 7$, $\alpha = 1{,}86$, $p < 10^6$



(b) Rango$(E) = 8$, $\alpha = 2{,}01$, $p < 10^6$

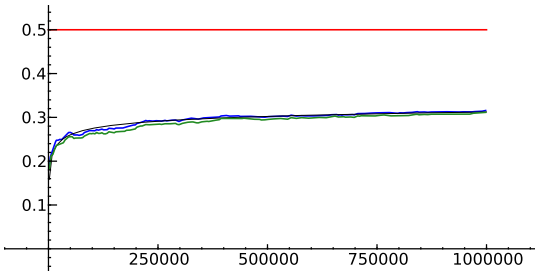


(c) Rango$(E) = 11$, $\alpha = 2{,}22$, $p < 10^6$

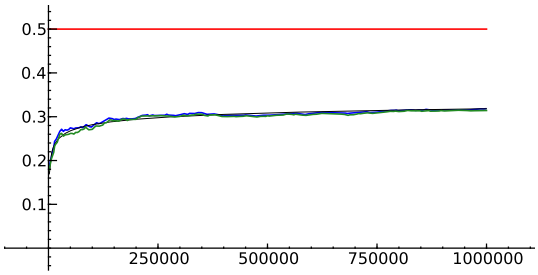


(d) Rango$(E) = 12$, $\alpha = 2{,}48$, $p < 10^6$

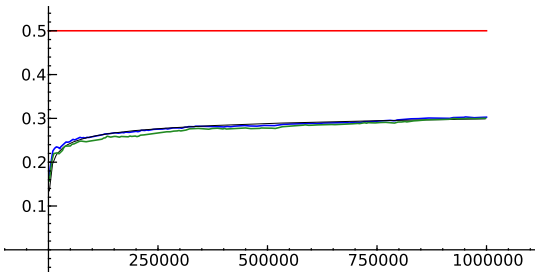
Figura A.13: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.



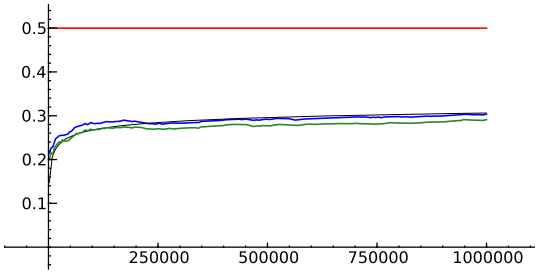
(a) Rango$(E) = 14$, $\alpha = 2{,}59$, $p < 10^6$



(b) Rango$(E) = 15$, $\alpha = 2{,}51$, $p < 10^6$

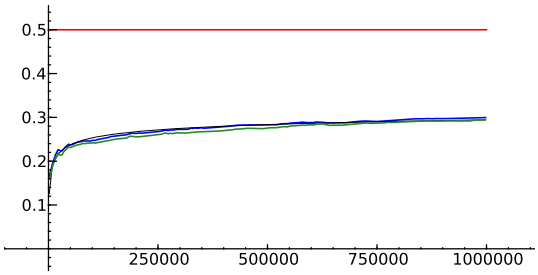


(c) Rango$(E) = 17$, $\alpha = 2{,}78$, $p < 10^6$

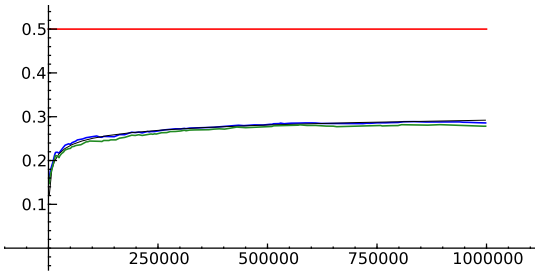


(d) Rango$(E) = 18$, $\alpha = 2{,}67$, $p < 10^6$

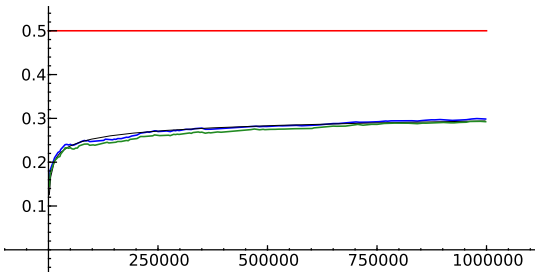
Figura A.14: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.



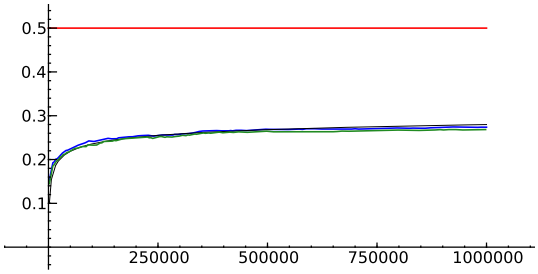
(a) Rango$(E) = 19$, $\alpha = 2{,}83$, $p < 10^6$



(b) Rango$(E) = 20$, $\alpha = 2{,}87$, $p < 10^6$

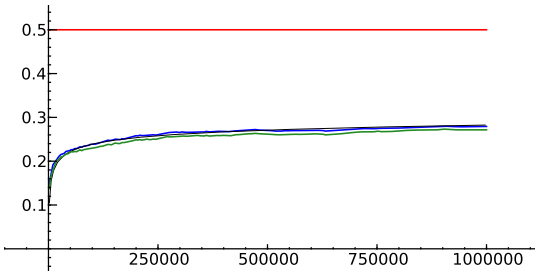


(c) Rango$(E) = 21$, $\alpha = 2{,}84$, $p < 10^6$

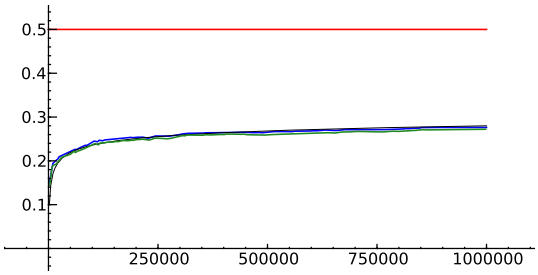


(d) Rango$(E) = 22$, $\alpha = 3{,}04$, $p < 10^6$

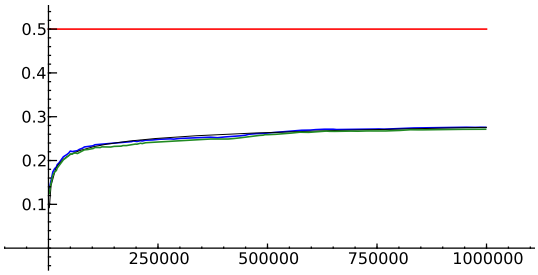
Figura A.15: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.



(a) Rango$(E) = 23$, $\alpha = 3{,}01$, $p < 10^6$



(b) Rango$(E) = 24$, $\alpha = 3{,}03$, $p < 10^6$



(c) Rango$(E) = 28$, $\alpha = 3{,}10$, $p < 10^6$

Figura A.16: Gráficas de $-\log_C(\Delta(C))$ y $-\log_C(\Delta_\infty(C))$ y sus aproximaciones $\frac{1}{2} - \frac{\alpha}{\log(X)}$ en negro para curvas elípticas E.

Índice de figuras

Bibliografía

[CR] Leonard S. Charlap and David P. Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Expository Report 31, December 1993

[Coh] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)

[Csi] János A. Csirik, *An exposition of the SEA algorithm*, http://www.csirik.net/

[Pari] http://pari.math.u-bordeaux.fr/

[Sage] http://www.sagemath.org/

[Sch] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494. MR MR777280 (86e:11122)

[Sil] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original. MR MR1329092 (95m:11054)

[ST] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR MR1171452 (93g:11003)

[Ste1] William Stein, *On convergence in the Sato-Tate conjecture* http://wiki.sagemath.org/days5/sched

[Ste2] William Stein, *Elementary number theory: primes, congruences, and secrets*, Undergraduate Texts in Mathematics, Springer, New York, 2009, A computational approach. MR MR2464052

[Swi] Christopher J. Swierczewski, *Connections Between the Riemann Hypothesis and the Sato-Tate Conjecture*

[Tay] Taylor, Richard (2008), .ªutomorphy for some l-adic lifts of automorphic mod l Galois representations. II", Publ. Math. Inst. Hautes Études Sci. 108: 183–239