Trabajo Monográfico

Introducción a las curvas elípticas

Orientador: Gonzalo Tornaria (CMAT-FCIEN)

Licenciatura en Matemáticas
Facultad de Ciencias
Universidad de la República
Uruguay

02 de marzo de 2007

Índice general

Introducción

1. Introducción.

El tema principal de esta monografía es introducir las curvas elípticas, estudiando en mayor detalle las curvas elípticas racionales.

En el primer capítulo introduciremos las curvas elípticas, definiremos la ley de grupo, veremos que se pueden llevar a una expresión reducida (la forma normal de Weierstrass), y daremos fórmulas explícitas para la ley de grupo. Culminaremos el capítulo mostrando algunos ejemplos.

En el segundo capítulo estudiaremos las curvas elípticas definidas sobre $\mathbb{C}$. Probaremos que el grupo de una curva elíptica compleja es isomorfo al grupo de un translaciones de un toro; más aún, el isomorfismo de grupos también preserva la estructura analítica de la curva elíptica. A partir de esto calcularemos el grupo de los puntos cuyo orden es divisor de un natural fijo m.

Luego estudiaremos la estructura de grupo de una curva elíptica real que resulta isomorfo al grupo de rotaciones del círculo o producto de este por $\mathbb{Z}_2$ según la cantidad de componentes conexas de la curva, y usaremos esto para estudiar los puntos de orden finito.

En el tercer capítulo probaremos un teorema de Nagell-Lutz que nos permite calcular los puntos de orden finito sobre una curva elíptica racional.

En el cuarto capítulo probaremos el teorema de Mordell que dice que el grupo de una curva elíptica racional es finitamente generado, es decir que a partir de una cantidad finita de puntos, con el método de trazado de rectas y tangentes que define la ley de grupo, uno puede hallar cualquier otro punto racional.

Mientras que la parte de torsión es bien conocida — tenemos el teorema de Nagell-Lutz que nos permite obtener dichos puntos en una cantidad finita de pasos y el Teorema de Mazur que caracteriza los posibles grupo de torsión de una curva elíptica racional — la parte libre no es muy conocida. Existe una importante conjetura sobre el rango de una curva elíptica racional que es la Conjetura de Birch y Swinnerton-Dyer (BSD) que relaciona el rango de una curva elíptica racional con el orden de anulación de cierta L-serie asociada a la curva.[1] Describir esa L-serie no es trabajo fácil y será necesario estudiar cúbicas sobre cuerpos finitos para su construcción y funciones modulares para obtener una prolongación

[1] `http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf`

analítica al plano complejo de la L-serie.[2]

La conjetura BSD no solo es importante porque nos permite calcular el rango de una curva elíptica, sino también por mostrar el poder unificador que es una característica de la matemática moderna. Aquí confluyen cuatro ramas de la matemática como ser la Teoría de Números, la Geometría, el Álgebra y el Análisis. La Teoría de Números porque estamos buscando soluciones racionales de cierta ecuación que es la ecuación que define la curva elíptica. Luego entra en juego la Geometría cuando observamos que una recta que pasa por dos puntos racionales de la cúbica ha de pasar por un tercero, esto nos permite obtener un procedimiento que nos permite a partir de algunos puntos seguir construyendo otros. A partir de esa operación definimos una suma en los puntos de la cúbica que la dota de estructura de grupo abeliano finitamente generado, he aquí donde entra el Álgebra. El Análisis entra en juego para poder entender mejor este grupo, a cada curva elíptica racional le podemos asociar una L-serie que es un objeto analítico cuyos coeficientes dan una idea de como crecen los puntos en la reducción de la cúbica sobre cuerpos finitos, dicha L-serie así construida converge para complejos con parte real mayor que $3/2$, pero dichas L-series están en correspondencia con otras L-series que son las L-series asociadas a funciones modulares las cuales sabemos que se prolongan analíticamente al plano complejo. La conjetura predice que el orden de anulación de nuestra L-serie en $s = 1$ coincide con el rango de la curva elíptica.

Palabras Claves: Curvas elípticas, Teorema de Mordell, Weierstrass.

[2]Se hace esto a través de un teorema de Wiles que asocia a cada curva elíptica una forma modular con la misma L-serie asociada.

2. Introduction.

The principal topic of this book is to introduce the elliptic curves, with special emphasis in rational elliptic curves.

In the first chapter we will introduce the elliptic curves, we will define the group law, will see that one can be take reduced expression (the Weierstrass normal form), and we will give explicit formulae for the group law. We will culminate this chapter showing some examples.

In the second chapter we will study complex elliptic curves. We will prove that the group of a complex elliptic curve is isomorphic to the group of rotation of the torus, moreover it isomorphism is not only an group isomorphism but also is an isomorphism between Riemman Surfaces. From this will calculate the group of the points whose order is a divisor of a fixed natural m.

Next we will study the structure of group of a real elliptic curve that is isomorphic to the rotation group of circle or direct sum of this with $\mathbb{Z}_2$ according to the quantity of connected components of the curve, and we will use this to study the finite order points.

In the third chapter we will prove Nagell-Lutz Theorem that it give us an algorithm to calculate the points of finite order in a rational elliptic curve.

In the fourth chapter we will prove the Mordell Theorem who says that the group of a rational elliptic curve is finitely generated, that is to say that from a finite quantity of points, with the method of tracing straight and tangent that it defines the group law, one can find any other rational point.

Whereas the torsion subgroup is well-known - we have Nagell-Lutz Theorem for calculate the points of finite order and Mazur Theorem that caracterizes all possible torsion subgroup of a rational elliptic curve - the free part it is not. There is an important conjeture called Birch and Swinnerton-Dyer conjeture (BSD) that relates the rank of a rational elliptic curve with the order of annulment of certain L-serie associated to the curve. [3] To describe this L-serie it's not an easy work it needs study cubic over finite fields for its construction and modular functions for to obtain an analytic prolongation to the complex plane. [4]

The BSD conjeture not only is important because it allows us to calculate the rank of a rational elliptic curve, but also for showing the unifier character who is a characteristic of the modern mathematics. Here four branches of the mathematics come together as being the Number Theory, Geometry, Algebra and Analysis. The Number Theory because we are looking rational solutions of certain equation that is the equation that defines the elliptic curve. The Geometry appears when we observe that a straight line that intersect the cubic in two rational points it must pass through a third point of the cubic also with rational coordinates, this give us a procedure that allows us from some points to keep constructing others. From this operation we define a sum in the points of the cubic one

[3] `http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/birchswin.pdf`

[4] This is possible thanks to Wiles Theorem that associated with every elliptic curve a modular form with the same associate L-serie

that provides it with group structure, it group is a finitely generated abelian group, here we use algebra to understand this group. The Analysis help us to understand better this group, every rational elliptic curve has associate a L-series that is an analytical object whose coefficients give us an idea of as the points grow in the reduction of the cubic over finite fields, this L-series converges for complex numbers with real part greater than $3/2$, but for Wiles's Theorem this L-series is the L-series associated with a modular functions therefore it can extended analytically to the complex plane. The conjecture predicts that the order of zero of our L-series in $s = 1$ coincides with the rank of the elliptic curve.

Keywords: Elliptic curves, Mordell's Theorem, Weierstrass.

CAPíTULO 1

La ley de grupo en una curva elíptica.

1. Rectas y cónicas racionales.

1.1. Las rectas racionales. Comenzemos por el caso más sencillo posible que es el de las rectas racionales, es decir, queremos resolver una ecuación de la forma

$$r : ax + by + c = 0, \tag{1}$$

con a, b y c racionales dados y a ó b distinto de cero.

Supongamos sin pérdida de generalidad que $a \neq 0$ entonces por cada valor racional de y tenemos

$$x = \frac{-by - c}{a} \tag{2}$$

luego tenemos parametrizado el conjunto solución

$$P = \left(\frac{-bt - c}{a}, t \right) \tag{3}$$

1.2. Las cónicas racionales. A continuación otro caso bien conocido y estudiado que es el de las cónicas racionales. Las cónicas racionales vienen dada por una ecuación de la forma

$$C : ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{4}$$

donde los coeficientes a, b, c, d, e y f son racionales dados y además a, b ó c es distinto de cero.

Antes de comenzar con este caso conviene hacer una observación sencilla, que es que si una recta racional r corta a una cónica racional C en un punto racional $P = (x_0, y_0)$ entonces la corta en general en otro punto que también tendrá coordenadas racionales. Veamos que queremos decir con esto, consideremos la ecuación de la cónica C como en (4) y para comenzar supongamos que el polinomio $ax^2 + bx + c$ no posea raíces racionales no nula, supongamos que el coeficiente de x en la recta r sea no nulo entonces podemos escribir la ecuación de r en la forma

$$x = ny + m, \tag{5}$$

donde $n \neq 0$, sustituyendo x de la ecuación (5) en la ecuación (4) obtenemos una ecuación para y de la forma

$$Ay^2 + By + C = 0,$$

con A, B y C racionales y $A = an^2 + bn + c \neq 0$ por la suposición de que $ax^2 + bx + c$ no tenia raíces no nulas, así que hay una segunda raíz y_0' que ha de ser también racional puesto que cumple $y_0 + y_0' = -B/A$ con y_0, A y B racionales, si llamamos $x_0' = ny_0' + m$ entonces el punto racional $P' = (x_0', y_0')$ es el otro punto de corte de r con C. En el caso que el polinomio $ax^2 + bx + c$ tenga una raíz racional no nula n entonces en este caso P es el único punto de corte (afin) de la recta con la cónica, en este caso definimos un nuevo

punto del infinito" $P' = [n : 1 : 0]$ y definimos este como el segundo punto de corte de r con C (esto se da cuando la recta r es una asíntota de C y este punto P' corresponde justamente a esa dirección asintótica).

En el caso que el coeficiente de x en la recta r sea nulo entonces la recta r es una recta vertical de la forma $y = k$ donde k es un racional fijo, al sustituir en (4) obtenemos una ecuación de segundo grado en x, $Ax^2 + Bx + C = 0$ donde $A = a$ con A, B y C racionales, en el caso que $a \neq 0$ entonces dicha ecuación posee otra raíz x_0' que también ha de ser racional puesto que $x_0 + x_0' = -B/a$ y el segundo punto de corte de r con C viene dado por $P' = (x_0', k)$ que es un punto racional. El único caso problematico en este caso viene dado cuando $a = 0$, es este caso P es el único punto (afin) de corte de r y C y definimos un nuevo punto del infinito" $P' = [1 : 0 : 0]$ y lo definimos como el segundo punto de corte de r y C.

Ahora supongamos que tenemos un punto racional P de C (no necesariamente una ecuación como (4) ha de tener puntos racionales, el problema de si una cónica posee o no un punto racionales lo discutiremos más adelante), consideremos una recta racional r que no pase por P y tal que r no esté contenida en C (para chequear esto último alcanza tomar tres puntos cualesquiera de r, si todos están en C entonces $r \subset C$).

Por cada punto racional $Q \in r$ (hallados, por ejemplo, como en (2)) consideremos la recta r_Q que pasa por P y Q, como pasa por dos puntos racionales, la recta es racional y corta a C en el punto racional P, luego por la observación previa ha de cortarla en un segundo punto racional que llamaremos Q', de esa manera podemos parametrizar los puntos racionales de la cónica C con los puntos racionales de r.

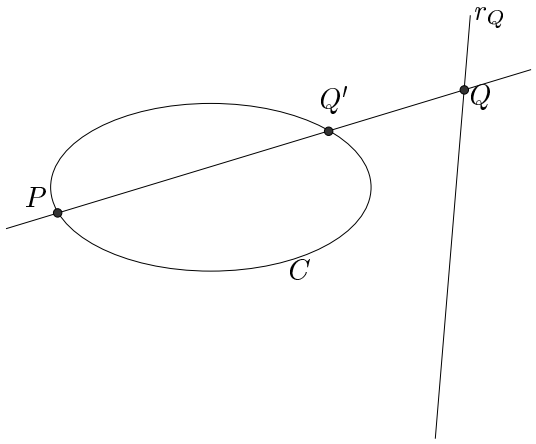


FIGURA 1. Obtención de los puntos racionales en una cónica.

El problema de ver si una cónica racional posee algún punto racional es un poco más complicado. Observemos que toda solución racional (x, y) de (4) puede escribirse en la forma $x = X/Z$ e $y = Y/Z$ con X, Y, Z enteros y $Z \neq 0$, sustituyendo en (4) y luego multiplicando ambos miembros por Z^2 obtenemos una ecuación homogenea en las variables X, Y y Z de segundo grado donde nos interesan las soluciones enteras no nulas. De esta forma puede usarse un teorema de Hasse que establece que una condición necesaria para la existencia de dicha solución es que exista solución real y solución p-ádica para todo primo

p, un teorema de Lagrange reduce esto último a probar un sistema finito de congruencias.

Veamos a continuación como encontrar todas las ternas pitagóricas hallando los puntos racionales de cierta cónica.

EJEMPLO 1.1. Ternas Pitagóricas:

Consideremos la cónica racional de ecuación

$$C : x^2 + y^2 = 1, \tag{6}$$

observemos que el punto racional $P = (-1, 0)$ pertenece a la cónica y elijamos como recta racional r para proyectar a la recta de ecuación $x = 0$.

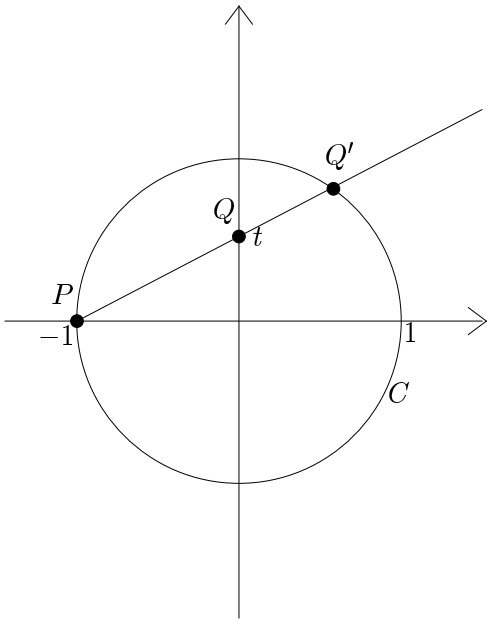


FIGURA 2. Puntos racionales en el círculo unidad.

Los puntos racionales sobre r son de la forma $Q = (0, t)$ con $t \in \mathbb{Q}$ los puntos (reales) sobre la recta PQ son de la forma

$$Q(\lambda) = P + \lambda(Q - P) = (-1, 0) + \lambda(1, t) = (-1 + \lambda, \lambda t),$$

donde $\lambda \in \mathbb{R}$, para que además $Q(\lambda) \in C$ λ debe verificar

$$(-1 + \lambda)^2 + \lambda^2 t^2 = 1,$$

o equivalentemente

$$(1 + t^2)\lambda^2 - 2\lambda = 0.$$

El valor $\lambda = 0$ corresponde al punto P, el otro punto de intersección Q' corresponde al valor de λ tal que $(1 + t^2)\lambda - 2 = 0$ que es

$$\lambda = \frac{1 + t^2}{2},$$

para ese valor de λ obtenemos los correspondientes valores de x e y:

$$x = \lambda - 1 = \frac{1-t^2}{1+t^2} \quad \text{e} \quad y = \frac{2t}{1+t^2} \tag{7}$$

a medida que t recorre los racionales el punto $Q' = (x, y)$ donde x e y son como en (7) recorre todos los puntos racionales del círculo C.

Una terna pitagórica es una terna de enteros (X, Y, Z) que son los lados de un triángulo rectángulo, es decir son enteros positivos y verifican

$$X^2 + Y^2 = Z^2. \tag{8}$$

Observemos que si (X, Y, Z) es una terna pitagórica y $n \in \mathbb{Z}^+$ entonces (nX, nY, nZ) también es una terna pitagórica. Una terna pitagórica se dice primitiva si $\text{mcd}(X, Y, Z) = 1$, si (X, Y, Z) es una terna pitagórica y $d = \text{mcd}(X, Y, Z)$ entonces $(X/d, Y/d, Z/d)$ es una terna pitagórica primitiva, pues está compuesta de enteros coprimos y además si dividimos ambos miembros de la ecuación (8) por d^2 obtenemos que

$$\left(\frac{X}{d}\right)^2 + \left(\frac{Y}{d}\right)^2 = \left(\frac{Z}{d}\right)^2,$$

lo que prueba que es una terna pitagórica, así que toda terna pitagórica proviene de una terna pitagórica primitiva así que alcanza con conocer estas últimas, las restantes se obtienen por una homotecia de razón entera.

Sea pues (X, Y, Z) una terna pitagórica primitiva, dividiendo ambos miembros de (8) por Z^2 obtenemos que

$$\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1,$$

por lo tanto $(X/Z, Y/Z)$ es un punto racional de la cónica $C : x^2 + y^2 = 1$, que por lo que acabamos de ver entonces

$$\frac{X}{Z} = \frac{1-t^2}{1+t^2}, \quad \frac{Y}{Z} = \frac{2t}{1+t^2}, \tag{9}$$

donde t recorre los racionales, pongamos $t = a/b$ con a y b enteros coprimos, además como X/Z e Y/Z son positivos tenemos que $t \in (0, 1)$, es decir a y b son positivos con $a < b$. Sustituyendo $t = a/b$ en (37)y multiplicando numerador y denominador de x e y por b^2 obtenemos que

$$\frac{X}{Z} = \frac{b^2-a^2}{b^2+a^2}, \quad \frac{Y}{Z} = \frac{2ab}{b^2+a^2}. \tag{10}$$

Si a y b son de distinta paridad entonces

$$\text{mcd}(b^2-a^2, b^2+a^2) = mcd(2b^2, b^2+a^2) = \text{mcd}(b^2, b^2+a^2) = \text{mcd}(b^2, a^2) = \text{mcd}(a, b)^2 = 1,$$

donde la segunda igualdad es porque si a y b son de distinta paridad entonces $b^2 + a^2$ es impar y por lo tanto coprimo con 2. Además tenemos

$$\text{mcd}(2ab, b^2 + a^2) = \text{mcd}(a, b^2 + a^2) \cdot \text{mcd}(b, b^2 + a^2) = \text{mcd}(a, b^2) \cdot \text{mcd}(b, a^2) = 1,$$

donde la última igualdad es porque si a y b no tienen factores comunes tampoco lo tendrán a y b^2 ni b y a^2. Luego las fracciones de (10) están escritas en forma irreducible, luego

por la coprimidad de X, Y y Z (observar que son coprimos dos a dos pues si dos de ellos comparten un factor, por la ecuación (8) el tercero también lo tendrá) tenemos que:

$$\begin{cases} X = b^2 - a^2 \\ Y = 2ab \\ Z = b^2 + a^2 \end{cases} \quad \text{con } a \text{ y } b \text{ coprimos, de distinta paridad y } b > a \tag{11}$$

Veamos que el caso en que $t = a/b$ con a y b coprimos impares ya viene contemplado en el caso anterior, en efecto, consideremos los enteros $m = (b+a)/2$ y $n = (b-a)/2$, en este caso tenemos:

$$\mathrm{mcd}(b^2 - a^2, b^2 + a^2) = \mathrm{mcd}(2b^2, b^2 + a^2) = \mathrm{mcd}(2, b^2 + a^2) = 2,$$

donde en el segundo igual se usó que b^2 y $b^2 + a^2$ son coprimos (se desprende facilmente de que a y b lo son), también tenemos que

$$\mathrm{mcd}(2ab, b^2 + a^2) = \mathrm{mcd}(2, b^2 + a^2) \cdot \mathrm{mcd}(a, b^2 + a^2) \cdot \mathrm{mcd}(b, b^2 + a^2) = 2 \cdot 1 \cdot 1 = 2,$$

así que la ecuación (10) implica en este caso que:

$$\begin{cases} X = \frac{b^2-a^2}{2} = 2\left(\frac{b+a}{2}\right)\left(\frac{b-a}{2}\right) = 2mn \\ Y = ab = \left(\frac{b+a}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2 = m^2 - n^2 \\ Z = \frac{b^2+a^2}{2} = \left(\frac{b+a}{2}\right)^2 + \left(\frac{b-a}{2}\right)^2 = m^2 + n^2 \end{cases}$$

además si $d|m$ y $d|n$ entonces $d|m + n = b$ y $d|m - n = a$ así que $d = 1$ lo cual prueba que m y n son coprimos, claramente $m > n$ y son de distinta paridad puesto que si $b = 2s + 1$ y $a = 2t + 1$ con s y t enteros entonces $m = s + t + 1$ y $n = s - t$ así que $m - n = 2t + 1$ que es impar. Luego este caso ya estaba contemplado en el caso en que a y b eran de distinta paridad, se chequea directamente que cada terna formada como en (10) conforma una terna pitagórica primitiva por lo que todas son como en (10).

2. La ley de grupo.

Llegó el turno a las cúbicas, la idea para conocer los puntos racionales sobre una cúbica se basa en una idea geométrica, una recta que pasa por dos puntos de una curva pasará por un tercero. De esa forma si partimos con una cantidad de puntos podemos a partir de este procedimiento en general encontrar cada vez más y más puntos.

Por ejemplo, partimos de una cúbica $\mathcal{C}$ definida sobre un cierto cuerpo $\mathbb{K}$ y consideremos el conjunto $E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : F(X, Y) = 0\}$ donde F es un polinomio de tercer grado con coeficientes en $\mathbb{K}$.

Consideremos la operación anteriormente descrita sobre $\mathcal{C}$,

$$* : \mathcal{C} \times \mathcal{C} \to \mathcal{C} : (P, Q) \mapsto P * Q$$

donde $P * Q$ denota el tercer punto de intersección de la recta que pasa por P y Q con la cúbica (si $P = Q$ tomamos la recta tangente a la cúbica por P y consideramos el otro punto de intersección con la cúbica).

Veamos que condiciones necesitamos para que la operación binaria $*$ esté bien definida, para comenzar tomemos dos puntos P y Q pertencecientes a $E(\mathbb{K})$ y consideremos la recta que pasa por ambos puntos $rX + sY + t = 0$ (observemos que como las coordenadas de P y Q están en $\mathbb{K}$ entonces también lo estarán los coeficientes r, s y t de la recta que pasa por ellos).

Como los coeficientes r y s de la recta no pueden ser ambos nulos, entonces es posible despejar una variable en función de la otra, supongamos que $s \neq 0$ entonces ponemos $Y = mX + n$ con $m = -r/s$ y $n = -t/s$. Sustituyendo en la ecuación del polinomio cúbico

$$F(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j = 0$$

que define a $\mathcal{C}$, tenemos que los posibles valores de X verifican una ecuación con coeficientes en $\mathbb{K}$ de la forma

$$AX^3 + BX^2 + CX + D = 0,$$

donde $A = dm^3 + cm^2 + bm + a$.

Supongamos primeramente que $A \neq 0$ entonces la ecuación de arriba tiene dos soluciones x_P y x_Q que corresponde a la coordenada en X de los puntos P y Q, en virtud de las relaciones entre coeficientes y raíces, la tercer raíz x verificará

$$\frac{-B}{A} = x_P + x_Q + x,$$

y por lo tanto $x \in \mathbb{K}$, luego $y = mx + n$ tambien pertences a $\mathbb{K}$ así que la recta que pasa por P y Q corta a la cúbica $\mathcal{C}$ en un tercer punto que también tiene sus dos coordenadas sobre $\mathbb{K}$.

Veamos ahora que sucede en el caso que al sustituir nos quede $A = dm^3 + cm^2 + bm + a = 0$. En este caso observemos que no hay tercer punto de corte en el plano afin $\mathbb{K}^2$, el tercer punto de corte corresponde a un punto del plano proyectivo con $Z = 0$, en efecto, consideremos las ecuaciones homogeneas de la recta que pasa por P y Q y de la cúbica $\mathcal{C}$:

$$\begin{cases} Y = mX + nZ \\ aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0 \end{cases}$$

Observando las intersecciones con la recta impropia $Z = 0$, obtenemos que las coordenadas $[x : y : 0]$ de tales puntos han de verificar:

$$\begin{cases} Y = mX \\ aX^3 + bX^2Y + cXY^2 + dY^3 = 0 \end{cases}$$

Como x e y no pueden ser ambos nulos, por la primer ecuación tenemos que $x \neq 0$ y por lo tanto podemos tomar un representante con $x = 1$ y tenemos que $y = m$, por otra parte como teniamos que $dm^3 + cm^2 + bm + a = 0$, entonces se verifica la segunda ecuación y por lo tanto tenemos un único punto en la intersección con $Z = 0$ dado por $[1 : m : 0]$ que está en $P^2(\mathbb{K})$ pues $m \in \mathbb{K}$. A partir de ahora consideraremos a la cúbica $\mathcal{C}$ con "los puntos del infinito" incluidos, esto es aquellos puntos con $Z = 0$ que verifican el polinomio homogeneo que define $\mathcal{C}$, explicitamente:

$$\mathcal{C}(K) = \{[x : y : z] \in P^2(\mathbb{K}) : F(X, Y, Z) = 0\}$$

donde F es un polinomio homogeneo de tercer grado y como es usual estamos identificando los puntos del proyectivo $[x : y : 1]$ con los puntos del plano afin via $[x : y : 1] \mapsto (x, y)$.

Necesitaremos además que $P * P$ esté bien definido para todo P lo cual equivale que en todo punto haya una única recta tangente, lo cual equivale a pedir que no hayan puntos singulares en la cúbica (puntos singulares son aquellos para los cuales $\nabla F(P) = 0$).

DEFINICIÓN 1.1. Una curva elíptica sobre $\mathbb{K}$ es un par $(E(\mathbb{K}), \mathcal{O})$ donde $E(\mathbb{K})$ es el conjunto de puntos del plano proyectivo $P^2(\mathbb{K})$ que verifican una ecuación del tipo:

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

donde F es un polinomio homogeneo de tercer grado con coeficientes en $\mathbb{K}$ sin puntos singulares y $\mathcal{O} \in E(\mathbb{K})$.[1]

Notación. Si $\mathbb{K} \subset \mathbb{L}$ son cuerpos, denotaremos por $E(\mathbb{L})$ a los puntos de $P^2(\mathbb{L})$ que verifican $F(X, Y, Z) = 0$, si el polinomio cúbico F tiene sus coeficientes en $\mathbb{K}$ diremos que la curva elíptica E está definida sobre $\mathbb{K}$ y lo notaremos por $E/\mathbb{K}$.

En resumen para que la operación $*$ esté bien definida es preciso definirla sobre una curva elíptica $E/\mathbb{K}$.

Algunas propiedades de $* : E \times E \to E$:

1. Es conmutativa, es decir $P * Q = Q * P$
2. Si $P * Q = R$ entonces $Q * R = P$ y $R * P = Q$.

Las demostraciones son inmediatas de la definición.

Lamentablemente esta operación no goza de las propiedades usuales que uno desearía como las que definen un grupo. En lugar de definir a $*$ como nuestra suma en una curva elíptica definiremos la suma que denotaremos $\oplus$ de la siguiente manera:

Comenzamos tomando un punto cualquiera en la curva que denotaremos por $\mathcal{O}$ y para todo par de puntos P y Q de E (no necesariamente distintos) definimos $P \oplus Q = (P * Q) * \mathcal{O}$.

[1] Este punto distinguido $\mathcal{O}$ es el que tomaremos como neutro de la ley de grupo de la curva elíptica

Geométricamente para obtener el punto $P \oplus Q$ se traza primero la recta que pasa por P y Q para obtener el tercer punto de corte de esta recta con E, que es $P * Q$, luego se traza la recta que pasa por este último punto y por $\mathcal{O}$ para obtener a $P \oplus Q$ al tercer punto de corte de está última recta con E (ver figura).

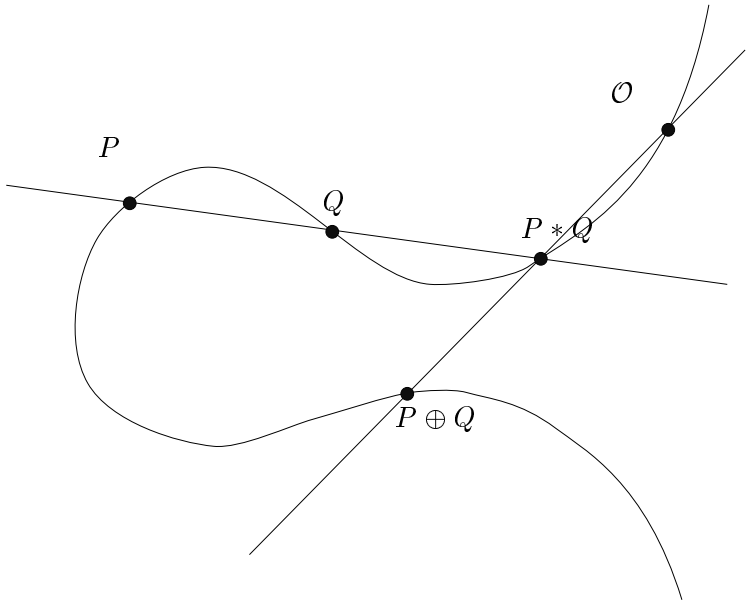


FIGURA 3. Ley de grupo en una curva elíptica.

Veamos que efectivamente la operación $\oplus$ dota a E de estructura de grupo abeliano cuyo neutro es $\mathcal{O}$.

Lo más fácil de verificar es la conmutatividad de $\oplus$, en efecto

$$P \oplus Q = (P * Q) * \mathcal{O} = (Q * P) * \mathcal{O} = Q \oplus P,$$

donde se ha utilizado la conmutatividad de $*$.

Veamos ahora que $\mathcal{O}$ juega el papel de neutro:

Sea $P \in E$ y consideremos $Q = P * \mathcal{O}$ tenemos que:

$$P \oplus \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = Q * \mathcal{O} = P$$

donde se ha utilizado la segunda propiedad de $*$.

Ahora veamos la existencia de opuesto:

Sea $P \in E$, consideremos $S = \mathcal{O} * \mathcal{O}$ y $P' = P * S$, tenemos que:

$$P \oplus P' = (P * P') * \mathcal{O} = S * \mathcal{O} = \mathcal{O}$$

y por lo tanto $P' = -P$ (también aquí se ha utilizado la propiedad 2 de $*$).

Ahora queda la más dificil por probar que es la asociatividad:

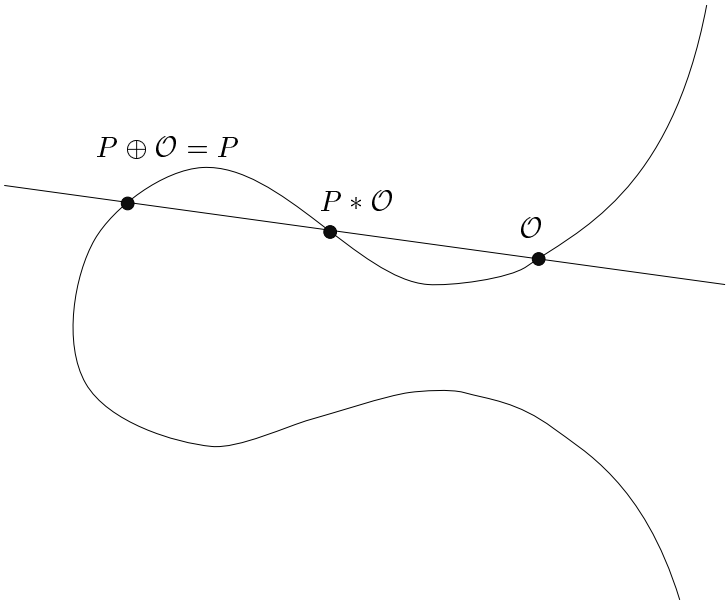


FIGURA 4. $\mathcal{O}$ como elemento neutro de la ley de grupo.

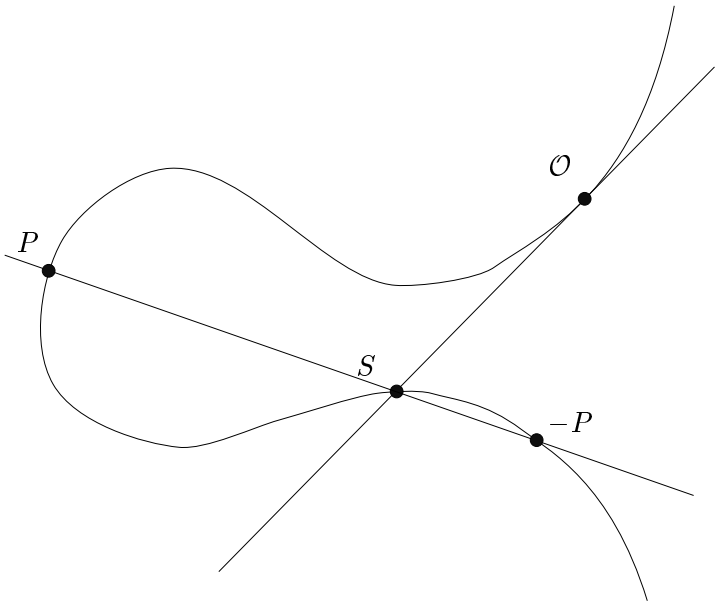


FIGURA 5. Obtención geométrica del opuesto.

Queremos probar que para P, Q y R perteneciente a E se cumple que $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$, para ello es suficiente probar que $(P \oplus Q) * R = P * (Q \oplus R)$ (basta luego aplicar $*\mathcal{O}$ de ambos lados de la igualdad para obtener la propiedad asociativa).

Usaremos el siguiente teorema:

Teorema: Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ son dos cúbicas definidas sobre $\mathbb{K}$ que se cortan en nueve puntos. Sea $\mathcal{C}$ otra cúbica definida sobre $\mathbb{K}$ que pasa por ocho de los nueve puntos de

intersección de $\mathcal{C}_1$ y $\mathcal{C}_2$ entonces pasa por el noveno.[2]

Veamos como probar la ley asociativa a partir de este teorema:

En efecto, sean P, Q y R puntos de la cúbica E y $\mathcal{O} \in E$ el punto especial que hemos elegido por neutro y consideremos los ocho puntos:

$$\mathcal{O}, P, Q, R, P * Q, P \oplus Q, Q * R, Q \oplus R \tag{12}$$

y también consideremos el punto de intersección de la recta que pasa por $Q \oplus R$ y por P con la que pasa por $P \oplus Q$ y por R.

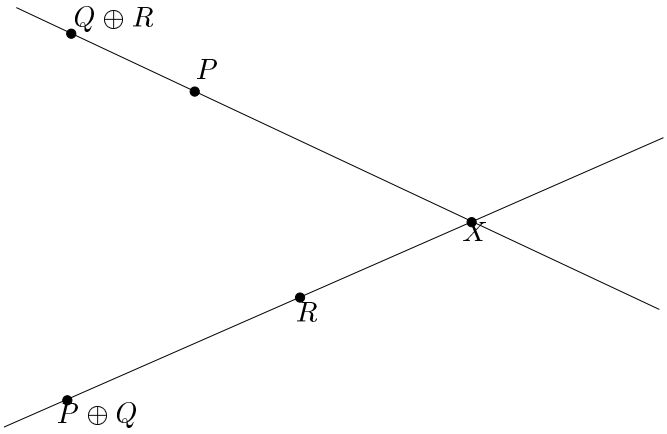


FIGURA 6. El punto X.

Consideremos las siguientes rectas:
r_1 = la recta que pasa por los puntos P, Q y $P * Q$.
s_1 = la recta que pasa por los puntos $\mathcal{O}, Q * R$ y $Q \oplus R$.
t_1 = la recta que pasa por los puntos $R, P \oplus Q$ y X.

y por otra parte:
r_2 = la recta que pasa por los puntos Q, R y $Q * R$.
s_2 = la recta que pasa por los puntos $\mathcal{O}, P \oplus Q$ y $P * Q$.
t_2 = la recta que pasa por los puntos $P, Q \oplus R$ y X.

Aplicamos ahora el teorema anterior con las cúbicas $\mathcal{C}_1 = r_1 s_1 t_1$,$\mathcal{C}_2 = r_2 s_2 t_2$ y $\mathcal{C}$ es nuestra curva elíptica inicial E. Tenemos que la cúbicas $\mathcal{C}_1$ y $\mathcal{C}_2$ se intersectan en 9 puntos que son los ocho mencionados en (12) y el punto X (no se pueden intersectar en más puntos pues coincidirian), E pasa por los ocho puntos de (12) así que por el teorema mencionado anteriormente ha de pasar por X, pero como $Q \oplus R, P, P \oplus Q$ y R también son puntos de E tenemos que $X = (Q \oplus R) * P = (P \oplus Q) * R$ como queriamos probar.

[2]Ver por ejemplo [**8**] pág 81.

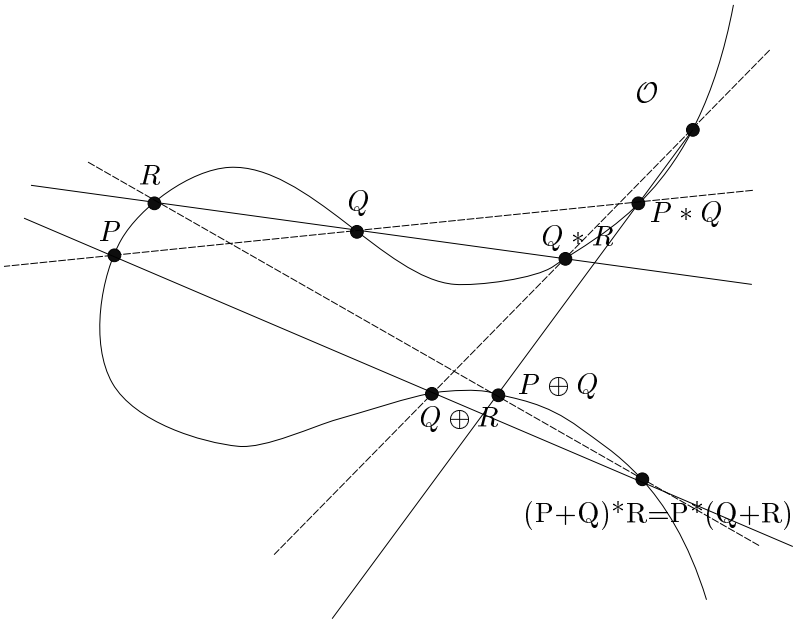


FIGURA 7. Propiedad asociativa de la ley de grupo en una curva elíptica.

3. Forma Normal de Weierstrass.

En este capítulo veremos que dada una curva elíptica sobre un cuerpo $\mathbb{K}$, definida por un polinomio de tercer grado, es posible mediante un cambio de coordenadas proyectivo ponerla en la siguiente forma:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \qquad \mathcal{O} = [0 : 1 : 0] \tag{13}$$

Cuando la ecuación que define la cúbica tiene la forma (13) decimos que E extá expresada en su forma normal de Weierstrass.

Si la característica del cuerpo $\mathbb{K}$ fuese distinta a 2 y 3 entonces es posible, completando cuadrados ponerla en la forma:

$$E : Y^2 = X^3 + aX + b \tag{14}$$

que llamaremos forma normal reducida de la curva elíptica E.

Comenzaremos con unos resultados previos elementales de geometría proyectiva.

3.1. Cambios de variables. Cuando realizamos un cambio de variable en una curva elíptica nos interesan cambios que preserven la estructura de grupo. De la forma en que está definida la ley de grupo, alcanza con que lleve rectas en rectas.

Veamos esto desde el plano proyectivo, a cada recta afin $r : aX + bY + c = 0$ con a y b no ambos nulos, le podemos hacer corresponder una única recta proyectiva $r^* : aX + bY + cZ = 0$.

Observemos que para $Z = 1$ obtenemos lo puntos de la recta r, con $Z = 0$ obtenemos un punto extra (punto impropio de la recta) $[b : -a : 0]$. De esa forma $r^* = r \cup \{[b : -a : 0]\}$

donde estamos identificando el punto del plano afin (x, y) con el punto $[x : y : 1]$ del plano proyectivo.

Observemos además que cada recta proyectiva puede ponerse en correspondencia con un plano que pasa por el origen en el espacio afin tridimensional $\mathbb{K}^3$ (haciendole corresponder el plano con la misma ecuación). Bajo esta correspondencia, a todo cambio de coordenadas proyectivo que lleve rectas proyectivas en rectas proyectivas, les corresponden transformaciones en $\mathbb{K}^3$ que lleve planos en planos, que son justamente las transformaciones lineales de $\mathbb{K}^3$, para que sea cambio de coordenadas, le pediremos además que sean biyectivos a los mapas lineales.

La siguiente proposición nos será de gran utilidad para realizar los cambios de coordenadas en la próxima sección.

PROPOSICIÓN 1.2. *Si r, s y t son tres rectas proyectivas no concurrentes entonces existe un cambio de coordenadas $T : P^2(\mathbb{K}) \longrightarrow P^2(\mathbb{K})$ tal que:*

$$\begin{aligned} T(r) &= \{[x : y : z] \in P^2(\mathbb{K}) : x = 0\} \\ T(s) &= \{[x : y : z] \in P^2(\mathbb{K}) : y = 0\} \\ T(t) &= \{[x : y : z] \in P^2(\mathbb{K}) : z = 0\} \end{aligned}$$

DEMOSTRACIÓN. Por las correspondencias anteriormente descritas, que las rectas proyectivas r, s y t sean no concurrentes es equivalente a pedirle que sus respectivos planos afines solo se corten en el origen (los puntos proyectivos corresponden con rectas afines).

Denotemos por $\widehat{r}, \widehat{s}$ y $\widehat{t}$ a sus correspondientes planos de $\mathbb{K}^3$, consideremos v_1, v_2 y v_3 vectores no nulos de $\widehat{r} \cap \widehat{s}, \widehat{r} \cap \widehat{t}$ y $\widehat{s} \cap \widehat{t}$ respectivamente. El hecho que $\widehat{r} \cap \widehat{s} \cap \widehat{t} = \{0\}$ es equivalente a que el conjunto de vectores $\{v_1, v_2, v_3\}$ sea linealmente independientes, luego existe una única transformación lineal $T : \mathbb{K}^3 \longrightarrow \mathbb{K}^3$ tal que:

$$\begin{cases} T(v_1) = (0, 0, 1) \\ T(v_2) = (0, 1, 0) \\ T(v_3) = (1, 0, 0) \end{cases}$$

Esta T cumple:

$$\begin{aligned} T(\widehat{r}) &= \mathbb{K}T(v_1) + \mathbb{K}T(v_2) = \mathbb{K}(0, 0, 1) + \mathbb{K}(0, 1, 0) = \{(x : y : z) \in P^2(\mathbb{K}) : x = 0\} \\ T(\widehat{s}) &= \mathbb{K}T(v_1) + \mathbb{K}T(v_3) = \mathbb{K}(0, 0, 1) + \mathbb{K}(1, 0, 0) = \{(x : y : z) \in P^2(\mathbb{K}) : y = 0\} \\ T(\widehat{t}) &= \mathbb{K}T(v_2) + \mathbb{K}T(v_3) = \mathbb{K}(0, 0, 1) + \mathbb{K}(0, 1, 0) = \{(x : y : z) \in P^2(\mathbb{K}) : x = 0\} \end{aligned}$$

lo cual prueba la propisición via la correspondencia entre planos afines y rectas proyectivas. □

COROLARIO 1.3. *Si r y s son dos rectas proyectivas distintas entonces existe un cambio de coordenadas tal que $T(r) = \{[x : y : z] : z = 0\}$ y $T(s) = \{[x : y : z] : x = 0\}$.*

DEMOSTRACIÓN. Considerar una tercer recta que no pase por $r \cap s$ y aplicar la proposición anterior. □

3.2. Forma Normal de Weierstrass. Sea $(E, \mathcal{O})$, donde E es una curva elíptica con un punto distinguido $\mathcal{O} \in E$, supongamos que E viene dada por los ceros de un polinomio sobre $\mathbb{K}$:

$$E(\mathbb{K}) = \{[U : V : W] \in P^2(\mathbb{K}) : F(U, V, W) = 0$$

donde F es un polinomio homogeneo de tercer grado con coeficientes en $\mathbb{K}$.

Queremos encontrar un cambio de coordenadas, o sea una transformación lineal biyectiva $T : \mathbb{K}^3 \longrightarrow \mathbb{K}^3$ tal que $T(\mathcal{O}) = [0 : 1 : 0]$ y tal que la curva elíptica E' definida por la ecuación:

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

donde $F^T = F \circ T^{-1}$, esté en su forma normal de Weierstrass.

Separaremos en dos casos, según $\mathcal{O}$ sea un punto de inflexión o no.

Caso 1. $\mathcal{O}$ es un punto de inflexión de E.

Consideremos t la recta tangente a la cúbica E que pasa por $\mathcal{O}$ y s una recta que pasa por $\mathcal{O}$ y otro punto de E distinto de $\mathcal{O}$.

Por el colorario de la Proposición 1.2, es posible elegir un cambio de coordenadas $T : P^2(\mathbb{K}) \longrightarrow P^2(\mathbb{K})$ tales que:

1. T(t): Z=0
2. T(s): X=0

como lo muestra la siguiente figura:

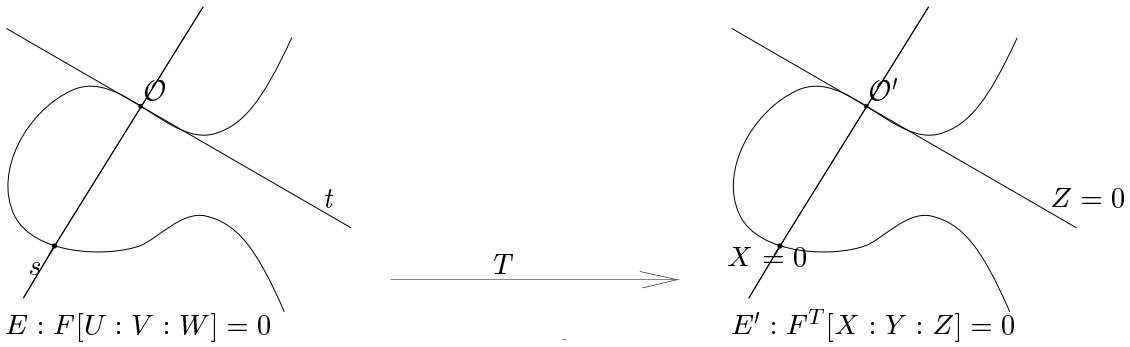


FIGURA 8. Cambio de variables - primer caso.

Comenzemos escribiendo la ecuación genérica para F^T:

$$FT^{-1}(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0 \tag{15}$$

Sea $\mathcal{O}' = T(\mathcal{O})$, como $\mathcal{O}' = (Z = 0) \cap (X = 0)$ entonces $\mathcal{O}' = [0 : 1 : 0]$.

Como $Z = 0$ es tangente a E' en $\mathcal{O}'$ siendo $\mathcal{O}' = [0 : 1 : 0]$ de inflexión, tenemos que $E' \cap \{Z = 0\} = \{\mathcal{O}', \mathcal{O}', \mathcal{O}'\}$ y por lo tanto la ecuación:

$$aX^3 + bX^2Y + cXY^2 + dY^3 = 0$$

tiene un cero triple en $X = 0$, luego:

$$a \neq 0 \text{ y } b = c = d = 0 \tag{16}$$

La ecuación de la curva E' toma la siguiente forma:

$$aX^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0 \tag{17}$$

Ahora cortemos E' con la recta $X = 0$, los tres puntos de corte verifican la ecuación:

$$gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0 \tag{18}$$

Con $Z = 0$ tenemos el punto $[0 : 1 : 0]$ que es simple puesto que la mayor potencia de Z que aparece en el término de la izquierda de la ecuación (18) es uno.

Con $Z = 1$ debemos tener dos puntos más, las coordenadas en Y de esos puntos son las raices de la ecuación $gY^2 + iY + j = 0$, por lo tanto $g \neq 0$.

Finalmente, dado que a y g son no nulos, podemos multiplicar por a^2g^3 ambos miembros de (17) y reagrupar términos obteniendo una ecuación equivalente:

$$(agX)^3 + eg(agX)^2 + f(agX)(ag^2Y) + (ag^2Y)^2 + hag^2(agX) + iag(ag^2Y) + a^2g^3j = 0 \tag{19}$$

Realizamos finalmente el cambio de variables:

$$\begin{cases} X_1 = -agX \\ Y_1 = ag^2Y \end{cases}$$

Obteniendo una nueva curva elíptica cuya ecuación toma la forma:

$$-X_1^3 - A_2X_1^2 + A_1X_1Y_1 + Y_1^2 - A_4X_1 + A_3Y_1 - A_6 = 0$$

o equivalentemente:

$$Y_1^2 + A_1X_1Y_1 + A_3Y_1 = X_1^3 + A_2X_1^2 + A_4X_1 + A_6$$

que es la forma de Weierstrass.

Ahora veamos el segundo caso, en que $\mathcal{O}$ no es un punto de inflexión:

Caso 2. $\mathcal{O}$ no es un punto de inflexión de E.

Este caso es un poco más dificil que el anterior, aunque sigue las mismas ideas. Para comenzar trazemos la recta r tangente a E por $\mathcal{O}$, esta recta corta a otro punto distinto de $\mathcal{O}$ con multiplicidad 1 (pues $\mathcal{O}$ no es de inflexión), llamémosle $P = \mathcal{O} * \mathcal{O}$ al otro punto de contacto distinto de $\mathcal{O}$. Por el punto P trazamos la recta s tangente a E' y consideremos $Q = P * P$ el tercer punto de corte de s con E que denotaremos por l. Observemos que $Q \neq \mathcal{O}$ pues si $P * P = \mathcal{O}$ entonces $P = P * \mathcal{O}$, pero como $\mathcal{O} * \mathcal{O} = P$ tenemos que $\mathcal{O} = P * \mathcal{O}$, y por lo tanto $P = \mathcal{O}$ lo cual es absurdo pues $\mathcal{O}$ no es de inflexión.

Ahora por la proposición 1.2, es posible elegir un cambio de coordenadas $T : P^2(\mathbb{K}) \longrightarrow P^2(\mathbb{K})$ tal que:

1. T(r): Z=0
2. T(s): X=0
3. T(l): Y=0

como lo muestra la siguiente figura:

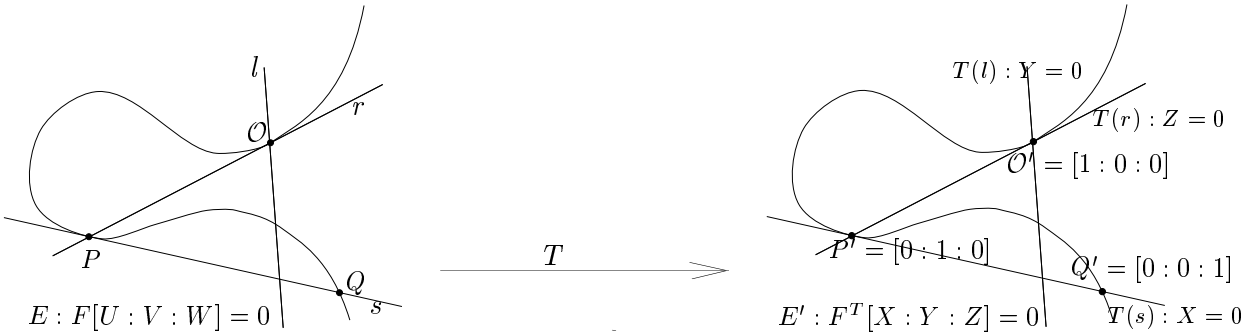


FIGURA 9. Cambio de variables - segundo caso.

Comenzemos escribiendo la ecuación genérica para F^T:

$$FT^{-1}(X,Y,Z) = aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3 = 0 \tag{20}$$

Sean $\mathcal{O}' = T(\mathcal{O})$, $P' = T(P)$ y $Q' = T(Q)$ tenemos que $\mathcal{O}' = (Z = 0) \cap (X = 0) = [0 : 1 : 0]$, $P' = (Z = 0) \cap (X = 0)$ y $Q' = (X = 0) \cap (Y = 0)$.

Ahora cortemos E' con las rectas $X = 0$, $Y = 0$ y $Z = 0$ para sacar relaciones entre los coeficientes:

$E \cap \{Z = 0\} : aX^3 + bX^2Y + cXY^2 + dY^3 = 0.$

$Z = 0$ corta a E' en $[1 : 0 : 0]$ con multiplicidad 2 así que $Y = 0$ es raíz doble de $a + bY + cY^2 + dY^3 = 0$, luego $a = b = 0$ y $c \neq 0$.

$Z = 0$ corta a E' en $[0 : 1 : 0]$ con multiplicidad 1 así que $X = 0$ es raíz simple de $aX^3 + bX^2 + cX + d = 0$ de donde $d = 0$ y $c \neq 0$.

$E \cap \{Y = 0\} : eX^2Z + hXZ^2 + jZ^3 = 0.$

$Y = 0$ corta a E' en $[1 : 0 : 0]$ con multiplicidad 1 así que $Z = 0$ es raíz doble de $eZ + hZ^2 + jZ^3 = 0$, luego $e \neq 0$.

$Y = 0$ corta a E' en $[0 : 0 : 1]$ con multiplicidad 1 así que $X = 0$ es raíz simple de $eX^2 + hX + j = 0$ de donde $j = 0$ y $h \neq 0$.

$E \cap \{X = 0\} : gY^2Z + iYZ^2 = 0.$

$X = 0$ corta a E' en $[0 : 1 : 0]$ con multiplicidad 2 así que $Z = 0$ es raíz doble de $gZ + iZ^2 = 0$, luego $g = 0$ y $i \neq 0$.

$X = 0$ corta a E' en $[0 : 0 : 1]$ con multiplicidad 1 así que $Y = 0$ es raíz simple de $gY^2 + iY = 0$ de donde $i \neq 0$.

Así que la ecuación para E' toma la forma:

$$cXY^2 + eX^2 + fXY + hX + iY = 0 \tag{21}$$

donde c e i son escalares no nulos.

Multiplicando por X ambos miembros de la ecuación (21) nos queda:

$$c(XY)^2 + eX^3 + fX(XY) + hX^2 + i(XY) = 0 \tag{22}$$

realizando el cambio de variables:

$$\begin{cases} U = X \\ V = XY \end{cases} \tag{23}$$

Obtenemos:

$$cV^2 + eU^3 + fUV + hU^2 + iV = 0 \tag{24}$$

o equivalentemente:

$$cV^2 + fUV + iV = (-e)U^3 + (-h)U^2$$

que es está en la forma normal de Weierstrass (en las variables U y V).

Observemos que el cambio de variables (23) no es proyectivo así podria no preservar la estructura de grupo en la cúbica, para demostrar que preserva podemos tomar dos puntos de la cúbica definida por la ecuación (21) $P = [X_1 : Y_1 : Z_1]$ y $Q = [X_2 : Y_2 : Z_2]$, calcular $P \oplus Q = [X_3 : Y_3 : Z_3]$ y probar que $P' = [X_1 : X_1Y_1 : Z_1]$ y $Q' = [X_2 : X_1Y_2 : Z_2]$ verifican $P' \oplus Q' = [X_3 : X_3Y_3 : Z_3]$ donde esta última suma se realiza para la cúbica definida por la ecuación (24).[3]

3.3. Forma Normal reducida. En la sección anterior vimos que toda curva elíptica puede llevarse a travez de un cambio de coordenadas que preserva la ley de grupo a una ecuación de la forma:

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad \mathcal{O} = [0 : 1 : 0] \tag{25}$$

denominada la ecuación normal de Weierstrass de la curva.

En el caso en que la característica de $\mathbb{K}$ sea distinta de 2 entonces se puede dividir entre 2 así que podemos considerar el cambio de variable Y por $Y - 1/2(a_1x + a_3)$ y la ecuación (25) nos queda:

$$Y^2 - (a_1X + a_3)Y + \frac{1}{4}(a_1X + a_3)^2 + (a_1X + a_3) = X^3 + a_2X^2 + a_4X + a_6$$

$$Y^2 = X^3 + (a_2 - a_1^2/4)X^2 + (a_4 - a_1a_3/2)X + a_6 - a_3^2/4$$

es decir toma la forma:

$$Y^2 = X^3 + aX^2 + bX + c \tag{26}$$

Ahora bien, si la característica de $\mathbb{K}$ fuese además distinta de 3 podemos dividir entre 3 y considerar el cambio de variable que cambia X por $X - a/3$, haciendo este cambio en la

[3] Ver [**1**]

ecuación (26) logramos eliminar el término en X^2 puesto que el nuevo coeficiente de X^2 es ahora $-3 \cdot a/3 + a = 0$ y la ecuación toma la forma:

$$Y^2 = X^3 + aX + b$$

que llamaremos forma normal reducida.

4. Fórmulas explícita para la ley de grupo.

En esta sección consideremos una curva elíptica sobre un cuerpo $\mathbb{K}$ expresada de la forma de Weiestrass (forma normal reducida)

$$E : Y^2 = X^3 + aX + b \quad a, b \in \mathbb{K}.$$

Recordemos que toda curva elíptica se podía llevar a una de este tipo mediante transformaciones birracionales que preservan la ley de grupo de la cúbica y que además llevaban el cero al punto $[0 : 1 : 0] \in P^2(\mathbb{K})$, por lo tanto este será nuestro cero en la forma normal reducida que a partir de ahora lo notaremos por $\mathcal{O}$.

Observemos que $\mathcal{O}$ resulta un punto de inflexión de la curva, pues si $[x : y : z] \in E \cap \{Z = 0\}$ entonces $z = 0$ y como está en la cúbica $y^2z = x^3 + axz^2 + bz^3$ por lo tanto $0 = x^3$, es decir $x = 0$ por lo tanto $Z = 0$ es la tangente a la curva elíptica en $[x : y : z] = [0 : 1 : 0] = \mathcal{O}$ el cual resulta ser un punto triple de la cúbica. En particular tenemos que $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

Fórmula para el opuesto.

Sea $P = (x_1, y_1) = [x_1 : y_1 : 1] \in E : Y^2 = X^3 + aX + b$, veamos quien es $-P$:

$$(-P) \oplus P = \mathcal{O} \Leftrightarrow ((-P) * P) * \mathcal{O} = \mathcal{O} \Leftrightarrow (-P) * P = \mathcal{O} \Leftrightarrow (-P) = P * \mathcal{O}.$$

Donde la segunda equivalencia es porque $\mathcal{O}$ es de inflexión (i.e $\mathcal{O} * \mathcal{O} = \mathcal{O}$). Pero $\{X = x_1Z\} \cap E = \{[x_1 : y_1 : 1], [x_1 : -y_1 : 1], [0 : 1 : 0]\}$, por lo tanto $-(x_1, y_1) = (x_1, -y_1)$.

Fórmula para la duplicación.

Sea $P = (x_1, y_1) = [x_1 : y_1 : 1] \in E : Y^2 = X^3 + aX + b$, veamos quien es $2P$: Observemos primero que si $2P = \mathcal{O}$ entonces $P = (x_1, 0)$, en efecto $P \oplus P = \mathcal{O} \Leftrightarrow P * P = \mathcal{O} * \mathcal{O} = \mathcal{O} \Leftrightarrow P = P * \mathcal{O} = -P$, es decir $(x_1, y_1) = (x_1, -y_1)$ por lo tanto $y_1 = 0$.

Para el caso en que $y_1 \neq 0$ como la recta $X = x_1$ no puede ser tangente a E (pues de serlo cortaría a la cúbica en 4 puntos que son x (doble), $-x$ y $\mathcal{O}$ lo cual es imposible), entonces la recta tangente será de la forma $y = mx + n$, y por lo visto anteriormente $2x \neq \mathcal{O}$, así que podemos ponerlo en la forma $2x = (x_0, y_0)$

La pendiente de esta recta debe coincidir con la pendiente de la cúbica, por lo tanto derivando formalmente tenemos $2YY' = (3X^2 + a)X'$ como E es no singular,para puntos con $Y \neq 0$ la pendiente viene dada por $\frac{Y'}{X'} = \frac{3X^2+a}{2Y}$, es decir $m = \frac{3x_1^2+a}{2y_1}$.
Las coordenadas en X de los puntos de corte de la recta $Y = mX + n$ con $E : Y^2 = X^3 + aX + b$ verificarán

$$(mX + n)^2 = X^3 + aX + b,$$

o lo que es lo mismo:

$$X^3 - m^2X^2 + (a - 2mn)X + b - n^2 = 0,$$

que tendrá por raíces x_1 (doble) y x_0, por la relación entre coeficientes y raíces tenemos que $2x_1 + x_0 = m^2$ de donde

$$x_0 = m^2 - 2x_1 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = \frac{3x_1^4 + 6ax_1^2 + a^2 - 8x_1y_1^2}{4y_1^2}.$$

Como $P \in E$, tenemos que $y_1^2 = x_1^3 + ax_1 + b$, sustituyendo arriba y haciendo cuentas nos queda

$$x_0 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3 + ax_1 + b)}.$$

Para calcular y_0 necesitariamos conocer n, como $P \in Y = mX + n$ entonces $n = y_1 - mx_1$, luego

$$y_0 = mx_0 + n = mx_0 + y_1 - mx_1 = m(x_0 - x_1) + y_1 = \frac{3x_1^2 + a}{2y_1}(x_0 - x_1) + y_1.$$

como ya calculamos x_0 podemos sutituirla en la ecuación y luego de algunas cuentas obtenemos

$$y_0 = \frac{x_1^6 + 5ax_1^4 + 20bx_1^3 - 5a^2x_1^2 - 4abx_1 - a^3 - 8b^2}{(2y_1)^3}.$$

Fórmula para la suma.

Sean $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E : Y^2 = X^3 + aX + b$, veamos quien es $P_1 + P_2$.

Observemos primero que si $P_1 + P_2 = \mathcal{O} \Rightarrow P_1 = -P_2 \Rightarrow (x_1, y_1) = (x_2, -y_2)$ luego $x_1 = x_2$.

Si $x_1 = x_2$ como $X = x_1 Z \cap E = \{(x_1, y_1), (x_1, -y_1), \mathcal{O}\}$ solo puede pasar que $y_1 = y_2$ o que $y_1 = -y_2$; en el primer caso tenemos $P_1 = P_2$ y podemos aplicar la fórmula de duplicación, en el segundo caso $P_1 = -P_2$ y tenemos $P_1 + P_2 = \mathcal{O}$.

Ahora veamos que pasa en el caso en que $x_1 \neq x_2$, por lo que acabamos de ver $P_1 \oplus P_2 \neq \mathcal{O}$ y por lo tanto podemos poner $P_1 \oplus P_2 = (x_0, y_0)$.

Si la recta $Y = mX + n$ pasa por $P_1 = (x_1, y_1)$ y por $P_2 = (x_2, y_2)$ entonces tenemos que $m = \frac{y_2 - y_1}{x_2 - x_1}$ y $n = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}$.

Al igual que antes, las X-coordenadas de los puntos de corte de la recta $Y = mx + n$ con la cúbica E verifican $(mX + n)^2 = x^3 + aX + b$ que tiene raíces x_1, x_2 y x_0, por la relación entre coeficientes y raíces $x_0 + x_1 + x_2 = m^2$ y por lo tanto $x_0 = m^2 - x_1 - x_2$, sustituyendo m y n, luego de operar nos queda

$$x_0 = \frac{x_1x_2^2 + x_1^2x_2 - 2y_1y_2 + a(x_1 + x_2) + 2b}{(x_1 - x_2)^2}$$

Y finalmente usando que $(x_0, y_0) \in Y = mX + n$ nos queda

$$y_0 = mx_0 + n = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)x_0 + \frac{x_1y_2 - x_2y_1}{x_1 - x_2} = \frac{(y_2 - y_1)x_0 + x_2y_1 - x_1y_2}{x_2 - x_1}$$

5. Ejemplos.

Para finalizar esta sección presentaremos un par de problemas.

El primero de ellos es un caso particular del Último Teorema de Fermat, más precisamente veremos el caso de exponente 4. Se cree que el propio Fermat tenía una demostración para este caso, la prueba que daremos consiste en utilizar un método llamado método del descenso infinito muy utilizado por Fermat para resolver algunas ecuaciones diofánticas y veremos como se interpreta este problema con curvas elíptica. Me parece un ejemplo conveniente porque nos va a ayudar a tener un poco más de idea para la prueba del Teorema de finitud de Mordell.

El segundo trata de un problema milenario que es el de los números congruentes, que al fin pudo ser resuelto utilizando algunos resultados sobre curvas elíptica. No daremos la solución al problema, pero diremos como se interpreta este en términos de curvas elípticas.

Para ambos ejemplos resulta conveniente recordar el resultado sobre ternas pitagóricas primitivas, que dice que si a, b y c son enteros positivos tales que $a^2 + b^2 = c^2$ con $\mathrm{mcd}(a, b) = 1$ y a impar entonces:

$$\begin{cases} a = m^2 - n^2 \\ b = 2mn \\ c = m^2 + n^2 \end{cases}$$

para algunos enteros positivos m y n, con $m > n$ coprimos y de distinta paridad.

Ejemplo 1.2. Las únicas soluciones de la ecuación diofántica $X^4 + Y^4 = Z^4$ son las triviales (es decir aquellas en las que $XY = 0$).

Observemos que si (x, y, z) fuese una solución no trivial de

$$X^4 + y^4 = Z^4,$$

entonces (x, y, z^2) sería una solución no trivial de

$$X^4 + Y^4 = Z^2. \tag{27}$$

Luego alcanza probar que la ecuación (27) no posee soluciones no triviales.

Supongamos que (x, y, z) fuese una solución no trivial de (27), podemos suponer que $\mathrm{mcd}(x, y) = 1$, pues si $\mathrm{mcd}(x, y) = d$, luego $\mathrm{mcd}(x/d, y/d) = 1$ y la tripleta $(x/d, y/d, z/d^2)$ verifica (1) puesto que $(x/d)^4 +^(y/d)^4 = (x^4 + y^4)/d^4 = z^2/d^4 = (z/d^2)^2$ (observar que como $d^4 | x^4 + y^4 = z^2$ entonces $d^2 | z$).

Como $(x^2)^2 + (y^2)^2 = z^2$ y $\mathrm{mcd}(x^2, y^2) = 1$ (sin perdida de generalidad podemos suponer que x es impar) entonces existen enteros m y n con $m > n$ coprimos y de distinta

paridad tal que:

$$\begin{cases} x^2 = m^2 - n^2 \\ y^2 = 2mn \\ z = m^2 + n^2 \end{cases}$$

Como $\text{mcd}(m,n) = 1$ entonces $\text{mcd}(n,x) = 1$ pues $n^2 + x^2 = m^2$, luego existen enteros a y b con $a > b$ coprimos y de distinta paridad tal que:

$$\begin{cases} x = a^2 - b^2 \\ n = 2ab \\ m = a^2 + b^2 \end{cases}$$

Luego tenemos que $y^2 = 2mn = 4ab(a^2 + b^2)$ y como $\text{mcd}(a,b) = 1$ resulta que a, b y $a^2 + b^2$ son coprimos dos a dos, luego cada uno debe ser cuadrado perfecto, es decir, existen r y s enteros positivos tales que $a = r^2$, $b = s^2$ y $a^2 + b^2 = t^2$, por lo tanto $r^4 + s^4 = t^2$. Si $rs = 0 \Rightarrow ab = 0 \Rightarrow n = 0 \Rightarrow y = 0$, pero esto no puede ser porque (x,y,z) era una solución no trivial, por lo tanto (r,s,t) sería otra solución no trivial de (27) con $\text{máx}\{x,y\} > \text{máx}\{r,s\} > 0$ (pues $y^2 = 4ab(a^2+b^2) = 4r^2s^2(r^4+s^4) > (rs)^2 \geq \text{máx}\{r,s\}^2$).

Repitiendo este proceso construiriamos una sucesión infinita de enteros positivos estrictamente decreciente, lo cual es imposible y por lo tanto (27) no puede tener soluciones no triviales.

Ahora veamos como se interpreta todo esto en términos de curvas elípticas.

Consideremos la supuesta solución (x,y,z) de (27) y la solución (r,s,t) construida a partir de ella. Sean también m, n, p y q como antes.

Como $x^4 + y^4 = z^2$ entonces $(x/y)^4 + 1 = (z/y^2)^2$, definimos los racionales $M = x/y$ y $N = z/y^2$, luego $M^4 + 1 = N^2$ y por lo tanto $(M^2 + N)(M^2 - N) = 1$ en particular $N - M^2 \neq 0$ y definimos $P = (x_1, y_1)$ donde $x_1 = \frac{2}{N-M^2}$ y $y_1 = \frac{4M}{N-M^2}$, podemos despejar N y M en función de x_1 e y_1 y nos queda que $M = \frac{y_1}{2x_1}$ y $N = \frac{y_1^2+8x_1}{4x_1^2}$, sustituyendo estos valores en $M^4 + 1 = N^2$ y luego de operar nos queda $y_1^2 = x_1^3 - 4x_1$ es decir acabamos de asociarle a cada solución no trivial de (1) un punto $(M,N) \in \mathbb{Q}^2$ que verifica $M^4 + 1 = N^2$ y a estos últimos los pusimos en biyección con los puntos racionales sobre la curva elíptica $Y^2 = X^3 - 4X$ distintos del origen.

Podemos repetir el proceso partiendo esta vez de la solución no trivial de (1) (r,s,t) primero haciéndole corresponder $(A,B) \in \mathbb{Q}^2$ dados por $A = r/s$ y $B = t/s^2$, y luego a este último, el punto (r_1, s_1) sobre $Y^2 = X^3 - 4X$ dado por $(r_1, s_1) = (\frac{2}{B-A^2}, \frac{2A}{B-A^2})$ (la inversa en este caso nos queda $(A,B) = (\frac{s_1}{2r_1}, \frac{s_1^2+8r_1}{4r_1^2})$). Ahora veamos que relación hay entre (x_1, y_1) y (r_1, s_1). Como $x_1 = \frac{2}{N-M^2}$, comenzemos por calcular $N - M^2$:

$$N - M^2 = (z/y^2) - (x/y)^2 = \frac{z - x^2}{y^2} = \frac{(n^2 + m^2) - (m^2 - n^2)}{2mn}$$

$$= n/m = \frac{2ab}{a^2 + b^2} = \frac{2r^2s^2}{r^4 + s^4} = \frac{2(r/s)^2}{(r/s)^4 + 1} = \frac{2A^2}{A^4 + 1}.$$

Asi que hay que calcular A^2:

$$A^2 = \frac{s_1^2}{4r_1^2} = \frac{r_1^3 - 4r_1}{4r_1^2} = \frac{r_1^2 - 4}{4r_1}.$$

Finalmente podemos dejar x_1 en función de r_1:

$$x_1 = \frac{2}{N - M^2} = \frac{A^4 + 1}{A^2} = \frac{(\frac{r_1^2-4}{4r_1}^2 + 1)}{\frac{r_1^2-4}{4r_1}} = \frac{(r_1^2 - 4)^2 + (4r_1)^2}{(r_1^2 - 4)(4r_1)} = \frac{r_1^4 + 8r_1^2 + 16}{4r_1^3 - 16r_1}.$$

Pero está última es justo la expresión de la coordenada X del punto $2(r_1, s_1)$, eso quiere decir que el punto $(x_1, y_1) = \pm 2(r_1, s_1)$. O sea el método del descenso en este caso construye a partir de un punto P, otro punto "$\pm\frac{P}{2}$".

Antes de pasar al siguiente ejemplo, sería bueno observar que en la asociación hecha anteriormente entre soluciones no triviales de $X^4 + Y^4 = Z^2$ y puntos racionales sobre la curva elíptica $E : Y^2 = X^3 - 4X$ lo único que hemos usado es la descomposición única en productos de primos en $\mathbb{Z}$, así que esta construcción puede generalizarse a un dominio factorial cualquiera A, es decir podemos realizar la anterior construcción para asociar soluciones no triviales en A de $X^4 + Y^4 = Z^2$ con puntos sobre la curva elíptica $E(\mathbb{K}) : Y^2 = X^3 - 4X$ (donde en este caso $\mathbb{K}$ sería el cuerpo de fracciones de A), si bien la demostración de la no existencia de soluciones no triviales ya no va a valer para A (porque aquí hemos usado el orden de $\mathbb{Z}$) sin embargo sigue valiendo la construcción del punto $\pm\frac{P}{2}$ a partir de un punto P de la curva elíptica, y este nuevo punto también estará asociado a otra solución no trivial de la ecuación de $X^4 + Y^4 = Z^4$.

EJEMPLO 1.3. **(Números congruentes).**

DEFINICIÓN 1.4. Un racional positivo q se dice que es congruente si es igual al área de un triangulo rectángulo con lados racionales, es decir, tales que existan a, b y c racionales que cumplan que $q = \frac{ab}{2}$ y $a^2 + b^2 = c^2$.

Observemos que si q es congruente y r es un racional positivo, entonces qr^2 también será congruente (basta aplicar una homotecia de razón r al triángulo con área q para obtener otro con área qr^2), entonces definimos la relación en $\mathbb{Q}^+$: $x \sim y$ si existe q racional no nulo tal que $x = q^2 y$, que resulta una relación de equivalencia. La observación de arriba dice que si $x \sim y$ entonces x es congruente $\Leftrightarrow$ y es congruente.

Para simplificar notaciones vamos a introducir la siguientes deficiones:

DEFINICIÓN 1.5. Una terna pitagórica racional (TPR) es un tripleta (a, b, c) con a, b y c racionales positivos tales que $a^2 + b^2 = c^2$.

DEFINICIÓN 1.6. Una terna pitagórica primitiva (TPP) es una tripleta (a, b, c) con a, b y c enteros positivos coprimos tales que $a^2 + b^2 = c^2$.

Observemos que si (a, b, c) es una TPR entonces existe un $t \in \mathbb{Q}^+$ tal que (ta, tb, tc) es una TPP, esto es sencillo pues basta multiplicar por un entero positivo n tal que na, nb y

nc sean enteros y luego dividir por $m = \text{mcd}(na, nb)$, entonces $t = n/m$ sirve.

Pro último observemos que si x es racional entonces puede escribirse de la forma $x = nq^2$ donde n=entero positivo libre de cuadrados (i.e producto de primos distintos) y q racional. Para ver esto simplemente descomponemos x en sus factores primos, separando los que están elevados a exponente impar y par $x = p_1^{2\alpha_1+1} \dots p_k^{2\alpha+1} q_1^{2\beta} \dots q_l^{2\alpha_l}$ donde $p_1, p_2, \dots, p_k, q_1, q_2, \dots, q_l$ son primos y $\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_l$ son enteros, entonces $x = (p_1 p_2 \dots p_k)(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l})^2$. Por lo tanto todo racional es equivalente a un entero positivo libre de cuadrados (o sea para conocer los congruente alcanza con conocer los congruentes libres de cuadrados).

Las observaciones anteriores nos dan un método para listar los números congruente libre de cuadrados, alcanza con listar los que provienen de una TPP y luego tomar la parte libre de cuadrado (el n de la parte anterior). Podemos listar las TPP recordando que si (a, b, c) es una TPP con a impar entonces existen r y s coprimos y de distinta paridad tal que $(a, b, c) = (r^2 - s^2, 2rs, r^2 + s^2)$, denotemos por $q = ab/2$ su área y por n la parte libre de cuadrados de q y veamos cuales son los primeros números congruentes n libre de cuadrados que aparecerán en nuestra lista:

(r,s)	q	n
(2,1)	6	6
(3,2)	30	30
(4,1)	60	15
(4,3)	84	21
(5,2)	210	210
(5,4)	180	5
(6,1)	210	210
(6,5)	330	330

Aunque con esto nos aseguramos de listarlos a todos, dado un n no sabemos si aparecerá o no en nuestra tabla y si aparece puede que tarde mucho en aparecer. Otra observación es que cada valor de n puede repetirse como pasa por ejemplo con $n = 210$ en nuestra tabla que se obtiene para los triángulos $(21, 20, 29)$ y $(35, 12, 37)$. De hecho veremos usando herramientas de curvas elípticas que todos los n que aparecen en nuestra tabla se repiten infinitas veces.

El siguiente resultado relaciona los números congruentes con sucesiones de cuadrados racionales de tres términos y con la existencia de puntos "no triviales" en cierta curva elíptica.

PROPOSICIÓN 1.7. *Si n es un entero positivo libre de cuadrados, son equivalente las siguientes afirmaciones:*

1. *n es congruente.*
2. *Existen tres cuadrados racionales en progresión aritmética de diferencia n.*
3. *La curva elíptica $E_n(\mathbb{Q}) : Y^2 = X^3 - n^2 X$ posee algún punto racional distinto de $(-n, 0), (0, 0), (n, 0)$ y $\vartheta = [0 : 1 : 0]$*

DEMOSTRACIÓN. (1) $\Rightarrow$ (2): Tenemos que $n = ab/2$ con (a, b, c) TPR, entonces tenemos que:

$$\begin{aligned} c^2 - 4n &= a^2 - 2ab + b^2 = (a-b)^2 \\ c^2 &= c^2 \\ c^2 + 4n &= a^2 + 2ab + b^2 = (a+b)^2 \end{aligned}$$

Dividiendo entre 4 cada término de la progresión de arriba nos queda $(c/2)^2 - n, (c/2)^2$ y $(c/2)^2 + n$ que cumple lo requerido.

(2) $\Rightarrow$ (1): La prueba anterior nos da una buena idea de como formar la TPR (a, b, c) con $n = ab/2$ a partir de una sucesión $x - n, x, x + n$ de cuadrados racionales, simplemente definimos:

$$\begin{aligned} a &= \sqrt{x+n} - \sqrt{x-n} \\ b &= \sqrt{x+n} + \sqrt{x-n} \\ c &= 2\sqrt{x} \end{aligned}$$

Tenemos $a^2 + b^2 = 2(x+n) + 2(x-n) = 4x = c^2$ y $ab/2 = (x + n - (x-n))/2 = n$.

(2) $\Rightarrow$ (3): Si $x - n, x$ y $x + n$ son cuadrados de números racionales entonces su producto también lo será, sea $y^2 = (x-n)(x+n)x = x^3 - n^2x$, luego (x, y) es un punto racional en la curva elíptica E_n, pero si $x = n$ tendrímos que $x = n = 1$ (pues n es libre de cuadrados y x cuadrado) lo cual es imposible pues $x + n = 2$ no es cuadrado racional, así que $x - n > 0$ (por ser cuadrado), pero como $x + n > x > x - n > 0$ entonces $y \neq 0$ así que no es ninguno de los puntos $(-n, 0), (0, 0), (n, 0)$ ni ϑ.

La parte (3) $\Rightarrow$ (2) puede deducirse de un teorema más general sobre curvas elípticas que es el siguiente.

TEOREMA 1.8. *Sea $\mathbb{K}$ un cuerpo de característica distinta de 2 y de 3 y sea $E : Y^2 = f(X)$ una curva elíptica donde $f(X) = X^3 + aX + b$, supongamos ademas que $f(X) = (X - e_1)(X - e_2)(X - e_3)$ con e_1, e_2 y e_3 pertenecientes a $\mathbb{K}$. Si $P = (x_0, y_0) = 2Q$, con $P, Q \in E(\mathbb{K})$ entonces*

$$x_0 - e_1, x_0 - e_2, x_0 - e_3,$$

son cuadrados en $\mathbb{K}$.

La prueba del teorema puede verse por ejemplo en la página 47 de [**7**], veremos aquí como se deduce la implicancia a partir de este teorema:

(3) $\Rightarrow$ (2) (asumiendo el teorema): En nuestro caso $E_n : Y^2 = (X-n)(X-0)(X+n)$, así que nuestra curva factoriza en $\mathbb{Q}$ si $P = (x_0, y_0)$ es un punto racional en E_n distinto de $(-n, 0), (0, 0)$ y $(n, 0)$ entonces $2P \neq \vartheta$ (pues en caso contrario $P = (x_0, y_0) = -P = (x_0, -y_0)$ luego $y_0 = 0$ y por lo tanto $0 = (x_0 - n)(x_0 - 0)(x_0 + n)$ es decir $x_0 = 0, -n$ o n), luego podemos escribir $2P = (x, y)$ y por el teorema $x - n, x$ y $x + n$ serían cuadrados racionales.

□

CAPíTULO 2

Curvas elípticas sobre $\mathbb{C}$ y sobre $\mathbb{R}$.

1. Puntos de orden 2 y 3.

En esta sección $\mathbb{K} = \mathbb{C}$, $\mathbb{R}$ o $\mathbb{Q}$.

1.1. Puntos de orden 2. Al igual que antes partimos de una curva elíptica

$$E : Y^2 = f(X),$$

donde $f(X) = X^3 + aX + b$ con $a, b \in \mathbb{K}$. La condición de elíptica implica que f no posee raíces múltiples (o lo que es equivalente que $4a^3 + 27b^2 \neq 0$).

Si $P \in \mathbb{K}$ es un punto de orden 2 de la curva, entonces $P \neq \mathcal{O}$ y podemos poner $P = (x, y)$. Como $2P = \mathcal{O}$ entonces $P = (x, y) = -P = (x, -y)$ por lo tanto $y = 0$ y $f(x) = 0$, así que van a haber tantos puntos de orden 2 como raíces en $\mathbb{K}$ tenga f y son los puntos de la forma $P = (x, 0)$ con $f(x) = 0$ y $x \in \mathbb{K}$.

En el caso complejo como todo polinomio factoriza en $\mathbb{C}$ entonces habrán 3 puntos de orden 2, si $\mathbb{K} = \mathbb{R}$ entonces puede haber 1 o 3 puntos de orden 2 y 0, 1 o 3 en el caso $\mathbb{K} = \mathbb{Q}$.

En un grupo abeliano G los puntos de orden divisores de m ($m \in \mathbb{Z}^+$) forman un subgrupo que denotaremos por $G(m)$, es decir

$$G(m) = \{P \in E : mP = \mathcal{O}\}.$$

En particular para hallar $G(2)$ solo hay que agregar el elemento neutro $\mathcal{O}$ a los puntos de orden 2 (el único elemento de orden 1).

Observando que un grupo de orden 4 donde cada elemento tiene orden 2 debe ser producto de dos grupos cíclicos de dos elementos (i.e isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$) y que un grupo con dos elementos es isomorfo a $\mathbb{Z}_2$, nuestro análisis puede resumirse de la siguiente manera:
$E(2)$ es isomorfo a algunos de los siguientes grupos según los siguientes casos:

- Caso $\mathbb{K} = \mathbb{C} : \mathbb{Z}_2 \times \mathbb{Z}_2$.
- Caso $\mathbb{K} = \mathbb{R} : \mathbb{Z}_2 \times \mathbb{Z}_2$ ó $\mathbb{Z}_2$.
- Caso $\mathbb{K} = \mathbb{Q} : \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2$ ó $\{\mathcal{O}\}$.

1.2. Puntos de orden 3. Si m es un entero positivo y $E = E(\mathbb{K})$ es una curva elíptica sobre un cuerpo $\mathbb{K}$, denotaremos por $E[m]$ a los puntos de E tales que su orden sea un divisor de m, es decir

$$E[m] = \{P \in E : mP = \mathcal{O}\}.$$

Cuando queramos recalcar el cuerpo donde está definida la curva notaremos $E(\mathbb{K})[m]$ en vez de $E[m]$.

En la sección anterior vimos que los puntos de orden 2 estaban dados por puntos de la forma $P = (x, 0) \in \mathbb{K}^2$ con $f(x) = 0$. En general teníamos que $E[2] = \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2$ ó $\{\mathcal{O}\}$ según f tuviera tres, una o ninguna raíz sobre $\mathbb{K}$ respectivamente. Veremos a continuación que sucede con los puntos de orden 3, para el caso real y complejo.

Los puntos de $E[3]$ tienen una interpretación geómetrica interesante, ellos son exactamente los puntos de inflexión de la cúbica E. En efecto, P es de inflexión $\Leftrightarrow P * P = P \Leftrightarrow P \oplus P = P * \mathcal{O} = -P \Leftrightarrow 3P = \mathcal{O}$.

Si $P = (x, y) \in E(\mathbb{K})$ tiene orden 3 entonces $x(2P) = x(-P) = x(P)$. Recíprocamente, si $P = (x, y) \in E(\mathbb{K})$ verifica que $x(2P) = x(P)$ entonces $2P = \pm P$, pero como $P \neq \mathcal{O}$ entonces $2P = -P$ y $3P = \mathcal{O}$.

Aplicando la fórmula de adición tenemos que la condición necesaria y suficiente para que un punto $P \in E(\mathbb{K})$ tenga orden 3 es que

$$\frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b} = x,$$

o en forma equivalente

$$3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Así que si definimos $\psi_3(X) = 3X^4 + 6aX^2 + 12bX - a^2$ tenemos que la condición necesaria y suficiente para que $P = (x, y) \in \mathbb{K}^2$ sea un punto de $E(\mathbb{K})[3]$ es que su coordenada x verifique:

$$\begin{cases} \psi_3(x) = 0 & (1) \\ f(x) \text{ sea un cuadrado en } \mathbb{K} & (2) \end{cases}$$

Por cada $x \in \mathbb{K}$ que verifique (1) y (2) tenemos dos puntos sobre $E(\mathbb{K})$ de orden 3, que vienen dados por $(x, \pm\sqrt{f(x)})$ (observar que $f(x) \neq 0$ pues en caso contrario $ord(P) = 2$). Conviene aquí separar en dos casos:

- Si $\mathbb{K} = \mathbb{C}$ entonces la condición (2) se verifica trivialmente y ψ_3 tiene sus cuatro raíces complejas, que tienen que ser distintas. En efecto, cada raíz aporta dos puntos de $E(\mathbb{C})[3]$ cuya cantidad de elementos es un múltiplo de 3 (pues sus puntos, salvo el punto del infinito, tienen orden 3 y $E[3]$ es no trivial pues ψ_3 tiene raíz), así que $E(\mathbb{C})[3]$ tiene 3 ó 9 elementos, si tuviese 3 elementos entonces ψ_3 tendria una única raíz de múltiplicidad 4 y tendríamos que $\psi_3(X) = 3(X - \alpha)^4 = 3(X^4 - 4\alpha X^3 + \ldots)$ lo cual implica $\alpha = 0$ lo cual implica a su vez implica $a = b = 0$ que es imposible puesto que f no posee raíces múltiples. Así que $E(\mathbb{C})[3]$ tiene nueve elementos y todos de orden divisor de 3 así que $E(\mathbb{C})[3] = \mathbb{Z}_3 \times \mathbb{Z}_3$.

- Para $\mathbb{K} = \mathbb{R}$ tenemos que la condición (2) es equivalente a pedir que $f(x) > 0$. Para analizar con más cuidado (1) recordemos primero que la fórmula de duplicación puede expresarse tambien como

$$x(2P) = \left(\frac{f'(x)^2}{4f(x)}\right) - 2x.$$

Con la cual igualando a x y despejando todo para un lado, obtenemos la siguiente fórmula alternativa para ψ_3:

$$\psi_3(X) = 12Xf(X) - f'(X)^2.$$

Observemos ahora que si $\psi_3(x) = 0$ entonces $f'(x)^2 = 12xf(x)$ y que como $f'(X) = 3X^2 + a$, $f'(0) = 0$ solo para el caso en que $a = 0$.

Caso $a = 0$: Aquí se tiene $f(X) = X^3 + b$ con $b \neq 0$ y $\psi_3(X) = 3X^4 + 12bX = 3X(X^3 + 4b)$ que tiene como raíces $X = 0$ y $X = \sqrt[3]{-4b}$. Como $f(0)f(\sqrt[3]{-4b}) = -3b^2 < 0$ entonces existe un único valor de X que verifica (1) y (2) y por lo tanto $E(\mathbb{R})[3]$ consta de exactamente 3 puntos, luego $E(\mathbb{R}[3]) = \mathbb{Z}_3$.

Caso $a \neq 0$: Aquí tenemos que $f'(0) \neq 0$, así que si $x \in \mathbb{R}$ verifica $\psi_3(x) = 0$ tenemos $12xf(x) = f'(x)^2 > 0$, luego la condición (2) puede cambiarse por $(2')$ $x > 0$, en otras palabras las condiciones (1) y (2) son equivalente a encontrar una raíz positiva de ψ_3 (i.e por cada raíz positiva de ψ_3 tenemos dos puntos de $E(\mathbb{R})[3]$). Como el producto de las raíces (reales y complejas) de ψ_3 es $-a^2 < 0$ entonces f no puede tener todas sus raíces complejas (pues estas vienen de a pares conjugados). Como ψ_3 posee a lo sumo 4 raíces $\#E(\mathbb{R})[3] \leq 2 \cdot 4 + 1 = 9$ y si $E(\mathbb{R})[3]$ fuese no trivial, entonces su cardinal sería múltiplo de 3, tenemos que $\#E(\mathbb{R})[3] = 1, 3$ ó 9. Si fuese 9 esto quiere decir que ψ_3 tiene sus cuatro raíces reales positivas, lo cual es imposible dado que su producto es $-a^2 < 0$. Si f posee dos raíces reales x_0 y x_1 (y por lo tanto dos complejas conjugadas z y $\overline{z}$), como $x_0x_1\|z\|^2 = -a^2 < 0$ entonces $x_0x_1 < 0$ y por lo tanto ψ_3 posee exactamente una raíz real positiva y tenemos que $E(\mathbb{R})[3]$ tiene exactamente 3 elementos así que $E(\mathbb{R})[3] = \mathbb{Z}_3$. En el caso que ψ_3 tuviese todas sus cuatro raíces reales, como su producto es $-a^2 < 0$ entonces debe poseer al menos una raíz positiva, así que $E(\mathbb{R})[3]$ es no trivial y como no puede tener 9 elementos, debe tener exactamente 3, así que también aquí $E(\mathbb{R})[3] = \mathbb{Z}_3$.

En resumen, los puntos de $E[3]$ vienen dados según cada caso por:

- $E(\mathbb{C})[3] = \mathbb{Z}_3 \times \mathbb{Z}_3$.
- $E(\mathbb{R})[3] = \mathbb{Z}_3$

2. Puntos de orden finito en $E(\mathbb{C})$.

Para atacar el caso genérico ya surgen varias complicaciones. Para el caso que nuestra curva esté definida sobre $\mathbb{C}$ (de aquí en mas supondremos siempre que $\mathbb{K} = \mathbb{C}$) podemos utilizar las herramientas del análisis para clasificar los puntos de orden m.

Probaremos que $E(\mathbb{C})$ es isomorfo al grupo de un toro, que surge de cocientar $\mathbb{C}$ por cierto subgrupo especial llamado lattice:

DEFINICIÓN 2.1. Un retículo complejo es un subgrupo de $\mathbb{C}$ de la forma $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ donde ω_1 y ω_2 son dos complejos linealmente independientes (sobre $\mathbb{R}$).

Así que el problema de hallar los puntos de orden m en $E(\mathbb{C})$ se reduce al de hallar los puntos de orden m en el grupo cociente $\mathbb{C}/\mathbb{L}$ lo cual es considerablemente mas fácil y es lo primero que haremos.

PROPOSICIÓN 2.2. *Si denotamos* $(\mathbb{C}/\mathbb{L})[m]$ *al conjunto de los puntos de* $\mathbb{C}/\mathbb{L}$ *cuyo orden divide a* m *tenemos que* $(\mathbb{C}/\mathbb{L})[m] = \mathbb{Z}_m \times \mathbb{Z}_m$.

DEMOSTRACIÓN. Sea $\omega + \mathbb{L} \in \mathbb{C}/\mathbb{L}$ y supongamos que tenga orden m entonces $m\omega \in \mathbb{L}$, pongamos $m\omega = a\omega_1 + b\omega_2$ con $a, b \in \mathbb{Z}$, entonces tenemos que $\omega = (a/m)\omega_1 + (b/m)\omega_2$, si ahora hacemos la divisón entera entre m, $a = mq_1 + r_1$ y $b = mq_2 + r_2$ con $0 \leq r_1, r_2 < m$ tenemos $\omega + \mathbb{L} = (r_1/m)\omega_1 + (r_2/m)\omega_2 + (q_1\omega_1 + q_2\omega_2) + \mathbb{L} = (r_1/m)\omega_1 + (r_2/m)\omega_2 + \mathbb{L}$. Reciprocamente, todo punto de la forma $(s/m)\omega_1 + (t/m)\omega_2 + \mathbb{L}$ con $0 \leq s, t < m$ tiene orden m en $\mathbb{C}/\mathbb{L}$ así que ellos son exactamente los elementos de $(\mathbb{C}/\mathbb{L})[m]$. El isomorfismo con $\mathbb{Z}_m \times \mathbb{Z}_m$ es el obvio $(s/m)\omega_1 + (t/m)\omega_2 + \mathbb{L} \mapsto (s \ (mod\ m), t \ (mod\ m))$. □

Por la proposición anterior, si probamos que existe un isomorfismo de grupos entre $E(\mathbb{C})$ y el toro $\mathbb{C}/\mathbb{L}$ entonces tendremos que $E(\mathbb{C})[m] = \mathbb{Z}_m \times \mathbb{Z}_m$. El ingrediente principal para construir dicho isomorfismo es una función meromorfa $\wp$ llamada la función de Weierstrass que se construye a partir de un retículo complejo y verifica una ecuación diferencial de la forma $(\wp'(z))^2 = 4\wp^3(z) - g_2\wp(z) - g_3$ para ciertos complejos g_2 y g_3 (que dependen únicamente del retículo), es decir que para todo z donde $\wp$ sea analítica tenemos que $\phi(z) = (\wp(z), \wp'(z))$ es un punto de la cúbica $E : Y^2 = 4X^3 - g_2X - g_3$. Se puede probar que g_2 y g_3 verifican $4g_2^3 + 27g_3^2 \neq 0$ y por lo tanto la cúbica E es en realidad una curva elíptica. Podemos extender el dominio de ϕ a todo el plano complejo llevando los polos de $\wp$ al punto del infinito $\mathcal{O}$ de nuestra curva elíptica E. La función $\phi : \mathbb{C} \longrightarrow E$ resulta ser un morfismo sobreyectivo de grupos con kernel $\mathbb{L}$, luego induce un isomorfismo entre el cociente $\mathbb{C}/\mathbb{L}$ y los puntos de E. Luego todas las curvas elíptica que son asociadas a funciones de Weierstrass (y entonces a retículos) resultan isomorfas a toros complejos.

Recíprocamente dada una curva elíptica compleja $E : Y^2 = 4X^3 - aX - b$ (toda curva elíptica puede escribirse de esa forma puesto que $\sqrt[3]{4} \in \mathbb{C}$), es posible elegir un retículo tal que $g_2 = a$ y $g_3 = b$, así que toda curva elíptica es asociada a un retículo complejo y por lo tanto isomorfa a un toro.

Ahora manos a la obra con todo esto ...

Primero introduciremos ciertas funciones que nos serán de importancia, son las llamadas funciones elípticas.

DEFINICIÓN 2.3. Una función elíptica es una función meromorfa sobre $\mathbb{C}$ que posee dos períodos linealmente independientes sobre $\mathbb{R}$.

Un claro ejemplo de función elíptica son las constantes, de hecho estas son las únicas funciones elípticas enteras (o sea analítica en todo $\mathbb{C}$) como veremos a continuación.

PROPOSICIÓN 2.4. *Las únicas funciones elípticas sin polos son las constantes.*

DEMOSTRACIÓN. En efecto, sea f una función entera con períodos ω_1 y ω_2 linealmente independientes (i.e $\{\omega_1, \omega_2\}$ es una base de $\mathbb{C}$ como $\mathbb{R}$-espacio vectorial). Consideremos el paralelogramo $P = \{s\omega_1 + t\omega_2 : 0 \leq s, t \leq 1\}$, si $\omega \in \mathbb{C}$ entonces existen $x, y \in \mathbb{R}$ tal que $\omega = x\omega_1 + y\omega_2$, si escribimos $x = [x] + s$ e $y = [y] + t$ con $0 \leq s, t \leq 1$ tenemos que $f(\omega) = f((s\omega_1 + t\omega_2) + ([x]\omega_1 + [y]\omega_2)) = f(s\omega_1 + t\omega_2) \in f(P)$, así que $Im(f) = f(P)$ que es compacto (pues P lo es) y por lo tanto f es acotada, pero como es entera entonces debe ser constante (Teorema de Liuville). □

Otra interesante propiedad de las funciones elípticas es la que relaciona los ceros con los polos en un paralelogramo periódico. Comenzemos definiendo esto último.

DEFINICIÓN 2.5. Si f es una función elíptica no nula, llamaremos paralelogramo periódico para f a un paralelogramo de la forma $P(a) = \{a + s\omega_1 + t\omega_2 : 0 \leq s, t \leq 1\}$ donde ω_1 y ω_2 son períodos linealmente independientes para f y que cumpla que el borde de $P(a)$ no contenga ni ceros ni polos de f.

Observemos que como los ceros y polos de una función meromorfa no nula es un conjunto discreto entonces toda función elíptica posee un paralelogramo periódico.

PROPOSICIÓN 2.6. *Una función elíptica f posee la misma cantidad de ceros que de polos dentro de cada paralelogramo periódico P (contados con multiplicidades).*

DEMOSTRACIÓN. Todo período de f también lo es de f' y por tanto de f/f', la integral

$$\frac{1}{2\pi i}\int_{\partial P} \frac{f(z)}{f'(z)} dz = 0,$$

por causa de la periodicidad, pero esta integral cuenta la cantidad de ceros menos la cantidad de polos dentro de P lo que prueba la proposición. □

Otra cosa que aparecerá mucho, son sumas armónicas sobre retículos, por lo que es preferible tener un criterio para clasificarlas desde ahora.

PROPOSICIÓN 2.7. *Sea $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ un retículo y denotamos por $\mathbb{L}^* = \mathbb{L} - \{0\}$ entonces*

$$\sum_{\omega \in \mathbb{L}^*} \frac{1}{\omega^\alpha}$$

converge absolutamente si y solo si $\alpha > 2$.

DEMOSTRACIÓN. Consideremos el paralelogramo $P = \{s\omega_1 + t\omega_2 : -1 \leq s, t, \leq 1\}$ y sean r y R la mínima y la máxima distancia de los puntos de ∂P al origen. Si denotamos por $\|x\omega_1 + y\omega_2\| = \max\{|x|, |y|\}$ y llamamos $A(n) = \{\omega \in \mathbb{L} : \|\omega\| = n\}$, es claro que $A(n) \subset n\partial P = \partial(nP)$ y por lo tanto tendremos que $nr \leq \omega \leq nR$.

Como $A(n)$ posee $(2n+1) + (2(n-1)+1) = 4n$ puntos (los puntos de $A(n)$ son de la forma $\pm n\omega_1 + m\omega_2$ con $-n \leq m \leq n$ ó $m\omega_1 \pm n\omega_2$ con $-(n-1) \leq m \leq n-1$) tenemos la siguiente acotación

$$\sum_{k=1}^{n} \frac{4k}{(rk)^\alpha} \leq \sum_{k=1}^{n} \sum_{\omega \in A(k)} \frac{1}{|\omega|^\alpha} \leq \sum_{k=1}^{n} \frac{4k}{(Rk)^\alpha}.$$

Es decir:

$$\frac{4}{r^\alpha} \sum_{k=1}^{n} \frac{1}{k^{\alpha-1}} \leq \sum_{k=1}^{n} \sum_{\omega \in A(k)} \frac{1}{|\omega|^\alpha} \leq \frac{4}{R^\alpha} \sum_{k=1}^{n} \frac{1}{k^{\alpha-1}}$$

Claramente $\bigcup_{k=1} A(k) = \mathbb{L}^*$, así que la convergencia de $\sum_{k=1}^{n} \frac{1}{k^{\alpha-1}}$ para $\alpha > 2$ garantizan la convergencia absoluta de $\sum_{\omega \in \mathbb{L}^*} \frac{1}{\omega^\alpha}$ para $\alpha > 2$. Análogamente, la divergencia de $\sum_{k=1}^{n} \frac{1}{k^{\alpha-1}}$ para $\alpha \leq 2$ implican la no convergencia absoluta de $\sum_{k=1}^{n} \frac{1}{k^{\alpha-1}}$ para $\alpha \leq 2$. □

DEFINICIÓN 2.8. En vista de la proposición anterior, conviene definir las llamadas series de Eisenstein $G_n = \sum_{\omega \in \mathbb{L}^*} \frac{1}{\omega^n}$ para $n = 3, 4, 5, \ldots$.[1]

2.1. La función $\wp$ de Weierstrass. Aquí introduciremos la función $\wp$ de un retículo y probaremos que verifica la ecuación diferencial que hemos mencionado antes y para su curva elíptica asociada construiremos un isomorfismo entre el grupo de la curva elíptica y el grupo de un toro.

TEOREMA 2.9. *Sea $\mathbb{L}$ un retículo complejo y $\mathbb{L}^* = \mathbb{L} - \{0\}$, la serie*

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathbb{L}^*} \left\{ \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right\}$$

define una función meromorfa en $\mathbb{C}$ con polos de orden 2 en los puntos de $\mathbb{L}$. Además esta función es par (o sea $\wp(z) = \wp(-z)$ $\forall z \in \mathbb{C} - \mathbb{L}$).

Antes de probar esto necesitamos un par de lemas previos, el primero es un lemita de uniformización, el cual usaremos en reiteradas oportunidades para probar convergencias de algunas series, el segundo es prácticamente el teorema en si.

LEMA 2.10. *Si $R > 0$, existe una constante $M > 0$ tal que se verifica*

$$\frac{1}{|z-\omega|^\alpha} \leq \frac{M}{|\omega|^\alpha}$$

para todo $z \in \mathbb{C} : |z| \leq R$ y $\omega \in \mathbb{L} : |\omega| > R$

[1] Más adelante se prueba que $G_n = 0$ para n impar, de donde algunos autores como en [**6**] le llaman G_n a lo que aquí le llamamos G_{2n}, nosotros seguiremos las notaciones de [**4**].

DEMOSTRACIÓN DEL LEMA 2.10. Demostrar esa desigualdad es equivalente a probar que

$$\Big|\frac{z-\omega}{\omega}\Big|^{\alpha} \geq \frac{1}{M}$$

para todo $z \in \mathbb{C} : |z| \leq R$ y $\omega \in \mathbb{L} : |\omega| > R$, para ello primero tomemos entre todos los $\omega \in \mathbb{L}$, $|\omega| > R$ uno con norma minimal, llamémoslo ω_0 (existe porque $\mathbb{L}$ es discreto) y pongamos que $|\omega_0| = R + d$ con $d > 0$. Entonces para todo $z : |z| \leq R$ tenemos

$$\Big|\frac{z-\omega}{\omega}\Big|^{\alpha} = \Big|1 - \frac{z}{\omega}\Big|^{\alpha} \geq \Big(1 - \Big|\frac{z}{\omega}\Big|\Big)^{\alpha} \geq \Big(1 - \frac{R}{R+d}\Big)^{\alpha}.$$

Luego podemos tomar por ejemplo $M = (1 - \frac{R}{R+d})^{-\alpha}$. □

LEMA 2.11. *Si $R > 0$ entonces la serie*

$$\sum_{|\omega|>R} \Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\}$$

converge absoluta y uniformemente para $|z| \leq R$.

DEMOSTRACIÓN DEL LEMA 2.11. Si $|\omega| > R$, para todo $z : |z| \leq R$ tenemos

$$\Big|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big| = \Big|\frac{\omega^2 - (z-\omega)^2}{\omega^2(z-\omega)^2}\Big| = \Big|\frac{z(z-2\omega)}{\omega^2(z-\omega)^2}\Big| \leq \frac{|z|(|z|+2|\omega|)}{|\omega|^2} \cdot \frac{1}{|z-\omega|^2}$$

$$\leq \frac{R(R+2|\omega|)}{|\omega|^2} \cdot \frac{M}{|\omega|^2} = \frac{MR(2+\frac{R}{|\omega|})}{|\omega|^3} \leq \frac{3MR}{|\omega|^3}.$$

Estos últimos términos mayorantes tienen serie convergente por la proposición 2.7, así que queda probada la convergencia absoluta y uniforme usando el criterio de Weierstrass. □

DEMOSTRACIÓN DEL TEOREMA 2.9. Para cada $\omega \in \mathbb{L} : |\omega| > R$, la función $z \mapsto \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$ es una función holomorfa en $D(0,R)$ por lo tanto también lo será $z \mapsto \sum_{N>|\omega|>R}\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\}$. Luego por la proposición anterior tenemos que

$$\sum_{N>|\omega|>R} \Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\} \longrightarrow \wp_R(z) = \sum_{|\omega|>R} \Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\}$$

Donde la convergencia es uniforme en $\overline{D(0.R)}$ (y por lo tanto en subconjuntos compactos de $D(0,R)$) luego la función límite $\wp_R$ será también holomorfa en $D(0,R)$.

Además tenemos que

$$\wp(z) = \wp_R(z) + \sum_{0<|\omega|\leq R} \Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\} + \frac{1}{z^2}\ ,$$

siendo esta última suma una función meromorfa en $D(0,R)$ con polos de orden 2 en los puntos de $D(0,R) \cap \mathbb{L}$, luego $\wp$ también lo será, pero como esto vale para todo $R > 0$ tenemos que $\wp$ es meromorfa en $\mathbb{C}$ con polos de orden 2 en los puntos del retículo $\mathbb{L}$.

Solo nos resta probar la paridad, para ello observemos que mientras $\wp$ varia en $\mathbb{L}^*$ lo mismo sucede con $-\wp$, en vista de la convergencia absoluta podemos reordenar los

términos quedándonos

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\mathbb{L}^*}\Big\{\frac{1}{(z+\omega)^2} - \frac{1}{(-\omega)^2}\Big\} = \frac{1}{(-z)^2} + \sum_{\omega\in\mathbb{L}^*}\Big\{\frac{1}{(-z-\omega)^2} - \frac{1}{\omega^2}\Big\} = \wp(-z),$$

que es justo lo que queriamos probar. □

Ahora veremos que la fúnción $\wp$ resulta una función elíptica donde los puntos de su retículo asociado $\mathbb{L}$ son períodos para $\wp$.

TEOREMA 2.12. *La función de $\wp$ de Weierstrass y su derivada $\wp'$ verifican*

$$\wp(z+\omega) = \wp(z) \qquad y \qquad \wp'(z+\omega) = \wp'(z)$$

para todo $z \in \mathbb{C} - \mathbb{L}$ y $\omega \in \mathbb{L}$.

DEMOSTRACIÓN. Supongamos primero que la derivada de $\wp$ se pudiera obtener derivando término a término la serie que define $\wp$ entonces nos quedaría que

$$\wp'(z) = -2\Big\{\sum_{\omega\in\mathbb{L}}\frac{1}{(z-\omega)^3}\Big\}$$

Como hay convergencia absoluta para la serie que define $\wp$ en $z \in \mathbb{C} - \mathbb{L}$, también lo habrá para $\sum_{\omega\in\mathbb{L}}\frac{1}{(z-\omega)^3}$ y por lo tanto es posible reordenar términos (sin alterar el resultado, claro). Si $\omega_0 \in \mathbb{L}$, la serie $-2\{\sum_{\omega\in\mathbb{L}}\frac{1}{(z+\omega_0-\omega)^3}\} = \wp(z+\omega_0)$ es una reordenación de la serie que define $\wp'(z)$ (pues $\omega \mapsto -\omega_0 + \omega$ es una biyección de $\mathbb{L}$ en $\mathbb{L}$), así que $\wp'(z+\omega) = \wp'(z)$ para todo $\omega \in \mathbb{L}$.

Escribamos $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, donde ω_1 y ω_2 son dos complejos linealmente independientes, tenemos que

$$0 = \wp'(z+\omega_i) - \wp'(z) = \frac{d}{dz}\Big(\wp(z+\omega_i) - \wp(z)\Big),$$

para $i = 1, 2$, así que como $\mathbb{C} - \mathbb{L}$ es conexo, han de existir constantes R_1 y R_2 tales que $\wp(z+\omega_i) - \wp(z) = R_i$ para $i = 1, 2$ y para todo $z \in \mathbb{C} - \mathbb{L}$. Claramente $\frac{1}{2}\omega_i \notin \mathbb{L}$ (por la independencia lineal de los ω_i's), así que tomando $z = -\frac{\omega_i}{2}$ y usando la paridad de $\wp$ tenemos

$$R_i = \wp(\omega - \frac{\omega_i}{2}) - \wp(-\frac{\omega_i}{2}) = \wp(\frac{\omega_i}{2}) - \wp(-\frac{\omega_i}{2}) = 0,$$

para $i = 1, 2$ así que $R_1 = R_2 = 0$ lo que implica que $\wp(z) = \wp(z+\omega_1) = \wp(z+\omega_2)$ que a su vez implica que $\wp(z) = \wp(z+\omega)$ para todo $\omega \in \mathbb{L}$.

Así que solo resta probar la afirmación inicial, o sea que $\wp'$ se puede obtener derivando término a término la serie que define $\wp$, para ello alcanza probar que la serie

$$\sum_{\omega\in\mathbb{L}}\frac{1}{(z-\omega)^3}$$

define una función holomorfa para $z \in \mathbb{C} - \mathbb{L}$. Pero por el lema 2.10, la proposición 2.7 y el criterio de Weierstrass tenemos la convergencia absoluta de

$$\sum_{\omega:|\omega|>R}\frac{1}{(z-\omega)^3}$$

para $z \in \overline{D(0,R)}$, luego define una función holomorfa en $D(0,R)$ por ser límite uniforme en $\overline{D(0,R)}$ de las funciones $z \mapsto \sum_{\omega:N>|\omega|>R} \frac{1}{(z-\omega)^3}$ que son holomorfas en $D(0,R)$. Como

$$\sum_{\omega\in\mathbb{L}} \frac{1}{(z-\omega)^3} = \sum_{\omega:|\omega|>R} \frac{1}{(z-\omega)^3} + \sum_{\omega:|\omega|\leq R} \frac{1}{(z-\omega)^3}$$

Tenemos que $\sum_{\omega\in\mathbb{L}} \frac{1}{(z-\omega)^3}$ es una función meromorfa en $D(0,R)$ con polos de orden 3 en los puntos de $D(0,R)\cap\mathbb{L}$, como esto vale para todo $R>0$ tenemos que $\sum_{\omega:\omega\in\mathbb{L}} \frac{1}{(z-\omega)^3}$ es meromorfa en todo el plano con polos de orden 3 en los puntos del retículo. □

El próximo teorema nos da un desarrollo en serie de Laurent de la función $\wp$ alrededor de 0.

TEOREMA 2.13. *El desarrollo de Laurent de $\wp$ alrededor de 0 viene dado por*

$$\wp(z) = \frac{1}{z^2} + \sum_{m=1}^{\infty} (2m+1)G_{2m+2}z^{2m}$$

DEMOSTRACIÓN. Sea $R = min\{|\omega| : \omega \in \mathbb{L}, \omega \neq 0\}$, para cada $\omega \neq 0$ y $z : |z| < R$ tenemos

$$\frac{1}{(z-\omega)^2} = \frac{1}{(\omega-z)^2} = \frac{1}{\omega^2}\Big(\frac{1}{1-(z/\omega)}\Big)^2 = \frac{1}{\omega}\,\frac{d}{dz}\Big(\frac{1}{1-(z/w)}\Big) = \frac{1}{\omega}\,\frac{d}{dz}\sum_{n=0}^{\infty}(z/\omega)^n$$

$$= \frac{1}{\omega^2}\sum_{n=1}^{\infty} n(z/\omega)^{n-1} = \frac{1}{\omega^2}\sum_{n=0}^{\infty}(n+1)(z/\omega)^n = \frac{1}{\omega^2} + \frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)(z/\omega)^n$$

Por lo tanto

$$\wp(z) - \frac{1}{z^2} = \sum_{\omega\in\mathbb{L}^*}\Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\} = \sum_{\omega\in\mathbb{L}^*}\Big\{\frac{1}{\omega^2}\sum_{n=1}^{\infty}(n+1)(z/\omega)^n\Big\}.$$

Por la convergencia absoluta, podemos intercalar las sumatorias y nos queda

$$\wp(z) - \frac{1}{z^2} = \sum_{\omega\in\mathbb{L}^*}\Big\{\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big\} = \sum_{n=1}^{\infty}\Big\{\sum_{\omega\in\mathbb{L}^*}\frac{1}{\omega^2}\,(n+1)(z/\omega)^n\Big\}$$

$$= \sum_{n=1}^{\infty}\Big\{(n+1)\Big(\sum_{\omega\in\mathbb{L}^*}\frac{1}{\omega^{n+2}}\Big)z^n\Big\} = \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n.$$

Para terminar la prueba basta ver que para n impar $G_n = 0$, esto es fácil pues si ω varia en el retículo, también lo hace $-\omega$, luego por convergencia absoluta de G_n para $n>2$ podemos reordenar términos así que $G_n = \sum_{\omega\in\mathbb{L}}\frac{1}{(-\omega)^n}$, pero para n impar $(-\omega)^n = -(\omega^n)$ así que $G_n = \sum_{\omega\in\mathbb{L}}\frac{1}{-(\omega)^n} = -\sum_{\omega\in\mathbb{L}}\frac{1}{\omega^n} = -G_n$ y por lo tanto $G_n = 0$. □

Observemos que una vez más queda de manifiesto la paridad de $\wp$ dado que en su desarrollo de Laurent solo aparecieron términos pares.

El siguiente teorema establece una relación entre esta función con ciertas curvas elípticas.

TEOREMA 2.14. *La función $\wp$ de Weierstrass verifica la ecuación diferencial*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

DEMOSTRACIÓN. Si llamamos $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ al retículo que genera la función de Weierstrass, en la proposición anterior probamos que $\wp$ y $\wp'$ son funciones elípticas que tienen períodos linealmente independientes ω_1 y ω_2, claramente lo mismo sucederá con $(\wp')^2$ y con $\wp^3$ así que la función

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z),$$

es elíptica por ser combinación lineal de funciones elípticas con el par de períodos linealmente independiente común ω_1 y ω_2. Así que por la proposición 2.4 para probar que es constante alcanza probar que es entera, y dado que cada sumando que componen f son holomorfas en $\mathbb{C} - \mathbb{L}$, f también lo será, luego el conjunto de polos de f (si los hay) han de estar contenidos en el retículo $\mathbb{L}$. Por la periodicidad, para probar que f no tiene polos en $\mathbb{L}$ alcanza probar que no lo tiene en $z = 0$.

Usaremos el desarrollo en Serie de Laurent de $\wp$ en $z = 0$ (Teorema 2.13) para obtener el desarrollo de f en $z = 0$, aquí H representa una función holomorfa en $z = 0$:

$$\wp'(z) = -\frac{2}{z^3} + \sum_{m=1}^{\infty}(2m+1)(2m)G_{2m+2}z^{2m-1}$$

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + zH$$

para $\wp$ tenemos

$$\wp(z) = \frac{1}{z^2} - 3\frac{G_4}{z^2} - 5G_6z^4 + z^6H$$

$$4\wp(z)^3 = \frac{4}{z^6} + 36\frac{G_4}{z^2} + 60G_6 + z^2H.$$

Así que tenemos que

$$\wp'(z)^2 - 4\wp^3(z) = -\frac{60G_4}{z^2} - 140G_6 + zH.$$

Así que

$$f(z) = \wp'(z)^2 - 4\wp^3(z) + 60G_4\wp(z) = -140G_6 + zH.$$

Por lo tanto f es analítica en $z = 0$ y por lo tanto en todo $\mathbb{C}$ así que debe ser constante. Como $f(0) = -140g_6$ esa constante debe ser $-140g_6$ así que $f(z) + 140g_6 = 0$ que es lo que queriamos probar. □

Nota. El teorema anterior prueba que para $z \in \mathbb{C} - \mathbb{L}$ el punto $\phi(z) = (\wp(z), \wp'(z)) \in \mathbb{C}^2$ pertenece a la cúbica $E : Y^2 = 4X^3 - g_2X - g_3$ donde $g_2 = 60G_4$ y $g_3 = 140G_6$. Así que cada retículo complejo $\mathbb{L}$ tiene asociado una función de Weierstrass $\wp$ y esta a su vez tiene asociada una cúbica E de forma que $(\wp(z), \wp'(z)) \in E$, $\forall z \in \mathbb{C} - \mathbb{L}$, decimos en este caso que la cúbica E proviene del retículo $\mathbb{L}$ y a veces notaremos $E(\mathbb{L})$ cuando queramos recalcar que E proviene del retículo $\mathbb{L}$ (lo mismo para $\wp$, notaremos $\wp(\mathbb{L}, z)$ en vez de $\wp(z)$ cuando queramos resaltar la dependencia de $\wp$ con respecto a su retículo). Ahora veremos que las cúbicas asociadas a retículos son de hecho curvas elípticas.

TEOREMA 2.15. *Si $E : Y^2 = 4X^3 - g_2X - g_3$ es una cúbica asociada a un retículo $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ entonces E es una curva elíptica. O equivalentemente, se verifica la condición*

$$g_2^3(\mathbb{L}) - 27g_3^2(\mathbb{L}) \neq 0$$

para todo retículo complejo $\mathbb{L}$.

DEMOSTRACIÓN. Hay que probar que el polinomio $f(X) = 4X^3 - g_2X - g_3$ no posee raíces múltiples. Denotemos por e_1, e_2 y e_3 los valores de $\wp$ en los semiperiodos:

$$e_1 = \wp(\tfrac{\omega_1}{2}) \quad e_2 = \wp(\tfrac{\omega_2}{2}) \quad e_3 = \wp(\tfrac{\omega_1+\omega_2}{2})$$

Vamos a probar que e_1, e_2 y e_3 son las raíces de f y que son distintas dos a dos. Como $\wp'$ es la derivada de una función par entonces debe ser impar, luego debe anularse en cada semiperíodo de $\wp$ pues

$$\wp'\Big(\frac{\omega_1}{2}\Big) = \wp'\Big(\frac{\omega_1}{2} - \omega_1\Big) = \wp'\Big(-\frac{\omega_1}{2}\Big) = -\wp'\Big(\frac{\omega_1}{2}\Big)$$

por lo tanto $\wp'(\frac{\omega_1}{2}) = 0$, análogamente para los otros semiperíodos, pero por el Teorema 2.14, tenemos que

$$f(e_1) = f\left(\wp\left(\frac{\omega_1}{2}\right)\right) = 4\wp^3\left(\frac{\omega_1}{2}\right) - g_2\wp\left(\frac{\omega_1}{2}\right) - g_3 = \wp'\left(\frac{\omega_1}{2}\right)^2 = 0$$

y de igual forma se llega a $f(e_2) = 0$ y $f(e_3) = 0$, basta considerar los otros semiperíodos.

Falta ver que son distintos, para ello consideremos la función $g(z) = \wp(z) - \wp(\frac{\omega_1}{2})$, claramente g posee el mismo conjunto de períodos que $\wp$ así como polos de orden 2 en cada punto del retículo, consideremos un paralelogramo periódico $P(a) = \{a + t\omega_1 + s\omega_2 : 0 \leq t, s \leq 1\}$ con $a = x(\frac{\omega_1+\omega_2}{2})$ y $-1 \leq x \leq 0$ (esto es posible pues g es holomorfa y por lo tanto sus ceros son aislados). Por la Proposición 2.6 sabemos que dentro de $P(a)$ hay la misma cantidad de ceros que de polos, pero $z = 0$ es el único polo dentro de $P(a)$ que es de orden 2 y como $z = \frac{\omega_1}{2}$ es un cero doble de f (pues $g'(\frac{\omega_1}{2}) = \wp'(\frac{\omega_1}{2}) = 0$) no pueden haber otros ceros dentro de $P(a)$ de modo que $g(\frac{\omega_2}{2}) \neq 0$ y $g(\frac{\omega_1+\omega_2}{2}) \neq 0$ o lo que es lo mismo $\wp(\frac{\omega_1}{2}) \neq \wp(\frac{\omega_2}{2})$ y $\wp(\frac{\omega_1}{2}) \neq \wp(\frac{\omega_1+\omega_2}{2})$. De la misma forma, considerando $g(z) = \wp(z) - \wp(\frac{\omega_2}{2})$ llegamos a que $\wp(\frac{\omega_2}{2}) \neq \wp(\frac{\omega_1+\omega_2}{2})$. □

Observación 1. El teorema anterior prueba que el polinomio $f(X) = 4X^2 - g_2X - g_3$ factoriza como $f(X) = 4(X-e_1)(X-e_2)(X-e_3)$, luego la ecuación diferencial del Teorema 2.14 puede ponerse en la forma:

$$(\wp'(z))^2 = 4\Big(\wp(z) - \wp\Big(\frac{\omega_1}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_2}{2}\Big)\Big)\Big(\wp(z) - \wp\Big(\frac{\omega_1+\omega_2}{2}\Big)\Big)$$

Observación 2. El paralelogramo periódico $P(a)$ utilizado en el teorema contenia exactamente un punto del retículo $\mathbb{L}$ y por lo tanto un único polo de $\wp'$ que es de orden 3 y por la proposición 2.6, debe poseer tres ceros dentro de $P(a)$, así que los semiperíodos $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ y $\frac{\omega_1+\omega_2}{2}$ son los únicos ceros de $\wp'$ dentro de $P(a)$, luego por la periodicidad los ceros de $\wp'$ están dados por

$$Z(\wp') = \Big(\frac{\omega_1}{2} + \mathbb{L}\Big) \cup \Big(\frac{\omega_2}{2} + \mathbb{L}\Big) \cup \Big(\frac{\omega_1+\omega_2}{2} + \mathbb{L}\Big).$$

Esta observación es equivalente a pedir que $2z \in \mathbb{L}$, en efecto, claramente si z pertence al conjunto mencionado arriba verifica $2z \in \mathbb{L}$, recíprocamente, si $2z \in \mathbb{L}$ entonces tomemos $x \in P(a)$ tal que $z = x + \omega$ con $\omega \in \mathbb{L}$ (esto es posible pues con paralelogramos $P(a) + \omega$

donde ω varia en $\mathbb{L}$ cubrimos el plano) luego $2z = 2x + 2\omega$ por lo cual $2x = 2z - 2\omega \in \mathbb{L}$ y como $x \in P(a)$ entonces $x \in \{\frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2}\}$. En resumen, también podemos escribir

$$Z(\wp') = \{z \in \mathbb{C} - \mathbb{L} : 2z \in \mathbb{L}\}.$$

Si $\mathbb{L}$ es un retículo complejo, $\wp(z) = \wp(\mathbb{L}, z)$ su función de Weierstrass asociada y $E = E(\mathbb{L})$ su curva elíptica asociada, por el Teorema 2.14 tenemos definida una función $\phi : \mathbb{C} - \mathbb{L} \longrightarrow E - \{\mathcal{O}\}$ dada por $\phi(z) = (\wp(z), \wp'(z))$ donde $\mathcal{O} = [0 : 1 : 0]$ de la curva E. Extendemos esta función a todo el plano complejo definiéndola como $\mathcal{O}$ en los puntos del retículo:

$$\phi(z) = \begin{cases} [\wp(z) : \wp'(z) : 1] & \text{si } z \notin \mathbb{L} \\ [0 : 1 : 0] & \text{si } z \in \mathbb{L} \end{cases}$$

Nuestro siguiente objetivo es probar que la función $\phi : \mathbb{C} \longrightarrow E$ es un morfismo de grupos sobreyectivo, claro, los complejos con la suma habitual y los puntos de la curva elíptica con la suma $P \oplus Q = (P * Q) * \mathcal{O}$.

TEOREMA 2.16. *La función $\phi : \mathbb{C} \longrightarrow E$ definida como antes es una función sobreyectiva.*

Para probar esto, es conveniente probar un resultado previo en forma de lema.

LEMA 2.17. *La función $\wp$ es sobreyectiva. Además si $c \in \mathbb{C}$ y $\wp(z_0) = c$ tenemos que:*

$$\begin{array}{ll} \wp^{-1}(c) = \mathbb{L} + z_0 & \textit{si } 2z_0 \in \mathbb{L} \\ \wp^{-1}(c) = (\mathbb{L} + z_0) \cup (\mathbb{L} - z_0) & \textit{si } 2z_0 \notin \mathbb{L} \end{array}$$

DEMOSTRACIÓN DEL LEMA 2.17. La demostración es parecida a la del teorema anterior, para $c \in \mathbb{C}$ consideramos la función $f(z) = \wp(z) - c$, claramente f tiene polos de orden 2 en los puntos de $\mathbb{L}$ y si ω_1 y ω_2 son generadores del retículo $\mathbb{L}$ entonces son períodos linealmente independientes para f. Cada paralelogramo periódico de f de la forma $P(a) = \{a + t\omega_1 + s\omega_2 : 0 \leq t, s \leq 1\}$ contiene exactamente un polo doble de f y por la proposición 2.6 contiene también un cero doble o dos ceros simples de f. Sea $z_0 \in P(a)$ un cero de f, entonces $\wp(z_0) = f(z_0) + c = c$. Si z_0 fuese un cero doble de f (i.e si $f'(z_0) = \wp'(z_0) = 0$ o lo que es lo mismo si $2z_0 \in \mathbb{L}$) entonces no hay más ceros de f en $P(a)$ y por la periodicidad los únicos ceros de f en $\mathbb{C}$ van a ser de la forma $z_0 + \omega$ con $\omega \in \mathbb{L}$ y por lo tanto

$$\wp^{-1}(c) = f^{-1}(0) = \mathbb{L} + z_0.$$

Ahora si z_0 es un cero simple de f, por la proposición 2.6 debe haber otro cero simple de f en $P(a)$, como $\wp$ es par, $f(-z_0) = \wp(-z_0) - c = \wp(z_0) - c = 0$ asi que $-z_0$ es otro cero de f. Claramente $-z_0$ no tiene porque caer dentro de $P(a)$ pero como los paralelogramos $P(a)+\omega$ con ω variando en $\mathbb{L}$ podemos encontrar $\omega \in \mathbb{L}$ tal que $-z_0 + \omega \in P(a)$, si $-z_0 + \omega = z_0$ entonces $2z_0 = \omega \in \mathbb{L}$, luego $f'(z_0) = \wp'(z_0) = \wp(z_0 - \omega) = \wp(-z_0) = -\wp'(z_0)$ implica que $\wp'(z_0) = 0$ y por lo tanto z_0 sería un cero doble de f lo cual es absurdo, así que $-z_0 + \omega$ es el otro cero simple de f, por la periodicidad tenemos que

$$\wp^{-1}(c) = f^{-1}(0) = (z_0 + \mathbb{L}) \cup (-z_0 + \omega + \mathbb{L}) = (\mathbb{L} + z_0) \cup (\mathbb{L} - z_0).$$

□

DEMOSTRACIÓN DEL TEOREMA 2.16. Claramente $\varphi \in Im(\phi)$ pues $\varphi(\omega) = \varphi$ para todo $\omega \in \mathbb{L}$. Sea $P \in E$, $P \neq \varphi$ pongamos que $P = (x, y)$, por el lema 2.17 sabemos que existe $z \in \mathbb{C}$ tal que $\wp(z) = x$ y como $(\wp(z), \wp'(z)) \in E$ tenemos que $\wp'(z) = \pm y$. Si $\wp(z) = y$ entonces $\phi(z) = (\wp(z), \wp'(z)) = (x, y) = P$, en caso contrario $\wp(z) = -y$ y como $\wp$ es par y $\wp'$ impar tenemos que $\phi(-z) = (\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z)) = (x, y) = P$, en cualquier caso tenemos que $P \in Im(\phi)$ y por lo tanto ϕ es sobreyectiva. □

Ahora solo resta probar que es un homeomorfismo, como lo establece el siguiente teorema.

TEOREMA 2.18. *La función $\phi : \mathbb{C} \longrightarrow E$ es un epimorfismo de grupos.*

DEMOSTRACIÓN. Por el teorema anterior sabemos que es una función sobreyectiva así que solo resta probar que es un morfismo. Esto es, hay que probar que si z_1 y z_2 son dos complejos entonces $\phi(z_1) \oplus \phi(z_2) = \phi(z_1 + z_2)$ y para ello separemos la prueba en varios casos.

Caso 1. Si z_1 ó z_2 pertencen a $\mathbb{L}$:
Supongamos sin pérdida de generalidad que $z_2 \in \mathbb{L}$ entonces z_2 es período de ϕ (por serlo de $\wp$ y de $\wp'$) luego $\phi(z_1 + z_2) = \phi(z_1) = \phi(z_1) + \mathcal{O} = \phi(z_1) + \phi(z_2)$.

Caso 2. Si ni z_1 ni z_2 pertencen a $\mathbb{L}$ pero $z_1 + z_2 \in \mathbb{L}$:
Tenemos que $z_1 \in \omega - z_2$ con $\omega \in \mathbb{L}$, como $\wp$ es par y $\wp$ impar tenemos que $\phi(z_1) = (\wp(z_1), \wp'(z_1)) = (\wp(\omega - z_2), \wp(\omega - z_2)) = (\wp(-z_2), \wp'(-z_2)) = (\wp(z_2), -\wp(z_2)) = -\phi(z_2)$ así que $\phi(z_1) \oplus \phi(z_2) = \mathcal{O} = \phi(z_1 + z_2)$.

Caso 3. Si ni z_1 ni z_2 pertenecen a $\mathbb{L}$ pero $2z_1 \in \mathbb{L}$ y $2z_2 \in \mathbb{L}$:
Consideremos los semiperíodos $a_1 = \frac{\omega_1}{2}, a_2 = \frac{\omega_2}{2}$ y $a_3 = \frac{\omega_1 + \omega_2}{2}$ y para x y y complejos, notemos $x \sim y$ para decir que $x - y \in \mathbb{L}$, claramente por la periodicidad de $\wp$ y $\wp'$ tenemos que si $x \sim y$ entonces $\wp(x) = \wp(y)$ y $\wp'(x) = \wp'(y)$. En vista de la observación 2 del Teorema 2.15 tenemos que $z_1 \sim a_i$ y $z_2 \sim a_j$ para algunos i y j , $1 \leq i, j \leq 3$. Si $z_1 \sim z_2$ la condición $2z_1 \in \mathbb{L}$ implica que $z_1 + z_2 \in \mathbb{L}$ y caemos en el caso 2. En caso contrario podemos asegurar que $i \neq j$, sea k tal que $\{i, j, k\} = \{1, 2, 3\}$, tenemos que $z_1 + z_2 \sim a_i + a_j \sim a_k$ así que $z_1 + z_2 \sim a_k$ luego $\phi(z_1 + z_2) = \phi(a_k) = (\wp(a_k), \wp'(a_k)) = (\wp(a_k), 0)$ ($\wp'(a_k) = 0$ por la Observación 2 del Teorema 2.15) mientras que $\phi(z_1) \oplus \phi(z_2) = \phi(a_i) \oplus \phi(a_j) = (\wp(a_i), 0) \oplus (\wp(a_j), 0) = (\wp(a_k), 0)$ esto último sale del hecho que al ser $e_i = \wp(a_i)$ $i = 1, 2, 3$ las raíces del polinomio $f(X) = 4X^3 - g_1 X - g_2$ (Observación 1 del Teorema 2.15) entonces como ya habíamos estudiado antes los puntos $P_i = (e_i, 0)$ $i = 1, 2, 3$ son los puntos de orden 2 del grupo de la curva elíptica y por lo tanto teníamos que $P_i \oplus P_j = P_k$ si $\{i, j, k\} = \{1, 2, 3\}$.

Caso 4. Si $z_1, z_2, z_1 + z_2$ y $2z_1$ pertenecen a $\mathbb{C} - \mathbb{L}$:

Como z_1, z_2 y $z_1 + z_2$ no pertenecen a $\mathbb{L}$, podemos poner $\phi(z_1) = (x_1, y_1)$, $\phi(z_2) = (x_2, y_2)$ y $\phi(z_1) \oplus \phi(z_2) = (x, y)$, en efecto, si $\phi(z_1) \oplus \phi(z_2) = \mathcal{O}$ tendríamos que $x_1 = x_2$ y $y_1 = -y_2$, lo cual implica que $\wp(z_1) = \wp(z_2)$ y $\wp'(z_1) = -\wp'(z_2)$, pero la primera igualdad implica que $z_1 \in (\mathbb{L} + z_2) \cup (\mathbb{L} - z_2)$ (Teorema 2.16) pero como $z_1 + z_2 \notin \mathbb{L}$ tenemos que $z_1 \in \mathbb{L} + z_2$, pero por la periodicidad de $\wp'$ tendriamos que $\wp'(z_1) = \wp'(z_2)$, luego no

hay otra que $\wp'(z_1) = 0$ lo cual implica que $2z_1 \in \mathbb{L}$ (Observavión 2 del Teorema 2.15) lo que contradice nuestra hipótesis. Separemos este caso en dos subcasos según $z_1 - z_2$ pertenezcan o no a $\mathbb{L}$:
Primer subcaso: $z_1 - z_2 \in \mathbb{C} - \mathbb{L}$.

Como ya teníamos además que $z_1 + z_2 \in \mathbb{C}$ entonces $x_1 = \wp(z_1) \neq \wp(z_2) = x_2$.
y la fórmula para sumar puntos en una curva elíptica queda en este caso:

$$x = \frac{(y_1 - y_2)^2}{4(x_1 - x_2)^2} - (x_1 + x_2)$$

$$y = -\frac{(y_2 - y_1)x + (x_2 y_1 - x_1 y_2)}{x_2 - x_1},$$

donde $(x_1, y_1) \oplus (x_2, y_2) = (x, y)$.

Así que todo se reduce a probar que $x(\phi(z_1 + z_2)) = x$ y que $y(\phi(z_1 + z_2)) = y$ (observar que como pedimos que $z_1 + z_2 \notin \mathbb{L}$ entonces $\phi(z_1 + z_2) \neq \mathcal{O}$), probaremos la primera pues la segunda puede ser probada de forma similar.

Dado que $x_i = \wp(z_i)$ y $y_i = \wp'(z_i)$ para $i = 1, 2$ hay que probar que

$$\wp(z_1 + z_2) = \frac{(\wp'(z_1) - \wp'(z_2))^2}{4(\wp(z_1) - \wp(z_2))^2} - (\wp(z_1) + \wp(z_2)).$$

O equivalentemente (dado que $\wp(z_1) \neq \wp(z_2)$)

$$4(\wp(z_1) + \wp(z_2) + \wp(z_1 + z_2))(\wp(z_2) - \wp(z_1))^2 - (\wp'(z_2) - \wp'(z_1))^2 = 0.$$

Para probar esto vamos a usar la misma idea que para probar el Teorema 2.14, vamos a dejar fijo z_1 y tomar $z = z_2$ como variable esta resulta una función elíptica luego probaremos que es entera, luego por la proposición 2.4 debe ser constante, para ver que esa constante es cero evaluaremos en un valor conveniente de z. Definamos entonces la siguiente función

$$F(z) = 4(\wp(z_1) + \wp(z) + \wp(z_1 + z))(\wp(z) - \wp(z_1))^2 - (\wp'(z) - \wp'(z_1))^2.$$

Si llamamos como siempre ω_1 y ω_2 a un par de generadores del retículo $\mathbb{L}$, estos son periodos linealmente independientes de $z \mapsto \wp(z)$, $z \mapsto \wp(z + z_0)$ y de $z \mapsto \wp'(z)$ así que también lo serán de F, así que F es una función elíptica. Ahora tanto $\wp$ como su derivada tienen polos en los puntos de $\mathbb{L}$, mientras que la función $z \mapsto \wp(z + z_0)$ tiene sus polos en los puntos de $\mathbb{L} - z_0$, así que los posibles polos de F estarían contenidos en el conjunto $\mathbb{L} \cup (\mathbb{L} - z_0)$. Por la $\mathbb{L}$-periodicidad para probar que F es entera alcanza probar la analiticidad en $z = 0$ (lo cual implica la analiticidad $\forall z \in \mathbb{L}$) y en $z = -z_0$ (lo cual implica la analiticidad $\forall z \in \mathbb{L} - z_0$).

Para sacar un desarrollo de Laurent en $z = 0$ recordemos que el desarrollo de Laurent en $z = 0$ para $\wp$ viene dado por (Teorema 2.13):

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \dots$$

A partir de aquí obtenemos el desarrollo de Laurent para $\wp'$:

$$\wp'(z) = -\frac{2}{z^3} + 6g_4 z + 20G_6 z^3 + 42G_8 z^5 + \dots$$

Como $\wp$ es analítica en $z = z_1$ el desarrollo es serie de potencias de $z \mapsto \wp(z+z_1)$ en $z = 0$ viene dado por la fórmula de Taylor

$$\wp(z+z_1) = \wp(z_1) + \wp'(z_1)z + \frac{\wp''(z_1)}{2}z^2 + \frac{\wp^{(3)}(z)}{6}z^3 + \dots$$

Si H indica una función analítica en $z = 0$, para F tenemos el siguiente desarrollo en serie de Laurent en $z = 0$:

$$F(z) = 4\left(\frac{1}{z^2} + 2\wp(z_1) + \wp'(z_1)z + \left(3G_4 + \frac{1}{2}\wp''(z_1)\right)z^2 + \frac{1}{6}\wp'''(z_1)z^3 + z^4H\right)\left(\frac{1}{z^2} - \wp(z_1) + 3G_4z^2 + z^4H\right)^2$$
$$- \left(-\tfrac{2}{z^3} - \wp'(z_1) + 6G_4z + z^3H\right)^2$$

Haciendo cuentas y agrupando términos del mismo orden nos queda

$$F(z) = \frac{A}{z^6} + \frac{B}{z^4} + \frac{C}{z^3} + \frac{D}{z^2} + \frac{E}{z} + H,$$

donde:

$$\begin{aligned} A &= 4 - 4 = 0 \\ B &= -8\wp(z_1) + 8wp(z_1) = 0 \\ C &= 4\wp'(z_1) - 4\wp'(z_1) = 0 \\ D &= 2\wp''(z_1) - 12\wp^2(z_1) + 60G_4 \\ E &= -8\wp(z_1)\wp'(z_1) + \tfrac{2}{3}\wp'''(z_1) \end{aligned}$$

Para ver que $D = E = 0$ recordemos la ecuación diferencial que verificaba $\wp$ (Teorema 2.14)

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Derivando de ambos lados nos queda

$$2\wp'(z)\wp''(z) = 12\wp(z)^2\wp'(z) - 60G_4\wp'(z).$$

Para todo $z \in \mathbb{C} - \mathbb{L}$ tal que $2z \notin \mathbb{L}$ tenemos que $\wp'(z) \neq 0$ (Observación 2 del Teorema 2.15) y la ecuación diferencial anterior es equivalente para esos z a:

$$\wp''(z) = 6\wp(z)^2 - 30G_4 \tag{28}$$

Como $2z_1 \notin \mathbb{L}$ entonces esta ecuación es válida para $z = z_1$ lo cual prueba que $D = 0$. Derivando nuevamente ambos miembros de (28) obtenemos

$$\wp'''(z) = 12\wp(z)\wp'(z).$$

En particular tomando $z = z_1$ esto prueba que $E = 0$.

Como $A = B = C = D = E = 0$ resulta que F es analítica en $z = 0$ y por periodicidad en todo punto de $\mathbb{L}$, por lo tanto sus polos están contenidos en el conjunto $\mathbb{L} - z_1$, para probar la analiticidad de F en $z = -z_1$ observamos que en ese punto tanto la función $\wp$ como $\wp'$ son analíticas en $z = -z_1$ así que alcanza probar la analiticidad de

$$\wp(z+z_1)(\wp(z) - \wp(z_1))^2,$$

en $z = -z_1$. Como $\wp(z)$ tiene en $z = 0$ un polo de orden 2 entonces $-z_1$ es un polo de orden 2 de $\wp(z+z_1)$ así que hay que probar que $-z_1$ es un cero de orden mayor o igual a dos para $(\wp(z) - \wp(z_1))^2$ o equivalentemente que $-z_1$ es un cero de $\wp(z) - \wp(z_1)$ lo cual es cierto pues $\wp$ es par.

Como F es analítica en $-z_1$ por la periodicidad también lo será en todo $\mathbb{L} - z_0$, luego hemos probado que la función F es una función entera de z y como es elíptica ha de ser constante (prop 2.4) y como $F(z_1) = 0$ tenemos que F es la función nula y en particular

$F(z_2) = 0$.

Segundo subcaso: $z_1 - z_2 \in \mathbb{L}$.

En este caso por la periodicidad de $\wp$ tenemos que

$$x_1 = \wp(z_1) = \wp(z_2) = x_2$$

y también

$$-y_1 = \wp'(z_1) = \wp'(z_2) = y_2,$$

aquí la fórmula para sumar puntos queda (duplicación)

$$x = \frac{1}{4}\Big(\frac{f'(x_1)}{4y_1^2}\Big) - 2x_1 = \frac{(12x_1^2 - 60G_4)^2}{16y_1^2} - 2x_1,$$

$$y = y_1 + 6\frac{(x_1^2 - 5G_4)(x - x_1)}{y_1},$$

donde $f(X) = 4X^3 - g_2X - g_3$ (observar que $y_1 \neq 0$ pues $2z_1 \notin \mathbb{L}$). Queremos probar que $x(\phi(z_1 + z_2)) = x$ y que $y(\phi(z_1 + z_2)) = y$ y al igual que en el caso anterior probaremos solo la primera. La demostración es análoga a la del subcaso anterior pero más fácil. Hay que probar que

$$\wp(2z_1) = \frac{(12\wp(z_1)_1^2 - 60G_4)^2}{16\wp'(z_1)^2} - 2\wp(z_1),$$

o equivalentemente (puesto que $\wp'(z_1) \neq 0$)

$$16\wp'(z_1)^2(\wp(2z_1) + 2\wp(z_1)) - (12\wp^2(z_1) - 60G_4)^2 = 0.$$

Así que consideramos la función

$$F(z) = 16\wp'(z)^2(\wp(2z) + 2\wp(z)) - (12\wp^2(z) - 60G_4)^2,$$

que como es elíptica para ver que es constante basta ver que es entera y como sus posibles polos están contenidos en $\mathbb{L}$ por la periodicidad alcanza ver que es analítica en $z = 0$. Al igual que en el caso anterior usando los desarrollos en serie de Laurent de $\wp$ y $\wp'$ en $z = 0$ podemos ver que los términos correspondientes a z^n con $n \leq 1$ se cancelan de forma que F resulta constante y esa constante debe ser cero. □

Comentario. Como comentamos en la demostración se puede seguir un procedimiento análogo del que hicimos para probar que $x(\phi(z_1+z_2)) = x$ para probar que $y(\phi(z_1+z_2)) = y$ esta vez sustituyendo x por su valor ya probado $x = \wp(z_1 + z_2)$, construir una función elíptica adecuada etc. Otra cosa que podemos hacer es dado que $x(\phi(z_1 + z_2)) = x$ y como $\phi(z_1 + z_2) \in E$ entonces solo tenemos dos posibilidades $y(\phi(z_1 + z_2)) = y$ (en cuyo caso ya no hay nada que probar) o $y(\phi(z_1 + z_2)) = -y$, podemos considerar la función meromorfa $z \mapsto \frac{y}{\wp'(z_1+z))}$ (donde y se saca de la fórmula que queda en función de $\wp(z_1), \wp'(z_1), \wp(z)$ y de $\wp'(z)$) que toma a lo sumo dos valores entonces ha de ser constante, considerando los primeros términos del desarrollo de Laurent es fácil probar que el límite de esa función tiende a 1 cuando $z \to 0$.

Para culminar esta sección estableceremos el teorema que establece el objetivo principal de esta sección.

TEOREMA 2.19. *Si E es una curva elíptica que proviene de un retículo $\mathbb{L}$ entonces el grupo de la curva elíptica $(E, \oplus)$ es isomorfo al grupo del toro $(\frac{\mathbb{C}}{\mathbb{L}}, +)$.*

DEMOSTRACIÓN. El teorema anterior nos da un epimorfismo $\phi : \mathbb{C} \longrightarrow E$ cuyo kernel viene dado justamente por los puntos del retículo $\mathbb{L}$ así que por la propiedad universal del cociente para grupos tenemos inducido un isomorfismo $\widetilde{\phi} : \frac{\mathbb{C}}{\mathbb{L}} \longrightarrow E$. □

Hemos probado que toda curva elíptica que proviene de un retículo es isomorfa (como grupo) a un toro. Es posible probar que la ϕ que construimos también resulta ser un homeomorfismo e incluso un isomorfismo de superficies de Riemann como puede verse por ejemplo en el libro de Frances Kirwan "Complex algebraic curves".

En la próxima sección probaremos un resultado sorprendente, de hecho que toda curva elíptica proviene de un retículo complejo y de esa manera culminaría la prueba de que el grupo de toda curva elíptica es isomorfo al grupo de algún toro construido a partir de un retículo adecuado.

2.2. Curvas elípticas y retículos. Ya vimos que las curvas elípticas que provienen de retículos complejos son isomorfas como grupo a un toro. El objetivo de esta sección es probar que toda curva elíptica puede obtenerse de esa forma.

Si llamamos $\mathbb{L}$ al retículo complejo, su curva elíptica asociada venía dada por

$$E(\mathbb{L}) : Y^2 = 4X^3 - 60G_4X - 140G_6$$

donde las constantes G_4 y G_6 dependen únicamente del retículo y vienen dadas por

$$G_4(\mathbb{L}) = \sum_{\omega \in \mathbb{L}} \frac{1}{\omega^4} \qquad \text{y} \qquad G_6(\mathbb{L}) = \sum_{\omega \in \mathbb{L}} \frac{1}{\omega^6}.$$

Como hicimos antes denotaremos por $g_2 = 60G_4$ y $g_3 = 140G_6$, así que el objetivo de esta sección la podríamos expresar de la siguiente manera: Dada una curva elíptica $E : Y^2 = 4X^3 - aX - b$ (i.e tal que $a^3 + 27b^2 \neq 0$) probar que existe un retículo complejo $\mathbb{L}$ tal que

$$g_2(\mathbb{L}) = a \qquad \text{y} \qquad g_3(\mathbb{L}) = b.$$

Si $\mathbb{L}$ es un retículo complejo y ω_1 y ω_2 son dos complejos que verifican que $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ entonces decimos que ω_1 y ω_2 son un generador del retículo $\mathbb{L}$. Claramente el retículo queda determinado a partir de una pareja de generadores $(\omega_1, \omega_2) \in \mathbb{C}^2$ y asi podemos trabajar con g_2 y g_3 como funciones de (ω_1, ω_2) que vistas asi, resultan funciones homogeneas de grado -4 y -6 respectivamente. Esto quiere decir que

$$g_2(\lambda\omega_1, \lambda\omega_2) = \lambda^{-4} g_2(\omega_1, \omega_2) \qquad \text{y} \qquad g_3(\lambda\omega_1, \lambda\omega_2) = \lambda^{-6} g_3(\omega_1, \omega_2),$$

para todo $\lambda \neq 0$. Esto es inmediato a partir de las fórmulas para G_4 y G_6.

También el discriminante $\Delta = g_2^3 - 27g_3^2$ podemos verlo como función de (ω_1, ω_2) y resulta una función homogenea de grado -12, es decir, para todo $\lambda \neq 0$ se tiene que

$$\Delta(\lambda\omega_1, \lambda\omega_2) = \lambda^{-12}\Delta(\omega_1, \omega_2).$$

Por último introduciremos una función de retículo que nos será de gran ayuda, definimos la función J por la fórmula

$$J(\omega_1, \omega_2) = \frac{g_2^3(\omega_1, \omega_2)}{\Delta(\omega_1, \omega_2)}.$$

J está bien definida pues por el Teorema 2.15 tenemos que $\Delta(\omega_1, \omega_2) \neq 0$, además J resulta homogenea de grado 0 por ser cociente de dos homogeneas del mismo grado. Por lo tanto, si llamamos $\tau = \omega_2/\omega_1$ tenemos que

$$J(\omega_1, \omega_2) = J(1, \tau),$$

donde podemos suponer sin pérdida de generalidad que $Im(\omega_2/\omega_1) > 0$ (pues ω_1/ω_2 y ω_2/ω_1 son dos complejos no reales inversos uno del otro, por lo tanto tienen parte imaginaria opuestas entonces puedo elegirlos para que la razón entre el segundo y el primero tenga parte real positiva), luego podemos pensar J como función del semiplano positivo $\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}$ en los complejos y la notaremos simplemente como $J(\tau)$ en vez de $J(1, \tau)$.
Aunque las funciones g_2, g_3 y Δ no dependen únicamente de la razón $\tau = \omega_2/\omega_1$ igualmente nos resultará útil trabajar con ellas como fuciones de $\mathbb{H}$ definiéndolas para $\tau \in \mathbb{H}$ como $g_2(\tau) = g_2(1, \tau)$, $g_3(\tau) = g_3(1, \tau)$ y $\Delta(\tau) = \Delta(1, \tau)$.

El hecho de que toda curva elíptica sobre los complejos provenga de un retículo radica esencialmente en la sobreyectividad de la función J, veamos como probar lo primero asumiendo como hipótesis dicha sobreyectividad.

TEOREMA 2.20. *Si a y b son complejos tales que $a^3 - 27b^2 \neq 0$ entonces existe un par de complejos (ω_1, ω_2) linealmente independientes con $Im(\omega_2/\omega_1) > 0$ tales que*

$$g_2(\omega_1, \omega_2) = a \qquad y \qquad g_3(\omega_1, \omega_2) = b.$$

DEMOSTRACIÓN. Como estamos asumiendo la sobreyectividad de J y dado que $a^3 - 27b^2 \neq 0$ podemos tomar $\tau \in \mathbb{H}$ tal que

$$J(\tau) = \frac{a^3}{a^3 - 27b^2}.$$

Para ese valor de τ, elijamos un $\omega_1 \in \mathbb{C}$ de forma tal que

$$\frac{g_2(1, \tau)}{\omega_1^4} = a.$$

La existencia de tal ω_1 es inmediata si $a \neq 0$, si $a = 0$ observemos que por la elección de τ tenemos $J(\tau) = 0$ y por lo tanto $g_2(\tau) = 0$ así que en este caso cualquier valor complejo no nulo sirve para ω_1 .

Luego tenemos que

$$J(\tau) = \frac{g_2^3(\tau)}{g_2^3(\tau) - 27g_3^2(\tau)} = \frac{a^3}{a^3 - 27b^2}.$$

Así que $g_3^2(\tau) = b^2\omega_1^{12}$, si tomamos $\omega_2 = \tau\omega_1$, aplicando la homogeneidad de g_3 tenemos que

$$g_3^2(\omega_1, \omega_2) = \frac{g_3^2(1, \tau)}{\omega_1^{12}} = b^2.$$

Así que $g_3(\omega_1, \omega_2) = \pm b$, como

$$g_2(\omega_1, \omega_2) = \frac{1}{\omega_1^4}\, g_2(1, \tau) = a.$$

Si $g_3(\omega_1, \omega_2) = b$ ya tenemos lo que queriamos, en caso contrario $g_3(\omega_1, \omega_2) = -b$ y tenemos que

$$g_3(i\omega_1, i\omega_2) = \frac{1}{i^6}\, g_3(\omega_1, \omega_2) = (-1)(-b) = b,$$

y ademas

$$g_2(i\omega_1, i\omega_2) = \frac{1}{i^4}\, g_2(\omega_1, \omega_2) = a.$$

Así que en este otro caso, es el par $(i\omega_1, i\omega_2)$ el que nos sirve. □

Observación. Con los ω_1 y ω_2 del teorema anterior, nos construimos el retículo $\mathbb{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, para este retículo tendremos $g_2(\mathbb{L}) = a$ y $g_3(\mathbb{L}) = b$.

Así que todo se reduce a probar la sobreyectividad de la función J, veremos que J pertence a un grupo de funciones llamadas funciones modulares. Las funciones modulares son funciones muy importantes en el estudio analítico de las curvas elíptica que poseen propiedades muy importantes. No le sacaremos mayor provecho a tales funciones, más bien enfocaremos nuestra atención a probar lo que necesitamos, que es simplemente la sobreyectividad.

Comenzemos definiendo el grupo modular.

DEFINICIÓN 2.21. El grupo modular es el subgrupo formado por transformaciones de Mobius de la forma

$$A(z) = \frac{az + b}{cz + d},$$

donde a, b, c y d son enteros tales que $ad - bc = 1$. El grupo modular lo notaremos por Γ.

Como los coeficientes de A son reales, deja invariante al eje real y la condición que $ad - bc = 1 > 0$ implica que lleva al semiplano superior en si mismo. Así que las transformaciones del grupo modular se las pueden pensar como funciones en $\mathbb{H}$.

El grupo modular está generado por las funciones $T(\tau) = \tau + 1$ y $S(\tau) = -\frac{1}{\tau}$, si bien es elemental la prueba no la haremos aquí y de hecho lo único que usaremos es que tales funciones pertenecen al grupo modular lo cual es evidente.

Observemos que si una función f es invariante por el grupo modular (es decir si $f(A\tau) = f(\tau)$ para todo $A \in \Gamma$ y $\tau \in \mathbb{H}$) entonces en particular es periódica de período 1 (basta tomar $A\tau = \tau + 1$). Las funciones periódicas poseen desarrollo en serie de Fourier como veremos a continuación.

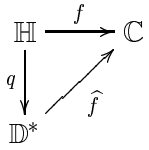
Desarrollo de Fourier.

PROPOSICIÓN 2.22. *Si $f : \mathbb{H} \longrightarrow \mathbb{C}$ es analítica con $f(\tau+1) = f(\tau)$ para todo $z \in \mathbb{H}$ entonces*

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n \tau}$$

donde la convergencia es absoluta y uniforme en subconjuntos compactos de $\mathbb{H}$.

DEMOSTRACIÓN. Definamos $q : \mathbb{H} \longrightarrow \mathbb{D}^*$, $\tau \mapsto e^{2\pi i \tau}$. Veamos que existe una función analítica $\widehat{f} : \mathbb{D}^* \longrightarrow \mathbb{C}$ tal que el siguiente diagrama conmute



En efecto, para cada $z \in \mathbb{D}$, tomemos $\tau \in q^{-1}(z)$ y definimos $\widehat{f}(z) = f(\tau)$. Observemos que $\widehat{f}$ está bien definida pues si tomásemos otro τ' tal que $q(\tau') = q(\tau) \Rightarrow e^{2\pi i \tau'} = e^{2\pi i \tau} \Rightarrow \tau' - \tau \in \mathbb{Z} \Rightarrow f(\tau') = f(\tau)$.

Como $q : \mathbb{H} \longrightarrow \mathbb{D}^*$ es localmente conforme, $\widehat{f}$ resulta ser una función analítica en $\mathbb{D}^*$ y por lo tanto posee desarrollo en serie de Laurent alrededor de $q = 0$: $\widehat{f}(q) = \sum_{n=-\infty}^{\infty} a_n q^n$ válido para todo $q \in \mathbb{D}^*$.

Luego para $\tau \in \mathbb{H}$, tomando $q = q(\tau)$, nos queda que

$$f(\tau) = \widehat{f}(q) = \sum_{n=-\infty}^{\infty} a_n q^n = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i \tau},$$

válido para todo $\tau \in \mathbb{D}$. □

Nota. Definiremos el valor de f en $\tau = \infty$ como el valor de $\widehat{f}$ en $q = 0$. El orden de zero o polo de f en $\tau = \infty$ lo definimos como el orden de cero o polo de $\widehat{f}$ en $q = 0$. Diremeos que f es holomorfa ó meromorfa en ∞ cuando $\widehat{f}$ sea holomorfa ó meromorfa respectivamente en cero.

Estamos listos ahora para definir las transformaciones modulares:

DEFINICIÓN 2.23. Sea $f : \mathbb{H} \longrightarrow \mathbb{C}$ una función meromorfa, decimos que f es modular si verifica las dos siguientes condiciones:

1. $f(A\tau) = f(\tau)$ para todo $A \in \Gamma$ y $\tau \in \mathbb{H}$.
2. f posee polo (o cero) en $\tau = \infty$, es decir si posee desarrollo de Fourier de la forma

$$\sum_{n=-m}^{\infty} a_n q^n,$$

donde $q = e^{2\pi i \tau}$ y $m \in \mathbb{Z}$.

Veremos a continuación un teorema sobre funciones modulares. Antes introduciremos un conjunto asociado al grupo modular:

DEFINICIÓN 2.24. El conjunto $R(\Gamma) \subset \mathbb{H}$ es el conjunto definido por

$$R(\Gamma) = \{\tau \in \mathbb{H} : -1/2 \leq Re(\tau) \leq 1/2, ||z|| \geq 1\} \cup \{\infty\}.$$

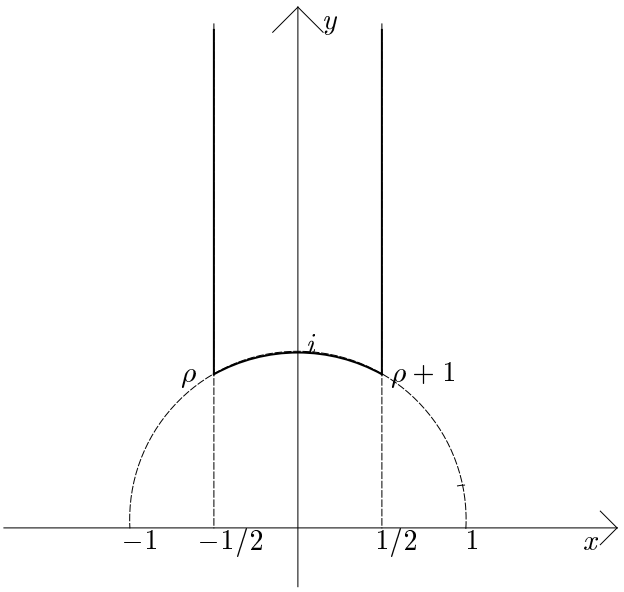


FIGURA 1. Region Fundamental.

Al conjunto $R(\Gamma)$ lo llamaremos región fundamental para el grupo modular Γ, este conjunto cumple la propiedad de ser conexo y compacto (con la topologia de S^2 restricta) y que para todo punto $\tau \in \mathbb{H}$, existe una transformación A del grupo modular que cumple que $A\tau \in R(\Gamma)$; esto último se expresa diciendo que el conjunto $R(\Gamma)$ es una clase de representantes del conjunto cociente $\mathbb{H}/\Gamma$. Además dados dos puntos del interior de $R(\Gamma)$, no existe ninguna transformación de Γ que lleve uno en el otro. A los puntos $\rho, i, \rho + 1$ e ∞ se le llaman los vértices de $R(\Gamma)$, donde $\rho = e^{\frac{2\pi i}{3}}$.

Observemos también que $R(\Gamma)$ por ser una clase de representantes para Γ, una función modular queda determinada conociendo sus valores en la región fundamental.

TEOREMA 2.25. *Si $f : \mathbb{H} \to \mathbb{C}$ es una función modular no nula entonces la cantidad de ceros de f en $R(\Gamma)$ coincide con la cantidad de polos de f en $R(\Gamma)$.*

Antes de demostrarlo una convención en cuanto al conteo de ceros y polos, consideremos el borde de $R(\Gamma)$ dividido en cuatro partes según la figura 2, a cada una de las cuales llamaremos lados de $R(\Gamma)$. El lado (1) se identifica con el lado (4) por la transformación del grupo modular $T(\tau) = \tau + 1$, de modo que si f posee algún cero o polo en el lado (1) también lo tendrá en el lado (4), a estos ceros o polos los contaremos una sola vez. La misma observación para los lados (2) y (3) que se corresponden através de la transformación del grupo modular $S(\tau) = -1/\tau$, los contaremos una sola vez. Si f posee cero o polo en i lo contaremos doble y si f posee cero o polo en ρ, lo contaremos triple (por ejemplo un polo de orden 2 en ρ lo contariamos seis veces), el orden de polo de f en ∞ es el m de la definición y el orden como cero es $-m$.

DEMOSTRACIÓN. Consideremos la región fundamental $R(\Gamma)$ con su borde dividido en cuatro partes según la siguiente figura:

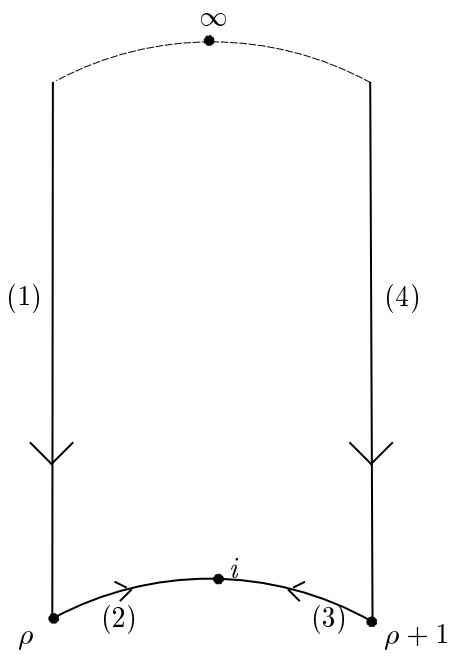


FIGURA 2. Region Fundamental.

Observemos que si hubiesen infinitos ceros o polos de f en $R(\Gamma)$ entonces acumularian, no pueden acumular en la zona finita de $R(\Gamma)$ pues f es meromorfa en $\mathbb{H}$, tampoco pueden acumular en ∞ pues implicaría que los ceros o polos de $\widehat{f}$ (definida como en la proposición anterior) acumularian en $q = 0$, pero por la segunda condición de función modular tenemos que esto es imposible pues $\widehat{f}$ tiene cero o polo en $q = 0$, en ninguno de los casos los ceros o polos pueden acumular cerca de $q = 0$.

En conclusión la función f solo posee una cantidad finita de ceros o polos en $R(\Gamma)$, luego existe un $M > 0$ tal que todo cero o polo complejo de f en $R(\Gamma)$ tiene parte imaginaria menor que M.

Consideremos entonces la integral sobre una curva cerrada como en la figura 3.

Se ha deformado el lado (1) con pequeños arcos de circunferencias con centro en los polos y ceros de f que se encuentran en ese lado y no son vértices, de modo que quedan fuera de la curva. Como son finitos podemos elegir los radios de tales circunferencias que sean tan pequeñas como para que el centro sea el único cero o polo de f dentro de tales circunferencias. En el lado (4) también se ha deformado el lado con pequeñas circunferencias que corresponden a las del lado (1) translada por $T(\tau) = \tau + 1$. De está forma los polos en el lado (1) y (4) están contados una sola vez en el interior de la curva de la figura.

Con respecto al lado (2) también se ha deformado con pequeños arcos de circunferencias centradas en los ceros y polos de f que se encuentran sobre ese lado y no son vértices de forma de excluirlos del interior de la curva de la figura, se trazaron sus correspondientes arcos en el lado (3) que son los transformados de los del lado (2) por la

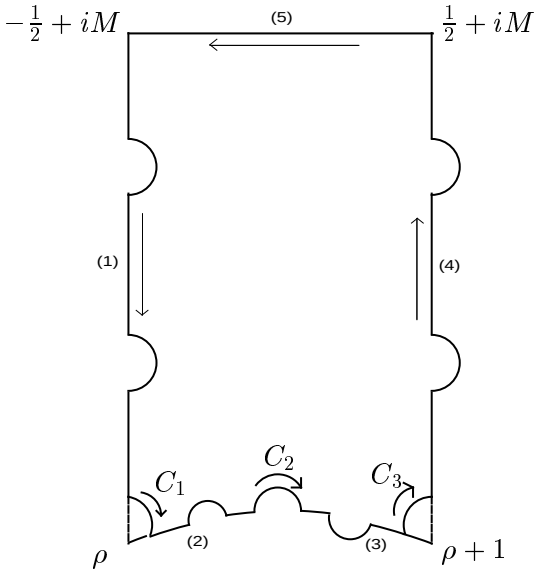


FIGURA 3. Curva de Integración.

transformación del grupo modular $S(\tau) = -1/\tau$, los ceros y polos que aparecian en el lado (2) quedaron en el exterior de la curva mientras que los del lado (3) quedaron en el interior, o sea estamos contando una sola vez los ceros y polos de (2) y (3) en el interior de la curva.

Centrado en $\rho = e^{2\pi i/3}$ se ha trazado un pequeño arco de circunferencia C_1 con extremos en z_1 en el lado (1) y z_2 en el lado (2) de forma que no contenga ningún cero ni polo (ni ningún otro vértice) en su interior con excepción quizas de su centro. Se traza con centro en el vértice $\rho + 1$ un arco de circunferencia C_3 con extremos en $-1/z_2$ en el lado (3) y $z_1 + 1$ en el lado (4), podemos suponer que no contiene ceros ni polos de f salvo quizas su centro (de no ser así achicamos el radio de C_1 de forma que esto acontezca).

Por la elección de M, si integramos sobre la curva de la figura anterior, nos queda que

$$\frac{1}{2\pi i}\oint f(z)dz = Z' - P', \tag{29}$$

donde Z' y P' cuenta los ceros y los polos de f respectivamente que se encuentra en la región $R(\Gamma)$, con excepción de sus vértices (principio del argumento).

Observemos que la integral sobre el lado (1) deformado, se cancela con la integral sobre el lado (4) deformado dado que están recorrido en sentidos opuestos y $f(\tau) = f(\tau + 1)$. También cancela la integral sobre el lado (2) deformado y el lado (3) deformado, pues $S(\tau) = -1/\tau$ mapea (2) en (3) con la dirección reversa y f es invariante por S. Así que la ecuación (29) nos queda

$$\frac{1}{2\pi i}\left\{\int_{C_1} f + \int_{C_2} f + \int_{C_3} f + \int_{(5)} f\right\} = Z' - P'.$$

Ahora vamos a calcular cada una de esas integrales, escribamos cerca de ρ a f como $f(\tau) = (\tau - \rho)^k g(\tau)$ con g analítica en ρ y $g(\rho) \neq 0$. Si f tiene un cero en ρ queda $m > 0$ y si tiene polo queda $m < 0$. La curva C_1 se parametriza como $\tau = \rho + re^{2\phi i\theta}$ donde r

es fijo, y θ varia desde $\phi/2$ hasta un ángulo α (que depende de r). La primer integral nos queda entonces

$$\frac{1}{2\pi i}\int_{C_1}\frac{f'(\tau)}{f(\tau)}d\tau = \frac{1}{2\pi i}\int_{C_1}\left(\frac{k}{\tau-\rho}+\frac{g'(\tau)}{g(\tau)}\right)d\tau =$$

$$= \frac{1}{2\pi i}\int_{\pi/2}^{\alpha}\left(\frac{k}{re^{\theta i}}+\frac{g'(\rho+re^{i\theta})}{g(\rho+re^{i\theta})}\right)rie^{\theta i}d\theta = \frac{-(\frac{\pi}{2}-\alpha)k}{2\pi}+\frac{r}{2\pi}\int_{\frac{\pi}{2}}^{\alpha}\frac{g'(\rho+re^{\theta i})}{g(\rho+re^{\theta i})}d\theta,$$

pero el último término tiende a 0 cuando $r\to 0$ pues la integral está acotada, por otro lado $\alpha\to\frac{\pi}{6}$ cuando $r\to 0$ así que nos queda

$$\lim_{r\to 0}\frac{1}{2\pi i}\int_{C_1}\frac{f'(\tau)}{f(\tau)}d\tau = -\frac{k}{6}.$$

De forma similar se prueba que

$$\lim_{r\to 0}\frac{1}{2\pi i}\int_{C_3}\frac{f'(\tau)}{f(\tau)}d\tau = -\frac{k}{6}.$$

Y escribiendo cerca de i a f como $f(\tau)=(\tau-i)^l h(\tau)$ con h analítica en i y $h(i)\neq 0$, operando de forma similar a como hicimos antes, nos queda que

$$\lim_{r\to 0}\frac{1}{2\pi i}\int_{C_2}\frac{f'(\tau)}{f(\tau)}d\tau = -\frac{l}{2}.$$

En cuanto a la integral sobre el lado (5) realizando el cambio de variables $q=e^{2\pi i\tau}$, como $\tau = s+Mi$ donde s varia desde $1/2$ hasta $-1/2$, entonces $q = e^{-2\pi M+2\pi is} = e^{-2\pi M}e^{2\pi is}$ recorre la circunferencia C con centro en el origen y radio $e^{-2\pi M}$ en sentido horario. Dado que $f(\tau)=\widehat{f}(q)$ entonces $f'(\tau)d\tau = \widehat{f}'(q)\frac{dq}{d\tau}$, nos queda que

$$\frac{1}{2\pi i}\int_{(5)}\frac{f'(\tau)}{f(\tau)}d\tau = \frac{1}{2\pi i}\int_{C}\frac{\widehat{f}'(q)}{\widehat{f}(q)}dq = ind_C(0)(Z_C-P_C) = -(Z_C-P_C) = P_C-Z_C,$$

donde Z_C y P_C denotan la cantidad de ceros y la cantidad de polos respectivamente de $\widehat{f}$ dentro de la circunferencia C. Pero dada la elección de M tenemos que la región de $R(\Gamma)$ de los puntos con parte imaginaria mayor que M son mapeados dentro de la circunferencia C através del mapa q así que el único posible cero o polo de $\widehat{f}$ dentro de C es en $q=0$. Ahora, si f tiene un desarrollo de Fourier de la forma

$$f(\tau)=\sum_{n=-m}^{\infty}a_n e^{2\pi i\tau},$$

entonces $\widehat{f}$ posee un desarrollo de potencias alrededor de $q=0$ de la forma

$$\widehat{f}(q)=\sum_{n=-m}^{\infty}a_n q^n,$$

así que en todo caso que $P_C-Z_C=m$.

Reuniendo todos los resultados nos queda que

$$\frac{-k}{6}+\frac{-l}{2}+\frac{-k}{6}+m = Z-P.$$

O lo que es lo mismo

$$P+m = Z+\frac{k}{3}+\frac{l}{2},$$

lo cual termina la demostración. □

Corolario 1. Si f es modular y no constante entonces, denotando con Z la cantidad de ceros de f en $R(\Gamma)$ entonces para cada complejo c, la ecuación $f(\tau) = c$ posee exactamente Z soluciones en $R(\Gamma)$ (contados con multiplicidades).

DEMOSTRACIÓN. Si P denota la cantidad de polos de f en $R(\Gamma)$, la función $f - c$ también tendrá P polos en $R(\Gamma)$ y al ser f modular también lo es $f - c$, aplicando el teorema nos queda $Z(f - c) = P(f - c) = P(f) = Z(f) = Z$. □

Corolario 2. Si f es modular y no constante entonces f es sobreyectiva.

DEMOSTRACIÓN. Si no fuese sobreyectiva omite algún valor $c_0 \in \mathbb{H}$, si f no fuese constante entonces por el corolario anterior $0 = Z(f - c_0) = Z(f) = Z(f - c) \quad \forall \tau \in \mathbb{H}$, lo que significa que f no toma ningún valor lo cual es absurdo. □

En particular como J no es constante, si probamos que es modular entonces estaremos probando la sobreyectividad de J. Más aún, probaremos que J es una función analítica en $\mathbb{H}$ con un polo de primer orden en ∞ (es decir que $\widehat{J}$ posee un polo de primer orden en 0), asi que $1 = P(J) = Z(J)$, luego por el corolario 1 tenemos que $J : R(\Gamma) - \{\infty\} \to \mathbb{C}$ es una biyección analítica (claro, contando los puntos de lados equivalentes una sola vez).

Ahora probaremos que J es modular, en primer lugar veamos que es analítica en $\mathbb{H}$.

2.2.1. Analiticidad de J. Recordemos que

$$J(\tau) = \frac{g_2(\tau)}{\Delta(\tau)}$$

donde $\Delta(\tau) = g_2^3(\tau) + 27g_3^2(\tau) \neq 0 \quad \forall \tau \in \mathbb{H}$. Así que alcanza probar que g_2 y g_3 son analíticas como funciones del semiplano superior.

TEOREMA 2.26. *Si $\alpha > 2$ entonces*

$$\sum_{(m,n)\in\mathbb{Z}^*} \frac{1}{(m + n\tau)^\alpha}$$

converge absolutamente y uniformemente en subconjuntos compactos de $\mathbb{H}$.

Obs. Asumiendo el teorema, como $\tau \mapsto \frac{1}{(m+n\tau)^4}$ y $\tau \mapsto \frac{1}{(m+n\tau)^6}$ son analíticas en $\mathbb{H}$ entonces g_2 y g_3 resultan ser funciones analíticas y por el comentario inicial también J lo será.

DEMOSTRACIÓN. La convergencia absoluta ya la tenemos probada por la proposición 3, pues es una suma armónica sobre el láttice con bases $(1, \tau)$, $\tau \in \mathbb{H}$ con $\alpha > 2$.

Consideremos conjuntos rectángulos de la forma $K(A, B) = [-A, A] \times [\frac{1}{B}, B]$ como se muestra en la figura debajo, con $A, B > 0$.

Para probar la convergencia uniforme en subconjuntos compactos alcanza probar la convergencia en los rectangulos $K(A, B)$ pues todo compacto está contenido en algunos de estos rectángulos con A y B suficientemente grandes.

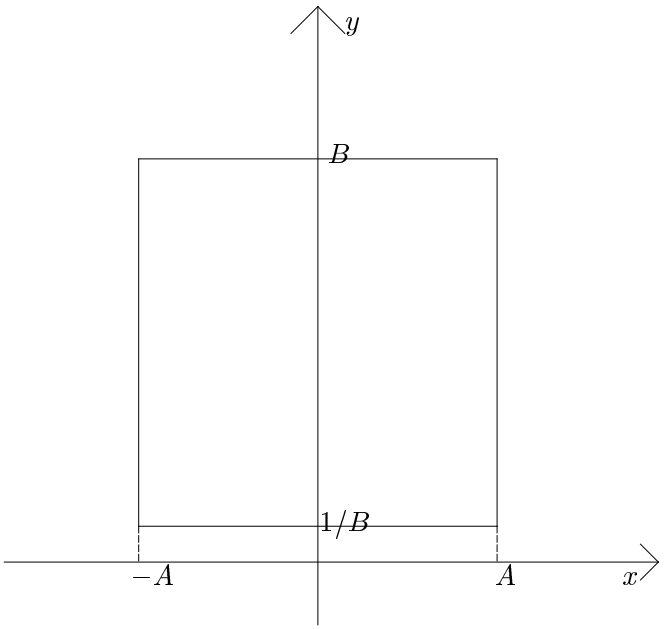


FIGURA 4. Rectángulos $K(A, B)$.

Sea $K = K(A, B)$ con A y B reales positivos fijos, queremos probar la convergencia uniforme sobre K. Como la serie

$$\sum_{(m,n)\in\mathbb{Z}^*} \frac{1}{(m+ni)^\alpha},$$

converge absolutamente por ser una armónica sobre un láttice con $\alpha > 2$, alcanza probar que existe algún $M = M(K) > 0$ tal que

$$\frac{1}{|m+n\tau|^\alpha} \leq \frac{M}{|m+ni|^\alpha},$$

para todo $\tau \in K$ y para todo $(m, n) \in \mathbb{Z}^*$, o equivalentemente que

$$\frac{|m+n\tau|^2}{|m+ni|^2} \geq \left(\frac{1}{M}\right)^{\frac{2}{\alpha}}.$$

Escribiendo a $\tau = x + yi$ y $z = m/n$ tenemos que

$$\frac{|m+n\tau|^2}{|m+ni|^2} = \frac{(m+nx)^2+y^2n^2}{m^2+n^2} = \frac{(z+x)^2+y^2}{z^2+1} = \frac{z^2+2xz+x^2+y^2}{z^2+1} \geq$$

$$\frac{z^2-|2x||z|-|x^2+y^2|}{z^2+1} \geq \frac{|z|^2-2A|z|-(A^2+B^2)}{|z|^2+1} \to 1 \quad \text{cuando } |z| \to \infty.$$

Por lo tanto existe $C > 0$ tal que si $|z| = |m/n| > C$ entonces se cumple que

$$\frac{|m+n\tau|^2}{|m+ni|^2} \geq \frac{1}{2}.$$

Para cuando $|z| \leq C$ consideremos la función

$$f : [-A, A] \times [1/B, B] \times [-C, C] \longrightarrow \mathbb{R} : (x, y, z) \mapsto \frac{(z+x)^2+y^2}{z^2+1},$$

f es una función continua con dominio compacto, por lo tanto $Im(f)$ es un subconjunto compacto de $\mathbb{R}$ así que la función f tiene mínimo m, como f es una función no negativa y que no se anula (pues $f(x,y,z)=0 \Rightarrow y=0$) entonces $m>0$.

Por lo tanto alcanza elegir $M>0$ tal que

$$\left(\frac{1}{M}\right)^{\frac{2}{\alpha}} = min\left\{\frac{1}{2}, m\right\},$$

por ejemplo $M = min\left\{\frac{1}{2}, m\right\}^{-\frac{\alpha}{2}}$ lo cual termina la prueba. □

Como observamos este teorema prueba la analiticidad de J como función del semiplano superior. El siguiente paso para probar la modularidad de J es probar que es una función invariante por la acción del grupo modular.

2.2.2. Invariancia de J por la acción de Γ. Como las funciones g_2 y g_3 son funciones de retículos, también Δ lo es y por lo tanto también J.

PROPOSICIÓN 2.27. *J es invariante por la acción del grupo modular.*

DEMOSTRACIÓN. Sea $\tau \in \mathbb{H}$ y $A \in \Gamma$, escribamos:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

con a, b, c y d enteros tales que $ab - cd = 1$.
Se quiere probar que $J(A\tau) = J(\tau)$ donde la acción por el grupo modular venia dada por

$$A\tau = \frac{a\tau + b}{c\tau + d}.$$

Sea $\mathbb{L}$ el retículo generado por 1 y τ, y $\mathbb{L}'$ el retículo generado por $\omega_1 = c\tau + d$ y $\omega_2 = a\tau + b$.

Tenemos que

$$J(\tau) = J(1, \tau) = J(\mathbb{L})$$

y por otra parte que:

$$J(A\tau) = J(1, A\tau) = J(c\tau + d, a\tau + b) = J(\omega_1, \omega_2) = J(\mathbb{L}'),$$

donde en el segundo igual se usó el hecho de que J es homogenea de grado 0. Así que para probar que $J(A\tau) = J(\tau)$ alcanza probar que los retículos $\mathbb{L}$ y $\mathbb{L}'$ coinciden.

Es inmediato ver que $\mathbb{L}' \subset \mathbb{L}$ puesto que

$$\omega_1 = c \cdot \tau + d \cdot 1 \in \mathbb{L} \quad \text{y} \quad \omega_2 = a \cdot \tau + b \cdot 1 \in \mathbb{L}.$$

Por otra parte tenemos que

$$a\omega_1 - c\omega_2 = ac\tau + ad - ac\tau - bc = ad - bc = 1$$

y que

$$-b\omega_1 + d\omega_2 = -bc\tau - bd + ad\tau + bd = (ad - bc)\tau = \tau.$$

Asi que

$$1 = a\omega_1 - c\omega_2 \in \mathbb{L}' \quad \text{y} \quad \tau = -b\omega_1 + d\omega_2 \in \mathbb{L}',$$

de donde obtenemos la otra inclusión $\mathbb{L} \subset \mathbb{L}'$ y por lo tanto la igualdad que queriamos. □

Como último paso para probar la modularidad probaremos que J es meromorfa en ∞, más aún probaremos que J tiene un polo de primer orden en ∞.

2.2.3. Desarrollo de Fourier de J. Observemos que

$$g_2(\tau+1) = 60 \sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}} \frac{1}{(m+n(\tau+1))^\alpha} = 60 \sum_{(m,n)\in\mathbb{Z}^*} \frac{1}{((m+n)+n\tau)^\alpha}$$

pero mientras (m,n) recorre todo $\mathbb{Z}^2-\{(0,0)\}$ también lo hace $(m+n,n)$ así que $g_2(\tau+1) = g_2(\tau)$.
De manera similar se vé que $g_3(\tau+1) = g_3(\tau)$, así que ambas tienen un desarrollo de Fourier.

LEMA 2.28. *Si $m \in \mathbb{Z}$ con $m > 1$ y consideramos $f : \mathbb{H} \to \mathbb{C}$ dada por*

$$f(\tau) = \sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau)^m},$$

entonces f es periódica de período 1 y posee un desarrollo en serie de Fourier de la forma

$$f(\tau) = (-1)^m \frac{(2\pi i)^m}{(m-1)!} \sum_{n=1}^{\infty} n^{m-1} q^n,$$

donde $q = e^{2\pi i\tau}$.

DEMOSTRACIÓN. Partimos de una identidad para la cotagente:

$$\pi cotg(\pi\tau) = \frac{1}{\tau} + \sum_{n=-\infty\ n\neq 0}^{+\infty} \left(\frac{1}{n+\tau} - \frac{1}{n}\right) \tag{30}$$

Por otra parte tenemos que

$$\pi cotg(\pi\tau) = \pi \frac{cos(\pi\tau)}{sen(\pi\tau)} = \pi i \frac{e^{\pi\tau i} + e^{-\pi\tau i}}{e^{\pi\tau i} e^{-\pi\tau i}} = -\pi i \frac{e^{2\pi i\tau}+1}{e^{2\pi i\tau}-1} = -\pi i \frac{1+q}{1-q} =$$

$$\pi(1+q)\sum_{n=0}^{\infty} q^n = -\pi i \left(\sum_{n=0}^{\infty} q^n + \sum_{n=1}^{\infty} q^n\right) = -\pi i \left(1 + 2\sum_{n=1}^{\infty} q^n\right).$$

Observemos que como $\tau \in \mathbb{H}$ entonces $q = e^{2\pi i\tau}$ pertence al disco unidad, luego es válido el desarrollo en serie de potencias de q en la quinta igualdad.

Sustituyendo en (30) nos queda que

$$\frac{1}{\tau} + \sum_{n=-\infty\ n\neq 0}^{+\infty} \left(\frac{1}{n+\tau} - \frac{1}{n}\right) = -\pi i \left(1 + 2\sum_{n=1}^{\infty} q^n\right),$$

derivando ambos lados respecto de τ nos queda

$$-\frac{1}{\tau^2} - \sum_{n=-\infty\ n\neq 0}^{+\infty} \frac{1}{(n+\tau)^2} = -2\pi i \sum_{n=1}^{\infty} n q^{n-1} (2\pi i q),$$

o bien

$$\sum_{n=-\infty}^{+\infty} \frac{1}{(n+\tau)^2} = -(2\pi i)^2 \sum_{n=1}^{\infty} n q^n.$$

Continuamos derivando con respecto de τ de ambos lados hasta m veces

$$2\sum_{n=-\infty}^{+\infty}\frac{1}{(n+\tau)^3}=-(2\pi i)^3\sum_{n=1}^{\infty}n^2q^n$$

$$-3!\sum_{n=-\infty}^{+\infty}\frac{1}{(n+\tau)^4}=-(2\pi i)^4\sum_{n=1}^{\infty}n^3q^n$$

$$4!\sum_{n=-\infty}^{+\infty}\frac{1}{(n+\tau)^3}=-(2\pi i)^5\sum_{n=1}^{\infty}n^4q^n$$

$$\vdots$$

$$(-1)^{m-1}(m-1)!\sum_{n=-\infty}^{+\infty}\frac{1}{(n+\tau)^m}=-(2\pi i)^m\sum_{n=1}^{\infty}n^{m-1}q^n$$

Despejando de la última ecuación tenemos

$$f(\tau)=\sum_{n=-\infty}^{+\infty}\frac{1}{(n+\tau)^m}=(-1)^m\frac{(2\pi i)^m}{(m-1)!}\sum_{n=1}^{\infty}n^{m-1}q^n.$$

□

Ahora podemos calcular el desarrollo de Fourier para g_2 y g_3.

TEOREMA 2.29. *Las funciones g_2 y g_3 poseen un desarrollo de Fourier de la forma*

$$g_2(\tau)=\frac{4\pi^4}{3}\left(1+240\sum_{k=1}^{\infty}\theta_3(k)q^k\right)\qquad y\qquad g_3(\tau)=\frac{8\pi^6}{27}\left(1-504\sum_{k=1}^{\infty}\theta_5(k)q^k\right),$$

válidos para todo $\tau\in\mathbb{H}$ donde $q=e^{2\pi i\tau}$ y $\theta_n(k)=\sum_{d|k}d^n$ es la función divisor de orden n.

DEMOSTRACIÓN. Recordemos que

$$\frac{1}{60}\ g_2(\tau)=\sum_{(m,n)\in\mathbb{Z}^2-\{(0,0)\}}\frac{1}{(m+n\tau)^4}.$$

En virtud de la convergencia absoluta podemos partir la suma en dos sumas según los índices pertenezcan o no al conjunto $A=\{(m,0):m\in\mathbb{Z},m\neq 0\}$, nos queda

$$\frac{1}{60}g_2(\tau)=\sum_{(m,n)\in A}\frac{1}{(m+0\cdot\tau)^4}+\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\left\{\frac{1}{(m+n\tau)^4}+\frac{1}{(m-n\tau)^4}\right\}.\qquad(31)$$

Ahora por un lado tenemos

$$\sum_{(m,n)\in A}\frac{1}{(m+0\cdot\tau)^4}=\sum_{m=1}^{+\infty}\left(\frac{1}{m^4}+\frac{1}{(-m)^4}\right)=2\sum_{m=1}^{\infty}\frac{1}{m^4}=2\zeta(4)=\frac{2\pi^4}{90}.\qquad(32)$$

Por otra parte

$$\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\left\{\frac{1}{(m+n\tau)^4}+\frac{1}{(m-n\tau)^4}\right\}=2\sum_{n=1}^{+\infty}\sum_{m=-\infty}^{+\infty}\frac{1}{(m+n\tau)^4}=$$

$$= \frac{16\pi^4}{3} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^3 q^{nr} = \frac{16\pi^4}{3} \sum_{k=1}^{\infty} \left(\sum_{d|k} d^3 \right) q^k, \tag{33}$$

donde el primer igual es porque $1/(m-n\tau)^4 = 1/(-m+n\tau)^4$ y mientras (m,n) recorre $\mathbb{Z} \times \mathbb{Z}^+$ también lo hace $(-m,n)$, luego reordeno la serie lo cual es posible por la convergencia absoluta; en el segundo igual hemos usado el lema anterior y en la última igualdad hemos reordenado en potencias de q lo cual es posible también gracias a la convergencia absoluta.

Finalmente, multiplicando ambos miembros de la ecuación (31) por 60 y sustituyendo cada sumando por los resultados de (32) y (33) nos queda

$$g_2(\tau) = 60 \left(\frac{2\pi^4}{90} + \frac{16\pi^4}{3} \sum_{k=1}^{\infty} \theta_3(k) q^k \right) = \frac{4\pi^4}{3} + 20 \cdot 16\pi^4 \sum_{k=1}^{\infty} \theta_3(k) q^k = \frac{4\pi^4}{3} \left(1 + 240 \sum_{k=1}^{\infty} \theta_3(k) q^k \right).$$

De forma análoga tenemos un resultado similar para g_3:

$$g_3(\tau) = \frac{8\pi^6}{27} \left(1 - 504 \sum_{k=1}^{\infty} \theta_5(k) q^k \right)$$

□

Observemos que hemos probado la analiticidad de g_2 y g_3 en el infinito lo cual implica a su vez la analiticidad de $\Delta = g_2^3 - 27 g_3^2$ y por lo tanto $J = g_2^3/\Delta$ será una función meromorfa en el infinito que era lo que faltaba ver para probar que f es una función modular y por lo tanto sobreyectiva.

Para culminar esta sección probaremos que J posee un polo de primer orden en el infinito que como habíamos observado anteriormente esto implica la inyectividad de J (restricta a $R(\Gamma) - \{\infty\}$ con la convención sobre los bordes).

PROPOSICIÓN 2.30. *J es una función modular con un polo de primer orden en el infinito (es decir $\widehat{J}$ posee un polo de primer orden en cero).*

DEMOSTRACIÓN. La modularidad de J ya la tenemos probada como mencionamos en la observación anterior. Como $J = g_2^3/\Delta$ entonces $\widehat{J} = \widehat{g_2^3}/\widehat{\Delta}$, como $\widehat{g_2}$ es analítica en el origen y $\widehat{g_2}(0) = \frac{4\pi^4}{3} \neq 0$ entonces para probar que $\widehat{J}$ posee un polo de primer orden en $q = 0$ alcanza probar que $\widehat{\Delta}$ posee un cero de primer orden en $q = 0$.

Tenemos que $\widehat{\Delta} = \widehat{g_2}^3 - 27\widehat{g_3}^2$ ahora utilizamos los desarrollos en serie de Fourier de g_2 y g_3 cuyos coeficientes son por definición los del desarrollo alrededor del origen de $\widehat{g_2}$ y $\widehat{g_3}$ tenemos entonces

$$\widehat{g_2}(q) = \frac{4\pi^4}{3} \left(1 + 240 \sum_{k=1}^{\infty} \theta_3(k) q^k \right) \qquad \text{y} \qquad \widehat{g_3}(q) = \frac{8\pi^6}{27} \left(1 - 504 \sum_{k=1}^{\infty} \theta_5(k) q^k \right),$$

así que

$$\widehat{g_2}(0) = \frac{4\pi^4}{3} \quad \text{y} \quad \widehat{g_3}(0) = \frac{8\pi^6}{27},$$

luego

$$\widehat{\Delta}(0) = \widehat{g_2}^3(0) - 27\widehat{g_3}^2(0) = \left(\frac{4\pi^4}{3}\right)^3 - 27\left(\frac{8\pi^6}{27}\right)^2 = 0.$$

Para ver que el cero es de primer orden calculemos primero los valores de $\widehat{g_2}'$ y $\widehat{g_3}$ en el origen:

$$\widehat{g_2}'(0) = \frac{4\pi^4}{3} \cdot 240\theta_3(1) = 320\pi^4 \widehat{g_3}'(0) = \frac{8\pi^6}{27} \cdot (-504)\theta_5(1) = -\frac{448\pi^6}{3}$$

puesto que $\theta_n(1) = 1^n = 1$ para todo $n \geq 1$.

Finalmente el cero es de primer orden puesto que

$$\widehat{\Delta}'(0) = 3\widehat{g_2}^2(0)\widehat{g_2}'(0) - 27 \cdot 2\widehat{g_3}(0)\widehat{g_3}'(0) = 3\left(\frac{4\pi^4}{3}\right)^2 \cdot 320\pi^4 - 27 \cdot 2\left(\frac{8\pi^6}{27}\right) \cdot \left(-\frac{448\pi^6}{3}\right) > 0.$$

□

3. Puntos de orden finito en $E(\mathbb{R})$.

Aquí estudiaremos los puntos de orden finito sobre una curva elíptica definida sobre los reales, probaremos que los puntos de orden m forman o bien un grupo cíclico de m elementos o bien es el producto de un grupo cíclico por un grupo de dos elementos.

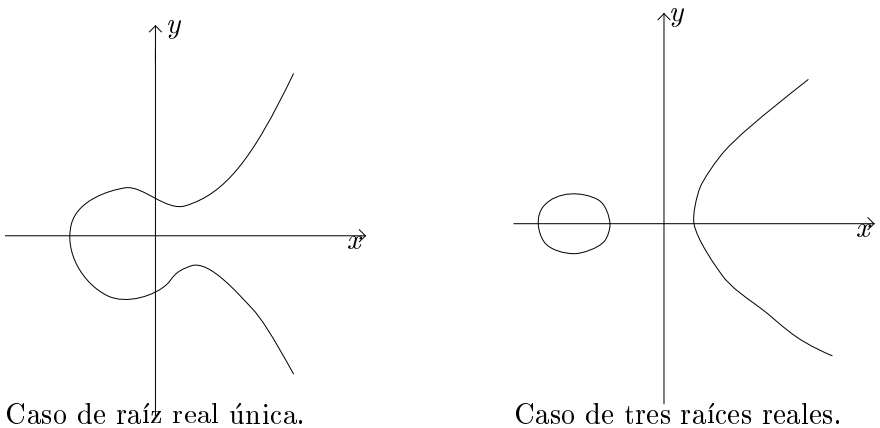
La herramienta que usaremos aquí para atacar este problema son los grupos de Lie. Un grupo de Lie es una variedad diferenciable $\mathcal{G}$ con una operación binaria que le da estructura de grupo, se le pide además que la operación de suma y tomar inverso sean funciones diferenciables.

Sea $E : Y^2 = X^3 + aX + b$ una curva elíptica con $a, b \in \mathbb{R}$, E posee estructura de variedad diferenciable unidimensional, en efecto si $F(X, Y) = X^3 + aX + b - Y^2$ tenemos que $\nabla F(x, y) \neq (0, 0)$ para todo $(x, y) \in E$ pues E es no singular (y por lo tanto el polinomio $f(X) = X^3 + aX + b$ no posee raíces dobles) así que por el Teorema de la función implícita E se parametriza con una variable alrededor de todo punto $(x, y) \in E$. Para el punto $[0 : 1 : 0]$ tomemos la ecuación proyectiva de la cúbica $E : Y^2Z = X^3 + aXZ^2 + bZ^3$ y la miramos nuevamente en el plano afín $Y = 1$, nos queda $E : Z = X^3 + aXZ^2 + bZ^3$, aquí tenemos que el polinomio $F(X, Z) = X^3 + aXZ^2 + bZ^3 - Z$ que verifica $\nabla F(0, 0) = (0, -1) \neq (0, 0)$ así que F se puede parametrizar diferenciablemente con una variable alrededor de $(0, 0)$ (que corresponde al punto $[0 : 1 : 0]$ de E).

La operación de suma en la curva elíptica resulta una función diferenciable al igual que tomar opuesto, esto se deduce observando las fórmulas explícitas para la ley de grupo (que resultan funciones racionales de sus variables).

Llamemos $f(X) = X^3 + aX + b$, la curva elíptica $E : Y^2 = f(X)$ tendrá una o dos componentes conexas según f posea una o tres raíces reales (ver figura).

Como todo grupo de Lie unidimensional compacto es isomorfo a S^1 con la multiplicación compleja, para el caso en que f posea una única raíz real tenemos que $(E, \oplus)$ es isomorfo a $(S^1, \cdot)$, así que los puntos de orden divisor de m en E es isomorfo al de los puntos de orden divisor de m en S^1 que es el grupo de las raíces m-ésimas de la unidad



Caso de raíz real única. Caso de tres raíces reales.

FIGURA 5. Curvas elípticas sobre $\mathbb{R}$

que es a su vez isomorfo a $\mathbb{Z}_m$.

Para el caso en que f se escinda en $\mathbb{R}$ tenemos que $E(\mathbb{R})$ posee dos componentes conexas, llamemos E_0 la componente que contiene al elemento neutro del grupo $\mathcal{O} = [0 : 1 : 0]$. Si $x, y \in E_0$, como la función $S_x : E \to E$: $S_x(a) = x + a$ es continua entonces lleva la componente conexa E_0 es otra componente conexa que contiene a $S_x(\mathcal{O}) = x$ y por lo tanto es la misma E_0, esto prueba que $x + y = S_x(y) \in E_0$. De la misma manera tenemos que $I : E \to E$ lleva E_0 a E_0 y por lo tanto tenemos que E_0 es un subgrupo de E.

Si $x \notin E_0$ entonces $x + E_0$ es la componente conexa de E que no contiene al neutro, en efecto, $a \mapsto x + a$ es continua, entonces lleva la componente conexa E_0 en otra componente conexa que contiene a $x + \mathcal{O} = x \in E_0$, entonces $E = E_0 \uplus x + E_0$ para todo $x \notin E_0$ y por lo tanto el grupo cociente $E/E_0 = \{E_0, x + E_0\}$ es isomorfo a $\mathbb{Z}_2$.

El isomorfismo que lleva E/E_0 en $\mathbb{Z}_2$ es la función que lleva $E_0 \mapsto 0$ y $E_1 \mapsto 1$ donde E_1 es la componente conexa de E que no contiene a la identidad.

Ahora definimos la función

$$\varphi : E \longrightarrow \frac{E}{E_0} \times E_0 : \varphi(x) = \begin{cases} (C(x), x) \\ (C(x), x - c) \end{cases},$$

donde $C(x)$ denota la componente conexa de E que contiene a x y c es cualquiera de los dos puntos de corte del eje real con E que pretenecen a la componente conexa de E que no contiene al punto $\mathcal{O}$ (la coodenada en X de c es nula y por lo tanto $2c = \mathcal{O}$) .

Veamos que es un morfismo: en la primera coordenada es claro pues es la proyección sobre el cociente, en la segunda solo queda chequear el caso en que $x, y \in E_1$ (los otros son claros), para este caso tenemos que $x+y \in E_1+E_1 = E_0$ y por lo tanto $\varphi(x+y) = (E_0, x+y)$ mientras que $\varphi(x) + \varphi(y) = (E_1, x - c) + (E_1, y - c) = (E_1 + E_1, (x - c) + (y - c)) = (E_0, x + y - 2c) = (E_0, x + y)$.

Es claramente inyectiva, para ver que es sobre tomemos $a \in\!\!\longrightarrow E/E_0 \times E_0$, si $a = (E_0, x)$ tenemos que $a = \varphi(x)$ pues $x \in E_0$, si $a = (E_1, x)$ tenemos que $x - c \in E_1$

(pues $x \in E_0$ y $c \in E_1$) y por lo tanto $\varphi(x-c) = (E_1, (x-c)-c) = (E_1, x-2c) = (E_1, x)$.

Como E_0 es un subgrupo de Lie de E que es conexo, compacto y unidimensional entonces es isomorfo al grupo S^1 con la multiplicación compleja y por lo tanto φ induce un isomorfismo entre $(E, \oplus)$ con el grupo producto $(\mathbb{Z}_2, +) \times (S^1, \cdot)$.

Observemos que un punto de orden divisor de m en $\mathbb{Z}_2 \times S^1$ es de la forma (ϵ, x) donde $m\epsilon = 0 \pmod 2$ y $x^m = 1$; si m es par la primer condición se verifica trivialmente y solo se requiere que x pertenezca al grupo de las raíces m-ésimas de la unidad y por lo tanto los elementos de orden divisor de m forman un grupo isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_m$. Para el caso en que m sea impar, la condición $m\epsilon = 0 \pmod 2$ es equivalente a pedir que $\epsilon = 0 \pmod 2$ y por lo tanto el subgrupo de los elementos de orden divisor de m forman un grupo isomorfo a $\mathbb{Z}_m$.

En resumen, tenemos dos casos:

1. Si f posee una única raíz real entonces $E(\mathbb{R})[m] \simeq \mathbb{Z}_m$.
2. Si f posee tres raíces reales entonces $E(\mathbb{R})[m] \simeq \begin{cases} \mathbb{Z}_m \text{ si } m \text{ es impar.} \\ \mathbb{Z}_2 \times \mathbb{Z}_m \text{ si } m \text{ es par.} \end{cases}$

CAPíTULO 3

Puntos de orden finito en $E(\mathbb{Q})$.

1. Puntos de orden finito en $E(\mathbb{Q})$.

En las secciones anteriores nos hemos encargado de estudiar los puntos de orden finito en $E(\mathbb{C})$ y $E(\mathbb{R})$, ahora nos encargaremos de ver que pasa para el caso racional.

Partamos con una curva elíptica $E/\mathbb{Q}$, supongamos que venga dada por una ecuación $E : Y^2 = X^3 + aX + b$ con $a, b \in \mathbb{Q}$, si m es el mínimo común múltiplo de los denominadores de a y b entonces la ecuación que define E puede escribirse como $m^6Y^2 = m^6X^3 + m^6aX + m^6b$ o equivalentemente $(m^2Y)^3 = (m^2X)^3 + am^4(m^2X) + bm^6$ con el cambio de variable $(A, B) = (m^2X, m^2Y)$ podemos escribir la curva $B^2 = A^3 + sA + t$ donde los coeficientes $s = am^4, t = bm^6$ son enteros. De aquí en más supondremos que la curva viene dada en su forma de Weiestrass reducida y que los coeficientes además son enteros.

El objetivo de esta sección es probar el Teorema de Nagell-Lutz que enunciaremos a continuación:

TEOREMA 3.1 (Teorema de Nagell-Lutz.). *Sea* $E : Y^2 = f(X)$, *donde* $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$.

Si $P = (x, y)$ *es un punto de orden finito de* $E(\mathbb{Q})$ *entonces:*

1. *El punto* P *tiene coordenadas enteras.*
2. $y = 0$ *(para el caso* $ord(P) = 2$*) ó* $y \mid \Delta$ *(para el caso* $ord(P) > 2$*), donde* Δ *es el discriminante de* f.

1.1. El discriminante. Si $f(X) = X^3 + aX + b \in \mathbb{Z}$, su discriminante viene dado por

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2,$$

donde α_1, α_2 y α_3 son las raíces complejas de f. Utilizando las relaciones entre coeficientes y raíces también puede escribirse

$$\Delta = -(4a^3 + 27b^2).$$

La propiedad que necesitaremos del discriminante es que puede ser escrito como combinación lineal de f y f'.

PROPOSICIÓN 3.2. *Existen polinomios* r *y* s *con coeficientes enteros tales que*

$$r(x)f(x) + s(x)f'(x) = \Delta.$$

DEMOSTRACIÓN. Tomar $r(X) = 18aX - 27b$ y $s(x) = -6aX^2 + 9bX - 4a^2$. □

Esta proposición es un caso particular de un teorema más general, pero para este caso resulta más sencillo dar fórmulas explícitas para r y s.

1.2. La condición de divisibilidad. Supongamos que tenemos probada la primera parte de Nagell-Lutz, si P fuese un punto de orden finito entonces también $2P$ lo será, luego tanto P como $2P$ tienen coordenadas enteras. La siguiente proposición reduce entonces la prueba del Teorema de Nagell-Lutz a probar solo la primera parte.

PROPOSICIÓN 3.3. *Si $P = (x, y)$ y $2P$ tienen coordenadas enteras entonces $y = 0$ o $y \mid \Delta$.*

DEMOSTRACIÓN. Si $2P = \mathcal{O}$ entonces $y = 0$.

Si $2P \neq \mathcal{O}$ entonces $y \neq 0$ y aplicamos la fórmula de duplicación

$$x(2P) = \left(\frac{f'(x)}{2y}\right)^2 - 2x.$$

Como $2P \neq \mathcal{O}$, por hipótesis $x(2P) \in \mathbb{Z}$, luego $2y \mid f'(x)$, así que $y \mid f'(x)$. Por otro lado $y \mid y^2 = f(x)$ así que

$$y \mid r(x)f(x) + s(x)f'(x) = D,$$

donde los polinomios $r, s \in \mathbb{Z}[X]$ son los de la proposición anterior. □

1.3. Teorema de Nagell-Lutz. En esta sección probaremos que los puntos de orden finito de la curva elíptica $E : Y^2 = X^3 + aX + b$ con $a, b \in \mathbb{Z}$, tienen coordenadas enteras completando la demostración de Nagell-Lutz.

Sea $P = (x, y) \in E(\mathbb{Q})$ un punto de orden finito, la idea central para probar que x e y son enteros es probar que sus denominadores no son divisibles por ningún primo p. Comenzamos escribiendo

$$x = \frac{m}{np^\mu} \quad \text{e} \quad y = \frac{u}{wp^\theta},$$

donde m, n, u y w son enteros con $\text{mcd}\{mnuw, p\} = 1$, y haremos la prueba por absurdo, suponiendo que $\mu > 0$ ó $\theta > 0$.

Como $(x, y) \in E(\mathbb{Q})$ tenemos que sus coordenadas verifican $y^2 = x^3 + ax + b$, sustituyendo x e y por sus expresiones como fracciones, nos queda

$$\frac{u^2}{w^2p^{2\theta}} = \frac{m^3 + an^2p^{2\mu}m + n^3p^{3\mu}b}{n^3p^{3\mu}}. \tag{34}$$

Observamos aquí que si $\mu > 0$ como p no divide a m tenemos que también $\theta > 0$. Ahora supongamos que $\mu < 0$, multiplicando por $p^{-3\mu}$ al numerador y denominador del segundo miembro de la ecuación (34) tenemos

$$\frac{u^2}{w^2p^{2\theta}} = \frac{p^{-3\mu}m^3 + an^2p^{-\mu}m + n^3b}{n^3},$$

como n no es divisible por p tenemos $\theta \leq 0$.

Esto prueba que $\mu > 0 \Leftrightarrow \theta > 0$, así que tenemos entonces que μ y θ son ambos positivos (y en particular x e y son no nulos) y de la ecuación (34) como $\text{mcd}\{m^3 + an^2p^{2\mu}m + n^3p^{3\mu}b, p\} = \text{mcd}\{m^3, p\} = \text{mcd}\{m, p\} = 1$ tenemos $2\theta = 3\mu > 0$, así que $\theta = 3\nu$ y $\mu = 2\nu$ para algún entero positivo ν. Luego los puntos $P = (x, y) \in E(\mathbb{Q})$ pueden escribirse de la forma

$$x = \frac{m}{np^{2\nu}} \quad \text{e} \quad y = \frac{u}{wp^{3\nu}}. \tag{35}$$

Consideremos los siguientes subconjuntos de $E(\mathbb{Q})$:

$$C(p^\nu) = \{P = (x, y) \in E(\mathbb{Q}) : \nu_p(x) \leq -2\nu \ , \ \nu_p(y) \leq -3\nu\} \cup \{\mathcal{O}\}$$

donde para $z \in \mathbb{Q}$, $z \neq 0$, $\nu_p(z)$ es la valuación p-ádica definida como el único entero k tal que $z = p^k \frac{m}{n}$ con $\text{mcd}\{mn, p\} = 1$ (cuya existencia y unicidad es inmediata a partir de la descomposición única en los enteros). Tenemos una cadena de subconjuntos de $E(\mathbb{Q})$:

$$C(p) \supset C(p^2) \supset C(p^3) \supset \ldots \supset C(p^\nu) \supset \ldots$$

Probamos hasta ahora que si $P = (x, y) \in E(\mathbb{Q})$ es un punto tal que $\nu_p(x) < 0$ ó $\nu_p(y) < 0$ entonces ambos son negativos y pertence a algún $C(p^\nu)$ para algún $\nu \in \mathbb{Z}^+$. Como p solo puede dividir una cantidad finita de veces a los númeradores de x e y tenemos que existe un ν máximo para el cual $P \in C(p^\nu)$.

La prueba del Teorema de Nagell-Lutz consiste en dos partes que enunciaremos como proposiciones:

PROPOSICIÓN 3.4. *Los subconjuntos $C(p^\nu)$ para $\nu \geq 1$ son subgrupos de $E(\mathbb{Q})$.*

PROPOSICIÓN 3.5. *Si denotamos por R al conjunto de racionales con valuación p-ádica no negativa (o sea tales que p no divida al denominador) tenemos que para cada $\nu = 1, 2, \ldots$ la función*

$$t_\nu : C(p^\nu) \longrightarrow \frac{p^\nu R}{p^{3\nu} R} \ , \quad t_\nu(P) = \begin{cases} x/y & \text{si } P = (x, y) \\ 0 & \text{si } P = \mathcal{O} \end{cases}$$

es un morfismo de grupos de kernel $C(p^{3\nu})$.

DEMOSTRACIÓN DE NAGELL-LUTZ A PARTIR DE LAS PROPOSICIONES ANTERIORES: Comenzemos tomando un punto $P = (x, y)$ de orden finito y supongamos que para algún primo p tenemos $\nu_p(x) < 0$ ó $\nu_p(y) < 0$, como ya vimos esto implica que $\nu_p(x) = -2\nu$ y $\nu_p(y) = -3\nu$ para algún $\nu \in \mathbb{Z}^+$.

Esto implica que $P \in C(p^\nu)$ pero $P \notin C(p^{\nu+1})$. Sea $m = ord(P)$, conviene separar en dos casos:

Si p no divide a m tenemos

$$0 = t_\nu(\mathcal{O}) = t_\nu(mP) \equiv mt(p) \pmod{p^{3\nu}}.$$

Por lo tanto

$$t_\nu(P) \equiv 0 \pmod{p^{3\nu}}$$

Así que $P \in \text{Ker}(t_\nu) = C(p^{3\nu})$ lo cual es absurdo puesto que $3\nu > \nu$.

Si p divide a m podemos escribir $m = np$ con $n \in \mathbb{Z}^+$ y considerar el punto $P' = nP \in C(p)$ (puesto que $P \in C(p)$ y $C(p)$ es un grupo). Consideremos el mayor entero ν tal que $P' \in C(p^\nu)$, tenemos

$$0 = t_\nu(\mathcal{O}) = t_\nu(pP') \equiv pt_\nu(P') \pmod{p^{3\nu}}.$$

Así que

$$t_\nu(P') \equiv 0 \pmod{p^{3\nu-1}}$$

Pero $P = (x, y) \in C(p^\nu)$ así que $x' = ap^{-2\nu}$ e $y' = bp^{-3\nu}$ donde a y b son racionales con valuación p-ádica nula, luego

$$t_\nu(P') = \frac{x}{y} = \frac{a}{b}p^\nu \equiv 0 \pmod{p^{3\nu-1}},$$

como $\nu_p(\frac{a}{b}) = \nu_p(a) - \nu_p(b) = 0 - 0 = 0$ esto implica que $\nu \geq 3\nu - 1$ lo cual es absurdo pues $\nu \geq 1$. □

Demostración de las proposiciones:

Comenzemos considerando el cambio de coordenadas

$$\varphi : P^2(\mathbb{Q}) \longrightarrow P^2(\mathbb{Q}), \quad [x : y : z] \mapsto [y : z : x].$$

Es claro que el punto $[x : y : z] \in P^2(\mathbb{Q})$ verifica la ecuación

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

si y solo si el punto $[z : x : y]$ verifica la ecuación

$$E' : Z^2X = Y^3 + aYX^2 + bX^3,$$

de modo que φ resulta un isomorfismo entre las curvas elípticas E y E'. La ecuación afin de esta nueva curva E' (con $Z = 1$) toma la forma

$$E' : X = Y^3 + aYX^2 + bX^3.$$

Si $P = (x, y) \in E$ con $y \neq 0$ entonces $\varphi(P) = [1 : x : y] = (1/y, x/y)$. Denotando por $s = 1/y$ y por $t = x/y$ tenemos que el punto (x, y) con $y \neq 0$ de E le corresponde através de φ el punto (s, t) de la curva elíptica

$$E' : S = T^3 + aTS^2 + bS^3.$$

Observemos que esta nueva curva E' consiste de puntos (s, t) como arriba, el punto del infinito $\mathcal{O} \in E$ fue a parar al origen $(0, 0) \in E'$ que es el neutro del grupo de la curva elíptica E' y los puntos de orden 2 de E que son de la forma $(\alpha, 0) = [\alpha : 0 : 1]$ con α raíz racional del polinomio $f(X) = X^3 + aX + b$, van a parar a los puntos $[1 : \alpha : 0] \in E'$ que son los puntos de orden 2 de E' (que llamaremos los puntos del infinito de la curva E').

Como el grupo de $E'(\mathbb{Q})$ es isomorfo a $E(\mathbb{Q})$ tenemos que $O = (0, 0)$ es de inflexión de E' así que se sigue cumpliendo que tres puntos suman cero si y solo si están alineados, luego si $P = (s, t) \in E'$ tenemos que $-P = P * O = (-s, -t)$ pues E' es simétrica respecto del origen.

Proposición 3.6. *Si denotamos por $C(p^\nu)'$ los puntos de $E'(\mathbb{Q})$ de la forma*

$$C(p^\nu)' = \{(s, t) \in E'(\mathbb{Q}) : \nu_p(t) \geq \nu\} \cup \{(0, 0)\},$$

tenemos que $\varphi^{-1}(C(p^\nu)') = C(p^\nu) \subset E(\mathbb{Q})$.

Luego para probar que $C(p^\nu)$ es un subgrupo de $E(\mathbb{Q})$ alcanza con probar que $C(p^\nu)'$ lo es de $E'(\mathbb{Q})$.

DEMOSTRACIÓN. Sea $P = (x, y) \in E$ con $y \neq 0$, en virtud de la ecuación (35) las coordenadas pueden ponerse en forma reducida de la siguiente manera

$$x = \frac{m}{np^{2\nu_0}} \quad \text{e} \quad y = \frac{u}{wp^{3\nu_0}}.$$

Observemos que si P verifica que $\varphi(P) \in C(p^\nu)'$ entonces $\nu_p(t) = \nu_p(x/y) = \nu_p(x) - \nu_p(y) = \nu_0$ con $\nu_0 \geq \nu$.

Habíamos probado que $\nu_p(x) = \frac{2}{3}\nu_p(y)$, luego tenemos

$$\nu_0 = \nu_p(x) - \nu_p(y) = 2/3\ \nu_p(y) - \nu_p(y) = -1/3\ \nu_p(y)$$

Luego

$$\nu_p(y) = -3\nu_0 \leq -3\nu,$$

y además

$$\nu_p(x) = 2/3\ \nu_p(y) = 2/3\ (-3\nu_0) = -2\nu_0 \leq -2\nu.$$

Luego $P \in C(p^\nu)$.

Para los puntos de la forma $P = [\alpha : 0 : 1]$ tenemos $\varphi(P) = [1 : \alpha : 0] \not\in C(p^\nu)'$.

Para $P = \mathcal{O}$ tenemos que $\varphi(P) = (0, 0) \in C(p^\nu)'$.

Recíprocamente, si $P = (x, y) \in C(p^\nu)$, $P \neq \mathcal{O}$ tenemos que $\nu_p(x) = -2\nu_0$ y $\nu_p(y) = -3\nu_0$ para algún $\nu_0 \geq \nu$. Luego $\nu_p(t) = \nu_p(x/y) = \nu_p(x) - \nu_p(y) = \nu_0 \geq \nu$ y por lo tanto $\varphi(P) \in C(p^\nu)'$, lo cual prueba la proposición 3.6. □

Con las mismas notaciones que arriba observemos que

$$\nu_p(s) = \nu_p(1/y) = -\nu_p(y) = 3\nu_0 = 3\nu_p(t),$$

pero como ya vimos, todo punto de $C(p^\nu)'$ distinto de $(0, 0)$ proviene de un punto de $C(p^\nu)$ distinto de $\mathcal{O}$ así que para todo punto $P = (s, t) \in C(p^\nu)'$ distinto del origen, tenemos que

$$\nu_p(s) = 3\nu_p(t), \tag{36}$$

esta última observación nos será de utilidad más adelante.

Ahora probemos que efectivamente, $C(p^\nu)'$ es un subgrupo de E'.

PROPOSICIÓN 3.7. *El subconjunto $C(p^\nu)'$ de $E'(\mathbb{Q})$ es además un subgrupo.*

DEMOSTRACIÓN. Tomemos entonces dos puntos $P_1 = (s_1, t_1)$ y $P_2 = (s_2, t_2)$ tales que $\nu_p(t_1) \geq \nu$ y $\nu_p(t_2) \geq \nu$, podemos suponer que P_1 y P_2 son distintos del origen (si alguno o ambos son $(0, 0)$ es claro que $P_1 \oplus P_2 \in C(p^\nu)'$ pues $(0, 0)$ es el neutro de $E'(\mathbb{Q})$).

Queremos probar que $P_1 \oplus P_2$ no es uno de los puntos del infinito y que $\nu_p(t(P_1 \oplus P_2)) \geq \nu$.

Sea $S = mT + n$ la recta que pasa por P_1 y por P_2 (o la recta tangente a $E'(\mathbb{Q})$ por P_1 si $P_1 = P_2$).

Comenzemos hallando $m = \frac{s_2 - s_1}{t_2 - t_1}$ para el caso en que $P_1 \neq P_2$, como ambos puntos están sobre la cúbica $E'(\mathbb{Q})$ se tiene

$$s_1 = t_1^3 + at_1s_1^2 + bs_1^3$$
$$s_2 = t_2^3 + at_2s_2^2 + bs_2^3.$$

Restamos ambas ecuaciones:

$$s_2 - s_1 = (t_2 - t_1)(t_2^2 + t_2t_1 + t_1^2) + a(t_2(s_2^2 - s_1^2) + s_1^2(t_2 - t_1)) + b(s_2 - s_1)(s_2^2 + s_2s_1 + s_1^2)$$

Pasamos los términos que contienen $s_2 - s_1$ para la izquierda y agrupamos en $s_2 - s_1$ y $t_2 - t_1$:

$$(s_2 - s_1)(1 - at_2(s_1 + s_2) - b(s_2^2 + s_2s_1 + s_1^2)) = (t_2 - t_1)(t_2^2 + t_2t_1 + t_1^2 + s_1^2a) \tag{37}$$

Como $\nu_p(t_1) \geq \nu > 0$ y $\nu_p(t_2) \geq \nu > 0$, por la ecuación (36) tenemos que también $\nu_p(s_1) \geq \nu$ y $\nu_p(s_2) \geq \nu$, como a y b son enteros entonces también $\nu_p(at_2(s_1 + s_2) + b(s_2^2 + s_2s_1 + s_1^2)) > 0$ lo cual implica

$$\nu_p(1 - at_2(s_1 + s_2) - b(s_2^2 + s_2s_1 + s_1^2)) = 0 \tag{38}$$

y en particular $1 - at_2(s_1 + s_2) - b(s_2^2 + s_2s_1 + s_1^2) \neq 0$.

Si $t_2 - t_1 = 0$ por la ecuación (37) también $s_2 - s_1 = 0$ lo cual implica $P_1 = P_2$, como supusimos que eran distintos entonces $t_2 - t_1 \neq 0$ luego

$$m = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_2t_1 + t_1^2 + s_1^2a}{1 - at_2(s_1 + s_2) - b(s_2^2 + s_2s_1 + s_1^2)}. \tag{39}$$

Para el caso en que $P_1 = P_2$, m es la pendiente de la tangente a la cúbica por $P_1 = (s_1, t_1)$, comenzamos por la ecuación de $E'(\mathbb{Q})$

$$s = t^3 + ats^2 + bs^3,$$

derivando formalmente:

$$\frac{ds}{dt} = 3t^2 + as^2 + 2ats\frac{ds}{dt} + 3bs^2\frac{ds}{dt}$$

de donde

$$\frac{ds}{dt} = \frac{3t^2 + as^2}{1 - 2ats - 3bs^2}.$$

Luego en el caso que $P_1 = P_2$, m viene dada por

$$m = \frac{3t_1^2 + as_1^2}{1 - 2at_1s_1 - 3bs_1^2},$$

que es la misma fórmula dada para m en (39) con $s_1 = s_2$ y $t_1 = t_2$, así que para ambos casos podemos usar (39).

Calculemos ahora la valuación p-ádica de m utilizando la fórmula (39). La ecuación (38) nos dice que el denominador de m tiene valuación p-ádica nula, mientras que para el numerador, dado que a es entero y que la valuación p-ádica de t_1, t_2 y s_1 es mayor o igual que ν (t_1 y t_2 por hipótesis y s_1 por (36)) tenemos que

$$\nu_p(t_2^2 + t_2t_1 + t_1^2 + s_1^2a) \geq 2\nu.$$

Por lo tanto

$$\nu_p(m) \geq 2\nu \tag{40}$$

La recta $S = mT + n$ intersecta a la cúbica

$$E'(\mathbb{Q}) : S = T^3 + aTS^2 + bS^3$$

en

$$P_1 = (s_1, t_1)\ ,\ P_2 = (s_2, t_2) \text{ y } -(P_1 \oplus P_2)$$

Veamos a continuación que $-(P_1 \oplus P_2)$ no es un punto del infinito, si lo fuese, sería de orden 2 así que como vimos $P_1 \oplus P_2 = -(P_1 \oplus P_2) = [1 : \alpha : 0]$ donde α es una raíz racional del polinomio $f(X) = X^3 + aX + b$. Luego el punto $[S : T : U] = [1 : \alpha : 0]$ sería solución de

$$\begin{cases} S = mT + nU \\ 0 = T^3 + aTS^2 + bS^3 \end{cases},$$

por lo tanto $1 = m\alpha$ y $\alpha^3 + a\alpha + b = 0$ lo cual implica que $m \neq 0$ y que

$$\left(\frac{1}{m}\right)^3 + a\left(\frac{1}{m}\right) + b = 0,$$

multiplicando por m^3 de ambos lados:

$$1 + am^2 + bm^3 = 0$$

lo cual es absurdo pues por (40) $\nu_p(m) \geq 2\nu$ y como a y b son enteros $\nu_p(am^2 + bm^3) \geq 4\nu > 0$ así que $\nu_p(1 + am^2 + bm^3) = 0$ por lo tanto $1 + am^2 + bm^3 \neq 0$.

Concluimos que el tercer punto de corte $-(P_1 \oplus P_2)$ debe ser afin así como $P_1 \oplus P_2 = (s, t)$ (y por lo tanto $-(P_1 \oplus P_2) = (P_1 \oplus P_2) * (0, 0) = (-s, -t)$).

Así que t_1, t_2 y $-t$ son raíces de la ecuación

$$mT + n = T^3 + aT(mT + n)^2 + b(mT + n)^3,$$

que es una ecuación de tercer grado en T, agrupando en potencias de T nos queda

$$(1 + am^2 + bm^3)T^3 + (2a + 3bm)mnT^2 + (an^2 + 3bmn^2 - m)T + (bn^2 - 1)n = 0. \tag{41}$$

Usando las relaciones entre coeficientes y raíces y que $1 + am^2 + bm^3 \neq 0$ tenemos que

$$t_1 + t_2 - t = -\frac{(2an + 3bmn)m}{1 + am^2 + bm^3}, \tag{42}$$

de donde

$$t = t_1 + t_2 + \frac{(2an + 3bmn)m}{1 + am^2 + bm^3}. \tag{43}$$

Nuestro objetivo era probar que $\nu_p(t) \geq \nu$, partimos de que $\nu_p(t_1) \geq \nu$ y que $\nu_p(t_2) \geq \nu$, que por (36) tenemos también que $\nu_p(s_1) \geq \nu$ y $\nu_p(s_2) \geq \nu$.

Recordemos que por (40) teniamos que $\nu_p(m) \geq 2\nu$, dado que $\nu_p(t_1) \geq \nu$ y $\nu_p(s_1) \geq \nu$, para n también tenemos que

$$\nu_p(n) = \nu_p(s_1 - mt_1) \geq \nu.$$

Ahora miramos la ecuación (43), dado que $\nu_p(m) \geq \nu$ y que a y b son enteros entonces

$$\nu_p(am^2 + bm^3) \geq \nu > 0,$$

luego

$$\nu_p(1 + am^2 + bm^3) = 0,$$

y como $\nu_p(m) \geq 2\nu$ y $\nu_p(n) \geq \nu$:

$$\nu_p((2an + 3bmn)m) = \nu_p((2a + 3bm)mn) \geq \nu_p(m) + \nu_p(n) \geq 3\nu,$$

lo cual prueba que

$$\nu_p\left(\frac{(2an + 3bmn)m}{1 + am^2 + bm^3}\right) \geq 3\nu,$$

y dado que $\nu_p(t_1)$ y $\nu_p(t_2)$ son mayores o iguales a ν también $\nu_p(t)$ lo será; no solo eso si no que hemos probado además que

$$t \equiv t_1 + t_2 \pmod{Rp^{3\nu}}, \tag{44}$$

donde $R = \{q \in \mathbb{Q} : \nu_p(q) \geq 0\}$ y $t = t(P_1 \oplus P_2)$. □

Como vimos, esta última proposición culmina además con la demostración de la proposición 3.4.

Demostración de la proposición 3.5. Tomemos dos puntos $P_1, P_2 \in C(p^\nu) \subset E(\mathbb{Q})$ distintos de $\mathcal{O}$. Sea $\varphi(P_1) = (s_1, t_1)$ y $\varphi(P_2) = (s_2, t_2)$, por la proposición 3.4, estos puntos han de estar en $C(p^\nu)'$. Sea $\varphi(P_1 \oplus P_2) = \varphi(P_1) \oplus \varphi(P_2) = (s, t)$, por la ecuación (44) de la proposición anterior tenemos que

$$t \equiv t_1 + t_2 \pmod{Rp^{3\nu}},$$

donde $t = t_\nu(P_1 \oplus P_2)$, $t_\nu(P_1) = t_1$ y $t_\nu(P_2) = t_2$ lo cual prueba que t_ν es un está bien definida y es un morfismo de $E(\mathbb{Q})$ a $p^\nu R/p^{3\nu}R$. Si P_1 ó P_2 fuese $\mathcal{O}$, la ecuación anterior se verifica trivialmente puesto que $t_\nu(\mathcal{O}) = 0$.

Para ver el kernel del morfismo tomemos un punto $P \in C(p^\nu)$ tal que $t_\nu(P) = 0 \pmod{p^{3\nu}R}$. Por definición $t_\nu(\mathcal{O}) = 0$ así que $\mathcal{O} \in \mathrm{Ker}(t_\nu)$ así que supongamos que $P = (x, y)$ no sea el punto del infinito. Por la ecuación (44) podemos escribir

$$x = \frac{m}{np^{2\nu_0}} \quad \text{e} \quad y = \frac{u}{wp^{3\nu_0}},$$

con $\nu_0 \geq \nu$ y $\mathrm{mcd}(mnuw, p) = 1$, así que

$$t_\nu(P) = x/y = (mw/nu)p^{\nu_0} \equiv 0 \pmod{p^{3\nu}R}$$

si y solo si $\nu_0 \geq 3\nu$ lo cual es equivalente a que $P \in C(p^{3\nu})$ como queriamos probar. □

CAPíTULO 4

Curvas elípticas sobre $\mathbb{Q}$ - El teorema de Mordell.

1. Estructura del grupo de una curva elíptica

Este capítulo estará enfocado a probar el Teorema de Mordell: "El grupo de los puntos racionales de una curva elíptica es finitamente generado".

1.1. Alturas sobre un grupo.

DEFINICIÓN 4.1. Sea G un grupo abeliano, una altura en G es una función $h : G \to [0, +\infty)$ que verifica las siguientes tres propiedades:

1. Para todo $r \in \mathbb{R}^+$ el conjunto $h^{-1}[0, r)$ es finito.
2. Si $P_0 \in G$, entonces existe una constante $\kappa(P_0) > 0$ tal que:
$$h(P + P_0) \leq 2h(P) + \kappa(P_0) \quad \forall P \in G$$
3. Existe una constante κ tal que :
$$h(2P) \geq 4h(P) - \kappa \quad \forall P \in G$$

La existencia de una altura sobre un grupo, nos asegura la existencia de un generador finito, a partir de la finitud de cierto cociente, como veremos a continuación:

TEOREMA 4.2. *Si G posee altura y $G/2G$ es finito entonces G es finitamente generado.*

DEMOSTRACIÓN. Como $G/2G$ es finito entonces existe un conjunto finito $A = \{a_1, a_2, \ldots, a_n\} \subset G$ tal que
$$G/2G = \{a_1 + 2G, a_2 + 2G, \ldots, a_n + 2G\}.$$

Para cada $x \in G$, construimos dos sucesiones $(a_{i_n}) \subset A$ y $(x_n) \subset G$ de la siguiente manera:
Primero tomamos $a_{i_1} \in A$ tal que $x \in a_{i_1} + 2G$ y tomamos $x_1 \in G$ tal que $x - a_{i_1} = 2x_1$.
Ahora tomamos $a_{i_2} \in A$ tal que $x_1 \in a_{i_2} + 2G$ y tomamos $x_2 \in G$ tal que $x_1 - a_{i_2} = 2x_2$.

Reiterando este proceso obtenemos dos sucesiones $(a_{i_n}) \subset A$ y $(x_n) \subset G$ con la propiedad que $x_k - a_{i_{k+1}} = 2x_{k+1}$ para todo $k \geq 1$.

Luego se tendrá $x = a_{i_1} + 2x_1 = a_{i_1} + 2a_{i_2} + 4x_2 = \ldots = a_{i_1} + 2a_{i_2} + \ldots + 2^{m-1}a_{i_m} + 2^m x_m$.
Luego alcanza probar que existen $m = m(x) \in \mathbb{Z}$ y $r \in \mathbb{R}^+$ (que no depende de x) tales que $h(x_m) < r$ (pues esto probaria que $A \cup h^{-1}[0, r)$ es un generador de G y como tanto A como $h^{-1}[0, r)$ son finitos, su unión tambien lo será).

Primero comparemos las alturas de x_m y x_{m+1} :
Observemos que $h(2P) \geq 4h(P) + \kappa$ es equivalente a que $h(P) \leq \frac{h(2P)}{4} + \frac{\kappa}{4}$.

Por lo tanto $\forall\ m \geq 1$ se tendrá

$$h(x_{m+1}) \leq \frac{h(2x_{m+1})}{4} + \frac{\kappa}{4} = \frac{h(x_m - a_{m+1})}{4} + \frac{\kappa}{4} \leq \frac{2h(x_m) + \kappa(-a_{m+1})}{4} + \frac{\kappa}{4}$$
$$\leq \frac{h(x_m)}{2} + \frac{\kappa + \kappa(-a_{m+1})}{4} \leq \frac{1}{2}h(x_m) + \widehat{\kappa},$$

donde $\widehat{\kappa} = \text{máx}\{\frac{\kappa+\kappa(-a_i)}{4} : 1 \leq i \leq n\}$, observemos que $\widehat{\kappa} > 0$ puesto que $\kappa > 0$ y $\kappa(-a_i) > 0$ para $i = 1, 2, \ldots, m$.

En particular $h(x_{m+1}) \leq \frac{3}{4}h(x_m) - \frac{1}{4}h(x_m) + \widehat{\kappa} = \frac{3}{4}h(x_m) - \frac{h(x_m)-4\widehat{\kappa}}{4}\ \forall m \geq 1$
Supongamos que para todo $m \geq 1$ se tiene que $h(x_m) \geq 4\widehat{\kappa} > 0$ entonces para todo $m \geq 1$ se tendrá también que $h(x_{m+1}) \leq \frac{3}{4}h(x_m)$ lo cual implica que $h(x_m) \longrightarrow 0$ cuando $m \longrightarrow \infty$ lo cual contradice que $h(x_m) \geq 4\widehat{\kappa} > 0$.

Luego existe algún $m \geq 0$ para el cual $h(x_m) \leq 4\widehat{\kappa}$. Observemos que $r = 4\widehat{\kappa}$ no depende del x inicial, puesto que ni κ ni $\kappa(-a_i)$ dependen para $i = 1, 2, \ldots, n$, por lo tanto hemos probado que el conjunto finito $A \cup h^{-1}[0, r)$ es un generador finito de G. □

1.2. Altura sobre el grupo de una curva elíptica. En esta sección construiremos una altura sobre el grupo de una curva elíptica. Comenzemos definiendo algunas funciones previas:

DEFINICIÓN 4.3. Si $x \in \mathbb{Q}$ podemos escribir a $x = \frac{a}{b}$ con a y b enteros coprimos, definimos $H(x) = \text{máx}\{|a|, |b|\}$.

Ahora extendemos nuestra definición de H para puntos racionales de una curva eliptica racional y definiremos una nueva función h.

DEFINICIÓN 4.4. Si $E : y^2 = x^3 + ax^2 + bx + c$ es una curva elíptica racional y $P = (x, y) \in E(\mathbb{Q})$ definimos $H(P) = \begin{cases} H(P) = H(x) & \text{si } P \neq \infty \\ H(P) = 1 & \text{si } P = \infty \end{cases}$

DEFINICIÓN 4.5. Si $E : y^2 = x^3 + ax^2 + bx + c$ es una curva elíptica racional, definimos la función $h : E(\mathbb{Q}) \to [0, +\infty) : h(P) = \log H(P)$.

Las siguientes proposiciónes estarán enfocadas a probar que h es una altura sobre el grupo de una curva elíptica racional.

PROPOSICIÓN 4.6. *Para todo real r se tiene que $h^{-1}(r) = \{P \in E(\mathbb{Q}) : h(P) < r\}$ es finito.*

DEMOSTRACIÓN. Si $P = (x, y) \neq \mathcal{O}$ entonces como $H(P) = e^{h(P)} < e^r$ tenemos que $x \in \{m/n : m \in \mathbb{Z}, n \in \mathbb{Z}, |m| < e^r, |n| < e^r, n \neq 0\}$ asi que solo hay una cantidad finita de posibilidades para x. Como $y^2 = x^3 + ax^2 + bx + c$ entonces por cada x hay a lo sumo dos valores de y. Luego la cantidad de posibilidades para P es finita. □

Antes de la siguiente proposición demostraremos un lema que nos será de utilidad.

LEMA 4.7. *Si $P = (x, y) \neq \mathcal{O}$ es un punto de $E(\mathbb{Q})$ entonces existen enteros m, n y s tales que*

$$x = \frac{m}{s^2}, \quad y = \frac{n}{s^3}, \quad \text{mcd}(m, s) = \text{mcd}(n, s) = 1.$$

Y además se tienen que $n \leq KH(P)^{\frac{3}{2}}$ *para cierta constante* K *que no depende de* P.

DEMOSTRACIÓN. Sea entonces $P = (x, y) \in E(\mathbb{Q}), P \neq \mathcal{O}$ y pongamos $x = \frac{m}{M}$ e $y = \frac{n}{N}$ con $\text{mcd}(m, M) = \text{mcd}(n, N) = 1$, $M > 0$ y $N > 0$.

Sustituyendo en la ecuación $y^2 = x^3 + ax^2 + bx + c$ y multiplicando ambos miembros de la igualdad por M^3N^2 nos queda

$$M^3n^2 = N^2m^3 + aMN^2m^2 + bM^2N^2m + cM^3N^2. \tag{45}$$

Luego $N^2|M^3n^2$ y como $\text{mcd}(N, n) = 1$ entonces $N^2|M^3$.
Recíprocamente de la ecuación (45) deducimos que $M^2|N^2m^2(m+aM)$ pero como $\text{mcd}(M, m+aM) = \text{mcd}(M, m) = 1$ y $\text{mcd}(M, m^2) = 1$ entonces $M^2|N^2$, luego $M|N$. Regresando a la ecuación (45) se tendrá que $M^3|N^2m^3$ por dividir al resto de los sumandos, pero como M y m son coprimos concluimos que también $M^3|N^2$, luego $M^3 = N^2$ por ser asociados y positivos. Como 2 y 3 son coprimos entonces existe $s > 0$ tal que $M^3 = N^2 = s^6$ lo que prueba la primer parte del lema.

Para probar la segunda parte basta sustituir $x = \frac{m}{s^2}$ e $y = \frac{n}{s^3}$ en la ecuación $y^2 = x^3 + ax^2 + bx + c$ y multiplicar por s^6 para obtener

$$n^2 = m^3 + as^2m^2 + bs^4m + cs^6. \tag{46}$$

Tomamos valor absoluto en (46) y aplicamos la desigualdad triangular para obtener

$$|n|^2 \leq |m|^3 + |a||sm|^2 + |b||s|^4|m| + |c||s|^6. \tag{47}$$

Como $H(P) = H(x) = \text{máx}\{|m|, |s|^2\}$, se tienen las desigualdades

$$H(P) \geq |m| \quad H(P)^{1/2} \geq |s|.$$

Acotando con estas desigualdades en (47) obtenemos

$$|n|^2 \leq |m|^3 + |a||sm|^2 + |b||s|^4|m| + |c||s|^6 \leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3.$$

Llamando $K = 1 + |a| + |b| + |c|$ y extrayendo raíz cuadrada se obtiene la segunda parte del lema. □

Ahora estamos listos para demostrar la siguiente proposición.

PROPOSICIÓN 4.8. *Dado* $P_0 \in E(\mathbb{Q})$ *existe una constante* $\kappa(P_0)$ *tal que para todo* $P \in E(\mathbb{Q})$ *se tiene la siguiente desigualdad*

$$h(P + P_0) \leq 2h(P) + \kappa(P_0).$$

DEMOSTRACIÓN. Para $P_0 = \mathcal{O}$ la desigualdad es inmediata, basta elegir como constante cualquiera $\kappa > 0$, sea pues $P = (x_0, y_0) \in E(\mathbb{Q}) - \{\mathcal{O}\}$.

Sin pérdida de generalidad, podemos probar la desigualdad salvo para una cantidad finita de puntos, supongamos entonces que $P = (x, y) \in E(\mathbb{Q}) - \{P_0, -P_0, \mathcal{O}\}$, entonces podemos aplicar la fórmula para sumar puntos con $x \neq x_0$, si $P + P_0 = (\xi, \eta)$ se tiene:

$$\xi = \lambda - (x + x_0 + a) \quad \text{donde } \lambda = \tfrac{y - y_0}{x - x_0}$$

Sustituyendo el valor de λ

$$\xi = \frac{(y-y_0)^2 - (x+x_0+a)(x-x_0)^2}{(x-x_0)^2}.$$

Aplicando distributiva y que $y^2 - x^3 = ax^2 + bx + c$ podemos poner a ξ en la forma

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}. \tag{48}$$

Para ciertas constantes $A, B, ..., G$ racionales, que solo dependen de a, b, c, x_0 e y_0. Multiplicando por un entero adecuado podemos suponer que tales constantes son números enteros. Por el lema anterior sabemos que $x = m/s^2$ y que $y = n/s^3$ con m, n y s enteros. Sustituyendo en (4) y multiplicando numerador y denominador por s^4 nos queda

$$\xi = \frac{Asn + Bm^2 + Cs^2m + Ds^4}{Em^2 + Fs^2m + Gs^4}. \tag{49}$$

Luego tenemos escrito en (5) a ξ como cociente de dos enteros que no necesariamente serán coprimos entre si, al reducirla achicamos el numerador y denominador, por lo que tenemos la siguiente cota

$$H(P + P_0) = H(\xi) \leq \text{máx}\{|Asn + Bm^2 + Cs^2m + Ds^4|, |Em^2 + Fs^2m + Gs^4|\}. \tag{50}$$

Recordemos las acotaciones

$$|n| \leq KH(P)^{3/2}, \qquad |m| \leq H(P), \qquad |s| \leq H(P)^{1/2}$$

y las usamos para acotar el numerador y denominador de ξ :

$$\begin{aligned} |Asn + Bm^2 + Cs^2m + Ds^4| &\leq |AK|H(P)^2 + |B|H(P)^2 + |C|H(P)^2 + |D|H(P)^2 \\ &= (|AK| + |B| + |C| + |D|)H(P)^2 \end{aligned}$$

$$|Em^2 + Fs^2m + Gs^4| \leq |E|H(P)^2 + |F|H(P)^2 + |G|H(P)^2 = (|E| + |F| + |G|)H(P)^2$$

Llamando $e^\kappa = \text{máx}\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$, tenemos:

$$H(P + P_0) = H(\xi) \leq e^\kappa H(P)^2 \quad \text{tomando logaritmo } h(P + P_0) = h(\xi) = 2h(P) + \kappa$$

□

Antes de pasar a la próxima proposición, probaremos un par de lemas previos.

LEMA 4.9. *Sean ϕ y φ dos polinomios con coeficientes enteros y sin raíces complejas comunes, entonces*

$$mcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\varphi\left(\frac{m}{n}\right)\right)|R,$$

para alguna constante $R > 0$ y $m, n \in \mathbb{Z}$ coprimos ($d = \text{máx}\{deg(\phi), deg(\varphi)\}$).

DEMOSTRACIÓN. Sean

$$\phi(X) = a_dX^d + a_{d-1}X^{d-1} + \ldots + a_0$$

y

$$\varphi(X) = b_eX^e + b_{e-1}X^{e-1} + \ldots + b_0$$

podemos suponer sin pérdida de generalidad que $d \geq e$, definamos además para m y n enteros coprimos:

$$\phi(m, n) = \phi(m)n^d = a_dm^d + a_{d-1}m^{d-1}n + \ldots + a_0n^d$$

y

$$\varphi(m,n) = b_e m^e n^{d-e} + b_{e-1} m^{e-1} n^{d-e+1} + \ldots + b_0 n^d$$

y sea $\gamma(m,n) =$
$mcd\{\phi(m,n), \varphi(m,n)\}$, afirmamos que alcanza con probar que $\gamma(m,n)|n^t K$ para algún t fijo (que no dependa de m y n).

Para probar la afirmación observemos que claramente $\gamma(m,n)$ divide a

$$n^{t-1} K\phi(m,n) = a_d m^d n^{t-1} K + a_{d-1} m^{d-1} n^t K + \ldots + a_0 n^{d+t-1} K$$

pues todos los términos salvo quizas el primero, es múltiplo de Kn^t así que $\gamma(m,n)$ divide al primer término que es $a_d m^d n^{t-1} K$. Luego $\gamma(m,n)$ divide a

$$\operatorname{mcd}(n^t K, a_d m^d n^{t-1} K) = K n^{t-1} \operatorname{mcd}(n, a_d m^d) = K n^{t-1} \operatorname{mcd}(n, a_d) | K n^{t-1} a_d$$

para el segundo igual se ha usado la coprimalidad de n y m. Y así sucesivamente, suponiendo que $\gamma(m,n)$ divida a $Kn^{t-i} a_d^i$ con $i > 1$, como $\gamma(m,n)$ divide a $n^{t-i-1} a_d^i K\phi(m,n) = a_d^{i+1} m^d n^{t-i-1} K + \ldots$ y divide a todos los términos excepto quizas al primero, entonces divide al primero luego $\gamma(m,n)$ divide a

$$\operatorname{mcd}(a_d^{i+1} m^d n^{t-i-1} K, K n^{t-i} a_d^i) = K a_d^i n^{t-i-1} \operatorname{mcd}(a_d, n) | K a_d^{1+1} n^{t-(i+1)}$$

. Se concluye entonces que $\gamma(m,n)|Ka_d^t$ que no depende de n y m.

Ahora a probar el lema, por inducción en $g = gr(\phi) + gr(\varphi)$.

Para $g = 0$ tenemos que $gr(\phi) = gr(\varphi) = 0$ y por lo tanto ϕ y φ son polinomios constantes y el lema es evidente en este caso.

Supongamos que $g > 0$ entonces $gr(\phi) = d > 0$ y consideramos el nuevo polinomio

$$\psi(X) = b_e \phi(X) - a_d \varphi(X) X^{d-e} \tag{51}$$

Observemos que toda raíz (compleja) común de ψ y de φ también ha de ser raíz de ϕ en virtud de la ecuación (51); dado que ϕ y φ no tenían raíces comunes, ψ y φ tampoco la tendrán.

Observemos además que $gr(\psi) < d \leq gr(\phi)$ lo cual implica que $gr(\varphi) + gr(\psi) < gr(\phi) + gr(\varphi)$ así que podemos aplicar nuestra hipótesis inductiva con los polinomios ψ y φ para obtener la existencia de una constante K' tal que

$$\operatorname{mcd}\left(\varphi\left(\frac{m}{n}\right) n^s, \psi\left(\frac{m}{n}\right) n^s\right) | K'$$

donde $s = \max\{gr(\varphi), gr(\psi)\} < d$
Como

$$\psi\left(\frac{m}{n}\right) n^d = \left(b_e \phi\left(\frac{m}{n}\right) - a_d \varphi\left(\frac{m}{n}\right)\left(\frac{m}{n}\right)^{d-e}\right) n^d = b_e \phi(m,n) - a_d \varphi\left(\frac{m}{n}\right) n^e m^{d-e},$$

tenemos que

$$\begin{aligned}
&\operatorname{mcd}(\phi(m,n), \psi(m,n)) \,|\, \operatorname{mcd}(b_e \phi(m,n), \psi(m,n)) \\
&= \operatorname{mcd}\left(\psi\left(\frac{m}{n}\right) n^d - a_d \varphi\left(\frac{m}{n}\right) n^e m^{d-e}, \varphi\left(\frac{m}{n}\right) n^d\right) \\
&| n^{d-e} \operatorname{mcd}\left(\psi\left(\frac{m}{n}\right) n^d - a_d \varphi\left(\frac{m}{n}\right) n^e m^{d-e}, \varphi\left(\frac{m}{n}\right) n^e\right) \\
&= n^{d-e} \operatorname{mcd}\left(\psi\left(\frac{m}{n}\right) n^d, \varphi\left(\frac{m}{n}\right) n^e\right)
\end{aligned}$$

$$|n^{d-e} \operatorname{mcd}\left(\psi\left(\frac{m}{n}\right) n^d, \varphi\left(\frac{m}{n}\right) n^s\right)$$
$$|n^{d-e} n^{d-s} \operatorname{mcd}\left(\psi\left(\frac{m}{n}\right) n^s, \varphi\left(\frac{m}{n}\right) n^s\right)$$
$$|n^{2d-e-s} K' | n^{2(d-e)} K'.$$

Pero en virtud de la afirmación, dado que $d-e$ no dependen de m ni de n, tenemos que existe una constante K tal que

$$\operatorname{mcd}\left(\phi(m,n), \psi(m,n)\right) | K$$

lo que da por culminado el lema. □

Ahora a continuación damos una cota para la altura de una función racional:

LEMA 4.10. *Si ϕ y ψ son funciones racionales sin raíces comunes entonces*

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m,n)}{\varphi(m,n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2,$$

para todo m y n enteros coprimos.

DEMOSTRACIÓN. Podemos aplicar exponencial para obtener otra desigualdad equivalente

$$H\left(\frac{m}{n}\right)^d e^{-\kappa_1} \leq H\left(\frac{\phi(m,n)}{\varphi(m,n)}\right) \leq H\left(\frac{m}{n}\right)^d e^{\kappa_2}.$$

Como $H\left(\frac{m}{n}\right) > 0$ esta desigualdad es equivalente a

$$e^{-\kappa_1} \leq \frac{H\left(\frac{\phi(m,n)}{\varphi(m,n)}\right)}{H\left(\frac{m}{n}\right)^d} \leq e^{\kappa_2}. \tag{52}$$

Si $\gamma(m,n) = \operatorname{mcd}\left(\phi(m,n), \varphi(m,n)\right)$ entonces

$$H\left(\frac{\phi(m,n)}{\varphi(m,n)}\right) = \operatorname{máx}\left\{\left|\frac{\phi(m,n)}{\gamma(m,n)}\right|, \left|\frac{\varphi(m,n)}{\gamma(m,n)}\right|\right\} = \frac{\operatorname{máx}\left\{|\phi(m,n)|, |\varphi(m,n)|\right\}}{\gamma(m,n)}$$

De donde

$$\frac{H\left(\frac{\phi(m,n)}{\varphi(m,n)}\right)}{H\left(\frac{m}{n}\right)^d} = \frac{\operatorname{máx}\left\{|\phi(m,n)|, |\varphi(m,n)|\right\}}{\gamma(m,n) \operatorname{máx}\left\{|m|^d, |n|^d\right\}}$$
$$= \frac{\operatorname{máx}\left\{\left|\phi\left(\frac{m}{n}\right)\right|, \left|\varphi\left(\frac{m}{n}\right)\right|\right\}}{\gamma(m,n) \cdot \operatorname{máx}\left\{\left|\frac{m}{n}\right|^d, 1\right\}}.$$

Eso nos lleva a considerar la función de variable real

$$f(x) = \frac{\operatorname{máx}\left\{|\phi(x)|, |\varphi(x)|\right\}}{\operatorname{máx}\left\{|x|^d, 1\right\}}.$$

Como ϕ y φ son polinomios y el valor absoluto y la función máximo son continuas entonces la función f es continua en todo el eje real. Además para todo $x : |x| > 1$ tenemos que

$$f(x) = \operatorname{máx}\left\{\left|\frac{\phi(x)}{x^d}\right|, \left|\frac{\varphi(x)}{x^d}\right|\right\}.$$

Como ϕ es un polinomio de grado d y φ un polinomio de grado menor o igual a d nos queda que:

$$\lim_{x\to\infty} f(x) = \begin{cases} |a_d| & \text{si } e < d \\ \operatorname{máx}\left\{|a_d|, |b_d|\right\} & \text{si e=d} \end{cases}$$

Definiendo $f(\infty) = \lim_{x\to\infty} f(x)$ tenemos que f es una función continua en toda la recta real extendida que es un compacto (pues es homeomorfo a S^1) así que tiene máximo M y mínimo m en $\overline{\mathbb{R}}$. Observemos que $m > 0$ pues por una parte a_d es no nulo, lo cual implica que $f(\infty) \neq 0$ y por otra parte f no puede anularse en la recta real (una raíz real de f sería una raíz común de ϕ y φ), por lo tanto, para todo $x \in \mathbb{R}$:

$$0 < \frac{m}{K} \leq \frac{m}{\gamma(m,n)} \leq \frac{f\left(\frac{m}{n}\right)}{\gamma(m,n)} = \frac{H\left(\frac{\phi(m,n)}{\varphi(m,n)}\right)}{H\left(\frac{m}{n}\right)^d} \leq \frac{M}{\gamma(m,n)} \leq M,$$

donde K es como en el lema anterior.

Para obtener la desigualdad (52) podemos tomar por ejemplo $\kappa_1 = -\log\left(\frac{m}{K}\right)$ y $\kappa_2 = \log(M)$. □

PROPOSICIÓN 4.11. *Existe una constante κ (solo dependiendo de la cúbica) tal que*

$$h(2P) \geq 4h(P) - \kappa$$

para todo $P \in E(\mathbb{Q})$.

DEMOSTRACIÓN. Es claro que alcanza probar la desigualdad excepto para una cantidad finita de puntos y luego acomodar la constante para dichos puntos para que valga en general, así que ignoraremos aquellos puntos tales que $2P = \mathcal{O}$ (que son a lo sumo 4 puntos). Para aquellos puntos $P = (x, y)$ tales que $2P \neq 0$ tenemos la fórmula de duplicación

$$x(2P) + 2x = \lambda^2 - a, \qquad \text{donde } \lambda = \frac{f'(x)}{2y},$$

despejando $x(2P)$ donde $y^2 = f(x)$ tenemos que

$$x(2P) = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \ldots}{4x^3 + \ldots},$$

como f y f' no tienen raíces complejas comunes (pues E es elíptica) entonces los polinomios en x en el numerador y el denominador de $x(2P)$ no tienen raíces complejas comunes, luego el lema 4.10 nos asegura la existencia de una constante κ tal que

$$h\left(x(2P)\right) \geq 4h(x) - \kappa.$$

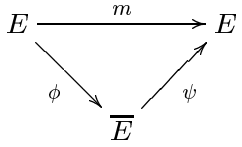
Pero por definición $h(P) = h(x)$ y $h(2P) = h\left(x(2P)\right)$ sustituyendo en la desigualdad anterior obtenemos la ecuación deseada. □

1.3. Factorización del morfismo multiplicación por 2. En la sección anterior hemos probado que el grupo de puntos raciones en nuestra cúbica está dotado de altura h, así que para probar la generación finita alcanza probar que $[E(\mathbb{Q}) : 2E(\mathbb{Q})] < \infty$ a eso enfocaremos nuestra atención a partir de ahora.

Es natural considerar el morfismo

$$m : E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}), \qquad P \mapsto 2P,$$

la imagen de ese morfismo es justamente el subgrupo $2E(\mathbb{Q})$. La idea que se utilizará para probar la finitud del subgrupo $Im(m)$ es factorizar el morfismo m como composición de dos morfismos $m = \psi\phi$.



La idea es que las imágenes de tales morfismos sean más fácil de controlar, luego para probar la finitud de $E/Im(m)$ es suficiente probar la finitud de $\overline{E}/Im(\phi)$ y de $E/Im(\psi)$ donde $\overline{E}$ es el dominio de ψ. Este resultado general sobre grupos abelianos será probado a continuación.

PROPOSICIÓN 4.12. *Si $\phi : G \longrightarrow H$ y $\psi : H \longrightarrow K$ son morfismos de grupos abelianos tales que $[H : Im(\phi)]$ y $[K : Im(\psi)]$ son finitos entonces $[K : Im(\psi\phi)]$ es finito y además se verifica que*

$$[K : Im(\psi\phi)] \leq [H : Im(\phi)][K : Im(\psi)].$$

DEMOSTRACIÓN. Sea $\{h_1, h_2, \ldots, h_n\}$ una conjunto de representantes del cociente $H/Im(\phi)$ y $\{k_1, k_2, \ldots, k_m\}$ un conjunto de representantes del cociente $K/Im(\psi)$. Alcanza ver que

$$S = \{k_i + \psi(h_j) : 1 \leq i \leq n, 1 \leq j \leq m\},$$

es un conjunto de representantes del cociente $K/Im(\psi\phi)$.

En efecto, sea $k \in K$, queremos probar que existe algún elemento $s \in S$ tal que $k - s \in Im(\psi\phi)$. Como $k \in K$ entonces existe $i : 1 \leq i \leq n$ tal que $k - k_i \in Im(\psi)$, sea $h \in H : k - k_i = \psi(h)$. Como $h \in H$ entonces existe $j : 1 \leq j \leq m$ tal que $h - h_j \in Im(\phi)$, luego existe $g \in G$ tal que $h - h_j = \phi(g)$ o lo que es lo mismo $h = h_j + \phi(g)$. Luego $k - k_i = \psi(h) = \psi(h_j + \phi(g)) = \psi(h_j) + \psi\phi(g)$ y por lo tanto $k - (k_i + \psi(h_j)) = \psi\phi(g) \in Im(\psi\phi)$ con $k_i + \psi(h_j) \in S$ como queriamos probar. □

Vamos a probar el Teorema de Mordell con una hipótesis adicional que es la existencia de algún punto racional de orden 2 (que equivale a que f tenga raíz racional). Si $P = (x_0, 0)$ es un punto racional de orden 2, entonces através del cambio de variable $(x, y) \mapsto (x - x_0, y)$ nuestra cúbica toma la forma

$$E(\mathbb{Q}) : Y^2 = X^3 + aX^2 + bX,$$

con este cambio de variable tenemos que el punto $T = (0, 0)$ es un punto de orden 2 de la cúbica.

Observemos que la condición de no singularidad para la cúbica anterior es que $f(X) = X^3 + aX^2 + bX = (X^2 + aX + b)X$ no tenga raíces dobles, lo cual equivale a que $b \neq 0$ y que $a^2 - 4b \neq 0$.

Asociado a la curva elíptica $E/\mathbb{Q}$ tenemos asociado un par $(\overline{E}/\mathbb{Q}, \phi_E)$ donde $\overline{E}$ es otra curva elíptica definida por la ecuación

$$\overline{E} : X^3 + \overline{a}X^2 + \overline{b}X,$$

donde $\overline{a} = -2a, \overline{b} = a^2 - 4b$ y $\phi : E \longrightarrow \overline{E}$ es un morfismo entre las curvas elípticas definido por la ecuación:

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), & \text{si } P = (x, y) \neq \mathcal{O}, T \\ \mathcal{O}, & \text{si } P = \mathcal{O} \text{ o } P = T \end{cases}$$

OBSERVACIÓN 4.13. Como $b \neq 0$ y $a^2 - 4b \neq 0$ tenemos que $\overline{b} = a^2 - 4b \neq 0$ y $\overline{a}^2 - 4\overline{b} = 4a^2 - 4(a^2 - 4b) = 16b \neq 0$ así que efectivamente la ecuación de $\overline{E}$ define una curva elíptica.

Veremos a continuación que $\phi_E(E(\mathbb{Q})) \subset \overline{E}(\mathbb{Q})$ y que es un morfismo.

PROPOSICIÓN 4.14. *La función $\phi = \phi_E$ definida anteriormente está bien definida y es un morfismo de curvas elípticas.*

DEMOSTRACIÓN. Veamos primero que $\phi(E(\mathbb{Q})) \subset \overline{E}(\mathbb{Q})$.

Observemos primero que por definición $\phi(\mathcal{O}) = \overline{\mathcal{O}} \in \overline{E}(\mathbb{Q})$.

Sea $P = (x, y) \in E(\mathbb{Q})$ y $\overline{P} = (\overline{x}, \overline{y}) = \phi(P)$ su correspondiente imagen por el mapa ϕ_E.

Si $P = T$ entonces $\phi(T) = \overline{\mathcal{O}} \in \overline{E}(\mathbb{Q})$.

Para $P = (x, y) \neq T$ claramente $\phi(P) \in \mathbb{Q}^2$ y además tenemos que

$$\overline{x}^3 + \overline{a}\overline{x}^2 + \overline{b}\overline{x} = \frac{y^6}{x^3} - \frac{2ay^4}{x^4} + \frac{(a^2 - 4b)y^2}{x^2} = \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + a^2 - 4b\right)$$

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

$$= \frac{y^2}{x^2}\left(\frac{y^4 - 2ax^2y^2 + a^2x^4 - 4bx^4}{x^4}\right) = \frac{y^2}{x^2}\left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right)$$

$$= \frac{y^2}{x^6}\left((x^3 + bx)^2 - 4bx^4\right) = \frac{y^2}{x^4}\left((x^2 + b)^2 - 4bx^2\right) = \frac{y^2}{x^4}(x^2 - b)^2$$

$$= \left(\frac{y(x^2 - b)}{x}\right)^2 = \overline{y}^2,$$

así que $\phi(P) \in E(\mathbb{Q})$.

Ahora nos resta ver que es un morfismo, es decir que para todo par de puntos $P, Q \in E(\mathbb{Q})$ se tiene que

$$\phi(P) \oplus \phi(Q) = \phi(P \oplus Q) \tag{53}$$

donde $\phi = \phi_E$.

Observemos primero que para $P = \mathcal{O}$ la ecuación (53) se verifica trivialmente puesto que $\phi(\mathcal{O}) = \overline{\mathcal{O}}$ es el neutro en $\overline{E}(\mathbb{Q})$, lo mismo sucede si $Q = \mathcal{O}$.

Si P ó Q fuese $T = (0, 0)$, supongamos $Q = T$, para probar (53) debemos probar que

$$\phi(P) = \phi(P \oplus T) \tag{54}$$

puesto que $\phi(T) = \overline{\mathcal{O}}$. Si $P = T$ se verifica (54) pues $T \oplus T = \mathcal{O}$ y $\phi(T) = \overline{\mathcal{O}}$.

Sea $P=(x_0,y_0)\in E(\mathbb{Q})$ con $P\neq T$, calculemos $P\oplus T$: la recta que pasa por T y P viene dada por $Y=(y_0/x_0)X$ (observar que $x_0\neq 0$ pues $P\neq T$), las coordenadas en X de los puntos T,P y $T*P$ son las raíces de la ecuación

$$\left(\left(\frac{y_0}{x_0}\right)X\right)^2=X^3+aX^2+bX,$$

o equivalentemente

$$X^3+\left(a-\frac{y_0^2}{x_0^2}\right)X^2+bX=0,$$

por relaciones entre coeficientes y raíces tenemos que

$$0+x_0+x(P*T)=-\left(a-\frac{y_0^2}{x_0^2}\right)=-\left(a-\frac{x_0^3+ax_0^2+bx_0}{x_0^2}\right)=-\left(a-x_0-a-\frac{b}{x_0}\right)=x_0+\frac{b}{x_0}.$$

De donde

$$x(P*T)=\frac{b}{x_0},$$

sustituimos en la ecuación de la recta para obtener $y(P*Q)$:

$$y(P*Q)=\frac{y_0}{x_0}\cdot\frac{b}{x_0}=\frac{y_0b}{x_0^2}$$

Si $\phi(P\oplus T)=(\overline{x}(P\oplus T),\overline{y}(P\oplus T))$ y $\phi(P)=(\overline{x}(P),\overline{y}(P))$ por lo tanto

$$P\oplus T=-(P*T)=(\frac{b}{x_0},\frac{-by_0}{x_0^2})$$

Así que tenemos que

$$\overline{x}(P\oplus T)=\left(\frac{y(P\oplus T)}{x(P\oplus T)}\right)^2=\frac{\left(\frac{-by}{x^2}\right)^2}{\left(\frac{b}{x}\right)^2}=\frac{y^2}{x^2}=\overline{x}(P),$$

lo mismo para las coordenadas en Y:

$$\overline{y}(P\oplus T)=\frac{y(P\oplus T)\left(x(P\oplus T)^2-b\right)}{x(P\oplus T)^2}=\frac{\left(\frac{-by}{x^2}\right)\left(\left(\frac{b}{x}\right)^2-b\right)}{\left(\frac{b}{x}\right)^2}=\frac{(-by)(b^2-bx^2)}{b^2x^2}=\frac{y(x^2-b)}{x^2}=\overline{y}(P)$$

Lo cual demuestra que efectivamente la ecuación (54) es cierta.

Para analizar el caso general observemos que $\phi(\mathcal{O})=\overline{\mathcal{O}}$ y que para todo $P=(x,y)\in E(\mathbb{Q})$ se tiene que

$$\phi(-P)=\phi(x,-y)=\left(\frac{(-y)^2}{x^2},\frac{(-y)(x^2-b)}{x^2}\right)=\left(\frac{y^2}{x^2},-\frac{y(x^2-b)}{x^2}\right)=-\phi(x,y)=\phi(P).$$

Así que para probar (53) es suficiente probar que

$$P_1\oplus P_2\oplus P_3=\mathcal{O}\Rightarrow\phi(P_1)\oplus\phi(P_2)\oplus\phi(P_3)=\overline{\mathcal{O}},\tag{55}$$

para todo $P_1,P_2,P_3\in E(\mathcal{Q})$, en efecto si se cumple (55) entonces

$$\phi(P_1\oplus P_2)=\phi(-P_3)=-\phi(P_3)=\phi(P_1)\oplus\phi(P_2).$$

Así que vamos a probar (55), además podemos suponer que P_1,P_2 y P_3 son distintos de $\mathcal{O}$ y de T pues estos casos ya fueron analizados previamente.

Supongamos que $P_1\oplus P_2\oplus P_3=\mathcal{O}$ entonces tenemos que los puntos P_1,P_2 y P_3 están alineados, sea $Y=\lambda X+\nu$ la recta que pasa por esos puntos, queremos hallar una recta

$Y = \overline{\lambda}X + \overline{\nu}$ que pase por $\phi(P_1), \phi(P_2)$ y $\phi(P_3)$.

Supongamos que $P = (x, y) \in \mathbb{Q}^2$ con $P \neq T$ un punto que verifique:

$$\begin{cases} y^2 = x^3 + ax^2 + bx \\ y = \lambda x + \nu \end{cases} \tag{56}$$

sea $\phi(P) = (\overline{x}, \overline{y})$ entonces se tiene que

$$\overline{y} = \frac{y(x^2 - b)}{x^2} = \frac{yx^2 - by}{x^2} = \frac{(\lambda x + \nu)x^2 - by}{x^2} = \frac{\lambda x^3 + \nu x^2 - by}{x^2} = \frac{\lambda(x^3 + bx) + \nu x^2 - b(y + \lambda x)}{x^2}$$
$$= \frac{\lambda(y^2 - ax^2) + \nu x^2 - b(y + \lambda x)}{x^2} = \frac{\lambda\nu(y^2 - ax^2) + \nu^2 x^2 - b(y - \lambda x)(y + \lambda x)}{\nu x^2}$$
$$= \frac{\lambda\nu(y^2 - ax^2) + \nu^2 x^2 - b(y^2 - \lambda^2 x^2)}{\nu x^2} = \frac{(\lambda\nu - b)y^2 + (-a\lambda\nu + \nu^2 + b\lambda^2)x^2}{\nu x^2}$$
$$= \left(\frac{\lambda\nu - b}{\nu}\right)\left(\frac{y}{x}\right)^2 + \left(\frac{-a\lambda\nu + \nu^2 + b\lambda^2}{\nu}\right) = \overline{\lambda}\overline{x} + \overline{\nu},$$

donde

$$\overline{\lambda} = \frac{\lambda\nu - b}{\nu} \qquad \text{y} \qquad \overline{\nu} = \frac{-a\lambda\nu + \nu^2 + b\lambda^2}{\nu}. \tag{57}$$

Esto quiere decir que ϕ lleva puntos alineados en la cúbica $E(\mathbb{Q})$ en puntos alineados de la cúbica $\overline{E}(\mathbb{Q})$ lo cual prueba (55) para el caso en que los puntos P_1, P_2 y P_3 sean distintos dos a dos. Para el caso genérico hay un tema de multiplicidades que chequear, lo cual haremos a continuación. Volvamos a considerar las rectas

$$r : Y = \lambda X + \nu \qquad \text{y} \qquad \overline{r} : Y = \overline{\lambda}X + \overline{\nu}$$

donde r es la recta que pasa por $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ y $P_3 = (x_3, y_3)$, y $\overline{r}$ es la recta cuyos coeficientes están determinados por las fórmulas de (57), que como vimos, ha de pasar por los puntos $\phi(P_1) = (\overline{x_1}, \overline{y_1})$, $\phi(P_2) = (\overline{x_2}, \overline{y_2})$ y $\phi(P_3) = (\overline{x_3}, \overline{y_3})$.

Queremos probar que

$$\phi(P_1) \oplus \phi(P_2) \oplus \phi(P_3) = \overline{\mathcal{O}}, \tag{58}$$

observemos que ningunos de los tres puntos va a ser $\overline{\mathcal{O}}$ porque estamos suponiendo que ni P_1, ni P_2, ni P_3 es $\mathcal{O}$ o T, así que la recta $\overline{r}$ no es vertical, es decir, si un punto $\overline{P}$ de la cúbica $\overline{E}(\mathbb{Q})$ pertenece a $\overline{r}$ entonces $-\overline{P}$ no puede pertenecer, excepto que $\overline{P} = -\overline{P}$ así que alcanza con probar que $\overline{x_1}, \overline{x_2}$ y $\overline{x_3}$ son las tres raíces de la ecuación

$$(\overline{\lambda}X + \overline{\nu})^2 = X^3 + \overline{a}X^2 + \overline{b}X, \tag{59}$$

lo cual es equivalente a

$$X^3 + (\overline{a} - \overline{\lambda}^2)X^2 + (\overline{b} - 2\overline{\lambda}\overline{\nu})X - \overline{\nu}^2 = 0. \tag{60}$$

Pero como ya sabemos que x_1, x_2 y x_3 son raíces, para probar que están dadas con las multiplicidades correctas es suficiente probar que

$$\overline{x_1} + \overline{x_2} + \overline{x_3} = \overline{\lambda}^2 - \overline{a}. \tag{61}$$

Recordando que $\overline{x_i} = x_i + a + b/x_i$ para $i = 1, 2, 3$ y los valores para $\overline{\lambda}$ y $\overline{a}$, tenemos que (61) es equivalente a

$$x_1 + x_2 + x_3 + 3a + b\left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}\right) = \frac{(\lambda\nu - b^2)^2}{\nu^2} + 2a,$$

lo cual a su vez es equivalente a

$$x_1 + x_2 + x_3 + b\left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}\right) = \frac{(\lambda\nu - b^2)^2}{\nu^2} - a. \tag{62}$$

Pero como $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$ entonces x_1, x_2 y x_3 son las tres raíces de

$$(\lambda X + \nu)^2 = X^3 + aX^2 + bX,$$

o equivalentemente, de la ecuación

$$X^3 + (a - \lambda^2)X^2 + (b - 2\lambda\nu)X - \nu^2 = 0, \tag{63}$$

usamos entonces las relaciones entre coeficientes y raíces para deducir (62) :

$$x_1 + x_2 + x_3 + b\left(\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}\right) = x_1 + x_2 + x_3 + b\left(\frac{x_1x_2 + x_1x_3 + x_2x_3}{x_1x_2x_3}\right)$$

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

lo cual prueba (62) y por lo tanto (58). □

La siguiente proposición dice que al aplicar dos veces la operación techo a una curva elíptica obtenemos otra curva elíptica isomorfa a la original.

PROPOSICIÓN 4.15. *Las curvas elípticas $\overline{\overline{E}}(\mathbb{Q})$ y $E(\mathbb{Q})$ son isomorfas, el isomorfismo viene dado por*

$$\eta : \overline{\overline{E}}(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) : (x, y) \mapsto \left(\frac{1}{4}x, \frac{1}{8}y\right).$$

DEMOSTRACIÓN. Recordemos que si $E : Y^2 = X^3 + aX^2 + bX$ entonces

$$\overline{E} : Y^2 = X^3 + \overline{a}X^2 + \overline{b}X \text{ donde } \overline{a} = -2a,\ \overline{b} = a^2 - 4b$$

así que

$$\overline{\overline{E}} : Y^2 = X^3 + \overline{\overline{a}}X^2 + \overline{\overline{b}}X \text{ donde } \overline{\overline{a}} = -2\overline{a} = 4a,\ \overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = 4a^2 - 4(a^2 - 4b) = 16b$$

es decir

$$\overline{\overline{E}} : Y^2 = X^3 + 4aX^2 + 16bX.$$

Busquemos ahora un isomorfismo $\eta : \overline{\overline{E}}(\mathbb{Q}) \longrightarrow E(\mathbb{Q})$ de la forma $\eta(x, y) = (\lambda x, \mu y)$ con λ y μ racionales no nulos.

Sea $(x, y) \in \overline{\overline{E}}(\mathbb{Q})$, tenemos que

$$\eta(x, y) \in E \Leftrightarrow (\mu y)^2 = (\lambda x)^3 + a(\lambda x)^2 + b(\lambda x) \Leftrightarrow \mu^2 y^2 = \lambda^3 x^3 + a\lambda^2 x^2 + b\lambda x,$$

pero como $(x, y) \in \overline{\overline{E}}(\mathbb{Q})$ verifica la ecuación

$$\mu^2 Y^2 = \mu^2 X^3 + 4a\mu^2 x^2 + 16b\mu^2,$$

así que alcanza con que

$$\begin{cases} \mu^2 = \lambda^3 \\ 4a\mu^2 = a\lambda^2 \\ 16b\mu^2 = b\lambda \end{cases} \tag{64}$$

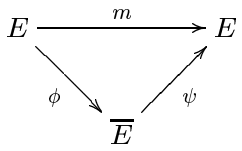
Sustituyendo el μ^2 de la primer ecuación en la segunda nos queda que $4a\lambda^3 = a\lambda^2$ lo cual se verifica si $4\lambda = 1$ o sea si $\lambda = 1/4$, luego para que se verifique la primer ecuación tenemos que $\mu = \sqrt{\lambda^3} = \sqrt{1/64} = 1/8$, por chequeo directo esos valores verifican el sistema (64).

Reciprocamente si $P = (u, v) \in E(\mathbb{Q})$ tenemos que el punto $Q = (4u, 8v) \in \overline{\overline{E}}(\mathbb{Q})$ pues

$$(8v)^2 = 64v^2 = 64(u^3 + au^2 + bu) = (4u)^3 + 4a(4u)^2 + 16b(4u),$$

y $\eta(Q) = P$ así que η es sobreyectivo, claramente es inyectivo y es un cambio de coordenadas, así que es un isomorfismo entre las curvas elípticas $\overline{\overline{E}}$ y E. □

Dada una curva elíptica $E/\mathbb{Q}$, denotamos por $\phi = \phi_E$ y por ψ el morfismo de $\overline{E}$ a E definido como $\psi = \eta \circ \phi_{\overline{E}}$, dado que las funciones $\phi_E, \phi_{\overline{E}}$ y η son morfismos, entonces tenemos definido un automorfismo $m : E \longrightarrow E$ tal que hace conmutar el diagrama



La siguiente proposición prueba que ese morfismo m definido por el diagrama anterior no es otra cosa que la multiplicación por 2.

PROPOSICIÓN 4.16. *Si $m : E(\mathbb{Q}) \to E(\mathbb{Q})$ es el morfismo $m(P) = 2P$ entonces los morfismos ϕ y ψ definidos anteriormente verifican la propiedad*

$$\psi(\phi(P)) = m(P) = 2P,$$

para todo $P \in E(\mathbb{Q})$.

DEMOSTRACIÓN. Si $P = \mathcal{O}$ tenemos que

$$\psi(\phi(\mathcal{O})) = \psi(\overline{\mathcal{O}}) = \mathcal{O} = 2 \cdot \mathcal{O}$$

Si $P = T$ tenemos que

$$\psi(\phi(T)) = \psi(\overline{\mathcal{O}}) = \mathcal{O} = 2 \cdot T.$$

Si $P = (x, 0) \in E(\mathbb{Q})$ fuese otro punto de orden 2 distinto de T entonces $\phi_E(x, 0) = (0, 0) = \overline{T}$, $\phi_{\overline{E}}(\overline{T}) = \mathcal{O}$ y $\eta(\mathcal{O}) = \mathcal{O}$ así que en la composición $\psi(\phi(P)) = \mathcal{O} = 2 \cdot P$.

Si $P = (x, y) \neq \mathcal{O}$ no es un punto de orden 2 de $E(\mathbb{Q})$ tenemos la siguiente fórmula de duplicación:

$$2P = 2(x, y) = \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3} \right)$$

Ahora conviene recordar la fórmula explícita para $\phi = \phi_E$ y de $\psi = \eta \circ \phi_{\overline{E}}$ obtenemos también una fórmula explícita para ψ:

$$\phi(P) = \begin{cases} (\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}), & \text{si } P = (x, y) \neq \mathcal{O}, T \\ \mathcal{O}, & \text{si } P = \mathcal{O} \text{ o } P = T \end{cases}$$

y

$$\psi(\overline{P}) = \begin{cases} (\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2-\overline{b})}{8\overline{x}^2}), & \text{si } \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, \overline{T} \\ \overline{\mathcal{O}}, & \text{si } \overline{P} = \overline{\mathcal{O}} \text{ o } \overline{P} = \overline{T} \end{cases}$$

Así que tenemos

$$\psi \circ \phi(x,y) = \psi\left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) = \left(\frac{y^2(x^2-b)^2}{x^4}\cdot\frac{x^4}{4y^4}, \frac{\frac{y(x^2-b)}{x^2}\cdot\left(\frac{y^4}{x^4}-(a^2-4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right)$$

$$= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)\left(y^4-(a^2-4b)x^4\right)}{8y^3x^2}\right) \tag{65}$$

Pero como $P=(x,y)\in E(\mathbb{Q})$ tenemos que $y^2 = x(x^2+ax+b)$ de donde

$$\frac{(x^2-b)\left(y^4-(a^2-4b)x^4\right)}{8y^3x^2} = \frac{(x^2-b)\left((x^2+ax+b)^2-(a^2-4b)x^2\right)}{8y^3}$$

$$= \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}. \tag{66}$$

Sustituyendo (66) en (65) obtenemos la fórmula de duplicación. □

1.4. El Teorema de Mordell. En la sección anterior hemos construido morfismos ϕ y ψ tales que compuestos eran el morfismo multiplicación por 2 en la curva elíptica $E/\mathbb{Q}$. Para probar el Teorema de Mordell faltaba probar que

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] < \infty \tag{67}$$

por la proposición 4.12 es suficiente probar que

$$[\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] < \infty \quad \text{y} \quad [E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q}))] < \infty. \tag{68}$$

De hecho, como $\psi = \eta \circ \phi_{\overline{E}}$ donde $\eta : \overline{\overline{E}}(\mathbb{Q}) \to E(\mathbb{Q})$ es un isomorfismo tenemos que

$$[E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q}))] = [\overline{\overline{E}}(\mathbb{Q}) : \phi_{\overline{E}}(\overline{E}(\mathbb{Q}))]. \tag{69}$$

En virtud de (69), para probar (68) y por lo tanto el Teorema de Mordell es suficiente probar que para toda curva elíptica $E/\mathbb{Q}$, se tiene que

$$[\overline{E}(\mathbb{Q}) : \phi_E(E(\mathbb{Q}))] < \infty.$$

Para probar esto último, es necesario conocer como es la imagen del morfismo $\phi = \phi_E$, la siguiente proposición nos ayudará a entender como es este conjunto imagen.

PROPOSICIÓN 4.17. *Sean $E: Y^2 = X^3 + aX^2 + bX$ y $\overline{E}: Y^2 = X^3 + \overline{a}X^2 + \overline{b}X$ donde $\overline{a} = -2a$ y $\overline{b} = a^2 - 4b$ dos curvas elíptica definidas sobre $\mathbb{Q}$, sean $\Gamma = E(\mathbb{Q})$ y $\overline{\Gamma} = \overline{E}(\mathbb{Q})$. Consideremos el morfismo $\phi = \phi_E : \Gamma \to \overline{\Gamma}$ definido en la sección anterior. Tenemos que:*

1. $\overline{\mathcal{O}} \in \phi(\Gamma)$.
2. $\overline{T} = (0,0) \in \phi(\Gamma) \Leftrightarrow \overline{b} = a^2 - 4b$ *es un cuadrado de un racional.*
3. *Si* $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ *con* $\overline{x} \neq 0$ *entonces* $\overline{P} \in \phi(\Gamma) \Leftrightarrow \overline{x}$ *es un cuadrado de un racional.*

DEMOSTRACIÓN. Por definición $\phi(\mathcal{O}) = \overline{\mathcal{O}}$ lo cual prueba la primera observación. Para la segunda, observemos que $\phi(\mathcal{O}) = \phi(T) = \overline{\mathcal{O}} \neq \overline{T}$ así que $\overline{T} = (0,0) \in \phi(\Gamma)$ si y solo si existe $P = (x,y)$ con $x \neq 0$ tal que

$$\phi(P) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) = (0,0)$$

esto es equivalente a la existencia de un punto $P = (x, y) \in \Gamma$ con $x \neq 0$ e $y = 0$ lo cual equivale la existencia de una raíz racional no nula de

$$X^3 + aX^2 + bX = (X^2 + aX + b)X = 0,$$

esto equivale a que el discriminante $\Delta = a^2 - 4b$ sea el cuadrado de un número racional.

Para probar la tercera afirmación, tomemos $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ con $x \neq 0$, observemos que si $\overline{P} \in \phi(\Gamma)$ entonces $\overline{x}$ es un cuadrado de un racional (directo de la fórmula de ϕ), para probar el recíproco supongamos que $\overline{x} = s^2$ donde s es un racional no nulo, queremos hallar $P = (x, y)$ tal que

$$\phi(P) = \phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) = (\overline{x}, \overline{y}) = (s^2, \overline{y})$$

Alcanza con que $(x, y) \in \Gamma$ verifique $y = sx$ donde x verique

$$\frac{(sx)(x^2 - b)}{x^2} = \overline{y}$$

Para lo cual alcanza con que x verifique $s(x^2 - b) = \overline{y}x$ o sea que x sea una raíz racional del polinomio

$$sX^2 - \overline{y}X - bs = 0, \tag{70}$$

una condición necesaria y suficiente para la existencia de dicha raíz racional es que el discriminante

$$\Delta = \overline{y}^2 - 4s(-bs) = \overline{y}^2 + 4s^2 b = \overline{y}^2 + 4\overline{x}b,$$

sea cuadrado perfecto. Pero dado que el punto $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ entonces satisface la ecuación

$$\overline{y}^2 = \overline{x}^3 - 2a\overline{x}^2 + (a^2 - 4b)\overline{x}$$

por lo tanto:

$$\overline{y}^2 + 4\overline{x}b = \overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} = \overline{x}(\overline{x}^2 - 2a\overline{x} + a^2) = (s(\overline{x} - a))^2 .$$

Luego los dos puntos racionales $P = (x, y)$ donde

$$x = \frac{\overline{y} \pm s(\overline{x} - a)}{2s}, \qquad y = \frac{\overline{y} \pm s(\overline{x} - a)}{2},$$

verifican que

$$\left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) = (\overline{x}, \overline{y}) \tag{71}$$

solo falta chequear que $(x, y) \in \Gamma$, sean x e y como arriba con los signos positivos

$$x^2 + ax + b = \left(\frac{\overline{y} + s(\overline{x} - a)}{2s}\right)^2 + a\left(\frac{\overline{y} + s(\overline{x} - a)}{2s}\right) + b = \frac{\overline{y}^2 + 2s\overline{x}\overline{y} + s^2\overline{x}^2 + a^2s^2 - 2s^2a^2 + 4bs^2}{4s^2}$$

$$= \frac{\overline{x}^3 - 2a\overline{x}^2 + (a^2 - 4b)\overline{x} + 2s\overline{y}\overline{x} + s^2\overline{x}^2 - a^2s^2 + 4bs^2}{4s^2}$$

$$= \frac{s^6 - 2as^4 + a^2s^2 - 4bs^2 + 2\overline{y}s^3 + s^6 - a^2s^2 + 4bs^2}{4s^2}$$

$$= \frac{s\overline{y} + s^4 - as^2}{2} = \frac{s\overline{y} + s^2(\overline{x} - a)}{2} = sy = \frac{y^2}{x},$$

lo cual prueba que efectivamente $P = (x, y) \in \Gamma$ y por la ecuación (71) verifica $\phi(P) = \overline{P}$. □

La idea final para probar que $[\overline{\Gamma} : \phi(\Gamma)]$ es finito, dado que $[\overline{\Gamma} : \phi(\Gamma)]$ no es otra cosa que el cardinal del grupo cociente $\overline{\Gamma}/\phi(\Gamma)$, es encontrar un morfismo inyectivo de este último con imagen finita. Probaremos a continuación que el morfismo:

$$\begin{array}{rccll} \overline{\alpha}: & \overline{\Gamma} & \longrightarrow & \mathbb{Q}^*/\mathbb{Q}^{*2} & (mod\ \mathbb{Q}^{*2}) \\ & \overline{\mathcal{O}} & \mapsto & 1 & (mod\ \mathbb{Q}^{*2}) \\ & \overline{T} & \mapsto & \overline{b} & (mod\ \mathbb{Q}^{*2}) \\ & (\overline{x},\overline{y}) & \mapsto & \overline{x} & (mod\ \mathbb{Q}^{*2}) \quad \text{si } x \neq 0 \end{array}$$

cumple con lo requerido, dando por culminado la prueba del Teorema de Mordell para curvas elíptica racionales con un punto de orden 2 racional.

Afirmación 1. La función $\overline{\alpha}$ definida anteriormente es un morfismo de grupos.

Demostración. Veamos primero que lleva opuestos en opuestos.

$$\begin{array}{ll} \overline{\alpha}(-\overline{\mathcal{O}}) = \overline{\alpha}(\overline{\mathcal{O}}) = 1 = 1^{-1} = \overline{\alpha}(\overline{\mathcal{O}})^{-1} & (\text{mód } \mathbb{Q}^{*2}) \\ \overline{\alpha}(-\overline{T}) = \overline{\alpha}(\overline{T}) = \overline{b} \equiv \overline{b}^{-1} = \phi(\overline{T})^{-1} & (\text{mód } \mathbb{Q}^{*2}) \\ \overline{\alpha}(-\overline{P}) = \overline{\alpha}\left((x,-y)\right) = x \equiv x^{-1} = \overline{\alpha}\left((x,y)\right)^{-1} = \overline{\alpha}(\overline{P})^{-1} & (\text{mód } \mathbb{Q}^{*2}) \end{array}$$

Donde $\overline{T} = (0,0)$ y $\overline{P} = (\overline{x},\overline{y}) \in \overline{\Gamma}$ con $\overline{x} \neq 0$. Se observa además que la curva elíptica $\overline{E}/\mathbb{Q}$ es no singular de donde $\overline{b} \neq 0$.

Como $\overline{\alpha}$ lleva opuestos en opuestos para probar que es un morfismo es suficiente probar que si $P_1 \oplus P_2 \oplus P_3 = \overline{\mathbb{O}}$ entonces

$$\phi(P_1)\phi(P_2)\phi(P_3) \equiv 1 \quad (\text{mód } \mathbb{Q}^{*2}) \tag{72}$$

Si alguno de los tres puntos P_1, P_2 ó P_3 fuese $\overline{\mathcal{O}}$, supongamos que fuese P_3 entonces tenemos que $\phi(P_3) = 1$ y que $P_1 = -P_2$, por lo tanto $\phi(P_1) = \phi(P_2)^{-1}$ así que

$$\phi(P_1)\phi(P_2)\phi(P_3) = \phi(P_1)\phi(P_2) = 1$$

y se verifica (72).

Si alguno de los puntos fuese $\overline{T} = (0,0)$ supongamos P_3, entonces tenemos que $\phi(P_3) = \overline{b}$ y (72) se reduce a probar que

$$\phi(P_1)\phi(P_2)\overline{b} \equiv 1 \quad (\text{mód } \mathbb{Q}^{*2}).$$

Como $\overline{b} \neq 0$, $\overline{b} \equiv \overline{b}^{-1} \quad (\text{mód } \mathbb{Q}^{*2})$ así que hay que probar que

$$\phi(P_1)\phi(P_2) \equiv \overline{b} \quad (\text{mód } \mathbb{Q}^{*2}).$$

Podemos suponer que P_1 y P_2 son distintos de $\overline{\mathcal{O}}$ y de $\overline{T}$, pues en cualquiera de los dos casos tenemos $P_1 = \overline{\mathcal{O}}$ ó $P_2 = \overline{\mathcal{O}}$ caso que ya tenemos analizado. Sea entonces $Y = \lambda X$ la recta que pasa por los puntos P_1, P_2 y $\overline{T}$, tenemos que x_1, x_2 y 0 son las tres raíces de la ecuación

$$(\lambda X)^2 = X^3 + \overline{a}X^2 + \overline{b}X,$$

así que x_1 y x_2 son las dos raíces de la ecuación

$$X^3 + (\overline{a} - \lambda^2)X + \overline{b},$$

asi que

$$\overline{\alpha}(P_1)\overline{\alpha}(P_2) = x_1x_2 \equiv \overline{b} \quad (\text{mód } \mathbb{Q}^{*2}).$$

Ahora veamos el caso en que ninguno de los tres puntos $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ y $P_3 = (x_3, y_3)$ es $\overline{\mathcal{O}}$ o $\overline{T}$. Tomemos $Y = \lambda X + \nu$ la recta que pasa por esos tres puntos (la recta tangente a la cúbica en caso de que coincidan), entonces x_1, x_2 y x_3 son las tres raíces de la ecuación

$$(\lambda X + \nu)^2 = X^3 + \overline{a}X^2 + \overline{b}X,$$

que despejando para un lado nos queda

$$X^3 + (\overline{a} - \lambda^2)X^2 + (b - 2\lambda\nu)X - \nu^2,$$

y tenemos que

$$\phi(P_1)\phi(P_2)\phi(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \pmod{\mathbb{Q}^{*\,2}}.$$

Lo cual termina de probar (72) y por lo tanto que $\overline{\alpha}$ es un morfismo.

Observemos además que por la proposición 4.17, la imagen del morfismo $\phi = \phi_E$ es justamente el kernel del morfismo $\overline{\alpha}$ por lo tanto la función $\overline{\alpha}$ induce un morfismo $\widetilde{\overline{\alpha}}$ inyectivo en el cociente

$$\widetilde{\overline{\alpha}} : \frac{\overline{\Gamma}}{\phi(\Gamma)} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*\,2}} : [P] \mapsto \phi(P),$$

donde $[P]$ representa la clase del punto $P \in \overline{\Gamma}$ en el cociente.

Solo resta probar que la imagen de $\widetilde{\overline{\alpha}}$ o lo que es lo mismo, la imagen de $\overline{\alpha}$ es un conjunto finito.

Afirmación 2. $\overline{\alpha}(\overline{\Gamma})$ es un conjunto finito.

DEMOSTRACIÓN. Recordemos que si $P = (x, y) \in \overline{\Gamma}$ con $x \neq 0$ (i.e $P \neq \overline{T}$) teníamos que $x = m/e^2$ e $y = n/e^3$ con m y e coprimos (y n y e coprimos en el caso que $y \neq 0$), sustituyendo en la ecuación de la cúbica

$$\frac{n^2}{e^6} = \frac{m^3}{e^6} + \frac{\overline{a}m^2}{e^4} + \frac{\overline{b}m}{e^2},$$

luego:

$$n^2 = m^3 + \overline{a}m^2e^2 + \overline{b}me^4 = m(m^2 + \overline{a}me^2 + \overline{b}e^4).$$

Observemos que

$$\operatorname{mcd}(m, m^2 + \overline{a}me^2 + \overline{b}e^4) = \operatorname{mcd}(m, \overline{b}e^4) = \operatorname{mcd}(m, \overline{b}).$$

luego si p es un primo que no divide a b pero divide a m entonces p no puede dividir a $m^2 + \overline{a}me^2 + \overline{b}e^4$ luego el exponente de p en la descomposición factorial de m es el mismo con el que aparece en n^2 que es par; si $p_1, p_2, \ldots, p_t$ son los divisores primos de b tenemos que

$$m = \pm(entero)^2 p_1^{\varepsilon_1} p_2^{\varepsilon_2} \ldots p_t^{\varepsilon_t},$$

donde $\varepsilon_i = 0$ ó 1 para todo $i = 1, 2, \ldots, t$, luego

$$\overline{\alpha}(P) = x = \frac{m}{e^2} \equiv m \equiv (entero)^2 p_1^{\varepsilon_1} p_2^{\varepsilon_2} \ldots p_t^{\varepsilon_t} \pmod{\mathbb{Q}^{*\,2}}.$$

Para $P = T$ también tenemos que

$$\overline{\alpha}(T) = \overline{b} \equiv p_1^{\varepsilon_1} p_2^{\varepsilon_2} \ldots p_t^{\varepsilon_t}$$

donde $\varepsilon_i = 0$ si p_i aparece con exponente par en la descomposición factorial de $\overline{b}$ y 1 si no.

En cualquier caso se tiene que la imagen de $\overline{\alpha}$ se encuentra contenida dentro del conjunto

$$\{p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_t^{\varepsilon_t} : \varepsilon_i = 0 \text{ ó } 1 \text{ para todo } i = 1, 2, \dots, t\} \subset \mathbb{Q}^*/\mathbb{Q}^{*2},$$

donde los p_i son los distintos primos que dividen a $\overline{b}$. Este conjunto es finito y posee 2^{t+1} elementos. Como $\widetilde{\overline{\alpha}}$ es inyectiva entonces tenemos

$$\left|\overline{\Gamma}/\phi(\Gamma)\right| = \left|Im(\widetilde{\overline{\alpha}})\right| = |Im(\overline{\alpha})| \leq 2^{t+1},$$

lo cual prueba la afirmación. □

Las dos afirmaciones anteriores prueban la finitud de $[\overline{\Gamma} : \phi(\Gamma)]$ que como vimos, es suficiente para probar la finitud de $[\Gamma : 2\Gamma]$ que era la parte que nos faltaba para probar el Teorema de Mordell, al menos para nuestra versión restringida asumiendo la existencia de un punto racional de orden 2. Enunciamos el Teorema de Mordell:

TEOREMA 4.18 (Mordell). *Si $E/\mathbb{Q}$ es una curva elíptica (con un punto racional de orden 2) y $\Gamma = E(\mathbb{Q})$ es el grupo de sus puntos racionales entonces Γ es un grupo finitamente generado.*

Aunque hemos probado el teorema bajo la hipótesis adicional de existencia de puntos de orden 2, el teorema sigue valiendo aún sin esa hipótesis. De hecho el matemático Weil generalizó este teorema para curvas elíptica definidas sobre cuerpos numéricos (ver por ejemplo [**3**],pag 199) .

2. El rango de una curva elíptica.

En la sección anterior hemos probado que si E es una curva elíptica definida sobre $\mathbb{Q}$ con un punto racional entonces su grupo Γ de puntos racionales sobre la cúbica es un grupo abeliano finitamente generado, luego por el Teorema de estructura para grupos abelianos finitamente generado tenemos que

$$\Gamma \simeq \mathbb{Z}^r \oplus \mathcal{T},$$

donde $\mathcal{T}$ es el subgrupo de torsión formado por los puntos de orden finito.

DEFINICIÓN 4.19. Llamamos rango de una curva elíptica al número r definido como arriba.

Para determinar el grupo de una curva elíptica debemos determinar la parte de torsión $\mathcal{T}$ y determinar el rango de curva.

El Teorema de Nagell- Lutz resuelve el primero de los problemas, pues nos da un procedimiento para encontrar todos los puntos de orden finito en una cantidad finita de pasos, lo que resuelve el problema algoritmicamente.

Además es bien conocido todos las posibles parte de torsión que puede tener una curva elíptica racional, el Teorema de Mazur establece que o bien $\mathcal{T} \simeq \mathbb{Z}_m$ con $1 \leq m \leq 10$ ó $m = 12$, o bien $\mathcal{T} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2m}$ con $\leq m \leq 4$.

Lamentablemente determinar el rango de una curva elíptica es un problema mucho más dificil, de hecho es muy poco lo que se conoce sobre el rango y se conjetura que solo hay un número finito de rangos posible, tampoco se conoce un algoritmo para determinar el rango.

A continuación analizaremos con más detalle algunos de los pasos de la prueba del Teorema de Mordell para obtener un procedimiento que nos ayudará a calcular el rango en algunos casos particulares.

2.1. Algunas fórmulas para el rango.

Como estamos suponiendo la existencia de un punto racional de orden 2, entonces haciendo un cambio de variable podemos suponer que $T = (0, 0)$ es un punto de orden 2 de la cúbica, la cual toma la forma

$$E : Y^2 = X^3 + aX^2 + bX.$$

La no singularidad implicaba que $b \neq 0$ y que $a^2 - 4b \neq 0$.

Por el Teorema de Mordell el grupo de sus puntos racionales Γ es un grupo finitamente generado. El Teorema de estructura establece además que la parte de torsión $\mathcal{T}$ es suma directa de grupos cíclicos y por lo tanto

$$T \simeq \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{\nu_t}},$$

donde los p_i son primos (no necesariamente distintos).

Si denotamos por κ a la cantidad de $i : p_i = 2$ tenemos que

$$\frac{\Gamma}{2\Gamma} = \frac{\mathbb{Z}^r}{2\mathbb{Z}^r} \oplus \frac{\mathbb{Z}_{p_1^{\nu_1}}}{2\mathbb{Z}_{p_1^{\nu_1}}} \oplus \ldots \frac{\mathbb{Z}_{p_t^{\nu_t}}}{2\mathbb{Z}_{p_t^{\nu_t}}} = \mathbb{Z}_2^{r+\kappa}. \tag{73}$$

Puesto que la multiplicación por 2 en $\mathbb{Z}_n$ es una isomorfismo si n es impar y tiene kernel $\{0, n/2\}$ si n es par.

Por otra parte podemos considerar el conjunto

$$\Gamma[2] = \{P \in \Gamma : 2P = \mathcal{O}\}.$$

Observemos que si $P = (x, y_1, \ldots, y_t) \in \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \ldots \oplus \mathbb{Z}_{p_t^{\nu_t}}$ observemos que $2P = (2x, 2y_1, \ldots, 2y_t) = (0, 0, \ldots, 0)$ si y solo si:

$$\begin{cases} x = 0 & \\ y_i = 0 & \text{para } i : p_i \text{ sea impar (i.e para } i : p_i \neq 2) \\ y_i \equiv 0 \pmod{p_i^{\nu_i - 1}} & \text{para } i : p_i \text{ sea par (i.e para } i : p_i = 2) \end{cases}$$

Los dos primeros casos quedan determinados, para la última solo hay dos soluciones módulo $p_i^{\nu_i}$ que son 0 y $p_i^{\nu_i - 1}$. Por lo tanto tenemos

$$\#\Gamma[2] = 2^\kappa.$$

Combinando esto último con la ecuación (73) obtenemos

$$[\Gamma : 2\Gamma] = 2^r \cdot \#\Gamma[2], \tag{74}$$

válida para cualquier grupo abeliano finitamente generado Γ.

Para nuestro caso particular en que Γ es el grupo de los puntos racionales de la cúbica $E : Y^2 = f(X)$ donde $f(X) = X(X^2 + aX + b)$, tenemos que $\Gamma[2]$ conciste en los puntos $\mathcal{O}$ y los puntos de la forma $(x, 0)$ donde x es una raíz racional de f así que:

$$\#\Gamma[2] = \begin{cases} 4 & \text{si } a^2 - 4b \text{ es un cuadrado.} \\ 2 & \text{si } a^2 - 4b \text{ no es cuadrado.} \end{cases} \tag{75}$$

Por otra parte teniamos morfismos ϕ y ψ cuya composición es la multiplicación por 2, así que

$$[\Gamma : 2\Gamma] = [\Gamma : \psi \circ \phi(\Gamma)] = [\Gamma : \psi(\overline{\Gamma})][\psi(\overline{\Gamma}) : \psi(\phi(\Gamma))], \tag{76}$$

donde la última igualdad se deduce de la inclusión de grupos $\Gamma \supset \psi(\overline{\Gamma}) \supset \psi(\phi(\Gamma)) = 2\Gamma$.

Para determinar el índice de $\psi(\phi(\Gamma))$ en $\psi(\overline{\Gamma})$ utilizaremos un resultado general sobre grupos abelianos que expondremos a continuación.

PROPOSICIÓN 4.20. *Sea A un grupo abeliano y B un subgrupo de A con índice finito en A, si $\psi : A \to A'$ es un morfismo de grupos entonces*

$$[\psi(A) : \psi(B)] = \frac{[A : B]}{[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap B]}.$$

DEMOSTRACIÓN. Usando teoremas clásicos sobre cociente de grupos tenemos:

$$\frac{\psi(A)}{\psi(B)} \simeq \frac{A}{B + \mathrm{Ker}(\psi)} \simeq \frac{A/B}{(B + \mathrm{Ker}(\psi))/B} \simeq \frac{A/B}{\mathrm{Ker}(\psi)/\mathrm{Ker}(\psi) \cap B}$$

□

Para nuestro caso nos queda

$$[\psi(\overline{\Gamma}) : \psi(\phi(\Gamma))] = \frac{[\overline{\Gamma} : \phi(\Gamma)]}{[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap \phi(\Gamma)]}. \tag{77}$$

Pero $\mathrm{Ker}\,\psi = \{\overline{\mathcal{O}}, \overline{T}\}$ y tenemos que $\overline{T} \in \phi(\Gamma) \Leftrightarrow \overline{b} = a^2 - 4b$ es un cuadrado perfecto. Así que tenemos que

$$[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap \phi(\Gamma)] = \begin{cases} 1 & \text{si } \overline{b} = a^2 - 4b \text{ es un cuadrado.} \\ 2 & \text{si } \overline{b} = a^2 - 4b \text{ no es un cuadrado.} \end{cases}$$

Comparando con la ecuación (75) tenemos que

$$[\mathrm{Ker}(\psi) : \mathrm{Ker}(\psi) \cap \phi(\Gamma)] = \frac{4}{\#\Gamma[2]}.$$

Sustituyendo en (77) nos queda

$$[\psi(\overline{\Gamma}) : \psi(\phi(\Gamma))] = \frac{[\overline{\Gamma} : \phi(\Gamma)] \cdot \#\Gamma[2]}{4}.$$

Y finalmente, sustituyendo el valor de este índice en (76) y utilizando la ecuación (74) tenemos

$$2^r = \frac{[\Gamma : 2\Gamma]}{\#\Gamma[2]} = [\Gamma : \psi(\overline{\Gamma})]\frac{[\psi(\Gamma) : \psi(\phi(\Gamma))]}{\#\Gamma[2]} = \frac{[\Gamma : \psi(\overline{\Gamma})] \cdot [\overline{\Gamma} : \phi(\Gamma)]}{4}. \tag{78}$$

Luego para calcular el rango alcanza con determinar los índices que aparecen en los numeradores de la última fracción, para ello conviene considerar nuevamente el morfismo $\overline{\alpha}$ introducido en la parte final de la prueba de Mordell. El morfismo $\overline{\alpha} : \overline{\Gamma} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ estaba definido por:

$$\begin{array}{lcll} \overline{\mathcal{O}} & \mapsto & 1 & (mod\ \mathbb{Q}^{*2}) \\ \overline{T} & \mapsto & \overline{b} & (mod\ \mathbb{Q}^{*2}) \\ (\overline{x}, \overline{y}) & \mapsto & \overline{x} & (mod\ \mathbb{Q}^{*2}) \quad \text{si } x \neq 0 \end{array}$$

El kernel de este morfismo era justamente $\phi(\Gamma)$ entonces inducia un morfismo inyectivo $\widetilde{\overline{\alpha}}$ en el cociente

$$\widetilde{\overline{\alpha}} : \overline{\Gamma}/\phi(\Gamma) \to \mathbb{Q}^*/\mathbb{Q}^{*2}, \qquad \widetilde{\overline{\alpha}}([P]) = \overline{\alpha}(P).$$

De donde:

$$[\overline{\Gamma} : \phi(\Gamma)] = \#\frac{\overline{\Gamma}}{\phi(\Gamma)} = \#Im(\widetilde{\overline{\alpha}}) = \#\overline{\alpha}(\overline{\Gamma})$$

En forma análoga si denotamos por $\overline{\overline{\Gamma}}$ los puntos racionales de $\overline{\overline{E}}$ se puede considerar el morfismo $\overline{\overline{\alpha}} : \overline{\overline{\Gamma}} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, definido de la misma manera que $\overline{\alpha}$, es decir $\overline{\overline{\alpha}}(\overline{\overline{\mathbb{O}}}) = 1, \overline{\overline{\alpha}}(\overline{\overline{T}}) = \overline{\overline{b}}$ y para $P = (x, y) \in \overline{\overline{\Gamma}}$ con $x \neq 0$, $\overline{\overline{\alpha}}(P) = x \pmod{\mathbb{Q}^{*2}}$ y de la misma manera se llega a que $[\overline{\overline{\Gamma}} : \overline{\phi}(\overline{\Gamma})] = \#\overline{\overline{\alpha}}(\overline{\overline{\Gamma}})$.

Pero $\psi = \nu \circ \overline{\phi}$ donde ν era el isomorfismo de $\overline{\overline{\Gamma}}$ a Γ dado por $\nu(x, y) = \left(\frac{x}{4}, \frac{y}{8}\right)$, así que $[\Gamma : \psi(\overline{\Gamma})] = [\overline{\overline{\Gamma}} : \overline{\phi}(\overline{\Gamma})] = \#\overline{\overline{\alpha}}(\overline{\overline{\Gamma}})$.

Finalmente observemos que si $\alpha : \Gamma \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ es el mapa que lleva a un punto $P = (x, y) \in \Gamma$ con $P \neq \mathcal{O}, T$ entonces $\alpha(P) = x \pmod{Q^{*2}}$, $\alpha(\mathcal{O}) = 1$ y $\alpha(T) = b$ entonces $Im(\alpha) = Im(\overline{\alpha})$ pues si $x \neq 0$ entonces $P = (x, y) \in \overline{\overline{\Gamma}} \Leftrightarrow \eta(P) = (\frac{x}{4}, \frac{y}{8}) \in \Gamma$ con

$x \equiv \frac{x}{4} \pmod{\mathbb{Q}^{*2}}$ y $\alpha(\overline{\overline{T}}) = \overline{\overline{b}} = 16b \equiv b = \alpha(T) \pmod{\mathbb{Q}^{*2}}$.

En virtud de lo que acabamos de ver, la ecuación (78) puede escribirse como

$$\frac{\#\alpha(\Gamma)\#\overline{\alpha}(\overline{\Gamma})}{4} = 2^r. \tag{79}$$

Esta ecuación es en la que nos basaremos para calcular los indices en los ejemplos. Ahora solo nos queda ver como determinar las imagenes de tales morfismos.

Para determinar la imagen de α debemos ver que valores racionales de x módulo cuadrados, son posibles para puntos $P = (x, y) \in \Gamma$.

Comenzemos considerando un punto $P = (x, y) \in \Gamma$ recordemos que x e y podían escribirse como fracciones irreducibles en la forma

$$x = \frac{m}{e^2}, \quad y = \frac{n}{e^3},$$

con $e > 0$.

Si $m = 0$ tenemos el punto $(x, y) = (0, 0) = T$ y $\alpha(T) = b$, luego $b \pmod{\mathbb{Q}^{*2}}$ es siempre un elemento en la imagen de α.

Si $\Delta = a^2 - 4b = s^2$ con s racional, entonces tenemos dos puntos más de orden 2 distintos de T, que vienen dados por

$$\left(\frac{-a+d}{2}, 0\right) \quad \text{y} \quad \left(\frac{-a-d}{2}, 0\right).$$

Y en este caso tenemos que $\frac{-a+d}{2}$ y $\frac{-a-d}{2} \pmod{\mathbb{Q}^{*2}}$ son elementos de la imagen de α.

Si $P = (\frac{m}{e^2}, \frac{n}{e^3})$ con $m, n \neq 0$ sustituyendo en la ecuación de la cúbica E y multiplicando ambos miembros por e^6 obteniamos que

$$n^2 = m^3 + am^2e^2 + bme^4 = m(m^2 + ame^2 + be^4). \tag{80}$$

Si

$$d = \text{mcd}(m, m^2 + ame^2 + be^4) = \text{mcd}(m, be^4) = \text{mcd}(m, b)$$

donde elegimos a d con el mismo signo que m, podemos luego escribir $m = dm_1$ y $b = db_1$ con $m_1 > 0$ y b_1 enteros coprimos.
Sustituyendo en (80) obtenemos

$$n^2 = dm_1(d^2m_1^2 + adm_1e^2 + db_1e^4) = d^2m_1(dm_1^2 + am_1e^2 + b_1e^4).$$

Como $d^2|n^2$ entonces $d|n$ y podemos escribir $n = dn_1$ con n_1 entero y la ecuación anterior queda

$$n_1^2 = m_1(dm_1^2 + am_1e^2 + b_1e^4), \tag{81}$$

pero como

$$\text{mcd}(m_1, dm_1^2 + am_1e^2 + b_1e^4) = \text{mcd}(m_1, b_1e^4) = \text{mcd}(m_1, b_1) = 1,$$

donde la segunda igualdad es porque m_1 es coprimo con e pues m es coprimo con e y $m_1|m$, luego como $m_1 > 0$ tenemos que:

$$\begin{cases} m_1 = M^2 \\ dm_1^2 + am_1e^2 + b_1e^4 = N^2 \end{cases}$$

con M y N enteros. Por (81) nos queda que $n_1 = MN$ y sustituyendo $m_1 = M^2$ en la segunda ecuación del sistema anterior obtenemos

$$N^2 = dM^4 + aM^2e^2 + b_1e^4. \tag{82}$$

Observemos que M, N, e, d y b_1 de la ecuación anterior verifican las siguientes condiciones:

$$\begin{cases} \text{mcd}(M, e) = \text{mcd}(N, e) = \text{mcd}(d, e) = 1 \\ \text{mcd}(b_1, M) = \text{mcd}(N, M) = 1 \end{cases} \tag{83}$$

En efecto, como $\text{mcd}(m, e) = 1$ y $m = dM^2$ entonces $\text{mcd}(M, e) = \text{mcd}(d, e) = 1$. Si $\text{mcd}(e, N) \neq 1$ entonces hay algún primo p tal que $p|e$ y $p|N$, por (82) tenemos que $p|dM^4$ pero como p no puede dividir a d (pues $p|e$ y $\text{mcd}(d, e) = 1$) entonces $p|M^4$ luego $p|M$ pues p es primo, pero en este caso p sería divisor común de M y e que como vimos eran coprimos, esta contradicción implica que $\text{mcd}(e, N) = 1$.

Ahora supongamos que $\text{mcd}(b_1, M) \neq 1$ y tomemos un divisor primo común p, $p|M = m_1^2$ luego $p|m_1$ pues p es primo, pero en este caso p sería un divisor común de m_1 y b_1 lo cual es absurdo pues son coprimos, esto implica que $\text{mcd}(b_1, M) = 1$.

Finalmente si $\text{mcd}(M, N) = 1$ entonces podemos tomar un divisor primo común p, por (82) tenemos que $p|b_1e^4$ pero como p no puede dividir a e (pues $p|M$ y $\text{mcd}(M, e) = 1$) entonces $p|b_1$ lo cual es absurdo pues p también divide a M y $\text{mcd}(M, b_1) = 1$, así que $\text{mcd}(M, N) = 1$ lo cual termina de probar (83).

Consideremos pues para cada punto $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in \Gamma$ con $m \neq 0$ la ecuación diofántica

$$Eq(d): \quad N^2 = dM^4 + aM^2e^2 + b_1e^4$$

donde $d = \text{mcd}(m, b)$ con el signo de m, a y $b_1 = b/d$. Llamaremos a $Eq(d)$ la ecuación asociada a P. Diremos que una solución (M, e, N) de $Eq(d)$ es admisible si $Me \neq 0$ y primitiva si verifica (83). Nosotros acabamos de probar que el punto (M, e, N) formado como recién vimos es solución primitiva de la ecuación $Eq(d)$, donde $d = \text{mcd}(m, b)$ que como vimos esto implica que $\alpha(P) = d \pmod{\mathbb{Q}^{*2}}$. Sustituyendo de las ecuaciones anteriores podemos obtener fórmulas explícitas para M y N que son

$$M = \sqrt{\frac{m}{d}}, \qquad N = \frac{n}{\sqrt{dm}},$$

llamaremos a (M, e, N) la solución de $Eq(d)$ asociada a $P = (m, n)$, que como vimos es una solución primitiva.

Recíprocamente, para cada divisor d de b, definimos $b_1 = b/d$ y consideramos la ecuación diofántica

$$Eq(d): \quad N^2 = dM^4 + aM^2e^2 + b_1e^4, \tag{84}$$

donde a, d y b_1 son parámetros y M, e y N incógnitas. Si (M, e, N) es una solución admisible podemos asociarle el punto $P = (x, y)$ definido por

$$x = \frac{dM^2}{e^2}, \quad y = \frac{dMN}{e^3},$$

este punto verifica estar en Γ, en efecto

$$y^2 = \frac{d^2M^2}{e^6}N^2 = \frac{d^2M^2}{e^6}\left(dM^4 + aM^2e^2 + \frac{be^4}{d}\right) = \frac{d^3M^6}{e^6} + a\frac{d^2M^4}{ce^4} + b\frac{dM^2}{e^2}$$

$$= \left(\frac{dM^2}{e^2}\right)^3 + a\left(\frac{dM^2}{e^2}\right)^2 + b\left(\frac{dM^2}{e^2}\right) = x^3 + ax^2 + bx,$$

además $\alpha(P) = d \pmod{\mathbb{Q}^{*2}}$.

OBSERVACIÓN 4.21. Si P es el punto de Γ asociado a $Eq(d)$, no se cumple necesariamente que $Eq(d)$ sea la ecuación asociada al punto P porque no necesariamente se va a cumplir que $\mathrm{mcd}(dM^2, b) = d$ y en particular la ecuación $Eq(d)$ podría no tener soluciones primitivas como sucede por ejemplo con la ecuación $N^2 = -M^4 + 20e^4$ que posee la solución admisible $(2, 1, 2)$ pero no posee soluciones primitivas pues si M es impar la ecuación implica $N^2 \equiv -1 \pmod 4$ lo cual es imposible.

Si d es un racional no nulo entonces puede escribirse de forma única como $d = \ell k^2$ donde ℓ es un entero libre de cuadrados y k racional (ℓ es el producto de primos que aparece con exponente impar en d). Si la ecuación $Eq(d)$ con d entero y $d|b$ tiene solución admisible entonces sabemos que $D = d \pmod{\mathbb{Q}^{*2}} \in \alpha(\Gamma)$, pero a priori si $D \in \alpha(\Gamma)$ y d_0 es un entero que divide a b, no sabemos si $Eq(d_0)$ va a tener solución admisible. Lo único que sabemos es que hay algún d entero que divide a b tal que $d \equiv d_0 \pmod{\mathbb{Q}^{*2}}$ y que $Eq(d)$ posee solución admisible (más aún, sabemos que existe un d en esas condiciones tal que la ecuación $Eq(d)$ posee soluciones primitivas), pero como saber a priori cual es ese d?. La siguiente proposición nos ayuda al respecto.

PROPOSICIÓN 4.22. *Sea $D = d_0 \pmod{\mathbb{Q}^{*2}}$ es un punto de $Im(\alpha)$ distinto de $1 \pmod{\mathbb{Q}^{*2}}$ y de $b \pmod{\mathbb{Q}^{*2}}$. Si ℓ es la parte libre de cuadrados de d_0 entonces la ecuación $Eq(\ell)$ posee solución admisible (no necesariamente primitiva).*

DEMOSTRACIÓN. Sea $P = (\frac{m}{e^2}, \frac{n}{e^2}) \in \Gamma$ con $me \neq 0$ (obs $P \neq T$) tal que $\alpha(P) = D$, si $d = \mathrm{mcd}(m, b)$ y consideramos la ecuación asociada a P, $Eq(d)$, sabemos que posee solución primitiva (M, e, N). Sabemos además que $\alpha(P) = d \pmod{\mathbb{Q}^{*2}}$ así que $d \equiv d_0 \equiv \ell \pmod{\mathbb{Q}^{*2}}$ y por lo tanto ℓ es también la parte libre de cuadrados de d, es decir $d = \ell k^2$ con k entero (pues d lo es). Tenemos que

$$N^2 = dM^4 + aM^2e^2 + b_1e^4 \Rightarrow k^2N^2 = dk^2M^4 + ak^2M^2e^2 + b_1k^2e^4$$

$$\Rightarrow (kN)^2 = \ell(kM)^4 + a(kM)^2e^2 + b_1k^2e^4,$$

con $\ell \cdot b_1k^2 = b_1(\ell k^2) = b_1d = b$ así que (kM, e, kN) es una solución admisible de $Eq(\ell)$. $\square$

Así que tenemos un procedimiento sencillo para calcular la imagen de α, que es la siguiente:
Primero listamos todos los divisores d de b y nos quedamos con los libres de cuadrados. Si ℓ es un divisor libre de cuadrado de b entonces $\ell \pmod{\mathbb{Q}^{*2}} \in \alpha(\Gamma)$ si y solo si la ecuación diofántica $Eq(\ell)$ tiene solución admisible.

En el caso que ℓ no tenga otros divisores de b equivalente módulo cuadrados entonces tenemos también que $\ell \pmod{\mathbb{Q}^{*2}} \in \alpha(\Gamma)$ si y solo si la ecuación diofántica $Eq(\ell)$ tiene solución primitiva (a veces es más fácil probar que no hay soluciones primitivas).

Este va a ser el camino que tomaremos para calcular el cardinal de $\alpha(\overline{\Gamma})$, y siguiendo de forma análoga calcularemos también $\beta(\Gamma)$ siempre que podamos resolver la ecuación diofántica (84) para obtener el rango de la cúbica E.

OBSERVACIÓN 4.23. Para el caso de puntos de orden 2 distintos de T también están considerados al considerar los divisores $d = (a-s)/2$ y $d = (a+s)/2$ donde $a^2 - 4b = s^2$, pues para las ecuaciones

$$N^2 = \left(\frac{a \pm s}{2}\right) M^4 + aM^2e^2 + \left(\frac{a \mp s}{2}\right) e^4.$$

Los puntos correspondientes a las soluciones tomando $(M, e, N) = (1, 1, 0)$ son justamente los puntos de orden 2 distintos de T.

2.2. Ejemplos. Aquí ilustraremos el método dado anteriormente para determinar el rango y la estructura de grupo de algunas curvas elíptica particulares.

EJEMPLO 4.1. La curva elíptica $E : Y^2 = X^3 + X$.

En este caso $a = 0$ y $b = 1$ así que los posibles valores de $d|b$ son $d = 1$ ó $d = -1$ de donde

$$\alpha(\Gamma) \subset \{1, -1\} \pmod{\mathbb{Q}^{*2}}.$$

Como $\alpha(\mathcal{O}) = 1$ entonces $1 \in \alpha(\Gamma)$.

Por otro lado para $d = -1$ tenemos $b_1 = -1$ luego $-1 \in \alpha(\Gamma)$ si y solo si la ecuación diofántica

$$N^2 = -M^4 - e^4,$$

posee soluciones primitivas, pero con $M \neq 0$ nos queda $N^2 < 0$ por lo que la ecuación no posee soluciones reales com $M \neq 0$ luego $-1 \notin \alpha(\Gamma)$ así que $\alpha(\Gamma) = \{\mathcal{O}\}$.

Su curva asociada es $\overline{E} : Y^2 = X^3 - 4X$.

Los posibles valores de $d|\overline{b} = -4$ son $d = \pm 1, \pm 2, \pm 4$, pero $4 \equiv 1 \pmod{\mathbb{Q}^{*2}}$. así que

$$\overline{\alpha}(\overline{\Gamma}) \subset \{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}}. \tag{85}$$

Pero en virtud de (79) tenemos que

$$\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma}) = 2^{r+2} \geq 4$$

como $\#\alpha(\Gamma) = 1$ tenemos que $\#\overline{\alpha}(\overline{\Gamma})$ pero por (85) debe ser exactamente 4 y por lo tanto el rango $r = 0$.

Tenemos entonces que todos los puntos racionales de E son de torsión, luego para hallarlos tenemos el Teorema de Nagell-Lutz que dice que si $(x, y) \in \Gamma$ es de orden finito

entonces $y = 0$ ó $y|D$ donde D es el discriminante de la curva.

Para $y = 0$ tenemos que $x^3 + x = x(x^2 + 1) = 0$ luego hay solo un punto racional de orden 2 que es $T = (0, 0)$.

Para curvas elíptica de la forma $E : Y^2 = X^3 + aX^2 + bX$, el discriminante viene dado por

$$D = b^2(a^2 - 4b).$$

En nuestro caso, $D = -4$, luego los puntos de orden finito $P = (x, y)$ con $y \neq 0$ tienen coordenadas enteras y verifican $y| - 4$ así que $y = \pm 1, \pm 2, \pm 4$, pero vemos directamente que para cada uno de esos valores de y la ecuación $x^3 + x = y^2$ no posee soluciones enteras así que tenemos $\Gamma = \{\mathcal{O}, T\}$ luego

$$E(\mathbb{Q}) \simeq \mathbb{Z}_2.$$

EJEMPLO 4.2. La curva elíptica $E : Y^2 = X^3 - X$.

En este caso $a = 0, b = -1$ de donde los posibles valores de $d|b$ pueden ser $d = \pm 1$, al igual que antes

$$\alpha(\Gamma) \subset \{1, -1\} \pmod{\mathbb{Q}^{*2}}.$$

Tenemos que $\alpha(\mathbb{O}) = 1 \in \alpha(\Gamma)$ y $\alpha(T) = -1 \in \alpha(\Gamma)$ de donde $\#\alpha(\Gamma) = 2$.

Su curva asociada $\overline{E}$ viene dada por $\overline{E} : Y^2 = X^3 + 4X$ y los posibles valores de $d|\overline{b} = -4$ son $d = \pm 1, \pm 2, \pm 4$ que al igual que antes, como $4 \equiv 1 \pmod{\mathbb{Q}^{*2}}$ tenemos que

$$\overline{\alpha}(\overline{\Gamma}) \subset \{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}},$$

y que $\alpha(\overline{\mathcal{O}}) = 1 \in \overline{\alpha}(\overline{\Gamma})$. Observemos que si $d < 0$ entonces $b_1 = 4/d < 0$ y por lo tanto la ecuación

$$N^2 = dM^4 + b_1 e^4,$$

no posee soluciones con $M \neq 0$ pues no la posee en los reales. Luego

$$\overline{\alpha}(\overline{\Gamma}) \subset \{1, 2\},$$

pero por la ecuación (79) tenemos que

$$\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma}) = 2^{r+2} \geq 4.$$

Dado que $\#\alpha(\Gamma) = 2$ entonces $\#\overline{\alpha}(\overline{\Gamma}) \geq 2$ pero entonces ha de ser exactamente 2 y por lo tanto $r = 0$, esta curva también tiene rango nulo y todos sus puntos son de torsión.

Para hallar los puntos de torsión aplicamos nuevamente el Teorema de Nagell-Lutz, los puntos $P = (x, y)$ de orden 2 tienen $y = 0$ y $x^3 - x = 0$ que tiene solución $x = 0, \pm 1$ de donde hay tres puntos de orden 3.

Para los puntos de torsión de orden superior tenemos que $y|D = -4(-1)^3 = 4$ así que $y = \pm 1, \pm 2, \pm 4$, pero $y^2 = x^3 - x = (x - 1)x(x + 1)$ es múltiplo de 3 lo cual es absurdo, asi que no hay puntos de orden finito excepto los de orden 2 y por lo tanto

$$E(\mathbb{Q}) = \{\mathcal{O}, T, (1, 0), (-1, 0)\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

EJEMPLO 4.3. La curva elíptica $E : Y^2 = X^3 + 3X$.

Tenemos $a = 0, b = 3$ y los posibles $d|b$ son $d = \pm 1, \pm 3$ así que

$$\alpha(\Gamma) \subset \{\pm 1, \pm 3\}.$$

Tenemos además $\alpha(\mathcal{O}) = 1$ y $\alpha(T) = 3$ así que

$$\{1, 3\} \subset \alpha(\Gamma).$$

Para $d = -1$ tenemos $b_1 = -3$ y la ecuación asociada $N^2 = -M^4 - 3e^4$ no tiene solución con $M \neq 0$ así que $-1 \in \alpha(\Gamma)$, la ecuación (79) implica que $\#\alpha(\Gamma)$ debe ser potencia de 2, pero como $2 \leq \alpha(\Gamma) < 4$ ha de ser exactamente 2.

La curva asociada a E es $\overline{E} : Y^2 = X^3 - 12X$, los posibles valores de $d| - 12$ son $d = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$, pero módulos cuadrados racionales $1 \equiv 4$ y $3 \equiv 12$ así que

$$\alpha(\Gamma) \subset \{\pm 1, \pm 2, \pm 3, \pm 6\} \pmod{\mathbb{Q}^{*2}}.$$

Algunos puntos de $\overline{\alpha}(\overline{\Gamma})$ son $1 = \overline{\alpha}(\overline{\mathcal{O}})$ y $-3 \equiv -12 = \alpha(\overline{T}) \pmod{\mathbb{Q}^{*2}}$.

Las ecuaciones diofánticas asociadas a los restantes d vienen dadas por:

$$\begin{array}{lcll} Eq(-1) & : & N^2 = -M^4 + 12e^4 & (1) \\ Eq(2) & : & N^2 = 2M^4 - 6e^4 & (2) \\ Eq(-2) & : & N^2 = -2M^4 + 6e^4 & (3) \\ Eq(3) & : & N^2 = 3M^4 - 4e^4 & (4) \\ Eq(6) & : & N^2 = 6M^4 - 2e^4 & (5) \\ Eq(-6) & : & N^2 = -6M^4 + 2e^4 & (6) \end{array}$$

Observemos que las ecuaciónes (2) y (6) son la misma intercambiando las variables M y e, la misma observación vale para las ecuaciones (3) y (5), luego una de ellas tiene solución si y solo si la otra la tiene.

La ecuación (5) tiene la solución admisible $(M, e, N) = (1, 1, 2)$, la misma solución vale pues para la ecuación (3). Así que por ahora tenemos cuatro puntos en $\overline{\alpha}(\overline{\Gamma})$ que son $1, -2, -3$ y 6. Pero como el cardinal de $\#\overline{\alpha}(\overline{\Gamma})$ es potencia de 2, las posibilidades que nos quedan es que sea 4 ó 8, para ver que es 4 alcanza con ver que alguna de las ecuaciones no posee soluciones admisibles, por ejemplo veamos la (2), si (M, e, N) fuese una solución admisible entonces debe ser además primitiva porque el único divisor de $\overline{b} = -12$ congruente con $d = 2$ módulo cuadrados es el propio 2, luego $\text{mcd}(2MN, e) = \text{mcd}(6N, M) = 1$. Si $N = \dot{3} \Rightarrow 2M^4 = N^2 + 6e^4 = \dot{3} \Rightarrow M = \dot{3}$ contradiciendo que $\text{mcd}(6N, M) = 1$. Si $N \neq \dot{3} \Rightarrow 1 \equiv 2M^4 \pmod 3 \Rightarrow M^4 \equiv 2 \pmod 3$ lo cual es absurdo pues 2 no es un cuadrado módulo 3.

Se deduce pues que

$$2^r = \frac{2 \cdot 4}{4} = 2,$$

y por lo tanto en este caso $r = 1$, así que

$$E(\mathbb{Q}) = \mathbb{Z} \oplus T,$$

donde T es el subgrupo de torsión.

Para determinar la parte de torsión lo haremos como antes usando el Teorema de Nagell-Lutz, primero obtenemos los puntos de orden 2 con son $P = (x, y)$ con $y = 0$ y x verifica $x^3 + 3x = x(x^2 + 3) = 0$ por lo tanto $x = 0$ y T es el único punto de orden 2. Para puntos de torsión de mayor orden tenemos que son de la forma $P = (x, y)$ donde x e y son enteros e $y|D = -2^2 \cdot 3^3$.

Antes de tantear todas las posibilidades observemos que $D^2 \geq y^2 = x^3 + 3x \geq x^3$ de donde $x \leq D^{2/3} = 2^{4/3} \cdot 3^2 \approx 22,6$ así que $x \leq 22$, por otra parte, si $x \leq 0$ entonces $x^3 + 3x \leq 0$ pero entonces no puede ser igual a $y^2 > 0$ ($y = 0$ implica que P sea de orden 2) luego $x > 0$, además observemos que si x es par entonces $x^2 + 3$ es impar y como su producto es cuadrado perfecto entonces el 2 debe aparecer con exponente par en la descomposición factorial de x. Con todas estas observaciones nos hacemos una tablita:

x	$x^2 + 3$	y^2
1	4	2^2
3	12	6^2
4	19	NC
9	84	NC
12	147	42^2
16	259	NC

donde NC indica un valor que no es cuadrado perfecto, así que tenemos los puntos $P_1 = (1, 2), P_2 = (3, 6)$ y $P_3 = (12, 42)$ como posibles candidatos a pertencer al subgrupo de torsión de la cúbica, pero por la fórmula de duplicación, para puntos $P = (x, y)$ con $y \neq 0$ tenemos que

$$x(2P) = \frac{(x^2 - 3)^2}{4y^2}.$$

De modo que $x(P_1) = 1/4$, $x(P_2) = 1/4$ y $x(P_3)$ tampoco puede ser entero porque el numerador $12^2 - 3$ es impar, así que por el Teorema de Nagell-Lutz estos puntos no pueden tener orden finito, luego T consiste únicamente de los puntos $\mathcal{O}$ y $T = (0, 0)$ asi que

$$E(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}_2.$$

EJEMPLO 4.4. La curva elíptica $E : Y^2 = X^3 + 5X$.

Aquí $a = 0$ y $b = 5$ así que los posibles valores de d son $d = \pm 1, \pm 5$. Además tenemos que $\alpha(\mathcal{O}) = 1$ y $\alpha(T) = 5$, como

$$Eq(-1) : N^2 = -M^4 - 5e^4$$

no posee solución con $M \neq 0$ (pues N^2 es no negativo) entonces $d = -1$ no pertence a $\alpha(\Gamma)$, como $\#\alpha(\Gamma)$ es potencia de 2, no puede ser 3 así que

$$\alpha(\Gamma) = \{1, 5\} \pmod{\mathbb{Q}^{*2}}.$$

Su curva asociada $\overline{E} : Y^2 = X^3 - 20X$ así que $\overline{a} = 0$ y $\overline{b} = -20$, los posibles valores de d son los divisores de 20 que son $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10$ y ± 20, pero como $1 \equiv 4$ y $5 \equiv 20$ módulo cuadrados racionales entonces

$$\overline{\alpha}(\overline{\Gamma}) \subset \{\pm 1, \pm 2, \pm 5, \pm 10\}$$

Tenemos que $\overline{\alpha}(\overline{\mathcal{O}}) = 1$ y $\overline{\alpha}(\overline{T}) = -20 \equiv -5 \pmod{\mathbb{Q}^{*2}}$ son elementos de $\alpha(\Gamma)$. Para los restantes d consideramos sus ecuaciones asociadas:

$$\begin{array}{lcll} Eq(-1) & : & N^2 = -M^4 + 20e^4 & (1) \\ Eq(2) & : & N^2 = 2M^4 - 10e^4 & (2) \\ Eq(-2) & : & N^2 = -2M^4 + 10e^4 & (3) \\ Eq(5) & : & N^2 = 5M^4 - 4e^4 & (4) \\ Eq(10) & : & N^2 = 10M^4 - 2e^4 & (5) \\ Eq(-10) & : & N^2 = -10M^4 + 2e^4 & (6) \end{array}$$

La ecuación (1) tiene la solución admisible $(M, e, N) = (2, 1, 2)$ por lo que tenemos hasta ahora que $\#\alpha(\Gamma) \geq 3$, pero como es potencia de 2 ha de ser 4 ó 8. Para ver que no es 8 alcanza con ver que alguna de las ecuaciones de arriba no posee solución admisible.

Observemos que el único divisor de -20 que es congruente con 2 módulo cuadrados racionales es el mismo, así que si $Eq(2)$ posee solución admisible esta ha de ser primitiva, en particular $\text{mcd}(M, 10) = 1$ y entonces M no puede ser múltiplo de 5, por Fermat $M^4 \equiv 1 \pmod 5$ así que $N^2 \equiv 2M^4 \equiv 2 \pmod 5$ lo cual es absurdo porque 2 no es un cuadrado en $\mathbb{Z}_5$. Por lo tanto

$$2^r = \frac{\#\alpha(\Gamma) \cdot \#\overline{\alpha}(\overline{\Gamma})}{4} = \frac{2 \cdot 4}{4} = 2,$$

así que el rango $r = 1$.

Ahora para hallar la parte de torsión $\mathcal{T}$, aplicamos el Teorema de Nagell-Lutz, los puntos de orden 2 son $P = (x, 0)$ con $x^3 + 5x = x(x^2 + 5) = 0$ así que $x = 0$ y el único punto de orden 2 es T.

Si $P = (x, y)$ es un punto de orden mayor que 2 entonces $y | D = -4 \cdot 5^3$, observemos que $x^3 + 5x = y^2 > 0$ implica que x es positivo, además $x(x^2 + 5) = y^2$ por lo tanto $x | y^2$ entonces $x | D^2 = 2^4 \cdot 5^6$, tenemos que además x debe verificar la desigualdad $y^2 = x^3 + 5x > x^3$ luego $x < y^{2/3} \leq D^{2/3} = 2^{4/3} \cdot 5^2 \approx 62{,}9$ y como es entero $x \leq 62$, para chequear menos casos aún, si P es de orden finito, $2P$ también lo será y por lo tanto, por Nagell-Lutz debe tener coordenadas enteras.

Aplicando la fórmula de duplicación tenemos que

$$x(2P) = \left(\frac{3x^2 + 5}{2y}\right)^2 - 2x,$$

que para que sea entero, x debe ser impar. Los únicos x que verifican todas las condiciones son $x = 1, 5$ ó 25, pero para esos valores $x(x^2+5)$ no es cuadrado, así que los únicos puntos de torsión son $\mathcal{O}$ y T así que

$$E(\mathbb{Q}) \simeq \mathbb{Z} \oplus \mathbb{Z}_2.$$

2.3. La Conjetura de Birch y Swinnerton-Dyer. Excepto para casos muy particulares como los que acabamos de ver, para una curva elíptica genérica es un problema muy dificil hayar su rango. De hecho es aún un problema abierto si el rango de una curva elíptica puede ser arbitrariamente grande, es muy dificil encontrar curvas con rango grande.

Una de las conjeturas más importantes sobre el rango de una curva elíptica es la denominada conjetura de Birch-Swinnerton-Dyer que vincula el rango de una curva elíptica el grado de anulación de cierta L-serie asociada a la curva. A continuación se dará una idea de la construcción.

Dada la ecuación de la cúbica $E : Y^2 = X^3 + aX^2 + bX + c$ con a, b y c enteros tales que $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$, lo cual implica que el polinomio $f(X) = X^3 + aX^2 + bX + c$ no posee raíces dobles (complejas) lo cual a su vez implica la no singularidad de la curva.

Como los coeficientes son enteros, tiene sentido considerar la curva en $\mathbb{Z}_p$ (cambiando los coeficientes enteros por sus representantes módulo p), la condición de no singularidad es ahora que $\Delta \equiv 0 \pmod{p}$. Para aquellos primos tales que p no divide a Δ, obtenemos una curva elíptica en $\mathbb{Z}_p$.

Llamando $a_p = p + 1 - \#E(\mathbb{Z}_p)$, construimos la L-serie (incompleta)

$$L(E, s) = \prod_{p \nmid \Delta} (1 - a_p p^s + p^{1-2s})^{-1},$$

que converge para $Re(s) > 3/2$.

Probar esta convergencia no es inmediato, se necesita saber como crece $\#E(\mathbb{Z}_p)$, un resultado de Hasse prueba que

$$|\#E(\mathbb{Z}_p) - (p + 1)| \leq 2\sqrt{p}.$$

Otra propiedad de esta L-serie mucho más dificil de probar es que poseen prolongación analítica a todo $\mathbb{C}$ (Teorema de Wiles).

La idea para probar dicha prolongación analítica se basa en una correspondencia que a cada curva elíptica le hace corresponder una forma modular cuspidal de nivel N y peso 2 con la misma L-serie asociada, veamos que quiere decir un poco esto.

Consideramos en el grupo modular Γ que es el grupo de matrices 2×2 a coeficientes enteros y determinante 1 que actua en $\mathbb{H}$ por transformaciones de Mobius (ver cap 2.2), el subgrupo $\Gamma_0(N)$ llamado el subgrupo principal de congruencia de nivel N.

Una función holomorfa del semiplano superior f que verifique

$$f(A\tau) = (c\tau + d)^2 f(\tau), \qquad \text{para toda } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

y tal que sea holomorfa en el infinito (en el sentido que vimos en el capítulo 2, es decir que $\widehat{f}$ sea holomorfa en $q = 0$) se le llama forma modular holomorfa de peso 2 y nivel N.

Si además $f(\infty) = 0$ (es decir, si $\widehat{f}(0) = 0$) entonces decimos que f es una forma cuspidal, al conjunto de formas modulares cuspidales de peso 2 y nivel N denotaremos por $S_2(N)$.

Dado que $T(\tau) = \tau + 1$ es un elemento de $\Gamma_0(N)$, las funciones de $S_2(N)$ tienen un desarrollo de Fourier. Que se anule en ∞ quiere decir que su desarrollo de Fourier es de la forma

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \qquad \text{donde } q = e^{2\pi i \tau}.$$

A esta forma modular se le asocia la L-serie

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Estas L-series verifican una ecuación funcional de la forma

$$L^*(f, s) = \varepsilon L^*(f, 2 - s) \quad \text{con } \varepsilon = \pm 1 \qquad \text{donde } L^*(f, s) = (2\pi)^s N_f^{s/2} \Gamma(s) L(E, s),$$

donde N_f es una constante que depende de f y Γ es la función Gamma de Euler.

Através de esta ecuación funcional se prueba que las L-series asociadas a elementos de $S_2(N)$ poseen prolongación analítica con cierta simetria respecto al punto $s = 1$.

Por otro lado tenemos la correspondencia que enunciaremos a continuación.

TEOREMA 4.24 (Eichler-Shimura-Taniyama-Wiles). *Existe una correspondencia biunivoca que preserva L-series entre curvas elíptica módulo clase de isogenias y formas modulares cuspidales de peso 2 y nivel N.*

Una isogenia es un morfismo que preserva el $\mathcal{O}$ y dos curvas son equivalentes módulo isogenias si existe una isogenia que lleva una en la otra.

Como corolario del Teorema de Wiles tenemos que las L-series asociadas a curvas elíptica poseen prolongación analítica a todo el plano complejo y ecuación funcional con centro de simetría en $s = 1$. La conjetura de Birch y Swinnerton-Dyer establece una relación entre el orden de anulación de la L-serie en el punto $s = 1$ con el rango de la curva.

CONJETURA DE BIRCH Y SWINNERTON-DYER. El rango de una curva elíptica racional coincide con el orden de anulación de su L-serie asociada en $s = 1$.

En particular esta conjetura implica que $E(\mathbb{Q})$ es finito si y solo si $L(E, s) \neq 0$. Existen versiones más refinadas de la conjetura que relaciona al primer coeficiente no nulo en el desarrollo de Taylor en $s = 1$ con objetos asociados a la curva (ver por ejemplo [**2**]).

2.4. Curvas con Rango grandes. Como acabamos de ver no se conocen los posibles valores del rango que puede tomar una curva elíptica racional, veremos algunas curvas elípticas con el rango más alto conocido hasta el momento.

EJEMPLO 4.5. Un ejemplo de curva elíptica racional con mayor rango conocido hasta ahora es debida a Elkies en el ao 2006, si bien no se conoce el valor de su rango exactamente

se sabe que tiene rango por lo menos 28 (ver http://web.math.hr/ duje/tors/rk28.html). Su ecuación es

$$y^2 + xy + y = x^3 - x^2 - a_4x + a_6,$$

donde

$$a_4 = 20067762415575526585033208209338542750930230312178956502$$

y

$$a_6 = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$$

También se trata de hallar las curvas con mayor rango posible con parte de torsión dada. El ejemplo dado por Elkies tiene parte de torsión trivial y es la de mayor rango conocida hasta ahora. Una lista con curvas de mayor rango conocido dada la parte de torsión puede encontrarse en la página de la Universidad de Zagreb, Croacia (ver `http://web.math.hr/~duje/tors/tors.html`).

Algunos ejemplos son:

EJEMPLO 4.6. Con parte de torsión $\mathcal{T} \simeq \mathbb{Z}_2$ un ejemplo de mayor rango conocido con esa parte de torsión ($r \geq 18$) se debe al mismo Elkies (2006), su fórmula viene dada por

$$y^2 + xy = x^3 - 2617596009270588409631170178770120390355643896951 5x$$
$$+5106938147613148648974217710037377208977910325389056784832677511909488504 1.$$

EJEMPLO 4.7. Con parte de torsión $\mathcal{T} \simeq \mathbb{Z}_3$ un ejemplo de mayor rango conocido con esa parte de torsión ($r \geq 12$) se debe Eroshkin (2006), su fórmula viene dada por

$$y^2 = x^3 + x^2 - 2983377654209740279254049741990741532 25X$$
$$+2209525297419800283762159062541471723368027978017989315000.$$

EJEMPLO 4.8. Con parte de torsión $\mathcal{T} \simeq \mathbb{Z}_4$ un ejemplo de mayor rango conocido con esa parte de torsión ($r \geq 12$) se debe Elkies (2006), su fórmula viene dada por

$$y^2 + xy = x^3 - 1086750289534747727483801311783198679020964x$$
$$+4359731657153238983117057508099695528139965116613369767277319 84.$$

EJEMPLO 4.9. Con parte de torsión $\mathcal{T} \simeq \mathbb{Z}_5$ un ejemplo de mayor rango conocido con esa parte de torsión ($r \geq 6$) se debe Dujella - Lecacheux (2001), su fórmula viene dada por

$$y^2 + y = x^3 + x^2 - 1712371016075117860x + 8857879575356913895129401 64.$$

Bibliografía

[1] Joseph H. Silverman y John Tate. *Rational Points on Elliptic Curves.* Springer - Verlag.
[2] Noemi M. Lalin. *Introducción a las Curvas Elípticas.* Tesis de Grado. UBA.
[3] Carlos Ivorra Catillos. *Curvas elípticas.* Ver en http://www.uv.es/ ivorra/Libros/Libros.htm
[4] Tom M. Apostol *Modular Functions and Dirichlet Series in Number Theory.* Springer - Verlag.
[5] Frances Kirwan *Complex Algebraic Curves.* London Matematical Society - Student text 23
[6] Jean-Pierre Serre *A Course in Arithmetic.* Springer - Verlag.
[7] Neal Koblitz *Introduction to Elliptic Curves and Modular Forms.* Springer - Verlag.
[8] William Fulton *Curvas Algebraicas - Introducción a la Geometría Algebraica.* Editorial Reverté S.A.