# Conjetura de Birch y Swinnerton-Dyer

Javier Silva

Diciembre 2021

# Índice general

# Introducción

Durante miles de años la matemática como disciplina ha invertido gran esfuerzo en el estudio de ecuaciones. Más específicamente, se ha investigado y desarrollado múltiples herramientas y perspectivas para encontrar soluciones enteras o racionales. Por ejemplo, Euclídes dió una respuesta completa y satisfactoria acerca de las soluciones enteras de $x^n + y^n = z^n$ para $n = 2$. Sin embargo, el problema se vuelve inmensamente complicado para potencias mayores de $n$, prueba de ello es que pasaran aproximadamente 350 años desde que Fermat afirmara que no habían soluciones enteras positivas para el caso $n \geq 3$, hasta que Andrew Wiles lograra una demostración en 1995. Esta demostración requirió múltiples y avanzadas herramientas de distintas áreas, a primera vista no relacionadas, más allá del alcance de cualquier matemático contemporáneo a Fermat. En un ámbito más general, en 1970 Yu. V. Matiyasevich demostró que el décimo problema de Hilbert era insoluble, es decir, no existe un algoritmo general que indique si existen soluciones enteras para cualquier ecuaciíon polinomial diofantina dada. Sin embargo, en casos especificos existen avances satisfactorios en el estudio de la solubilidad de ecuaciones, y es aquí donde entra la conjetura titular.

La conjetura de Birch y Swinnerton-Dyer (que de ahora en adelante abreviaremos BSD) fue propuesta por los matemáticos británicos Bryan John Birch y Peter Swinnerton-Dyer, en 1965. Es uno de los problemas abiertos más importantes para la matemática contemporánea, tanto así que el Clay Mathematics Institute la incluyó como uno de sus 7 Problemas del Milenio, con una recompensa de un millón de dólares por resolverla. Reminiscente a la lista de 23 problemas de Hilbert, esta lista de 7 problemas tiene como objeto incentivar y guíar la investigación matemática contemporánea. En particular, la conjetura BSD trata acerca de curvas elípticas y sus soluciones racionales.

La conjetura BSD es uno de los problemas más abiertos dificiles de resolver en la actualidad y entender su enunciado requiere un nivel considerable de conocimiento técnico. El objetivo de este trabajo es posicionar la conjetura BSD de manera expedita y amigable al alcance de un estudiante de pregrado. El lector sólo necesitará conocimientos elementales de teoría de grupos, teoría de anillos y análisis complejo. Se proporcionarán e ilustrarán los conceptos necesarios, se enunciará la conjetura y se expondrán los avances que se han logrado para resolverla.

# Capítulo 1

# Curvas Elípticas

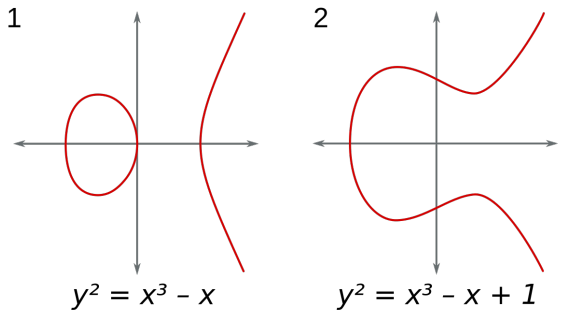
Las curvas elípticas son en sí objeto de extenso estudio presentes en múltiples áreas de la matemática y poseen gran utilidad teórica y práctica. Por ejemplo, en el ámbito de la criptografía (que se encarga de la seguridad y codificación de comunicación informática), la Criptografía de Curva Elíptica (ECC, por sus siglas en inglés) proporciona un nivel de seguridad equivalente al método RSA mientras que es más rápida y asequible computacionalmente. Se cree que su implementación como método estándar será inevitable dado el avance exponencial de la tecnología y computación (y con ello, la habilidad de hackear la seguridad informática actual que proporciona el método RSA). Así como la ECC, hay muchos algoritmos que usan curvas elípticas, por ejemplo: Elliptic-curve Diffie–Hellman key exchange, Supersingular isogeny key exchange, Elliptic curve digital signature algorithm, EdDSA digital signature algorithm etc...

El estudio de las curvas elípticas puede rastrearse hacia los antiguos griegos y ha tenido grandes avances en el siglo XX gracias al desarrollo de la teoría de números, análisis complejo y geometría algebraica. Estando presente bajo la lupa de distintas perspectivas matemáticas, admite múltiples definiciones (que se complementan o implican entre sí). Nosotros ocuparemos la siguiente:

**Definición 1.** *Sea $k$ un cuerpo. Una curva algebraica $E$ sobre $k$ es una curva cúbica no-singular $f(x, y) = 0$ con coeficientes en $k$, junto con un punto especificado $\mathcal{O}$ "al infinito".*

Un ejemplo prototípico es $y^2 = x^3 + ax + b$, con $a, b \in k$.

Figura 1.1: Ejemplo de curva elíptica



**Observación 1.** El término "no-singular" (o "suave") significa que sus derivadas parciales no se anulan. En el caso $k = \mathbb{R}$ esto es familiar. En contextos más generales, se definen las derivadas parciales sobre anillos de polinomios tal que se cumplan las reglas usuales de cálculo, es decir, acomodamos la definición para nuestros propósitos. En el ejemplo superior, "no singular" equivale a que $4a^3 + 27b^2 \neq 0$, es decir, discriminante $\Delta$ no nulo.
En cualquier caso, este concepto se traduce geométricamente en que la curva no tenga auto-intersecciones o cúspides.

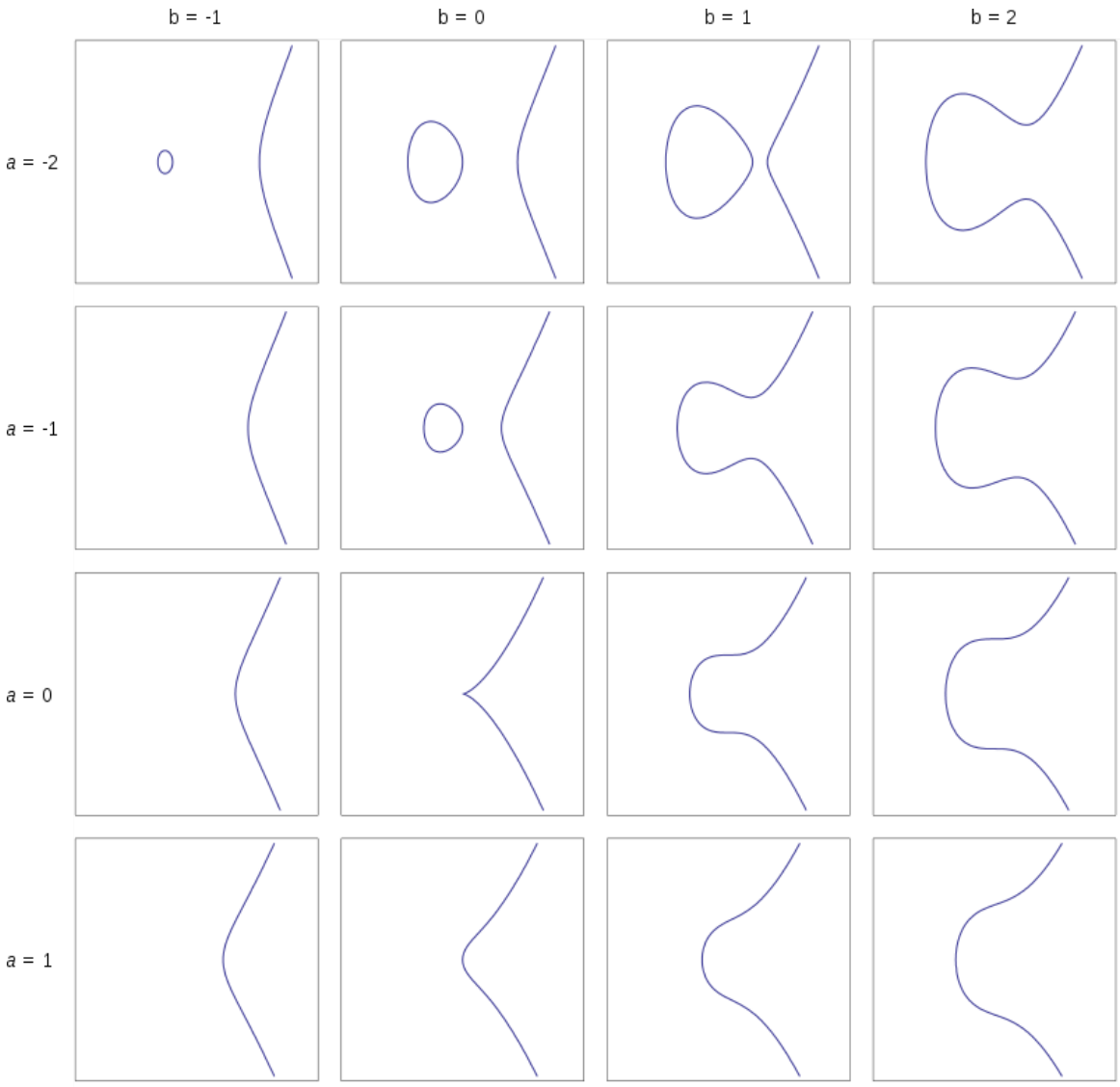
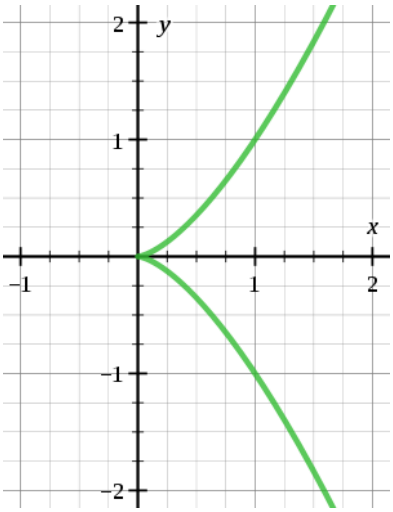



Figura 1.2: Un catálogo de curvas elípticas. Se muestra la región $[-3, 3]^2$. Para $(a, b) = (0, 0)$ la función no es suave, por lo que **no** es una curva elíptica.

Figura 1.3: Ejemplo de una cúspide, para la parábola semi-cúbica $x^3 - y^2 = 0$. Esta curva **no** es elíptica.




Con herramientas de geometría algebraica se puede demostrar que las curvas elípticas son especiales, en el sentido que se les puede asignar una ley (que denotaremos simplemente "+") entre sus elementos que la convierten en un grupo abeliano escrito aditivamente. Es posible encontrar de manera explicita esta ley, sin embargo esto escapa del propósito de este trabajo. Por suerte, es bastante fácil visualizarla geométricamente:

Figura 1.4: Definimos el punto al infinito $\mathcal{O}$ como la identidad para $+$. Como la curva elíptica es simétrica respecto al eje horizontal, para todo $P \in E$ definimos $-P$ como el punto opuesto a $P$ en la curva, así $P + (-P) = \mathcal{O}$.

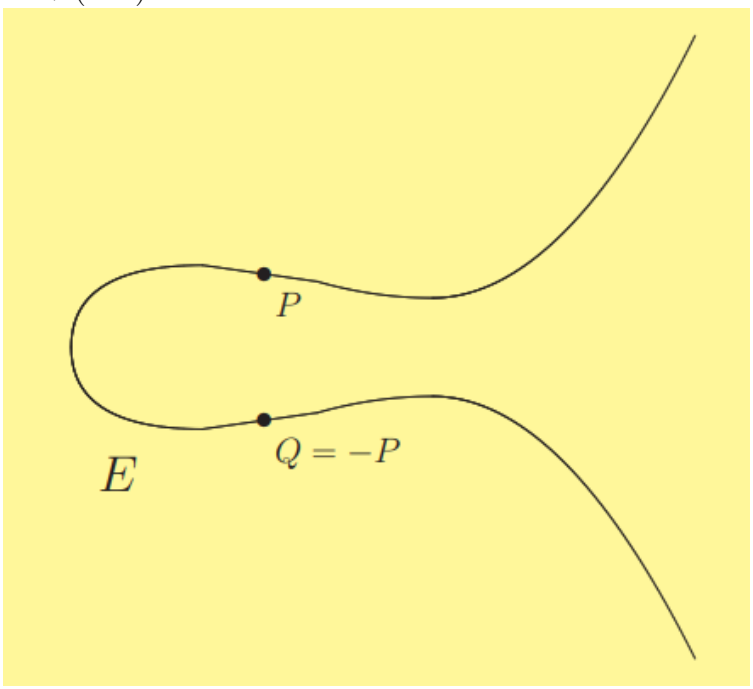


Figura 1.5: Tomamos $P, Q \in E$, los unimos con una recta y vemos que ésta intersecta a $E$ en un único punto $R$. Definimos entonces $P + Q := -R$

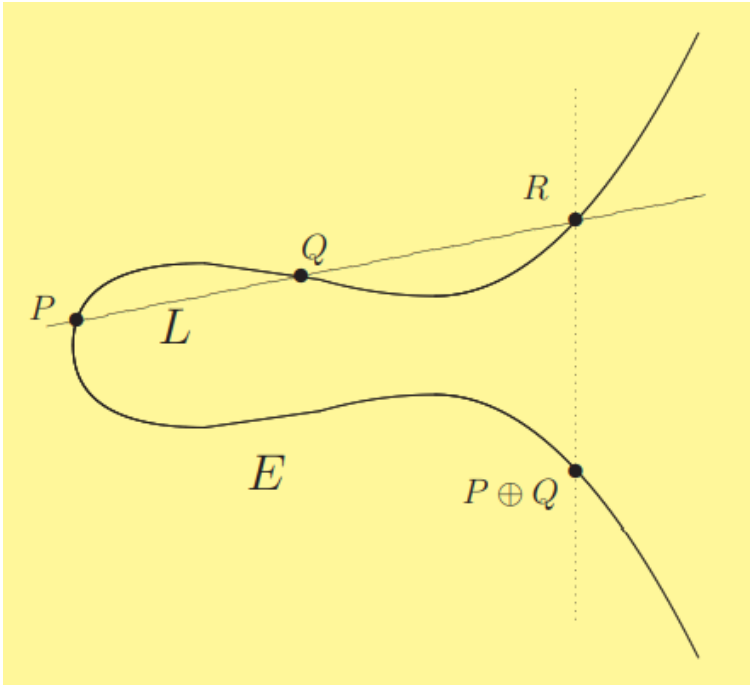



Figura 1.6: Si $P = Q$, tomamos la recta $L$ tangente a $E$ en $P$, la cual intersectará a $E$ en un punto $R$. Definimos así $P + P := -R = 2P$

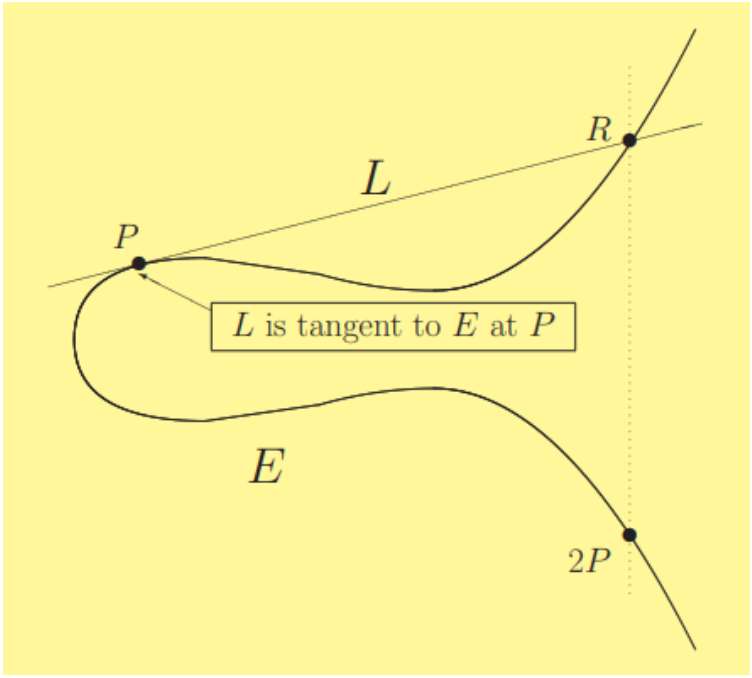
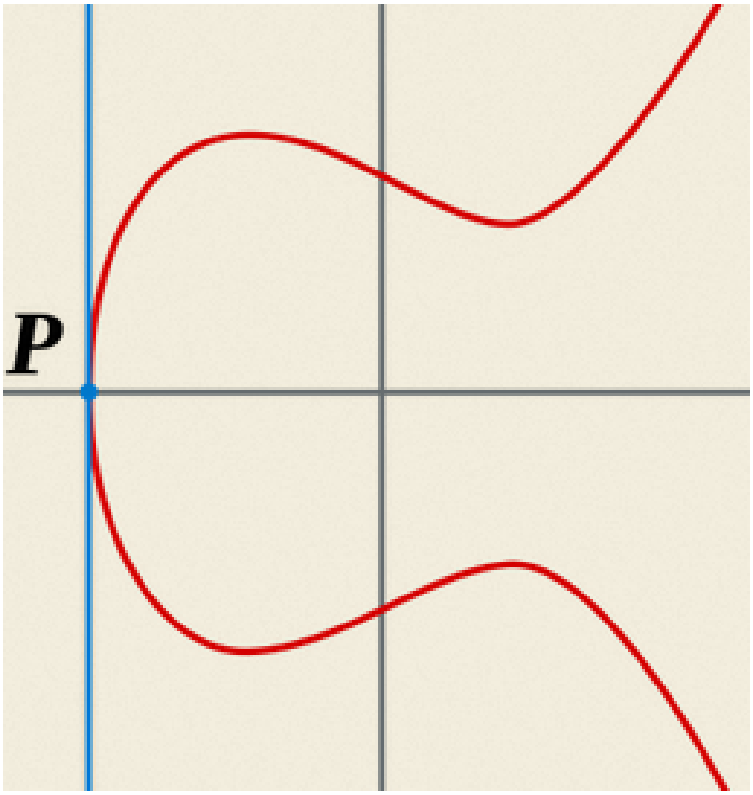


Figura 1.7: Puede suceder que la recta tangente a $E$ en $P$ no intersecte a $E$, por ejemplo cuando $P$ es un punto de inflexión. Tomamos $R := P$ en el caso anterior y así $P + P$ es opuesto a sí mismo.




**Teorema 1.** *La tupla* $(E, +)$ *es un grupo abeliano.*

# Capítulo 2

# Puntos racionales sobre curvas elípticas

En la introducción comentamos que hay gran interés matemtático en encontrar soluciones enteras o racionales a ecuaciones. Ahora abordaremos la tarea de encontrar puntos racionales en una curva elíptica.

**Definición 2.** *Decimos que un punto* $(a, b)$ *en el plano es racional si* $a, b \in \mathbb{Q}$. *Llamamos racional a una curva planar* $f(x, y) = 0$ *si* $f \in \mathbb{Q}[X, Y]$.

Si consideramos una recta racional

$$ax + by + c = 0,$$

se puede deducir que la recta que pasa entre dos puntos racionales es racional, y la intersección de dos rectas (no paralelas) racionales da un punto racional. Si intersectamos una recta racional con una cúbica racional (por ejemplo, una curva elíptica) el(los) punto(s) de intersección no tienen por qué ser racionales. Sin embargo, si podemos encontrar dos puntos racionales en una curva elíptica $E$, podemos encontrar un tercero;

Si conocemos $P, Q \in \mathbb{Q}$ sobre $E$ los unimos a través de una recta, esta recta será racional e intersecta a $E$ en un tercer punto. Estamos buscando soluciones a un sistema

$$\begin{cases} ax+by+c=0 \\ x^3+dx+e=y^2 \end{cases}$$

Al intentar resolver este sistema, obtenemos una ecuación cúbica $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$. Por construcción sabemos que $P$ y $Q$ son raíces de esta ecuación, así nos permitimos escribir $(x - P)(x - Q)(x - R) = 0$. A priori, no sabemos si $R$ es racional, sin embargo observamos que al factorizar la ecuación cúbica por $(x - P)$ nos queda un polinomio cuadrático, digamos $ax^2 + bx + c$, con $Q$ como una de sus raíces, y sabemos que la suma de las raíces es igual a $-b/2a$. Es decir $Q + R = -b/2a \in \mathbb{Q}$ por hipótesis, por lo que necesariamente $R \in \mathbb{Q}$.

**Definición 3.** *Sea $E$ curva elíptica sobre un cuerpo $k$ con punto al infinito $\mathcal{O}$. Denotamos* $E(k) := \{(x, y) \in E \text{ tal que } x, y \in K\} \cup \{\mathcal{O}\}$.

En particular, nos hemos ocupado de indagar en $E(\mathbb{Q})$. En efecto, acabamos de mostrar que la tupla $(E(\mathbb{Q}), +)$ tiene cerradura. Con un poco más de trabajo se puede demostrar que $(E(\mathbb{Q}), +)$ hereda las propiedades del grupo $(E, +)$, por lo tanto tenemos:

**Teorema 2.** *(Poincaré, 1900)* $(E(\mathbb{Q}), +)$ *es un subgrupo de* $(E, +)$.

Todo esto nos da cuenta de algo trascendental; tenemos un objeto análitico que tiene tiene propiedades algebraicas, dando cuenta que áreas como análisis y algebra están conectadas. Indagar más en el tópico de curvas elípticas nos presentaría más aristas interconectadas en este ámbito, como problemas aritméticos relacionados e incrustaciones de estas curvas en espacios complejos (análisis complejo), espacios proyectivos (geometría algebraica y topología).

Ahora que sabemos que $(E(\mathbb{Q}), +)$ es un grupo, podemos usar la teoría de grupos para nuestra ventaja. En particular, podríamos preguntarnos, ¿cuántos puntos racionales en $E$ necesitamos conocer de antemano para poder generarlos todos? Aquí es donde presentamos un magno teorema:

**Teorema 3.** *(Mordell, 1923)*

*El (sub)grupo (abeliano)* $(E(\mathbb{Q}), +)$ *es finitamente generado.*

Entonces, solo necesitamos conocer un conjunto finito de puntos racionales en $E$ para obtenerlos todos.
La idea de la demostración es la siguiente: mostrar que el grupo cociente $E(\mathbb{Q})/mE(\mathbb{Q})$ es finito para todo $m > 1$. Luego, definir una función $h$ (llamada función "altura") en $E(\mathbb{Q})$, imponiendo $h(\mathcal{O}) = 0$ y $h(P) = \log \text{máx}\{|p|, |q|\}$, con $P = (x, y)$ y $x = p/q$ ($p$ y $q$ coprimos). Se muestra que $h(mP)$ crece aproximadamente como $m^2$ y que dada una una constante arbitraria $c > 0$, existen (sólo) un número finito de puntos racionales en $E$ con "altura" $h$ menor que $c$. Finalmente, se aplica una variación de descenso infinito; se aplican sucesivamente divisones euclídeas a un punto racional $P$ hasta llegar a una combinación lineal de elementos en el grupo cociente, cuyos factores tienen alturas acotadas. Con todo esto, se llega a que $P$ es una combinación lineal de finitos factores racionales. De cualquier manera, el rango es un invariante importante de $E$.

Como $(E(\mathbb{Q}), +)$ es finitamente generado, podemos aplicar el Teorema Fundamental De Los Grupos Abelianos Finitamente Generados y obtener:

**Corolario 1.** $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})^{tors}$, *donde* $r \geq 0$ *y* $E(\mathbb{Q})^{tors}$ *es el grupo torsión de* $E(\mathbb{Q})$, *es decir, el grupo abeliano finito de los elementos de orden finito.*

**Definición 4.** *Con la notación anterior, llamamos a $r$ el rango de la curva elíptica.*

**Observación 2.** Notar que si el rango de $E$ es $r > 0$ entonces $E(\mathbb{Q})$ es infinito, por otro lado si el rango es $r = 0$, $E(\mathbb{Q})$ es finito. Otra manera (equivalente) de definir el rango de $E$ es como el número de elementos basales con orden infinito.

# Capítulo 3

# Conjetura BSD -Versión clásica

El corolario al teorema de Mordell nos dice que el rango de una curva elíptica es finito, pero no nos dice como encontrarlo. Hay mucho por desarrollar en este ámbito; actualmente no existen métodos lo suficientemente generales o raudos para calcular el rango de curvas elítpicas arbitrarias. Se conjetura que no hay cota superior para el rango y se ha demostrado que existen curvas con rango mayor o igual a 28. Se ha demostrado que la mayoría (en un sentido matemático apropiado) de las curvas elípticas tienen rango 0 o 1. Esto significa que el tener rango mayor a 1 es una anomalía estadística. La conjetura más importante acerca del rango de una curva elíptica $E$ (y en general, la mas importante en toda esta área) es la conjetura BSD, la cual presentaremos en su versión original de 1965.

**Definición 5.** *Decimos que una curva elíptica $E$ está en forma de Weierstrass si escribimos $E : y^2 = x^3 + ax + b$.*

**Definición 6.** *Sea $E$ curva elíptica racional en forma de Weierstrass, $p$ número primo. Definimos $N_p :=$ Número de soluciones de $\{y^2 \equiv x^3 + ax + b \bmod p\}$.*

**Conjetura 1.** *(Birch y Swinnerton-Dyer, 1965) Sea $E$ curva elíptica racional en forma de Weierstrass, $r$ rango de $E$ y $p$ primo, entonces*

$$\prod_{p \leq x} \frac{N_p}{p} \approx C log(x)^r, \text{ con } x \to \infty \text{ y } C \text{ una constante.}$$

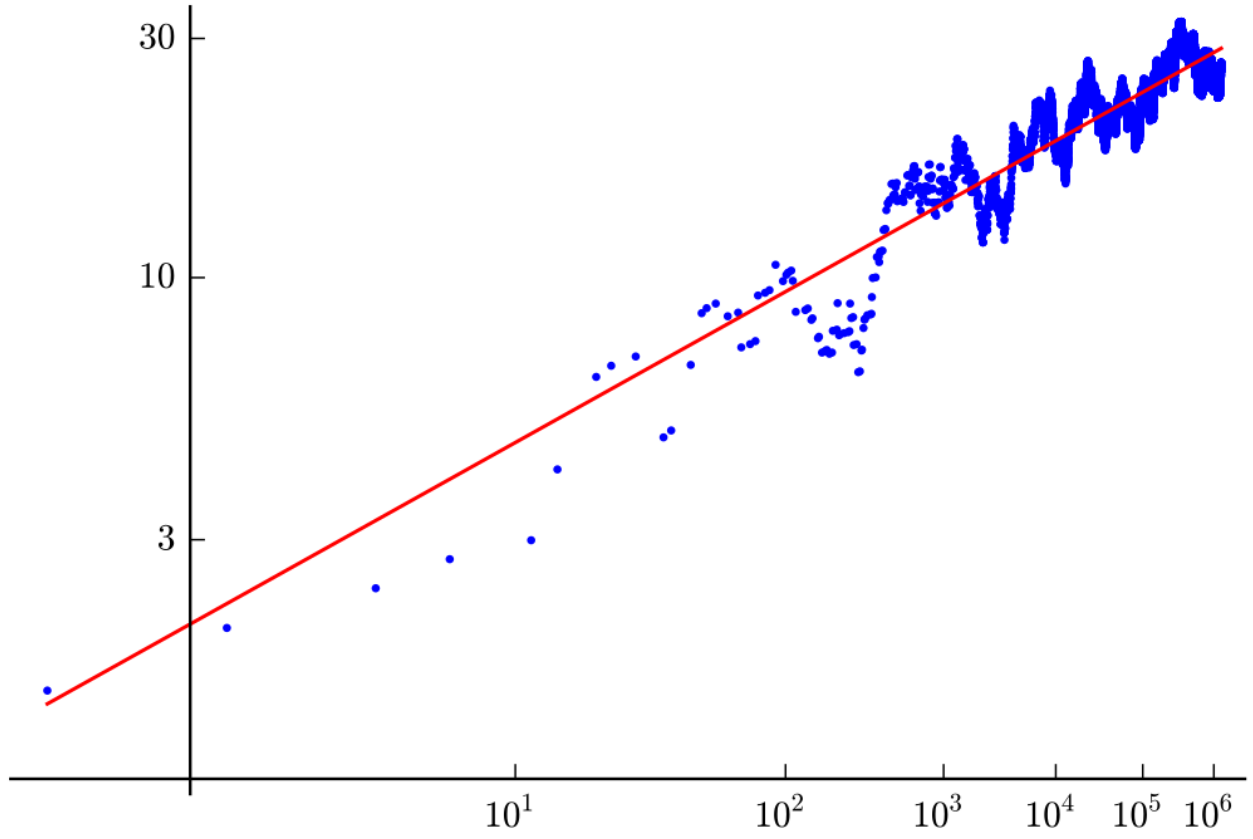



Figura 3.1: Gráfica de $\prod_{p \leq x} \frac{N_p}{p}$ para la curva $y^2 = x^3 - 5x$ sobre los primeros 100.000 primos. El eje $x$ es $\log(\log(x))$ y el eje $y$ está a escala logarítmica. El rango de esta curva elíptica es 1, y la conjetura predice que los datos debíeran formar una línea de pendiente igual al rango de la curva. Para comparar, se dibujó una recta de pendiene 1 en rojo.

Birch y Swinnerton-Dyer conjeturaron este resultado basandose en evidencia númerica por computadora, en el laboratorio de computación de Cambridge. Dada la capacidad gráfica y computacional de los años 60' (minúscula comparada a la actual), la conjetura se basó incialmente en gráficas sutiles y tenues, lo que produjo escepticismo en J. W. S. Cassels, el supervisor doctoral de Birch. Sin embargo, con el tiempo la evidencia númerica se acumuló, junto con resultados parciales (que discutiremos más en adelante) por lo que hoy la conjetura se piensa verdadera.

Hoy en día la conjetura tiene una forma más general y para poder discutirla, debemos hablar de funciones $L$.

# Capítulo 4

# Funciones L

Las funciones L forman un tópico central en teoría de números desde la demostración del Teorema De Los Numeros Primos En Progresión Aritmética por parte de Dirichlet (1837) y desde el trascendental artículo de Riemann "Sobre El Número De Primos Menores Que Una Cantidad Dada" (1859). Llevan este nombre en honor de Estas funciones provienen de las llamadas series de Dirichlet, por lo que empezaremos allí.

**Definición 7.** *Una serie de Dirichlet es una serie de la forma*

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

*con* $(a_n)_{n\geq 1}$ *una sucesión compleja y* $s \in \mathbb{C}$.

El ejemplo prototípico de serie de Dirichlet es la famosa función zeta de Riemann:

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

Esta función juega un papel protagónico en la teoría de números contemporánea, tanto así que la hipótesis de Riemann (caracterización de los ceros de $\zeta(s)$) fue incluída tanto en los 23 Problemas de Hilbert, como en los 7 Problemas Del Milenio, además de tener repercusiones en áreas como estadística, teoría de probabilidad y mecánica cuántica.
Es un buen e ilustrativo ejercicio demostrar la siguiente identidad:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}$$

Esta identidad es gracias a Euler, quien la demostró el caso $s \in \mathbb{R}$, antes de existir la noción establecida de números complejos. En su honor, la expresión de la derecha lleva el nombre de Producto de Euler. A priori, la función $\zeta(s)$ es convergente para todo $\mathrm{Re}(s) > 1$ y se puede extender analíticamente a todo $\mathbb{C}$ con un polo simple en $s = 1$ con residuo 1.
Estos resultados no son aislados, forman parte importante del estudio de series de Dirichlet.

Antes de dar nuestra definición de función $L$ hacemos un comentario: en la actualidad se conocen muchos ejemplos importantes de funciones denotadas como funciones $L$, sin embargo su definición no está estandarizada. Un intento de esto es la llamada clase de Selberg, que intenta axiomatizar e incluir las propiedades deseables y notorias de la mayoría de las funciones llamadas $L$. Con esto en mente, nosotros consideraremos la siguiente definición:

**Definición 8.** *Sea $S$ una serie de Dirichlet. Si $S$ se puede extender analíticamente a una función meromorfa $F : \mathbb{C} \to \mathbb{C}$, llamamos a esta extensión una función $L$ de la serie $S$.*

Las funciones $L$ nos permiten obtener información extra acerca de la serie de Dirichlet, en particular en lugares donde la serie no está definida o contenga polos. Estas están intimamente relacionadas con las funciones "Zeta" (por ej, la función de Riemann recién mencionada), en particular muchas funciones Zeta se "factorizan" a través de funciones $L$. Historicamente, la distinción a veces se da simplemente por nomenclatura, y diversos autores llamaron "Zeta" o $L$ a funciones especiales con las que trabajaban. Por ejemplo, Peter Gustav Lejuene Dirichlet las nombró así por su apellido.

Acabamos de definir una función $L$ a partir de una serie de Dirichlet $S$. Esta misma idea se puede aplicar a diversos objetos matemáticos, por ejemplo a curvas elípticas. Para esto, definimos primero los "factores locales" de $E$.

**Definición 9.** *Sea $E$ una curva elíptica racional y sea $p$ primo. Definimos $a_p := p - N_p$ (ver capítulo 3). Definimos el $p-$ésimo factor local de $E$ como*

$$L_p(E, s) := 1 - a_p p^{-s} + p^{1-2s}$$

Para cada primo $p$, el factor local correspondiente nos entrega información aritmética de la curva $E$ en el primo $p$.

**Definición 10.** *Sea $E$ una curva elíptica racional, la función $L$ asociada a $E$ es*

$$L(E, s) := \prod_{\substack{p \text{ primo} \\ p \nmid 2\Delta}} L_p(E, s)^{-1}$$

A priori, esta es una función compleja con variable $s$ y convergente para $\mathrm{Re}(s) > 3/2$. El matemático alemán Helmut Hasse conjeturó que $L(E, s)$ se podría extender a una función holomorfa en todo el plano complejo (esto es más fuerte que meromorfa). Eventualmente esto se demostró como cierto.

# Capítulo 5

# Conjetura BSD - Versión moderna

Finalmente estamos listos para la pregunta de un millón de dólares. Esta es una refinación de la conjetura original y encapsula una perspectiva más amplia.

**Conjetura 2.** *(Birch y Swinnerton-Dyer) Sea $E$ una curva elíptic racional, sea $r$ el rango de $E$ y sea $L(E,s)$ la función $L$ asociada a $E$. Entonces, la expansión de Taylor de $L(E,s)$ en $s=1$ es de la forma*

$$L(E,s) = c(s-1)^r + \text{ Términos de orden mayor,}$$

*con $c \neq 0$ constante.*

La conjetura se puede refinar incluso más, pero requiere conocimientos de geometría algebraica. Además, BSD se puede planetar sobre cualquier cuerpo de números (extensión finita de $\mathbb{Q}$). Desde su concepción han aparecido conjeturas mucho más elaboradas acerca de valores especiales de funciones $L$ por parte de matemáticos como Tate, Lichtenbaum, Deligne, Bloch, Beilinson y otros.

Para terminar, nombramos unos resultados parciales sobre BSD (que usan lenguaje más técnico del presentado en este trabajo).

1. Coates y Wiles (1977) probaron que si $E$ es una curva sobre un cuerpo de números $F$ con multiplicación compleja por un cuerpo cuadrático imaginario $K$ con número de clase 1, $F = K$ ó $F = \mathbb{Q}$ y $L(E,s) \neq 0$ entonces $E(F)$ es grupo finito. Este resultado fue generalizado para $F$ extension finita abeliana arbitraria de $K$, por Arthaud (1978)

2. Gross y Zagier (1986) mostraron que si una curva elíptica modular tiene un cero de primer orden en $s=1$ entonces tiene un punto racional de orden infinito

3. Kolyvagin (1989) mostró mostro que una curva elíptica modular $E$ para la cual $L(E,s) \neq 0$ tiene rango 0. Por otro lado, si $L(E,s)$ tiene un cero de primer orden en $s=1$, entonces $E$ tiene rango 1.

4. Rubin (1991) mostró que para curvas elípticas definidas sobre un cuerpo cuadrático imaginario $K$ con multiplicación compleja por $K$, la $p-$parte del grupo de Tate-Shafarevich tiene el orden predicho por BSD para todo primo $p > 7$, cuando $L(E,s) \neq 0$ en $s=1$.

# Bibliografía


1. http://www.claymath.org/millennium-problems/birch-and-swinnerton-dyer-conjecture.

2. Hilbert, David (July 1902). "Mathematical problems". Bull. Amer. Math. Soc. 8 (10): 437–479.

3. An Introduction to the Theory of Elliptic Curves Joseph H. Silverman Brown University and NTRU Cryptosystems, Inc. Summer School on Computational Number Theory and Applications to Cryptography University of Wyoming June 19 – July 7, 2006.

4. Rational points on elliptic curves, Silverman Tate 2015.

5. An Introduction to the Theory of L-functions Jörn Steuding (Würzburg University). A course given at Universidad Aut´onoma de Madrid, 2005/06.

6. Elliptic Curves and the Special Values of L-functions ICTS, 2021 Introduction to Elliptic Curves: Lecture 3 Anupam Saikia Department of Mathematics, Indian Institute of Technology Guwahati Anupam Saikia IIT Guwahati August 3, 2021.