Introducción a las Curvas Elípticas

Tesis de Licenciatura en Matemáticas

Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Alumna: Matilde Noemí Lalín
Director: Dr. Fernando Rodríguez-Villegas [1]
Codirector: Dr. Carlos Sánchez[2]

1999

[1]University of Texas at Austin
[2]Universidad de Buenos Aires

Índice

1. Introducción

Consideremos el siguiente problema:

Un entero positivo n se dice **congruente** cuando es igual al área de un triángulo rectángulo de lados racionales. Por ejemplo el triángulo rectángulo de lados 3, 4 y 5 tiene área 6 y por lo tanto n=6 es congruente. Los números congruentes fueron estudiados alrededor de 984 A.C. y luego por Fibonacci en 1225 y por Fermat. Por ejemplo, Fermat probó que el 1, 2 y el 3 no son congruentes. Fibonacci probó que el 5 lo es por el triángulo de lados $(\frac{3}{2}, \frac{20}{3}, \frac{41}{6})$.

Un primer paso para estudiar el problema es la siguiente:

Proposición 1 *Si $n \in \mathbb{Z}$ positivo es libre de cuadrados, entonces son equivalentes:*

(1) *n es congruente: $n = \frac{a.b}{2}$, donde (a, b, c) es una tripla Pitagórica.*

(2) *Existen tres cuadrados racionales en progresión aritmética con diferencia n.*

(3) *Existe un punto racional en*

$$Y^2Z = X^3 - n^2XZ^2 \tag{1}$$

distinto de $(-n, 0), (0, 0), (n, 0)$ y $\mathbf{o} = [0 : 1 : 0]$ (del plano proyectivo)

Demostración: (1) $\Rightarrow$ (2). Dados (a, b, c) sea $x = \frac{c^2}{4}$. Entonces $\frac{(a-b)^2}{4} = x - n$ y $\frac{(a+b)^2}{4} = x + n$ por lo tanto $x - n$, x y $x + n$ son cuadrados de números racionales.

(2) $\Rightarrow$ (1). Dados x tales que $x - n$, x y $x + n$ son todos cuadrados, sean:

$$\begin{aligned} a &= (x+n)^{\frac{1}{2}} + (x-n)^{\frac{1}{2}} \\ b &= (x+n)^{\frac{1}{2}} - (x-n)^{\frac{1}{2}} \\ c &= 2x^{\frac{1}{2}} \end{aligned}$$

Entonces a, b y c son racionales y $a^2 + b^2 = c^2$.

(2) $\Rightarrow$ (3). Si x es el término medio de la progresión, entonces el producto de los tres es $x^3 - n^2x$ y es un cuadrado. Luego se satisface la ecuación (1) con el x (el término medio de la progresión). La progresión no puede ser $-2n, -n, 0$, $-n, 0, n$, o $0, n, 2n$ porque n es libre de cuadrados, luego $x \neq -n, 0, n$. Entonces se satisface (3).

Mas adelante vamos a ver (3) $\Rightarrow$ (2).

La ecuación (1) que obtuvimos es lo que se llama una curva elíptica. Ya veremos como extraer información de esta ecuación, parte de la cual nos orientará acerca de si un número es congruente o no.

2. Curvas Planas

Sea k un cuerpo. El plano afín sobre k es k^2. Un polinomio no constante $f \in k[X, Y]$, sin factores repetidos en $\overline{k}[X, Y]$, define una **curva afín** $\mathcal{C}$ sobre k cuyos puntos sobre K, con K una extensión de k son:

$$\mathcal{C}(K) = \{(x, y) \in K^2 | f(x, y) = 0\}$$

La curva $\mathcal{C}$ se dice **irreducible** si f lo es y **geométricamente irreducible** si f es irreducible sobre $\overline{k}$.

Un punto $\mathbf{x} = (x, y) \in \mathcal{C} : f(x, y) = 0$ se dice **singular** si

$$\frac{\partial f(\mathbf{x})}{\partial x} = \frac{\partial f(\mathbf{x})}{\partial y} = 0$$

En caso contrario, $\mathbf{x}$ se dice **no singular**. Decimos que $\mathcal{C}$ sobre k es **no singular** si lo es en cada punto de $\mathcal{C}(\overline{k})$.

El **plano proyectivo** sobre k se define como

$$\mathbb{P}^2(k) = \{[x : y : z] | x, y, z \in k, (x, y, z) \neq (0, 0, 0)$$

$$[x : y : z] = [x' : y' : z'] \iff \exists \lambda \in k | (x, y, z) = (\lambda x', \lambda y', \lambda z')\}$$

Una **línea** o **recta** en el plano proyectivo se define como el conjunto

$$\mathcal{L}(k) = \{[x : y : z] | ax + by + cz = 0\}$$

El plano afín k^2 tiene una inmersión natural en $\mathbb{P}^2(k)$, la función que manda (X, Y) en $[X : Y : 1]$. El conjunto que "se pierde" con $Z = 0$ es la **recta del infinito**. Los puntos con $Z = 0$ se llaman **puntos del infinito**.

Decimos que un polinomio $F \in k[X, Y, Z]$ es **homogéneo** de grado d si cada monomio de F tiene grado d. Esto sucede si y solo si:

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X, Y, Z)$$

El conjunto de los polinomios homogéneos de grado d en k se denota con $k[X,Y,Z]_d$.

Sea $F \in k[X,Y,Z]_d$ polinomio homogéneo no constante. Identificamos dos polinomios si son múltiplos uno de otro. Aunque F no se puede evaluar en los puntos de $\mathbb{P}^2(k)$ como una función, el conjunto:

$$\mathcal{C}(k) = \{[x:y:z] \in \mathbb{P}^2(k) | F(x,y,z) = 0\}$$

está bien definido y se llama el conjunto de los **k-puntos racionales** de la **curva proyectiva** $\mathcal{C}$ sobre el cuerpo k que queda determinada por el polinomio F.

Un punto $\mathbf{x} = [x:y:z] \in \mathcal{C} : F(x,y,z) = 0$ se dice **singular** si

$$\frac{\partial F(\mathbf{x})}{\partial x} = \frac{\partial F(\mathbf{x})}{\partial y} = \frac{\partial F(\mathbf{x})}{\partial z} = 0$$

En caso contrario, $\mathbf{x}$ se dice **no singular**. Decimos que $\mathcal{C}$ sobre k es **no singular** si lo es en cada punto de $\mathcal{C}(\overline{k})$.

Queremos estudiar la curva $\mathcal{C}$ determinada por $F(X,Y,Z) = 0$ en un punto $[x_0 : y_0 : z_0]$. Sea A una transformación lineal inversible tal que $A(x_0, y_0, z_0) = (0,0,1)$. De este modo podemos trabajar en el plano afín con

$$f(X,Y) = F(A^{-1}(X,Y,1))$$

y para investigar como se comporta $\mathcal{C}$ cerca del punto $[x_0 : y_0 : z_0]$, bastará estudiar como se comporta la ecuación afín

$$f(X,Y) = 0$$

cerca del $(0,0)$. Escribimos

$$f(X,Y) = f_0(X,Y) + f_1(X,Y) + ...$$

donde cada f_j es un polinomio homogéneo de grado j. La suma será finita porque f es un polinomio. Como $f(0,0) = 0$, $f_0 \equiv 0$. Se ve que un punto es no singular cuando $f_1 \not\equiv 0$. En ese caso la ecuación $f_1(X,Y) = 0$ es la ecuación de la recta tangente a f en el $(0,0)$. Si pensamos a f_1 como polinomio de tres variables independiente de la tercera,

$$L_T = f_1 \circ A$$

es la ecuación de la **recta tangente** a $\mathcal{C}$ en el punto $[x_0 : y_0 : z_0]$.

Mas general, si $f_j \equiv 0 \quad \forall j < l$ y además $f_l \not\equiv 0$, entonces decimos que $\mathcal{C}(k)$ tiene multiplicidad l en $\mathbf{x}$ y escribimos $l = m_F(\mathbf{x})$.

Sea ahora $\mathcal{C} : F = 0$, $F \in k[X, Y, Z]_d$ como antes, $\mathcal{L} : R = 0$, $R \in k[X, Y, Z]_1$ una recta del plano proyectivo y $\mathbf{x} = [x_0 : y_0 : z_0] \in \mathcal{C}(k) \cap \mathcal{L}(k)$. A es como antes y tenemos:

$$\begin{aligned} f(X,Y) &= F(A^{-1}(X,Y,1)) = f_1(X,Y) + ... + f_d(X,Y) \\ r(X,Y) &= R(A^{-1}(X,Y,1)) \end{aligned}$$

Como $r(0,0) = 0$, $r(X,Y) = bX - aY$ con a, b no ambos nulos. Entonces $\phi(t) = (at, bt)$ parametriza a la recta. Luego,

$$\begin{aligned} f(\phi(t)) &= f_1(at,bt) + f_2(at,bt) + ... + f_d(at,bt) \\ &= tf_1(a,b) + t^2 f_2(a,b) + ... + t^d f_d(a,b) \end{aligned}$$

Hay dos posibilidades. Si $f \circ \phi$ no es el polinomio identicamente cero, entonces $f(\phi(t))$ tiene un cero de algún orden en $t = 0$ y este orden es

$$i(\mathbf{x}, \mathcal{L}, \mathcal{C})$$

la **multiplicidad de intersección** de la recta $\mathcal{L}$ y la curva $\mathcal{C}$ en el punto $\mathbf{x}$. Si $f \circ \phi$ es el polinomio nulo, diremos que $i(\mathbf{x}, \mathcal{L}, \mathcal{C}) = \infty$. También definiremos que $i(\mathbf{x}, \mathcal{L}, \mathcal{C}) = 0$ en el caso en que $\mathbf{x} \notin \mathcal{C}(k) \cap \mathcal{L}(k)$. Se puede probar que esta definición no depende de la elección de la transformación A.

En realidad la multiplicidad de intersección se puede definir de un modo más general para dos curvas afines que no tengan una componente común que pase por $\mathbf{x}$, y vale que

$$i(\mathbf{x}, \mathcal{C}, \mathcal{D}) \geq m_{\mathcal{C}}(\mathbf{x}) m_{\mathcal{D}}(\mathbf{x})$$

pero a nosotros sólo nos interesa trabajar el caso en que una de las curvas es una recta, y entonces esta definición es mucho mas manejable.

Supongamos ahora que $\mathbf{x}$ es un punto no singular de $\mathcal{C}$ y sigamos con la notación de antes. Tenemos,

$$\begin{aligned} i(\mathbf{x}, \mathcal{L}, \mathcal{C}) = 1 &\Leftrightarrow f_1(a,b) \neq 0 \\ &\Leftrightarrow (a,b) \notin L_T(k) \\ &\Leftrightarrow \text{Imagen}(\phi) \not\subseteq L_T(k) \\ &\Leftrightarrow \mathcal{L}(k) \not\subseteq L_T(k) \\ &\Leftrightarrow \mathcal{L} \text{ no es la misma que } L_T \end{aligned}$$

Entonces la recta tangente tiene multiplicidad de intersección 2 o mas. Cuando $\mathbf{x}$ es no singular con recta tangente con multiplicidad de intersección mayor que 2, se dice que es un **punto de inflexión**.

Se puede probar que

Proposición 2 *Supongamos que la característica de k no es 2. Sea $\mathcal{C}$ una curva plana definida sobre k por medio del polinomio homogéneo F de grado $d \geq 2$ y sea $\mathbf{x} = [x_0 : y_0 : z_0]$ un punto no singular de la curva. Entonces $\mathbf{x}$ es un punto de inflexión si y solo si $\det H(\mathbf{x}) = 0$, donde*

$$H(x_0, y_0, z_0) = \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}_{(x_0, y_0, z_0)}$$

es la matriz Hessiana de F.

Recordemos:

Teorema 3 *(Bezout) Sea $F \in k[X, Y, Z]_m$ y $G \in k[X, Y, Z]_n$ que determinan dos curvas planas $\mathcal{C}$ y $\mathcal{D}$ respectivamente. Entonces $\mathcal{C}(\overline{k}) \cap \mathcal{D}(\overline{k})$ es no vacío. Mas aún, si suponemos que no tienen ninguna componente irreducible en común, entonces se intersectan sobre $\overline{k}$ en exactamente mn puntos, contados con su multiplicidad de intersección.*

A efectos prácticos, por lo que comentamos sobre la multiplicidad de intersección, lo que implica Bezout es que ambas curvas no pueden coincidir en mas de mn puntos en el sentido siguiente:

$$\sum_{\mathbf{x} \in \mathcal{C}(\overline{k}) \cap \mathcal{D}(\overline{k})} m_{\mathcal{C}}(\mathbf{x}) m_{\mathcal{D}}(\mathbf{x}) \leq mn$$

Entonces una cúbica no singular tiene al menos un punto de inflexión, pues hay que considerar las intersecciones de

$$F(X, Y, Z) = 0$$

y

$$\det H(X, Y, Z) = 0$$

Si la primera tiene grado d, la segunda tiene grado $3(d-2)$, y por el Teorema de Bezout la intersección es no vacía para $d \geq 3$.

También por Bezout, cada recta intersecta a una cúbica no singular en a lo sumo tres puntos. Si tenemos que la cúbica está definida sobre $\mathbb{Q}$ y hay una recta que pasa por dos puntos racionales de la cúbica (contándolos con multiplicidad), entonces la recta corta a la curva en algún otro punto que en principio está definido en alguna extensión de $\mathbb{Q}$, pero resultará definido sobre $\mathbb{Q}$.

En efecto, si

$$f(X,Y) = \sum a_{ij} X^i Y^j \in \mathbb{Q}[X,Y]$$

y (x,y) es un cero de f definido en alguna extensión K de $\mathbb{Q}$ que podemos suponer que es de Galois tomando la clausura normal, $\sigma \in$ Gal $(K/\mathbb{Q})$, vale que

$$0 = \sigma f(x,y) = \sigma\left(\sum a_{ij} x^i y^j\right) = \sum a_{ij} (\sigma x)^i (\sigma y)^j = f(\sigma x, \sigma y).$$

Entonces Gal $(K/\mathbb{Q})$ actúa sobre la curva $\mathcal{C}$ definida por $f(X,Y)$. Mas general, si $\mathcal{C}_1$ y $\mathcal{C}_2$ son dos curvas, entonces Gal $(K/\mathbb{Q})$ estabiliza el conjunto intersección. En nuestro caso, la intersección consta de tres puntos en alguna extensión de $\mathbb{Q}$. Hay tres casos. Puede ser que ninguno de los tres puntos esté definido sobre $\mathbb{Q}$. Puede ser que haya uno solo. O bien, puede ser que haya dos. Sean $\mathbf{x}_1, \mathbf{x}_2$ y $\mathbf{x}_3$ los puntos en cuestión y supongamos que $\mathbf{x}_1, \mathbf{x}_2$ están definidos sobre $\mathbb{Q}$ y $\mathbf{x}_3$ definido sobre una extensión K. Sea $\sigma \in$ Gal $(K/\mathbb{Q})$. Si $\sigma\mathbf{x}_3 \neq \mathbf{x}_3$, entonces por lo que acabamos de decir,

$$\sigma\mathbf{x}_3 = \mathbf{x}_i$$

Para $i = 1$ o 2. Pero $\mathbf{x}_i$ está definido sobre $\mathbb{Q} \Rightarrow \sigma\mathbf{x}_3$ definido sobre $\mathbb{Q}$, $\Rightarrow \mathbf{x}_3$ definido sobre $\mathbb{Q}$.

3. Números p-ádicos

Una función de un cuerpo k a valores reales se llama **valor absoluto** si satisface:

(1) $|r| \geq 0$ con igualdad si y solo si $r = 0$.

(2) $|rs| = |r||s|$.

(3) $|r + s| \leq |r| + |s|$.

Por (2), $|1.r| = |1||r| \Rightarrow |1| = 1$ (tomando $r \neq 0$). Luego $1 = |1| = |(-1)(-1)| = |-1|^2 \Rightarrow |-1| = 1$. De donde

$$|r| = |-r| \quad \forall r \in k$$

Por (1), (3) y la propiedad anterior, (k, d) resulta un espacio métrico con

$$d(r, s) = |r - s|$$

El valor absoluto usual es un ejemplo de valor absoluto (general) en $\mathbb{Q}$ pero hay otros.

Sea p un primo fijo. Cualquier racional $r \neq 0$ se puede escribir de la forma

$$r = p^n \frac{u}{v}$$

con $n \in \mathbb{Z}$, $u, v \in \mathbb{Z}$, $p \not| u$, $p \not| v$. Definimos

$$|r|_p = p^{-n}$$

y

$$|0|_p = 0$$

La definición claramente satisface los puntos (1) y (2). Para ver (3), sea

$$s = p^m \frac{w}{z}$$

con $m \in \mathbb{Z}$, $w, z \in \mathbb{Z}$, $p \not| w$, $p \not| z$. Entonces,

$$|s|_p = p^{-m}$$

Sin pérdida de generalidad podemos suponer que $m \geq n$, o sea que $|s|_p \leq |r|_p$. Luego,

$$r + s = p^n \frac{uz + p^{m-n} vw}{vz}$$

Vale $p \not| vz$. El numerador $uz + p^{m-n} vw$ es un entero que, al menos cuando $n = m$, podría ser divisible por p, pero que no lo es cuando $n \neq m$. Entonces,

$$|r + s|_p \leq p^{-n}$$

con igualdad si $n \neq m$.

Es decir,

$(3')$ $|r+s|_p \leq \max\{|r|_p, |s|_p\}$ con igualdad cuando $|r|_p \neq |s|_p$.

Claramente $(3') \Rightarrow (3)$, con lo cual $|\cdot|_p$ es un valor absoluto. Se llama **valor absoluto p-ádico**. La desigualdad $(3')$ se llama desigualdad ultramétrica. Un valor absoluto que satisface una desigualdad ultramétrica se llama no arquimedeano.

Diremos que una sucesión $\{a_n\}$ es fundamental o de Cauchy si dado $\epsilon > 0$, $\exists n_0 = n_0(\epsilon)$ tal que

$$|a_m - a_n|_p < \epsilon, \qquad \forall m, n \geq n_0$$

La sucesión $\{a_n\}$ converge a b si

$$|a_n - b|_p < \epsilon, \qquad \forall n \geq n_0(\epsilon)$$

El problema es que con esta métrica, $\mathbb{Q}$ no es completo. Por ejemplo con $p = 5$, construyamos una sucesión $\{a_n\}$ que cumpla:

$$a_n^2 + 1 \equiv 0_{mod\, 5^n}$$

$$a_{n+1} \equiv a_{n mod\, 5^n}$$

Digamos $a_1 = 2$. Supongamos que ya tenemos construído a_n. Escribimos $a_{n+1} = a_n + c5^n$ con $c \in \mathbb{Z}$ a determinar. Como

$$(a_n + c5^n)^2 + 1 \equiv 0_{mod\, 5^{n+1}}$$

$$a_n^2 + 1 + 2{,}5^n a_n c + 5^{2n} c^2 \equiv 0_{mod\, 5^{n+1}}$$

de donde

$$2a_n c + k \equiv 0_{mod\, 5}$$

donde $k = \frac{a_n^2+1}{5^n} \in \mathbb{Z}$. Como $5 \not| a_n$ se puede resolver la congruencia anterior para algún c.

La sucesión que se obtuvo es fundamental con la métrica 5-adica pues

$$|a_m - a_n|_5 \leq 5^{-n} \quad \forall m \geq n$$

Supongamos que a_n tiende a un $l \in \mathbb{Q}$. Entonces

$$a_n^2 + 1 \to l^2 + 1$$

Pero por construcción

$$a_n^2 + 1 \to 0$$

Entonces $l^2 + 1 = 0$ absurdo!

Vamos a completar a $\mathbb{Q}$ respecto de la métrica inducida por $|\cdot|_p$. Sea $\mathcal{S}$ el conjunto de las sucesiones de Cauchy $\{a_n\}$ para $|\cdot|_p$ con $a_n \in \mathbb{Q}$. Entonces $\mathcal{S}$ es un anillo con las operaciones:

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \qquad \{a_n\}\{b_n\} = \{a_n b_n\}$$

Una sucesión $\{a_n\}$ es nula si $a_n \to 0$. El conjunto $\mathcal{N}$ de las sucesiones nulas es un ideal de $\mathcal{S}$.

Sea $\{a_n\} \in \mathcal{S}$ pero $\{a_n\} \notin \mathcal{N}$. Se puede ver que hay al menos un N tal que $|a_N - a_n|_p < |a_N|_p$ para todo $n > N$. En efecto, supongamos que para todo N existe un $n > N$ tal que $|a_N|_p \leq |a_N - a_n|_p$. Ahora bien, dado $\epsilon \in \mathbb{R} > 0$, existe n_0 tal que $\forall n, m > n_0$, $|a_n - a_m|_p < \epsilon$. Con esto se sigue que $\forall N > n_0$, $|a_N|_p < \epsilon$. Tomando ϵ arbitrariamente pequeño sale que $|a_N|_p \to 0$ lo cual es absurdo pues $\{a_n\} \notin \mathcal{N}$.

Consideremos entonces N tal que

$$|a_N - a_n|_p < |a_N|_p \quad \forall n > N$$

entonces $|a_n|_p \leq \text{máx}\{|a_N|_p, |a_n - a_N|_p\}$. Pero como $|a_N|_p > |a_n - a_N|_p$, resulta

$$|a_n|_p = |a_N|_p \quad \forall n \leq N$$

Escribimos $|\{a_n\}|_p = |a_N|_p$.

Si $a_n \neq 0$ para todo n, es fácil ver que $\{a_n^{-1}\} \in \mathcal{S}$. En efecto, $|a_n^{-1} - a_m^{-1}|_p = \left|\frac{a_m - a_n}{a_n a_m}\right|_p$. Si ahora tomamos $n, m > \text{máx}\{N, n_0\}$ donde N es como antes y n_0 es tal que $|a_n - a_m|_p < \epsilon |a_N|_p^2$ para todos $n, m > n_0$, entonces

$$|a_n^{-1} - a_m^{-1}|_p = \frac{|a_m - a_n|_p}{|a_n a_m|_p} < \epsilon \quad \forall n, m > \text{máx}\{N, n_0\}$$

Veamos que $\mathcal{N}$ es un ideal maximal de $\mathcal{S}$. Si no lo fuera, estaría contenido en algún ideal maximal $\mathcal{M}$. Existe un $\{a_n\} \in \mathcal{M} \setminus \mathcal{N}$. Entonces solo finitos de los a_n son cero y podemos reeplazarlos por algún racional no nulo (por ejemplo por 1). Hacer esto es como sumarle un elemento de $\mathcal{N}$, asi que seguimos en las mismas condiciones que antes. Podemos suponer que $a_n \neq 0$ para todo n. Entonces $\{a_n^{-1}\} \in \mathcal{S}$ y por lo tanto $\{a_n\}\{a_n^{-1}\} \in \mathcal{M}$. Con lo cual $\mathcal{M} = \mathcal{S}$ absurdo!

Como $\mathcal{N}$ es maximal, $\mathcal{S}/\mathcal{N}$ es un cuerpo.

Consideramos

$$\phi : \mathbb{Q} \to \mathcal{S}/\mathcal{N}$$
$$r \to \{r\}$$

La función $|\{a_n\}|_p$ en $\mathcal{S}$ induce una función en $\mathcal{S}/\mathcal{N}$ que es claramente un valor absoluto y coincide con $|\cdot|_p$ en la imagen de $\mathbb{Q}$. Finalmente, no es difícil ver por el argunmento diagonal que $\mathcal{S}/\mathcal{N}$ resulta completo.

Llamaremos $\mathbb{Q}_p$ a $\mathcal{S}/\mathcal{N}$, el cuerpo que resulta de la completación de $\mathbb{Q}$ con respecto a la métrica $|\cdot|_p$

El conjunto de los $\alpha \in \mathbb{Q}_p$ con $|\alpha|_p \leq 1$ se llama el conjunto de los enteros p-ádicos $\mathbb{Z}_p$. Como la métrica es no arquimedeana, resulta un anillo:

$$|\alpha|_p, |\beta|_p \leq 1 \Rightarrow |\alpha\beta|_p \leq 1,\ |\alpha \pm \beta|_p \leq 1$$

Un número racional b está en $\mathbb{Z}_p$ cuando es de la forma $b = \frac{u}{v}$ con $u, v \in \mathbb{Z}, \quad p \not| v$. Los números $\epsilon \in \mathbb{Q}_p$ con $|\epsilon|_p = 1$ son las unidades p-ádicas. Las unidades son exactamente los elementos que verifican que $\epsilon, \epsilon^{-1} \in \mathbb{Z}_p$. Todo $\beta \neq 0$ en $\mathbb{Q}_p$ es de la forma $\beta = p^n\epsilon$ con $n \in \mathbb{Z}$ y ϵ una unidad.

Lema 4 *En $\mathbb{Q}_p$ la serie $\sum_0^\infty \beta_n$ converge si y solo si $\beta_n \to 0$*

Demostración: Que la convergencia de la serie implica $\beta_n \to 0$, es cierto como en el análisis real. Para el otro lado, notemos que

$$\left|\sum_{n=0}^{N} \beta_n - \sum_{n=0}^{M} \beta_n\right|_p = \left|\sum_{n=M+1}^{N} \beta_n\right|_p \leq \max_{m<n\leq N} |\beta_n|_p$$

por una clara extensión de la desigualdad ultramétrica. Entonces $\{\sum_0^N \beta_n\}$ es fundamental y tiene un límite. $\diamond$

Vamos a dar una descripción mas precisa de $\mathbb{Z}_p$.

Proposición 5 *Los elementos de $\mathbb{Z}_p$ son las sumas*

$$\sum_{n=0}^{\infty} a_n p^n$$

con

$$a_n \in S = \{0, 1, ..., p-1\}$$

Demostración: Por el Lema anterior, la serie converge y su suma está claramente en $\mathbb{Z}_p$.

Sea ahora $\alpha \in \mathbb{Z}_p$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$, existe un $b \in \mathbb{Q}$ tal que

$$|b - \alpha|_p < 1.$$

Por otra parte hay un $a_0 \in S$ tal que

$$|a_0 - b|_p < 1.$$

En efecto, si $|b|_p < 1$ basta tomar $a_0 = 0$. Si no, $b = \frac{u}{v}$ con u, v coprimos con p. Entonces se toma a_0 tal que $a_0 v \equiv u_{mod\, p}$. Entonces,

$$\alpha = a_0 + p\alpha_1,$$

con $|\alpha_1|_p \leq 1$, o sea $\alpha_1 \in \mathbb{Z}$. Y luego procedemos por inducción para obtener:

$$\alpha = a_0 + a_1 p + ... + a_N p^N + \alpha_N p^{N+1}$$

con $\alpha_N \in \mathbb{Z}_p$. $\diamond$

Lo bueno que tienen los números p-ádicos es que muchas veces es mas fácil trabajar con ellos que con los racionales, por ejemplo si queremos encontrar puntos en una curva, es mas fácil ver si tiene puntos en los $\mathbb{Q}_p$ que en $\mathbb{Q}$. La pregunta es que información nos aporta esto sobre las soluciones en $\mathbb{Q}$. Claramente si la curva tiene un punto en $\mathbb{Q}$, entonces tendrá un punto en cada $\mathbb{Q}_p$. Para la recíproca tenemos el siguiente

Teorema 6 *(Hasse–Minkowski) Una condición necesaria y suficiente para la existencia de un punto racional en una curva de género 0 definida sobre $\mathbb{Q}$ es que haya un punto definido sobre $\mathbb{R}$ y sobre $\mathbb{Q}_p$ para todo primo p.*

Ya aclararemos un poco mas que significa que la curva tenga género 0, por ahora nos quedamos con la idea que son rectas y cónicas (mas precisamente son las curvas birracionalmente equivalentes a rectas y cónicas).

Una curva se dice que tiene soluciones en todos lados localmente cuando tiene puntos definidos sobre $\mathbb{R}$ y sobre $\mathbb{Q}_p$ para todo primo p. El Teorema se llama principio local-global. Desgraciadamente, su validez no se extiende a otras curvas, por ejemplo las curvas:

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

y

$$X^4 - 17 = 2Y^2$$

Tienen soluciones en todos lados localmente pero no tienen soluciones racionales.

Esto será relevante para nosotros mas adelante.

4. Curvas Elípticas

Sea $\mathcal{C}$ una curva afín definida por un polinomio irreducible $f(X,Y)$ sobre un cuerpo k algebraicamente cerrado. Entonces si $g(X,Y) \in k[X,Y]$, define una función

$$(x,y) \mapsto g(x,y) : \mathcal{C}(k) \to k$$

y estas son las **funciones regulares** en $\mathcal{C}$. El anillo de las funciones regulares sobre $\mathcal{C}$ es isomorfo a

$$k[x,y] = k[X,Y]/(f(X,Y))$$

Como $(f(X,Y))$ es irreducible, resulta un dominio íntegro. Se puede considerar el cuerpo de fracciones $k(x,y)$ y tenemos que

$$(x,y) \mapsto \frac{g(x,y)}{h(x,y)} : \mathcal{C}(k) \setminus \{\text{ceros de } h\} \to k$$

con $f \not| h$, es una **función meromorfa**.

Sea ahora $\mathcal{C}$ una curva proyectiva definida por un polinomio irreducible homogéneo $F(X,Y,Z)$ sobre k. Si $G(X,Y,Z)$ y $H(X,Y,Z)$ son polinomios homogéneos del mismo grado y H no es múltiplo de F, entonces

$$[x:y:z] \mapsto \frac{G(x,y,z)}{H(x,y,z)}$$

es una función bien definida en $\mathcal{C}(k) \setminus \{\text{ceros de } H\}$. Estas son funciones meromorfas sobre $\mathcal{C}$. Además, sea

$$k[x,y,z] = k[X,Y,Z]/(F(X,Y,Z)).$$

Se puede descomponer en sumandos de la forma $k[x,y,z]_d$. Luego

$$k(x,y,z)_0 = \left\{ \frac{g}{h} \in k(x,y,z) | \exists d, \text{ tal que } g,h \in k[x,y,z]_d \right\}$$

es un subcuerpo de $k(x,y,z)$ y sus elementos son las **funciones meromorfas** sobre $\mathcal{C}$.

Sea $\mathcal{C}$ una curva proyectiva plana sobre k un cuerpo perfecto (por ejemplo de característica cero o finito, que son los casos que nos interesan). Un **divisor D** en la curva es una suma formal de puntos de la curva:

$$\mathbf{D} = \sum_{\mathbf{x} \in \mathcal{C}} n_{\mathbf{x}} \mathbf{x}$$

donde $\mathbf{x}$ recorre todos los puntos de $\mathcal{C}$ y los enteros $n_{\mathbf{x}}$ son cero salvo finitos.

Los divisores forman un grupo que se llama Div $(\mathcal{C})$. La suma

$$\sum_{\mathbf{x}\in\mathcal{C}} n_{\mathbf{x}}$$

es el grado de $\mathbf{D}$.

Hay un orden parcial definido sobre los divisores. Decimos que

$$\sum_{\mathbf{x}\in\mathcal{C}} n_{\mathbf{x}}\mathbf{x} \geq \sum_{\mathbf{x}\in\mathcal{C}} m_{\mathbf{x}}\mathbf{x}$$

si

$$n_{\mathbf{x}} \geq m_{\mathbf{x}}$$

para todo $\mathbf{x}$.

Sea f una función sobre $\mathcal{C}$. Podemos asociarle un divisor,

$$(f) = \sum_{\mathbf{x}\in\mathcal{C}} \mathrm{ord}_{\mathbf{x}}(f)\mathbf{x}$$

Donde $\mathrm{ord}_{\mathbf{x}}(f) = i(\mathbf{x}, F, G) - i(\mathbf{x}, F, H)$ si $f = \frac{G}{H}$ como antes.

Dichos divisores se llaman **divisores principales**. El conjunto de los divisores principales se denota con Princ $(\mathcal{C})$.

Enunciamos sin demostración:

Proposición 7 *Cada divisor principal tiene grado 0*

Denotamos el conjunto de los divisores de grado 0 con $\mathrm{Div}^0(\mathcal{C})$.

El grupo

$$\text{Pic } (\mathcal{C}) = \text{Div } (\mathcal{C})/\text{Princ } (\mathcal{C})$$

se llama grupo de clases de divisores. La clase de los divisores principales está incluida en lo que se llama la clase canónica, compuesta por los divisores de los diferenciales holomorfos no nulos.

A cada divisor le asociamos el espacio lineal:

$$L(\mathbf{D}) = \{f \text{ función sobre } \mathcal{C} | (f) + \mathbf{D} \geq 0\}$$

Un divisor se dice definido sobre k si queda fijo por la acción de $\Gamma = \text{Gal } (\overline{k}/k)$, o sea si $n_{\sigma\mathbf{x}} = n_{\mathbf{x}}$, $\forall \mathbf{x}, \sigma$.

Finalmente, diremos que una curva $\mathcal{C}$ tiene género 1 si verifica:

$$\dim L(\mathbf{D}) = \begin{cases} 0 & \text{si } \deg(\mathbf{D}) < 0 \\ 1 & \text{si } \deg(\mathbf{D}) = 0 \\ \deg(\mathbf{D}) & \text{si } \deg(\mathbf{D}) > 0 \end{cases}$$

El género es un concepto complicado. Si la curva está definida sobre un subcuerpo de $\mathbb{C}$ y miramos sus puntos complejos, forman una variedad compleja holomorfa de dimensión 1, lo que se llama una superficie de Riemann. Esta resulta compacta y orientable y entonces es isomorfa a una suma de toros. El género es entonces la cantidad de "agujeros" que aparecen, o sea la cantidad de toros que están sumados. El problema es si la curva está definida sobre un cuerpo finito, ahi no tiene sentido hablar de los agujeros. Entonces, de modo mas general se define que el género es el número g tal que se cumple el siguiente:

Teorema 8 *(Riemann–Roch) Sea $\mathcal{X}$ una superficie de Riemann compacta, $\mathbf{D}$ un divisor y $\mathbf{W}$ en la clase canónica de Pic $(\mathcal{X})$, entonces existe un entero $g \geq 0$ fijo que no depende de $\mathbf{D}$ y $\mathbf{W}$ que cumple:*

$$\dim L(\mathbf{D}) = \deg(\mathbf{D}) + \dim L(\mathbf{W} - \mathbf{D}) - g + 1$$

A efectos prácticos, si $\mathcal{X}$ está dada por $F(X, Y, Z) = 0$ con F polinomio homogéneo de grado n y no singular, entonces

$$g = \frac{(n-1)(n-2)}{2}$$

y si F es singular, el género será menor que ese número.

La que dimos es la defínción abstracta de curva de género 1 que se deduce del Teorema de Riemann–Roch.

Definimos **curva elíptica** sobre k como una curva de género 1 con un punto distinguido, $\mathbf{o}$, ambos objetos definidos sobre k.

Si $\mathcal{C}$ es una curva elíptica, hay una correspondencia entre el subgrupo de las clases de divisores de grado 0,

$$\mathrm{Pic}^0(\mathcal{C}) = \mathrm{Div}^0(\mathcal{C})/\mathrm{Princ}\ (\mathcal{C})$$

y los puntos de $\mathcal{C}$ (todos definidos sobre k):

Sea $\mathbf{D}$ un divisor de grado cero. Como la curva tiene género 1, se tiene que $\dim L(\mathbf{D}+\mathbf{o}) = 1$, entonces las funciones que cumplen que

$$(f) + \mathbf{D} + \mathbf{o} \geq 0$$

son todas de la forma λf_0, con $\lambda \in k$ y f_0 fija. Como (f_0) tiene grado cero, hay un único punto $\mathbf{x} = \mathbf{x}(\mathbf{D})$ tal que:

$$(f_0) = \mathbf{x} - \mathbf{D} - \mathbf{o}$$

Mas aún, $\mathbf{x}(\mathbf{D}_1) = \mathbf{x}(\mathbf{D}_2)$ si y solo si $\mathbf{D}_1 - \mathbf{D}_2$ es un divisor principal. En efecto, si $L(\mathbf{D}_1 + \mathbf{o})$ y $L(\mathbf{D}_2 + \mathbf{o})$ están generados por las funciones f_1 y f_2 respectivamente, y si $\mathbf{x}(\mathbf{D}_1) = \mathbf{x}(\mathbf{D}_2)$, entonces

$$(f_2) - (f_1) = \mathbf{x}(\mathbf{D}_2) - \mathbf{x}(\mathbf{D}_1) - \mathbf{D}_2 + \mathbf{D}_1 = \mathbf{D}_1 - \mathbf{D}_2$$

y $\mathbf{D}_1 - \mathbf{D}_2$ resulta un divisor principal. Por otro lado, sea $\mathbf{D}_1 - \mathbf{D}_2$ un divisor principal, digamos de una función f_0. Asi como f_1 es un generador de $L(\mathbf{D}_1 + \mathbf{o})$, $f_0 f_1$ lo es de $L(\mathbf{D}_2 + \mathbf{o})$. Se cumple

$$(f_0 f_1) = (f_0) + (f_1) = \mathbf{D}_1 - \mathbf{D}_2 + \mathbf{x}(\mathbf{D}_1) - \mathbf{D}_1 - \mathbf{o}$$

y entonces $\mathbf{x}(\mathbf{D}_1) = \mathbf{x}(\mathbf{D}_2)$.

Además todo punto $\mathbf{x}$ aparece de esa forma pues basta tomar $\mathbf{D} = \mathbf{x} - \mathbf{o}$ (y eso da $f_0 = 1$). Como las clases de divisores de grado 0 tienen una estructura de grupo, tenemos una estructura natural de grupo abeliano donde $\mathbf{o}$ es el elemento nulo. Si escribimos

$$\mathbf{a} + \mathbf{b} = \mathbf{c}$$

esto significará que el divisor $\mathbf{a} + \mathbf{b}$ es equivalente al divisor $\mathbf{c} + \mathbf{o}$. Como $\mathbf{o}$ está definido sobre k, es claro que la ley de grupo también está definida sobre k.

Teorema 9 *Supongamos que* $car(k) \neq 2, 3$. *Entonces la curva elíptica* $(\mathcal{D}, \mathbf{o}_D)$ *es birracionalmente equivalente sobre* k *a una curva elíptica* $(\mathcal{C}, \mathbf{o}_C)$ *de la forma*

$$Y^2 = X^3 + AX + B$$

Idea de la Demostración: Por tener género 1, si miramos los divisores $2\mathbf{o}_D$ y $3\mathbf{o}_D$, sus espacios lineales respectivos tienen dimensión 2 y 3. Las funciones que tienen un polo de orden 3 en $\mathbf{o}_D$ y no tienen otros polos, son las que

están en $L(3\mathbf{o}_D) \setminus L(2\mathbf{o}_D)$ (el segundo es subespacio del primero). Como los espacios tienen distinta dimensión, hay al menos una función con un polo de orden 3 en $\mathbf{o}_D$ y ningún otro polo, que la notamos como Y_1. Análogamente, hay una función X_1 con polo de orden 2 en $\mathbf{o}_D$ y ningún otro polo. Si ahora miramos las funciones:

$$1,\, Y_1,\, X_1,\, Y_1^2,\, X_1^2,\, X_1^3,\, X_1Y_1$$

son siete funciones que tienen polos solamente en $\mathbf{o}_D$ y además el polo es de orden a lo sumo 6. Como $\dim L(6\mathbf{o}_D) = 6$, estas funciones son linealmente dependientes y entonces obtenemos una relación de la forma:

$$c_{yy}Y_1^2 + c_{xy}X_1Y_1 + c_yY_1 = c_{xxx}X_1^3 + c_{xx}X_1^2 + c_xX_1 + c$$

Como Y_1^2 y X_1^3 son las únicas funciones que tienen polo de orden exactamente 6 en la igualdad, se sigue que

$$c_{yy} = c_{xxx}$$

Si fuera $c_{yy} = 0$, nos queda una igualdad con una sola función con polo de orden máximo 5, X_1Y_1 y por lo tanto $c_{xy} = 0$. Por el mismo razonamiento se obtienen sucesivamente $c_{xx} = 0$, luego $c_y = 0$, $c_x = 0$, $c = 0$. Entonces $c_{yy} \neq 0$ y podemos suponer que es 1 dividiendo la ecuación y obtenemos:

$$Y_1^2 + a_1X_1Y_1 + a_3Y_1 = X_1^3 + a_2X_1^2 + a_4X_1 + a_6$$

Que se llama **forma general de Weierstrass** de la curva elíptica.

Si la característica no es 2, se puede hacer el cambio de variables

$$(X_0, Y_0) = (X_1, 2Y_1 + a_1X_1 + a_3)$$

y queda una ecuación de la forma:

$$Y_0^2 = 4X_0^3 + b_2X_0^2 + 2b_4X_0 + b_6$$

Si la característica no es 3, se puede hacer el cambio de variables

$$(X, Y) = (36X_0 + 3b_2, 108Y_0)$$

y queda una ecuación de la forma:

$$Y^2 = X^3 - 27c_4X - 54c_6$$

La notación de los coeficientes es standard. $\diamond$

Llamaremos a la ecuación de la forma:

$$Y^2 = X^3 + AX + B$$

forma canónica. A partir de ahora, salvo casos especiales trabajaremos con esta ecuación como ecuación general de una curva elíptica definida sobre $\mathbb{Q}$.

Convendría aclarar que punto del plano proyectivo corresponde a $\mathbf{o}$ en este caso. Si lo pensamos en el plano afín por un momento, estamos diciendo que la función $f(X, Z) = \frac{X}{Z}$ tiene un polo allí, por lo tanto es un punto de la recta del infinito. Al reemplazar por $Z = 0$ en la ecuación proyectiva

$$Y^2 Z = X^3 + AXZ^2 + BZ^3$$

Obtenemos $X = 0$, luego no puede ser otro que el punto $[0 : 1 : 0]$, al que llamaremos también punto del infinito de la curva. Además, si construimos el Hessiano de

$$F(X, Y, Z) = -Y^2 Z + X^3 + AXZ^2 + BZ^3$$

nos da

$$H(x_0, y_0, z_0) = \begin{pmatrix} 6x_0 + Az_0^2 & 0 & 2Az_0 \\ 0 & -2z_0 & -2y_0 \\ 2Az_0 & -2y_0 & 2Ax_0 + 6Bz_0 \end{pmatrix}_{(x_0, y_0, z_0)}$$

Con lo cual el punto $[0 : 1 : 0]$ es punto de inflexión de la curva.

Proposición 10 *Sean dados tres puntos $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3 \in \mathcal{C}$ dada en forma canónica. Entonces,*

$$\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \mathbf{o}$$

si y solo si son colineales. En particular $\mathbf{x} = (x_1, y_1) \Rightarrow -\mathbf{x} = (x_1, -y_1)$.

Demostración: La función

$$lX + mY + n$$

Con $l, m, n \in k$, $m \neq 0$, tiene un polo de orden 3 en $\mathbf{o}$ y ningún otro polo. Si sus tres ceros son $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ entonces, según la definición:

$$\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = 3\mathbf{o} = \mathbf{o}$$

Si $m = 0$, $l \neq 0$, la función tiene un polo de orden 2 en $\mathbf{o}$ y los dos ceros serán de la forma (x, y), $(x, -y)$, que están alineados con $\mathbf{o}$, el punto del infinito.

Por otro lado, si se tiene que los tres puntos suman cero, consideramos la recta que pasa por $\mathbf{x}_1$ y $\mathbf{x}_2$ (si coinciden, consideramos la tangente a la curva en ese punto). Esta intersecta a la curva en otro punto $\mathbf{y}$, en virtud de lo anterior:

$$\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{y} = \mathbf{o}$$

Pero entonces,

$$\mathbf{y} = \mathbf{x}_3.$$

$\diamond$

A partir de esta proposición, podemos describir la ley de grupo de la siguiente manera. Si $\mathbf{x}, \mathbf{y} \in \mathcal{C}$, la recta que pasa por ambos intersecta a la curva en un tercer punto que también está definido sobre k y lo llamamos $\mathbf{xy}$. En los casos especiales interpretamos cada punto según su multiplicidad, por ejemplo si $\mathbf{x} = \mathbf{y}$, lo que tomamos es la recta tangente, etc. Entonces

$$\mathbf{x} + \mathbf{y} = \mathbf{o}(\mathbf{xy})$$

En efecto, por la Proposición,

$$\mathbf{xy} = -(\mathbf{x} + \mathbf{y})$$

y luego

$$\mathbf{o}(\mathbf{xy}) = -(\mathbf{xy} + \mathbf{o}) = -(-(\mathbf{x} + \mathbf{y}) + \mathbf{o}) = \mathbf{x} + \mathbf{y}.$$

Esta interpretación del grupo de la curva es muy importante porque se entiende, es tangible. Podríamos haberlo definido asi desde un principio, pero esto nos dificultaría algunas demostraciones que veremos mas tarde y además la demostración de que la operación es asociativa es considerablemente complicada en este caso, mientras que por el camino que seguimos es una consecuencia trivial de la construcción.

4.1. Algunas Fórmulas

Nos va a resultar útil tener una fórmula que nos diga como sumar puntos en una curva del tipo

$$\mathcal{C} : Y^2Z = X^3 + AXZ^2 + BZ^3$$

Como ya observamos antes,

$$\mathbf{x}_1 = (x_1, y_1) \Rightarrow -\mathbf{x}_1 = (x_1, -y_1)$$

4.1.1. Fórmula de Adición

Sea $\mathbf{x}_2 = (x_2, y_2)$ y queremos calcular x, y si:

$$\mathbf{x} = (x, y), \qquad \mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$$

Si $\mathbf{x}_2 = -\mathbf{x}_1$, tenemos $\mathbf{x} = \mathbf{o}$. Si $\mathbf{x}_2 = \mathbf{x}_1$ es el caso de la fórmula de duplicación que veremos mas adelante. Entonces podemos suponer

$$\mathbf{x}_2 \neq \mathbf{x}_1$$

La recta que los une es

$$Y = lX + m$$

donde

$$l = \frac{y_1 - y_2}{x_1 - x_2}, \qquad m = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}$$

Esta recta corta a la curva en $\mathbf{x}_1, \mathbf{x}_2$ y $-(\mathbf{x}_1 + \mathbf{x}_2) = (x, -y)$.

Entonces las raíces de

$$X^3 + AX + B - (lX + m)^2 = X^3 - l^2X^2 + (A - 2lm)X + (B - m^2)$$

son x_1, x_2 y x. Por lo tanto,

$$x_1 + x_2 + x = l^2$$

y como

$$y = -lx - m$$

Concluimos,

$$\begin{aligned} x &= \frac{x_1 x_2^2 + x_1^2 x_2 - 2y_1 y_2 + A(x_1 + x_2) + 2B}{(x_1 - x_2)^2} \\ y &= \frac{(y_2 - y_1)x + x_2 y_1 - x_1 y_2}{x_1 - x_2} \end{aligned}$$

4.1.2. Fórmula de Duplicación

Ahora consideramos

$$(x, y) = \mathbf{x} = 2\mathbf{x}_1 = 2(x_1, y_1)$$

Si $y_1 = 0$, tenemos $\mathbf{x} = \mathbf{o}$. Entonces podemos quedarnos con el caso:

$$y \neq 0$$

Necesitamos la tangente

$$Y = lX + m$$

a la curva en $\mathbf{x}$. Acá la pendiente l debe coincidir con la dirección tangente a la curva en el punto $\mathbf{x}$. Para hallarla diferenciamos formalmente la curva:

$$2YY' = (3X^2 + A)X'$$

de donde

$$l = \frac{3x_1^2 + A}{2y_1}$$

Entonces, por la fórmula de adición:

$$x = l^2 - 2x_1 = \frac{(3x_1^2 + A)^2 - 8x_1y_1^2}{4y_1^2}$$

Para y necesitamos el valor de m:

$$m = y_1 - lx_1 = \frac{2y_1^2 - 3x_1^3 - Ax_1}{2y_1} = \frac{-x_1^3 + Ax_1 + 2B}{2y_1}$$

Entonces

$$y = -lx - m$$

Concluimos,

$$\begin{aligned} x &= \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4(x_1^3 + Ax_1 + B)} \\ y &= \frac{x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - A^3 - 8B^2}{(2y_1)^3} \end{aligned}$$

5. Resultantes

Sean

$$\begin{aligned} f(X) &= a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \\ g(X) &= b_mX^m + b_{m-1}X^{m-1} + ... + b_0 \end{aligned}$$

con $a_n \neq 0, b_m \neq 0$, polinomios en $A[X]$ con A dominio de factorización única.

Entonces

$$[R(f,g)] = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_{n-2} & a_{n-1} & a_n & 0 & \cdots & 0 \\ \vdots & \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & a_2 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_{m-2} & b_{m-1} & b_m & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_{m-3} & b_{m-2} & b_{m-1} & b_m & \cdots & 0 \\ \vdots & \vdots & & & & & & & \vdots \\ 0 & 0 & \cdots & b_0 & b_1 & b_2 & b_3 & \cdots & b_n \end{pmatrix}$$

se llama la matriz resultante y su determinante se nota $R(f,g)$.

Proposición 11 *Sean f y g como antes, son equivalentes:*

(1) *f y g tienen un factor común de grado > 0*

(2) *$af + bg = 0$ para ciertos $a, b \in A[X]$ no nulos con $\deg(a) < m$ y $\deg(b) < n$*

(3) *$R(f,g) = 0$*

Demostración: (1) $\Rightarrow$ (2) Si $u|f$ y $u|g$, $f = bu$, $g = -au$ verifican.

(2) $\Rightarrow$ (1) Factorizamos f y bg. Si (1) fuera falso, los factores de f de grado positivo aparecerían en b y esto contradice el hecho que $\deg(b) < \deg(f)$.

(2) $\Leftrightarrow$ (3) Para a, b de la forma

$$\begin{aligned} a(X) &= \alpha_0 + \alpha_1 X + ... + \alpha_{m-1} X^{m-1} \\ b(X) &= \beta_0 + \beta_1 X + ... + \beta_{n-1} X^{n-1} \end{aligned}$$

Tenemos

$$(\alpha_0 ... \alpha_{m-1} \beta_0 ... \beta_{n-1})[R(f,g)] = (c_0 c_1 ... c_{n+m-1})$$

donde

$$a(X)f(X) + b(X)g(X) = c(X) = c_0 + c_1 X + ... + c_{n+m-1} X^{n+m-1}$$

Existen a y b no triviales tal que $c(X) = 0$ si y solo si $R(f,g) = 0$. En principio se obtienen a y b con coeficientes en el cuerpo de fracciones del anillo pero se puede multiplicar por un número conveniente para eliminar los denominadores.$\diamond$

Proposición 12 *Sean f y g como antes. Cuando $R(f,g) \neq 0$, existen $a, b \in A[X]$ con $\deg(a) < m$ y $\deg(b) < n$ tales que $a(X)f(X)+b(X)g(X) = R(f,g)$ (aca estamos pensando a $R(f,g)$ como un polinomio de grado cero).*

Demostración: Como $R(f,g) \neq 0$, la fórmula de los cofactores nos da:

$$[R(f,g)]^{-1} = R(f,g)^{-1}[S(f,g)]$$

donde $[S(f,g)]$ es una matriz con entradas en A.

Entonces, la primer fila de $[S(f,g)]$ es:

$$(\alpha_0 ... \alpha_{m-1} \beta_0 ... \beta_{n-1}) = (R(f,g), 0, .., 0)[R(f,g)]^{-1}$$

y definimos $a(X)$ y $b(X)$ como antes y funcionan. $\diamond$

Si permitimos $a_n = b_m = 0$, claramente $R(f,g) = 0$. Si $a_n \neq 0$ y $b_m = 0$, tenemos

$$R(f,g) = a_n R(f, \tilde{g})$$

donde $\tilde{g} = b_{m-1}X^{m-1} + ... + b_1 X + b_0$.

Si ahora consideramos

$$\begin{aligned} F &= a_n X^n + ... + a_1 X Y^{n-1} + a_0 Y^n \\ G &= b_m X^m + ... + b_1 X Y^{m-1} + b_0 Y^m \end{aligned}$$

polinomios homogéneos, tendrán un cero $(X,Y) \neq (0,0)$ en la clausura algebraica de A si y solo si $R(F,G) = 0$ (tomando la resultante respecto de la variable X).

Proposición 13 *Si $A = k[X_1, ...X_r]$ y si f y g son como antes con a_j homogéneo de grado $n-j$ y b_j homogéneo de grado $m-j$, entonces $R(f,g)$ es homogéneo de grado nm.*

Demostración: Si a cada fila de la matriz $[R(f,g)](tX_1, ..., tX_r)$ la multiplicamos por $t^m, t^{m-1}, ..., t, t^n, t^{n-1}, ..., t$ en ese orden y luego a cada columna le sacamos un factor $t^{n+m}, t^{n+m-1}, ..., t$ en ese orden, obtenemos la matriz $[R(f,g)](X_1, ..., X_r)$ Entonces:

$$t^{(1+...+m+1+...+n)}[R(f,g)](tX_1, ..., tX_r) = t^{(1+...+(n+m))}[R(f,g)](X_1, ..., X_r)$$

Y entonces es homogéneo de orden

$$\frac{(n+m)(n+m+1)}{2} - \left(\frac{n(n+1)}{2} + \frac{m(m+1)}{2} \right) = nm$$

◇

Escribimos

$$f(X) = a_n \prod_{j=1}^{n} (X - \phi_j)$$

$$g(X) = b_m \prod_{k=1}^{m} (X - \psi_k)$$

Si a_n, b_m, ϕ_j, ψ_k se toman como variables, $R(f, g)$ es un polinomio en ellas que se anula cuando algún ϕ_j es igual a algún ψ_k. Luego

$$\prod_{j,k} (\phi_j - \psi_k) | R(f, g)(\phi_1, ..., \phi_n, \psi_1, ..., \psi_m)$$

pero como $R(f, g)$ tiene que ser homogéneo de grado nm entonces es igual a ese producto salvo una constante:

$$R(f, g) = \delta \prod_{j,k} (\phi_j - \psi_k) = \gamma \prod_{j} g(\phi_j) = \beta \prod_{k} f(\psi_k)$$

Finalmente, si ponemos $g = f'$, $R(f, f')$ se llama discriminante y se nota $\Delta(f)$. El discriminante se anula si y solo si f y f' tienen raíces en común que es lo mismo que decir que f tiene alguna raíz múltiple.

Por ejemplo, si $f(X) = X^3 + AX + B$, $\Delta(f) = 4A^3 + 27B^2$. f tendrá todas sus raíces simples sii $4A^3 + 27B^2 \neq 0$.

6. Teorema de Mordell

6.1. Descenso

Nuestro objetivo es probar el siguiente:

Teorema 14 *(Mordell) El grupo $F(\mathbb{Q})$ de una curva elíptica F definida sobre $\mathbb{Q}$ es finitamente generado.*

Este Teorema también es conocido como el Teorema de la Base Finita o el Teorema de Mordell-Weil.

La prueba se subdivide en dos partes:

(1) El "teorema de finitud débil", que nos dice que el grupo

$$F(\mathbb{Q})/2F(\mathbb{Q})$$

es finito. La prueba se basa en la construcción de un monomorfismo de $F(\mathbb{Q})/2F(\mathbb{Q})$ en un grupo finito. La prueba es mas elemental si la curva tiene un punto racional de orden dos, y por ello, solo estudiaremos este caso. El caso general es análogo pero utiliza teoría algebraica de números.

También debemos remarcar que la prueba no es constructiva en el sentido que no nos proporciona quienes son exactamente los generadores de $F(\mathbb{Q})/2F(\mathbb{Q})$.

(2) El "descenso". Si $\mathbf{b_1}, ..., \mathbf{b_r}$ son generadores de $F(\mathbb{Q})/2F(\mathbb{Q})$ y $\mathbf{a}$ un punto, entonces existe un $\mathbf{b_s}$ tal que

$$\mathbf{a} - \mathbf{b_s} \in 2F(\mathbb{Q}),$$

o sea,

$$\mathbf{a} = \mathbf{b_s} + \mathbf{2c}, \qquad \mathbf{c} \in F(\mathbb{Q}) \tag{2}$$

Nos fabricaremos una *altura* H que va a medir el "tamaño" de un punto $\mathbf{a} \in F(\mathbb{Q})$. Lo que va a salir es que $H(\mathbf{c}) < H(\mathbf{a})$ si $H(\mathbf{a})$ es mayor que alguna constante K en la ecuación (2). Y eso va a implicar que $F(\mathbb{Q})$ estará generado por los $\mathbf{b_s}$ y por una cantidad finita de $\mathbf{a}$ que cumplen $H(\mathbf{a}) \leq K$.

Para entender esto mejor veamos la demostración del Teorema de Fermat para el caso $n = 4$:

Proposición 15 *(Fermat) La ecuación $X^4 + Y^4 = Z^4$ no tiene soluciones enteras con $X \neq 0$, $Y \neq 0$.*

Demostración: Es suficiente con ver que la ecuación

$$X^4 + Y^4 = Z^2$$

no tiene soluciones no triviales en los enteros. Supongamos que tenemos una solución no trivial, si la pensamos como

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

asumiendo que $(x; y) = 1$ con x impar, y par, entonces existen enteros m y n tales que

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad (m; n) = 1$$

y como $m^2 = x^2 + n^2$ con x impar, obtenemos enteros p y q tales que

$$m = p^2 + q^2, \qquad x = p^2 - q^2, \qquad n = 2pq, \qquad (p; q) = 1$$

como y es par, escribimos

$$\left(\frac{y}{2}\right)^2 = \frac{mn}{2} = pq(p^2 + q^2)$$

Como p, q y p^2+q^2 con coprimos dos a dos, cada uno de ellos es un cuadrado y podemos escribir

$$p = r^2, \qquad q = s^2, \qquad r^4 + s^4 = t^2$$

Lo que hemos hecho es pasar de una solución de $x^4 + y^4 = z^2$ a una solución de $r^4 + s^4 = t^2$. Veamos como están relacionadas

$$\left(\frac{y}{2}\right)^2 = pq(p^2 + q^2) = r^2 s^2 (r^4 + s^4)$$

entonces,

$$y = 2rs\sqrt{r^4 + s^4}$$

Si la nueva solución fuera trivial, $rs = 0$ lo que implicaría que $y = 0$ y la primer solución sería trivial, absurdo. Entonces llegamos a una nueva solución no trivial que verifica $r < y, s < y$. O sea,

$$\text{máx}\,\{|r|, |s|\} < \text{máx}\,\{|x|, |y|\}$$

Este procedimiento no puede durar para siempre, pues solo tenemos finitos números enteros positivos para el valor de $\text{máx}\,\{|r|, |s|\}$ y llegamos a una contradicción. $\diamond$

Analicemos el procedimiento de la demostración. Si escribimos la ecuación original de la forma:

$$\left(\frac{z}{y^2}\right)^2 = 1 + \left(\frac{x}{y}\right)^4$$

Sean $M = \frac{x}{y}$, $N = \frac{z}{y^2}$. Escribiendo:

$$\left\{ \begin{array}{lcl} a & = & \frac{2}{N - M^2} \\ b & = & \frac{4M}{N - M^2} \end{array} \right.$$

$$\begin{cases} M & = & \frac{b}{2a} \\ N & = & \frac{b^2+8a}{4a^2} \end{cases}$$

Llegamos a $b^2 = a^3 - 4a$. Haciendo la misma cuenta con r, s y t tenemos $d^2 = c^3 - 4c$.

Sea $R = \frac{r}{s}$, luego,

$$R^2 = \left(\frac{d}{2c}\right)^2 = \frac{c^3 - 4c}{4c^2} = \frac{c^2 - 4}{4c}$$

Entonces,

$$N - M^2 = \frac{z - x^2}{y^2} = \frac{(m^2 + n^2) - (m^2 - n^2)}{2mn} = \frac{n}{m} = \frac{2r^2 s^2}{r^4 + s^4} = \frac{2R^2}{R^4 + 1}$$

por lo tanto,

$$a = \frac{2}{N - M^2} = \frac{R^4 + 1}{R^2} = \frac{(\frac{c^2-4}{4c})^2 + 1}{(\frac{c^2-4}{4c})} = \frac{c^4 + 8c^2 + 16}{4c^3 - 16c}$$

o sea que $(a, b) = \pm 2(c, d)$ en la curva $F(X, Y, Z) = Y^2 Z - (X^3 - 4XZ^2)$.

Entonces el método del descenso en este caso pasa de un punto $p \in F(\mathbb{Q})$ a un punto $\pm\frac{p}{2} \in F(\mathbb{Q})$.

6.2. Teorema de la Base Finita Débil

Sean $\mathcal{C}$ y $\mathcal{D}$ dos curvas elípticas definidas sobre $\mathbb{Q}$. Una **isogenía** es un morfismo (función racional regular)

$$\phi: \mathcal{C} \longmapsto \mathcal{D}$$

definida sobre el cuerpo base que manda la identidad de $\mathcal{C}$ en la identidad de $\mathcal{D}$. Se puede probar que son suryectivas y homomorfismos.

Como ya dijimos, vamos a suponer que $\mathcal{C}$ tiene un punto racional de orden 2. Mediante un cambio admisible de coordenadas podemos suponer que

$$\mathcal{C} : Y^2 Z - X(X^2 + aXZ + bZ^2) = F(X, Y, Z)$$

Siendo $(0, 0)$ el punto de orden 2. Para que sea no singular, el polinomio en X no debería tener raíces dobles con lo que

$$b \neq 0, \qquad a^2 - 4b \neq 0$$

Sea $\mathbf{x} = (x, y)$ un punto *genérico* de $\mathcal{C}$ o sea, x trascendente e y definido por la relación

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

El cuerpo $\mathbb{Q}(x, y)$ es el **cuerpo de funciones** de $\mathcal{C}$ sobre $\mathbb{Q}$.

La transformación

$$\mathbf{x} \mapsto \tilde{\mathbf{x}} = \mathbf{x} + (0, 0)$$

es un automorfismo de $\mathbb{Q}(x, y)$ de orden 2. Queremos encontrar el cuerpo fijo. La recta por $(0, 0)$ y (x, y) es

$$X = tx, \qquad Y = ty$$

que intersecta a la curva $\mathcal{C}$ en los puntos $(0, 0)$, $\mathbf{x}$ y $-\tilde{\mathbf{x}} = (\tilde{x}, -\tilde{y})$.

Reemplazando en la ecuación original,

$$\begin{aligned} (ty)^2 &= tx((tx)^2 + a(tx) + b) \\ y^2t^2 &= x^3t^3 + ax^2t^2 + bxt \end{aligned}$$

(x, y) fijos. Sabemos que $t = 0, 1$ verifican la ecuación. Buscamos el tercer valor de t.

$$t(x^3t^2 + (ax^2 - y^2)t + bx) = x^3t(t - 1)\left(t - \frac{b}{x^2}\right)$$

Entonces,

$$\begin{aligned} \tilde{x} &= \frac{b}{x} \\ \tilde{y} &= -\frac{by}{x^2} \end{aligned}$$

Los invariantes que podemos tomar son:

$$\lambda = x + \tilde{x} + a = \frac{x^2 + ax + b}{x} = \left(\frac{y}{x}\right)^2 = t^2$$

$$\mu = y + \tilde{y}$$

Buscamos una relación algebraica entre λ y μ

$$\begin{aligned} \mu^2 &= \left(y - \frac{by}{x^2}\right)^2 = y^2\left(\frac{x^2 - b}{x^2}\right)^2 \\ &= \frac{x^2 + ax + b}{x}\left(x^2 - 2b + \frac{b^2}{x^2}\right) = \lambda\left(x^2 - 2b + \frac{b^2}{x^2}\right) \end{aligned}$$

El segundo factor es igual a:

$$\left(x+\frac{b}{x}\right)^2-4b=(\lambda-a)^2-4b=\lambda^2-2a\lambda+(a^2-4b)$$

por lo tanto

$$\mu^2=\lambda(\lambda^2-2a\lambda+(a^2-4b))$$

Podemos expresar x, y en función de λ, μ

$$\lambda^{\frac{1}{2}}=\frac{y}{x}\Rightarrow y=\lambda^{\frac{1}{2}}x$$

$$\lambda=x+a+\frac{b}{x}$$

$$\frac{\mu}{\lambda^{\frac{1}{2}}}=\frac{y-\frac{by}{x^2}}{\frac{y}{x}}=x-\frac{b}{x}$$

luego,

$$x=\frac{\lambda+\frac{\mu}{\lambda^{\frac{1}{2}}}-a}{2}$$

Entonces la extensión $\mathbb{Q}(x,y)/\mathbb{Q}(\lambda,\mu)$ es de grado 2, y por Teoría de Gal ois, $\mathbb{Q}(\lambda,\mu)$ es el cuerpo de invariantes. El punto (λ,μ) es un punto genérico de la curva

$$\mathcal{D}: Y^2Z-X(X^2-2aXZ+(a^2-4b)Z^2)=G(X,Y,Z)$$

La función

$$\phi:\mathcal{C}\longmapsto\mathcal{D}$$

dada por

$$\mathbf{x}=(x,y)\mapsto\lambda=(\lambda,\mu)$$

preserva la ley de grupo.

En efecto, sean $\mathbf{a},\mathbf{b}\in\mathcal{C}$ y sea $f\in\mathbb{Q}(x,y)$ una función con polos simples en $\mathbf{a}$ y $\mathbf{b}$ y ceros simples en $\mathbf{o}$ y $\mathbf{a}+\mathbf{b}$. Sea $\tilde{f}$ la función que resulta de conjugar f con la función $\mathbf{x}\mapsto\tilde{\mathbf{x}}$. Entonces $f\tilde{f}\in\mathbb{Q}(\lambda,\mu)$ y claramente tiene polos simples en $\phi(\mathbf{a})$, $\phi(\mathbf{b})$ y ceros simples en $\phi(\mathbf{a}+\mathbf{b})$ y $\phi(\mathbf{o})=\mathbf{o}$. Luego

$$\phi(\mathbf{a}+\mathbf{b})=\phi(\mathbf{a})+\phi(\mathbf{b})$$

La ecuación de $\mathcal{D}$ tiene la misma forma general que la de $\mathcal{C}$. Repitiendo el proceso con λ y $\mathcal{D}$, obtenemos ρ, σ con

$$\sigma^2 = \rho(\rho^2 + 4a\rho + 16b);$$

y por lo tanto,

$$\xi = \frac{\rho}{4}, \qquad \eta = \frac{\sigma}{16}$$

es un punto genérico de $\mathcal{C}$ nuevamente.

Llamaremos

$$\psi : \mathcal{D} \longmapsto \mathcal{C}$$

a la función dada por

$$\lambda = (\lambda, \mu) \mapsto \xi = (\xi, \eta)$$

Los puntos que ϕ manda a $(\lambda, \mu) = (0, 0)$ son exactamente los puntos con $y = 0$ (que no son el (0,0), que va a parar a $\mathbf{o}$) que son los de 2-torsión. Entonces el kernel de $(x, y) \mapsto (\xi, \eta)$ es exactamente el conjunto de los puntos de 2-torsión y el $\mathbf{o}$. Con lo cual el morfismo debe ser la multiplicación por ± 2.

Ahora consideraremos el efecto de la isogenía

$$\phi : \mathcal{C} \longmapsto \mathcal{D}$$

en los puntos racionales.

Lema 16 *: Sea $(u, v) \in G(\mathbb{Q})$. Entonces $(u, v) \in \phi F(\mathbb{Q})$ si y solo si: o bien $u \in (\mathbb{Q}^*)^2$ o bien $u = 0$, $a^2 - 4b \in (\mathbb{Q}^*)^2$.*

Demostración: Si $u \neq 0$, se sigue de las observaciones anteriores especializando $\lambda \mapsto u, \mu \mapsto v$. El punto $(0, 0)$ viene de puntos de la forma $(\alpha, 0)$ con $\alpha^2 + a\alpha + b = 0$ y $\alpha \in \mathbb{Q}$ si y solo si $a^2 - 4b \in (\mathbb{Q}^*)^2$.$\diamond$

Esto sugiere la función:

$$q : G(\mathbb{Q}) \longmapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

dada por

$$q((u, v)) = \begin{cases} u(\mathbb{Q}^*)^2 & \text{si } u \neq 0 \\ (a^2 - 4b)(\mathbb{Q}^*)^2 & \text{si } u = 0 \\ (\mathbb{Q}^*)^2 & \text{si } (u, v) = \mathbf{o} \end{cases}$$

Además,

$$v^2 = u(u^2 - 2au + a^2 - 4b) \tag{3}$$

implica que

$$q((u,v)) = (u^2 - 2au + a^2 - 4b)(\mathbb{Q}^*)^2 \tag{4}$$

para $(u,v) \neq \mathbf{o}$.

Lema 17 *La función*

$$q : G(\mathbb{Q}) \longmapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

es un homomorfismo de grupos.

Demostración: Escribimos la ecuación de $\mathcal{D}$ como:

$$V^2 = U(U^2 + a_1U + b_1)$$

Sea $\mathbf{u_j} = (u_j, v_j)$ $(j = 1, 2, 3) \in G(\mathbb{Q})$ con

$$\mathbf{u_1} + \mathbf{u_2} + \mathbf{u_3} = \mathbf{o}$$

Si los $\mathbf{u_j}$ son iguales a $\mathbf{o}$, no hay nada que probar.

Si solo uno de ellos es $\mathbf{o}$, digamos $\mathbf{u_1} = \mathbf{o}$, entonces $\mathbf{u_2} = -\mathbf{u_3}$ y por la definición, $q(\mathbf{u_2}) = q(\mathbf{u_3})$ y eso implica que $q(\mathbf{u_1})q(\mathbf{u_2})q(\mathbf{u_3}) = (\mathbb{Q}^*)^2$.

Si ninguno es $\mathbf{o}$, están en la intersección de $\mathcal{D}$ con una recta de la forma

$$V = mU + c$$

Si substituímos en la ecuación de $\mathcal{D}$, tenemos:

$$U(U^2 + a_1U + b_1) - (mU + c)^2 = (U - u_1)(U - u_2)(U - u_3)$$

Mirando el término independiente,

$$u_1u_2u_3 = c^2$$

y eso implica que $q(\mathbf{u_1})q(\mathbf{u_2})q(\mathbf{u_3}) = (\mathbb{Q}^*)^2$ a menos que alguno de ellos sea el $(0,0)$. En ese caso, digamos $\mathbf{u_1} = (0,0)$, los otros no pueden ser $(0,0)$ porque sino uno de ellos sería $\mathbf{o}$ y ese caso ya lo consideramos. Como antes tenemos:

$$U(U^2 + a_1U + b_1) - (mU + c)^2 = U(U - u_2)(U - u_3)$$

Entonces U divide a $(mU + c)^2$ y $\Rightarrow c = 0$. Luego:

$$U^2 + a_1U + b_1 - m^2U = (U - u_2)(U - u_3)$$

Poniendo $U = 0$, nos da:

$$u_2u_3 = b_1 = a^2 - 4b.$$

$\diamond$

Lema 18 *La imagen de*

$$q : G(\mathbb{Q}) \longmapsto \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

es finita.

Demostración: Sin pérdida de generalidad,

$$a_1 \in \mathbb{Z}, \qquad b_1 \in \mathbb{Z}$$

Un elemento de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ puede escribirse como $r(\mathbb{Q}^*)^2$ con $r \in \mathbb{Z}$ libre de cuadrados. Veremos que $r(\mathbb{Q}^*)^2$ está en la imagen de q solo en caso que $r|b_1$.

Supongamos que $q((u, v)) = r(\mathbb{Q}^*)^2$. Luego $\exists s, t \in \mathbb{Q}$ tales que

$$\begin{aligned} u^2 + a_1u + b_1 &= rs^2 \\ u &= rt^2 \end{aligned}$$

por las ecuaciones (3) y (4). Si escribimos $t = \frac{l}{m}$ con $l, m \in \mathbb{Z}$, $(l; m) = 1$

Reemplazando la segunda ecuación en la primera,

$$\begin{aligned} r^2t^4 + a_1rt^2 + b_1 &= rs^2 \\ r^2l^4 + a_1rl^2m^2 + b_1m^4 &= rn^2 \end{aligned}$$

donde $n = m^2s \in \mathbb{Z}$.

Sea p primo tal que $p|r$, $p \not| b_1$. Luego $p|m$ y también $p^3|rn^2$ pues $p|n$ por $m|n$ y $p|r$. Entonces $p^3|r^2l^4$, con lo cual $p|l$. Absurdo pues habíamos supuesto $(l; m) = 1$. $\diamond$

Juntando los lemas anteriores obtenemos:

Teorema 19 *$G(\mathbb{Q})/\phi F(\mathbb{Q})$ es finito.*

Lema 20 *Sean A, B grupos abelianos tales que*

$$A \xrightarrow{\alpha} B \xrightarrow{\beta} A$$

con α, β homomorfismos de grupos tales que $\gamma = \beta \circ \alpha$. Entonces se tiene la sucesión exacta:

$$0 \to B[\beta]/\alpha(A[\gamma]) \xrightarrow{i_1} B/\alpha A \xrightarrow{\beta} A/\gamma A \xrightarrow{i_2} A/\beta B \to 0$$

donde $A[\gamma]y\, B[\beta]$ denotan los kernels de los morfismos γ y β respectivamente, y además i_1 e i_2 son inclusiones.

Demostración: i_1 es inyectiva. En efecto, sea $b \in B[\beta]$, con $i_1(\overline{b}) = \overline{0}$. Esto ocurre si $b \in \alpha A$, y escribimos $b = \alpha(a)$. Pero $0 = \beta(b) = \beta(\alpha(a)) = \gamma(a)$ Entonces $a \in A[\gamma], \Rightarrow b = \alpha(a) \in \alpha(A[\gamma]) \Rightarrow \overline{b} = \overline{0}$ en $B[\beta]/\alpha(A[\gamma])$.

$Im\, i_1 = Ker\, \beta$. Claramente $\beta(\overline{b}) = \overline{0}$ si $\overline{b} \in B[\beta]/\alpha(A[\gamma])$. Por otra parte si $\overline{b} \in Ker\beta$, entonces $\beta(b) \in \gamma A$. Escribimos $\beta(b) = \gamma(a) = \beta(\alpha(a))$. Sea $c = b - \alpha(a)$. Luego $\beta(c) = 0$. $b = c + \alpha(a) \Rightarrow \overline{b} = \overline{c}$ en $B/\alpha A$. Pero $\overline{c} \in B[\beta]/\alpha(A[\gamma])$, por lo tanto $\overline{b} \in Im\, i_1$.

$Im\, \beta = Ker\, i_2$. Es claro que si $a \in A$ verifica $a \in \beta B$, entonces $a = \beta(b)$ para algún $b \in B$ y luego $a \in Im\, \beta$. Si $a \in Im\, \beta$, se tiene que $a = \beta(b)$ para algún $b \in B$ y entonces $\overline{a} = \overline{0}$ en $A/\beta B$.

i_2 es suryectiva pues $\gamma A \subseteq \beta B$. Y con esto hemos probado la exactitud en todos los puntos de la sucesión. $\diamond$

Corolario 21 *$F(\mathbb{Q})/2F(\mathbb{Q})$ es finito.*

Demostración: Consideramos el Lema anterior con

$$A = F(\mathbb{Q}), \qquad B = G(\mathbb{Q}), \qquad \alpha = \phi, \qquad \beta = \psi$$

Como $G(\mathbb{Q})/\phi F(\mathbb{Q})$ y $F(\mathbb{Q})/\psi G(\mathbb{Q})$ son ambos finitos por el Teorema anterior, aplicamos el Lema y sale que $F(\mathbb{Q})/2F(\mathbb{Q})$ es finito. $\diamond$

Además hemos obtenido una forma de calcular $F(\mathbb{Q})/2F(\mathbb{Q})$ a partir de $G(\mathbb{Q})/\phi F(\mathbb{Q})$ y $F(\mathbb{Q})/\psi G(\mathbb{Q})$. En efecto por aplicación del Lema nos queda:

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle \psi(G(\mathbb{Q})/\phi F(\mathbb{Q})), F(\mathbb{Q})/\psi G(\mathbb{Q}) \rangle$$

Si miramos con cuidado las ecuaciones de la demostración del Lema anterior, podemos obtener mas información acerca de $F(\mathbb{Q})/2F(\mathbb{Q})$. En efecto, probamos:

Lema 22 *El grupo $G(\mathbb{Q})/\phi F(\mathbb{Q})$ es isomorfo al grupo de los $q(\mathbb{Q}^*)^2 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ tales que:*

(1) *$q \in \mathbb{Z}$ es libre de cuadrados y $q|b_1$.*

(2) *La ecuación*

$$ql^4 + a_1 l^2 m^2 + \left(\frac{b_1}{q}\right) m^4 = n^2$$

tiene solución con $l, m, n \in \mathbb{Z}$ no todos nulos.

Mas aún, el punto $(0,0)$ de $G(\mathbb{Q})$ se corresponde con $q =$ el producto de los primos que dividen a b_1 manteniendo el signo de b_1.

Demostración: En efecto, si tenemos l, m, n y q, podemos recuperar u como:

$$u = q\frac{l^2}{m^2}$$

por las cuentas de los Lemas anteriores. Por el primer Lema acerca de q y por su construcción, q resulta inyectiva sobre $G(\mathbb{Q})/\phi F(\mathbb{Q})$. Por lo tanto tenemos un isomorfismo.

Si miramos el $(0,0)$ su imagen es $(a^2 - 4b)(\mathbb{Q}^*)^2 = b_1(\mathbb{Q}^*)^2$. $\diamond$

Este Lema nos determina el grupo $F(\mathbb{Q})/2F(\mathbb{Q})$. Desgraciadamente no es tan útil como podría suponerse pues al no tener un principio local-global para las cuárticas, no tenemos un forma efectiva para decidir si tienen solución global o no. Entonces, aunque en algunos casos podemos determinar $F(\mathbb{Q})/2F(\mathbb{Q})$, en general tendremos un "error" generado por las cuárticas que tienen solución local en todos lados pero no tienen solución global. Mas adelante veremos esto en mas detalle.

Veamos algún ejemplo:

Consideremos la curva:

$$\mathcal{C} : Y^2Z - X(X^2 + 3XZ + 5Z^2) = F(X, Y, Z)$$

Aplicando la función ϕ obtenemos la curva:

$$\mathcal{D} : Y^2Z - X(X^2 - 6XZ - 11Z^2) = G(X, Y, Z)$$

Para calcular $G(\mathbb{Q})/\phi F(\mathbb{Q})$: Buscamos los $q| - 11$. Sabemos que -11 le corresponde al $(0,0)$. $q = 1$ es trivial. Si miramos $q = -1$:

$$-l^4 - 6l^2m^2 + 11m^4 = n^2$$

tiene solución $(l, m, n) = (1, 1, 2)$ y entonces

$$u = q\frac{l^2}{m^2} = -1, \qquad (u, v) = (-1, \pm 2) \in \mathcal{D}$$

El caso $q = 11$ no nos interesa si estamos buscando generadores, pues $11 = (-1)(-11)$ y ya tenemos los puntos que corresponden con -1 y con -11. $\Rightarrow$

$$G(\mathbb{Q})/\phi F(\mathbb{Q}) = \langle (0, 0), (-1, 2) \rangle$$

y son generadores "en serio", ninguno de ellos está en $\phi F(\mathbb{Q})$.

Para calcular $F(\mathbb{Q})/\psi G(\mathbb{Q})$: Buscamos los $q|5$. Sabemos que 5 le corresponde al $(0, 0)$. Como $q = 1$ es trivial, hay que ver que pasa con $q = -5$ y $q = -1$. Si miramos $q = -1$:

$$\begin{aligned} -l^4 + 3l^2m^2 - 5m^4 &= n^2 \\ -\left(l^2 - \frac{3}{2}m^2\right)^2 - \frac{11}{4}m^4 &= n^2 \end{aligned}$$

y esto claramente no tiene solución. Con $q = -5$ tampoco va a haber solución pues si la hubiera como $-1 = 5(-5)^{-1}$ entonces habría solución para $q = -1$. $\Rightarrow$

$$F(\mathbb{Q})/\psi G(\mathbb{Q}) = \langle (0, 0) \rangle$$

Entonces,

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle \psi((0, 0)), \psi((-1, 2)), (0, 0) \rangle$$

Calculemos:

$$\psi((0, 0)) = \mathbf{o}$$

$\psi((-1, 2))$:

$$\rho = \frac{\lambda^2 - 6\lambda - 11}{\lambda} = \frac{1 + 6 - 11}{-1} = 4$$

$$\sigma = \mu\left(1 - \left(\frac{-11}{\lambda^2}\right)\right) = 2\left(1 + \frac{11}{1}\right) = 24$$

$$\xi = \frac{\rho}{4} = 1, \qquad \eta = \frac{\sigma}{8} = 3$$

$\Rightarrow$

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle (1, 3), (0, 0) \rangle$$

6.3. Alturas y Teorema de la Base Finita

Ahora vamos a pasar a ver la segunda parte de la demostración del Teorema de Mordell.

Sea $\mathbf{u} = [u_0 : ... : u_n]$ un punto del espacio proyectivo n-dimensional sobre $\mathbb{Q}$. Como las coordenadas son homogéneas podemos suponer sin pérdida de generalidad que

$$u_j \in \mathbb{Z}, (u_0; ...; u_n) = 1.$$

La **altura** $H(\mathbf{u})$ se define como

$$H(\mathbf{u}) = \max_j \{|u_j|\}$$

con la normalización anterior.

Si $x \in \mathbb{Q}$, escribimos

$$H(x) = \max \{|u_0|, |u_1|\}$$

donde $x = \frac{u_0}{u_1}$ con $u_0, u_1 \in \mathbb{Z}$ coprimos.

Lema 23 (1) *Sean* $D(X_0, X_1), E(X_0, X_1) \in \mathbb{Q}[X_0, X_1]_n$. *Sea* $\mathbf{u} = [u_0 : u_1]$ *un punto de la recta proyectiva racional, y supongamos que* $D(u_0, u_1), E(u_0, u_1)$ *no se anulan. Entonces:*

$$H(D(\mathbf{u}), E(\mathbf{u})) \leq cH(\mathbf{u})^n$$

con c *independiente de* $\mathbf{u}$.

(2) *Supongamos que la resultante de* D *y* E *es no nula. (Es lo mismo que decir que no tienen ningún cero en común en* $\overline{\mathbb{Q}}$*). Entonces existe* $\gamma > 0$, *independiente de* $\mathbf{u}$ *tal que:*

$$H(D(\mathbf{u}), E(\mathbf{u})) \geq \gamma H(\mathbf{u})^n$$

Demostración: Por homogeneidad, podemos suponer que

$$D(X_0, X_1), E(X_0, X_1) \in \mathbb{Z}[X_0, X_1]$$

y que $\mathbf{u} = [u_0 : u_1]$ está normalizado. Tenemos:

$$|D(\mathbf{u})|, |E(\mathbf{u})| \leq c(\max \{|u_0|, |u_1|\})^n$$

para cierto c. Y entonces obtenemos (1).

Ahora supongamos que estamos en las hipótesis de (2) y sea R la resultante. Entonces existen $L_j(X_0, X_1), M_j(X_0, X_1) \in \mathbb{Z}[X_0, X_1](j = 0, 1)$ homogéneos tales que:

$$L_j D + M_j E = R X_j^{2n-1} \qquad (j = 0, 1)$$

Substituyendo por $\mathbf{u}$ en la ecuación anterior, obtenemos:

$$L_0(u_0, u_1)D(u_0, u_1) + M_0(u_0, u_1)E(u_0, u_1) = R u_0^{2n-1}$$

$$L_1(u_0, u_1)D(u_0, u_1) + M_1(u_0, u_1)E(u_0, u_1) = R u_1^{2n-1}$$

y deducimos que

$$(D(\mathbf{u}); E(\mathbf{u}))|(R u_0^{2n-1}; R u_1^{2n-1}) = R$$

entonces cualquier divisor en común está uniformemente acotado independientemente de $\mathbf{u}$.

Además, como en la demostración de (1), hay un c' tal que

$$|L_j(\mathbf{u})|, |M_j(\mathbf{u})| \leq c'(\text{máx}\,\{|u_0|, |u_1|\})^{n-1} \qquad (j = 0, 1)$$

Luego,

$$2c'(\text{máx}\,\{|u_0|, |u_1|\})^{n-1}\,\text{máx}\,\{|D(u_0, u_1)|, |E(u_0, u_1)|\} \geq |R||u_0|^{2n-1}, |R||u_1|^{2n-1}$$

Por lo tanto,

$$H(D(u_0, u_1), E(u_0, u_1)) \geq \frac{1}{|R|}\,\text{máx}\,\{|D(u_0, u_1)|, |E(u_0, u_1)|\} \geq \frac{1}{2c'}\,\text{máx}\,\{|u_0|, |u_1|\}^n$$

$\diamond$

Sean ahora $\mathbf{u} = [u_0 : u_1]$ y $\mathbf{v} = [v_0 : v_1]$ dos puntos de la línea proyectiva. Y sea

$$\mathbf{w} = [u_0 v_0 : u_0 v_1 + u_1 v_0 : u_1 v_1] = [w_0 : w_1 : w_2]$$

Lema 24

$$\frac{1}{2} \leq \frac{H(\mathbf{w})}{H(\mathbf{u})H(\mathbf{v})} \leq 2$$

Demostración: Supongamos que $\mathbf{u}$ y $\mathbf{v}$ ya están normalizados. Es fácil ver que $(w_0; w_1; w_2) = 1$ y entonces para la desigualdad de la izquierda es suficiente probar que

$$\max\{|w_0|, |w_1|, |w_2|\} \geq \frac{1}{2} \max\{|u_0|, |u_1|\} \max\{|v_0|, |v_1|\}$$

Si los máximos de la derecha se alcanzan con el mismo subíndice, ya está. Si no, podemos suponer sin pérdida de generalidad que estos son $|u_0|$ y $|v_1|$. Si $2|u_0v_0| \geq |u_0v_1|$ o bien $2|u_1v_1| \geq |u_0v_1|$ listo, si eso no se cumple, entonces,

$$2|v_0| < |v_1|, \qquad 2|u_1| < |u_0|$$

$\Rightarrow$

$$|u_0v_1| \geq 4|u_1v_0|$$

Y lo que hay que probar es que

$$2|u_0v_1 + u_1v_0| \geq |u_0v_1|$$

Pero

$$2|u_0v_1+u_1v_0| \geq 2(|u_0v_1|-|u_1v_0|) = |u_0v_1|+(|u_0v_1|-2|u_1v_0|) \geq |u_0v_1|+2|u_1v_0| \geq |u_0v_1|$$

La desigualdad de la derecha es inmediata pues:

$$\begin{aligned} |u_0v_0| &\leq 2\max\{|u_0|, |u_1|\} \max\{|v_0|, |v_1|\} \\ |u_0v_1 + u_1v_0| &\leq 2\max\{|u_0|, |u_1|\} \max\{|v_0|, |v_1|\} \\ |u_1v_1| &\leq 2\max\{|u_0|, |u_1|\} \max\{|v_0|, |v_1|\} \end{aligned}$$

$\diamond$

En el contexto de las curvas elípticas,

$$\mathcal{C} : Y^2Z - (X^3 + AXZ^2 + BZ^3) = F(X, Y, Z)$$

con $A, B \in \mathbb{Z}$, $\quad 4A^3 + 27B^2 \neq 0$,

Se define la altura de un punto $\mathbf{x} = (x, y) \in \mathcal{C}$ como la altura de la coordenada X. O sea, si $\mathbf{x} = [x : y : z]$, tenemos

$$H(\mathbf{x}) = H(x, z), \qquad (\mathbf{x} \neq \mathbf{o})$$

$$H(\mathbf{o}) = 1$$

.

Lema 25 *Existen constantes $c_1, \gamma_1 > 0$ que dependen sólo de $\mathcal{C}$ tales que*

$$\gamma_1 \leq \frac{H(2\mathbf{x})}{H(\mathbf{x})^4} \leq c_1$$

Demostración: Escribiendo $\mathbf{x} = (x, y), \quad 2\mathbf{x} = (x_2, y_2)$ tenemos

$$x_2 = \frac{D(x)}{E(x)}$$

donde

$$\begin{aligned} D(X) &= (3X^2 + A)^2 - 8X(X^3 + AX + B) \\ E(X) &= 4(X^3 + AX + B) \end{aligned}$$

La resultante entre $3X^2 + A$ y $X^3 + AX + B$ es $4A^3 + 27B^2 \neq 0$. La resultante entre $D(X)$ y $E(X)$ es:

$$R(D, E) = \delta \prod_{j=1}^{3} D(r_j)$$

con $\delta \neq 0$ donde r_j $(j = 1, 2, 3)$ son las raíces de $E(X)$.

Pero como $3X^2 + A = (X^3 + AX + B)' = F(X)'$,

$$R(D, E) = \delta \prod_{j=1}^{3} (F'(r_j))^2 = \delta(\Delta(F))^2 = \delta(4A^3 + 27B^2)^2 \neq 0$$

Entonces se dan las condiciones del primer Lema con $n = 4$ si se lo aplica a $x = \frac{u_0}{u_1}$. $\diamond$

Lema 26 *Sean $\mathbf{x_1}, \mathbf{x_2} \in F(\mathbb{Q})$. Entonces*

$$H(\mathbf{x_1} + \mathbf{x_2})H(\mathbf{x_1} - \mathbf{x_2}) \leq c_2 H(\mathbf{x_1})^2 H(\mathbf{x_2})^2$$

donde c_2 depende sólo de la curva $\mathcal{C}$.

Demostración: Escribimos

$$\mathbf{x_1} + \mathbf{x_2} = \mathbf{x_3}$$

$$\mathbf{x_1} - \mathbf{x_2} = \mathbf{x_4}$$

y $\mathbf{x_j} = (x_j, y_j)$. Entonces

$$[1 : x_3 + x_4 : x_3 x_4] = [w_0 : w_1 : w_2]$$

donde

$$\begin{aligned} w_0 &= (x_2 - x_1)^2 \\ w_1 &= 2(x_1 x_2 + A)(x_1 + x_2) + 4B \\ w_2 &= x_1^2 x_2^2 - 2Ax_1 x_2 - 4B(x_1 + x_2) + A^2 \end{aligned}$$

En efecto, por la fórmula de adición,

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2$$

$$x_4 = \left(\frac{y_1 + y_2}{x_1 - x_2}\right)^2 - x_1 - x_2$$

de donde

$$\begin{aligned} x_3 + x_4 &= \frac{2(y_1^2 + y_2^2)}{(x_1 - x_2)^2} - 2(x_1 + x_2) \\ &= \frac{2(x_1^3 + x_2^3) + 2A(x_1 + x_2) + 4B - 2(x_1 - x_2)^2(x_1 + x_2)}{(x_1 - x_2)^2} \end{aligned}$$

$$\begin{aligned} (x_3 + x_4)(x_2 - x_1)^2 &= 2(x_1^3 + x_2^3) + 2A(x_1 + x_2) + 4B - 2(x_1^3 + x_2^3 - x_1 x_2(x_1 + x_2)) \\ &= 2(x_1 x_2 + A)(x_1 + x_2) + 4B \end{aligned}$$

Para ver w_2:

$$x_3 x_4 = \left(\frac{y_1^2 - y_2^2}{(x_1 - x_2)^2}\right)^2 + (x_1 + x_2)^2 - (x_1 + x_2)\frac{2(y_1^2 + y_2^2)}{(x_1 - x_2)^2}$$

$$x_3 x_4 (x_2 - x_1)^2 = \left(\frac{y_1^2 - y_2^2}{x_1 - x_2}\right)^2 + (x_1^2 - x_2^2)^2 - 2(x_1 + x_2)(y_1^2 + y_2^2)$$

$$\begin{aligned} &= \left(\frac{x_1^3 - x_2^3 + A(x_1 - x_2)}{x_1 - x_2}\right)^2 + (x_1^2 - x_2^2)^2 - 2(x_1 + x_2)(x_1^3 + x_2^3 + A(x_1 + x_2) + 2B) \\ &= ((x_1^2 + x_2^2) + x_1 x_2 + A)^2 + (x_1^2 - x_2^2)^2 - 2(x_1 + x_2)(x_1^3 + x_2^3 + A(x_1 + x_2) + 2B) \\ &= (x_1^2 + x_2^2)^2 + x_1^2 x_2^2 + A^2 + 2A(x_1^2 + x_2^2) + 2Ax_1 x_2 + 2x_1 x_2(x_1^2 + x_2^2) + (x_1^2 - x_2^2)^2 \end{aligned}$$

$$-2(x_1+x_2)(x_1^3+x_2^3) - 2A(x_1+x_2)^2 - 4B(x_1+x_2)$$
$$= x_1^2x_2^2 - 2Ax_1x_2 - 4B(x_1+x_2) + A^2 + (x_1^2+x_2^2)^2 + 2x_1x_2(x_1^2+x_2^2) + (x_1^2-x_2^2)^2$$
$$-2(x_1+x_2)(x_1^3+x_2^3)$$
$$= x_1^2x_2^2 - 2Ax_1x_2 - 4B(x_1+x_2) + A^2$$

Si se escriben x_1 y x_2 como cociente de números enteros, y se homogeniza, se ve claramente que:

$$H(w_0, w_1, w_2) \leq c_3 H(x_1)^2 H(x_2)^2$$

Para algún c_3. Por otro lado,

$$H(w_0, w_1, w_2) = H(1, x_3 + x_4, x_3x_4) \geq \frac{1}{2} H(x_3)H(x_4)$$

por un Lema anterior. Y aca se deduce la afirmación para $c_2 = 2c_3$. $\diamond$

Corolario 27

$$\text{mín}\left\{H(\mathbf{x}_1 + \mathbf{x}_2), H(\mathbf{x}_1 - \mathbf{x}_2)\right\} \leq c_4 H(\mathbf{x}_1)H(\mathbf{x}_2)$$

donde $c_4 = c_2^{\frac{1}{2}}$.

Lema 28 *Sea* λ *dado. Existen solo finitos* $\mathbf{x} \in F(\mathbb{Q})$ *tales que* $H(\mathbf{x}) \leq \lambda$

Demostración: Si $\mathbf{x} = (x, y)$ con $H(\mathbf{x}) = H(x) \leq \lambda$. Entonces $x = \frac{u_0}{u_1}$ con $u_0, u_1 \in \mathbb{Z}$ y como $|u_0|, |u_1| \leq \lambda$, entonces hay finitas posibilidades para elegir a $x \Rightarrow$ hay finitas posibilidades para $\mathbf{x}$. $\diamond$

Ahora ya estamos en condiciones de probar el Teorema que queremos: *Demostración (Teorema de Mordell):* Por el Teorema Débil, $F(\mathbb{Q})/2F(\mathbb{Q})$ es finito. Sean $\mathbf{b}_1, ..., \mathbf{b}_s \in F(\mathbb{Q})$ representantes de las clases de $F(\mathbb{Q})$ módulo $2F(\mathbb{Q})$.

Sea $\mathbf{a} \in F(\mathbb{Q})$. Existe un j tal que $\mathbf{a} \pm \mathbf{b}_j \in 2F(\mathbb{Q})$ para ambas elecciones del signo. Por el Corolario anterior, hay una elección de signo tal que

$$H(\mathbf{a} \pm \mathbf{b}_j) \leq c_4 H(\mathbf{a})H(\mathbf{b}_j)$$

Como $\mathbf{a} \pm \mathbf{b}_j = 2\mathbf{c}$, $\mathbf{c} \in F(\mathbb{Q})$,

$$H(\mathbf{a} \pm \mathbf{b}_j) \geq \gamma_1 H(\mathbf{c})^4$$

Por un Lema anterior. Juntando las desigualdades anteriores tenemos:

$$H(\mathbf{c})^4 \leq \frac{c_4}{\gamma_1} H(\mathbf{a}) H(\mathbf{b}_j) \leq \kappa H(\mathbf{a})$$

donde

$$\kappa = \frac{c_4}{\gamma_1} \operatorname{máx} \{H(\mathbf{b}_j)\}$$

Entonces o bien

$$H(\mathbf{c}) \leq \frac{1}{2} H(\mathbf{a})$$

o bien

$$H(\mathbf{a}) \leq (16\kappa)^{\frac{1}{3}} = \lambda$$

Se sigue que $F(\mathbb{Q})$ está generado por los $\mathbf{b}_j$ y los $\mathbf{a}$ que cumplen $H(\mathbf{a}) \leq \lambda$, que son finitos por el Lema anterior. $\diamond$

Hemos probado que $F(\mathbb{Q})$ es un grupo abeliano finitamente generado entonces podemos escribir:

$$F(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$$

Donde T es un grupo abeliano finito, el subgrupo de torsión. El entero r se llama **rango** de la curva.

6.4. Mas acerca de las Alturas

En analogía con un Lema anterior se puede probar que:

$$H(\mathbf{x_1} + \mathbf{x_2}) H(\mathbf{x_1} - \mathbf{x_2}) \geq \gamma_2 H(\mathbf{x_1})^2 H(\mathbf{x_2})^2$$

Con $\gamma_2 > 0$. Esto se debe a que los w_0, w_2, w_2, pensados como polinomios en x_1, x_2, no tienen ceros comunes en la clausura algebraica. En efecto $w_0 = 0 \Rightarrow x_1 = x_2$ y entonces w_1 y w_2 se vuelven las funciones E y D respectivamente de los Lemas anteriores que vimos que tienen resultante no nula. Por lo tanto la desigualdad se obtiene como la segunda parte del primer Lema.

Podemos definir la **altura logarítmica**:

$$h_0(\mathbf{x}) = \log H(\mathbf{x})$$

Ahora, por las observaciones anteriores,

$$|h_0(\mathbf{x_1} + \mathbf{x_2}) + h_0(\mathbf{x_1} - \mathbf{x_2}) - 2h_0(\mathbf{x_1}) - 2h_0(\mathbf{x_2})| \leq c$$

Para cierta constante c. En particular:

$$|h_0(2\mathbf{x}) - 4h_0(\mathbf{x})| \leq c$$

Proposición 29 *Existe una única función $h : F(\mathbb{Q}) \longmapsto \mathbb{R}$ que satisface:*
(1) $h(\mathbf{x}) - h_0(\mathbf{x})$ *está acotada*
(2) $h(2\mathbf{x}) = 4h(\mathbf{x})$

Observación 30 *La función está dada por*

$$h(\mathbf{x}) = \lim_{n\to\infty} \frac{h_0(2^n\mathbf{x})}{4^n}$$

Y se cumple $h(\mathbf{x}) \geq 0$ con igualdad si y solo si $\mathbf{x}$ tiene orden finito. Además $\{\mathbf{x}|h(\mathbf{x}) \leq \lambda\}$ es un conjunto finito para cada λ.

Demostración: Para la unicidad supongamos que tenemos la h que satisface (1) y (2) con cota c' en (1). Entonces,

$$|4^n h(\mathbf{x}) - h_0(2^n\mathbf{x})| = |h(2^n\mathbf{x}) - h_0(2^n\mathbf{x})| \leq c'$$

Y luego

$$\left| h(\mathbf{x}) - \frac{h_0(2^n\mathbf{x})}{4^n} \right| \leq \frac{c'}{4^n}$$

Y entonces necesariamente h tiene que estar dada por la fórmula de la Observación anterior.

Habíamos dicho que

$$|h_0(2\mathbf{x}) - 4h_0(\mathbf{x})| \leq c \tag{5}$$

Si $n \geq m \geq 0$

$$\begin{aligned} \left| \frac{h_0(2^n\mathbf{x})}{4^n} - \frac{h_0(2^m\mathbf{x})}{4^m} \right| &\leq \sum_{k=m}^{n-1} \frac{|h_0(2^{k+1}\mathbf{x}) - 4h_0(2^k\mathbf{x})|}{4^{k+1}} \\ &\leq \sum_{k=m}^{n-1} \frac{c}{4^{k+1}} \leq \frac{c}{3{,}4^m} \end{aligned}$$

Entonces la sucesión es de Cauchy y existe el límite.

Además tomando límite en n, se tiene (1). El resultado (2) es claro de la ecuación 5.

También es claro que $h(\mathbf{x}) \geq 0$ pues $h_0(\mathbf{x}) \geq 0$ ya que $H(\mathbf{x}) \geq 1$.

Si $\mathbf{x}$ es de torsión entonces $2^n\mathbf{x}$ varía en un conjunto finito. Luego $h_0(2^n\mathbf{x})$ está acotado y $h(\mathbf{x}) = 0$ al tomar el límite. Si $\mathbf{x}$ es de orden infinito, como el conjunto $\{\mathbf{x}|h(\mathbf{x}) \leq 1\}$ es finito, debemos tener $h(2^n\mathbf{x}) > 1$ para algún n y entonces $h(\mathbf{x}) > 4^{-n} > 0$.$\diamond$

h se llama **altura canónica**.

Proposición 31

$$h(\mathbf{x_1} + \mathbf{x_2}) + h(\mathbf{x_1} - \mathbf{x_2}) = 2h(\mathbf{x_1}) + 2h(\mathbf{x_2})$$

Demostración: Es claro por la Proposición anterior y por las observaciones hechas antes de esta.$\diamond$

Proposición 32 *Existe una única forma bilineal $\langle \mathbf{x}, \mathbf{y} \rangle$ en $F(\mathbb{Q})$ que cumple que $\langle \mathbf{x}, \mathbf{x} \rangle = 2h(\mathbf{x})$. Esta forma desciende a $F(\mathbb{Q})/T \cong \mathbb{Z}^r$ y es definida positiva ahí.*

Demostración: Si la forma existe, tiene que estar definida por

$$\langle \mathbf{x}, \mathbf{y} \rangle = h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y}).$$

Esto nos da la unicidad. Para la existencia, la definimos asi. Claramente es simétrica. Veamos aditividad en la primer variable. Usaremos varias veces la Proposición anterior.

$$\langle \mathbf{x}, -\mathbf{y} \rangle = h(\mathbf{x} - \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y}) = -(h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y})) = -\langle \mathbf{x}, \mathbf{y} \rangle$$

Luego

$$\langle \mathbf{x} + \tilde{\mathbf{x}}, \mathbf{y} \rangle + \langle \mathbf{x} - \tilde{\mathbf{x}}, \mathbf{y} \rangle = h(\mathbf{x}+\tilde{\mathbf{x}}+\mathbf{y}) + h(\mathbf{x}-\tilde{\mathbf{x}}+\mathbf{y}) - h(\mathbf{x}+\tilde{\mathbf{x}}) - h(\mathbf{x}-\tilde{\mathbf{x}}) - h(\mathbf{y}) - h(\mathbf{y})$$

$$= 2h(\mathbf{x} + \mathbf{y}) + 2h(\tilde{\mathbf{x}}) - 2h(\mathbf{x}) - 2h(\tilde{\mathbf{x}}) - 2h(\mathbf{y}) = 2\langle \mathbf{x}, \mathbf{y} \rangle$$

Intercambiando $\mathbf{x}$ con $\tilde{\mathbf{x}}$ obtenemos

$$\langle \mathbf{x} + \tilde{\mathbf{x}}, \mathbf{y} \rangle - \langle \mathbf{x} - \tilde{\mathbf{x}}, \mathbf{y} \rangle = \langle \mathbf{x} + \tilde{\mathbf{x}}, \mathbf{y} \rangle + \langle \tilde{\mathbf{x}} - \mathbf{x}, \mathbf{y} \rangle = 2\langle \tilde{\mathbf{x}}, \mathbf{y} \rangle$$

sumando,

$$\langle \mathbf{x} + \tilde{\mathbf{x}}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \langle \tilde{\mathbf{x}}, \mathbf{y} \rangle$$

Entonces la forma es bilineal y positiva.

Luego cumple la desigualdad de Cauchy,

$$|\langle \mathbf{x}, \mathbf{y} \rangle|^2 \leq 4h(\mathbf{x})h(\mathbf{y})$$

Si $\mathbf{y}$ es un punto de torsión, entonces $h(\mathbf{y}) = 0$ y luego por lo anterior $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, por lo tanto,

$$0 = \langle \mathbf{x}, \mathbf{y} \rangle = h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y}) = h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x})$$

y entonces

$$h(\mathbf{x}) = h(\mathbf{x} + \mathbf{y})$$

Con lo cual h desciende a $F(\mathbb{Q})/T$. $\diamond$

Sean $\mathbf{x}_1, ..., \mathbf{x}_r$ $\mathbb{Z}$-base de $\mathbb{Z}^r$ y sea $c_{i,j} = \langle \mathbf{x}_i, \mathbf{x}_j \rangle$. Lo que vimos es que la matriz (c_{ij}) es semidefinida positiva.

Ahora queremos extender nuestra conclusión a que la matriz es estrictamente positiva.

Lema 33 *(Minkowski) Si K es un conjunto compacto convexo de $\mathbb{R}^r$ que contiene al 0, es cerrado bajo los negativos y tiene volumen $> 4^r$, entonces K contiene un miembro no nulo de $\mathbb{Z}^r$.*

Demostración: Sea n un entero suficientemente grande como para que el cubo C de centro 0 y lado $4n$ contenga a K. Supongamos que K no contiene ningún elemento no nulo de $\mathbb{Z}^r$.

Afirmamos que los conjuntos $l + \frac{1}{2}K$ con $l \in \mathbb{Z}^r$ son disjuntos. En efecto, si $l_1 + \frac{1}{2}k_1 = l_2 + \frac{1}{2}k_2$ con $l_1 \neq l_2$, entonces $l_1 - l_2 = \frac{1}{2}(k_2 - k_1) \in K$ por las hipótesis, y esto es una contradicción.

Si las coordenadas de l son $\leq n$ entonces $l + \frac{1}{2}K$ está en C. Por lo tanto,

$$(4n)^r = vol(C) \geq \sum_{|coord(l)| \leq n} vol\left(l + \frac{1}{2}K\right) \geq (2n)^r vol\left(\frac{1}{2}K\right) = n^r vol(K)$$

y como $vol(K) > 4^r$ se llega a una contradicción.$\diamond$

Proposición 34 *Con la notación de antes, (c_{ij}) es definida positiva.*

Demostración: Como es semidefinida positiva y simétrica podemos elegir una base ortonormal de vectores

$$v^1, ..., v^r$$

correspondientes a los autovalores

$$\lambda_1 \geq ... \geq \lambda_r \geq 0$$

Supongamos que $\lambda_r = 0$. Identificaremos $\mathbf{x} = \sum_i m_i \mathbf{x}_i$ con el vector $(m_1, ..., m_r)$ Entonces,

$$\left\langle \sum_k b_k v^k, \sum_l b_l v^l \right\rangle = \sum_{k,l} b_k b_l \sum_{i,j} v_i^k c_{ij} v_j^l = \sum_k \lambda_k b_k^2$$

Sea ϵ el menor valor de $h(\mathbf{x})$, para $\mathbf{x} \notin T$. Existe y es positivo pues $\{\mathbf{x} | h(\mathbf{x}) \leq C\}$ es finito. Sea K el conjunto compacto convexo de los vectores columna:

$$K = \left\{ \sum_{k=1}^{r} b_k v^k | \max_{1 \leq k \leq r-1} |b_k| \leq \left(\frac{\epsilon}{2r\lambda_1} \right)^{\frac{1}{2}}, |b_r| \leq M \right\}$$

donde M se toma lo suficientemente grande como para que $vol(K) > 4^r$. Por el Lema anterior, K contiene un punto con coordenadas enteras no nulo $\mathbf{x} = \sum b_k v^k$.

$$h(\mathbf{x}) = \left\langle \sum_k b_k v^k, \sum_l b_l v^l \right\rangle = \sum_{k=1}^{r} \lambda_k b_k^2 = \sum_{k=1}^{r-1} \lambda_k b_k^2$$

pues $\lambda_k = 0$

$$\leq \sum_{k=1}^{r-1} \lambda_1 \left(\frac{\epsilon}{2r\lambda_1} \right) \leq \frac{\epsilon}{2}$$

Y esto es una contradicción. Luego $\lambda_r > 0$ y la matriz es definida positiva estricta.$\diamond$

La matriz (c_{ij}) depende de la base elegida, pero no su determinante. Se llama **regulador elíptico** de $\mathcal{C}$ al número:

$$R = det(\langle \mathbf{x}_i, \mathbf{x}_j \rangle)$$

7. Los Puntos de Torsión

7.1. Reducción de Curvas

La idea es, como ya dijimos, aproximar lo que pasa en $\mathbb{Q}$ con lo que pasa en $\mathbb{Q}_p$ con la ayuda de la reducción a los cuerpos finitos $\mathbb{F}_p$.

En general, la reducción de un punto $\mathbf{x} = [x : y : z]$ del plano proyectivo se hace de la siguiente manera: Se multiplica por un elemento de $\mathbb{Q}_p$ a las coordenadas para que

$$\text{máx}\left\{|x|_p, |y|_p, |z|_p\right\} = 1$$

Y entonces se reducen las nuevas coordenadas módulo p. Por la condición anterior, nos aseguramos de no obtener $[0 : 0 : 0]$.

Para reducir una curva, se reducen los coeficientes haciendo antes el mismo proceso que hicimos con los puntos (multiplicando por un elemento de $\mathbb{Q}_p$ de modo que el máximo valor absoluto de los coeficientes sea 1), pero esta vez podría ser que la curva nos quede singular. Como las rectas también se reducen de la misma manera, conservamos la ley de grupo en los puntos no singulares de las cúbicas.

Además tenemos el siguiente

Lema 35 *(Lema de Hensel) Sea $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$, y sea $\overline{a} = (a_1, ..., a_n) \in \mathbb{Z}^n$ con la propiedad que para cierto $m \geq 0$,*

$$f(\overline{a}) \equiv 0_{mod\, p^{2m+r}}$$

con $r \geq 1$, y para cierto i,

$$\left(\frac{\partial f}{\partial X_i}\right)(\overline{a}) \not\equiv 0_{mod\, p^{m+1}}.$$

Entonces existe un $\overline{b} \in \mathbb{Z}^n$ tal que

$$\overline{b} \equiv \overline{a}_{mod\, p^{m+r}}$$

y

$$f(\overline{b}) \equiv 0_{mod\, p^{2m+r+1}}$$

Demostración: Consideremos la expansión de Taylor:

$$f(X_1,...,X_n) = f(a_1,...,a_n) + \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i}\right)_{\overline{a}} (X_i - a_i) + \text{términos de mayor grado.}$$

Sea $b_i = a_i + h_i p^{m+r}, \quad h_i \in \mathbb{Z}$. Luego,

$$f(b_1,...,b_n) = f(a_1,...,a_n) + \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i}\right)_{\overline{a}} h_i p^{m+r} + \text{términos divisibles por } p^{2m+2r}.$$

Tenemos que elegir h_i para que

$$f(a_1,...,a_n) + \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i}\right)_{\overline{a}} h_i p^{m+r}$$

sea divisible por p^{2m+r+1}. Por las hipótesis, sabemos que hay un $k \leq m$ tal que $p^k | \left(\frac{\partial f}{\partial X_i}\right)_{\overline{a}}$ para todo i, pero p^{k+1} no los divide a todos. Será suficiente tomar los h_i tal que satisfagan:

$$\frac{f(a_1,...,a_n)}{p^{k+m+r}} + \sum_{i=1}^{n} \frac{\left(\frac{\partial f}{\partial X_i}\right)_{\overline{a}}}{p^k} h_i \equiv 0_{mod\, p^{m+1-k}}$$

$\diamond$

Teorema 36 *Bajo las hipótesis del Lema, existe un* $\overline{b} \in \mathbb{Z}_p^n$ *tal que* $f(\overline{b}) = 0$ *y* $\overline{b} \equiv \overline{a}_{mod\, p^{m+1}}$.

Demostración: Aplicando el Lema, obtenemos, $\overline{a}_{2m+2} \in \mathbb{Z}^n$ tal que $\overline{a}_{2m+2} \equiv \overline{a}_{mod\, p^{m+1}}$ y $f(\overline{a}_{2m+2}) \equiv 0_{mod\, p^{2m+2}}$. Aplicando de vuelta, obtenemos $\overline{a}_{2m+3} \in \mathbb{Z}^n$ tal que $\overline{a}_{2m+3} \equiv \overline{a}_{2m+2 mod\, p^{m+2}}$ y $f(\overline{a}_{2m+3}) \equiv 0_{mod\, p^{2m+3}}$. Continuando con el proceso, llegamos a una sucesión

$$\overline{a}, \overline{a}_{2m+2}, \overline{a}_{2m+3}, ...$$

La sucesión es de Cauchy en $\mathbb{Q}_p$ y sea $\overline{b}$ su límite. La función $f : \mathbb{Z}^n \to \mathbb{Z}$ es continua con la topología p-ádica y entonces

$$f(\overline{b}) = f(\lim_r \overline{a}_{2m+r}) = \lim_r f(\overline{a}_{2m+r}) = 0$$

◇

Sea

$$\mathcal{C} : Y^2Z - X^3 - AXZ^2 - BZ^3 = F(X, Y, Z)$$

una curva elíptica. Si $p|\Delta = 4A^3 + 27B^2$, la ecuación es singular sobre $\mathbb{F}_p$. Si $p \not| \Delta$, $p \neq 2, 3$ se obtiene otra curva elíptica sobre $\mathbb{F}_p$.

Podría suceder que $p|\Delta$ pero que sin embargo existe otra forma de Weierstrass de $\mathcal{C}$ con reducción no singular. Por ejemplo,

$$X \to p^2X, \qquad Y \to p^3Y$$

manda la curva $Y^2 = X^3 + p^4AX + p^6B$ en $Y^2 = X^3 + AX + B$, eliminando una potencia p^{12} del discriminante.

Una ecuación en forma de Weierstrass con coeficientes p-enteros se dice **minimal** para el primo p si la potencia de p que divide a Δ no puede disminuirse haciendo un cambio admisible de variables sobre $\mathbb{Q}$ con la propiedad que los nuevos coeficientes sean p-enteros. Es lo mismo que decir que no podemos aumentar el valor de $|\Delta|_p$.

Una ecuación se dice que está en forma **global - minimal de Weierstrass** si es minimal para todos los primos y los coeficientes son enteros. Pero en este caso hay que considerar la ecuación general con los a_i por el caso de $p = 2$ y $p = 3$. Existe una forma de definir el discriminante para este tipo de fórmulas, que mediante cambios de variables coincide con el discriminante usual salvo potencias (fijas) de 2 y de 3.

Veamos los distintos casos de reducción. En una curva elíptica reducida no hay mas de una singularidad, ya que si la característica es distinta de 2, se puede hacer un cambio para pasar la curva a la forma:

$$Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 = G(X)$$

las singularidades aparecen cuando el polinomio G tiene una raíz múltiple, y como es de grado 3, solo puede haber una raíz múltiple. Para el caso de característica 2, lo deducimos mas adelante.

Sea (x, y) el punto singular. Trasladándolo al origen se obtiene la curva:

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

(tomando en cuenta que ahora el $(0, 0)$ es un punto de la curva). Como las derivadas respecto de X y de Y deben dar cero en el $(0, 0)$, se tiene que $a_3 = a_4 = 0$.

Nos queda

$$X^3 = Y^2 + a_1XY - a_2X^2$$

Acá podemos mirar el caso de $p = 2$. Al derivar respecto de Y y de X e igualando las derivadas a cero nos da $a_1X = 0$ y $a_1Y = X^2$ y de acá sale que el único punto que puede ser singular es el $(0, 0)$.

Factorizando

$$X^3 = (Y - \alpha X)(Y - \beta X)$$

donde $\alpha, \beta \in \overline{k}$. En el caso en que $\alpha = \beta$, decimos que el $(0, 0)$ es una **cúspide**. En caso contrario es un **nodo**, que pude ser partido si $\alpha, \beta \in k$ o no partido en caso contrario.

Podemos parametrizar nuestra curva haciendo pasar rectas por el punto $(0, 0)$. En efecto, la recta

$$Y = lX$$

intersecta a la curva en $(0, 0)$ y en $(l^2 + a_1l - a_2, l^3 + a_1l^2 - a_2l)$. Entonces obtenemos una parametrización:

Proposición 37 *Si $\mathcal{C}$ es una curva elíptica singular dada en forma*

$$Y^2 + a_1XY = X^3 + a_2X^2$$

la función:

$$t \longmapsto (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$$

manda $k \setminus \{\alpha, \beta\}$ uno a uno sobre $F(k) \setminus \{(0, 0), \mathbf{o}\}$. Si estamos en un cuerpo finito de q elementos, esto nos muestra que el cardinal de $F(k) \setminus \{(0, 0)\}$ en cada caso es:

$$\begin{cases} q & \textit{caso cúspide} \\ q - 1 & \textit{caso de nodo partido} \\ q + 1 & \textit{caso de nodo no partido} \end{cases}$$

Demostración: $X = 0$ da sólo $Y = 0$ y $(0, 0)$ es singular. Entonces cualquier punto no singular distinto de $\mathbf{o}$ cumple $Y = tX$ para un único $t \in k$. Substituyendo en la curva nos da la parametrización. Para excluir $X = 0$ de la imagen, tenemos que sacar las raíces de $t^2 + a_1t - a_2$, que son α y β. Si $X = 0$ no está en la imagen, la función es uno a uno pues $t = \frac{Y}{X}$. La tabla sale de volcar toda esta información.$\diamond$

7.2. Curvas Elípticas sobre $\mathbb{Q}_p$

Sea

$$\mathcal{C} : Y^2Z-(X^3+AXZ^2+BZ^3) = F(X,Y,Z), \qquad A, B \in \mathbb{Q}_p, \qquad 4A^3+27B^2 \neq 0$$

Después de un cambio de variables se puede suponer que los coeficientes están en $\mathbb{Z}_p$. Se puede reducir la ecuación módulo p, considerando los coeficientes en $\mathbb{F}_p$. Se obtiene una función de reducción:

$$F(\mathbb{Q}_p) \longmapsto \overline{F}(\mathbb{F}_p)$$

$$\mathbf{x} \to \overline{\mathbf{x}}$$

Sea

$$F^0(\mathbb{Q}_p) = \{\mathbf{x} \in F(\mathbb{Q}_p) | \overline{\mathbf{x}} \text{ es no singular}\}$$

Tenemos entonces la misma función pero restringida a $F^0(\mathbb{Q}_p)$.

$$F^0(\mathbb{Q}_p) \longmapsto \overline{F}^0(\mathbb{F}_p)$$

Es un homomorfismo, pues si $\mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3 = \mathbf{o}$, entonces hay una recta que pasa por los tres puntos y reduciendo todo módulo p, en el caso en que sean no singulares tenemos definida la operación de grupo y entonces vale $\overline{\mathbf{x}}_1 + \overline{\mathbf{x}}_2 + \overline{\mathbf{x}}_3 = \overline{\mathbf{o}}$. Además el homomorfismo es suryectivo por el Lema de Hensel. Sea $F^1(\mathbb{Q}_p)$ su kernel.

Definimos

$$F^n(\mathbb{Q}_p) = \left\{ \mathbf{x} \in F^1(\mathbb{Q}_p) | \frac{x}{y} \in p^n\mathbb{Z}_p \right\}$$

Teorema 38 *La filtración*

$$F(\mathbb{Q}_p) \supset F^0(\mathbb{Q}_p) \supset F^1(\mathbb{Q}_p) \supset ... \supset F^n(\mathbb{Q}_p) \supset ...$$

tiene las siguientes propiedades:

(1) *El cociente $F(\mathbb{Q}_p)/F^0(\mathbb{Q}_p)$ es finito.*

(2) *La función $\mathbf{x} \to \overline{\mathbf{x}}$ define un isomorfismo $F^0(\mathbb{Q}_p)/F^1(\mathbb{Q}_p) \to \overline{F}^0(\mathbb{F}_p)$.*

(3) *Para $n \geq 1$, $F^n(\mathbb{Q}_p)$ es subgrupo de $F(\mathbb{Q}_p)$ y la función $\mathbf{x} \to p^{-n}\frac{x}{y}$ es un isomorfismo $F^n(\mathbb{Q}_p)/F^{n+1}(\mathbb{Q}_p) \to \mathbb{F}_p$.*

(4) $\bigcap_n F^n(\mathbb{Q}_p) = \mathbf{o}$.

Demostración: (1)Vamos a probar que $F(\mathbb{Q}_p)$ tiene una topología respecto de la cual es compacto y $F^0(\mathbb{Q}_p)$ es un subgrupo abierto. Como $F(\mathbb{Q}_p)$ es unión de las coclases de $F^0(\mathbb{Q}_p)$, se seguirá que tiene que haber una cantidad finita de tales coclases.

Consideremos $\mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$ con la topología producto, $\mathbb{Q}_p^3 \setminus \{(0,0,0)\}$ con la topología inducida como subespacio, y $\mathbb{P}^2(\mathbb{Q}_p)$ con la topología cociente

$$\mathbb{Q}_p^3 \setminus \{(0,0,0)\} \longmapsto \mathbb{P}^2(\mathbb{Q}_p)$$

Entonces $\mathbb{P}^2(\mathbb{Q}_p)$ es la unión de las imágenes de los conjuntos $\mathbb{Z}_p^* \times \mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p^* \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p^*$, cada uno de los cuales es compacto y abierto. Entonces $\mathbb{P}^2(\mathbb{Q}_p)$ es compacto. El subconjunto $F(\mathbb{Q}_p)$ es cerrado, por ser los ceros de un polinomio. Con esta topología dos puntos que están cerca tienen la misma reducción módulo p. Entonces $F^0(\mathbb{Q}_p)$ es la intersección de $F(\mathbb{Q}_p)$ con un subconjunto abierto de $\mathbb{P}^2(\mathbb{Q}_p)$.

(2) Ya vimos que es suryectivo y aplicamos el Primer Teorema de Isomorfismos de grupos.

(3) Sea $(x,y) \in F^1(\mathbb{Q}_p)$, entonces claramente $y \notin \mathbb{Z}_p$. Sean

$$x = p^{-r}x_1, \quad y = p^{-s}y_1 \quad \text{con } x_1, y_1 \in \text{unidades de } \mathbb{Z}_p.$$

Reemplazando en la ecuación,

$$p^{-2s}y_1^2 = p^{-3r}x_1^3 + Ap^{-r}x_1 + B$$

Tomando $|\cdot|_p$ en ambos lados, $-2s = -3r$, y como son enteros, $r = 2n, \quad s = 3n$. El n tiene que ser positivo pues en caso contrario, $x, y \in \mathbb{Z}_p$ y no podría estar en el kernel. Llamaremos nivel de (x,y) al n. El nivel de $\mathbf{o}$ es ∞.

Por todo lo anterior, si $\mathbf{x} = [x : y : z] \in F^n(\mathbb{Q}_p) \setminus F^{n+1}(\mathbb{Q}_p)$, podemos expresar $\mathbf{x} = [p^n x_1 : y_1 : p^{3n}z_1]$ con $x_1, y_1, z_1 \in \mathbb{Z}_p$, y_1 unidad de $\mathbb{Z}_p$. Se tiene

$$p^{3n}y_1^2 z_1 = p^{3n}x_1^3 + Ap^{7n}x_1 z_1^2 + Bp^{9n}z_0^3$$

Entonces el punto $\mathbf{x}_0 = [\overline{x_1} : \overline{y_1} : \overline{z_1}]$ está en la curva:

$$\mathcal{C}_0 : Y^2Z - X^3 = F_0(X,Y,Z)$$

Como $y_1 \neq 0$, $\mathbf{x}_0$ es no singular en $\mathcal{C}_0$. Pensando en la ley de grupo en términos de cuerdas y tangentes, la función

$$F^n(\mathbb{Q}_p) \longmapsto F_0(\mathbb{Q}_p)$$

$$\mathbf{x} \to \mathbf{x}_0$$

es un homomorfismo. Su kernel es $F^{n+1}(\mathbb{Q}_p)$, que entonces es un subgrupo, y se sigue del Lema de Hensel que su imagen son los puntos no singulares de $F_0(\mathbb{Q}_p)$, pero

$$F_0(\mathbb{Q}_p) \setminus \{\text{puntos singulares}\} \longmapsto \mathbb{F}_p$$
$$\mathbf{x} \to \frac{x}{y}$$

es un isomorfismo. En efecto, si $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ están alineados en la curva, pasan por la recta $Z = lX + b$ y por lo tanto x_1, x_2, x_3 son las raíces de

$$lX + b = X^3$$

entonces, $x_1+x_2+x_3 = 0$. Además, si $\mathbf{x} = \left[\frac{x}{y} : 1 : \frac{1}{y}\right]$, $-\mathbf{x} = \left[\frac{-x}{y} : 1 : \frac{-1}{y}\right]$, entonces $\mathbf{x} \to \frac{x}{y}$ es morfismo, y resulta suryectivo pues se deduce de la ecuación de la curva reducida que

$$\frac{1}{x} = \left(\frac{x}{y}\right)^2$$

(dado un valor en $\mathbb{F}_p$ no nulo debemos tomar x tal que su inverso sea igual a ese valor elevado al cuadrado, por otro lado si el valor es cero, debemos tomar $x = 0$). De esta cuenta también sale que es inyectiva ya que la igualdad de imágenes implica la igualdad de los x y de ahí sale el y por una cuestión de signos.

(4) Si $\mathbf{x} \in \bigcap F^n(\mathbb{Q}_p)$, entonces $x = 0$, $y \neq 0$ (por $\mathbf{x} \in F^1(\mathbb{Q}_p)$). Por lo tanto, o bien $z = 0$, o bien $y^2 = Bz^2$ pero como z tendría que ser divisible por p e y no (para que $[x : y : z]$ reduzca a $\mathbf{o}$ módulo p), se llega a una contradicción, $\Rightarrow z = 0$ y listo.$\diamond$

Para $\mathbf{x} \in F^1(\mathbb{Q}_p)$, definimos

$$u(\mathbf{x}) = \begin{cases} \frac{x}{y} & \text{si } \mathbf{x} = (x, y) \neq \mathbf{o} \\ 0 & \text{si } \mathbf{x} = \mathbf{o} \end{cases}$$

Notemos que $|u(\mathbf{x})|_p = p^{-n}$ si $\mathbf{x}$ tiene nivel n.

Lema 39 *Sean $\mathbf{x}_1, \mathbf{x}_2 \in F^1(\mathbb{Q}_p)$, entonces*

$$|u(\mathbf{x}_1 + \mathbf{x}_2) - u(\mathbf{x}_1) - u(\mathbf{x}_2)|_p \leq \text{máx}\left\{|u(\mathbf{x}_1)|_p^5, |u(\mathbf{x}_2)|_p^5\right\}$$

Demostración: Podemos suponer que ninguno de $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_1 + \mathbf{x}_2$ es $\mathbf{o}$ porque esos casos son triviales. Sin pérdida de generalidad,

$$|u(\mathbf{x}_1)|_p \geq |u(\mathbf{x}_2)|_p$$

Sea n el nivel de $\mathbf{x}_1$. Vamos a trabajar con la curva $\mathcal{C}_0$ definida antes donde a $\mathbf{x} = [p^n x_1 : y_1 : p^{3n} z_1]$, lo mandamos al $\mathbf{x}_0 = [x_1 : y_1 : z_1]$. Como ninguno de los puntos $\mathbf{x}_1, \mathbf{x}_2$ va a parar al punto singular $(0, 0)$ de $\mathcal{C}_0$, entonces la recta que une $\mathbf{x}_{10}, \mathbf{x}_{20}$ es de la forma

$$Z = lX + mY$$

con $|l|_p, |m|_p \leq 1$. Escribimos que $\mathbf{x}_1, \mathbf{x}_2$ están en la recta:

$$p^{-3n} Z = lp^{-n} X + mY$$

o sea,

$$Z = lp^{2n} X + mp^{3n} Y$$

Esta intersecta a $\mathcal{C}$ en

$$\begin{aligned} 0 &= -Y^2(lp^{2n}X + mp^{3n}Y) + X^3 + AX(lp^{2n}X + mp^{3n}Y)^2 + B(lp^{2n}X + mp^{3n}Y)^3 \\ &= c_3 X^3 + c_2 X^2 Y + c_1 X Y^2 + c_0 Y^3 \end{aligned}$$

Con

$$\begin{aligned} c_3 &= 1 + Al^2 p^{4n} + Bl^3 p^{6n} \\ c_2 &= 2Almp^{5n} + 3Bl^2 mp^{7n} \end{aligned}$$

Entonces,

$$|c_3|_p = 1 \qquad |c_2|_p \leq p^{-5n}$$

Las raíces $\frac{X}{Y}$ de la ecuación cúbica anterior son $-u(\mathbf{x}_1 + \mathbf{x}_2), u(\mathbf{x}_1)$ y $u(\mathbf{x}_2)$. Como su suma es $\frac{-c_2}{c_3}$, se sigue el resultado. $\diamond$

Corolario 40

$$|u(s\mathbf{x})|_p = |s|_p |u(\mathbf{x})|_p$$

para todo $\mathbf{x} \in F^1(\mathbb{Q}_p)$ *y todo* $s \in \mathbb{Z}$.

Demostración: Por inducción, para $s > 0$ tenemos,

$$|u(s\mathbf{x}) - su(\mathbf{x})|_p \leq |u(\mathbf{x})|_p^5$$

Si la igualdad no fuera cierta, el miembro de la izquierda es igual a máx $\{|u(s\mathbf{x})|_p, |su(\mathbf{x})|_p\}$. Entonces sale que

$$|s|_p|u(\mathbf{x})|_p \leq |u(\mathbf{x})|_p^5.$$

Como $|u(\mathbf{x})|_p < 1$, esto es absurdo a menos que $p|s$ y en ese caso con $s = p$ también es absurdo. Luego $|u(s\mathbf{x})|_p = |su(\mathbf{x})|_p$ para $p \not| s$ y para $s = p$. Entonces se aplica inducción para conseguirlo para las potencias de p, y luego inducción en k para conseguirlo para el caso $s = kp^l$ con $p \not| k$. Para los negativos es claro porque $|\cdot|_p$ no se influye por el cambio de signos. $\diamond$

Corolario 41 *$F^1(\mathbb{Q}_p)$ es libre de torsión.*

Demostración: En efecto, si $\mathbf{x} \in F^1(\mathbb{Q}_p)$ es de orden k, vale

$$0 = |u(\mathbf{o})|_p = |u(k\mathbf{x})|_p = |k|_p|u(\mathbf{x})|_p$$

Luego $u(\mathbf{x}) = 0 \Rightarrow x = 0$ pero como $\mathbf{x} \in F^1(\mathbb{Q}_p)$, entonces z tendría que ser 0 y eso implica que $\mathbf{x} = \mathbf{o}$. $\diamond$

Corolario 42 *Supongamos que $p \neq 2$, $|4A^3 + 27B^2|_p = 1$. Entonces el subgrupo de torsión de $F(\mathbb{Q}_p)$ es isomorfo a un subgrupo de $F(\mathbb{F}_p)$.*

Demostración: Como $F(\mathbb{Q}_p) = F^0(\mathbb{Q}_p)$,

$$F(\mathbb{F}_p) = F(\mathbb{Q}_p)/F^1(\mathbb{Q}_p)$$

donde $F^1(\mathbb{Q}_p)$ es libre de torsión. $\diamond$

7.3. Torsión Global

Teorema 43 *(Lutz–Nagell) Sea*

$$Y^2Z - (X^3 + AXZ^2 + BZ^3) = F(X, Y, Z)$$

una curva elíptica no singular y T su grupo de torsión. Si $\mathbf{x} = [x : y : 1] \in T$ entonces $x, y \in \mathbb{Z}$ y además, o bien $y = 0$, o bien $y^2|\Delta = 4A^3 + 27B^2$.

Demostración: Sea (x, y) de torsión. Como $F(\mathbb{Q}) \subset F(\mathbb{Q}_p)$, tenemos que

$$x, y \in \mathbb{Z}_p \qquad \forall p$$

entonces

$$x, y \in \mathbb{Z}.$$

Sea ahora p primo distinto de 2, $p \not| \Delta$. Por el Corolario anterior o por el Teorema de Mordell, el grupo de torsión de $F(\mathbb{Q})$ es finito. Variando los p podríamos restringir considerablemente el orden. Pero lo que hacemos es buscar los puntos de torsión directamente. Si $2(x, y) = \mathbf{o}$, entonces $y = 0$. Si no $2(x, y) = (x_1, y_1)$ también es de torsión y tiene sus coordenadas enteras. Como

$$x_1 + 2x = \left(\frac{3x^2 + A}{2y}\right)^2 = \frac{(3x^2 + A)^2}{4(x^3 + Ax + B)}$$

y entonces $y^2 = x^3 + Ax + B$ divide a $(3x^2 + A)^2$.

Pero, pensando en la resultante de F,

$$(3X^2 + 4A)(3X^2 + A)^2 \equiv 4A^3 + 27B^2_{mod\, X^3+AX+B}$$

y por lo tanto,

$$y^2 | (4A^3 + 27B^2)$$

como queríamos. $\diamond$

Debemos agregar que hay resultados más fuertes sobre el grupo de torsión de un curva elíptica. Por ejemplo, Mazur determinó que todas las posibilidades para el grupo de torsión son:

$$\mathbb{Z}/n\mathbb{Z} \qquad 1 \leq n \leq 10 \quad o \quad n = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq n \leq 4$$

y todas ellas aparecen.

8. Una Cota para el Rango

Sea $\mathcal{C}$ una curva elíptica con un punto de orden 2 racional, o sea de la forma

$$Y^2 = X(X^2 + aX + b)$$

Podemos suponer que $a, b \in \mathbb{Z}$. Entonces si las otras raíces son α y β, el discriminante es

$$\Delta = (\alpha - \beta)^2 \alpha^2 \beta^2 = (a^2 - 4b)b^2$$

Sea T_1 el conjunto de los primos que dividen a $a^2 - 4b$ o a b pero no a ambos y sea T_2 el conjunto de los primos que dividen a ambos números. Entonces T_1 son los primos para los cuales dos de las raíces de

$$X(X - \alpha)(X - \beta)$$

coinciden en la reducción ya que si $p|b$, entonces cero es raíz de $X^2 + aX + b$, y si $p|(a^2 - 4b)$, este polinomio tiene una raíz doble. T_2 son los primos para los cuales las tres raíces coinciden, pues $p|b$ y también $p|a^2$, con lo cual los coeficientes son cero en la reducción.

Asi, lo que queda es que T_1 son los primos para los cuales la reducción tiene una singularidad de nodo y T_2 para los cuales tiene una cúspide.

Sean t_1 y t_2 la cantidad de elementos de T_1 y T_2.

Proposición 44 *Si $\alpha, \beta \in \mathbb{Q}$, el rango r de la curva anterior satisface*

$$r \leq t_1 + 2t_2 - 1$$

Demostración: Recordando el método para calcular $F(\mathbb{Q})/2F(\mathbb{Q})$, lo que tenemos es que $G(\mathbb{Q})/\phi F(\mathbb{Q})$ es isomorfo a un subgrupo de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ que lo podemos describir como subgrupo de

$$\mathbb{Z}/2\mathbb{Z} \oplus \sum_{p|b_1} \mathbb{Z}/2\mathbb{Z}$$

El primer sumando corresponde al signo $\pm$. Lo mismo sucede con $F(\mathbb{Q})/\psi G(\mathbb{Q})$, pero cambiando b_1 por b. Entonces nos queda que $F(\mathbb{Q})/2F(\mathbb{Q})$ es isomorfo a un subgrupo de

$$\mathbb{Z}/2\mathbb{Z} \oplus \sum_{p|b_1} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \sum_{p|b} \mathbb{Z}/2\mathbb{Z}$$

Y esto lo podemos escribir mejor como

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \sum_{p \in T_1} \mathbb{Z}/2\mathbb{Z} \oplus \sum_{p \in T_2} (\mathbb{Z}/2\mathbb{Z})^2$$

Vamos a probar que en realidad hace falta poner un solo sumando para el tema del signo. Para eso tenemos que ver que -1 no aparece en el grupo isomorfo a $G(\mathbb{Q})/\phi F(\mathbb{Q})$ o en el isomorfo a $F(\mathbb{Q})/\psi G(\mathbb{Q})$.

En el caso en que $\alpha < 0$, $q = -1$ aparece en el grupo isomorfo a $G(\mathbb{Q})/\phi F(\mathbb{Q})$ si la ecuación

$$-l^4 + a_1 l^2 m^2 - b_1 m^4 = n^2$$

tiene una solución entera no trivial. Tomando en cuenta que α, β son las raíces de $X^2 + aX + b$, y como $a_1 = -2a$, $b_1 = a^2 - 4b$, entonces

$$a_1 = 2(\alpha + \beta) \qquad b_1 = (\alpha - \beta)^2$$

Luego nos queda,

$$\begin{aligned} -l^4 + 2(\alpha+\beta)l^2m^2 - (\alpha-\beta)^2 m^4 &= n^2 \\ -(l^2 + (\alpha-\beta)m^2)^2 + 4\alpha l^2 m^2 &= n^2 \end{aligned}$$

y se llega a un absurdo porque el término de la izquierda es menor o igual a cero (y es cero solo en el caso trivial).

Si $\beta < 0$ también se puede hacer lo mismo. Si $\alpha, \beta \geq 0$, miramos el $q = -1$ del grupo isomorfo a $F(\mathbb{Q})/\psi G(\mathbb{Q})$. Hay que ver la ecuación

$$-l^4 + al^2 m^2 - bm^4 = n^2$$

Como $a = -(\alpha + \beta) \leq 0$ y $b = \alpha\beta \geq 0$, todos los términos de la izquierda son menores o iguales a cero y entonces no puede haber solución no trivial.

Con todo esto, podemos decir que $F(\mathbb{Q})/2F(\mathbb{Q})$ es isomorfo a un subgrupo de

$$\mathbb{Z}/2\mathbb{Z} \oplus \sum_{p \in T_1} \mathbb{Z}/2\mathbb{Z} \oplus \sum_{p \in T_2} (\mathbb{Z}/2\mathbb{Z})^2$$

Entonces el orden de $F(\mathbb{Q})/2F(\mathbb{Q})$ está acotado por 2 elevado a la potencia $t_1 + 2t_2 + 1$. Cada copia de $\mathbb{Z}$ de la parte libre aporta una copia de $\mathbb{Z}/2\mathbb{Z}$ en $F(\mathbb{Q})/2F(\mathbb{Q})$.

Por otro lado el grupo de torsión de $F(\mathbb{Q})$ contiene una copia de $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. En efecto, consideramos $T \overset{\times 2}{\mapsto} T$. Como T es finito, el kernel y el cokernel tienen la misma dimensión y entonces

$$T/2T \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Luego hay al menos dos copias de $\mathbb{Z}/2\mathbb{Z}$ que las aporta el subgrupo de torsión y entonces el rango está acotado por

$$r \leq t_1 + 2t_2 - 1$$

$\diamond$

9. Números Congruentes

Como aplicación a lo que vimos hasta ahora, vamos a volver a los números congruentes. Primero probemos lo que había quedado pendiente:

Proposición 45 *Sea n un entero libre de cuadrados, y supongamos que existe un punto racional (x, y) en la curva*

$$Y^2 = X^3 - n^2 X$$

que no es $(-n, 0)$, $(0, 0)$, $(n, 0)$ ni $\mathbf{o}$. Entonces existen tres cuadrados racionales en progresión aritmética con diferencia n. Con lo cual n es congruente.

Demostración: Sea $\mathbf{x} = (x, y)$ la solución no trivial. Como $y \neq 0$, entonces $\mathbf{x}$ no tiene orden 1 ni 2. Luego $2\mathbf{x} \neq \mathbf{o}$. Escribimos $2\mathbf{x} = (x_1, y_1)$. Sea $Y = mX + b$ la recta tangente en $\mathbf{x}$, que intersecta a la curva nuevamente en $-2\mathbf{x} = (x_1, -y_1)$. Entonces $\mathbf{x}$ y $-2\mathbf{x}$ satisfacen:

$$(mX + b)^2 = X(X - n)(X + n)$$

De hecho, x, x y x_1 son las tres raíces del polinomio anterior. Podemos escribir

$$X(X - n)(X + n) - (mX + b)^2 = (X - x)^2(X - x_1)$$

Poniendo $X = 0$,

$$-b^2 = x^2(-x_1)$$

y sale que x_1 es un cuadrado pues $x \neq 0$. Con $X = -n$,

$$-(-mn + b)^2 = (n - x)^2(n - x_1)$$

y sale que $x_1 - n$ es un cuadrado. Análogamente, $x_1 + n$ es un cuadrado. $\diamond$

Corolario 46 *(Fermat) $n = 2$ no es un número congruente.*

Demostración: Si 2 fuera congruente, el (1) $\Rightarrow$ (3) de la Proposición 1 diría que

$$Y^2 = X^3 - 4X$$

tiene una solución no trivial. Transformando con

$$\begin{cases} X' &= \frac{Y}{2X} \\ Y' &= \frac{Y^2+8X}{4X^2} \end{cases}$$

(ver la parte de descenso de Fermat), se obtiene una ecuación de la forma

$$X'^4 + 1 = Y'^2$$

que sabemos que no tiene solución por lo visto mediante el descenso de Fermat. $\diamond$

Lema 47 *Si n es libre de cuadrados, entonces la curva elíptica*

$$Y^2 = X^3 - n^2X$$

tiene el subgrupo de torsión isomorfo a

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Demostración: Consideremos la curva reducida a $\mathbb{F}_p$. Si $p \not| \Delta$, $p \geq 7$ y $p \equiv 3_{mod\,4}$ entonces la curva tiene $p+1$ puntos en $\mathbb{F}_p$.

En efecto, si $x \neq 0$, consideramos el par x, $-x$. Si $x^3 - n^2x$ es cero, cada uno de los dos da lugar a una solución. Si no es cero, como -1 no es cuadrado módulo p, uno solo entre $x^3 - n^2x$ y $-(x^3 - n^2x)$ es un cuadrado y da dos soluciones. Luego los x no nulos dan $p-1$ soluciones. A esto hay que agregarle $(0,0)$ y $\mathbf{o}$ y se obtienen $p+1$ soluciones.

Vimos que para primos suficientemente grandes el grupo de torsión T de $F(\mathbb{Q})$ es isomorfo a un subgrupo de $F(\mathbb{F}_p)$. Luego $|T|$ divide a $p+1$ para p grandes con $p \equiv 3_{mod\,4}$.

Vamos a usar el Teorema de Dirichlet que dice que hay infinitos primos de la forma $ak+b$ con a, b enteros fijos tal que $(a;b) = 1$ y k varía entre los enteros positivos.

Veamos que 8 no divide a $|T|$. Por el Teorema de Dirichlet podemos elegir un primo como dijimos antes que además cumpla que $p \equiv 3_{mod\,8}$. Si 8 divide a $|T|$ entonces $8|p+1$, pero $p \equiv 3_{mod\,8}$ implica que $p+1 \equiv 4_{mod\,8}$ absurdo.

Veamos que 3 no divide a $|T|$. Por el Teorema de Dirichlet podemos elegir un primo como dijimos antes que además cumpla que $p \equiv 7_{mod\,12}$. Luego $p \equiv 3_{mod\,4}$. Si 3 divide a $|T|$ entonces $3|p+1$, pero $p+1 \equiv 8_{mod\,12}$ implica que $p+1 \equiv 8_{mod\,3}$ absurdo.

Veamos que ningún primo impar q mayor que 3 divide a $|T|$. Por el Teorema de Dirichlet podemos elegir un primo como dijimos antes que además cumpla que $p \equiv 3_{mod\,4q}$. Luego $p \equiv 3_{mod\,4}$. Si q divide a $|T|$ entonces $q|p+1$, pero $p+1 \equiv 4_{mod\,4q}$ implica que $p+1 \equiv 4_{mod\,q}$ absurdo.

Por lo tanto $|T|$ divide a 4. Sabemos que hay tres puntos de orden 2 que son $(-n,0)$, $(0,0)$, y $(n,0)$. Entonces T tiene que ser necesariamente del tipo $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. $\diamond$

Proposición 48 *Un entero n libre de cuadrados es no congruente si y solo si la curva elíptica*

$$Y^2 = X^3 - n^2X$$

tiene rango cero.

Demostración: Si la curva tiene rango cero, $F(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Por (1) $\Rightarrow$ (3) de la Proposición 1, n es no congruente. Por otro lado, si n es no congruente, no puede tener otros puntos racionales aparte de los cuatro triviales y entonces el rango es cero.$\diamond$

Corolario 49 *(Fermat) $n = 1$ no es un número congruente.*

Demostración: La curva elíptica $Y^2 = X^3 - X$ es de la forma de las curvas de la sección anterior con $a = 0, b = -1, b_1 = 4$ y raíces reales. Aplicando la cota del rango que obtuvimos en la sección anterior, el único primo a considerar es $p = 2$ que es del tipo T_1, luego $r = 0$ y $n = 1$ es no congruente.$\diamond$

Recordemos:

Teorema 50 *(Ley de reciprocidad cuadrática) Para p, q primos impares*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Y además

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Ahora podemos pasar a la siguiente

Proposición 51 *Sea p un primo impar. Consideramos la curva*

$$Y^2 = X^3 - p^2X$$

Entonces el rango r satisface:

$$\begin{array}{ll} r \leq 2 & si\ p \equiv 1_{mod\,8} \\ r = 0 & si\ p \equiv 3_{mod\,8} \\ r \leq 1 & si\ p \equiv 5\ o\ 7_{mod\,8} \end{array}$$

En consecuencia cualquier $p \equiv 3_{mod\,8}$ es un número no congruente.

Demostración: Hacemos el descenso con la curva

$$\mathcal{C} : Y^2Z - X(X^2 - p^2Z^2) = F(X, Y, Z)$$

Pasando por la curva

$$\mathcal{D} : Y^2Z - X(X^2 + 4p^2Z^2) = G(X, Y, Z)$$

Para calcular $G(\mathbb{Q})/\phi F(\mathbb{Q})$: Buscamos los $q|4p^2$ que sean libres de cuadrados. Sabemos que 1 le corresponde al $(0, 0)$ (y también al $\mathbf{o}$). Hay que ver que pasa con $q = \pm 1, \pm 2, \pm p, \pm 2p$.

El caso $q = -1$ da la ecuación $-l^4 - 4p^2m^4 = n^2$ que claramente no tiene soluciones no triviales. Lo mismo sucede con todos los casos de $q < 0$.

El caso $q = 2$ da la ecuación:

$$2l^4 + 2p^2m^4 = n^2$$

Mirando módulo p, $2l^4 \equiv n^2_{mod\,p}$. Entonces para que tenga solución es necesario que 2 sea un cuadrado módulo p, o sea que

$$p \equiv 1 \text{ o } -1_{mod\,8}.$$

Entonces en ese caso obtenemos a lo sumo un punto que llamaremos $\mathbf{x}_1$.

El caso $q = p$ da la ecuación:

$$pl^4 + 4pm^4 = n^2$$

Entonces $p|n$ y escribimos $n = pn'$. Nos queda $l^4 + 4m^4 = pn'^2$. Mirando módulo p, $l^4 \equiv -4m^4_{mod\, p}$. Para que tenga solución es necesario que -4 sea una potencia cuarta módulo p. En principio como 4 es un cuadrado siempre, entonces -1 debería ser un cuadrado. Con lo cual es necesario que $p \equiv 1_{mod\, 4}$. Escribimos $-1 = \delta^2$ en $\mathbb{F}_p$.

Hay dos posibilidades. Si 2 es un cuadrado módulo p, es el caso cuando $p \equiv 1$ o $-1_{mod\, 8}$ (este último no sirve porque dijimos que $p \equiv 1_{mod\, 4}$), entonces necesitamos que δ sea un cuadrado. Sea x un generador del grupo multiplicativo de $\mathbb{F}_p$ (que es cíclico). Consideramos

$$x^{\frac{p-1}{8}}$$

es un elemento de orden 8, luego si se lo eleva a la cuarta da -1 y entonces en el caso $p \equiv 1_{mod\, 8}$ tanto 4 como -1 son potencias cuartas y puede llegar a haber una solución.

Si 2 no es un cuadrado módulo p, es el caso cuando $p \equiv 3$ o $5_{mod\, 8}$, a nosotros solo nos sirve el segundo que es el que es coherente con $p \equiv 1_{mod\, 4}$. Necesitamos que δ no sea un cuadrado módulo p (para que 2δ si lo sea). Supongamos que $\delta = \epsilon^2$ en $\mathbb{F}_p$. Entonces $\epsilon^4 = -1$. Por otro lado, por $p \equiv 5_{mod\, 8}$, $\frac{p-1}{4}$ es impar. Haciendo

$$(\epsilon^4)^{\frac{p-1}{4}} = (-1)^{\frac{p-1}{4}}$$

lo cual es absurdo porque se obtiene $1 = -1$.

Entonces en el caso $q = p$ se obtiene a lo sumo un punto $\mathbf{x}_2$ si

$$p \equiv 1_{mod\, 4}$$

El caso $q = 2p$ da la ecuación:

$$2pl^4 + 2pm^4 = n^2$$

Se deduce que $2p|n$ y escribimos $n = 2pn'$. Nos queda $l^4 + m^4 = 2pn'^2$. Mirando módulo p, $l^4 \equiv -m^4_{mod\, p}$. Entonces -1 es cuadrado módulo p y esto sucede cuando $p \equiv 1_{mod\, 4}$ que está dentro de los casos considerados antes.

Para calcular $F(\mathbb{Q})/\psi G(\mathbb{Q})$: Buscamos los $q|-p^2$ que sean libre de cuadrados. Sabemos que -1 le corresponde al $(0, 0)$ y como solo buscamos generadores, solo tenemos que mirar además que pasa con $q = p$. Obtenemos la ecuación:

$$pl^4 - pm^4 = n^2$$

Esta ecuación tiene solución $(l, m, n) = (1, 1, 0)$ y entonces

$$u = q\frac{l^2}{m^2} = p \qquad (u, v) = (p, 0)$$

.

Entonces obtenemos

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle \psi(\mathbf{x}_1), \psi(\mathbf{x}_2), (0, 0), (p, 0) \rangle$$

Recordando que $\mathbf{x}_1$ y $\mathbf{x}_2$ aparecen a lo sumo cuando $p \equiv 1$ o $-1_{mod\,8}$ y $p \equiv 1_{mod\,4}$ respectivamente. Como los puntos $(0, 0)$ y $(p, 0)$ son generadores del grupo de torsión, se obtiene lo que se quería considerando caso por caso las congruencias módulo 8. $\diamond$

10. El Grupo de Tate–Shafarevich

10.1. Cohomología de Galois

Sea Γ un grupo finito que actúa sobre un grupo abeliano A. Si $\sigma \in \Gamma$, un **cociclo** es una función $\Gamma \mapsto A$

$$\sigma \mapsto a_\sigma$$

que satisface la **identidad de los cociclos**:

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau$$

donde $\sigma, \tau \in \Gamma$. Notemos que de aca se deduce que $a_1 = 0$

Si $b \in A$ es fácil ver que:

$$a_\sigma = \sigma b - b$$

es un cociclo. Los cociclos de este tipo se llaman **cobordes**.

Los cociclos forman un grupo con la adición punto a punto.

$$\{a_\sigma\} + \{b_\sigma\} = \{a_\sigma + b_\sigma\}$$

Los cobordes son un subgrupo. El grupo cociente es

$$H^1(\Gamma, A),$$

el **primer grupo de cohomología**.

A su vez, $\tau \in \Gamma$ actúa sobre el cociclo:

$$\{a_\sigma\} : \sigma \mapsto a_\sigma$$

de la siguiente manera:

$$\tau\{a_\sigma\} : \tau\sigma\tau^{-1} \mapsto \tau a_\sigma = a_{\tau\sigma} - a_\tau$$

escribiendo σ en lugar de $\tau\sigma\tau^{-1}$:

$$\tau\{a_\sigma\} : \sigma \mapsto a_{\sigma\tau} - a_\tau$$

es un cociclo y en realidad,

$$\tau\{a_\sigma\} - \{a_\sigma\} : \sigma \mapsto a_{\sigma\tau} - a_\tau - a_\sigma = \sigma a_\tau - a_\tau$$

es un coborde. Entonces

Lema 52 *Γ actúa trivialmente en $H^1(\Gamma, A)$.*

Lema 53 *Cada elemento de $H^1(\Gamma, A)$ es de orden finito dividiendo a $|\Gamma|$.*

Demostración: Sea $\{a_\sigma\} \in H^1(\Gamma, A)$. Entonces, por lo que vimos, también queda representado por el cociclo

$$\tau\{a_\sigma\} = \{a_{\sigma\tau} - a_\tau\}$$

Pero entonces

$$\sum_\tau \tau\{a_\sigma\} = \sum_\tau \{a_{\sigma\tau}\} - \{a_\tau\} = \{0\}$$

recordando que $\{a_1\} = \{0\}$ $\diamond$

Lema 54 *Sea $m \in \mathbf{Z}, m > 1$. Sea $\Delta_m \subset A$ el conjunto de los elementos de orden dividiendo a m. Supongamos que todo elemento de A es divisible por m en A.*

Entonces todo elemento de $H^1(\Gamma, A)$ de orden m se puede representar como un cociclo $\{d_\sigma\}$ con $d_\sigma \in \Delta_m$.

Demostración: Sea $\{a_\sigma\} \in H^1(\Gamma, A)$. Por hipótesis, $m\{a_\sigma\}$ es un coborde, o sea

$$ma_\sigma = \sigma b - b$$

con $b \in A$. Con las hipótesis, $b = mc$, $c \in A$ entonces,

$$ma_\sigma = m\sigma c - mc$$

o sea,

$$m(a_\sigma - \sigma c + c) = 0$$

Entonces el elemento $\{a_\sigma\} \in H^1(\Gamma, A)$ es representado por

$$\sigma \mapsto a_\sigma - \sigma c + c \in \Delta_m$$

como se quería.$\diamond$

Notemos con A^Γ al conjunto de elementos de a que quedan fijos por la acción de Γ.

Proposición 55 *Con la notación y las hipótesis de antes,*

$$A^\Gamma / mA^\Gamma$$

es canónicamente isomorfo a un subgrupo de $H^1(\Gamma, \Delta_m)$

Demostración: Sea $a \in A^\Gamma$. Por hipótesis,

$$a = mb$$

con $b \in A$. Aplicando $\sigma \in \Gamma$,

$$a = \sigma a = m\sigma b$$

y entonces,

$$md_\sigma = 0, \qquad d_\sigma = \sigma b - b$$

Entonces$\{d_\sigma\}$ es un cociclo con valores en Δ_m.

Para a dado, cualquier otra elección de b es de la forma $b + c$ con $c \in \Delta_m$. Luego, el elemento de $H^1(\Gamma, \Delta_m)$ dado por $\{d_\sigma\}$ queda unívocamente determinado por a.

Si $a \in mA^\Gamma$, podemos tomar $b \in A^\Gamma$ y entonces $d_\sigma = 0$ para todo σ y la imagen en $H^1(\Gamma, \Delta_m)$ es 0.

Ahora supongamos que el cociclo construido mas arriba es un coborde,

$$d_\sigma = \sigma c - c$$

$\forall \sigma \in \Gamma$, $c \in \Delta_m$, entonces

$$\sigma(b - c) = b - c$$

$\Rightarrow$

$$b - c \in A^\Gamma, \qquad m(b - c) = a.$$

$\diamond$

Juntando lo anterior,

Teorema 56 *Supongamos que $m > 1$ es un entero y que todo elemento de A es divisible por m. Entonces la sucesión:*

$$0 \mapsto A^\Gamma / mA^\Gamma \mapsto H^1(\Gamma, \Delta_m) \mapsto [H^1(\Gamma, A)]_m \mapsto 0$$

es exacta, donde $[...]_m$ denota el grupo de elementos de orden dividiendo m, y el tercer morfismo está inducido por $\Delta_m \hookrightarrow A$

Demostración: Por los Lemas anteriores, solo tenemos que probar la exactitud en $H^1(\Gamma, \Delta_m)$, o sea que la imagen de

$$A^\Gamma / mA^\Gamma \mapsto H^1(\Gamma, \Delta_m)$$

es exactamente el kernel de

$$H^1(\Gamma, \Delta_m) \mapsto [H^1(\Gamma, A)]_m$$

Sea $\{d_\sigma\}$ un elemento de la imagen. Por hipótesis, $d_\sigma = \sigma b - b$, $b \in A$ y entonces si consideramos a $\{d_\sigma\}$ tomando valores en A, resulta un coborde. Luego imagen $\subset$ kernel.

Sea $\{d_\sigma\}$ un elemento del kernel, o sea un coborde de A: $d_\sigma = \sigma b - b$ para cierto $b \in A$. Entonces,

$$\sigma(mb) - mb = md_\sigma = 0, \qquad (\forall \sigma)$$

$\Rightarrow mb \in A^\Gamma$. Entonces kernel $\subset$ imagen. $\diamond$

Sea k un cuerpo y sea $\overline{k}$ su clausura separable (que es igual a la clausura algebraica en característica 0). Sea

$$\Gamma = \text{Gal } (\overline{k}/k)$$

Diremos que una acción $a \mapsto \sigma a$ ($\sigma \in \Gamma, a \in A$) de Γ en el grupo abeliano A es **continua** si:

Para todo $a \in A$ existe una extensión κ de k de grado finito $[\kappa : k] < \infty$ (dependiendo de a) tal que:

$$\sigma a = a \qquad \forall \sigma \in \text{Gal } (\overline{k}/\kappa) \subset \text{Gal } (\overline{k}/k)$$

Por ejemplo, $k = \mathbb{Q}$, $\mathcal{C}$ la curva $Y^2Z - (X^3 + AXZ + BZ^2) = F(X, Y, Z)$ definida sobre $\mathbb{Q}$, y $A = F(\mathbb{Q})$.

Un **cociclo continuo** es una función

$$\sigma \mapsto a_\sigma$$

con $\sigma \in \Gamma, a_\sigma \in A$ para la cual

(1) se satisface la identidad del cociclo:

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau, \qquad (\sigma, \tau \in \Gamma)$$

(2) es continua en el sentido que existe una extensión normal κ/k de grado $[\kappa : k] < \infty$ tal que a_σ depende solo de la acción de σ en κ (κ depende de $\{a_\sigma\}$).

En particular,

$$a_\tau = 0 \qquad \forall \tau \in \text{Gal } (\overline{k}/\kappa)$$

o sea,

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau = a_\sigma - 0 \qquad \forall \tau \in \text{Gal } (\overline{k}/\kappa)$$

y entonces

$$a_\sigma \in \kappa \qquad \forall \sigma \in \text{Gal } (\overline{k}/k)$$

Si $\{a_\sigma\}, \{b_\sigma\}$ son cociclos continuos, entonces claramente $\{a_\sigma + b_\sigma\}$ es continuo.

Un coborde $\{\sigma c - c\}, c \in A$ es continuo por nuestra hipótesis que Γ actúa continuamente sobre A.

$H^1(\Gamma, A)$ *es el grupo de los cociclos continuos módulo los cobordes.*

Como en el caso Γ finito, tenemos

Teorema 57 *$H^1(\Gamma, A)$ es de torsión*

Teorema 58 *Sea $m > 1$ un entero y supongamos que todo elemento de A es divisible por m. Entonces la sucesión*

$$0 \mapsto A^\Gamma/mA^\Gamma \mapsto H^1(\Gamma, \Delta_m) \mapsto [H^1(\Gamma, A)]_m \mapsto 0$$

es exacta donde (como antes):

(1) *A^Γ es el conjunto de los $a \in A$ fijos por la acción de Γ.*

(2) *Δ_m es el conjunto de los elementos de A de orden dividiendo m.*

(3) *$[H^1(\Gamma, A)]_m$ es el conjunto de los elementos de $H^1(\Gamma, A)$ de orden dividiendo m.*

10.2. Jacobiana

Sean:

$$\mathcal{C}_j : Y^2Z = X^3 + A_jXZ^2 + B_jZ^3 \qquad (j = 1, 2)$$

y sea

$$\phi : \mathcal{C}_1 \longmapsto \mathcal{C}_2$$

una correspondencia birracional. Si consideramos $\phi(\mathbf{x}) - \phi(\mathbf{o}_1)$ en lugar de $\phi(\mathbf{x})$, podemos suponer que

$$\phi(\mathbf{o}_1) = \mathbf{o}_2$$

La correspondencia debe mandar funciones con polos de orden dos en $\mathbf{o}_1$ en funciones con polo de orden dos en $\mathbf{o}_2$, por lo tanto

$$\phi(X) = aX + b$$

para algunos a, b fijos. Similarmente,

$$\phi(Y) = cY + dX + e$$

Mirando la forma de la ecuación para $\mathcal{C}_2$, sale que $d = e = 0$, $b = 0$, $a^3 = c^2$, y por lo tanto podemos escribir:

$$a = s^2, \qquad c = s^3$$

Para algún s. Entonces

$$A_2 = s^4A_1, \qquad B_2 = s^6B_1 \tag{6}$$

En particular, $\frac{A_1^3}{B_1^2} = \frac{A_2^3}{B_2^2}$ es invariante por correspondencias birracionales.

En general se trabaja con el invariante:

$$j = j(\mathcal{C}) = \frac{1728(4A^3)}{4A^3 + 27B^2}$$

de la curva:

$$\mathcal{C} : Y^2Z = X^3 + AXZ^2 + BZ^3$$

La notación es standard y el 1728 viene de un factor que aparece cuando se quiere calcular el discriminante de la curva cuando está en forma general de Weierstrass.

Con estas observaciones queda clara la siguiente

Proposición 59 *Dos curvas elípticas en forma canónica que son birracionalmente equivalentes se relacionan por la fórmula* (6) *para algún* s. *En particular tienen el mismo* j.

Corolario 60 *Cualquier equivalencia birracional de la curva*

$$\mathcal{C} : Y^2Z = X^3 + AXZ^2 + BZ^3$$

que mande $\mathbf{o}$ *en* $\mathbf{o}$ *es de la forma:*

$$Y \to s^3Y, \qquad X \to s^2X$$

Si $AB \neq 0$ *entonces* $s^2 = 1$. *Si* $B = 0$, $s^4 = 1$ *y si* $A = 0$, $s^6 = 1$.

Demostración: Es claro de la fórmula (6) con $\mathcal{C} = \mathcal{C}_1 = \mathcal{C}_2$.$\diamond$

Sea $\mathcal{D}$ una curva de género 1 definida sobre $\mathbb{Q}$. En general no tiene por que tener un punto racional y si lo tiene, no siempre es fácil encontrarlo. Pero si es fácil encontrar un punto definido sobre la clausura algebraica de los racionales. Entonces existe una correspondencia birracional:

$$\phi : \mathcal{D} \longmapsto \mathcal{C}$$

definida sobre $\overline{\mathbb{Q}}$, donde $\mathcal{C}$ está en forma canónica pero definida sobre $\overline{\mathbb{Q}}$.

Sea $\sigma \in \text{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$, puede actuar sobre la correspondencia birracional para dar:

$$\sigma\phi : \mathcal{D} \longmapsto \sigma\mathcal{C}$$

donde

$$\sigma\mathcal{C} : Y^2Z = X^3 + \sigma AXZ^2 + \sigma BZ^3$$

Entonces $\mathcal{C}$ y $\sigma\mathcal{C}$ son birracionalmente equivalentes sobre $\overline{\mathbb{Q}}$ por $(\sigma\phi)\phi^{-1}$. Por lo tanto,

$$\sigma j(\mathcal{C}) = j(\sigma\mathcal{C}) = j(\mathcal{C})$$

O sea $j(\mathcal{C}) \in \mathbb{Q}$ o equivalentemente $\frac{A^3}{B^2} \in \mathbb{Q}$. Luego, por medio de una transformación $X \to t^2X, \quad Y \to t^3Y \quad (t \in \overline{\mathbb{Q}})$ podemos suponer sin pérdida de generalidad que $\mathcal{C}$ está definida sobre $\mathbb{Q}$. En general ϕ está definida sólo sobre $\overline{\mathbb{Q}}$. Ahora,

$$\theta_\sigma = (\sigma\phi)\phi^{-1}$$

es un automorfismo de $\mathcal{C}$.

$\tau \in$ Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ puede actuar sobre θ_σ dando:

$$\tau\theta_\sigma = (\tau\sigma\phi)(\tau\phi)^{-1} = [(\tau\sigma\phi)\phi^{-1}][\phi(\tau\phi)^{-1}] = \theta_{\tau\sigma}\theta_\tau^{-1}$$

Entonces

$$\theta_{\tau\sigma} = (\tau\theta_\sigma)\theta_\tau$$

Con lo que satisfacen la identidad de los cociclos.

Supongamos primero que $AB \neq 0$. Por la Proposición y el Corolario anteriores, el automorfismo θ_σ de $\mathcal{C}$ debe ser

$$\theta_\sigma : \mathbf{x} \to \epsilon_\sigma\mathbf{x} + a_\sigma$$

Para algún punto a_σ definido sobre $\mathbb{Q}$ y $\epsilon_\sigma = \pm 1$

Por la identidad de los cociclos y por ser $\epsilon_\sigma \in \mathbb{Q}$ se debe cumplir,

$$\epsilon_{\tau\sigma} = \epsilon_\sigma\epsilon_\tau$$

Queremos asegurar que $\epsilon_\sigma = 1 \ \forall\sigma$. Si no, $\exists d \in \mathbb{Q}$ tal que

$$\sigma(\sqrt{d}) = \epsilon_\sigma\sqrt{d}, \qquad \forall\sigma$$

La transformación:

$$\psi : X \to dX, \qquad Y \to d\sqrt{d}Y$$

nos da una nueva $\mathcal{C}'$ definida sobre $\mathbb{Q}$:

$$\mathcal{C}' : Y^2Z = X^3 + \frac{A}{d^2}XZ^2 + \frac{B}{d^3}Z^3$$

Ahora, si ponemos:

$$\phi' = \psi\phi$$

Tenemos,

$$\theta'_\sigma = (\sigma\phi')\phi'^{-1} = (\sigma\psi\phi)\phi^{-1}\psi^{-1} = (\sigma\psi)\theta_\sigma\psi^{-1}$$

y esta función claramente es de la forma $\mathbf{x} \to \mathbf{x} + \mathbf{a}_\sigma$ en $\mathcal{C}'$.

Si $AB = 0$ se puede llegar a la misma conclusión. Pero es mas complicado. Para eso demostremos primero el Teorema:

Teorema 61 *(Hilbert 90) Sea κ/k una extensión finita y de Galois. Para $\sigma \in Gal\,(\kappa/k)$ sea $\theta_\sigma \in k^*$ dado que satisface la identidad de los cociclos:*

$$\theta_{\tau\sigma} = (\tau\theta_\sigma)\theta_\tau$$

Entonces $\{\theta_\sigma\}$ es un coborde, o sea

$$\theta_\sigma = (\sigma\gamma)\gamma^{-1}$$

$\forall\sigma$ para algún $\gamma \in \kappa^*$.

Demostración: Como la extensión es separable y finita, es simple y podemos escribir

$$\kappa = k(\beta).$$

Como $1, \beta, ..., \beta^{n-1}$ es una base de κ sobre k, son linealmente independientes. A medida que τ varía en el grupo de Galois, $\tau\beta$ recorre sus conjugados, que son las potencias de β. Entonces

$$\mu = \sum_\tau \theta_\tau(\tau\beta) \neq 0$$

$$\sigma\mu = \sum_\tau \sigma\theta_\tau(\sigma\tau\lambda) = \sum_\tau \theta_{\sigma\tau}\theta_\sigma^{-1}(\sigma\tau\lambda) = \theta_\sigma^{-1}\sum_\tau \theta_{\sigma\tau}(\sigma\tau\lambda) = \theta_\sigma^{-1}\sum_\tau \theta_\tau(\tau\lambda) = \theta_\sigma^{-1}\mu$$

Si ahora hacemos

$$\gamma = \mu^{-1},$$

nos queda

$$\sigma\mu = \theta_\sigma^{-1}\mu \quad \Rightarrow \quad \sigma\mu^{-1} = \theta_\sigma\mu^{-1} \quad \Rightarrow \quad \sigma\gamma = \theta_\sigma\gamma$$

y entonces,

$$(\sigma\gamma)\gamma^{-1} = \theta_\sigma$$

$\diamond$

Supongamos que $B = 0$, entonces $\epsilon_\sigma^4 = 1$. Definimos

$$\mathbf{x} \to \epsilon\mathbf{x}$$

como

$$X \to \epsilon^2 X, \qquad Y \to \epsilon^3 Y$$

Entonces Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ actúa sobre ϵ y

$$\epsilon_{\tau\sigma} = (\tau\epsilon_\sigma)\epsilon_\tau$$

Por Hilbert 90 existe $\delta \in \overline{\mathbb{Q}}$ tal que

$$\sigma\delta = \epsilon_\sigma\delta$$

Elevando a la cuarta,

$$\sigma\delta^4 = \delta^4$$

Para todo σ, entonces $\delta^4 \in \mathbb{Q}$. Entonces podemos cambiar $\mathcal{C}$ como antes para que $\epsilon_\sigma = 1$ en la nueva $\mathcal{C}'$:

$$\psi : X \to \delta^4 X, \qquad Y \to \delta^6 Y$$

$$\mathcal{C}' : Y^2 Z = X^3 + \frac{A}{\delta^8} X Z^2 + \frac{B}{\delta^{12}} Z^3$$

Como antes, ponemos,

$$\phi' = \psi\phi$$

y es la misma cuenta que en el caso anterior.

Similarmente para $A = 0$, en este caso, $\epsilon_\sigma^6 = 1$, definimos como antes,

$$\mathbf{x} \to \epsilon\mathbf{x}$$

como

$$X \to \epsilon^2 X, \qquad Y \to \epsilon^3 Y$$

como antes, $\epsilon_{\tau\sigma} = (\tau\epsilon_\sigma)\epsilon_\tau$, y por Hilbert 90 obtenemos un $\delta \in \overline{\mathbb{Q}}$ tal que $\sigma\delta = \epsilon_\sigma\delta$. Pero ahora, al elevar a la sexta se obtiene

$$\sigma\delta^6 = \delta^6$$

entonces $\delta^6 \in \mathbb{Q}$.

Como antes cambiamos a $\mathcal{C}'$:

$$\psi : X \to \delta^6 X, \qquad Y \to \delta^9 Y$$

$$\mathcal{C}' : Y^2 Z = X^3 + \frac{A}{\delta^{12}} X Z^2 + \frac{B}{\delta^{18}} Z^3$$

y es como los casos anteriores.

En definitiva probamos:

Teorema 62 *Sea $\mathcal{D}$ una curva de género 1 definida sobre $\mathbb{Q}$. Existe una curva elíptica $\mathcal{C}$ definida sobre $\mathbb{Q}$ y una equivalencia birracional*

$$\phi : \mathcal{D} \longmapsto \mathcal{C}$$

definida sobre $\overline{\mathbb{Q}}$ tal que para todo $\sigma \in Gal\ (\overline{\mathbb{Q}}/\mathbb{Q})$ la función

$$\theta_\sigma = (\sigma\phi)\phi^{-1} : \mathcal{C} \longmapsto \mathcal{C}$$

es de la forma

$$\theta_\sigma : \mathbf{x} \to \mathbf{x} + a_\sigma$$

Para algún $a_\sigma \in F(\overline{\mathbb{Q}})$.

Mas aún, $\mathcal{C}$ es única salvo equivalencia birracional sobre $\mathbb{Q}$.

La curva elíptica $\mathcal{C}$ se llama la **jacobiana** de $\mathcal{D}$.

10.3. Espacios Principales Homogéneos

Consideremos la siguiente situación:

Sean $\mathcal{A}$ y $\mathcal{B}$ dos curvas definidas sobre $\mathbb{Q}$ y sea

$$\phi : \mathcal{A} \longmapsto \mathcal{B}$$

una equivalencia birracional definida sobre $\overline{\mathbb{Q}}$. Sea $\sigma \in$ Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$. Como antes consideramos:

$$\theta_\sigma = (\sigma\phi)\phi^{-1} : \mathcal{B} \longmapsto \mathcal{B}$$

Por las mismas cuentas que antes, θ_σ verifica la identidad de los cociclos:

$$\theta_{\tau\sigma} = (\tau\theta_\sigma)\theta_\tau$$

Si tenemos otra equivalencia birracional definida sobre $\overline{\mathbb{Q}}$

$$\phi' : \mathcal{A} \longmapsto \mathcal{B}$$

y se cumple:

$$\phi' = \omega\phi$$

para algún automorfismo

$$\omega : \mathcal{B} \longmapsto \mathcal{B}$$

Entonces,

$$\theta'_\sigma = (\sigma\phi')(\phi'^{-1}) = \sigma\omega\theta_\sigma\omega^{-1}$$

.

Si ϕ está definida sobre $\mathbb{Q}$,

$$\theta'_\sigma = (\sigma\omega)\omega^{-1}$$

y resulta ser un coborde. Es el caso en que $\mathcal{A}$ y $\mathcal{B}$ son birracionalmente equivalentes sobre $\mathbb{Q}$ pero hicimos las cuentas con una equivalencia diferente.

Por otro lado, dados $\mathcal{B}$ y los cociclos $\{\theta_\sigma\}$ podemos reconstruir $\mathcal{A}$ salvo una equivalencia birracional sobre $\mathbb{Q}$.

Para ver como, supongamos que tenemos $\mathcal{A}$ y que (x, y) y $(\tilde{x}, \tilde{y})$ son puntos genéricos de $\mathcal{B}$ y $\mathcal{A}$ respectivamente. Por el momento supongamos que tenemos las curvas definidas sobre un cuerpo k (perfecto, por ejemplo de característica 0 o finito, para usar teoría de Galois).

Si tenemos una función racional

$$\psi : \mathcal{A} \longmapsto \mathcal{B}$$

definida sobre k es lo mismo que tener la inyección:

$$k(\tilde{x}, \tilde{y}) \to k(x, y)$$

$$(\tilde{x}, \tilde{y}) \to \psi((\tilde{x}, \tilde{y}))$$

En particular, ser equivalentes birracionalmente sobre k es lo mismo que tener un isomorfismo:

$$k(x, y) \cong k(\tilde{x}, \tilde{y})$$

Sea K una extensión finita de k con base $\mathcal{S} = \{v_1, v_2, ..., v_n\}$, entonces, $\mathcal{S}$ es también base de $K(\tilde{x}, \tilde{y})/k(\tilde{x}, \tilde{y})$ si $(\tilde{x}, \tilde{y})$ es un punto genérico sobre k. Si

además la extensión es de Galois, cada $\sigma \in \text{Gal } (K/k)$ define en forma única un $\tilde{\sigma} \in \text{Gal } (K(\tilde{x},\tilde{y})/k(\tilde{x},\tilde{y}))$ tal que:

$$\tilde{\sigma}\alpha = \sigma\alpha, \qquad \alpha \in K$$

$$\tilde{\sigma}\tilde{x} = \tilde{x} \qquad \tilde{\sigma}\tilde{y} = \tilde{y}$$

Los $\tilde{\sigma}$ forman un grupo $\tilde{\Gamma}$ isomorfo al grupo $\Gamma = \text{Gal } (K/k)$ y que tiene a $k(\tilde{x},\tilde{y})$ como cuerpo fijo.

En nuestro contexto, supongamos que $\mathcal{A}$ y $\mathcal{B}$ son birracionalmente equivalentes sobre K por medio de la funcion ψ. En ese caso $K(\tilde{x},\tilde{y})$ y $K(x,y)$ son isomorfos, pero el isomorfismo no es necesariamente la extensión de un isomorfismo entre $k(\tilde{x},\tilde{y})$ y $k(x,y)$ (pues eso implicaría equivalencia sobre k). Vamos a tratar el isomorfismo entre $K(\tilde{x},\tilde{y})$ y $K(x,y)$ como una identificación, escribimos:

$$K(\tilde{x},\tilde{y}) = K(x,y)$$

Ahora consideramos los morfismos $\tilde{\sigma}$ de antes y nos preguntamos por el valor $\tilde{\sigma}(x,y)$.

$$\tilde{\sigma}(x,y) = \tilde{\sigma}(\psi((\tilde{x},\tilde{y}))) = (\tilde{\sigma}\psi)(\tilde{\sigma}(\tilde{x},\tilde{y})) = (\sigma\psi)(\tilde{x},\tilde{y}) = (\sigma\psi)\psi^{-1}((x,y)) = \theta_\sigma((x,y))$$

Donde los cociclos se definen como antes. Entonces, si ahora pensamos en $K(x,y)$, que lo conocemos pues tenemos como dato la curva $\mathcal{B}$ y los cociclos, y consideramos la acción $\tilde{\sigma}$:

$$\tilde{\sigma}\alpha = \sigma\alpha, \qquad \alpha \in K$$

$$\tilde{\sigma}(x,y) = \theta_\sigma(x,y)$$

De vuelta, el grupo $\tilde{\Gamma}$ es isomorfo a Γ. Consideramos el cuerpo fijo por este grupo, y lo llamamos $\tilde{k}$.

Como (x,y) es trascendente sobre K, entonces

$$[K:k] = [K(x,y):k(x,y)] = |\Gamma|$$

Pero $|\Gamma| = |\tilde{\Gamma}|$, $\Rightarrow$

$$[K:k] = [K(x,y):\tilde{k}]$$

Claramente, $k \subset \tilde{k}$ pues k queda fijo por la acción de Γ y por lo tanto también por la de $\tilde{\Gamma}$. Como el grupo $\tilde{\Gamma}$ es finito, $\tilde{k}$ tiene grado de trascendencia 1 sobre k. Además $\tilde{k}$ no puede tener elementos de K. Sea $w_1 \in \tilde{k}$ un elemento

que no está en k. Entonces es trascendente sobre k, pues si no lo fuera, al estar en $K(x,y)$ y no ser trascendente, tendría que ser elemento de K pero entonces al quedar fijo por Γ tendría que estar en k, absurdo. Luego, no puede ser algebraico. Entonces $k(w_1) \subseteq \tilde{k}$. La extensión $K(x,y)/k(w_1)$ es finita pues ambos cuerpos tienen grado de trascendencia 1 sobre k y la extensión K/k es finita, además el cuerpo $\tilde{k}$ está "en el medio",

$$k(w_1) \subseteq \tilde{k} \subset K(x,y).$$

Entonces $\tilde{k}/k(w_1)$ es finita y podemos escribir:

$$\tilde{k} = k(w_1, w_2, ..., w_m)$$

Ahora bien,

$$K(w_1, ..., w_m) \subseteq K(x,y)$$

Además

$$[K(w_1, ..., w_m) : k(w_1, ..., w_m)] = [K : k]$$

pues como antes, $(w_1, ..., w_m)$ es trascendente sobre K.

Entonces

$$[K(w_1, ..., w_m) : k(w_1, ..., w_m)] = [K(x,y) : k(w_1, ..., w_m)]$$

y por la inclusión $K(w_1, ..., w_m) \subseteq K(x,y)$, obtenemos que

$$K(w_1, ..., w_m) = K(x,y)$$

Pero entonces la curva correspondiente al cuerpo de funciones $K(w_1, ..., w_m)$ es birracionalmente equivalente a $\mathcal{B}$ sobre K.

Falta ver que está definida sobre k. Si $f(W_1, ..., W_m)$ es un polinomio con coeficientes en K tal que

$$f(w_1, ..., w_m) = 0$$

Entonces, aplicando $\tilde{\sigma}$:

$$\tilde{\sigma}(f(w_1, ..., w_m)) = 0$$

Pero $\tilde{\sigma} w_i = w_i$ por construcción de los w_i, luego

$$(\sigma f)(w_1, ..., w_m) = 0$$

donde el morfismo está actuando sobre los coeficientes del polinomio. Si

$$f(W_1, ..., W_m) = \sum_{j=1}^{n} v_j g_j(W_1, ...W_m)$$

donde los g_j son polinomios con coeficientes en k. Entonces sale que

$$g_j(w_1, ..., w_m) = 0$$

por lo tanto los $(w_1, ..., w_m)$ están definidos por ecuaciones con coeficientes en k y eso implica que la curva está definida sobre k.

Ahora nos gustaría adaptar lo anterior al caso de $k = \mathbb{Q}$ y $K = \overline{\mathbb{Q}}$. El problema es que acá la extensión no es finita. Mas general, queremos el caso con $K = \overline{k}$. Pero si nuestros cociclos son continuos, no tendremos problemas, porque dado el cociclo θ_σ solo necesitamos un extensión finita de k para definir la acción $\tilde{\sigma}$ y entonces podemos aplicar todo lo anterior.

Sea $\mathcal{D}$ una curva de género 1 definida sobre $\mathbb{Q}$. Vimos que existe una curva elíptica $\mathcal{C} : Y^2Z = X^3 + AXZ^2 + BZ^3$ definida sobre $\mathbb{Q}$ y que se llama jacobiana y cumple una serie de cosas, entre otras que existe un morfismo

$$\theta_\sigma : \mathcal{C} \longmapsto \mathcal{C}$$

$$\theta_\sigma : \mathbf{x} \to \mathbf{x} + a_\sigma$$

Volviendo a la notación de antes, los a_σ satisfacen la identidad de los cociclos:

$$\tau a_\sigma = a_{\tau\sigma} - a_\tau$$

Como los a_σ están en el grupo conmutativo $F(\overline{\mathbb{Q}})$ y podemos utilizar toda la Teoría de Cohomología de Galois.

Reemplazando la funcion ϕ por $\phi\psi$ donde

$$\psi : \mathcal{C} \mapsto \mathcal{C}, \qquad \mathbf{x} \to \mathbf{x} + \mathbf{b}, \qquad \mathbf{b} \in F(\overline{\mathbb{Q}})$$

Se reemplaza a_σ por

$$a_\sigma + (\sigma\mathbf{b} - \mathbf{b})$$

Entonces $\{a_\sigma\}$ determina un elemento de

$$H^1(\Gamma, F(\overline{\mathbb{Q}}))$$

donde $\Gamma = \text{Gal}\ (\overline{\mathbb{Q}}/\mathbb{Q})$.

Ahora veamos que información nos da cada elemento de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$ acerca de $\mathcal{D}$.

En primer lugar, podemos reconstruir $\mathcal{D}$ y la equivalencia birracional a partir de a_σ. Sea (x, y) un punto genérico de $\mathcal{C}$. Existe una acción $\tilde{\sigma}$ de Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ en $\overline{\mathbb{Q}}(x, y)$ dada por

(1) $\tilde{\sigma}$ actúa como σ en $\overline{\mathbb{Q}}$.

(2) $\tilde{\sigma}(x, y) = \theta_\sigma(x, y) = (x, y) + a_\sigma$.

Entonces por la discusión anterior, el cuerpo fijo es el cuerpo de funciones de una curva $\mathcal{D}$ definida sobre $\mathbb{Q}$ y ϕ, definida sobre $\overline{\mathbb{Q}}$, está dada por la identificación de los dos cuerpos de funciones sobre $\overline{\mathbb{Q}}$.

Lema 63 *La función ϕ le otorga a $\mathcal{D}$ la estructura de espacio principal homogéneo sobre $\mathcal{C}$, o sea, existe un morfismo*

$$\mu : \mathcal{D} \times \mathcal{C} \longmapsto \mathcal{D}$$

definida sobre $\mathbb{Q}$ tal que

(1) $\mu(\mathbf{y}, \mathbf{o}) = \mathbf{y}$

(2) $\mu(\mu(\mathbf{y}, \mathbf{x}_1), \mathbf{x}_2) = \mu(\mathbf{y}, \mathbf{x}_1 + \mathbf{x}_2)$

(3) *Para todos los $\mathbf{y}_1, \mathbf{y}_2 \in \mathcal{D}$, existe un único $\mathbf{x} \in \mathcal{C}$ tal que $\mu(\mathbf{y}_1, \mathbf{x}) = \mathbf{y}_2$*

Además su inversa

$$\nu : \mathcal{D} \times \mathcal{D} \longmapsto \mathcal{C}$$

definida tal que

$$\mu(\mathbf{y}_1, \mathbf{x}) = \mathbf{y}_2$$

es equivalente a

$$\nu(\mathbf{y}_2, \mathbf{y}_1) = \mathbf{x}$$

resulta definida sobre $\mathbb{Q}$.

Demostración: En efecto, si $\mathbf{y}_1, \mathbf{y}_2$ puntos genéricos independientes de $\mathcal{D}$, que los tomamos como fijos bajo la acción de Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$. Definimos:

$$\nu(\mathbf{y}_2, \mathbf{y}_1) = \phi(\mathbf{y}_2) - \phi(\mathbf{y}_1)$$

Entonces,

$$\sigma\nu(\mathbf{y}_2, \mathbf{y}_1) = (\phi(\mathbf{y}_2) + a_\sigma) - (\phi(\mathbf{y}_1) + a_\sigma) = \nu(\mathbf{y}_2, \mathbf{y}_1)$$

O sea que ν está definida sobre $\mathbb{Q}$. Asimismo,

$$\mu(\mathbf{y}, \mathbf{x}) = \phi^{-1}(\mathbf{x} + \phi(\mathbf{y}))$$

Verifica todas las condiciones. $\diamond$

Llamaremos al par $(\mathcal{D}, \nu)$ **espacio principal homogéneo** de $\mathcal{C}$ definido sobre $\mathbb{Q}$.

Diremos que dos espacios homogéneos $(\mathcal{D}_1, \nu_1), (\mathcal{D}_2, \nu_2)$, definidos sobre $\mathbb{Q}$ son de la misma clase si existe una equivalencia birracional

$$\lambda : \mathcal{D}_1 \longmapsto \mathcal{D}_2$$

definida sobre $\mathbb{Q}$ tal que el diagrama:

$$\begin{array}{ccccc} \mathcal{D}_1 & \times & \mathcal{C} & \stackrel{\mu_1}{\rightarrow} & \mathcal{D}_1 \\ \downarrow \lambda & & & & \downarrow \lambda \\ \mathcal{D}_2 & \times & \mathcal{C} & \stackrel{\mu_2}{\rightarrow} & \mathcal{D}_2 \end{array}$$

es conmutativo.

La clase trivial de espacios principales homogéneos es la que incluye al $(\mathcal{C}, -)$ donde "–" es la resta usual de la curva.

El cociclo $\{a_\sigma\}$ o el correspondiente elemento de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$ determinan el par $(\mathcal{D}, \nu)$. El cociclo $\{-a_\sigma\}$ determina el par $(\mathcal{D}, -\nu)$. Entonces para obtener una estructura de grupo tenemos que considerar no solo las curvas $\mathcal{D}$ con jacobiana dada, sino los pares $(\mathcal{D}, \nu)$. Pero cada elemento de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$ determina $\mathcal{D}$ salvo una equivalencia racional definida sobre $\mathbb{Q}$. Podría suceder que $(\mathcal{D}, \nu)$ y $(\mathcal{D}, -\nu)$ fueran de la misma clase. Por ejemplo cuando $\mathcal{C}$ es su propia jacobiana. Consideremos:

$$\phi_j : (\mathcal{D} =)\mathcal{C} \longmapsto \mathcal{C}, \qquad (j = 1, 2)$$

donde $\phi_1(\mathbf{x}) = \mathbf{x}$ y $\phi_2(\mathbf{x}) = -\mathbf{x}$. En ambos casos el cociclo a_σ es cero pero

$$\nu_1(\mathbf{x}_2, \mathbf{x}_1) = \mathbf{x}_2 - \mathbf{x}_1$$

$$\nu_2(\mathbf{x}_2, \mathbf{x}_1) = \mathbf{x}_1 - \mathbf{x}_2$$

Para no tener estos problemas, trabajamos con las clases de espacios principales homogéneos. Y cada elemento de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$ nos determina una clase.

Por otro lado, cada espacio principal homogéneo nos determina un elemento de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$. Consideremos la función

$$\phi : \mathcal{D} \longmapsto \mathcal{C}$$

Por la construcción de siempre, el cociclo es

$$a_\sigma = (\sigma\phi)(\xi) - \phi(\xi)$$

donde ξ es un punto genérico de $\mathcal{D}$ fijo por Galois. Sea ahora α un punto de $\mathcal{D}$ definido sobre $\overline{\mathbb{Q}}$ entonces,

$$\sigma(\phi(\alpha)) = (\sigma\phi)(\sigma\alpha) = \phi(\sigma\alpha) + a_\sigma$$

Luego,

$$\nu(\alpha, \sigma\alpha) = \phi(\alpha) - \phi(\sigma\alpha) = \phi(\alpha) - \sigma(\phi(\alpha)) + a_\sigma$$

Por lo tanto $\{\nu(\alpha, \sigma\alpha)\}_\sigma$ es un cociclo y difiere de $\{a_\sigma\}_\sigma$ por un coborde. En definitiva:

Teorema 64 *Existe un isomorfismo canónico entre los espacios principales homogéneos $(\mathcal{D}, \nu)$ (salvo equivalencia birracional en $\mathbb{Q}$) y los elementos de $H^1(\Gamma, F(\overline{\mathbb{Q}}))$. El elemento correspondiente a $(\mathcal{D}, \nu)$ está dado por el cociclo $\{\nu(\alpha, \sigma\alpha)\}_\sigma$, donde α es un punto algebraico de $\mathcal{D}$.*

Mas en general si $(\mathcal{D}, \nu)$ es un espacio principal homogéneo sobre $\mathcal{C}$, podemos definir una función:

$$Jac : \mathrm{Div}^0(\mathcal{D}) \longmapsto \mathcal{C}$$

de la forma

$$\sum_{\mathbf{x}} n_{\mathbf{x}}\mathbf{x} \to \sum_{\mathbf{x}} n_{\mathbf{x}}\nu(\mathbf{x}, \mathbf{b})$$

donde $\mathbf{b}$ es un punto fijo de $\mathcal{D}$. La primera suma es la suma formal de los divisores pero la segunda se hace en $\mathcal{C}$.

La función no depende del $\mathbf{b}$ que se elija pues

$$\nu(\mathbf{y}_1, \mathbf{y}_2) = \nu(\mathbf{y}_1, \mathbf{y}_3) + \nu(\mathbf{y}_3, \mathbf{y}_2)$$

De hecho, con la notación de la ϕ, podemos escribir:

$$\sum_{\mathbf{x}} n_{\mathbf{x}}\nu(\mathbf{x}, \mathbf{b}) = \sum_{\mathbf{x}} n_{\mathbf{x}}(\phi(\mathbf{x}) - \phi(\mathbf{b})) = \sum_{\mathbf{x}} n_{\mathbf{x}}\phi(\mathbf{x}) - \phi(\mathbf{b}) \sum_{\mathbf{x}} n_{\mathbf{x}} = \sum_{\mathbf{x}} n_{\mathbf{x}}\phi(\mathbf{x})$$

pues no debemos olvidarnos que partimos de un divisor de grado 0.

Un divisor $\mathbf{D} = \sum_{\mathbf{x}} n_{\mathbf{x}}\mathbf{x}$ está en el kernel de Jac precisamente cuando los $\phi(\mathbf{x})$ con sus multiplicidades son los ceros y polos de una función en $\mathcal{C}$. Identificando $\mathcal{D}$ y $\mathcal{C}$ via ϕ, esto es lo mismo que decir que $\mathbf{D}$ es divisor principal de $\mathcal{D}$.

Si $\mathbf{D}$ está definido sobre $\overline{k}$

$$\sigma Jac(\mathbf{D}) = \sum_{\mathbf{x}} \sigma n_{\mathbf{x}} \sigma(\phi(\mathbf{x})) = \sum_{\mathbf{x}} \sigma n_{\mathbf{x}} (\phi(\sigma\mathbf{x}) + a_\sigma) = \sum_{\mathbf{x}} \sigma n_{\mathbf{x}} \phi(\sigma\mathbf{x}) = Jac(\sigma\mathbf{D})$$

En particular, si $\mathbf{D}$ está definido sobre $\mathbb{Q}$, también lo está $Jac(\mathbf{D})$. Entonces tenemos un monomorfismo de grupos:

$$\mathrm{Div}^0(\mathcal{D})/\mathrm{Princ}\ (\mathcal{D}) \longmapsto \mathcal{C}$$

donde los divisores de grado cero están definidos sobre $\mathbb{Q}$. Además, si $\mathbf{x} \in \mathcal{C}$ resulta ser la imagen de la clase del divisor:

$$\mathbf{D} = \phi^{-1}(\mathbf{x}) - \mathbf{o}$$

luego el morfismo es un isomorfismo.

Ahora bien, si un divisor $\mathbf{D}$ de grado 0 está definido sobre $\mathbb{Q}$ y es principal, entonces es el divisor de una función en $\mathcal{D}$ definida sobre $\mathbb{Q}$. Para eso supongamos que f es una función con divisor $\mathbf{D}$ definida sobre $\overline{\mathbb{Q}}$. Sea $\sigma \in \mathrm{Gal}\ (\overline{\mathbb{Q}}/\mathbb{Q})$. Luego $\mathbf{D}$ es también el divisor de σf y entonces,

$$\frac{\sigma f}{f} \in \overline{\mathbb{Q}}^*$$

Se verifica que $\theta_\sigma = \frac{\sigma f}{f}$ es un cociclo con valores en $\overline{\mathbb{Q}}^*$. En efecto,

$$\theta_{\tau\sigma} = \frac{\tau\sigma f}{f} = \left(\tau \frac{\sigma f}{f}\right) \frac{\tau f}{f} = (\tau\theta_\sigma)\theta_\tau$$

Entonces por Hilbert 90 es un coborde y cumple

$$\frac{\sigma f}{f} = \frac{\sigma\lambda}{\lambda}$$

para algún $\lambda \in \overline{\mathbb{Q}}^*$ y $\forall\sigma$. Entonces

$$\lambda^{-1} f$$

queda fijo por la acción del grupo de Galois y por lo tanto está definida sobre $\mathbb{Q}$ y tiene divisor $\mathbf{D}$ que es lo que queríamos probar.

Todas estas observaciones tienen por objeto mostrar que la curva $\mathcal{C}$ que construímos a partir de $\mathcal{D}$ es de hecho la jacobiana de la curva según la definición usual mas general, que dice que la jacobiana de una curva de género $g \geq 1$ es una variedad de dimensión g que resulta tener una estructura de grupo isomorfa a

$$\mathrm{Div}^0(\mathcal{D})/\mathrm{Princ}\ (\mathcal{D})$$

El caso de las curvas de género 1, resulta particular porque la variedad Jacobiana resulta ser una curva por tener dimensión 1. Para las curvas elípticas (con un punto en el cuerpo base), podemos considerar el isomorfismo:

$$\mathcal{D} \longmapsto Jac(\mathcal{D})$$

$$\mathbf{x} \longmapsto \mathbf{x} - \mathbf{o}$$

Y esto es coherente con el hecho que las curvas elípticas sean las que tienen una estructura de grupo.

10.4. El Grupo de Tate–Shafarevich

Como antes, tenemos una curva

$$\mathcal{C} : Y^2Z - (X^3 + AXZ^2 + BZ^3) = F(X, Y, Z)$$

Lo que vimos es que el primer grupo de cohomologías es canónicamente isomorfo al grupo de clases de equivalencia de $(\mathcal{D}, \nu)$, donde $\mathcal{D}$ es una curva de género 1 y ν es su estructura de espacio principal homogéneo. A este grupo se lo llama el grupo de Weil-Châtelet y se denota con $WC = WC(\mathcal{C})$.

Sea $m > 1$ un entero. El grupo $F(\overline{\mathbb{Q}})$ es divisible por m pues para encontrar un $\mathbf{b}$ que satisfaga $m\mathbf{b} = \mathbf{a} \in F(\overline{\mathbb{Q}})$ solo hay que resolver algunas ecuaciones. Aplicando la Teoría de Cohomología vista antes obtenemos la sucesión exacta:

$$0 \mapsto F(\mathbb{Q})/mF(\mathbb{Q}) \mapsto H^1(\Gamma, \Delta_m) \mapsto [H^1(\Gamma, F(\overline{\mathbb{Q}}))]_m \mapsto 0$$

Donde $\Gamma = \mathrm{Gal}\ (\overline{\mathbb{Q}}/\mathbb{Q})$, $\Delta_m \subset F(\overline{\mathbb{Q}})$ es el subgrupo de los elementos de orden m y $[...]_m$ denota el subgrupo de elementos de orden dividiendo m.

Ahora estamos en una situación similar a la que llegamos con el descenso en la demostración del Teorema de Mordell– Weil. Queremos encontrar los

elementos de $H^1(\Gamma, \Delta_m)$ que son imágenes de $F(\mathbb{Q})/mF(\mathbb{Q})$. Por la exactitud de la sucesión, estos son precisamente el kernel de la función

$$H^1(\Gamma, \Delta_m) \mapsto H^1(\Gamma, F(\overline{\mathbb{Q}})) = WC(\mathcal{C})$$

Estar en el kernel significa que la imagen es trivial como espacio principal homogéneo.

Lema 65 *Una condición necesaria y suficiente para que un espacio principal homogéneo $(\mathcal{D}, \nu)$ esté en la clase trivial es que haya un punto de $\mathcal{D}$ definido sobre $\mathbb{Q}$.*

Demostración: La necesidad es obvia. Supongamos que $\mathbf{b} \in \mathcal{D}$ definido sobre $\mathbb{Q}$. Entonces

$$\lambda : \mathbf{x} \to \mu(\mathbf{b}, \mathbf{x})$$

es una transformación bilineal de $\mathcal{C}$ en $\mathcal{D}$ que funciona bien.$\diamond$

Para $m = 2$ estamos de vuelta en la situación de la demostración del Teorema de la Base Finita Débil. Como habíamos remarcado, no hay un algoritmo que decida si hay o no un punto racional en la curva $\mathcal{D}$. Sin embargo, no hay dificultad en decidir si hay un punto en $\mathcal{D}$ en todos lados localmente. Como veremos, los elementos de WC para los cuales hay un punto en $\mathcal{D}$ en todos lados localmente, forman un subgrupo. Se conoce como el grupo de Tate–Shafarevich y se nota con la letra rusa Ш.

Para probar que Ш es un subgrupo, veamos un poco de localización. Para cualquier primo p (incluyendo ∞), el subíndice p denota el objeto definido sobre $\mathbb{Q}_p$ (recordemos que $\mathbb{Q}_\infty = \mathbb{R}$). Consideremos una inmersión fija:

$$\lambda : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$$

Sean $\Gamma = \text{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$ y $\Gamma_p = \text{Gal}\,(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Entonces λ induce un morfismo,

$$\tilde{\lambda} : \Gamma_p \hookrightarrow \Gamma$$

Si A es un Γ-módulo continuo, entonces es un Γ_p-módulo continuo via $\tilde{\lambda}$.

Sea $\{a_\sigma\}$, $\sigma \in \Gamma$ un cociclo continuo. Restringiendo a los $\sigma \in \Gamma_p$, queda un Γ_p-cociclo continuo. Entonces tenemos el siguiente homomorfismo de grupos:

$$\lambda I : H^1(\Gamma, A) \longmapsto H^1(\Gamma_p, A)$$

En principio λI depende de la inmersión λ, pero veamos que no. Cualquier inmersión $\Lambda : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ es de la forma

$$\Lambda = \lambda\mu$$

con μ un automorfismo de $\overline{\mathbb{Q}}/\mathbb{Q}$. Luego μ actúa trivialemente sobre $H^1(\Gamma, A)$, y entonces $\Lambda I = \lambda I$. Por lo tanto la función:

$$H^1(\Gamma, A) \longmapsto H^1(\Gamma_p, A)$$

es canónica.

Hay una función:

$$j_p : WC \longmapsto WC_p$$

que manda la clase de equivalencia de los espacios principales homogéneos $(\mathcal{D}, \nu)$ definidos sobre $\mathbb{Q}$, en la misma clase definida sobre $\mathbb{Q}_p$.

Desde el punto de vista cohomológico, tenemos una función:

$$j_p : H^1(\Gamma, F(\mathbb{Q})) \longmapsto H^1(\Gamma_p, F(\mathbb{Q}_p))$$

inducida por la inclusión $F(\mathbb{Q}) \subset F(\mathbb{Q}_p)$. Como dijimos, j_p no depende de la inclusión $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Claramente Ш es la intersección de los kernels de todas las funciones de localización j_p (incluyendo $p = \infty$). Para m dado, sea S_m el grupo de los elementos de $H^1(\Gamma, \Delta_m)$ cuya imagen está en $Ш \subset H^1(\Gamma, F(\mathbb{Q}))$. Se llama el m-grupo de Selmer. Entonces tenemos la sucesión exacta:

$$0 \to F(\mathbb{Q})/mF(\mathbb{Q}) \to S_m \to [Ш]_m \to 0$$

En el caso de $m = 2$, nos encontramos en la prueba del Teorema Débil de la Base Finita, en donde probamos que S_2 es finito y construible. Se puede probar lo mismo para S_m con m general.

Redondeando, el grupo de Selmer es calculable, mayoriza a $F(\mathbb{Q})/mF(\mathbb{Q})$ y el error está dado por Ш, que lo podemos considerar como la obstrucción del principio local-global para curvas de género 1 con jacobiana dada $\mathcal{C}$.

11. Curvas con LLI no trivial

Mas adelante veremos una familia de curvas cuyo Ш es no trivial. Para construirla tenemos que buscar curvas donde falle el principio local-global.

Proposición 66 *Si p primo, $p \equiv 1_{mod\,8}$ y 2 no es cuarta potencia módulo p, entonces la curva*

$$Y^2 = 2 - 2pX^4$$

no tiene puntos racionales, aunque tiene soluciones sobre $\mathbb{Q}_p$ para todo p y sobre $\mathbb{R}$.

Demostración: Supongamos que (x, y) es un punto racional de

$$Y^2 = 2 - 2pX^4$$

Sea $x = \frac{r}{t}$, $y = \frac{m}{n}$ con $(r; t) = (m; n) = 1$. Entonces

$$m^2t^4 = n^2(2t^4 - 2pr^4)$$

Si $2|(t^4; 2t^4 - 2pr^4)$, sea 2^k la máxima potencia de 2 que divide a t, y como $(r; t) = 1$, $2 \not| p$ se tiene que la máxima potencia de 2 que aporta $2t^4 - 2pr^4$ es 2. Con lo cual $2^{4k-1}|n^2$. Entonces $2^{2k}|n \Rightarrow 2|m^2$, lo cual es absurdo porque $(m; n) = 1$.

Si $p|(t^4; 2t^4 - 2pr^4)$, se hace el mismo razonamiento. Claramente no puede haber otros factores en común pues $(r; t) = 1$. Entonces

$$(t^4; 2t^4 - 2pr^4) = 1.$$

Como

$$y^2 = \frac{2t^4 - 2pr^4}{t^4}$$

sale que $y = \frac{2s}{t^2}$ para algún entero s. Obtenemos

$$2s^2 = t^4 - pr^4$$

Sea q un primo impar que divide a s. Entonces $t^4 \equiv pr^4_{mod\,q}$ y luego $\left(\frac{p}{q}\right) = 1$. Por la ley de reciprocidad cuadrática, tomando en cuenta que $p \equiv 1_{mod\,8}$, esto implica que $\left(\frac{q}{p}\right) = 1$. Además también vale que $\left(\frac{2}{p}\right) = 1$ y entonces todos los factores primos de s son cuadrados módulo p. Por lo tanto, s^2 es una cuarta potencia módulo p. La ecuación

$$2s^2 \equiv t^4_{mod\,p}$$

muestra que 2 es una cuarta potencia módulo p y llegamos a una contradicción.

Claramente la curva tiene puntos en $\mathbb{R}$. Para ver que tiene puntos en $\mathbb{Q}_p$ usamos el Lema de Hensel.

Será suficiente ver que la curva tiene un punto no singular en cada $\mathbb{F}_q$. Cuando $q \neq 2, p$, la curva tiene buena reducción módulo q. En ese caso, veremos mas adelante que si N_q es la cantidad de soluciones proyectivas de la curva sobre $\mathbb{F}_q$, y la curva es no singular, entonces se cumple que

$$|N_q - 1 - q| \leq 2\sqrt{q}$$

Con lo cual $N_q \geq 1 + q - 2\sqrt{q} > 0$ y habrá algún punto en $\mathbb{F}_q$.

Para el caso $q = 2$, es suficiente mirar la curva

$$2Y^2 = 1 - pX^4$$

pues (x, y) es un punto de esta curva si y solo si $(x, 2y)$ lo es de la curva original.

Mirando módulo 32, y tomando en cuenta que $p \equiv 1_{mod\,8}$, tenemos las siguientes soluciones:

$p \equiv_{mod\,32}$	$x =$	$y =$
1	1	4
9	3	2
17	3	4
25	1	2

Llamamos $\overline{a}$ al punto solución en cada caso. Entonces $\overline{a}$ verifica

$$f(\overline{a}) \equiv 0_{mod\,2^{2,2+1}}$$

donde $f(X, Y) = 2Y^2 - 1 + pX^4$. Pero

$$\left(\frac{\partial f}{\partial X}\right)(\overline{a}) = 4pX^3(\overline{a}) \equiv 4 \not\equiv 0_{mod\,2^{2+1}}$$

se aplican las hipótesis del Lema de Hensel con $m = 2$.

Para el caso $q = p$, como 2 es cuadrado módulo p, sea α tal que $\alpha^2 \equiv 2_{mod\,p}$. Entonces el punto $\overline{a} = (0, \alpha^{-1})$ verifica que:

$$f(\overline{a}) \equiv 0_{mod\,p^{0+1}}$$

Además,

$$\left(\frac{\partial f}{\partial Y}\right)(\overline{a}) \equiv 4\alpha^{-1} \not\equiv 0_{mod\,p^{0+1}}$$

y entonces se aplican las hipótesis del Lema.$\diamond$

12. Conjeturas de Birch–Swinnerton-Dyer

Hemos visto que hay dificultades para calcular el rango de una curva elíptica, y que radican en la existencia del grupo Ш. Ahora vamos a enfocar el problema desde otro punto de vista, relacionando el rango de la curva con la cantidad de puntos que tienen las reducciones de la curva módulo p primo.

12.1. Función Zeta de una Curva Elíptica

Sea Δ el discriminante minimal de $\mathcal{C}$ curva elíptica. Si $\mathbb{F}_{p^n}$ es el cuerpo de p^n elementos, sea

$$Z_{\mathcal{C},p}(T) = exp\left(\sum_{n=1}^{\infty} \frac{N_{p^n}}{n} T^n\right)$$

donde N_{p^n} es el número de soluciones proyectivas de $\mathcal{C}$ sobre $\mathbb{F}_{p^n}$. Enunciamos sin demostración el siguiente

Teorema 67 *Sea $\mathcal{C}$ una curva proyectiva no singular definida sobre un cuerpo finito $\mathbb{F}_p$. Entonces*

(1) *$Z_{\mathcal{C},p}(T)$ es una función racional con coeficientes en $\mathbb{Z}$.*

(2)

$$Z_{\mathcal{C},p}(T) = \frac{P(T)}{(1-T)(1-pT)}$$

con $P(T) \in \mathbb{Z}[T]$ de grado $2g$ donde g es el género de la curva y $P(T)$ es de la forma

$$P(T) = \prod_{j=1}^{2g} (1 - \alpha_j T)$$

con $|\alpha_j| = p^{\frac{1}{2}} \quad j = 1, 2, ..., 2g$.

(3)

$$Z_{\mathcal{C},p}\left(\frac{1}{pT}\right) = p^{\frac{e}{2}} T^e Z_{\mathcal{C},p}(T)$$

con $e = 2 - 2g$

Dicho Teorema se conoce como Conjeturas de Weil (a pesar que ha sido demostrado) y tiene una versión mas general para variedades proyectivas.

En nuestro caso, como $g = 1$, $P(T)$ es de grado 2,

$$P(T) = 1 - (\alpha_p + \beta_p)T + \alpha_p\beta_p T^2$$

Llamamos $a_p = \alpha_p + \beta_p$ y por el Teorema,

$$|a_p| \leq |\alpha_p| + |\beta_p| \leq 2\sqrt{p}$$

y $|\alpha_p\beta_p| = p$ y como $\alpha_p\beta_p$ tiene que ser entero, es igual a p o $-p$.

Ahora miramos la ecuación funcional que tiene que satisfacer según el Teorema anterior:

$$\frac{\left(1 - \alpha_p \frac{1}{pT}\right)\left(1 - \beta_p \frac{1}{pT}\right)}{\left(1 - \frac{1}{pT}\right)\left(1 - \frac{p}{pT}\right)} = \frac{(1 - \alpha_p T)\,(1 - \beta_p T)}{(1 - T)(1 - pT)}$$

pues $g = 1 \Rightarrow e = 0$.

El término de la izquierda resulta ser igual a:

$$\frac{\frac{1}{p}(pT - \alpha_p)(pT - \beta_p)}{(1 - T)(1 - pT)}$$

Al evaluar en $T = 0$, el término de la derecha da 1 y este último da $\frac{\alpha_p\beta_p}{p}$ y como tienen que dar lo mismo,

$$\alpha_p\beta_p = p$$

Entonces

$$Z_{\mathcal{C},p}(T) = \frac{1 - a_p T + pT^2}{(1 - T)(1 - pT)}$$

Mirando los coeficientes de T en las dos expresiones de $Z_{\mathcal{C},p}(T)$, sale que

$$\log Z_{\mathcal{C},p}(T) = \log \frac{(1 - \alpha_p T)(1 - \beta_p T)}{(1 - T)(1 - pT)} = \sum_{n=1}^{\infty} (1 + p^n - \alpha_p^n - \beta_p^n)\frac{T^n}{n} = \sum_{n=1}^{\infty} \frac{N_{p^n}}{n} T^n$$

Igualando coeficientes,

$$N_{p^n} = 1 + p^n - \alpha_p^n - \beta_p^n$$

En particular,

$$N_p = 1 + p - a_p$$

Entonces vale

$$|N_p - 1 - p| \leq 2\sqrt{p}$$

Además, como sabemos que $\alpha_p\beta_p = p$, $\alpha_p + \beta_p = 1 + p - N_p$, entonces con N_p podemos despejar α_p y β_p y con ellos nos quedan determinados los valores de N_{p^n} para todo n.

12.2. Conjeturas

Birch y Swinnerton-Dyer tuvieron la idea que si $F(\mathbb{Q})$ era grande, entonces también serían grandes los N_p y formularon la

Conjetura 68 *Para una curva elíptica $\mathcal{C}$ definida sobre $\mathbb{Q}$ con rango r,*

$$\lim_{M\to\infty} \frac{\prod_{p\leq M, p\nmid N} \frac{N_p}{p}}{(\log M)^r} = constante$$

Acá N es el conductor de la curva, es producto de los primos para los cuales la reducción no es buena elevados a ciertas potencias (lo veremos mas adelante). Esta conjetura no es muy buena para determinar el valor de r pues el producto oscila demasiado con el aumento de M.

Sea $\mathcal{V}$ una variedad proyectiva no singular sobre $\mathbb{Q}$, es decir los ceros de una colección de polinomios homogéneos en las variables $X_0, X_1, ..., X_n$. Si reescalamos cada polinomio como para que los coeficientes estén en $\mathbb{Z}$ pero que no tengan ningún factor común y los reducimos módulo p primo, definirán una variedad $\mathcal{V}_p$ sobre $\mathbb{F}_p$, que si es no singular decimos que hay buena reducción en p. Todos salvo finitos primos serán de buena reducción.

Para cada primo bueno definimos la función zeta:

$$\zeta_{\mathcal{V},p}(s) = Z_{\mathcal{V},p}(p^{-s})$$

donde

$$Z_{\mathcal{V},p}(T) = exp\left(\sum_{n=1}^{\infty} \#V_p(\mathbb{F}_{p^n})\frac{T^n}{n}\right)$$

y definimos

$$\zeta_{\mathcal{V}}(s) = \prod_p \zeta_{\mathcal{V},p}(s)$$

Conjetura 69 *(Hasse–Weil) Sea $\mathcal{V}$ una variedad proyectiva no singular sobre $\mathbb{Q}$. Entonces $\zeta_{\mathcal{V}}(s)$ puede extenderse analíticamente a una función meromorfa en todo el plano satisfaciendo una ecuación funcional que relaciona $\zeta_{\mathcal{V}}(s)$ con $\zeta_{\mathcal{V}}(d+1-s)$, siendo s la dimensión de la variedad.*

Para una curva elíptica, si S es el conjunto de los primos con mala reducción, nos queda

$$\zeta_{\mathcal{C}}(s) = \prod_{p\notin S} \frac{1 - a_p p^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} = \frac{\zeta_S(s)\zeta_S(s-1)}{L_S(s)}$$

donde $\zeta_S(s)$ es la función zeta de Riemann exceptuando los factores correspondientes a los primos de S y

$$L_S(\mathcal{C}, s) = \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \prod_{p \notin S} \frac{1}{1 - \alpha_p p^{-s}} \frac{1}{1 - \beta_p p^{-s}}$$

Ahora bien, el producto $\prod_p \frac{1}{1-p^{-s}}$ converge para $\Re(s) > 1$, y entonces

$$\prod_p \frac{1}{1 - p^{\frac{1}{2}} p^{-s}}$$

converge para $\Re(s) > \frac{3}{2}$. Como $|\alpha_p| = |\beta_p| = p^{\frac{1}{2}}$, sale que $L_S(\mathcal{C}, s)$ converge para $\Re(s) > \frac{3}{2}$.

Queremos agregar factores a $L_S(\mathcal{C}, s)$ correspondientes a los primos de mala reducción.

En el caso de $p|\Delta$ se define también $a_p = 1 + p - N_p$, donde N_p es la cantidad de puntos de la curva sobre $\mathbb{F}_p$ contando la singularidad una vez. La singularidad que puede ser de diferentes tipos.

Considerando los casos, obtenemos:

$$a_p = \begin{cases} 0 & \text{caso cúspide} \\ 1 & \text{caso de nodo partido} \\ -1 & \text{caso de nodo no partido} \end{cases}$$

Definimos la función:

$$L(\mathcal{C}, s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p \not| \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Notemos que al evaluar cada factor en $s = 1$ se obtiene:

$$= \frac{1}{1 - a_p p^{-1} + p^{-1}} = \frac{p}{p - a_p + 1} = \frac{p}{N_p}$$

$$= \frac{1}{1 - a_p p^{-1}} = \frac{p}{p - a_p} = \frac{p}{N_p - 1}$$

en ambos casos, el factor es

$$\frac{p}{\#F^{ns}(\mathbb{F}_p)}$$

donde F^{ns} denota los puntos no singulares.

El conductor $N_{\mathcal{C}/\mathbb{Q}}$ de $\mathcal{C}$ se define como

$$N_{\mathcal{C}/\mathbb{Q}} = \prod_{p\, malo} p^{f_p}$$

donde

$$f_p = \begin{cases} f_p = 1 & \text{si } \mathcal{C} \text{ tiene un nodo en la reducción módulo } p \\ f_p \geq 2 & \text{si } \mathcal{C} \text{ tiene una cúspide en la reducción módulo } p \text{ y es igual a 2 si } p \neq 2,3 \end{cases}$$

Definamos

$$\Lambda(\mathcal{C}, s) = N_{\mathcal{C}/\mathbb{Q}}^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(\mathcal{C}, s)$$

Tenemos una versión mas precisa de la conjetura de Hasse–Weil:

Conjetura 70 *La función $\Lambda(\mathcal{C}, s)$ puede extenderse analíticamente a una función meromorfa en todo el plano satisfaciendo la ecuación funcional*

$$\Lambda(\mathcal{C}, s) = w\Lambda(\mathcal{C}, 2-s), \qquad w = \pm 1$$

Sea ahora $\mathcal{C}$ curva elíptica sobre $\mathbb{Q}$ y sea

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

su ecuación minimal sobre $\mathbb{Q}$, y sea

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

Recordemos que tenemos definida una forma bilineal sobre $F(\mathbb{Q})$:

$$\langle \mathbf{x}, \mathbf{y} \rangle = h(\mathbf{x} + \mathbf{y}) - h(\mathbf{x}) - h(\mathbf{y})$$

y si $\mathbf{x}_1, ..., \mathbf{x}_r$ es una base de la parte libre de $F(\mathbb{Q})$, entonces el regulador elíptico es

$$R = det(\langle \mathbf{x}_i, \mathbf{x}_j \rangle)$$

que resulta independiente de la base elegida y positivo.

Conjetura 71 *(Birch–Swinnerton-Dyer) Sea $\mathcal{C}$ una curva elíptica definida sobre $\mathbb{Q}$ y sea $F(\mathbb{Q})$ el conjunto de los puntos racionales. Entonces*

$$F(\mathbb{Q}) \text{ es infinito si y solo si } L(\mathcal{C}, 1) = 0$$

Mas general, si

$$F(\mathbb{Q}) = T \oplus \mathbb{Z}^r$$

entonces, r es el orden del cero en $L(\mathcal{C}, s)$ en $s = 1$.

Si

$$L(\mathcal{C}, s) = C(s-1)^r + ...$$

es el desarrollo de Taylor alrededor de $s = 1$, entonces,

$$\frac{C|T|^2}{\Omega R \prod_{p|N} c_p} = |Ш|$$

Donde

$$\Omega = \int_{F(\mathbb{R})} |\omega| \qquad c_p = (F(\mathbb{Q}_p) : F^0(\mathbb{Q}_p))$$

Todos los términos de la Conjetura se pueden calcular excepto $|Ш|$, que en principio ni siquiera se sabe que sea finito en general.

Si $\mathbf{x}_1, ..., \mathbf{x}_r$ son elementos linealmente independientes de $F(\mathbb{Q})$, entonces

$$\frac{det(\langle \mathbf{x}_i, \mathbf{x}_j \rangle)}{(F(\mathbb{Q}) : \sum \mathbb{Z}\mathbf{x}_i)^2}$$

es independiente de la elección de los $\mathbf{x}_i$ y es igual a

$$\frac{R}{|T|^2}$$

cuando forman una base.

La integral

$$\int_{F(\mathbb{Q}_p)} |\omega|$$

tiene sentido y de hecho se puede probar que es igual a

$$\frac{(F(\mathbb{Q}_p) : F^1(\mathbb{Q}_p))}{p} = \frac{c_p N_p}{p}$$

13. Ejemplos

13.1. Una curva con rango no nulo

Consideremos el mismo ejemplo que habíamos visto para el caso del Teorema de la Base Finita Débil. Habíamos trabajado con la curva:

$$\mathcal{C} : Y^2Z - X(X^2 + 3XZ + 5Z^2) = F(X, Y, Z)$$

Calculamos que

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle (1, 3), (0, 0) \rangle$$

y no aparecieron cuárticas "extrañas", o sea que $[Ш]_2$ nos dio trivial.

Miremos la torsión. $(0, 0)$ es de torsión de orden 2, y además no es doble de nadie pues si no, desaparecería al hacer $F(\mathbb{Q})/2F(\mathbb{Q})$. Con el mismo razonamiento, $(1, 3)$ tampoco es doble de nadie. Para buscar puntos de torsión (x, y) mas en general, por Lutz–Nagell, o bien $y = 0$, o bien $y^2|\Delta$. El caso $y = 0$ no nos da nuevas soluciones pues $X^2 + 3X + 5$ no tiene raíces reales. Para calcular Δ, hacemos el cambio

$$X' = X + 1$$

Queda

$$Y^2Z = X'^3 + 2X'Z^2 - 3Z^3$$

$\Rightarrow \Delta = 4{,}2^3 + 27.(-3)^2 = 275$. A partir de ahora trabajaremos con esta curva. Los puntos de la curva original $(0, 0)$ y $(1, 3)$ pasaron a $(1, 0)$ y $(2, 3)$. Luego hay que mirar

$$y^2|275 = 5^2{,}11$$

con lo cual $(2, 3)$ no es de torsión. Además se concluye que $|y| = 1$ o 5.

En el primer caso,

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

Entonces $4 = x'(x'^2 + 2)$, con lo cual $2|x'$. Escribimos $x' = 2x'_1$, queda $1 = x'_1(2x'^2_1 + 1)$ y esto claramente no tiene solución entera.

En el segundo caso,

$$25 = x'^3 + 2x' - 3$$

Entonces $28 = x'(x'^2 + 2)$, como antes $2|x'$, $x' = 2x'_1$, queda $7 = x'_1(2x'^2_1 + 1)$ y esto no tiene solución entera tomando en cuenta que 7 es primo.

Entonces no hay mas puntos de torsión.

$$T = \langle (1,0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$$

El rango es 1, pues si hubiera mas de un generador, estos tendrían que aparecer en $F(\mathbb{Q})/2F(\mathbb{Q})$, por no ser dobles de nadie. Entonces tenemos que encontrar un generador. Buscamos un punto racional $[x' : y : 1]$ tal que $H(x')$ sea lo mas chica posible. Claramente, $x' = 1$ nos da la solución $(1, 0)$. Entonces, buscamos con $H(x') = 2$. Ahi el $(2, 3)$, funciona y entonces tiene que ser un generador de la parte libre.

Ahora $R = 2h((2,3))$. Con Pari calculamos $R = 2 * 0,394888973 = 0,789777946$, $N = 440$, $c_2 = 2$, $c_5 = 2$, $c_{11} = 1$. Luego $\prod_{p|N} c_p = 4$. $|T|^2 = 4$. También con Pari calculamos: $C = 1,734674621$, $\Omega = 2,196408028$.

Entonces:

$$\frac{C|T|^2}{\Omega R \prod_{p|N} c_p} = \frac{1,734674621{,}4}{2,196408028{,}0,789777946{,}4} = 1$$

Lo cual es coherente con el hecho de haber obtenido $|[Ш]_2| = 1$.

13.2. Un ejemplo con LLI no trivial

Busquemos una curva con Ш no trivial. Recordando el método para hallar una base de $F(\mathbb{Q})/2F(\mathbb{Q})$, lo que hacíamos era partir de la curva

$$\mathcal{C} : Y^2Z - X(X^2 + aXZ + bZ^2) = F(X, Y, Z)$$

y pasar por la curva

$$\mathcal{D} : Y^2Z - X(X^2 - 2aXZ + (a^2 - 4b)Z^2) = Y^2Z - X(X^2 + a_1XZ + b_1Z^2) = G(X, Y, Z)$$

Había que buscar soluciones enteras no triviales de las cuárticas del tipo:

$$ql^4 + a_1l^2m^2 + \left(\frac{b_1}{q}\right)m^4 = n^2$$

El problema surge cuando la cuártica

$$q + a_1X^2 + \left(\frac{b_1}{q}\right)X^4 = Y^2$$

tiene solución en todos lados localmente pero no tiene soluciones racionales. Buscaremos la curva $\mathcal{C}$ para que aparezcan cuárticas de ese tipo.

Vamos a partir de la cuártica

$$Y^2 = 2 - 2pX^4$$

con $p \equiv 1_{mod\,8}$ y 2 no es cuarta potencia módulo p, de la cual sabemos que no cumple el principio de Hasse.

Entonces

$$q = 2, \qquad a_1 = 0, \qquad \frac{b_1}{q} = -2p$$

Deducimos que

$$b_1 = -4p, \qquad a = 0, \qquad b = p$$

Entonces, sea

$$\mathcal{C} : Y^2Z - X(X^2 + pZ^2) = F(X, Y, Z)$$

Aplicando la función ϕ obtenemos:

$$\mathcal{D} : Y^2Z - X(X^2 - 4pZ^2) = G(X, Y, Z)$$

Para calcular $G(\mathbb{Q})/\phi F(\mathbb{Q})$: Buscamos los $q| - 4p$ que sean libres de cuadrados. Sabemos que $-p$ le corresponde al $(0, 0)$. Hay que ver $\pm 1, \pm 2, \pm p, \pm 2p$.

Como $(\pm 1)(\mp p) = -p$ y $(\pm 2)(\mp 2p) = -4p$, que dan el $(0, 0)$, bastará con ver que pasa con $\pm 2, \pm p$. $q = -p$ ya lo sabemos.

El caso $q = 2$ da la ecuación:

$$2l^4 - 2pm^4 = n^2$$

que tiene soluciones en todos lados localmente pero no tiene soluciones en $\mathbb{Q}$. Esto nos da una pauta que $[Ш]_2$ es no trivial.

El caso $q = -2$ da la ecuación:

$$-2l^4 + 2pm^4 = n^2$$

de donde sale que $2|n$ y podemos escribir $n = 2n'$ y queda

$$-l^4 + pm^4 = 2n'^2$$

Se prueba que esta curva tiene soluciones en todos lados localmente pero no tiene solución racional de modo análogo a la primer curva que dimos. Para probar que no tiene soluciones racionales hay que usar que -1 es cuarta

potencia módulo p lo cual es cierto por ser $p \equiv 1_{mod\,8}$. Entonces con $q = -2$ obtenemos otro elemento de $[Ш]_2$.

El caso $q = p$ no hace falta analizarlo demasiado pues $(-2)2 = -4$, que le corresponde a p, también dará un elemento de $[Ш]_2$.

Por lo tanto,

$$G(\mathbb{Q})/\phi F(\mathbb{Q}) = \langle (0,0) \rangle$$

Calculemos $F(\mathbb{Q})/\psi G(\mathbb{Q})$: Buscamos los $q|p$. Sabemos que $q = p$ le corresponde al $(0,0)$.

Como $(\pm 1)(\pm p) = p$ bastará con ver que pasa con -1. Este da la ecuación:

$$-l^4 - pm^4 = n^2$$

que claramente no tiene soluciones en $\mathbb{R}$, pues el miembro de la izquierda es siempre negativo y el de la derecha positivo, y ambos valen cero solo en el caso trivial. Entonces

$$F(\mathbb{Q})/\psi G(\mathbb{Q}) = \langle (0,0) \rangle$$

Por lo tanto

$$F(\mathbb{Q})/2F(\mathbb{Q}) = \langle \psi(0,0), (0,0) \rangle = \langle (0,0) \rangle$$

Ahora bien, $(0,0)$ es un punto de torsión de orden 2, además no es doble de nadie, pues si lo fuera, sería cero en $F(\mathbb{Q})/2F(\mathbb{Q})$. Para ver si hay otros puntos de torsión usamos el Teorema de Lutz–Nagell.

Como en nuestro caso, $\Delta = 4p^3$, hay que mirar los casos $y = 0, \quad y^2|4p^3$. Si $p \not| y$, entonces $y^2 \leq 4$ y por lo tanto, $|x(x^2 + p)| \leq 4$ y esto es imposible pues el mínimo p posible es 17 y entonces solo vale con $x = 0$ pero este caso es el $(0,0)$. Si $p|y$, entonces $p^2|x(x^2 + p)$, por lo tanto $p|x$ o $p|(x^2 + p)$. En cualquier caso, $p|x$. Escribimos $x = px_1$, $y = py_1$. Obtenemos:

$$y_1^2 = x_1(px_1^2 + 1)$$

Con $|y_1| = 1$ o 2 (pues tiene que pasar $y_1^2|4p$). Claramente

$$1 = x_1(px_1^2 + 1) \qquad 4 = x_1(px_1^2 + 1)$$

No tienen solución por lo mismo que en el primer caso.

Entonces, en nuestra curva:

$$T = \langle (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$$

Además el rango es cero pues si no lo fuera, el generador del grupo libre debería sobrevivir en $F(\mathbb{Q})/2F(\mathbb{Q})$.

Comprobemos la conjetura de Birch–Swinnerton-Dyer en este caso. Tenemos que $|T|^2 = 4$, $R = 1$.

Para $\prod_{p|N} c_p$, hay que mirar los primos de mala reducción. Estos son a lo sumo 2 y p que son los que dividen a Δ. Como claramente $|4p^3|_2 > 2^{-12}, |4p^3|_p > p^{-12}$, la ecuación está en forma minimal.

$c_2 = (F(\mathbb{Q}_2) : F^0(\mathbb{Q}_2))$. Miremos primero que pasa módulo 2. En este caso,

$$\mathcal{C} : Y^2Z - (X^3 + XZ^2) = F(X, Y, Z)$$

Vale

$$\frac{\partial F}{\partial X} = 3X^2 + Z^2 \qquad \frac{\partial F}{\partial Y} = 0 \qquad \frac{\partial F}{\partial Z} = Y^2$$

El único punto singular módulo 2 es entonces $[1 : 0 : 1]$. Buscamos los puntos de $F(\mathbb{Q}_2)$ que reducen a este punto. Volviendo a la ecuación original, escribimos $Y = 2Y_1$ y obtenemos:

$$4Y_1^2Z - X(X^2 + pZ^2) = 0$$

sobre $\mathbb{Q}_2$. Mirando módulo 4,

$$X(X^2 + pZ^2) \equiv 0_{mod\,4}$$

Como X es impar y $p \equiv 1_{mod\,4}$, sale que

$$X^2 \equiv -Z^2_{mod\,4}$$

y esto es absurdo.

Entonces todas las soluciones son no singulares módulo 2 y

$$c_2 = 1.$$

$c_p = (F(\mathbb{Q}_p) : F^0(\mathbb{Q}_p))$. Módulo p la ecuación queda

$$\mathcal{C} : Y^2Z - X^3 = F(X, Y, Z)$$

Vale

$$\frac{\partial F}{\partial X} = -3X^2 \qquad \frac{\partial F}{\partial Y} = 2YZ \qquad \frac{\partial F}{\partial Z} = Y^2$$

Entonces las soluciones singulares son las que cumplen $x = 0, \quad y = 0$, módulo p (pues si pedimos $z = 0$ igualmente tenemos que pedir $y = 0$ y llegamos a un absurdo).

Luego, tenemos el $\mathbf{o}$ que es no singular, y consideramos la siguiente función:

$$\alpha : F^0(\mathbb{Q}_p) \longmapsto F(\mathbb{Q}_p) \setminus F^0(\mathbb{Q}_p)$$
$$\alpha(\mathbf{x}) = \mathbf{x} + (0,0)$$

Cuando hicimos la demostración del Teorema de la Base Finita Débil teníamos esta función y habíamos calculado que

$$\alpha(x,y) = \left(\frac{p}{x}, \frac{-py}{x^2}\right)$$
$$\alpha(\mathbf{o}) = (0,0)$$

Claramente la función está bien definida porque si partimos de un punto (x,y) que es no singular en su reducción módulo p, no puede ser que $x = 0$, ya que eso corresponde al punto $(0,0)$ que tiene reducción singular. Es claro que esa es la imagen, pues si $\mathbf{x}$ y $\mathbf{x} + (0,0)$ fueran puntos con reducción no singular módulo p, también lo sería $(\mathbf{x} + (0,0)) - \mathbf{x} = (0,0)$ absurdo. Además la función es claramente inyectiva. Para ver que es suryectiva, miremos su inversa, restar $(0,0)$. Sea

$$\beta : F(\mathbb{Q}_p) \setminus F^0(\mathbb{Q}_p) \longmapsto F^0(\mathbb{Q}_p)$$
$$\beta(\mathbf{x}) = \mathbf{x} - (0,0)$$

Entonces,

$$\beta(x,y) = \beta(px_1, py_1) = \left(\frac{1}{x_1}, \frac{-y_1}{x_1^2}\right)$$
$$\beta(0,0) = \mathbf{o}$$

Y esta función es la inversa de α. Entonces "la mitad" de las soluciones tienen reducción singular y "la mitad" no. Luego:

$$c_p = 2.$$

Juntando todo,

$$\prod_{p|N} c_p = 2$$

Para calcular $L(\mathcal{C},1)$ (como el rango es cero, esto es lo mismo que calcular C) y Ω, utilizaremos el programa Pari. Estos valores si dependen de p. Por ejemplo

p	17	41	97	193
$L(\mathcal{C},1)$	$3,652371821$	$2,930834192$	$2,363166275$	$1,989747127$
Ω	$1,826185910$	$1,465417096$	$1,181583137$	$0,994873564$
$L(\mathcal{C},1)/\Omega$	2	2	2	2

Ahora

$$\frac{L(\mathcal{C},1)}{\Omega}\frac{|T|^2}{\prod_{p|N} c_p} = 2\frac{4}{2} = 4$$

Entonces, si aceptamos la conjetura en este caso, $|Ш| = 4$, lo que es coherente con el hecho de haber obtenido $|[Ш]_2| = 4$.

Notas

Secciones 2 y 4

Estas secciones tratan temas muy generales por lo que se encuentran en muchos libros. Para generalidades acerca de curvas hay un muy buen tratamiento en [Kn] y en [Mi]. También es interesante la parte introductoria de [Sch]. Los resultados no demostrados de esa parte se pueden encontrar en [Kn] y [Wa]. La sección de curvas elípticas está mas basada en los desarrollos de [Ca1] y [Ca2]. Dos referencias siempre presentes para estos temas son [Sil] y [Ta].

Sección 3

Los números p-ádicos también se pueden encontrar en muchas fuentes, por ejemplo [QG] y también [Se] aunque el desarrollo expuesto sigue a [Ca2].

Sección 5

El tema de resultantes también es general. Puede encontrarse en [Kn], [Ca2], [Mi] o [Wa].

Sección 6

La demostración del Teorema de Mordell es la que aparece en [Ca2] donde se encuentra la versión completa (incluyendo el caso en que la curva no tenga puntos de orden 2). Se pueden encontrar otras demostraciones en [Ca1],[Kn], [Mi], [Sch] y [Sil]. El desarrollo acerca de las propiedades de las alturas está basado en el de [Kn].

Sección 7

Los resultados sobre puntos de torsión de una curva elíptica son bastante generales. En este caso se sigue a [Mi], pero también a [Ca2] y [Kn]. Para los resultados acerca de reducción de curvas, se puede consultar [Sil] y [Ta].

Sección 8

La cota del rango de una curva elíptica con tres puntos de orden dos está adaptada del resultado que aparece en [Kn].

Secciones 1 y 9

El contenido de los resultados sobre números congruentes puede encontrarse básicamente en [Kn].

Sección 10

Este desarrollo está tomado principalmente de [Ca2]. Con diversos tratamientos puede encontrarse en [Ca1], [Mi], [Sch], [Sil] y [Ta].

Sección 11

El ejemplo está desarrollado con mayor profundidad en [Sil] y se menciona en [Mi].

Sección 12

Un desarrollo general sobre funciones zeta y sus propiedades puede encontrarse en [RV]. Los detalles acerca de la Conjetura de Birch–Swinnerton-Dyer se encuentran en [Mi], [Sil] y en [Ta].

Referencias

[Ca1] Cassels, J.W.S., Diophantine equations with special reference to elliptic curves, *Journal London Math. Soc.*, 41 (1966), 193 - 291.

[Ca2] Cassels, J.W.S., *Lectures on Elliptic Curves*, London Math. Soc., Student Texts 24, Cambridge University Press, Cambridge, 1991.

[Kn] Knapp, A.W., *Elliptic Curves*, Princeton University Press, Princeton, 1992.

[Mi] Milne, J.S., *Elliptic Curves*, notes for Math 679, University of Michigan, 1996.

[QG] Quadros Gouvêa, F., *Primeiros Passos p-adicos*, 17 Colóquio Brasileiro de Matemática, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 1989.

[RV] Rodríguez-Villegas, F., *Introducción a las Funciones Zeta de Hasse–Weil*, Decimosegunda Escuela Venezolana de Matemáticas, Caracas, 1999.

[Se] Serre, J.P., *A course in Arithmetic*, Springer-Verlag, New York, 1973.

[Sch] Schaefer, E., *Rational points on algebraic curves*, Santa Clara University, 1999.

[Sil] Silverman, J.H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Ta] Tate, J.T., The arithmetic of elliptic curves, *Invent. Math.*, 23 (1974), 179 - 206.

[Wa] Walker, R.J., *Algebraic Curves*, Dover Publications, Inc., New York, 1962.