UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS

SECCIÓN DE POSGRADO Y SEGUNDA ESPECIALIZACIÓN PROFESIONAL

Tesis para Optar el Grado Académico de Maestro en Ciencias con Mención en Matemática Aplicada

TÍTULO

CONSTRUCIÓN DE CURVAS ELÍPTICAS DE RANGO ALTO Y GRUPO DE TORSIÓN PRESCRITO SOBRE LOS RACIONALES

POR

MANUEL TEODOSIO TORIBIO CANGANA

ASESOR

DR. OSWALDO JOSÉ VELÁSQUEZ CASTAÑÓN

LIMA- PERU

2012

Dedicatoria

Dedico este trabajo a la memoria de mis padres:
Santos Juan
y Fabiana.

Abstract

The objective of this work is the study of the fine group structure of the objects known as elliptic curves. An elliptic curve is given by a cubic equation in a non-singular Weierstrass form. In this case, the set of rational points, meaning the points $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ that satisfy the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

plus a point that we denote by $\mathcal{O}$, and that comes from the original projective form of the curve, constitute an abelian group with an operation defined from intersection of curves, via Bezout's theorem on the projective plane. We prove that this set is finitely generated, result known as Mordell-Weil's theorem. More precisely, $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ is the *subgroup of torsion* (the points of finite order) and $\mathbb{Z}^r$ is the *free part*. To determine the torsion subgroup we use the Lutz-Nagell's theorem, which provides an algorithm to determine the points with finite order; this added to a Mazur's theorem, which classifies the groups that can be obtained, imply that the calculation of the torsion subgroup of a given curve is always feasible. On the other hand, the number r in Mordell's theorem is called the *rank* of the elliptic curve. The rank of a randomly chosen elliptic curve over $\mathbb{Q}$ is small, and it's not easy to generate elliptic curves over $\mathbb{Q}$ with moderately high rank. However, it is conjectured that there exist elliptic curves over $\mathbb{Q}$ with arbitrarily high rank. For calculations we use Néron-Tate's bilinear form, which allows to determine if a finite number of points on the curve are $\mathbb{Z}$-independent, and the Birch Swinnerton-Dyer's conjecture, which tells us that the Hasse-Weil function L of an elliptic curve is holomorfic in $s = 1$ and the order of the zeros at $s = 1$ is equal to the rank of the elliptic curve. This gives us an estimate of the rank which we can always verify.

In the present work, we review the surrounding theory and, with the help of the calculation system PARI/GP, we review the records of high rank elliptic curves achieved until today.

Resumen

El objetivo de este trabajo es el estudio de la estructura fina de grupo de los objetos conocidos como *curvas elípticas*. Una curva elíptica proviene de una ecuación cúbica en la forma de Weierstrass no singular. En este caso, el conjunto de puntos racionales, esto es los puntos $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ que satisfacen la ecuación

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

mas un punto que denotamos $\mathcal{O}$, y que proviene de la forma proyectiva original de la curva, constituyen un grupo abeliano con una operación de intersección de curvas, vía el teorema de Bézout en el plano proyectivo. Demostramos que este conjunto es finitamente generado, resultado conocido como el teorema de Mordell-Weil. Más precisamente $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ donde $E(\mathbb{Q})_{\text{tors}}$ es el *subgrupo de torsión* (los puntos de orden finito) y $\mathbb{Z}^r$ es la *parte libre*. Para determinar el subgrupo de torsión se utiliza el teorema de Lutz-Nagell, que proporciona un algoritmo para descartar los puntos de orden finito; esto sumado a un teorema de Mazur, que clasifica los grupos que se pueden obtener implican que el cálculo del subgrupo de torsión de una curva dada es siempre factible. Por otro lado, el número r en el teorema de Mordell se llama el *rango* de la curva elíptica. El rango de una curva elíptica sobre $\mathbb{Q}$ elegida al azar casi siempre es pequeño, y no es sencillo generar curvas elípticas sobre $\mathbb{Q}$ de rango moderadamente alto. Sin embargo, se conjetura que existen curvas elípticas sobre los racionales de rango arbitrariamente grande. Para los cálculos, usamos la forma bilineal de Néron-Tate, que permite determinar si una cantidad finita de puntos de la curva son $\mathbb{Z}$-independientes, y la conjetura de Birch Swinnerton-Dyer, que nos dice que la función L de Hasse-Weil de una curva elíptica es holomorfa en $s = 1$ y el orden de anulación en $s = 1$ es igual al rango de la curva elíptica. Esto nos da una estimación del rango que siempre logramos verificar.

En el presente trabajo, revisamos la teoría circundante y, con ayuda del sistema de cálculo PARI/GP, revisamos los records de curvas elípticas de rango alto logrados hasta hoy.

Contenido

Introducción **1**

1 Teoría básica **6**

1.1 El plano proyectivo 6

1.2 Curvas elípticas 8

1.3 Ley de grupo en una curva elíptica 14

1.4 Subgrupo de torsión 20

2 Curvas elípticas sobre los racionales **23**

2.1 El método del descenso 24

2.2 El teorema débil de Mordell 26

2.3 Alturas y el teorema Mordell-Weil 36

2.4 El teorema de Mordell-Weil-Néron 41

2.5 Los teoremas de Mazur y Lutz-Nagell 42

3 El rango del grupo de Mordell **49**

3.1 Forma bilineal de Néron-Tate 49

3.2 Aplicando PARI/GP 52

3.3 Reducción de curvas elípticas 55

3.4 Una cota superior para el rango 56

4 Curvas elípticas de rango alto **59**

4.1 La función zeta de Riemann 59

4.2 La función zeta de una curva elíptica sobre cuerpos finitos 64

4.3 La función L de Hasse-Weil de una curva elíptica 66

4.4 Rango analítico. Conjeturas 67

4.5 Trabajando sobre el anillo $\mathbb{Q}[t]$ 69

4.6 Modelo cuártico de una curva elíptica 71
4.7 Una curva de rango ≥ 14 73
4.8 Una curva de rango ≥ 21 74
4.9 El récord 76

Conclusiones **80**

Bibliografía **81**

Introducción

Un entero positivo n se dice que es *congruente* cuando es igual al área de un triángulo rectángulo de lados racionales. Por ejemplo, el triángulo rectángulo de lados 3,4 y 5 genera el número congruente 6. El número congruente más pequeño es el 5, que es el área del triángulo rectángulo de lados 3/2, 20/3 y 41/6. Otros ejemplos de números congruentes son:

n	lados del triángulo
7	24/5, 35/12, 337/60
13	780/323, 323/30, 106921/9690
14	8/3, 63/6, 65/6
15	15/2, 4, 17/2
20	3, 40/3, 41/3
21	7/2, 12, 25/2
22	33/35, 140/3, 4901/105
23	80155/20748, 41496/3485, 905141617/72306780

Si n es congruente, entonces al multiplicar a n por el cuadrado de otro número entero sigue siendo congruente. Por ejemplo, desde que el 5 es congruente, se deduce que $20 = 4 \times 5$ es congruente (en este caso los lados del triángulo se duplican y el área se cuadruplica). Por lo tanto, la búsqueda de los números congruentes se centra en aquellos números n que son libres de cuadrados.

Mientras tener un triángulo rectángulo de lados racionales nos asegura que su área, de ser entera es congruente, verificar que un número no es congruente implica probar que ningún triángulo rectángulo dado tiene área igual al número; es más, aún sabiendo que un número es congruente, la tabla anterior nos da indicios de que no hay una forma sencilla de determinar el triángulo rectángulo correspondiente. Planteamos entonces la siguiente interrogante: *¿Cómo caracterizamos de manera*

sencilla los números congruentes? Se demostrará al final del capítulo 2 que n es congruente si y solo si, existe una solución no trivial en $\mathbb{Q} \times \mathbb{Q}$ de la ecuación

$$y^2 = x^3 - n^2 x. \tag{1}$$

entendiendo por solución trivial a cualquiera de los pares $(-n, 0), (0, 0)$ o $(n, 0)$.

La ecuación (1) es un ejemplo de lo que llamaremos una curva elíptica. Veremos como extraer información de esta ecuación, por ejemplo para decidir si un número es, o no congruente. Ya en 1982 Jerrold Tunnell, de la Universidad de Rutgers (USA), logró un progreso significativo usando esta conexión (números congruentes y curvas elípticas). Tunnell encontró una fórmula para determinar si un número es congruente o no, sin embargo la validez de su fórmula depende de la verdad de un caso particular de uno de los grandes problemas "abiertos" en matemática, conocido como la *conjetura de Birch y Swinnerton-Dyer*. Hasta nuestros días, esta conjetura aún no han sido demostrada; el estímulo para trabajar en ella se ha incrementado cuando en mayo del 2000 la fundación Clay de Matemática, ofrece a la primera persona que desarrolle una demostración correcta un premio de un millon de dólares.

El estudio de las curvas elípticas es actualmente un área activa de investigación, que se ha desarrollado vertiginosamente en las últimas tres décadas, por ejemplo en las aplicaciones a la criptografía, las técnicas de factorización, y los test de primalidad con curvas elípticas. Sin duda, el trabajo de Taniyama sobre el *último teorema de Fermat* puso en oídos de muchos por primera vez las curvas elípticas. La historia de este teorema comenzó con Diofanto, y precisamente fue leyendo una traducción al latín del libro *Arithmetica* de Diofanto, cuando Pierre de Fermat (1601-1665) enunció el teorema que a tantos matemáticos ha tenido atareados en los últimos años. El enunciado del teorema dice que la ecuación

$$x^n + y^n = z^n$$

no tiene soluciones enteras no triviales para $n > 2$.
Más de 300 años ha llevado demostrar este teorema, sobre el que Fermat, sobre el margen del libro de Diofanto, afirma que tenía una demostración, pero se exime de darla argumentando que el márgen de este libro es demasiado estrecho como para escribirla. Fue recién en 1994 cuando el inglés Andrew John Wiles obtuvo la

demostración. Wiles atacó el enigma de Fermat resolviendo un problema totalmente diferente, relacionádolo precisamente con las formas modulares y las curvas elípticas.

Dado un cuerpo K de característica distinta de 2, una curva elíptica E sobre K puede verse como el conjunto de soluciones sobre la clausura algebraica $\overline{K}$, de una ecuación de la forma

$$y^2 = x^3 + ax^2 + bx + c$$

donde $a, b, c \in K$ y $f(x) = x^3 + ax^2 + bx + c$ no tiene raíces múltiples. Al conjunto $E(\overline{K})$ de sus soluciones se le puede dar estructura de grupo abeliano tomando como elemento neutro al punto proyectivo $\mathcal{O} = (0 : 1 : 0)$. Si se considera el conjunto $E(K)$ de las soluciones en K, se tiene que este es un subgrupo de $E(\overline{K})$. Si E es una curva elíptica sobre $\mathbb{Q}$, por el teorema de Mordell de 1922 se sabe que $E(\mathbb{Q})$ es un grupo abeliano finitamente generado y por el teorema de estructura para este tipo de grupos, podemos escribir

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

donde $E(\mathbb{Q})_{\text{tors}}$ es el subgrupo de torsión y r es el rango de $E(\mathbb{Q})$ respectivamente. Por el teorema de Mazur sabemos que el subgrupo de torsión $E(\mathbb{Q})_{tors}$ de $E(\mathbb{Q})$ es isomorfo exactamente a uno de los siguientes quince grupos

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z}, & n = 1, 2, \ldots, 10 \text{ y } 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & n = 1, 2, 3, 4. \end{array}$$

Por otro lado hay muy pocos resultados concernientes al cálculo del rango de una curva elíptica arbitraria, es decir no se sabe cuáles son los valores posibles de r. El rango de una curva elíptica sobre $\mathbb{Q}$ elegida al azar casi siempre es pequeño, y no es sencillo generar curvas elípticas sobre $\mathbb{Q}$ de rango moderadamente alto. Sin embargo, se conjetura que existen curvas elípticas sobre los racionales de rango arbitrariamente grande.

El actual récord lo posee una curva elíptica con rango 28 hallada por Noam Elkies en el año 2006. El rango más alto de una curva elíptica conocido con exactitud (y no sólo su límite inferior) es igual a 19, y fue encontrado por el mismo Elkies en el año 2009. Esto mejora los registros anteriores debido a Kretschmer (rango 10), Schneider-Zimmer (rango 11), Fermigier (rango 14), Dujella (rango 15) y Elkies

Rango $\geq$	Año	Autor(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney - Pomerance
7	1975	Penney - Pomerance
8	1977	Grunewald - Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies

Tabla 1: Fuente `http://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`

(rango 17 y 18)
La tabla 1 muestra algunos datos históricos sobre el rango de las curvas elípticas.

Por otro lado, sea T uno de los quince grupos abelianos finitos, dados por el teorema de Mazur. Si denotamos por $B(T)$ al supremo del conjunto de los rangos de todas las curvas elípticas sobre $\mathbb{Q}$ con grupo de torsión isomorfos a T, esto es

$$B(T) = \sup\big\{\, \mathrm{rang}(E(\mathbb{Q})) \;:\; E \text{ curva elíptica sobre } \mathbb{Q},\ E(\mathbb{Q})_{\mathrm{tors}} \cong T\big\},$$

se conjetura que $B(T)$ no está acotado para ningún T. En la tabla 2 se dan las mejores cotas inferiores encontrados hasta nuestros días para $B(T)$.

El trabajo está dividido en cuatro capítulos. En el primero se da la definición precisa de una curva elíptica mostrando con detalle su estructura algebraica. En el segundo capítulo demostramos el teorema de Mordel-Weil haciendo uso del teorema

T	B(T)	Autor(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008,2009)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella - Lecacheux (2009), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella - Eroshkin (2008), Elkies (2008), Dujella (2008)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella - Kulesz (2001), Elkies (2006), Eroshkin (2009,2011), Dujella - Lecacheux (2009), Dujella - Eroshkin (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	8	Elkies (2005), Eroshkin (2008), Dujella - Eroshkin (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell - Goins (2003), Rathbun (2003,2006), Dujella - Rathbun (2006), Flores - Jones - Rollick - Weigandt - Rathbun (2007), Fisher (2009)

Tabla 2: Fuente `http://web.math.pmf.unizg.hr/~duje/tors/tors.html`

del descenso y del concepto de altura definida en $E(\mathbb{Q})$. Para determinar la parte de torsión de este grupo damos los teoremas de Lutz-Nagell y el teorema de Mazur. En el tercero, esencialmente se define la forma bilineal de Neron-Tate que permite saber si un conjunto finito de puntos de la curva son $\mathbb{Z}$-independientes y se dan cotas superiores para el rango, aunque desde el punto de vista práctico no es muy útil.
En el cuarto capítulo se estudia el rango desde el punto de vista analítico, y utilizando el sistema de cálculo PARI/GP se revisan las curvas elípticas de rango alto obtenidas hasta nuestros días.

Capítulo 1

Teoría básica

1.1 El plano proyectivo

Sea K un cuerpo. El *plano proyectivo* $\mathbb{P}^2(K)$ o simplemente $\mathbb{P}^2$ está dado por clases de equivalencia de tripletes (x, y, z) con $x, y, z \in K$ donde al menos uno de ellos x, y o z es no nulo. Los tripletes (x_1, y_1, z_1) y (x_2, y_2, z_2) son *equivalentes* si existe un elemento no nulo $\lambda \in K$ tal que

$$(x_1, y_1, z_1) = \lambda(x_2, y_2, z_2),$$

en este caso escribimos $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, y la clase de equivalencia de (x, y, z) se denota por $(x : y : z)$, es decir

$$\mathbb{P}^2 := \frac{K^3 \setminus \{(0,0,0)\}}{\sim} = \left\{ (x : y : z) \;\; ; \;\; (x, y, z) \in K^3 \setminus \{(0,0,0)\} \right\}$$

Si $(x : y : z) \in \mathbb{P}^2$ con $z \neq 0$, entonces $(x : y : z) = (x/z : y/z : 1)$ y estos son llamados los puntos *finitos* de $\mathbb{P}^2$, y los puntos de la forma $(x : y : 0)$ son llamados *puntos infinitos* de $\mathbb{P}^2$.

El *plano afín* sobre K es el conjunto de pares ordenados de elementos de K y se denota usualmente por $\mathbb{A}^2(K)$ o simplemente $\mathbb{A}^2$. Tenemos entonces una identificación natural de $\mathbb{A}^2$ con $U = \{(x : y : z) \in P^2 \;/\; z \neq 0 \}$ dada por

$$\begin{array}{rccc} \varphi : & \mathbb{A}^2 & \longrightarrow & U \\ & (x, y) & \longmapsto & (x : y : 1) \end{array}$$

cuya inversa es

$$\begin{array}{rccc} \psi : & U & \longrightarrow & \mathbb{A}^2 \\ & (x : y : z) & \longmapsto & \left(\frac{x}{z}, \frac{y}{z}\right) \end{array}$$

de esta manera, el plano afín se identifica con los puntos finitos de $\mathbb{P}^2$. "Añadir" los puntos infinitos a $\mathbb{A}^2$ para obtener $\mathbb{P}^2$, se puede ver como una manera de compactificar el plano afín.

Un polinomio $F(x, y, z) \in K[x, y, z]$ es *homogéneo* de grado $d > 0$ si sus términos son de la forma $ax^i y^j z^k$ donde $a \in K$ e $i+j+k = d$. En este caso, para todo $\lambda \in K$

$$F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x, y, z).$$

Si $F(x, y, z)$ es un polinomio homogéneo de algún grado positivo y si $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, entonces $F(x_1, y_1, z_1) = 0$ si y sólo si $F(x_2, y_2, z_2) = 0$. Por lo tanto, un cero de un polinomio homogéneo $F(x, y, z)$ en $\mathbb{P}^2$ no depende de la elección del representante de la clase de equivalencia, así tenemos la siguiente buena definición.

Definición 1.1.1. Sea $F \in K[x, y, z]$ un polinomio homogéneo de grado positivo d. El punto $(x : y : z)$ de $\mathbb{P}^2$ es un cero de F, si $F(x, y, z) = 0$.

Si $F(x, y, z)$ es un polinomio arbitrario en x, y, z, no podemos hablar de un cero de F en $\mathbb{P}^2$. Por ejemplo, si $F(x, y, z) = x^2 + 2y - 3z$ entonces $F(1, 1, 1) = 0$, pero $F(2, 2, 2) = 2$, a pesar de que $(1 : 1 : 1) = (2 : 2 : 2)$. Para evitar este problema se trabaja sólo con polinomios homogéneos.

Si $f(x, y) \in K[x, y]$, podemos homogenizarlo insertando potencias apropiadas de z. Por ejemplo, si $f(x, y) = -y^2 + x^3 + Ax + B$ obtenemos el polinomio homogéneo $F(x, y, z) = -y^2 z + x^3 + Axz^2 + Bz^3$. En general si $f(x, y) \in K[x, y]$ es de grado n, entonces

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

es un polinomio homogéneo de grado n en $K[x, y, z]$, llamado la *homogenización* de f. Recíprocamente si $F(x, y, z)$ es un polinomio homogéneo en x, y, z sobre K; el polinomio

$$f(x, y) = F(x, y, 1)$$

es llamado la *des-homogenización* de F.

Ahora podemos ver lo que significa que dos rectas paralelas se intersectan en el infinito. En efecto: sean $\mathcal{L}_1 : y = mx + b_1$ y $\mathcal{L}_2 : y = mx + b_2$ dos rectas paralelas no verticales y distintas ($\therefore$ $m \neq 0$ y $b_1 \neq b_2$), entonces estas tienen las formas homogéneas

$$y = mx + b_1 z, \quad y = mx + b_2 z,$$

y cuando resolvemos estas ecuaciones para encontrar la intersección, obtenemos $(b_1 - b_2)z = 0$ con $b_1 \neq b_2$, es decir

$$z = 0 \quad \text{e} \quad y = mx.$$

Como no podemos tener $(x, y, z) = (0, 0, 0)$, debemos tener que $x \neq 0$. Por lo tanto dividiendo por x encontramos que la intersección de estas rectas es el punto infinito

$$(x : mx : 0) = (1 : m : 0).$$

Análogamente, las rectas verticales distintas $x = c_1$ y $x = c_2$ se intersectan en el punto infinito

$$\mathcal{O} = (0 : 1 : 0).$$

1.2 Curvas elípticas

Sea $\overline{K}$ una clausura algebraica fija de un cuerpo K. Una *curva elíptica* sobre K es una curva proyectiva plana $E \subseteq \mathbb{P}^2(\overline{K})$ no singular definida por una ecuación de la forma

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3. \tag{1.1}$$

donde $a_1, a_2, a_3, a_4, a_6 \in K$.
Si afinizamos la curva elíptica E haciendo $z = 1$, obtenemos una curva dada por la ecuación afín

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Si $car(K) \neq 2$, hacemos el cambio

$$\begin{cases} x &= x \\ y &= \frac{1}{2}(Y - a_1x - a_3), \end{cases}$$

y conseguimos describir la curva con la ecuación

$$Y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}, \tag{1.3}$$

donde

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad \text{y} \quad b_6 = a_3^2 + 4a_6.$$

Si además $car(K) \neq 3$, en la ecuación (1.3), hacemos el cambio

$$\begin{cases} x &= X - \frac{1}{12}b_2 \\ Y &= Y, \end{cases}$$

obteniendo la ecuación

$$Y^2 = X^3 - \frac{c_4}{2^4 \cdot 3}X - \frac{c_6}{2^5 \cdot 3^3} \tag{1.4}$$

con

$$c_4 = b_2^2 - 24b_4, \quad \text{y} \quad c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$

Y así tenemos que E está dada por la ecuación

$$y^2 = x^3 + Ax + B \tag{1.5}$$

donde $A = -\frac{c_4}{2^4 \cdot 3}$ y $B = -\frac{c_6}{2^5 \cdot 3^3}$.

La ecuación dada en (1.5) es conocida como la **ecuación de Weierstrass** de la curva elíptica E, mientras (1.2) es llamada *ecuación de Weierstrass generalizada*.

Nota.- De aquí en adelante $car(K) \notin \{2, 3\}$, puesto que nuestro interés en este trabajo es estudiar las curvas elípticas sobre un cuerpo de característica cero.

Por otro lado, supongamos que comenzamos con una ecuación de la forma

$$cy^2 = dx^3 + ax + b$$

con c y d no nulos. Multiplicando ambos lados de la ecuación por c^3d^2 obtenemos

$$(c^2dy)^2 = (cdx)^3 + (ac^2d)(cdx) + (bc^3d^2),$$

y con el cambio de variables

$$Y = c^2dy \quad \text{y} \quad X = cdx$$

obtenemos de nuevo una ecuación en la forma de Weierstrass.

Para ver qué puntos de E pertenecen al infinito, hacemos $z = 0$ en (1.1) y obtenemos que $x^3 = 0$, por lo tanto $x = 0$ e y puede ser cualquier elemento no nulo de K, y dividiendo por y encontramos que $\mathcal{O} = (0 : 1 : 0)$ es el **único** punto del infinito, en E. Así

$$E(K) = \left\{(x : y : z) \in \mathbb{P}^2; \quad y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\right\},$$

o bien

$$E(K) = \left\{(x, y) \in A^2(K); \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\right\} \cup \left\{\mathcal{O}\right\}.$$

Como podemos observar, al afinizar de esta forma sólo perdemos un punto de la curva, el punto $\mathcal{O}$. Es decir todos los puntos pueden encontrarse en esta afinización salvo el punto del infinito $\mathcal{O}$

Y como se vio al final de la sección (1.1) el punto $\mathcal{O} = (0 : 1 : 0)$ pertenece a toda recta vertical. Luego toda recta vertical interseca a la curva elíptica E en este punto del infinito.

En lo que sigue casi siempre trabajaremos con coordenadas afines y tratamos el punto del infinito como un caso especial cuando sea necesario.
Un punto $P = (x_0 : y_0 : z_0) \in E(K)$ es un *punto singular* si

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

donde F es el polinomio homógeneo que define la curva proyectiva $E(K)$, es decir

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3).$$

Si la curva no tiene puntos singulares se dice que es una *curva no singular*, regular o lisa. Por ejemplo, el punto $\mathcal{O}$ es no singular, ya que

$$\frac{\partial F}{\partial z}(\mathcal{O}) = y^2 + a_1xy + 2a_3yz - (a_2x^2 + 2a_4xz + 3a_6z^2)\Big|_{(0,1,0)} = 1 \neq 0$$

La *recta tangente* a la curva proyectiva $E(K)$, en un punto no singular $P \in E(K)$, es la recta de ecuación

$$\frac{\partial F}{\partial x}(P) \cdot x + \frac{\partial F}{\partial y}(P) \cdot y + \frac{\partial F}{\partial z}(P) \cdot z = 0.$$

Por ejemplo, la recta tangente a $E(K)$ en el punto $\mathcal{O}$ es $z = 0$.
Ahora si

$$\begin{aligned} E(K) &= \{(x : y : z) \in \mathbb{P}^2 / y^2z = x^3 + Axz^2 + Bz^3\} \\ &= \{(x, y) \in \mathbb{A}^2 / y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}. \end{aligned}$$

El discriminante y el invariante j de $E(K)$ son respectivamente

$$\triangle = -16(4A^3 + 27B^2) \qquad \text{y} \qquad j = 1728\frac{(4A)^3}{\triangle}. \tag{1.6}$$

Supongamos que

$$f(x) = x^3 + Ax + B = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

con $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$. Se demuestra que el *discriminante* de esta cúbica

$$d = \left[(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)\right]^2$$

es igual a $-(4A^3 + 27B^2)$. Por lo tanto,

$$d = -(4A^3 + 27B^2) \qquad \text{y} \qquad \triangle = 16 \cdot d \tag{1.7}$$

Teorema 1.1. *Sea $\mathcal{C}$ la curva cúbica dada por $y^2 = x^3 + Ax + B$. Entonces, son equivalentes:*

1. *$\mathcal{C}$ es singular;*
2. *$\triangle = 0$;*
3. *$d = 0$;*
4. *f tiene raíces múltiples;*

Por consiguiente, $\mathcal{C}$ es no singular si y solo si $4A^3 + 27B^2 \neq 0$.

Demostración. Es obvio, por la definición del discriminante, que $d = 0$ es equivalente a que $f(x)$ tenga raíces multiples. También es obvio que $\triangle = 0$ si y sólo si $d = 0$, por la relación (1.7). Por lo tanto, sólo nos queda ver que $\mathcal{C}$ es singular si y sólo si $d = 0$. Nuestra curva viene dada por

$$\mathcal{C} : y^2 z = x^3 + Axz^2 + Bz^3.$$

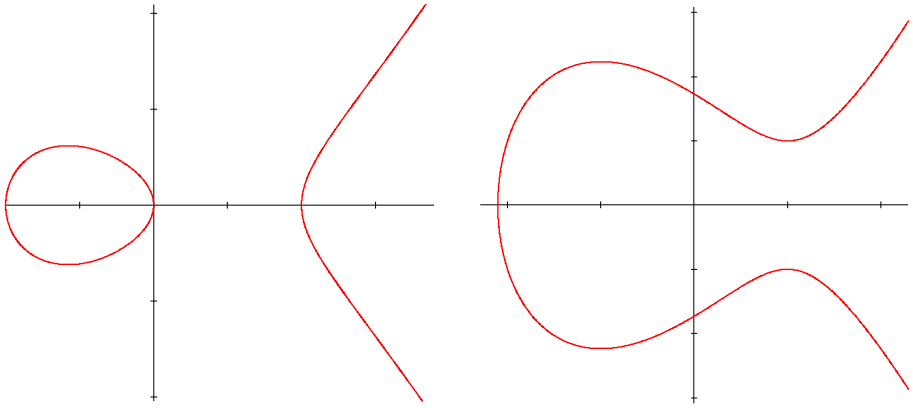
Sabemos que el único punto de intersección de $\mathcal{C}$ con la recta del infinito, $z = 0$, es $\mathcal{O}$ (que es no singular). Por lo tanto, si un punto $P = (x_0 : y_0 : z_0) \in \mathcal{C}$ es singular se tiene que $z_0 \neq 0$. Así que podemos suponer que $z_0 = 1$. Ahora bien, si un punto $P = (x_0 : y_0 : 1) \in \mathcal{C}$ es singular, se ha de tener que

$$\frac{\partial F}{\partial x}(x_0, y_0, 1) = \frac{\partial F}{\partial y}(x_0, y_0, 1) = \frac{\partial F}{\partial z}(x_0, y_0, 1) = 0.$$

donde $F(x, y, z) = y^2 z - (x^3 + Axz^2 + Bz^3)$. Es decir,

$$\begin{cases} -3x_0^2 - A &= 0, \quad (i) \\ 2y_0 &= 0, \quad (ii) \\ y_0^2 - 2Ax_0 - 3B &= 0. \quad (iii) \end{cases}$$

La ecuación (ii) nos dice que $y_0 = 0$. Ahora vamos a distinguir dos casos, cuando $A \neq 0$ y cuando $A = 0$.



(i) $y^2 = x^3 - x$ (ii) $y^2 = x^3 - 3x + 5$

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

1. $A \neq 0$.

   Entonces por (iii) tenemos que $x_0 = -\frac{3B}{2A}$, y sustituyendo esto en (i) obtenemos

   $$\frac{1}{4A^2}(27B^2 + 4A^3) = 0 \text{ si y solo si } d = 0$$

2. $A = 0$.

   Tenemos

   $$\begin{cases} -3x_0^2 = 0 \\ -3B = 0 \end{cases} \quad \text{si y solo si} \quad \begin{cases} x_0 = 0 \\ B = 0, \end{cases}$$

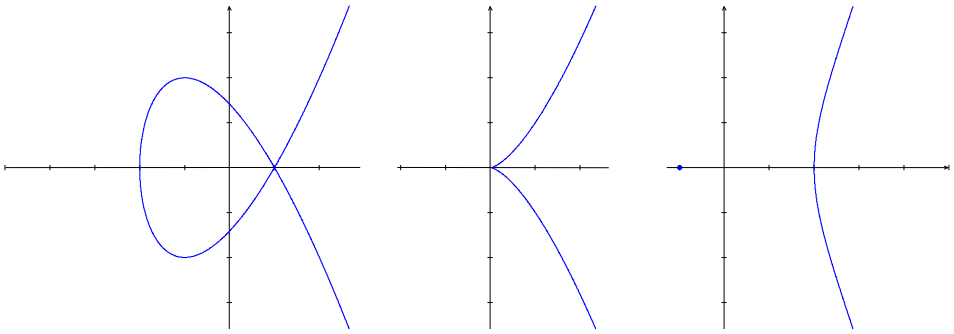
   Con lo que llegamos a que esto ocurre si y solo si $d = 27B^2 = 0$.

□

No es posible hacer dibujos significativos de curvas elípticas sobre un cuerpo arbitrario; sin embargo, sobre $\mathbb{R}$ o sobre $\mathbb{Q}$ si, como lo veremos enseguida. Sea $\triangle$ el discriminante de la curva definida por

$$\mathcal{C} = \{(x, y) \in \mathbb{A}^2 \ / \ y^2 = f(x) = x^3 + Ax + B \ \} \cup \{\mathcal{O}\}$$

1. $\triangle \neq 0$, entonces $\mathcal{C}$ es **no singular**, por lo tanto $\mathcal{C}$ es una curva elíptica. Se tienen los dos casos siguientes:



(i) $y^2 = x^3 - 3x + 2$ (ii) $y^2 = x^3$ (iii) $y^2 = x^3 - 3x - 2$

Figura 1.2: Curvas cúbicas singulares sobre $\mathbb{R}$

(a) $\triangle > 0$, entonces la ecuación $f(x) = 0$ tiene tres raíces reales distintas, y el grafo real afín de la curva tiene dos componentes conexa: una no compacta, que es la componente de la curva cuyo cierre proyectivo contiene a $\mathcal{O}$, y una compacta de forma oval (Figura 1.1, (i)).

(b) $\triangle < 0$, entonces la ecuación $f(x) = 0$ tiene una sola raíz real, y el grafo real afín de la curva tiene una sola componente conexa (Figura 1.1, (ii)).

2. $\triangle = 0$, entonces $\mathcal{C}$ **es singular** . Este caso se divide en tres subcasos. Como el polinomio $f(x)$ tiene al menos una raíz doble, escribimos $f(x) = (x-\alpha)^2(x-\beta)$ y como $f(x) = x^3 + Ax + B$ obtenemos que $2\alpha + \beta = 0$, por lo tanto

$$f(x) = (x - \alpha)^2(x + 2\alpha).$$

(a) $\alpha > 0 \Longrightarrow$ El grafo real afín tiene una única componente conexa, que posee un punto doble en $x = \alpha$. Las tangentes en el punto doble tienen pendientes reales distintas (Figura 1.2, (i)).

(b) $\alpha = 0 \Longrightarrow$ La curva tiene una cúspide en $(0, 0)$, es decir las tangentes en el punto singular $(0, 0)$ son la misma (Figura 1.2, (ii)).

(c) $\alpha < 0 \Longrightarrow$ El grafo real afín tiene dos componentes conexas. una no compacta, y un punto aislado de coordenadas $(\alpha, 0)$. De hecho este punto es de nuevo un punto doble, pero con tangentes distintas de pendientes complejas (Figura 1.2, (iii)).

1.3 Ley de grupo en una curva elíptica

Dada la curva elíptica

$$E(K) = \big\{(x, y) \in A^2(K); \quad y^2 = x^3 + Ax + B\big\} \cup \big\{\mathcal{O}\big\}.$$

Si L es una recta proyectiva. Dado que la ecuaciónproyectiva de $E(K)$ es de grado 3, el teorema de Bezout nos asegura que L interseca a $E(K)$ en exactamente 3 puntos, con multiplicidades, digamos P, Q y R. Es claro que estos tres puntos no son necesariamente distintos, (véase el caso en que L es tangente a $E(K)$). Podemos así definir una ley de grupo "+" sobre E. Empezamos con dos puntos de $E(K)$.

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

en una curva elíptica E, dada por la ecuación $y^2 = x^3 + Ax + B$. Definimos un nuevo punto P_3 como sigue: Dibujamos la recta $\mathcal{L}$ a través de P_1 y P_2, y sabemos que $\mathcal{L}$ interseca a E en un tercer punto P_3', reflejamos P_3' con respecto al eje X y obtenemos P_3; luego definimos

$$P_1 + P_2 = P_3.$$

Asumamos primero que $P_1 \neq P_2$ y que los dos son distintos de $\mathcal{O}$. Dibujamos la recta $\mathcal{L}$ a través de P_1 y P_2. Su pendiente es

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Si $x_1 = x_2$, entonces $\mathcal{L}$ es vertical. Trataremos ese caso más adelante, así que asumamos que $x_1 \neq x_2$. La ecuación de $\mathcal{L}$ es

$$y = m(x - x_1) + y_1.$$

Para encontrar la intersección con E, sustituímos para obtener

$$[m(x - x_1) + y_1]^2 = x^3 + Ax + B.$$

Esto se puede escribir de la forma

$$x^3 - m^2x^2 + ax + b = 0$$

Las tres raíces de esta cúbica corresponden a los tres puntos de intersección de $\mathcal{L}$ con E, pero en el presente caso ya conocemos dos raíces x_1 y x_2, pues P_1 y P_2 son puntos de E y $\mathcal{L}$. Por lo tanto si $P_3' = (x_3', y_3')$, obtenemos

$$x_3' = m^2 - x_1 - x_2$$

y

$$y_3' = m(x_3' - x_1) + y_1.$$

Ahora, reflejamos con respecto al eje x para obtener el punto $P_3 = (x_3, y_3)$ donde

$$x_3 = m^2 - x_1 - x_2 \quad \text{y} \quad y_3 = m(x_1 - x_3) - y_1.$$

En el caso que $x_1 = x_2$ pero $y_1 \neq y_2$, la recta a través de P_1 y P_2 es vertical, y por lo tanto interseca a E en $\mathcal{O}$. Reflejando $\mathcal{O}$ con respecto al eje x obtenemos el mismo punto $\mathcal{O}$ (es por esto que ponemos $\mathcal{O}$ al tope y al fondo del eje y). Por lo tanto, en este caso

$$P_1 + P_2 = \mathcal{O}.$$

Ahora consideremos el caso $P_1 = P_2 = (x_1, y_1)$. Cuando los dos puntos coinciden tomamos la recta $\mathcal{L}$ a través de ellos como la recta tangente, y la diferenciación implícita nos permite encontrar la pendiente m de esta recta

$$m = \frac{3x_1^2 + A}{2y_1} \quad \text{si } y_1 \neq 0$$

(cuando $y_1 = 0$, la recta es vertical y hacemos $P_1 + P_2 = \mathcal{O}$, como antes). Por lo tanto, asumiendo que $y_1 \neq 0$, la ecuación de $\mathcal{L}$ es

$$y = m(x - x_1) + y_1,$$

y como antes obtenemos la ecuación cúbica

$$x^3 - m^2x^2 + \alpha x + \beta = 0.$$

Esta vez, conocemos sólo una raíz x_1, pero es una raíz doble pues $\mathcal{L}$ es tangente a E en P_1. Por lo tanto, procediendo como antes obtenemos que

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

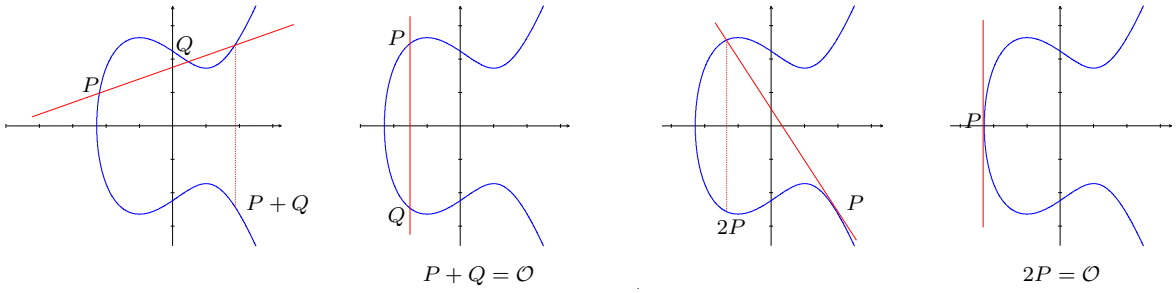


Figura 1.3: La operación de grupo

Finalmente, supongamos que $P_2 = \mathcal{O}$. La recta a través de P_1 e $\mathcal{O}$ es una recta vertical que interseca a E en el punto P_1' que es el reflejo de P_1 con respecto al eje x. Cuando reflejamos P_1' con respecto al eje x, regresamos a P_1. Por lo tanto,

$$P_1 + \mathcal{O} = P_1$$

para todo punto $P_1 \in E$.
Resumimos todo esto, en la siguiente definición.

Definición 1.3.1 (**Suma de puntos en una curva elíptica)**. Sea E la curva elíptica $y^2 = x^3 + Ax + B$ sobre un cuerpo K. Sean $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ puntos en E con $P_1 \neq \mathcal{O}$ y $P_2 \neq \mathcal{O}$. Definimos $P_1 + P_2 = P_3 = (x_3, y_3)$ como sigue:

i) Si $x_1 \neq x_2$, entonces

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{donde} \quad m = \frac{y_2 - y_1}{x_2 - x_1}.$$

ii) Si $x_1 = x_2$ pero $y_1 \neq y_2$, entonces $P_1 + P_2 = \mathcal{O}$.

iii) Si $P_1 = P_2$ y $y_1 \neq 0$, entonces

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{donde} \quad m = \frac{3x_1^2 + A}{2y_1}.$$

iv) Si $P_1 = P_2$ y $y_1 = 0$, entonces $P_1 + P_2 = \mathcal{O}$.

Además, definimos

$$P + \mathcal{O} = P \quad \text{para todo } P \text{ en } E.$$

Cuando P_1 y P_2 tienen coordenadas en un cuerpo L extensión de K, entonces $P_1 + P_2$ también tiene coordenadas en L. Por lo tanto $E(L)$ es cerrado bajo la suma de puntos que acabamos de definir. Ahora mostraremos que esta operación tiene buenas propiedades.

Teorema 1.2. *La suma de puntos en una curva elíptica E, satisface las siguientes propiedades:*

1. *Conmutativa*
   $P_1 + P_2 = P_2 + P_1 \quad$ *para todo* $P_1, P_2 \in E$.

2. *Existencia del elemento neutro*
   $P + \mathcal{O} = P \quad$ *para todo* $P \in E$.

3. *Existencia de inverso de un punto*
   Dado $P \in E$, *existe* $P' \in E$ *tal que* $P + P' = \mathcal{O}$.

4. *Asociativa*
   $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3) \quad$ *para todo* $P_1, P_2, P_3 \in E$.

En otras palabras, los puntos de E forman un grupo abeliano aditivo con $\mathcal{O}$ como elemento neutro.

Demostración. La conmutatividad es obvia, del hecho de que la recta a través de P_1 y P_2 es la misma que la recta a través de P_2 y P_1. La propiedad de existencia del elemento neutro $\mathcal{O}$, se cumple por definición o considerando que la recta que une P con $\mathcal{O}$ es vertical. Por otro lado si P esta en E y P' es el reflejo de P con respecto al eje x, entonces $P + P' = \mathcal{O}$, puesto que la recta que une P con P' es vertical y ella contiene al punto del infinito $\mathcal{O}$. Finalmente, necesitamos probar la asociatividad. Esta es de lejos la propiedad más sutil y menos obvia de la suma de puntos de E, los detalles de la prueba pueden verse [Kna92]. □

Algunas fórmulas explícitas viene dados por:

- **Fórmula para el inverso:** Si $P = (x, y) \in E(K)$, entonces:
  Para la ecuación de Weierstrass generalizada

$$-P = (x, -y - a_1 x - a_3).$$

  Para la ecuación de Weierstrass(reducida)

$$-P = (x, -y).$$

- **Fórmula de duplicación:** Si $P = (x, y) \in E(K)$, entonces:

  Para la ecuación de Weierstrass generalizada

$$2P == \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

  Para la ecuación de Weierstrass(reducida)

$$2P = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

- **Fórmula de la suma:** $P_1 + P_2$ cuando $P_1 \neq \pm P_2$

  Si $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$, entonces:

  Para la ecuación de Weierstrass generalizada

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - (x_1 + x_2)$$

  Para la ecuación de Weierstrass(reducida)

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2)$$

Veamos algunos

Ejemplos:

1. En la curva $y^2 = x^3 - 25x$, tenemos

$$2(-4, 6) = (-4, 6) + (-4, 6) = \left(\frac{1681}{144}, -\frac{62279}{1728}\right),$$

$$(-4, 6) + (-5, 0) = (45, -300),$$

$$(0, 0) + (-5, 0) = (5, 0),$$

$$2(5, 0) = \mathcal{O}.$$

2. En la curva $E: \ y^2 = x^3 - 5x + 8, \quad P = (1, 2) \in E.$

$$2P = \left(-\frac{7}{4}, -\frac{27}{8}\right)$$

$$3P = P + 2P = \left(\frac{553}{121}, -\frac{11950}{1331}\right).$$

   También tenemos que

$$4P = 2P + 2P = \left(\frac{45313}{11664}, \frac{8655103}{1259712}\right)$$

3. En la curva $E: \ y^2 = x^3 - 36x, \quad P = \left(\frac{25}{4}, \frac{35}{8}\right) \in E.$

$$2P = \left(\frac{1442401}{19600}, -\frac{1726556399}{2744000}\right)$$

$$4P = \left(\frac{4386303618090112563849601}{2337101647159432205584 00}, -\frac{87043691090855808282759356506262544 01}{1129838585124636197372166844964480 00}\right)$$

Si P es un punto de una curva elíptica E, y k es un entero positivo, entonces kP denota $P + P + \cdots + P$ (con k sumandos). Si $k < 0$, entonces $kP = (-P) + (-P) + \cdots + (-P)$, con $|k|$ sumandos. Para calcular kP cuando k es un entero muy grande, es ineficiente sumar P a sí mismo sucesivamente. Es mucho más rápido y eficiente usar el método de las *duplicaciones sucesivas*. Por ejemplo, para calcular $19P$, calculamos

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P \quad \text{y} \quad 16P = 8P + 8P$$

luego

$$19P = 16P + 2P + P.$$

Este método nos permite calcular kP para k grande, rápidamente. La dificultad es que el tamaño de las coordenadas de los puntos se incrementan velozmente (como puede verse en el último ejemplo) si trabajamos por ejemplo sobre los números racionales. Sin embargo, cuando trabajamos sobre un cuerpo finito, por ejemplo $\mathbb{F}_p$, este no es un problema, porque podemos reducir módulo p continuamente y por tanto los números implicados son relativamente pequeños. La asociatividad nos permite hacer estos cálculos sin preocuparnos del orden de los sumandos. Este método se puede implementar mediante el siguiente algoritmo.

Algoritmo para calcular kP

Sea k un entero positivo y sea P un punto en una curva elíptica E. La siguiente secuencia genera, el punto kP.

1. Iniciamos con: $a = k$, $B = \mathcal{O}$ y $C = P$.
2. Si a es par, sea $a = a/2$, y sean $B = B$, $C = 2C$.
3. Si a es impar, sea $a = a - 1$, y sean $B = B + C$, $C = C$.
4. Si $a \neq 0$, ir al paso 2.

5. Salida B.

El valor en la salida de B, es kP.

Por otro lado, si estamos trabajando sobre un cuerpo finito "grande" K y nos dan los puntos P y kP sobre la curva elíptica $E(K)$, no es fácil determinar el valor de k. Este es el llamado *problema de logaritmo discreto* para curvas elípticas, y es la base para las aplicaciones criptográficas con curvas elípticas.

1.4 Subgrupo de torsión

Los puntos de torsión, es decir, aquellos cuyos órdenes son finitos, juegan un rol importante en el estudio de las curvas elípticas. Si se estudian las curvas elípticas sobre cuerpos finitos, todos sus puntos son puntos de torsión. En el siguiente capítulo usamos los puntos de "2-torsión", en un procedimiento conocido como *descenso*.

Sea E una curva elíptica definida sobre un cuerpo K. Sea n un entero positivo. Estamos interesados en

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

donde $\overline{K}$ es la clausura algebraica de K.
Cuando la característica de K no es 2, E se puede poner en la forma $y^2 =$cúbica, y es fácil determinar $E[2]$. Sea

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

con $e_1, e_2, e_3 \in \overline{K}$. Un punto P satisface $2P = \mathcal{O}$ si y sólo si la recta tangente en P es vertical, y esto ocurre cuando $y = 0$, por tanto

$$E[2] = \big\{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\big\}.$$

y por la teoría de grupos, este es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. De esta forma se tiene la siguiente proposición.

Proposición 1.1. *Sea E una curva elíptica sobre un cuerpo K. Si la característica de K no es 2, entonces*

$$E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Ahora echemos un vistazo a $E[3]$. Asumamos primero que la característica de K no es 2 ni 3, de tal forma que E puede ser dada por la ecuación $y^2 = x^3 + Ax + B$. Un punto $P \neq \mathcal{O}$ satisface $3P = \mathcal{O}$ si y sólo si $2P = -P$. Esto significa que la x-coordenada de $2P$ es igual a la x-coordenada de P (la y-coordenadas de P y de $2P$ difieren por lo tanto en el signo. Si fueran iguales entonces $2P = P$, luego $P = \mathcal{O}$). En decir

$$m^2 - 2x = x, \quad \text{donde} \quad m = \frac{3x^2 + A}{2y}.$$

Usando el hecho de que $y^2 = x^3 + Ax + B$, encontramos que

$$(3x^2 + A)^2 = 12x(x^3 + Ax + B).$$

Simplificando, obtenemos

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0,$$

y como el discriminante de este polinomio es $-6912(4A^3 + 27B^2)^2$ (que no es cero), el polinomio no tiene raíces múltiples, así existen 4 valores distintos de x (en $\overline{K}$), y para cada x obtenemos dos valores de y, y así obtenemos ocho puntos de orden 3. Como $\mathcal{O}$ también está en $E[3]$, vemos que $E[3]$ es un grupo de orden 9 en el cual todo elemento es de 3-torsión. Se sigue que

$$E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Ahora veamos lo que pasa con característica 3. Podemos asumir que E es de la forma $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Nuevamente, queremos que la x-coordenada de $2P$ sea igual a la de P. Calculamos la x-coordenada de $2P$ por el procedimiento usual y la igualamos a la x-coordenada x de P (algunos términos desaparecen, ya que en $\mathbb{Z}/3\mathbb{Z}$ $3 = 0$), obteniendo

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0.$$

Simplificando $(4 = 1)$ tenemos que

$$a_2x^3 + a_2a_6 - a_4^2 = 0.$$

Notemos que no podemos tener $a_2 = a_4 = 0$, pues entonces $x^3 + a_6 = (x + \sqrt[3]{a_6})^3$ tendría raíces múltiples. Luego al menos uno de a_2, a_4 es no nulo.

Si $a_2 = 0$, tenemos $-a_4^2 = 0$, lo que no puede pasar, así que no hay valores de x. Por lo tanto en este caso $E[3] = \{\mathcal{O}\}$.

Si $a_2 \neq 0$ obtenemos una ecuación de la forma $a_2(x^3 + a) = 0$, que tiene una sola raíz triple en característica 3. Por lo tanto, existe un valor de x, y dos correspondientes de y. Así obtenemos 2 puntos de orden 3. Como también tenemos el punto $\mathcal{O}$, vemos que $E[3]$ tiene orden 3, y $E[3] \cong \mathbb{Z}/3\mathbb{Z}$.

El caso general se dada en el siguiente teorema.

Teorema 1.3. *Sea E una curva elíptica sobre un cuerpo K y $n \geq 1$ un entero.*

1. *Si $Car(K) = 0$ o $0 < Car(K) = p \nmid n$, entonces*

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

2. *Si $Car(K) = p > 0$ y $p \mid n$, escribimos $n = p^r n'$ con $p \nmid n'$. Entonces*

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \qquad \vee \quad E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\,'\mathbb{Z}.$$

La prueba de este teorema puede verse en [Was08], pág. 86.

Definición 1.4.1. El subgrupo de torsión de $E(K)$ denotado por $E(K)_{tors}$ es el conjunto de puntos de orden finito de $E(K)$, es decir

$$E_{\text{tors}} = \bigcup_{n=1}^{\infty} E[n].$$

Tal y como ya hemos dicho anteriormente, en este trabajo estamos interesados principalmente en el estudio de curvas elípticas definidas sobre los racionales, de modo que su característica es cero.

En este caso el grupo de torsión de una curva elíptica es infinito, pues hay n^2 puntos de n torsión para toda $n \geq 1$, tal y como ya hemos visto, y dado que la proposición anterior nos proporciona todas las nociones necesarias para entender su estructura, resulta natural preguntarse sobre la estructura de los puntos de torsión K-racionales.

Veremos en el siguiente capítulo, un teorema que nos garantizará que el número de puntos de torsión K-racional es finito, más aún existen teoremas de estructura suficientemente fuertes, e incluso técnicas efectivas para su cálculo.

Capítulo 2

Curvas elípticas sobre los racionales

El objetivo principal de este capítulo es demostrar que.

Si E es una curva elíptica definida sobre $\mathbb{Q}$, entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.

Este resultado es conocido como el teorema de Mordell, y la demostración de este teorema consistirá en aplicar el llamado teorema del descenso que veremos en la primera sección de este capítulo. Dicho teorema nos asegura que si en un grupo abeliano G hay definida una función altura que cumpla determinadas condiciones y si existe un entero $m \geq 2$ de tal forma que el grupo cociente G/mG es finito, entonces G está finitamente generado.
En la siguiente sección, demostraremos el teorema débil de Mordell, que nos asegura que $E(\mathbb{Q})/E(Q)_{\text{tors}}$ es finito. Ya en la sección 3.3 definiremos una función altura en el grupo abeliano $E(\mathbb{Q})$, de tal forma que aplicando el teorema del descenso junto con el teorema débil de Mordell, tendremos demostrado el teorema de Mordell, que aplicando el teorema de estructura para este tipo de grupos, podemos escribir

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

donde $E(\mathbb{Q})_{\text{tors}}$ es el subgrupo de torsión de $E(\mathbb{Q})$ y r es el rango de $E(\mathbb{Q})$.

2.1 El método del descenso

Teorema 2.1 (Método del descenso)**.** *Sea A un grupo abeliano y $h : A \to \mathbb{R}$ una función con las siguientes propiedades:*

(i) Dado $Q \in A$. Existe una constante $C_1 = C_1(Q)$, dependiendo de A y Q, tal que para todo $P \in A$

$$h(P+Q) \leq 2h(P) + C_1$$

(ii) Existe un entero $m \geq 2$ y una constante C_2, que depende sólo de A, tal que para todo $P \in A$

$$h(mP) \geq m^2 h(P) - C_2$$

(iii) Para cada constante C_3,

$$\{P \in A : h(P) \leq C_3\} \text{ es un conjunto es finito.}$$

Si el grupo cociente A/mA es finito, entonces A es finitamente generado.

Demostración. Sea $\{Q_1, Q_2, \cdots Q_r\}$ un conjunto de representantes de las clases de A/mA. Si $P \in A$, existirá $i_1 \in \{1, \cdots r\}$ y existirá $P_1 \in A$ tal que

$$P = mP_1 + Q_{i_1}$$

Continuando el proceso inductivamente, obtenemos

$$\begin{aligned} P_1 &= mP_2 + Q_{i_2}, \\ P_2 &= mP_3 + Q_{i_3}, \\ &\vdots \\ P_{n-1} &= mP_n + Q_{i_n}. \end{aligned}$$

Por lo que podemos escribir

$$P = Q_{i_1} + mP_1 = Q_{i_1} + mQ_{i_2} + m^2 P_2 = \cdots = m^n P_n + \sum_{j=1}^{n} m^{j-1} Q_{i_j}.$$

Es decir,

$$P \in \langle Q_2, \cdots Q_r, P_n \rangle.$$

Si demostramos que existe una constante C independiente del punto P tal que $h(P_n) \leq C$ para un cierto n, habremos acabado, ya que tendremos que A está generado por

$$\{Q_1, Q_2, \cdots Q_r\} \cup \{P \in A \ / \ h(P) \leq C\},$$

y este conjunto es finito por la propiedad (iii) de h. Vamos a buscar entonces dicha constante.

Para cada j, tenemos por (ii) que

$$h(mP_j) \geq m^2 h(P_j) - C_2,$$

así que

$$h(p_j) \leq \frac{1}{m^2}\left[h(mP_j) + C_2\right] = \frac{1}{m^2}\left[h(P_{j-1} - Q_{i_j}) + C_2\right].$$

Y por (i) obtenemos

$$h(p_j) \leq \frac{1}{m^2}\left[2h(P_{j-1}) + C_1' + C_2\right], \tag{2.1}$$

donde $C_1' = \max\limits_{1\leq i\leq r}\{C_1(-Q_i)\}$. Además C_1' y C_2 no dependen de P_j. Ahora asumamos la desigualdad (2.1) sucesivamente, empezando de P_n y llegando hasta P. Así obtenemos:

$$\begin{aligned}
h(P_n) &\leq \frac{1}{m^2}\left[2h(P_{n-1}) + C_1' + C_2\right] \\
&= \frac{1}{m^2}h(P_{n-1}) + \frac{1}{m^2}[C_1' + C_2] \\
&\leq \frac{1}{m^2}\left[\frac{1}{m^2}\left[2h(P_{n-2}) + C_1' + C_2\right]\right] + \frac{1}{m^2}[C_1' + C_2] \\
&= \left(\frac{2}{m^2}\right)^2 h(P_{n-2}) + \left[\frac{1}{m^2} + \frac{1}{m^4}\right][C_1' + C_2] \leq \cdots \\
&\vdots \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \left[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \cdots + \frac{2^{n-1}}{m^{2n}}\right][C_1' + C_2] \\
&\leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{1}{2}[C_1' + C_2]\sum_{i=1}^{n}\left(\frac{2}{m^2}\right)^i
\end{aligned}$$

Y usando que $m \geq 2$ obtenemos

$$h(P_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \frac{C_1' + C_2}{2} \cdot \frac{\frac{2}{m^2}}{1 - \frac{2}{m^2}} \leq 2^{-n}h(P) + \frac{C_1' + C_2}{2}$$

Se sigue que tomando n suficientemente grande, se cumplirá que

$$h(P_n) \leq 1 + \frac{C_1' + C_2}{2},$$

y por tanto todo elemento de A es una combinación lineal (como $\mathbb{Z}$-módulo) de puntos del conjunto

$$\{Q_1, Q_2, \cdots Q_r\} \cup \left\{ Q \in A \ / \ h(Q) \leq 1 + \frac{C_1' + C_2}{2} \right\},$$

que es un conjunto finito por la propiedad (iii). Esto prueba que A esta finitamente generado. □

2.2 El teorema débil de Mordell

Teorema 2.2 (débil de Mordell)**.** *Si E es una curva elíptica definida sobre $\mathbb{Q}$, entonces el grupo abeliano $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.*

Antes de la demostración veremos algunos resultados que nos serán necesarios:

Proposición 2.1. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ por una ecuación de Weierstrass de la forma*

$$y^2 = f(x) = x^3 + ax^2 + bx + c = (x - \alpha)(x - \beta)(x - \gamma).$$

donde K es el cuerpo de descomposición de $f(x)$. Si

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\phi} E(K)/2E(K)$$

es el homomorfismo canónico, entonces,

$$|ker\phi| \leq 2^{2[K:\mathbb{Q}]}.$$

Demostración. : Si $P = (x, y)$ es un elemento de $E(K)$ y $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, entonces

$$P^\sigma = (\sigma(x), \sigma(y)) \in E(K).$$

Además σ actúa sobre $E(K)$ como un homomorfismo de grupos, esto es,

$$(P \oplus Q)^\sigma = P^\sigma \oplus Q^\sigma,$$

ya que E está definida sobre $\mathbb{Q}$.

Definiremos ahora

$$E[2] = \{Q \in E(K) : [2]Q = \mathcal{O}\}$$

Para cada $P \in \ker \phi$, elegimos $Q_P \in E(K)$ de manera que $[2]Q_P = P$. Entonces obtenemos una aplicación:

$$\begin{array}{rccc} \lambda_P : & \mathrm{Gal}(K/\mathbb{Q}) & \longrightarrow & E[2] \\ & \sigma & \longmapsto & \lambda_p(\sigma) = Q_P^\sigma \ominus Q_P. \end{array}$$

Veamos que se tiene $\lambda_P(\sigma) \in E[2]$ para todo $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$:

$$\begin{array}{rcl} [2]\lambda_P(\sigma) & = & [2](Q_P^\sigma \ominus Q_P) = ([2]Q_P)^\sigma \ominus [2]Q_P = \\ & = & P^\sigma \ominus P = \mathcal{O}, \end{array}$$

ya que como $P \in E(\mathbb{Q}), P^\sigma = P$. Si $\lambda_P = \lambda_{P'}$, entonces

$$Q_P^\sigma \ominus Q_P = \lambda_P(\sigma) = \lambda_{P'}(\sigma) = Q_{P'}^\sigma \ominus Q_{P'} \quad \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q}).$$

Por tanto,

$$(Q_P \ominus Q_{P'})^\sigma = Q_P^\sigma \ominus Q_{P'}^\sigma = Q_P \ominus Q_{P'} \quad \forall \sigma \in \mathrm{Gal}(K/\mathbb{Q}),$$

y como K es una extensión normal de $\mathbb{Q}$, se tiene que $K^{\mathrm{Gal}(K/\mathbb{Q})} = \mathbb{Q}$ (es decir, los elementos de K que son invariantes bajo la acción de todo el grupo $\mathrm{Gal}(K/\mathbb{Q})$, son elementos de $\mathbb{Q}$). Por tanto,

$$Q_P \ominus Q_{P'} \in E(\mathbb{Q}).$$

Así pues, si $\lambda_p = \lambda_{P'}$, se tiene $P' - P = [2](Q_{P'} - Q_P) \in 2E(\mathbb{Q})$. Tenemos por tanto una aplicación inyectiva

$$\lambda : \mathrm{ker}\phi \longrightarrow \mathcal{F}(\mathrm{Gal}(K/\mathbb{Q}), E[2]),$$

de modo que

$$|ker\phi| \leq \#\mathcal{F}(\mathrm{Gal}(K/\mathbb{Q}), E[2]).$$

Ahora, utilizando el teorema fundamental de la teoría de Galois tenemos que

$$\#\mathcal{F}(\mathrm{Gal}(K/\mathbb{Q}), E[2]) = 4^{|\,\mathrm{Gal}(K/\mathbb{Q})|} = 4^{[K:\mathbb{Q}]},$$

y obtenemos el resultado deseado. □

Corolario 2.1. *Si $|E(K)/2E(K)|$ es finito, entonces $|E(\mathbb{Q})/2E(\mathbb{Q}|$ es finito.*

En lo que sigue de esta sección, denotaremos por:

$$K^* = K \setminus \{0\} \text{ el grupo multiplicativo,}$$

$$K^{*2} = \{k \in K^* : \exists k' \in K^* \text{ tal que } k = (k')^2\}, \text{ y}$$

E una curva elíptica dada por $y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x)$, con K el cuerpo de descomposición de $f(x)$.

Proposición 2.2. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Definimos*

$$\varphi_\alpha : E(K) \longrightarrow K^*/K^{*2}$$

mediante

$$\varphi_\alpha = \begin{cases} (x-\alpha)K^{*2} & si \quad P = (x,y) \text{ con } P \neq \mathcal{O} \text{ y } x \neq \alpha, \\ (\alpha-\beta)(\alpha-\gamma)K^{*2} & si \quad P = (\alpha, 0), \\ 1 \cdot K^{*2} & si \quad P = \mathcal{O}. \end{cases}$$

Entonces φ_α es un homomorfismo de grupos

$$E(K)/2E(K) \longrightarrow K^*/K^{*2},$$

que llamaremos también φ_α.

Demostración. Si tenemos $P_1 \oplus P_2 = P_3$ con $P_i \in E(K)$ para $i = 1, 2, 3$, queremos comprobar que

$$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3)^{-1} \in K^{*2}.$$

Observamos que si $k \in K^*/K^{*2}$, entonces $k = k^{-1}$. Además, por la definición de φ_α, para todo $P \in E(K)$ se tiene $\varphi_\alpha(P) = \varphi_\alpha(\ominus P)$. Por tanto, para ver que φ_α es un homomorfismo de grupos basta con ver que

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \longrightarrow \varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

Si $P_i = \mathcal{O}$, por ejemplo $i = 1$, entonces $P_2 \oplus P_3 = \mathcal{O}$. Por tanto como $\varphi_\alpha(P_2) = \varphi_\alpha(\ominus P_3) = \varphi_\alpha(P_3)$ se tiene

$$\varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) = [\varphi_\alpha(P_2)]^2 \in K^{*2}.$$

Es decir, podemos asumir que P_i es un elemento de la forma (x_i, y_i) con $i = 1, 2, 3$.

Vamos a diferenciar dos casos:

1. $x_i \neq \alpha, i = 1, 2, 3$.

   Sea $y = mx + b$ la recta que une P_1, P_2, P_3. Cada $P_i = (x_i, y_i)$ satisface

   $$(x - \alpha)(x - \beta)(x - \gamma) = y^2 = (mx + b)^2.$$

   Entonces $(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = 0$ para $x = x_1, x_2, x_3$. Es decir,

   $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3).$$

   Poniendo $x = \alpha$ obtenemos

   $$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = (m\alpha + b)^2;$$

   y por la definición de φ_α, tenemos

   $$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

2. $x_1 = \alpha$.

   Entonces $(x_2, y_2)(x_3, y_3) \neq (\alpha, 0)$, ya que si no alguno de los tres puntos sería $\mathcal{O}$, posibilidad que hemos descartado anteriormente. Sea de nuevo $y = mx + b$ la recta que une P_1, P_2, P_3. Ahora, como $x_1 = \alpha$, obtenemos

   $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - \alpha)(x - x_2)(x - x_3). \tag{2.2}$$

   Entonces $(x - \alpha) | (mx + b)^2$, y por lo tanto $mx + b = m(x - \alpha)$. Sustituyendo en la ecuación (2.2) tenemos

   $$(x - \alpha)(x - \beta)(x - \gamma) - m^2(x - \alpha)^2 = (x - \alpha)(x - x_2)(x - x_3);$$

   y dividiendo por $x - \alpha$,

   $$(x - \beta)(x - \gamma) - m^2(x - \alpha)^2 = (x - x_2)(x - x_3).$$

   Tomando $x = \alpha$ conseguimos

   $$(\alpha - \beta)(\alpha - \gamma) = (\alpha - x_2)(\alpha - x_3),$$

   que no es más que

   $$\varphi_\alpha(P_1) = \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3).$$

   Luego

   $$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

□

Proposición 2.3. *Sea E una curva elíptica definida sobre K con car$(K) \neq 2, 3$. Supongamos que E está dada por*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3 + rx^2 + sx + t \text{ con } \alpha, \beta, \gamma \in K.$$

Dado $P_2 = (x_2, y_2) \in E(K), P_2 \neq \mathcal{O}$, existe $P_1 = (x_1, y_1) \in E(K)$ tal que $[2]P_1 = P_2$ si y sólo si

$$\begin{cases} x_2 - \alpha = \alpha_1^2 \\ x_2 - \beta = \beta_1^2 \\ x_2 - \gamma = \gamma_1^2 \end{cases} \quad \text{con } \alpha_1, \beta_1, \gamma_1 \in K.$$

Demostración.
($\Rightarrow$) Supongamos que existe $P_1 = (x_1, y_1)$ tal que $[2]P_1 = P_2$. Sea $y = mx + b$ la recta tangente a E en P_1. La recta corta a E en P_1 dos veces y en P_2. Por tanto las raíces de

$$x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = 0$$

son x_1, como raíz doble, y x_2. Entonces tenemos

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_2)(x-x_1)^2.$$

Pongamos $x = \alpha$:

$$-(mx+b)^2 = (\alpha - x_2)(\alpha - x_1)^2.$$

Es obvio que $\alpha - x_1 \neq 0$, ya que si $x_1 = \alpha$, entonces $P_1 = (\alpha, 0)$ y tendríamos $[2]P_1 = \mathcal{O} = P_2$, en contradicción con la hipótesis $P_2 \neq \mathcal{O}$. Por tanto,

$$x_2 - \alpha = \left(\frac{m\alpha + b}{\alpha - x_1}\right)^2 = \alpha_1^2.$$

Análogamente para β y γ.

($\Leftarrow$) Para simplificar, vamos a hacer un cambio de variables, para así tener $x_2 = 0$ y con esto obtener $y_2^2 = -\alpha\beta\gamma = t$. Por tanto tenemos como hipótesis

$$\begin{cases} -\alpha = \alpha_1^2 \\ -\beta = \beta_1^2 \\ -\gamma = \gamma_1^2 \end{cases} \quad \text{con } \alpha_1, \beta_1, \gamma_1 \in K.$$

Entonces podemos elegir

$$y_2 = \alpha_1\beta_1\gamma_1.$$

Busquemos ahora P_1. Sea $y = mx + b$ una recta que pasa por P_2 y es tangente a E en un punto (x_1, y_1), es decir,

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = x(x-x_1)^2.$$

Observamos que $y_2 = b$ ya que $y = mx + b$ pasa por $(0, y_2)$. Entonces,

$$\frac{1}{x}[x^3 + rx^2 + sx - m^2x^2 - 2my_2x] = (x-x_1)^2,$$

esto es, el polinomio

$$x^2 + rx + s - m^2x - 2my_2 \tag{2.3}$$

tiene raíces repetidas. Por tanto su discriminate es nulo,

$$(m^2 - r)^2 - 4(s - 2my^2) = 0. \tag{2.4}$$

Si encontramos una solución $m_0 \in K$ de la ecuación (2.4) obtendríamos que $x_1 = \frac{1}{2}(m_0^2 - r)$ es na raíz doble de (2.3), y que por tanto

$$[2](x_1, m_0x_1 + y_2) = (x_2, -y_2) = \ominus P_2.$$

Con esto,

$$[2](x_1, -m_0x_1 - y_2) = P_2.$$

Vamos a buscar una solución de (2.4). Introducimos una nueva variable u:

$$(m^2 - r + u)^2 = (m^2 - r)^2 + 2um^2 - 2ur + u^2$$

y utilizando (2.4),

$$(m^2-r+u)^2 = 4(s-2my_2)+2um^2-2ur+u^2 = 2um^2-8y_2m+u^2-2ur+4s. \tag{2.5}$$

El lado derecho de esta ecuación es el cuadrado de un polinomio en m. Para verlo, necesitamos encontrar una raíz doble de $2um^2 - 8y_2m + u^2 - 2ur + 4s$, y para ello el discriminante ha de ser cero:

$$64y_2^2 - 8u(u^2 - 2ru + 4s) = 0.$$

Utilizando que $y_2^2 = t$, tenemos

$$-u^3 + 2ru^2 - 4su + 8t = 0.$$

Las raíces de esta ecuación son $-2\alpha, -2\beta$ y -2γ, por serlo α, β y γ de la ecuación $x^3 + rx^2 + sx + t = 0$. Y si ponemos $u = -2\alpha$ en (2.5),

$$(m^2 - r - 2\alpha)^2 = -4\alpha m^2 - 8y_2 m + 4\alpha^2 + 4r\alpha + 4s.$$

Ahora podemos escribir r y s en términos de α, β, γ, deduciendo

$$\begin{cases} r = -(\alpha + \beta + \gamma), \\ s = \alpha\beta + \alpha\gamma + \beta\gamma; \end{cases}$$

y utilizando

$$\begin{cases} -\alpha = \alpha_1^2, \\ -\beta = \beta_1^2, \\ -\gamma = \gamma_1^2, \end{cases}$$

junto con $y_2 = \alpha\beta\gamma$ obtenemos

$$(m^2 - \alpha + \beta + \gamma)^2 = 4(\alpha_1 m - \beta_1\gamma_1)^2.$$

Así que

$$\begin{aligned} m^2 - \alpha + \beta + \gamma &= \pm 2(\alpha_1 m - \beta_1\gamma_1) \\ m^2 \mp 2\alpha_1 m - \alpha &= -\beta - \gamma \mp 2\beta_1\gamma_1 \\ (m \mp \alpha_1)^2 &= \beta_1^2 \mp 2\beta_1\gamma_1 + \gamma_1^2 = (\beta_1 \mp \gamma_1)^2. \end{aligned}$$

En definitiva, obtenemos las siguientes soluciones de (2.4):

$$\begin{aligned} m &= \alpha_1 \pm (\beta_1 - \gamma_1) \\ m &= \alpha_1 \pm (\beta_1 + \gamma_1) \\ m &= -\alpha_1 \pm (\beta_1 - \gamma_1) \\ m &= -\alpha_1 \pm (\beta_1 + \gamma_1), \end{aligned}$$

todas ellas pertenecientes a K. Así culmina esta demostración. □

Análogamente a la definición de φ_α, podemos definir el homomorfismo de grupos $\varphi_\beta : E(K) \to K^*/K^{*2}$. Así obtenemos la siguiente proposición:

Proposición 2.4. *El homomorfismo*

$$\varphi_\alpha \times \varphi_\beta : E(K)/2E(K) \longrightarrow K^*/K^{*2} \times K^*/K^{*2},$$

es inyectivo.

Demostración. : Sea $P \neq \mathcal{O}$, de la forma (x, y). Supongamos que $P \in \ker \varphi_\alpha \times \varphi_\beta$, de forma que

$$\varphi_\alpha(P), \varphi_\beta(P) \in K^{*2}.$$

Vamos a diferenciar varios casos:

1. $P \neq (\alpha, 0), (\beta, 0)$. La hipótesis es que $x - \alpha, x - \beta \in K^{*2}$. Además como $P \in E(K)$,
$$(x - \alpha)(x - \beta)(x - \gamma) = y^2 \in K^{*2},$$
luego $x - \gamma \in K^{*2}$ y por el Lema 2.3 tendremos que $P \in 2E(K)$.

2. $P = (\alpha, 0)$. La hipótesis es ahora que
$$\begin{cases} \varphi_\alpha(P) \in K^{*2} \\ \varphi_\beta(P) \in K^{*2} \end{cases} \quad \text{es decir} \quad \begin{cases} (\alpha - \beta)(\alpha - \gamma) \in K^{*2} \\ (\beta - \alpha) \in K^{*2} \end{cases}$$
por tanto,
$$\begin{cases} \alpha - \beta \in K^{*2} \\ \alpha - \gamma \in K^{*2} \end{cases}.$$
Además $\alpha - \alpha = 0 \in K^{*2}$. Aplicando de nuevo el lema 2.3 obtenemos que $P = (\alpha, 0) \in 2E(K)$.

3. $P = (\beta, 0)$. Análogo al caso 2.

□

Necesitamos ahora enunciar un teorema que se enmarca en la teoría algebraica de números.

Teorema 2.3. *Sea K un cuerpo de números y sea $\mathcal{O}_K$ el anillo de enteros de K. Entonces existe una anillo R con $\mathcal{O}_K \subseteq R \subseteq K$ tal que:*

(i) R es un dominio de ideales principales

(ii) El grupo de unidades de R está finitamente generado.

Demostración. : Para la demostración de este teorema puede consultarse [Kna92], capítulo 4, sección 9. □

: Construido este anillo R, tenemos que por ser un dominio de factorización única, podemos escribir

$$K^*/K^{*2} = \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{p \text{ primo en } R} \mathcal{Z}/2\mathcal{Z}, \tag{2.6}$$

donde $\mathcal{U}(R)$ denota el conjunto de unidades de R y $\mathcal{U}^2(R)$, el de los cuadrados de las unidades de R.

Veremos que la imagen de $\varphi_\alpha \times \varphi_\beta$ en $K^*/K^{*2} \times K^*/K^{*2}$ es cero en casi todas las coordenadas de la descomposición de $K^*/K^{*2} \times K^*/K^{*2}$ obtenida aplicando (2.6) a los dos factores.

Si p es un primo en R y r es un elemento de K, escribiremos $p^a \| r$ si $r = p^a q$ y $q \in K$ es tal que p no es un factor ni de su denominador ni de su numerador. Utilizaremos todo esto para ver que $E(K)/2E(K)$ es finito.

Observación 2.1. Si K es el cuerpo de fracciones de un dominio R y E es una curva elíptica dada por

$$y^2 = x^3 + Ax + B \quad A, B \in K,$$

podemos tomar r el máximo común divisor de A y B, y hacer el cambio

$$\begin{cases} X = r^2 x, \\ Y = r^3 y. \end{cases}$$

Con esto, podemos suponer que $A, B \in R$. En particular, si $K = \mathbb{Q}$, la curva elíptica E tiene una forma de Weierstrass de la forma

$$y^2 = x^3 + Ax + B \quad \text{con } A, B \in \mathbb{Z}.$$

Además, si $x^3 + Ax + B = (x - \alpha)(x - \beta)(x - \gamma) = f(x) \in f(x) \in \mathbb{Z}[x]$ y K es el cuerpo de descomposición del polinomio $f(x)$, entonces por lo anterior, se deduce que $\alpha, \beta, \gamma \in \mathcal{O}_K$.

Proposición 2.5. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, por la observación anterior, podemos suponer que E viene dada por la ecuación*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma) = f(x) \quad \textit{con } \alpha, \beta, \gamma \in \mathcal{O}_K,$$

donde K es el cuerpo de descomposición de $f(x)$. Sea $\varphi_\alpha \times \varphi_\beta$ el homomorfismo anteriormente definido y d el discriminante de $f(x)$. Entonces el homomorfismo inducido por $\varphi_\alpha \times \varphi_\beta$,

$$E(K)/2E(K) \longrightarrow \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p|d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}),$$

es inyectivo.

Demostración. : Sea $P = (x, y) \in E(K) \setminus \{\mathcal{O}\}$. Queremos comprobar que las coordenadas de P en la descomposición (2.6) correspondientes a primos p que no dividan a d son cero.

Fijamos un primo $p \in R$ y definimos los enteros a, b, c como

$$p^a \| (x - \alpha), \quad p^b \| (x - \beta) \quad p^c \| (x - \gamma).$$

Como $(x - \alpha)(x - \beta)(x - \gamma) = y^2$ se debe cumplir que

$$a + b + c \equiv 0 \bmod 2. \tag{2.7}$$

Cuando $x \neq \alpha, \beta, \gamma$ vamos a diferencia dos casos:

1. Al menos uno de a, b, c es < 0. Digamos $a < 0$. Como $\alpha \in \mathcal{O}_K$ y $\mathcal{O}_K \subseteq R$, entonces $\alpha \in R$, y por tanto,

   $$p^{|a|} \| (\text{denominador de } x).$$

   Con esto tenemos que $p^a \| (x - \alpha), (x - \beta), (x - \gamma)$. Es decir, $a = b = c$ y de (2.7) deducimos que

   $$a \equiv b \equiv c \equiv 0 \bmod 2.$$

   Luego la imagen de $P = (x, y)$ en la p-ésima coordenada de la descomposición (2.6) es cero.

2. Al menos uno de a, b, c es > 0. Digamos $a > 0$. Si $p \not| d$, entonces $p \not| (\alpha - \beta)$. Como

   $$x - \beta = (x - \alpha) + (\alpha - \beta),$$

y $a > 0$, se tiene $b = 0$. Análogamente, con $\alpha - \gamma$ obtenemos $c = 0$. Y usando de nuevo (2.7) llegamos a

$$a \equiv b \equiv c \equiv 0 \bmod 2.$$

Por tanto la imagen de $P = (x, y)$ en la p-ésima coordenada de la descomposición (2.6) es de nuevo cero.

Nos queda por el caso en que $P \in \{(\alpha, 0), (\beta, 0), (\gamma, 0)\}$. Para éstos, $\varphi_\alpha(P)$ y $\varphi_\beta(P)$ son productos de $(\alpha-\beta), (\alpha-\gamma)$ y $(\beta-\gamma)$. Si $p \not| d$, entones $p \not| (\alpha-\beta), p \not| (\alpha-\gamma)$ y $p \not| (\beta - \gamma)$, por tanto $a = b = c = 0$.

Se concluye que la imagen de cualquier $P = (x, y)$ en todas las coordenadas tales que $p \not| d$ de la descomposición (2.6) son cero. □

Ahora, como el grupo de unidades de $R, \mathcal{U}(R)$, es finitamente generado,

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\}$$

es finito. Por lo tanto el grupo

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p|d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}),$$

es finito, y utilizando este hecho junto con la proposición 2.5 obtenemos que $E(K)/2E(K)$ es finito.

Para demostrar el teorema débil de Mordell, sólo nos queda aplicar el corolario 2.1 al hecho de que $E(K)/2E(K)$ es finito, para así obtener que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.

2.3 Alturas y el teorema Mordell-Weil

En esta sección demostraremos el teorema Mordell-Weil. Este resultado fue probado por el matemático británico Louis Mordell(1888-1972) en 1922 para curvas elípticas definidas sobre $\mathbb{Q}$, y fue generalizado en 1928 por el matemático frances André Weil(1906- 1998) quien probó el resultado no sólo para curvas elípticas sobre cuerpos numéricos, sino también para variedades abelianas.

Definición 2.3.1. Sea $x = \dfrac{a}{b} \in \mathbb{Q}$ con a y b primos entre sí. se define la altura de x por

$$h_0(x) = \log \max\{|a|, |b|\}$$

Para cualquier constante $C \geq 0$, es fácil ver que el conjunto el conjunto

$$\{x \in \mathbb{Q} \ / \ h_0(x) \leq C \ \}$$

es finito.

Definición 2.3.2. Sea $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \ / \ y^2 = x^3 + Ax + B \ \} \cup \{\mathcal{O}\}$ con $A, B \in \mathbb{Z}$. La función $h : E(\mathbb{Q}) \to \mathbb{R}$ definida por

$$h(P) = \begin{cases} h_0(\frac{a}{b}) & , \quad P = (\frac{a}{b}, y) \neq \mathcal{O} \\ \\ 0 & , \quad P = \mathcal{O} \end{cases}$$

se llama *altura* en $E(\mathbb{Q})$.

Una de las propiedades importantes que goza esta función se da en el siguiente proposición

Proposición 2.6. *Existe una constante C_1 tal que*

$$\Big| h(P + Q) + h(P - Q) - 2h(P) - 2h(Q) \Big| \leq C_1$$

para todo $P, Q \in E(\mathbb{Q})$.

Demostración. Ver [Was08, p. 219, Proposition 8.19]. □

Es conveniente reemplazar h por una función $\hat{h}$ que tenga mas y mejores propiedades. La existencia, buena definición y propiedades de esta nueva función que denotaremos por $\hat{h}$ y llamaremos **altura canónica** se da en el siguiente teorema.

Teorema 2.4. *Si E es una curva elíptica definida sobre $\mathbb{Q}$, entonces existe una única función*

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$$

con las siguientes propiedades:

1. *Existe $C_1 \geq 0$ tal que $\left|\hat{h}(P) - \frac{1}{2}h(P)\right| \leq \frac{C_1}{6}$ para todo $P \in E(\mathbb{Q})$.*

2. $\hat{h}(P) \geq 0$ *para todo* $P \in E(\mathbb{Q})$.

3. *Fijada* $C \geq 0$, *el conjunto* $\left\{ P \in E(\mathbb{Q}) \ / \ \hat{h}(P) \leq C \ \right\}$ *es finito.*

4. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ *para todo* $P, Q \in E(\mathbb{Q})$.

5. $\hat{h}(mP) = m^2\hat{h}(P)$ *para todo entero* m *y todo punto* $P \in E(\mathbb{Q})$.

6. $\hat{h}(P) = 0$ *si y sólo si* $P \in E(Q)_{\text{tors}}$.

Demostración. 1. Haciendo $P = Q$ en la proposición (2.6), obtenemos

$$|h(2P) - 4h(P)| \leq C_1 \tag{2.8}$$

para todo P (recordando que $h(\mathcal{O}) = 0$).
Definimos $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ por

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P) \tag{2.9}$$

Necesitamos probar que el límite existe. Tenemos

$$\frac{1}{4^n} h(2^n P) = h(P) + \sum_{j=1}^{n} \frac{1}{4^j} \left[h(2^j P) - 4h(2^{j-1} P) \right].$$

Por (2.8),

$$\left| \frac{1}{4^j} \left[h(2^j P) - 4h(2^{j-1} P) \right] \right| \leq \frac{C_1}{4^j},$$

luego

$$\lim_{n\to\infty} \frac{1}{4^n} h(2^n P) = h(P) + \sum_{j=1}^{\infty} \frac{1}{4^j} \left[h(2^j P) - 4h(2^{j-1} P) \right] \tag{2.10}$$

Por lo tanto, $\hat{h}(P)$ existe, y como $\sum_{j=1}^{\infty} \frac{C_1}{4^j} = \frac{C_1}{3}$ de (2.10) y la definición de $\hat{h}$, obtenemos

$$|\hat{h}(P) - \frac{1}{2} h(P)| \leq C_1/6. \tag{2.11}$$

2. Como $h(2^n P) \geq 0$, es claro que $\hat{h}(P) \geq 0$ para todo P.

3. Si $\hat{h}(P) \leq C$, usando (2.11) concluimos que $h(P) \leq 2C + \frac{C_1}{3}$. Luego existe sólo una cantidad finita de puntos P, que satisfacen la desigualdad.

4. Por el proposición (2.6) tenemos

$$\frac{1}{4^n}|h(2^nP+2^nQ)+h(2^nP-2^nQ)-2h(2^nP)-2h(2^nQ)| \leq \frac{c_1}{4^n}.$$

Haciendo $n \to \infty$, y usando (2.8) obtenemos

$$\left|2\widehat{h}(P+Q)+2\widehat{h}(P-Q)-4\widehat{h}(P)-4\widehat{h}(Q)\right| \leq 0$$

de donde se concluye el resultado deseado.

5. Como la altura depende sólo de la x-coordenada, $\hat{h}(-P) = \hat{h}(P)$. Por lo tanto, podemos asumir que $m \geq 0$. Procedemos entonces inductivamente. Para $m = 0$

$$\hat{h}(0P) = \hat{h}(\mathcal{O}) = \frac{1}{2}\lim_{n\to\infty}\frac{1}{4^n}h(2^n\mathcal{O}) = \frac{1}{2}\lim_{n\to\infty}\frac{1}{4^n}h(\mathcal{O}) = 0 = 0^2\hat{h}(P).$$

Para $m = 1$ es trivial. También haciendo $P = Q$ en la parte 4, obtenemos $\hat{h}(2P) = 2^2\hat{h}(P)$. Ahora sea $m \in \mathbb{Z}_{\geq 2}$ y supongamos el resultado válido para cada $n \in \mathbb{Z}_{\geq 1}$, tal que $n \leq m$, entonces

$$\begin{aligned}
\hat{h}((m+1)P) &= -\hat{h}((m-1)P)+2\hat{h}(mP)+2\hat{h}(P) \quad \text{(por la parte 4)} \\
&= [-(m-1)^2+2m^2+2]\hat{h}(P) \\
&= (m+1)^2\hat{h}(P).
\end{aligned}$$

Luego, el resultado es cierto para todo $m \in \mathbb{Z}_{\geq 0}$.

6. Si $P \in E(\mathbb{Q})_{tors}$ entonces $mP = \mathcal{O}$ para algún $m \in \mathbb{Z} \setminus \{0\}$, luego

$$m^2\hat{h}(P) = \hat{h}(mP) = \hat{h}(\mathcal{O}) = 0,$$

de donde $\hat{h}(P) = 0$. Recíprocamente, sea $P \in E(Q)$ tal que $\hat{h}(P) = 0$. Como $\hat{h}(mP) = m^2\hat{h}(P) = 0$ para todo $m \in \mathbb{Z}$.

$$\left\{mP \ / \ m \in \mathbb{Z}\ \right\} \subseteq \left\{P \in E(\mathbb{Q}) \ / \ \hat{h}(P) \leq 0\ \right\}.$$

Siendo el conjunto de la derecha finito existen $m_1, m_2 \in \mathbb{Z}$ tales que $m_1P = m_2P$, así existe $m_0 = (m_1 - m_2) \in \mathbb{Z}$ tal que $m_0P = \mathcal{O}$. Por lo tanto, $P \in E(Q)_{tors}$. Lo que completa la prueba.

□

Ahora ya estamos listos para deducir el teorema central de este capítulo.

Teorema 2.5 (Mordell-Weil)**.** *Si E es una curva elíptica definida sobre $\mathbb{Q}$, entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado*

Demostración. Sean $R_1, \ldots, R_n$ representantes de las clases del grupo cociente finito $E(\mathbb{Q})/2E(\mathbb{Q})$, es decir $E(\mathbb{Q})/2E(\mathbb{Q}) = \{\overline{R}_1, \overline{R}_2, \ldots, \overline{R}_n\}$. Si

$$c = \max\left\{\hat{h}(R_1), \hat{h}(R_2), \cdots, \hat{h}(R_n)\right\},$$

por el *item* 3 del teorema 2.4, el conjunto de puntos de $E(\mathbb{Q})$ de altura canónica $\leq c$ es finito. Sean $Q_1, Q_2, \ldots, Q_m$ dichos puntos; y sea G el subgrupo de $E(\mathbb{Q})$ generado por

$$R_1, \ldots, R_n, Q_1, \ldots, Q_m.$$

Afirmamos que $G = E(\mathbb{Q})$. Supongamos que $G \subsetneq E(\mathbb{Q})$. Sea $P_0 \in E(\mathbb{Q})$ un elemento que no está en G. Fijado un número real c' tal que $\hat{h}(P_0) \leq c'$, el conjunto

$$\left\{\widetilde{P} \in E(\mathbb{Q}) \setminus G \ : \ \hat{h}(\widetilde{P}) \leq c' \ \right\}$$

es finito y P_0 esta en él. Luego podemos elegir $P \in E(\mathbb{Q}) \setminus G$ tal que $\hat{h}(P)$ sea el mínimo con la condición $\hat{h}(P) \leq c'$. Por otro lado en $E(\mathbb{Q})/2E(\mathbb{Q})$ $\overline{P} = \overline{R}_i$ para algún $i \in \{1, 2 \cdots, n\}$, entonces existe $P_1 \in E(\mathbb{Q})$ tal que

$$P - R_i = 2P_1.$$

y por 4), 5) y 1) del teorema 2.4,

$$\begin{aligned} 4\hat{h}(P_1) &= \hat{h}(2P_1) = \hat{h}(P - R_i) \\ &= 2\hat{h}(P) + 2\hat{h}(R_i) - \hat{h}(P + R_i) \\ &\leq 2\hat{h}(P) + 2c + 0 \\ &< 2\hat{h}(P) + 2\hat{h}(P) = 4\hat{h}(P) \end{aligned}$$

(la última desigualdad se debe a que $c < \hat{h}(P)$, de lo contrario $\hat{h}(P) \leq c$ y por ende $P = Q_j \in G$ ¡Absurdo!). Por lo tanto,

$$\hat{h}(P_1) < \hat{h}(P).$$

Como P tiene la menor altura canónica entre los puntos que no están en G, debemos tener que $P_1 \in G$. Por lo tanto,

$$P = R_i + 2P_1 \in G.$$

Esta contradicción prueba que $E(\mathbb{Q}) = G$. □

Corolario 2.2. *La función altura canónica* $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$ *satisface las condiciones* $(i), (ii)$ *y* (iii) *del teorema del descenso con*

$$C_1 = 2\widehat{h}(\mathbb{Q}) \quad y \quad C_2 = 0.$$

Usando este corolario, podemos dar otra demostración del teorema de Mordell.

Segunda demostración de teorema 2.5. El teorema débil de Mordell nos dice que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito, y el corolario 2.1 nos asegura que la función altura canónica satisface las hipótesis del teorema del descenso. Por lo tanto el teorema del descenso nos asegura que $E(\mathbb{Q})$ esta finitamente generado. □

2.4 El teorema de Mordell-Weil-Néron

En esta sección no haremos mas que enunciar varias generalizaciones del teorema de Mordell. La primera consistirá en considerar curvas elípticas definidas sobre cuerpos de números algebraicos.

Teorema 2.6 (Mordell-Weil)**.** *. Sea* E *una curva elíptica definida sobre un cuerpo numérico* K*. Entonces* $E(K)$ *es un grupo abeliano finitamente generado.*

La demostración de este resultado se basa, al igual que la del teorema de Mordell, en la aplicación del teorema del descenso al grupo abeliano que forman los puntos racionales de E. Pero a diferencia del caso en que $K = \mathbb{Q}$, no podemos definir una función altura de forma tan explícita, por lo que se han de utilizar otras técnicas; y estas son las desarrolladas por la teoría general de funciones altura ver [Sil86], Capítulo VIII, secciones 5 y 6. Para utilizar el teorema del descenso necesitamos que exista un entero $m \geq 2$ tal que $\frac{E(K)}{mE(K)}$ sea finito. Este resultado nos lo da el siguiente teorema, que no es más que una generalización del teorema débil de Mordell al caso de cuerpos de números algebraicos ver [Sil86], capítulo VIII, theorem 1.1.

Teorema 2.7 (Mordell-Weil, versión débil)**.** *Sea* E *una curva elptica definida sobre un cuerpo de números algebraicos* K*. Entonces para cualquier entero* $m \geq 2$*,* $\frac{E(K)}{mE(K)}$ *es un grupo finito.*

El siguiente paso es trabajar con variedades abelianas. Aquí, una curva elíptica no es más que una variedad abeliana de dimensión 1, un resultado es el siguiente.

Teorema 2.8 (Weil)**.** *Sea K un cuerpo cuerpo de números algebraicos y sea $\mathcal{A}$ una variedad abeliana definida sobre K. Entonces $\mathcal{A}(K)$ está finitamente generado.*

Tanto este último teorema como el que hemos llamado teorema de Mordell-Weil, fueron demostrados por André Weil en 1928. El mismo Weil, en 1930, aplicó la demostración de este teorema al caso de curvas elípticas definidas sobre $\mathbb{Q}$, para así dar una prueba más sencilla que la que dío Mordell. Por último, el matemático Frances André Néron (30 noviembre 1922 - 6 abril 1985), generalizó el teorema de Weil al caso en que el cuerpo K es un cuerpo finitamente generado sobre un cuerpo primo.

Teorema 2.9 (Mordell-Weil-Néron)**.** *Sea K un cuerpo finitamente generado sobre un cuerpo primo y sea $\mathcal{A}$ una variedad abeliana definida sobre K. Entonces $A(K)$ está finitamente generado.*

2.5 Los teoremas de Mazur y Lutz-Nagell

Nótese que el teorema de Mordell-Weil implica que $E(\mathbb{Q})_{\text{tors}}$ es un grupo abeliano finito. La pregunta es inmediata: ¿qué grupos finitos surgen en este contexto? Barry Mazur (9 dic, 1937) de la universidad Harvard encontró la respuesta a esta interrogante, y es como sigue.

Teorema 2.10 (Mazur)**.** *Sea E/Q una curva elíptica. Entonces, el subgrupo de torsión $E(\mathbb{Q})_{tors}$ de $E(\mathbb{Q})$ es isomorfo exactamente a uno de los siguientes quince grupos*

$$\mathbb{Z}/n\mathbb{Z} \text{ con } 1 \leq n \leq 10 \text{ o } n = 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad 1 \leq n \leq 4$$

Además, para cada uno de estos grupos existe al menos una curva $E/\mathbb{Q}$, cuyo grupo de torsión racional es isomorfo a él. A continuación se incluye una tabla con ejemplos de cada uno de los posibles grupos de torsión caracterizados en el teorema.

El teorema de Mazur es, por supuesto, de gran interés dentro de la teoría de curvas elípticas. Una consecuencia útil es que si el orden de un punto racional $P \in E(\mathbb{Q})$ es mayor que 12, entonces *" P es en verdad de orden infinito"* y por tanto la curva tiene infinitas soluciones racionales.

Curva	$E(\mathbb{Q})_{\text{tors}}$	Generadores
$y^2 = x^3 - 4$	trivial	$\mathcal{O}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$	$[-2 : 0 : 1]$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$	$[0 : 2 : 1]$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$	$[2 : 4 : 1]$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$	$[0 : 1 : 1]$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$	$[2 : 3 : 1]$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$	$[3 : 8 : 1]$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$	$[-2 : 10 : 1]$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$	$[3 : 1 : 1]$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$	$[0 : 9 : 1]$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$	$[0 : 210 : 1]$
$y^2 = x^3 - 4x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	$[0 : 0 : 1], [2 : 0 : 1]$
$y^2 = x^3 + 2x^2 - 3x$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	$[0 : 0 : 1], [3 : 6 : 1]$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	$[2 : -2 : 1], [-3 : 18 : 1]$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$[30 : -90 : 1], [-40 : 400 : 1]$

Tabla 2.1: Casos de ocurrencia de grupos de torsión posibles en el teorema de Mazur

El siguiente resultado fue demostrado independientemente por E. Lutz y T. Nagell, y ofrece un algoritmo muy simple para determinar los puntos de torsión de una curva.

Teorema 2.11 (Lutz-Nagell)**.** *Sea E es una curva elíptica definida sobre $\mathbb{Q}$ con ecuación de Weierstrass*

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}.$$

Si $P = (x(P) : y(P) : 1) \in E(\mathbb{Q})_{\text{tors}} \setminus \{\mathcal{O}\}$, entonces:

1. *$x(P), y(P) \in \mathbb{Z}$;*
2. *$y(P) = 0$ (y por lo tanto $2P = \mathcal{O}$), o bien $y(P)^2 \Big| (4A^3 + 27B^2)$.*

Debemos tener en cuenta que el teorema de Lutz-Nagell no da condiciones suficientes para encontrar los puntos de torsión, sólo nos da condiciones necesarias. ya que es posible encontrar curvas elípticas definidas sobre $\mathbb{Q}$ que tengan puntos con coordenadas enteras tales que $y(P)^2$ divida al discriminante $d = -(4A^3 + 27B^2)$ del polinomio cúbico $f(x) = x^3 + Ax + B$ pero que, sin embargo, no son puntos de orden finito.

Ejemplo 2.1. Sea E la curva elíptica definida por

$$E : y^2 = x^3 - 4$$

Entonces $d = -(4A^3 + 27B^2) = -3^3 \cdot 2^4$. Si $P = (x : y : 1)$ es un punto de torsión, la posibilidad $y = 0$ no se da, ya que la ecuación $x^3 - 4 = 0$ no tiene soluciones enteras. Por lo tanto E no tiene puntos de 2-torsión. Ahora buscamos enteros y tales que $y^2 \big| d$, entonces

$$y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}.$$

Comprobamos que los únicos posibles puntos de torsión son

$$\mathcal{O}, P_1 = (2, 2), P_2 = (2, -2) \in E(\mathbb{Q}).$$

Veamos si P_1 o P_2 tiene orden finito. Como

$$x(P_i) = 2, \quad x(2P_i) = 5 \quad \text{y} \quad x(4P_i) = \frac{5 \cdot 157}{4 \cdot 11^2} \notin \mathbb{Z}.$$

Entonces $P_i \notin E(\mathbb{Q})_{\text{tors}}$. Así obtenemos que

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}. \tag{2.12}$$

Ejemplo 2.2. Sea E la curva elíptica definida por

$$E : y^2 = x^3 + 4.$$

Entonces $d = -(4A^3 + 27B^2) = -3^3 \cdot 2^4$. Si $P = (x : y : 1)$ es un punto de torsión, la posibilidad $y = 0$ no se da, ya que la ecuación $x^3 + 4 = 0$ no tine soluciones enteras. Por lo tanto E no tine puntos de 2-torsión. Ahora buscamos enteros y tales que $y^2 \big| d$, entonces

$$y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$$

Comprobamos que los únicos posibles puntos de torsión son

$$\mathcal{O}, P_1 = (0, 2), P_2 = (0, -2) \in E(\mathbb{Q}).$$

Veamos si P_1 o P_2 tiene orden finito. Un cálculo rápido muestra que

$$3(0, \pm 2) = \mathcal{O}.$$

Por lo tanto el subgrupo de torsión de $E(\mathbb{Q})$ es cíclico de orden 3, es decir

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (0, 2), (0, -2)\} \cong \mathbb{Z}/3\mathbb{Z}. \tag{2.13}$$

Ejemplo 2.3. Sea E la curva elíptica definida por

$$y^2 = x^3 + 8.$$

Entonces $d = -(4A^3 + 27B^2) = 1728 = -2^6 \cdot 3^3$. Sea $P = (x : y : 1)$ un punto de torsión, si $y = 0$, entonces $x = -2$, luego el punto $(-2, 0)$ tiene orden 2. Si $y \neq 0$, entonces $y^2 \mid 2^6 \cdot 3^3$, lo que significa que $y \mid 24$, es decir

$$y \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$$

Intentando con todas estas distintas posibilidades, encontramos los puntos $(1, \pm 3)$ y $(2, \pm 4)$. Sin embargo,

$$2(1, 3) = 2(2, -4) = (-7/4, -13/8) \qquad \text{y} \qquad 2(2, 4) = 2(1, -3) = (-7/4, 13/8).$$

Como estos puntos no tienen coordenadas enteras, no pueden tener orden finito. Por lo tanto el subgrupo de torsión de $E(\mathbb{Q})$ es cíclico de orden 2, es decir

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (-2, 0)\} \cong \mathbb{Z}/2\mathbb{Z}. \tag{2.14}$$

Usando el teorema Lutz-Nagell y obtenemos un posible punto de torsión P. ¿Cómo decidimos si es un punto de torsión o no? En el ejemplo previo, multiplicamos P por un entero y obtuvimos un punto que no era de torsión. Por lo tanto, P no era de torsión. En general, el teorema de Lutz-Nagell da explícitamente una lista finita de posibles puntos de torsión. Si P es un punto de torsión, entonces, para todo n, el punto nP debe ser o $\mathcal{O}$ o debe estar en la lista. Como hay un número finito de puntos en la lista, tendremos $nP = mP$ para algunos $n \neq m$, en cuyo caso P es de torsión y $(n-m)P = \mathcal{O}$, o algún múltiplo nP no está en la lista y P no es de torsión.

Alternativamente, podemos usar el teorema de Mazur, que indica que el orden de un punto de torsión en $E(\mathbb{Q})$ es a lo más 12. Por lo tanto, si $nP \neq \mathcal{O}$ para todo $n \leq 12$, entonces *P no es de torsión.*

Otra técnica importante que nos ayuda determinar los subgrupos de torsión, tiene que ver con la reducción módulo un primo no negativo, como se ilustra en el siguiente.

Ejemplo 2.4. Para encontrar la torsión en $y^2 = x^3 + 8$, tenemos que $4A^3 + 27B^2 = 1728 = 2^6 \cdot 3^3$, luego no podemos usar los primos 2 ni 3 en la reducción, puesto que $d = 0$. La reducción módulo 5, es

$$E(\mathbb{F}_5) = \{(x, y) \in \mathbb{F}_5 \times \mathbb{F}_5 \ / \ y^2 = x^3 + 3\} \cup \{\mathcal{O}\}$$

Para contar los puntos de $E(\mathbb{F}_5)$, hacemos una lista de los valores de $x \in \mathbb{F}_5$, de $x^3 + 3$ (módulo 5), luego de las raíces cuadradas y de $x^3 + 3$ (módulo 5), así.

x	x^3+3	y	puntos
0	3	$-$	$---$
1	4	± 2	$(1,2); (1,-2)$
2	1	± 1	$(2,1); (2,-1)$
3	0	0	$(3,0))$
4	2	$-$	$---$

Por lo tanto, $E(\mathbb{F}_5) = \big\{(1,2); (1,3), (2,1); (2,4); (3,0), \mathcal{O}\big\}$. Análogamente $E(\mathbb{F}_{13})$ tiene orden 16, luego por el teorema anterior el subgrupo $E(\mathbb{Q})_{\text{tors}}$ tiene orden que divide a 6 y a 16; se sigue entonces que el grupo de torsión tiene orden que divide a 2, y como $(-2, 0)$ es un punto de orden 2, la torsión tiene orden exactamente 2. Esto es por supuesto el mismo resultado obtenido en (1.2) usando el teorema Lutz-Nagell.

Como aplicación de lo hecho hasta ahora, respondemos aquí a la interrogante planteada en la introducción de este trabajo con respecto a los números congruentes.

Teorema 2.12 (Números congruentes)**.** *Si $n \in \mathbb{Z}^+$ es libre de cuadrados, son equivalentes:*

1. *n es congruente: $n = \frac{1}{2}ab$ y $a^2 + b^2 = c^2$ con $a, b, c \in \mathbb{Q}$.*
2. *Existen tres cuadrados racionales en progresión aritmética de razón n.*
3. *Existe $(x, y) \in \mathbb{Q}\times\mathbb{Q}$ distinto de $(-n, 0), (0, 0)$ y $(n, 0)$ que satisface la ecuación*

$$y^2 = x^3 - n^2x \tag{2.15}$$

Demostración. $1 \Longrightarrow 2$) Siendo n congruente, existen $a, b, c \in \mathbb{Q}$: $n = \frac{1}{2}ab$ y $a^2 + b^2 = c^2$. Luego considerando $r = \frac{c}{2}$ se tiene que

$$r^2 \pm n = \left(\frac{c}{2}\right)^2 \pm \frac{1}{2}ab = \frac{a^2 + b^2}{4} \pm \frac{1}{2}ab = \left(\frac{a \pm b}{2}\right)^2.$$

Así los números $r^2 - n$, r^2 y $r^2 + n$ son cuadrados de números racionales en progresión aritmética de razón n.
$2 \Longrightarrow 1$) Sean $u, v, w \in \mathbb{Q}$ tales que u^2, v^2 y w^2 estan en progresión aritmética de razón n, es decir $x - n = u^2, x = v^2$ y $x + n = w^2$. Luego considerando

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

se concluye que $a, b, c \in \mathbb{Q}$, $a^2 + b^2 = c^2$ y $n = \frac{1}{2}ab$.
$2 \Longrightarrow 3$) Sean $u, v, w \in \mathbb{Q}$ tales que u^2, v^2 y w^2 estan en progresión aritmética de razón n, es decir $x - n = u^2, x = v^2$ y $x + n = w^2$. Si $y = uvw$ tenemos que

$$y^2 = u^2v^2w^2 = (x - n)x(x + n) = x^3 - n^2x.$$

Además $(x, y) \in \mathbb{Q}^2$, y es distinto de $(-n, 0), (0, 0)$ y $(n, 0)$ puesto que n un entero libre de cuadrados.
Falta demostrar que $(3 \Longrightarrow 2)$. En efecto: Sea $P = (x_1, y_1) \in \mathbb{Q}\times\mathbb{Q}$ una solución no trivial de (2.15) (es decir $x_1 \neq 0, x_1 \neq -n, x_1 \neq n$). Como $y_1 \neq 0$ $P \neq \mathcal{O}$ y $2P \neq \mathcal{O}$.

Si $2P = (x_2, y_2)$ y $\mathcal{L} : y = mx + b$ es la recta tangente en P, que interseca a la curva en $-2P = (x_2, -y_2)$. Entonces las coordenadas de P y $-2P$ satisfacen

$$\begin{cases} y^2 = x(x-n)(x+n) \\ y = mx + b \end{cases}$$

luego x_1 y x_2 son las únicas raíces de

$$(mx + b)^2 = x(x-n)(x+n).$$

Podemos escribir entonces

$$x(x-n)(x+n) - (mx+b)^2 = (x-x_1)^2(x-x_2).$$

Haciendo $x = 0$

$$-b^2 = x_1^2(-x_2)$$

y sale que $x_2 = \left(\frac{b}{x_1}\right)^2$ es un cuadrado. Con $x = -n$,

$$-(-mn+b)^2 = (-n-x_1)^2(-n-x_2)$$

y sale que $x_2 + n = \left(\frac{b-mn}{n+x_1}\right)^2$ es un cuadrado. Análogamente, con $x = n$ sale que $x_2 - n$ es un cuadrado. □

Capítulo 3

El rango del grupo de Mordell

El teorema de Mordell-Weil establece que el rango de $E(K)$ es finito para cualquier curva elíptica E definida sobre un cuerpo numérico K. Resulta natural entonces preguntarse ¿cómo encontrar el rango en una curva elíptica prefijada?. A pesar de haber visto que el grupo de torsión es relativamente sencillo de calcular, hay muy pocos resultados concernientes al cálculo del rango de una curva elíptica arbitraria, y no se conocen algoritmos eficientes para ello.

El rango de una curva elíptica sobre $\mathbb{Q}$ elegida al azar casi siempre es pequeño, y no es sencillo generar curvas elípticas sobre $\mathbb{Q}$ de rango moderadamente alto. Se conjetura que existen curvas elípticas sobre los racionales de rango arbitrariamente alto; y esto es lo que trataremos de lograr de aquí en adelante.

3.1 Forma bilineal de Néron-Tate

Sean $P_1, P_2, \cdots, P_r$ puntos en una curva elíptica E. Queremos saber bajo que condiciones estos puntos son *independientes*, en el sentido que los únicos enteros a_i tales que $a_1P_1 + \cdots + a_rP_r = \mathcal{O}$ son los triviales.

Definición 3.1.1. Sea E una curva elíptica sobre $\mathbb{Q}$. Los puntos $P_1, P_2, \cdots, P_r \in E(\mathbb{Q})$ son independientes, si lo son como $\mathbb{Z}$-módulos. Esto es, si $a_1P_1+\cdots+a_rP_r = \mathcal{O}$ con $a_i \in \mathbb{Z}$, entonces $a_i = 0$ para todo $i = 1, 2, \cdots, r$.

El siguiente teorema da las condiciones suficientes para que esto se cumpla.

Teorema 3.1. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ y sea $\hat{h}$ la altura canónica. Si para $P, Q \in E(\mathbb{Q})$ definimos*

$$\langle P, Q\rangle = \frac{1}{2}\left[\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right], \tag{3.1}$$

entonces $\langle\cdot,\cdot\rangle : E(\mathbb{Q})\times E(\mathbb{Q}) \longrightarrow \mathbb{R}$ es la única forma $\mathbb{Z}$-bilineal definida en $E(\mathbb{Q})$ tal que $\langle P, P\rangle = \hat{h}(P)$. Más aún, Si $P_1, P_2, \ldots, P_r$ son puntos en $E(\mathbb{Q})$ y el determinante

$$\det(\langle P_i, P_j\rangle) \neq 0,$$

entonces $P_1, \ldots, P_r$ son independientes.

Demostración. La segunda parte del teorema es verdadera para cualquier emparejamiento bilineal. Asumamos por el momento que el emparejamiento es bilineal y probemos la segunda parte. Supongamos que $a_1P_1+\cdots+a_rP_r = \mathcal{O}$ y que $a_r \neq 0$, por ejemplo. Entonces la última fila de la matriz $\left(\langle P_i, P_j\rangle\right)$ es una combinación lineal de las $r-1$ primeras filas. Por lo tanto, el determinante se anula. Esta contradicción prueba que los puntos deben ser independientes.
Por otro lado, como la forma ha de ser bilineal, debe cumplir

$$\langle P+Q, P+Q\rangle = \langle P, P\rangle + 2\langle P, Q\rangle + \langle Q, Q\rangle.$$

Como se ha de cumplir que $h(P) = \langle P, P\rangle$, si la forma bilineal existe ha de estar dada por

$$\langle P, Q\rangle = \frac{1}{2}\left[\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right].$$

Esto nos da la unicidad, la simetría de la forma bilineal y $\langle P, P\rangle = \hat{h}(P)$. La prueba de la bilinealidad es más difícil. Para esto, basta probar la linealidad en la primera variable, esto es

$$\langle P+Q, R\rangle = \langle P, R\rangle + \langle Q, R\rangle.$$

En efecto, recordando que la ley del paralelogramo para la altura canónica está dada por

$$\hat{h}(S+T) + \hat{h}(S-T) = 2\hat{h}(S) + 2\hat{h}(T) \quad \forall\ S, T \in E(\mathbb{Q})$$

y haciendo sucesivamente (S, T) igual a: $(P+Q, R)$, $(P, Q-R)$, $(P+R, Q)$ y (Q, R) obtenemos las siguientes ecuaciones:

$$\begin{aligned}
\hat{h}(P+Q+R) + \hat{h}(P+Q-R) &= 2\hat{h}(P+Q) + 2\hat{h}(R);\\
2\hat{h}(P) + 2\hat{h}(Q-R) &= \hat{h}(P+Q-R) + \hat{h}(P-Q+R);\\
\hat{h}(P+Q+R) + \hat{h}(P+R-Q) &= 2\hat{h}(P+R) + 2\hat{h}(Q);\\
4\hat{h}(Q) + 4\hat{h}(R) &= 2\hat{h}(Q+R) + 2\hat{h}(Q-R).
\end{aligned}$$

Sumando estas ecuaciones, obtenemos

$$2\big(\hat{h}(P+Q+R)-\hat{h}(P+Q)-\hat{h}(R)\big)=$$

$$2\big(\hat{h}(P+R)-\hat{h}(P)-\hat{h}(R)+\hat{h}(Q+R)-\hat{h}(Q)-\hat{h}(R)\big).$$

Dividiendo por 4 y usando la definición (**??**) se obtiene el resultado.
Finalmente, como

$$\begin{aligned}\langle -P,Q\rangle &= \tfrac{1}{2}[\hat{h}(Q-P)-h(P)-h(Q)]\\ &= \tfrac{1}{2}[\hat{h}(P+Q)-h(P)-h(Q)] \quad = -\langle P,Q\rangle,\end{aligned}$$

entonces $\langle -P,Q\rangle = -\langle P,Q\rangle$, y así $\langle kP,Q\rangle = k\langle P,Q\rangle$ par todo $k\in\mathbb{Z}$. Esto completa la demostración. □

Definición 3.1.2. La única forma bilineal $\langle,\rangle : E(\mathbb{Q})\times E(\mathbb{Q}) \longrightarrow \mathbb{R}$ dada por (3.1) se llama **forma bilineal de Néron-Tate**.

Ejemplo 3.1. *Sea E la curva elíptica dada por $y^2 = x^3 + 73$, y sean $P=(2,9)$, $Q=(3,10)$ puntos en E. Entonces*

$$\begin{aligned}\langle P,P\rangle &= 0.9239\ldots\\ \langle P,Q\rangle &= -0.9770\ldots\\ \langle Q,Q\rangle &= 1.9927\ldots.\end{aligned}$$

Como

$$\det\begin{pmatrix} 0.9239 & -0.9770\\ -0.9770 & 1.9927\end{pmatrix} = 0.8865\ldots \neq 0,$$

los puntos P y Q son independientes en E.

Al inicio de la sección 3.2, precisaremos la forma en que se realizaron estos cálculos.

Observación 3.1. Para todo $m,n\in\mathbb{Z}$ y para todo $P;Q\in E(\mathbb{Q})$ se tiene

$$-2mn\langle P,Q\rangle = 2\langle -mP,nQ\rangle = \hat{h}(nQ-mP)-\hat{h}(mP)-\hat{h}(nQ),$$

y entonces

$$0\leq \hat{h}(nQ-mP) = m^2\hat{h}(P)-2mn\langle P,Q\rangle + n^2\hat{h}(Q),$$

dividiendo por n^2

$$x^2\hat{h}(P)-2x\langle P,Q\rangle+\hat{h}(Q)\geq 0 \quad \text{para todo } x\in\mathbb{Q}$$

y por consiguiente para todo $x \in \mathbb{R}$. Por tanto $4\langle P, Q\rangle^2 - 4\hat{h}(P)\hat{h}(Q) \leq 0$, o

$$\left|\langle P, Q\rangle\right|^2 \leq \hat{h}(P)\hat{h}(Q) \tag{3.2}$$

A esta desigualdad se le conoce como la *desigualdad de Schwartz*.

Observación 3.2. Ahora si $Q \in E(Q)_{\text{tors}}$, teniendo en cuenta que $\hat{h}(Q) = 0$ y la desigualdad de Schwartz, obtenemos que $\langle P, Q\rangle = 0$ para todo $P \in E(\mathbb{Q})$. Luego

$$0 = \langle P, Q\rangle = \frac{1}{2}[\hat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)] = \frac{1}{2}[\hat{h}(P+Q) - \widehat{h}(P)],$$

esto es

$$\hat{h}(P+Q) = \hat{h}(P) \quad \text{ para todo } P \in E(\mathbb{Q}) \text{ y } Q \in E(\mathbb{Q})_{\text{tors}}.$$

Así

$$\hat{h} : \frac{E(\mathbb{Q})}{E(\mathbb{Q})_{\text{tors}}} \longrightarrow \mathbb{R} \tag{3.3}$$

esta bien definida.

Proposición 3.1. *La matriz simétrica* $\left(\langle P_i, Q_i\rangle\right)_{1\leq i,j\leq r}$ *dada en el teorema (3.1) es definida positiva.*

Para la prueba de esta proposición nos remitimos a [Kna92, p. 102].

3.2 Aplicando PARI/GP

En esta sección daremos algunos ejemplos de aplicación usando el sistema de cálculo PARI-GP.

Ejemplo 3.2. En el ejemplo 3.1, hemos realizado los siguientes cálculos:

```
E=ellinit([0,0,0,0,73]);
P=[2, 9];
Q=[3, 10];
```

Esto nos permite ingresar la curva elíptica $E : y^2 = x^3 + 73$ y los puntos $P = (2, 9)$, $Q = (3, 10)$ pertenecientes a E, seguidamente al digitar

```
M=ellheightmatrix(E,[P,Q]);
```

obtenemos la matriz de Gram de $\langle P, Q\rangle$ con respecto a la forma bilineal de Néron-Tate, esto es

$$M = \begin{pmatrix} 0.92394317160039718794398860 40 & -0.97704341280383244116259337 47 \\ -0.97704341280383244116259337 47 & 1.99271684209964681795895037 2 \end{pmatrix}$$

Finalmente con

```
d=matdet(M);
```

obtenemos que el determinante de la matriz M es igual a

$$0,886543288687715440704579918 9.$$

Ejemplo 3.3. Dada la curva elíptica

$$E : y^2 = x^3 - 82x$$

vemos que los puntos:

$$\mathcal{O},\ (0,0),\ (-8,12),\ (-1,9) \quad \text{y} \quad (49/4, 231/8)$$

pertenecen a esta curva, ahora aplicando el sistema de cálculo PARI-GP, ingresamos los siguientes datos:

```
E=ellinit([0,0,0,-82,0]);
P1=[-8, 12];
P2=[-1, 9];
P3=[49/4, 231/8];
```

Seguidamente al digitar

```
d=matdet(ellheightmatrix(E,[P1, P2, P3]));
```

obtenemos el determinante d de la matriz de Gram de $\{P1, P2, P3\}$ con respecto a la forma bilineal de Néron-Tate, este valor es

$$d = 10.207892029767887379642364 29.$$

Esto nos demuestra que el rango de esta curva es ≥ 3.
Además al digitar

```
elltors(E);
```

obtenemos $\Big[2,[2],[[0,0]]\Big]$, lo que dice que el orden de $E(\mathbb{Q})_{tors}$ es 2, $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ y su generador es $(0,0)$, note que el orden del $(0,0)$ es 2, esto se comprueba con

```
ellorder(E, [0,0])
```

Ejemplo 3.4. Sea E la curva elíptica dada por

$$y^2 + xy = x^3 - 1574593253082908988 0x + 240282199570959694263392784 00$$

extraído de http:/web.math.hr/∼duje/tors/tors.html. Se tiene que los puntos:

$$P1 = (2188064030, -7124272297330), \quad P2 = (-2815745040, -214568724545880)\text{y}$$

$$P3 = (3643261410, -122557804465830)$$

están en esta curva. Ahora aplicamos el sistema de cálculo PARI-GP, ingresando:

```
E = ellinit([1,0,0,- 15745932530829089880, \\
    240282199570959694263392784 00]);
P1 = [2188064030, -7124272297330];
P2 = [-2815745040,-214568724545880];
P3 = [3643261410,-122557804465830];
```

Seguidamente al digitar

```
M=ellheightmatrix(E,[P1,P2,P3]);
```

obtenemos la matriz de Gram de $\{P1, P2, P3\}$ con respecto a la forma bilineal de Néron-Tate, esto es

$$M = \begin{pmatrix} 7.261842396396632856899561047 & -3.571608727612764003743178114 & a \\ -3.571608727612764003743178114 & 9.433486448726431512480241704 & b \\ -3.151543672981636435093343825 & -0.195795812610253928126957456 1 & c \end{pmatrix}$$

donde

$$a = -3.151543672981634350933438 25$$
$$b = -0.195795812610259281269574561$$
$$c = 9.753977730417593641447133 35.$$

Finalmente con

```
d=matdet(M);
```

obtenemos que el determinante de la matriz M es igual a

$$d = 445.384043809639796255451138 4.$$

Esto demuestra que los puntos $P1, P2$ y $P3$ son $\mathbb{Z}$-independientes. Más aún, Connell (2000) y Dujella (2000) afirman que $\text{rang}(E(\mathbb{Q})) = 3$.

3.3 Reducción de curvas elípticas

Sea E una curva elíptica definida sobre $\mathbb{Q}$ en la forma de Weierstrass

$$E : y^2 = x^3 + Ax + B \quad A, B \in \mathbb{Q}.$$

Si es necesario, por un cambio de coordenadas de la forma

$$(x, y) \longmapsto (c^2x, c^3y)$$

con $c \in \mathbb{Q}$, podemos suponer que $A, B \in \mathbb{Z}$.
Considere la aplicación reducción módulo un primo p de $\mathbb{Z}$.

$$\begin{array}{rccc} red_p: & \mathbb{Z} & \longrightarrow & \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \\ & x & \longmapsto & \overline{x} \end{array}$$

Si se aplica red_p sobre los coeficientes de E, obtenemos la curva

$$\widetilde{E} : y^2 = x^3 + \overline{A}x + \overline{B}.$$

definida sobre $\mathbb{F}_p$, que puede por su puesto, ser singular (si $\overline{\triangle} = 0$).

Definición 3.3.1. Se dice que:

1. p es un primo bueno o de buena reducción, si $\overline{\Delta} \neq \overline{0}$ esto es si $p \nmid \triangle$.
   En este caso $\widetilde{E}$ es una curva elíptica sobre $\mathbb{F}_p$.

2. p es un primo malo o de mala reducción, si $\overline{\Delta} = \overline{0}$ esto es si $p \mid \triangle$.
   En este caso se tienen tres posibilidades: cúspide (Figura (1.2)-ii), nodo (Figura (1.2)-i), nodo partido (Figura (1.2)-iii).

Ejemplo 3.5. Dada la curva elíptica $E : y^2 + y = x^3 - x^2 + 2x - 2$. Los primos de mala reducción para E son solamente 5 y 7. Puesto que $\triangle = -875 = -5^3 \times 7$. Esto se ha logrado, trabajando con pari/gp, así:

```
E=ellinit([0,-1,1,2,-2]);
E.disc;
```

3.4 Una cota superior para el rango

En la demostración del teorema débil de Mordell-Weil se incluye el grupo $E(\mathbb{Q})/2E(\mathbb{Q})$ en el grupo $G = \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Aquí, estableceremos una cota explícita para el orden de G, que nos dará información sobre el rango de $E(\mathbb{Q})$.

Dada una curva elíptica

$$E : y^2 = f(x) = x^3 + Ax + B = (x-\alpha)(x-\beta)(x-\gamma)$$

con $\alpha, \beta, \gamma \in K$ (cuerpo de descomposición de f). Si d es el discriminante de f, sabemos que existe un dominio $\mathcal{R}$ tal que

$$E(K)/2E(K) \hookrightarrow \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{p \text{ primo en } R \\ \text{tal que } p|d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}).$$

Por lo tanto

$$|E(K)/2E(K)| \leq \left|\mathcal{U}(\mathbb{R})/\mathcal{U}^2(\mathcal{R})\right|^2 \times 2^{2\#\{p \text{ primo en } \mathcal{R} \,:\, p|d\}}. \tag{3.4}$$

Además, de la proposición (2.1) obtenemos que

$$|E(\mathbb{Q})/2E(\mathbb{Q})| \leq |E(K)/2E(K)| + 4^{[K:\mathbb{Q}]}. \tag{3.5}$$

Vamos a diferenciar tres casos, dependiendo del número de puntos de 2-torsión que tenga $E(\mathbb{Q})$.

- $\alpha, \beta, \gamma \notin \mathbb{Z}$. Entonces $E(\mathbb{Q})_{\text{tors}}$ no tiene como subgrupo a $\mathbb{Z}/2\mathbb{Z}$ y por el teorema de Mazur obtenemos

  $$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/(2n+1)\mathbb{Z} \qquad 1 \leq 2n+1 \leq 9$$

  Por tanto,

  $$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

  Utilizando (3.4) y (3.5) tenemos:

  $$|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^r \leq \left|\mathcal{U}(\mathbb{R})/\mathcal{U}^2(\mathcal{R})\right|^2 \times 2^{2\#\{p \in \mathcal{R} \text{ primo} \,:\, p|d\}} + 4^{[K:\mathbb{Q}]},$$

  y así

  $$r \leq \log_2 \left[\left[\left|\mathcal{U}(\mathbb{R})/\mathcal{U}^2(\mathcal{R})\right| \right]^2 \times 2^{2\#\{p \in \mathcal{R} \text{ primo} \,:\, p|d\}} + 4^{[K:\mathbb{Q}]} \right] \tag{3.6}$$

- $\alpha \in \mathbb{Z}, \beta, \gamma \notin \mathbb{Z}$ Entonces $E(\mathbb{Q})_{\text{tors}}$ contiene a $\mathbb{Z}/2\mathbb{Z}$, pero no a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. El teorema de Mazur nos dice entonces que

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq 2n \leq 12$$

Por tanto,

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^r.$$

Utilizando de nuevo (3.4) y (3.5) tenemos que:

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+1} \leq \left|\mathcal{U}(\mathbb{R})/(\mathcal{U}^2(\mathcal{R}))\right|^2 \times 2^{2\#\{p \in \mathcal{R} \text{ primo } : \ p|d\}} + 4^{[K:\mathbb{Q}]},$$

y entonces

$$r \leq \log_2 \left[\left|\mathcal{U}(\mathbb{R})/(\mathcal{U}^2(\mathcal{R}))\right|^2 \times 2^{2\#\{p \in \mathcal{R} \text{ primo } : \ p|d\}} + 4^{[K:\mathbb{Q}]} \right] - 1 \tag{3.7}$$

- $\alpha, \beta, \gamma \in \mathbb{Z}$ Entonces $E[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, y el teorema de Mazur nos dice que

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq n \leq 4$$

por lo que

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^r.$$

Luego

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+2} \leq 2^2 \cdot 2^{2\#\{p \in \mathbb{Z} \text{ primo } : p|d\}},$$

y que

$$r \leq 2\#\{p \in \mathbb{Z} \text{ primo } \ : \ p \mid d\} \tag{3.8}$$

En este último caso es posible encontrar una cota mucho mejor que la obtenida en (3.8). Antes, para cada primo p en $\mathbb{Z}$, consideremos la reduccíon módulo p definida en la sección (3.3) y recordando que el discriminante d de la cúbica $f(x) = (x-\alpha)(x-\beta)(x-\gamma)$ esta dada por $d = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$, damos la siguiente definición

Definición 3.4.1. Sea E una curva elíptica definida sobre $\mathbb{Q}$ dada por

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \quad \text{con} \quad \alpha, \beta, \gamma \in \mathbb{Z}$$

Se dice que el primo:

- p es bueno si $p \nmid d$
- p es malo si p divide sólo a uno de los números: $(\alpha-\beta)$, $(\beta-\gamma)$, $(\gamma-\alpha)$
- p es muy malo si p divide a cada uno de los números: $(\alpha-\beta)$, $(\beta-\gamma)$, $(\gamma-\alpha)$

Teorema 3.2. *Sea E la curva elíptica sobre $\mathbb{Q}$ dada por*

$$y^2 = x^3 + Ax + B = (x-\alpha)(x-\beta)(x-\gamma).$$

Si $\alpha, \beta, \gamma \in \mathbb{Z}$, entonces

$$\operatorname{rang}(E(\mathbb{Q})) \leq n_1 + 2n_2 - 1 \tag{3.9}$$

donde n_1 es el número de primos malos, y n_2 es el número de primos muy malos, en las reducciones de la curva E.

Demostración. Para la prueba de este teorema vea [Kna92, Theorem 4.19, p. 108]. □

Ejemplo 3.6. Como aplicación de este teorema, podemos probar que la curva

$$E : y^2 = x^3 - x = x(x-1)(x+1).$$

no tiene más que las soluciones triviales de orden 2. En efecto, el discriminante de la cúbica $f(x) = x^3 - x$ es $d = \frac{\triangle}{16} = 4$, por tanto $p = 2$ es el único primo de mala reducción, que según la definición (3.4.1), p=2 es un primo malo, luego el teorema (3.2) nos permite concluir que $\operatorname{rang}(E(\mathbb{Q})) = 0$ (por lo tanto E sólo tiene puntos de torsión). Finalmente, el teorema de Lutz-Nagell implica que los únicos puntos de torsión son de orden 2, así

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Todo esto es corroborado usando pari/pg de la siguiente forma:

```
E=ellinit([0,0,0,-1,0]);
%1 = [0, 0, 0, -1, 0, 0, -2, 0, -1, 48, 0, 64, 1728,\\
[1.0000000000000000000000000000,0.E-38,-1.0000000000000000000000000000]~,\\
2.6220575542921198104648395 90, 2.6220575542921198104648395 90*I, \\
-0.5990701173677961037199612462, -1.7972103521033883111598837 38*I, \\
6.8751858180203728274900957 80]
elltors(E);
%2 = [4, [2, 2], [[1, 0], [0, 0]]]
```

Capítulo 4

Curvas elípticas de rango alto

4.1 La función zeta de Riemann

Para $s > 1$, definimos la *función zeta de Riemann* por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

que converge para $s > 1$ y diverge si s=1. Riemann tuvo la idea de considerar la función zeta para valores complejos de s, y estudiarla utilizando los métodos del análisis complejo.

Recordando que para valores complejos de la variable s, n^s se define por: $n^s = e^{s \log n}$, y como $|n^s| = n^{\mathrm{Re}(s)}$, la serie que define la función zeta converge si $\mathrm{Re}(s) > 1$, por lo que tiene sentido definirla en el semiplano $\mathrm{Re}(s) > 1$ del plano complejo. Además, por el test de Weierstrass, dicha serie converge uniformemente en cada semiplano $\mathrm{Re}(s) \geq 1 + \varepsilon$ (para $\varepsilon > 0$), en particular esto significa que la serie converge uniformemente sobre los compactos del semiplano $\mathrm{Re}(s) > 1$; esto implica que la función zeta de Riemann es una función analítica en dicho semiplano.

Definición 4.1.1. Una función $\varphi : \mathbb{N} \to \mathbb{C}$, se dice multiplicativa si $\varphi(1) = 1$ y si $\varphi(mn) = \varphi(m)\varphi(n)$, para todo par m, n de números naturales coprimos.
Se dirá que φ es completamente multiplicativa si $\varphi(mn) = \varphi(m)\varphi(n)$, para todo $m, n \in \mathbb{N}$. En este caso, para cada primo p

$$\varphi(p^k) = \varphi(p)^k$$

Proposición 4.1. *Si φ es una función multiplicativa y la serie de números complejos $\sum_{n=1}^{\infty}\varphi(n)$ converge absolutamente, entonces para $s\in\mathbb{C}$ tal que $Re(s)>1$ la serie*

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}$$

converge absolutamente y en su dominio de convergencia tiene una descomposición como un producto infinito

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\prod_{p\ primo}\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\frac{\varphi(p^3)}{p^{3s}}+\cdots\right).$$

Prueba.- La convergencia absoluta de la serie se sigue del hecho de que $\varphi(n)$ está acotada y de la convergencia de la serie de números reales $\sum_{n=1}^{\infty}1/n^{\alpha}$, para $\alpha>1$. Para la descomposición en producto infinito (llamado un *producto de Euler*) fijemos un natural N y consideremos un producto parcial

$$\begin{aligned}\prod_{p<N}\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\frac{\varphi(p^3)}{p^{3s}}+\cdots\right) &= \sum_{e_1}\frac{\varphi(p_1^{e_1})}{p_1^{e_1 s}}\sum_{e_2}\frac{\varphi(p_2^{e_2})}{p_2^{e_2 s}}\cdots\sum_{e_k}\frac{\varphi(p_k^{e_k})}{p_k^{e_k s}}\\ &= \sum_{e_1,\cdots,e_k}\frac{\varphi(p_1^{e_1})}{p_1^{e_1 s}}\frac{\varphi(p_2^{e_2})}{p_2^{e_2 s}}\cdots\frac{\varphi(p_k^{e_k})}{p_k^{e_k s}}\\ &= \sum_{e_1,\cdots,e_k}\frac{\varphi(p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k})}{p_1^{e_1 s}p_2^{e_2 s}\cdots p_k^{e_k s}}\\ &= \sum_{P(n)<N}\frac{\varphi(n)}{n^s}\end{aligned}$$

donde $p_1,\cdots,p_k$ son los primos menores que N y $P(n)$ es el mayor factor primo de n de tal forma que la última suma es sobre todos los enteros n cuyos factores primos son menores que N. Note que en la tercera igualdad usamos la multiplicatividad de φ. Ahora, como todo natural menor que N no tiene factores primos mayores que N, entonces

$$\left|\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}-\sum_{P(n)<N}\frac{\varphi(n)}{n^s}\right|\leq\sum_{n=N}^{\infty}\left|\frac{\varphi(n)}{n^s}\right|$$

y el término en la derecha tiende a 0 cuando $N\to\infty$, lo cual da el resultado deseado. □

Si en la demostración de esta proposición consideramos una función φ completamente multiplicativa y acotada, se tiene que la serie dentro del producto infinito es una serie geométrica que converge a $1/(1-\varphi(p)p^{-s})$. Así

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \prod_{p \ primo} \frac{1}{1-\varphi(p)p^{-s}}.$$

Considerando la función completamente multiplicativa constante $\varphi = 1$, hemos probado el siguiente teorema.

Teorema 4.1 (Euler)**.** *Si $s \in \mathbb{C}$ es tal que $\mathrm{Re}(s) > 1$, entonces*

$$\zeta(s) = \prod_{p \ primo} \frac{1}{1-p^{-s}}$$

Observación.- Para cada $N \in \mathbb{N}$ fijo (arbitrario)

$$\lim_{s\to 1^+} \zeta(s) \geq \lim_{s\to 1^+} \sum_{n\leq N} \frac{1}{n^s} = \sum_{n\leq N} \frac{1}{n} \qquad (s \in \mathbb{R})$$

y como la serie armónica diverge, haciendo que $N \to +\infty$, obtenemos que $\lim_{s\to 1^+} \zeta(s) = +\infty$, es decir

$$\lim_{s\to 1^+} \prod_{p \ primo} \frac{1}{1-p^{-s}} = +\infty,$$

lo que implica que existen infinitos primos, puesto que si sólo existieran finitos primos este límite debería ser finito (este fue el argumento que utilizó Euler para probar la infinitud de las primos, usando el análisis).

Antes de pasar al resultado tal vez más importante de esta sección definiremos la función gamma de Euler.

Definición 4.1.2. Para cada $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 0$, definimos la función gamma de Euler Γ por

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt.$$

Un resultado importante de esta función se da en el siguiente

Teorema 4.2. *La función Γ se extiende a una función meromorfa en todo el plano complejo $\mathbb{C}$, con polos simples en $0, -1, -2, -3 \cdots$ y residuos*

$$\mathrm{Res}(\Gamma, -m) = \frac{(-1)^m}{m!} \qquad \textit{para } m \geq 0$$

Lema 4.1. *Si* $x \in \mathbb{R}^+$ *y* $\psi(x) = \dfrac{\theta(x)-1}{2} = \displaystyle\sum_{n=1}^{\infty} e^{-(n^2\pi x)}$, *se tiene la ecuación funcional*

$$\theta(x^{-1}) = x^{1/2}\theta(x) \quad \textit{para } x > 0.$$

En consecuencia

$$2\psi(x^{-1}) = -1 + x^{1/2} + 2x^{1/2}\psi(x).$$

Aunque no demostraremos este lema, si mencionamos que para su prueba es necesario el uso de la fórmula de sumación de Poisson.

Definición 4.1.3. Para cada $s \in \mathbb{C}$ tal que $\mathrm{Re}(s) > 1$, definimos la función zeta completada por

$$\zeta^*(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

Teorema 4.3 (Ecuación funcional de la función zeta de Riemann)**.** *La función* ζ^* *admite una extensión analítica a todo el plano complejo, salvo los puntos* $s = 0$ *y* $s = 1$ *donde posee polos simples con residuos*

$$\mathrm{Res}(\zeta^*, 0) = -1 \ , \quad \mathrm{Res}(\zeta^*, 1) = 1$$

Además, satisface la ecuación funcional

$$\zeta^*(s) = \zeta^*(1-s)$$

es decir,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Prueba.- En $\Gamma(\frac{s}{2}) = \displaystyle\int_0^{\infty} e^{-t}t^{s/2-1}dt$ realizando el cambio de variable $t = n^2\pi x$, obtenemos $\Gamma(\frac{s}{2}) = (n^2\pi)^{s/2}\displaystyle\int_0^{\infty} e^{-(n^2\pi x)}x^{s/2-1}dx$. De donde

$$\Gamma(\frac{s}{2})(n^2\pi)^{-s/2} = \int_0^{\infty} e^{-(n^2\pi x)}x^{s/2-1}dx,$$

y sumando con respecto a $n \geq 1$

$$\Gamma(\frac{s}{2})(\pi)^{-s/2}\zeta(s) = \sum_{n=1}^{\infty}\int_0^{\infty} e^{-(n^2\pi x)}x^{s/2-1}dx = \int_0^{\infty}\left(\sum_{n=1}^{\infty} e^{-(n^2\pi x)}\right)x^{s/2-1}dx.$$

El cambio entre la suma y la integral es posible gracias a la convergencia uniforme de la suma. Luego

$$\begin{aligned}\Gamma(\tfrac{s}{2})(\pi)^{-s/2}\zeta(s) &= \int_1^\infty x^{s/2-1}\psi(x)dx + \int_0^1 x^{s/2-1}\psi(x)dx \\ &= \int_1^\infty x^{s/2-1}\psi(x)dx + \int_1^\infty x^{-s/2-1}\psi(x^{-1})dx.\end{aligned}$$

Teniendo en cuenta las propiedades de la función ψ

$$\begin{aligned}\int_1^\infty x^{-s/2-1}\psi(x^{-1})dx &= \int_1^\infty \frac{x^{-s/2-1}}{2}(-1+x^{1/2}+2x^{1/2}\psi(x))dx \\ &= \frac{1}{z(z-1)} + \int_1^\infty (x^{-s/2-1/2})\psi(x)dx.\end{aligned}$$

En consecuencia

$$\zeta^*(s) = \Gamma\left(\frac{s}{2}\right)(\pi)^{-s/2}\zeta(s) = \frac{1}{z(z-1)} + \int_1^\infty (x^{-s/2-1/2} + x^{s/2-1})\psi(x)dx.$$

La última expresión nos da la extensión analítica de $\zeta^*(s)$ para todo $s \in \mathbb{C}$, excepto en 0 y 1. Además, es evidente que

$$\zeta^*(s) = \zeta^*(1-s)$$

. □

Corolario 4.1. *La función $\zeta(s)$ admite una prolongación analítica a todo el plano complejo, salvo el punto $s = 1$ donde tiene un polo simple con residuo 1. Ella satisface la ecuación funcional*

$$\zeta(1-s) = 2(2\pi)^{-s}\cos\left(\frac{\pi s}{2}\right)\Gamma(s)\zeta(s) \tag{4.1}$$

Reescribimos la ecuación funcional (4.1) como

$$\zeta(s) = 2^s\pi^{s-1}sen\left(\frac{\pi s}{2}\right)\Gamma(1-s)\zeta(1-s) \tag{4.2}$$

De esta fórmula, cuando $\mathrm{Re}(s) < 0$, la función zeta se anula en los puntos donde $sen\left(\frac{\pi s}{2}\right) = 0$, es decir $s = 2k$ con $k \in \mathbb{Z}^-$ (s entero par negativo), llamados los ceros triviales de la función zeta. Existen otros valores complejos s comprendidos entre $0 < \mathrm{Re}(s) < 1$, para los cuales la función zeta también se anula, llamados ceros "no triviales". La conjetura de Riemann hace referencia a estos ceros no triviales afirmando.

Hipótesis de Riemann. Los ceros no triviales de la función zeta de Riemann se encuentran en la recta $\mathrm{Re}(s) = 1/2$ (recta crítica).

4.2 La función zeta de una curva elíptica sobre cuerpos finitos

Sea E una curva elíptica definida sobre $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. La *función zeta de* E es definida por la serie formal de potencias en T

$$Z(E,T) := \exp\left(\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{p^n})}{n} T^n\right).$$

Enunciamos ahora un teorema que se conoce como la conjetura de Weil, a pesar que ya ha sido demostrado. La versión general de este teorema se da en variedades proyectivas, en 1959 Bernard Dwork dió un primer avance demostrando la racionali dad de la función zeta, y posteriormente fue el matemático Pierre Deligne quien en 1973 completa la demostración.

Teorema 4.4 (Conjetura de Weil para curvas elípticas sobre cuerpos finitos)**.** *Sea E una curva elíptica definida sobre $\mathbb{F}_p$, entonces, existe un entero a_p tal que*

1. $Z(E,T) = \dfrac{1 - a_pT + pT^2}{(1-T)(1-pT)}$ *(racionalidad)*
2. $1 - a_pT + pT^2 = (1-\alpha T)(1-\beta T)$, *donde* $|\alpha| = |\beta| = \sqrt{p}$ *(hipótesis de Riemann)*
3. $Z(E, \frac{1}{pT}) = Z(E,T)$ *(ecuación funcional)*

Prueba.- Solamente probaremos las partes 2 y 3.
2.- Como $a_p, p \in \mathbb{Z}$, existen $\alpha, \beta \in \mathbb{C}$ tal que $1 - a_pT + pT^2 = (1-\alpha T)(1-\beta T)$, entonces

$$\alpha + \beta = a_p, \quad \alpha\beta = p$$

de donde

$$\alpha, \beta = \frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p}). \tag{4.3}$$

En particular, α y β son enteros algebraicos, pues son raíces de $x^2 - a_px + p \in \mathbb{Z}[x]$. Por otro lado, usando la teoría de las series formales:

$$\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{p^n})}{n} T^n = \log Z(E,T) = \log \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-pT)} = \sum_{n=1}^{\infty} (1 + p^n - \alpha^n - \beta^n)\frac{T^n}{n}.$$

Luego, igualando los coeficientes

$$\#E(\mathbb{F}_{p^n}) = 1 + p^n - \alpha^n - \beta^n; \tag{4.4}$$

en particular, $\#E(\mathbb{F}_p) = 1 + p - \alpha - \beta$, es decir

$$\#E(\mathbb{F}_p) = 1 + p - a_p. \tag{4.5}$$

Entonces vale

$$|\#E(\mathbb{F}_p) - 1 - p| = |a_p| = |\alpha + \beta| \leq 2\sqrt{p}$$

(la igualdad no puede ocurrir puesto que p es primo). Así, hemos probado que

$$|a_p| < 2\sqrt{p} \qquad \text{(teorema de Hasse).}$$

Luego $a_p^2 - 4p < 0$, es decir, el discriminante de esta ecuación cuadrática $x^2 - a_p x + p = 0$ es negativo, de donde α y β son complejos conjugados, esto es $\alpha = \overline{\beta}$ y $\alpha\beta = p$, de donde $|\alpha| = |\beta| = \sqrt{p}$.

3.-

$$\begin{aligned} Z(E, \tfrac{1}{pT}) &= \frac{(1 - \frac{\alpha}{pT})(1 - \frac{\beta}{pT})}{(1 - \frac{1}{pT})(1 - \frac{1}{T})} \\ &= \frac{(\alpha - pT)(\beta - pT)}{(1 - pT)(p - pT)} \\ &= \left(\frac{\alpha\beta}{p}\right) \frac{(1 - \frac{p}{\alpha}T)(1 - \frac{p}{\beta}T)}{(1 - pT)(1 - T)} \\ &= \frac{p}{p} \frac{(1 - \beta T)(1 - \alpha T)}{(1 - pT)(1 - T)} = Z(E, T). \end{aligned}$$

□

Observación.- Si conocemos $\#E(\mathbb{F}_p)$, de (4.5) conocemos el valor de a_p , y de (4.3) sabremos los valores de α y β, así de (4.4) podremos calcular $\#E(\mathbb{F}_{p^n})$ para cualquier entero $n \geq 1$.

4.3 La función L de Hasse-Weil de una curva elíptica

Dada la curva elíptica $E : y^2 = x^3 + ax + b$ con $a, b \in \mathbb{Z}$. La *función zeta no completa* de la curva E, es definida por

$$\zeta(E, s) = \prod_{p \notin S} Z(E/\mathbb{F}_p, p^{-s})$$

donde S es el conjunto finito de los números primos con mala reducción. Por el teorema (4.4)

$$\zeta(E, s) = \prod_{p \notin S} \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})} = \frac{\zeta_S(s)\zeta_S(s-1)}{L_S(E, s)}$$

donde $\zeta_S(s)$ es la función ζ de Riemann usual exceptuando los factores correspondientes a los primos de S y

$$L_S(E, s) = \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \prod_{p \notin S} \frac{1}{1 - \alpha_p p^{-s}} \cdot \frac{1}{1 - \beta_p p^{-s}}.$$

Como el producto $\prod_p \frac{1}{1 - p^{-s}}$ converge para $\mathrm{Re}(s) > 1$, se tiene que

$$\prod_p \frac{1}{1 - p^{\frac{1}{2}} p^{-s}}$$

converge para $\mathrm{Re}(s) > 3/2$. Y como $|\alpha_p| = |\beta_p| = p^{1/2}$, se tiene que $L_S(E, s)$ converge si $\mathrm{Re}(s) > 3/2$.

¿Qué sucede si $p \in S$ (es decir si $p|\Delta$)?. En este caso

$$a_p = 1 + p - \#E(\mathbb{F}_p) = \begin{cases} 0, & \text{caso cúspide} \\ 1, & \text{caso de nodo partido} \\ -1, & \text{caso de nodo no partido} \end{cases}$$

Definición 4.3.1. Dada la curva elíptica $E : y^2 = x^3 + ax + b$ con $A, B \in \mathbb{Z}$. Para $s \in \mathbb{C}$ se define la función L de Hasse-Weil de la curva E como

$$L(E, s) = \prod_{p \notin S} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \in S} \frac{1}{1 - a_p p^{-s}}$$

donde S es el conjunto de los números primos con mala reducción.

4.4 Rango analítico. Conjeturas

El conductor de una curva elíptica E sobre $\mathbb{Q}$, se define por

$$N_{E/\mathbb{Q}} = \prod_p p^{f_p}$$

donde

$$f_p = \begin{cases} 0, & \text{si } E \text{ tiene buena reducción módulo } p \\ 1, & \text{si } E \text{ tiene reducción multiplicativa módulo } p \\ 2+\delta_p, & \text{si } E \text{ tiene reducción aditiva módulo } p \end{cases}$$

donde $\delta_p = 0$ para $p = 2, 3$ y $\delta_p \geq 0$ en los otros casos, ver [Sil86], Apendice C, pág 361.

Definición 4.4.1. Sea E una curva elíptica sobre $\mathbb{Q}$, definimos la función $\Lambda(E, s)$ por

$$\Lambda(E, s) := N_{E/\mathbb{Q}}^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(E, s)$$

Teorema 4.5 (Conjetura de Hasse-Weil para curvas elípticas)**.** *La función $\Lambda(E, s)$ puede extenderse analíticamente a una función meromorfa en todo el plano complejo $\mathbb{C}$, y satisface la ecuación funcional*

$$\Lambda(E, s) = \pm\Lambda(E, 2 - s).$$

Continuando el trabajo de Wiles-Taylor sobre la demostración del último teorema de Fermat, en el año 1999 se anunció la demostración de la conjetura de Shimura-Taniyama-Weil (cada curva elíptica puede asociarse unívocamente con un objeto matemático denominado forma modular), y como consecuencia de ésto la veracidad de la conjetura de Hasse-Weil (para toda curva elíptica $E/\mathbb{Q}$, la función $L(E, s)$ se extiende a una función entera). Entonces, tiene sentido la siguiente interrogante;

¿qué ocurre con el valor de $L(E; s)$ en $s = 1$? (equidistante de s y $2 - s$)

Ya a principios de los años 1960's cuando aún no se sabía que $L(E; s)$ estaba definida en $s = 1$, *Birch y Swinnerton-Dyer* formularon unas conjeturas asombrosas.

Las conjeturas de Birch Swinnerton-Dyer (BSD)
Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces

1. **Conjetura BSD (débil).**
   $E(\mathbb{Q})$ tiene infinitos puntos si y sólo si $L(E,1)=0$.

2. **Conjetura BSD.**
   La función $L(E,s)$ es holomorfa en $s=1$ y el orden de anulación en $s=1$ es el rango de la curva elíptica E. Es decir,

$$\operatorname{ord}_{s=1} L(E/\mathbb{Q},s) = \operatorname{rang}(E(\mathbb{Q})$$

   el rango análitico es igual al rango algebraico

Hasta nuestros días, estas conjeturas aún no han sido demostradas, el estímulo para trabajar en ellas se ha incrementado cuando en mayo del 2000 la fundación Clay de Matemática, ofrece a la primera persona que desarrolle una demostración correcta de esta conjetura un premio de un millon de dólares. Algunos avances en esta dirección son:

Teorema 4.6 (J. Coates- A. Wiles, 1977)**.** *Sea $E/\mathbb{Q}$ una curva elíptica con multiplicación compleja. Si $E(\mathbb{Q})$ es infinito, entonces $L(E;1)=0$.*

Teorema 4.7 (Gross-Zagier-Rubin, 1983)**.** *Sea $E/\mathbb{Q}$ una curva elíptica con multiplicación compleja.*

1. *Si $L(E;1)\neq 0$, entonces* $\operatorname{rang} E(\mathbb{Q})=0$.

2. *Si $L(E;1)=0$ y $L'(E;1)\neq 0$, entonces* $\operatorname{rang}(E(\mathbb{Q}))=1$.

Teorema 4.8 (Tunnel, 1983)**.** *Si $A>0$ es un entero libre de cuadrados y $E: y^2 = x^3 - A^2x$ es la curva elíptica correspondiente, entonces:*

$$L(E,1) = \frac{a(n-2m)^2}{\sqrt{d}} C_0$$

donde $C_0 = 0,163878597\cdots$, $a=1$ ó $a=2$ según A sea impar o par respectivamente, y si

$$n = \#\big\{(x;y;z)\in\mathbb{Z}^3 : x^2+2ay^2+8z^2 = A/a\big\}$$

y

$$m = \#\big\{(x;y;z)\in\mathbb{Z}^3 : x^2+2ay^2+32z^2 = A/a\big\}.$$

Se sigue que:

- *Si $n \neq 2m$, entonces A no es congruente.*
- *Si $n = 2m$, entonces $L(E;1) = 0$, de donde* $\operatorname{rang}(E(\mathbb{Q})) \geq 1$ *(asumiendo que la conjetura de BSD sea cierta), lo cual implica que A es congruente.*

4.5 Trabajando sobre el anillo $\mathbb{Q}[t]$

Sea $\alpha_1, \alpha_2, \cdots, \alpha_8 \in \mathbb{Q}[t][x]$ distintos 2 a 2. Si

$$p := \prod_{i=1}^{8}(x - \alpha_i),$$

entonces, existen $q, r \in \mathbb{Q}[t][x]$ tales que

$$p = q^2 - r, \quad \operatorname{grad}(q) = 4 \quad \text{y} \quad \operatorname{grad}(r) \leq 3.$$

Esta escritura se obtiene simplemente considerando polinomios:

$$q = \sum_{i=1}^{4} a_i x^i \ \text{ y } \ r = \sum_{i=0}^{3} b_i x^i,$$

y planteado el sistema de ecuaciones que surge de igualar los coeficientes de p y de $q^2 - r$, obteniendo así los valores de a_i y b_i. Si resultase que $\operatorname{grad}(r) = 3$, consideramos la curva de ecuación

$$E : y^2 = r(x).$$

Si r no es mónico con un cambio de coordenadas adecuado podemos conseguir que lo sea. Si además resulta que su discriminante es no nulo, E es una curva elíptica que contiene 8 puntos conocidos, puesto que:

$$q(\alpha_i)^2 = p(\alpha_i) + r(\alpha_i) = 0 + r(\alpha_i) = r(\alpha_i),$$

es decir, los puntos con coordenadas afines $P_i = \big(\alpha_i, q(\alpha_i)\big)$ son puntos de E para $1 \leq i \leq 8$, y como el punto $\mathcal{O} = (0 : 1 : 0)$ siempre está en E, en realidad tenemos 9 puntos conocidos en esta curva elíptica.
En este momento surge la siguiente interrogante, ¿como elegir los α_i?. Si los elegimos de la siguiente forma:

$$\alpha_i = k_i \pm t, \quad 1 \leq i \leq 4 \quad \text{y} \quad k_i \in \mathbb{Q},$$

el polinomio p queda así

$$p = \prod_{i=1}^{4} \big(x - (k_i \pm t)\big).$$

Ahora, debido a la simetría que tiene p, cuando calculamos el polinomio r nos queda

$$r(x) = At^2x^3 + Bt^2x^2 + t^2(Ct^2 + D)x + t^2(Et^2 + F)$$

donde $A, B, C, D, E, F \in \mathbb{Q}$ y dependen de k_1, k_2, k_3, k_4. Tenemos entonces la curva

$$y^2 = At^2x^3 + Bt^2x^2 + t^2(Ct^2 + D)x + t^2(Et^2 + F),$$

que dividiendo por t^2 y cambiando y por $\frac{y}{t}$ nos queda

$$E : y^2 = Ax^3 + Bx^2 + (Ct^2 + D)x + (Et^2 + F).$$

Lo que hay que hacer ahora, es elegir los k_i de manera que $A \neq 0$ y $\triangle \neq 0$; para que E sea efectivamente una curva elíptica. Una vez que nos aseguramos que E es realmente una curva elíptica, consideramos los 9 puntos que ya conocemos, y le aplicamos la forma bilineal de Neron-Tate para ver cuántos de ellos son $\mathbb{Z}$-independientes. Así, eligiendo

$$k_1 = 1, k_2 = -2, k_3 = 8 \quad \text{y} \quad k_4 = -4$$

obtenemos la curva elíptica sobre $\mathbb{Q}(t)$ de ecuación afín

$$E : y^2 = 12x^3 + 88x^2 + (-12t^2 + 96)x + 9t^2$$

donde los puntos P_i resultan ser:

$$\begin{aligned} P_1 &= (1 + t, -11t - 14) & P_2 &= (1 - t, -11t + 14) \\ P_3 &= (-2 + t, -7t + 8) & P_4 &= (-2 - t, -7t - 8) \\ P_5 &= (8 + t, 17t + 112) & P_6 &= (8 - t, 17t - 112) \\ P_7 &= (-4 + t, t - 16) & P_8 &= (-4 - t, t + 16) \end{aligned}$$

y son linealmente independientes, puesto que el determinante de la forma bilineal de Neron-Tate definida sobre $\mathbb{Q}(t)$ es diferente de cero. Ver [Sil94] capítulo III, teorema 4.3. Sorprendentemente, de una manera sencilla, hemos conseguido una familia de curvas elípticas de rango ≥ 8. En particular para $t = 1$, la curva

$$E : y^2 = 12x^3 + 88x^2 + 96x + 9$$

contiene los puntos

$$\begin{aligned} P_1 &= (2, -25) & P_2 &= (0, 3) \\ P_3 &= (-1, 1) & P_4 &= (-3, -15) \\ P_5 &= (9, 129) & P_6 &= (7, -95) \\ P_7 &= (-3, -15) & P_8 &= (-5, 17) \end{aligned}$$

4.6 Modelo cuártico de una curva elíptica

Una definición un poco desconocida de una curva elíptica, es el conjunto de puntos en el espacio proyectivo $\mathbb{P}_3(K)$ satisfaciendo

$$X_0X_3 = X_1^2 \quad \text{y} \quad X_2^2 = a_4X_3^2 + a_3X_3X_1 + a_2X_0X_3 + a_1X_1X_0 + a_0X_0^2,$$

donde $a_4 \neq 0$. Deshomogenizando respecto a la variable X_0, vemos que el modelo afín para esta curva es

$$y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Por esta razón, nos referiremos a este modelo de una curva elíptica, como el *modelo cuártico* y los puntos con $X_0 \neq 0$ son los puntos afines. Si $X_0 = 0$, entonces debe ser que $X_1 = 0$ y vemos que los puntos de $\mathcal{O}' = (0 : 0 : \sqrt{a_4} : 1)$ y $\mathcal{O} = (0 : 0 : -\sqrt{a_4} : 1)$ son puntos de la curva, llamados los puntos en el infinito para este modelo de la curva.

Por dehomogenización ya sea en X_0 o en X_3, se comprueba que esta curva es no singular en cada uno de sus puntos, incluyendo los puntos en el infinito $\mathcal{O}'$ y $\mathcal{O}$, si y sólo si la función

$$f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

no tiene ninguna raíz doble.

Si $f(x)$ no tiene raíces dobles, entonces la curva es no singular y tiene un género uno. Por lo tanto, si los coeficientes de $f(x)$ se encuentran en un cuerpo K y la curva contiene un punto K-racional, entonces este modelo describe una curva elíptica definida sobre K. Además, si a_4 es un cuadrado en K, entonces los dos

puntos en el infinito son K-racionales.

Estos dos modelos (cúbico y cuártico) de una curva elíptica nos da una mayor flexibilidad cuando se trata de la *construcción de las curvas elípticas de rango alto*. Sin embargo como toda nuestra teoría usa el modelo de Weierstrass, se puede utilizar el teorema de Riemann-Roch, para probar que toda curva elíptica puede ser puesta en la forma de Weierstrass. Ahora daremos a la transformación birracional que lleva el modelo cuártico en un modelo cúbico en la forma de Weierstrass.

Para transformar una cuártica de la forma

$$a^2x^4 + bx^3 + cx^2 + dx + e = y^2$$

a la forma de Weierstrass, sea $q = [a, b, c, d, e]$ (tenga en cuenta que la primera componente es a y no a^2). El comando *Wtrs* da la 5-tupla que representa la curva elíptica en la forma de Weierstrass $[a1, a2, a3, a4, a6]$

```
Wtrs(q)=[0, q[3], 0, q[2]*q[4]-4*q[1]^2*q[5],\\
                        q[2]^2*q[5]+q[1]^2*q[4]^2-4*q[1]^2*q[3]*q[5] ]
```

esto es

$$y^2 = x^3 + cx^2 + (bd - 4a^2e)x + (b^2e + a^2d^2 - 4a^2ce).$$

La función *newp* toma un punto, $P = [P[1], P[2]]$, en el modelo cuártico y devuelve un punto de la curva elíptica en forma de Weierstrass dada por *Wtrs*.

```
newp(q,P) =
           x1=P[1];
           y1=P[2];
           [-2*q[1]*y1+2*q[1]^2*x1^2+q[2]*x1,
                                                4*q[1]^2*x1*y1
                                                +q[2]*y1
                                                -4*q[1]^3*x1^3
                                                -3*q[1]*q[2]*x1^2
                                                -2*q[1]*q[3]*x1
                                                -q[1]*q[4]];
```

4.7 Una curva de rango ≥ 14

El método expuesto en esta sección es debido a Fermigier [**?**]. Sea $n \in \mathbb{N}$ tal que

$$n = p_1 p_2 p_3,\ p_i \text{ primo},\quad p_i \equiv 1(\mod 4)$$

existe entonces cuatro pares de números enteros

$$(a_1, b_1), (a_2, b_2), (a_3, b_3), (a_4, b_4)\ \ /\ \ a_i^2 + b_i^2 = n$$

Luego escribimos

$$x_i := -a_i^2 b_i^2 \quad i = 1, 2, 3, 4.$$

Para $P(x) = \prod_{i=1}^{4}(x - x_i)$, existen $Q(x)$ y $R(x)$ polinomio de grados 2 y 1 respectivamente tales que $P(x) = Q(x)^2 - R(x)$, esto es

$$P(x) = \prod_{i=1}^{4}(x - x_i) = Q(x)^2 - R(x) = (x^2 + d_1 x + d_0)^2 - (Ax + B)$$

y como $P(x_i) = 0$

$$ax_i + B = Q(x_i)^2 \quad i = 1, 2, 3, 4.$$

Por otro lado considere la curva

$$\mathcal{C} : y^2 = A(x^4 - nx^2) + B = Ax^2(x^2 - n) + B.$$

Para $x = a_i$

$$Aa_i^2(a_i^2 - n) + B = Aa_i^2(-b_i^2) + B = Ax_i + B = Q(x_i)^2$$

esto es

$$(a_i, Q(a_i)) \in \mathcal{C} \quad i = 1, 2, 3, 4.$$

Análogamente

$$(b_i, Q(b_i)) \in \mathcal{C} \quad i = 1, 2, 3, 4.$$

En particular para $n = 6210037 = 73 \cdot 97 \cdot 877$, obtenemos los pares $(359, 2466)$, $(649, 2406)$, $(1351, 2094)$ y $(1386, 2071)$. Por lo tanto

$$\begin{aligned} x_1 &= -783745466436, \quad x_2 = -2438263512036, \\ x_3 &= -8003207052036, \quad x_4 = -8239230604836. \end{aligned}$$

Si $x^4+c_3x^3+c_2x^2+c_1x+c_0 = P(x) = Q(x)^2 - R(x) = (x^2+d_1x+d_0)^2 - (Ax+B)$, entonces

$$d_1 = \frac{1}{2}c_3, \quad d_0 = \frac{1}{2}(c_2 - d_1^2), \quad A = 2d_0d_1 - c_1 \text{ y } B = d_o^2 - c_0.$$

En nuestro caso

$$\begin{aligned} A &= -28547814, \\ B &= -21926930204749905279, \\ y^2 &= A(x^4 - 6210037x^2) + B \end{aligned}$$

esto es

$$y^2 = -28547814x^4 + 1772829812091l8x^2 - 21926930204749905279,$$

que tiene grupo de torsión $\mathbb{Z}/2\mathbb{Z}$ y rango al menos 14, es decir

$$E(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}^r \qquad \text{con } r \geq 14.$$

Los generadores están dados por las x-coordenadas

$$359, -359, 649, 1351, 1386, 1694, 2071, 2094, 2406, 2466,$$
$$\frac{12331}{5}, \frac{24355}{19}, \frac{43190}{67}, \frac{55578}{43} \text{ y } \frac{62021}{97}.$$

4.8 Una curva de rango ≥ 21

Teorema 4.9 (Nagao-Kouya, 94)**.** *Sea E la curva elíptica*

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

donde

$$\begin{aligned} a &= -215843772422443922015169952702159835, \\ b &= -194743612777871519472559614354590541515017922413205 35. \end{aligned}$$

Entonces,

$$\text{rang}\left(E(\mathbb{Q})\right) \geq 21$$

Demostración. En PARI/GP, ingresamos la curva de la forma

```
E = ellinit([1,1,1, - 215843772422443922015169952702159835, \\
    - 194743612777871519472559614354590541515017922413205 35 ]);
```

Luego ingresamos los 21 puntos encontrados por Nagao-Kouya en el año 1994.

```
P1 = [800843008889340065933/16, 22662214190910903990783584765347/64]
P2 = [10610541066763914590637/2209,10877441148251784548400947780 34/103823]
P3 = [907186946780634143, 728916386168451830641677698]
P4 = [19683320108556444219408 3107/227919409,
     22778073989304408195874101847939237638 94/3440899317673]
P5 = [18546347413906465252800 0075/366301321,
     22569985783858324284947383046648197 8146/7010640982619]
P6 = [-12485261071234691432503/123904,
     15433033534289399822821717527025 39/43614208]
P7 = [-59703014087684747037/361, 74188124509415406852503612696 2/6859]
P8 = [-73270463404799613067/361, 86687813785863879289111794348 2/6859]
P9 = [-360733396398627565, 10698584048409672894788397 4]
P10 = [-389445180957906897, 74288355118790673852542098]
P11 = [-14744583503498585126654 07/14205361,
      22784934015783680843104090282593326 32/53540005609]
P12 = [-11430585603546889269177927 7/278589481,
      16972779768877136292841029663998709 5378/4649937027371]
P13 = [-21972533600828202797/81, 10079078658496350456387600530 2/729]
P14 = [-25047938415396324842058977/71216721,
      68347192566984943007522052612937752062/600997908519]
P15 = [34348280818851183522137152847 07/5137262501809,
      42799124838389250442349391653296975768124338 46/116438777352626943 77]
P16 = [-227656313261676647, 13366002432726894909529 7798]
P17 = [-40980894341059921378352 93/12552849,
      56600884139913517593014036598908897 06/44474744007]
P18 = [26578287358691780202126 17/1495729,
      41744997315499971865961317212732013 76/1829276567]
P19 = [88396500431424342412499 4323/850947241,
      23250077986002214917145041708721276812178/24822981967211]
P20 = [37543938941728172090 03/73441,
      12240979159912800999038364900202 98/19902511]
P21 = [19165312347502458410162233/17214201,
      75593839815741485450348997055551694952/71421719949]
```

Ahora verificamos que el determinante de la matriz de Gram $\big(\langle P_i, P_j\rangle\big)_{1\leq i,j\leq 21}$ asociado a la altura canónica de Néron-Tate sea distinto de cero.
En efecto, al digitar

```
matdet(ellheightmatrix(E,[P1,P2,P3,P4,P5,P6,P7,P8,P9,P10, \\
    P11,P12,P13,P14,P15,P16,P17,P18,P19,P20,P21]));
```

obtenemos que el determinante de la matriz $\big(\langle P_i, P_j\rangle\big)_{1\leq i,j\leq 21}$ es

$$1057662683061657998079887,489.$$

siendo este determinante distinto de cero, vemos que los puntos $P_1, P_2, \cdots, P_{21}$ son independientes. Así el rango de esta curva es ≥ 21. □

4.9 El récord

Teorema 4.10 (Elkies, 2006)**.** *Sea E la curva elíptica dada por*

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

donde

$$\begin{aligned} a &= -2006776241557552658503320820933854275093023031217895650 2 \\ b &= 3448161179503055646703298569039072037485594435931918036126 6008296291939448732243429. \end{aligned}$$

Entonces,

$$\operatorname{rang}\big(E(\mathbb{Q})\big) \geq 28$$

Demostración. En PARI/GP, ingresamos la curva de la forma

```
E=ellinit([1,-1,1,- 2006776241557552658503320820933854275093023\\
0312178956502, 3448161179503055646703298569039072037485594435\\
9319180361266008296291939448732243429]);
```

Luego ingresamos los 28 puntos encontrados por Elkies en el año 2006.

```
P1 = [-212415009125438107329213746 3, 259854492051899599030515511 0707\\
                                                        80628911531]
P2 = [233450986603470175688475453 7, 188720041954944691808683165 52803\\
                                                        627931531]
```

```
P3 = [-16717360540623690638790386 63, 25170937726114428780850694724131\\
                                                        9126049131]
P4 = [213913026013915666649298213 7, 366395091714397292024214596929412\\
                                                          97527531]
P5 = [153470676446712072388547733 7, 85429585346017694289021032862781 0\\
                                                          72799531]
P6 = [-27310794878756770333415750 63, 26252181548433219164128407262390\\
                                                        2143387531]
P7 = [27757262668445716497054585 37, 12845755474014060248869487699082 6\\
                                                          40369931]
P8 = [14943857293271889575418338 17, 88486605527733405986116494514049 2\\
                                                          33411451]
P9 = [18684382286208873585090652 57, 59237403214437708712725140393059 3\\
                                                          58589131]
P10 = [20089451088257437748665425 37, 47690677880125552882151750781541\\
424711531]
P11 = [23483605409180251696516329 37, 17492930006200557857340332476448\\
                                                        804363531]
P12 = [-14720840070904811744700086 63, 24664345065350371419994744154975\\
                                                        9798469131]
P13 = [29241286077080612133632889 37, 28350264431488878501488356474767 3\\
                                                          75899531]
P14 = [53749938910660618932939345 37, 28618890842726338645117503191647 98\\
                                                          93731531]
P15 = [17096907682333545233340085 57, 71898834974686089466159700529215 98\\
                                                          0921631]
P16 = [24509540113535931440725951 87, 44452281735326343570492625506107 1\\
                                                          4736531]
P17 = [29692547092735591674646749 37, 32766893075366270801333682543160 4\\
                                                          69687531]
P18 = [27119149349416926013328829 37, 20684366127783816986504139815065 90\\
                                                            613531]
P19 = [20078586077996854528778328 937, 27796085411378066046560517256246 24\\
                                                          030091531]
```

```
P20 = [215808245024073477431781069 7, 34994373401964026809969662241800 90\\
                                                                  1254731]
P21 = [200464545824705902240322493 7, 48049329780704645522439866999888 47\\
                                                                  5467531]
P22 = [297574945094799626494709133 7, 33398989826075322320208934410104 85\\
                                                                  7869131]
P23 = [-210249046768628515014734786 3, 25957639145987578957167739317168 72\\
                                                                  03227531]
P24 = [311583179915063034902194537, 16810438522998060354010947291566015\\
                                                                  3473931]
P25 = [277393100834186523144377181 7, 12632162834649921002414116273769 27\\
                                                                  5813451]
P26 = [215658118814376840936346138 7, 35125092964022908897004150516375 17\\
                                                                  8087331]
P27 = [386633049987241250881565913 7, 12119775565594422629303692671502 584\\
                                                                  7322531]
P28 = [223086828977357602377867873 7, 28558760030597485663387020600768 64\\
```

Ahora verificamos que el determinante de la matriz de Gram $\left(\langle P_i, P_j\rangle\right)_{1\leq i,j\leq 28}$ asociado a la altura canónica de Néron-Tate sea distinto de cero.
En efecto, al digitar

```
matdet(ellheightmatrix(E,[P1,P2,P3,P4,P5,P6,P7,P8,P9,P10,P11,P12,\\
P13,P14,P15,P16,P17,P18,P19,P20,P21,P22,P23,P24,P25,P26,P27,P28]));
```

obtenemos que el determinante de la matriz de gram $\left(\langle P_i, P_j\rangle\right)_{1\leq i,j\leq 28}$ es

$$3.857298234011609195578842652E34$$

y como este determinante es distinto de cero, vemos que los puntos $P_1, P_2, \cdots, P_{28}$ son independientes. Así el rango de esta curva es ≥ 28. □

Teorema 4.11 (**Eroshkin, 2011**). *Sea E la curva elíptica dada por*

$$y^2 + xy + y = x^3 - x^2 - 27329823028740498697734567519340 2x$$

$$+17639927528931247421878527659308327326261926287 29.$$

Entonces,

$$\text{rang}\left(E(\mathbb{Q})\right) \geq 5.$$

Demostración. En PARI/GP, ingresamos la curva en la forma

```
E=ellinit([1,-1,1,-2732982302874049869773456751934 02,
 1763992752893124742187852765930832732626192628729])
```

Luego ingresamos los 5 puntos encontrados por *Eroshkin* en el año 2011.

```
P1 = [2917519700212787, 995727611790608931699581]
P2 = [9749082105993237, 161813140897747451659631]
P3 = [16971589375305737, 141918868307673495765963 1]
P4 = [-29969163375951083/16, 964114642824423013521795 09/64]
P5 = [1058329448500103470 03/1089, 1073950829336930074855988831717/35937]
```

Ahora verificamos que el determinante de la matriz de Gram $\big(\langle P_i, P_j\rangle\big)_{1\leq i,j\leq 5}$ asociado a la altura canónica de Néron-Tate sea distinto de cero.
En efecto, al digitar

```
matdet(ellheightmatrix(E,[P1,P2,P3,P4,P5]))
```

obtenemos que el determinante de la matriz de Gram es $353306.3608288494940919466962 \neq 0$. Por lo tanto los puntos $P1, P2, P3, P4, P5$ son independientes. Así, $\text{rang}\big(E(\mathbb{Q})\big) \geq 5$. □

Conclusiones

- Utilizando el espacio proyectivo hemos construido un grupo abeliano no trivial, objeto de nuestro estudio. Demostramos tambien que el conjunto de los puntos racionales de una curva elíptica es un grupo finitamente generado.

- Hemos visto que un entero n es un número congruente, si y sólo si existe una solución no trivial de una curva elíptica particular.

- Utilizando la forma bilineal de Néron-Tate se dio condiciones suficientes para que un conjunto finito de puntos de una curva elíptica sea $\mathbb{Z}$-independiente, generando así una cota inferior para el rango de esa curva.

- Sea explica la famosa conjetura de Birch Swinnerton-Dyer, que hasta hoy es un problema sin resolver, con un premio de un millon de dólares ofrecido por el instituto de matemáticas Clay.

- Utilizando el sistema de cálculo PARI/GP se ha corroborado el récord de rango de las curvas elípticas.

- De igual forma utilizando también PARI/GP, se ha corroborado que existen curvas elípticas para cada uno de los quince grupos descritos por Barry Mazur.

- La presente es una línea de investigación vigente que engloba muchas áreas de la matemática como la teoría de números análitica y algebraica, el análisis complejo, la geometría algebraica y diferencial, la topología, el algebra conmutativa, etc.

- Porqué no mencionar una de las aplicaciones del futuro, *la criptografía con curvas elípticas*; se espera que las empresas migren a su utilización en los próximos años.

Bibliografía

[EW05] Graham Everet and Thomas Ward. *An Introduction to Number Theory*. Springer Verlag, 2005.

[Fer92a] S. Fermigier. Un exemple de courbe elliptique definie sur q de rang $\geq$ 19. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 315(6):719–722, 1992.

[Fer92b] S. Fermigier. Zéros des fonctions l de courbes elliptiques. *Experimental Mathematics*, 1(2):167–173, 1992.

[Fer96] S. Fermigier. Étude experimentale du rang de familles de courbes elliptiques sur. *Experimental Mathematics*, 5:119–130, 1996.

[Fer97] Stéfane Fermigier. Une courbe elliptique définie sur $\mathbf{Q}$ de rang ≥ 22. *Acta Arith.*, 82(4):359–363, 1997.

[Kna92] Anthony W. Knapp. *Elliptic curves*. Princeton University Press, 1992.

[KS01] Leopoldo Kulesz and Colin Stahlke. Elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. *Experiment. Math.*, 10(3):475–480, 2001.

[Kul03] Leopoldo Kulesz. Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. *Acta Arith.*, 108(4):339–356, 2003.

[NK94a] K. Nagao and T. Kouya. An example of elliptic curve over \ mathbf {Q} with rank $>$ 21. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 70(4):104–105, 1994.

[NK94b] K. Nagao and T. Kouya. An example of elliptic curve over $\mathbb{Q}$ with rank $>$ 21. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 70(4):104–105, 1994.

[PAR11] PARI Group, Bordeaux. *PARI/GP, versión* `2.5.0`, 2011. disponible en `http://pari.math.u-bordeaux.fr/`.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, 1986.

[Sil94] Joseph H. Silverman. *Advanced Topics in the aritmetic of Elliptic Curves*. Springer Verlag, 1994.

[Sim11] Denis Simon. Programa de cálculo del rango de curvas elípticas, 2011. disponible en `www.math.unicaen.fr/~simon/ellQ.gp`.

[Was08] Lawrence C. Washington. *Elliptic curves: number theory and criptography*. Chapman & Hall/CRC, Boca Raton, FL, 2008.