Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Curvas Elípticas y Triángulos de Herón

Trabajo de fin de grado

Grado en Matemáticas

Autor: José Ignacio Gómez García
Tutor: Enrique González Jiménez

Curso 2019-2020

Resumen

Un *triángulo de Herón* es un triángulo con lados y área enteros (o racionales). A lo largo de la historia han sido objeto de estudio de famosos matemáticos, y gracias al uso de curvas elípticas se han podido resolver numerosos problemas relacionados.

En este proyecto se presenta la teoría relacionada con las curvas elípticas con el objetivo de solucionar tres problemas relacionados con triángulos de Herón. En concreto, los teoremas de Mordell y Mazur son las principales herramientas para encontrar las respuestas a dichos problemas.

Para comprender estos teoremas y encontrar algunas respuestas, se hablará de curvas algebraicas y el plano proyectivo, y se definirá curva elíptica a partir de una forma de Weierstrass. Probaremos también que existe una operación que dotará de estructura de grupo abeliano al conjunto de puntos racionales de una curva elíptica.

Abstract

An *Heron triangle* is that whose sides and area are integer numbers (or rational). They have been widely studied along the history by many known mathematicians and, thanks to the use of elliptic curves, many related problems have been solved.

This project shows some theory related to elliptic curves in order to solve three Heron triangle problems. More precisely, Mordell's Theorem and Mazur's Theorem have both become known tools used to solve such problems.

Trying to understand these theorems and get some answers, we will learn about algebraic curves and the projective plane, while the concept of elliptic curve will be defined from a Weierstrass form. Moreover, we will prove there is an operation which gives abelian group structure to the set of rational points over an elliptic curve.

Índice general

Introducción

Los triángulos han sido, a lo largo de la historia, uno de los cuerpos geométricos más estudiados y, concretamente aquellos que contienen un ángulo recto (conocidos como triángulos rectángulos), se convirtieron en objeto estudio de grandes matemáticos.

Pitágoras (569-475 a.C.) ya formuló el famoso teorema que establece las relaciones entre los catetos y la hipotenusa de un triángulo rectángulo como $a^2+b^2 = c^2$. Además, planteó el problema relacionado con la construcción de triángulos rectángulos cuyos lados tuvieran longitudes enteras, conocidos como *ternas pitagóricas*.

El matemático Herón de Alejandría (10-75 d.C.) estableció la denominada *fórmula de Herón*, que establece la relación entre los lados de un triángulo y su área:

"*Sean a, b, c los lados de un triángulo, y $s = \frac{a+b+c}{2}$ su semiperímetro, su área será* $A = \sqrt{s(s-a)(s-b)(s-c)}$".

Este documento tiene como objetivo el estudio de los conocidos como *triángulos de Herón*. Nombrados así por el ya mencionado matemático, los triángulos de Herón son aquellos en los que tanto sus lados como su área son números enteros. En ocasiones, se puede considerar que un triángulo con lados y área racionales también es un triángulo de Herón, puesto que puede reescalarse para conseguir números enteros.

Uno de los principales métodos de análisis de triángulos de Herón consiste en el uso de *curvas elípticas*, y es en lo que centraremos nuestra atención a lo largo de este proyecto. En concreto, nos fijaremos en las curvas con coeficientes racionales, para lo que profundizaremos en la teoría sobre la que se sustentan.

En el capítulo 1 hablaremos sobre curvas algebraicas planas, el plano proyectivo y los puntos singulares y de inflexión, lo que nos llevará a enunciar la siguiente definición de una curva elíptica:

Una curva elíptica E definida sobre $\mathbb{Q}$ es una curva algebraica plana no singular definida por una forma de Weierstrass. Esto es, dados $a, b \in \mathbb{Q}$ tal que $4a^3 + 27b^2 \neq 0$ se tiene

$$E : y^2 = x^3 + ax + b.$$

En el capítulo 2 abordaremos esta definición y la dotaremos de una operación suma entre puntos de la curva. La mayor parte de este capítulo irá dirigida a probar que el conjunto de puntos racionales de una curva elíptica conforma un grupo abeliano con la operación mencionada.

A continuación, en el capítulo 3 enunciaremos los teoremas de Mordell, Nagell-Lutz y Mazur, que serán esenciales para estudiar el conjunto de puntos racionales de una curva elíptica y resolver problemas relacionados con triángulos de Herón. Se probará también que en una curva elíptica no existen puntos racionales de orden 11, 14 ni 15 (casos concretos del teorema de Mazur). Además, abordaremos uno de los famosos problemas del milenio, cuya resolución está premiada con la suma de un millón de dólares por el Clay Mathematics Institute: la Conjetura de Birch y Swinnerton-Dyer (Conjetura BSD).

Finalmente, en el capítulo 4 aplicaremos todo lo anterior para resolver tres problemas relacionados con triángulos de Herón:

- *Si dos triángulos tienen el mismo perímetro y el mismo área, ¿son congruentes?*

  Veremos que esto no es necesariamente cierto y, de hecho, aportaremos contraejemplos que lo demuestren.

- *¿Es posible encontrar dos triángulos rectángulos con lados enteros y la misma base, tales que sus alturas mantengan una relación $n:1$?*

  Llegaremos a la conclusión de que dos triángulos con estas características existen sí y solo sí la curva

  $$E_n : y^2 = x^3 + 4(n^2+1)x^2 + 16n^2x$$

  tiene infinitos puntos racionales.

- Problema del Número Congruente: *Dado un entero positivo n, encuentra un triángulo rectángulo con lados racionales tal que su área sea igual a n.*

  Probaremos que un número entero positivo n es congruente sí y solo sí la curva

  $$E_n : y^2 = x^3 - n^2x$$

  tiene infinitos puntos racionales.

Además, se incluyen tres apéndices que complementan al contenido principal del proyecto. En el apéndice A se encuentran las demostraciones relativas al capítulo 2 para las que hemos necesitado métodos computacionales. En el apéndice B se enuncia y demuestra el teorema de estructura para grupos abelianos finitamente generados, junto con una serie de definiciones y teoremas menores relacionados con él. Por último, en el apéndice C se recogen cálculos necesarios para demostrar que no existen puntos de torsión de orden 11 (relativo al teorema de Mazur) y, además, se prueba esto mismo para puntos de orden 14 y 15. Este último apéndice complementa al contenido de la sección 3.2.3

CAPÍTULO 1
Curvas algebraicas planas

Como veremos más adelante, una *curva elíptica* es un caso particular de *curva algebraica plana*. El objetivo de este capítulo es el de proporcionar una teoría sobre la que se sustente esta afirmación, para a continuación proponer la definición de *curva elíptica* con la que vamos a trabajar.

1.1. Curvas sobre el plano afín y el plano proyectivo

Definición 1.1. *(Curva algebraica plana afín)*: Sea $\mathbb{K}$ un cuerpo y $f(x,y) \in \mathbb{K}[x,y]$. La *curva algebraica plana (afín)* C asociada al polinomio f es el conjunto de raíces del polinomio f. Esto es

$$C = \{(x,y) \in \mathbb{A}^2(\overline{\mathbb{K}}) \,:\, f(x,y) = 0\}.$$

Para trabajar con curvas elípticas debemos extender la definición al plano proyectivo.

Definición 1.2. *(Plano Proyectivo)* Se define el *Plano Proyectivo* sobre un cuerpo $\mathbb{K}$ como

$$\mathbb{P}^2(\mathbb{K}) = \{[a:b:c] : a,b,c \in \mathbb{K} \textit{ no todos cero}\} \,/_{\sim}$$

donde la relación de equivalencia es la siguiente:

$[a:b:c] \sim [a':b':c']$ cuando $a = ta', b = tb', c = tc'$ para algún $t \in \mathbb{K}$.

A los números *a,b,c* se les denomina *coordenadas homogéneas* del punto $[a:b:c] \in \mathbb{P}^2(\mathbb{K})$. Nos referiremos a ellas como X, Y, Z, respectivamente.

Podemos definir, entonces, objetos geométricos como rectas o curvas sobre el plano proyectivo. Por ejemplo, una *recta* sobre $\mathbb{P}^2(\mathbb{K})$ es el conjunto de puntos $[a:b:c] \in \mathbb{P}^2(\overline{\mathbb{K}})$ cuyas coordenadas satisfacen

$$\alpha X + \beta Y + \gamma Z = 0,$$

para ciertas α, β, γ no todas cero. Resulta trivial, por la definición, que si un punto $[a:b:c]$ pertenece a una recta, todos los elementos de su clase de equivalencia también pertenecen a la misma recta.

El proceso de transformación de coordenadas afines a homegéneas se denomina *homogeneización.*

Definición 1.3. *(homogeneización)*: Dado un polinomio $f(x,y) = \sum a_{i,j}x^iy^j \in \mathbb{K}[x,y]$ de grado d, el *polinomio homogeneizado de* f se define como

$$F(X,Y,Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right) = \sum_{i,j} a_{i,j}X^iY^jZ^{d-i-j}.$$

A continuación vamos a aportar una segunda interpretación del plano proyectivo desde un punto de vista geométrico, que va a facilitar en gran medida la notación empleada y la noción de curva elíptica.

Sabemos que, sobre el plano afín, dos rectas se cortan en un único punto, siempre y cuando no sean paralelas (en cuyo caso, no tienen puntos en común). Por lo tanto, resulta natural plantear una expansión del plano afín con el conjunto de puntos de intersección de sus rectas paralelas, también llamados *puntos en el infinito.*

El proceso de completado del plano afín se denomina *proyectivización.* Consiste en tomar la inclusión

$$(x,y) \mapsto [x:y:1] \in \mathbb{P}^2(\mathbb{K})$$

de coordenadas afines a homogéneas. El complemento de esta imagen será el conjunto de puntos $[a:b:0] \in \mathbb{P}^2(\mathbb{K}),\ a,b \in \mathbb{K}$, los *puntos en el infinito*, y conformarán una recta denominada *recta en el infinito.*

Sean

$$A : f(x,y) = y - mx = 0$$

$$B : g(x,y) = y - mx - \alpha = 0$$

dos rectas paralelas con $\alpha, m \in \mathbb{K}$ (misma pendiente pero distintos cortes con los ejes, $\alpha \neq 0$) sobre el plano afín, y sus respectivas homogeneizaciones

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

$$G(X,Y,Z) = Y - mX - \alpha Z = 0.$$

Resulta sencillo comprobar que ambas rectas intersecan en $Z = 0$. Sin embargo, de la primera ecuación sabemos que $Y = mX$, por lo que el punto de intersección será $[X : mX : 0] \sim [1 : m : 0]$.

Otro caso de interés es aquel que viene dado por las rectas

$$A : f(x,y) = x - \alpha,$$

$$B : g(x,y) = x - \beta,$$

con $\alpha, \beta \in \mathbb{K}, \alpha \neq \beta$. Son de nuevo dos paralelas cuyas homogeneizaciones

$$F(X,Y,Z) = X - \alpha Z = 0,$$

$$G(X,Y,Z) = X - \beta Z = 0,$$

intersecan únicamente en $Z = 0$ y, por tanto, $X = 0$. Es decir, la intersección viene dada por el conjunto de puntos $[0 : m : 0] \sim [0 : 1 : 0]$.

Ahora sabemos que la recta no vertical que pasa por el $(0, 0)$ corta con todas sus paralelas en el mismo *punto en el infinito*, $[1 : m : 0]$, siendo m su pendiente. En el caso concreto en que dichas rectas son verticales, el punto de intersección será $[0 : 1 : 0]$, de nuevo un *punto en el infinito*.

En conclusión, todo conjunto de rectas con la misma dirección (o misma pendiente), cortarán en un único *punto en el infinito*. Y el conjunto de estos puntos será $\{[1 : m : 0] : m \in \mathbb{K}\} \cup [0 : 1 : 0]$, una recta sin puntos en $\mathbb{A}^2$ (la *recta en el infinito*), que se denota por $\mathbb{P}^1(\mathbb{K})$, la recta proyectiva.

Podemos entender ahora el plano proyectivo como

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1,$$

donde el punto $[a : b : c] \in \mathbb{P}^2$ se corresponde con

$$\begin{cases} [a/c : b/c : 1] = (a/c, b/c) \in \mathbb{A}^2 \ si \ c \neq 0, \\ [a : b : 0] = \begin{cases} [1 : b/a : 0] \in \mathbb{P}^1 \ si \ c = 0 \ y \ a \neq 0, \\ [0 : 1 : 0] \in \mathbb{P}^1 \ si \ c = a = 0. \end{cases} \end{cases}$$

Definición 1.4. *(Curva Proyectiva Plana)*: Sea $\mathbb{K}$ un cuerpo y $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ un polinomio homogéneo. La *curva proyectiva plana* C asociada al polinomio F es el conjunto

$$C = \{[X : Y : Z] \in \mathbb{P}^2(\overline{\mathbb{K}}) \ : \ F(X, Y, Z) = 0\}.$$

Se trata, por tanto, de una *curva algebraica plana* definida sobre el plano proyectivo.

Es necesario que el polinomio F sea homogéneo para que se cumpla que $[a : b : c] \in \mathbb{P}^2(\mathbb{K}) \sim [\lambda a : \lambda b : \lambda c]$ para todo $\lambda \in \mathbb{K}$ (condición impuesta por encontrarnos en el plano proyectivo). Esto es porque, sea $[a : b : c] \in \mathbb{P}^2(\mathbb{K})$ una solución de $F(X, Y, Z)$, si el polinomio es homogéneo tenemos que

$$0 = F(a, b, c) = F(\lambda a, \lambda b, \lambda c) = \lambda^d F(a, b, c)$$

y, en ese caso, $[\lambda a : \lambda b : \lambda c]$ también es solución.

Es posible obtener *curvas proyectivas* mediante la *proyectivización* de curvas planas en el plano afín. Además, dada una *curva proyectiva*, denominamos *parte afín* al conjunto de puntos $\{[a : b : 1] : a, b \in \overline{\mathbb{K}}\}$ pertenecientes a la curva.

Definición 1.5. *(Puntos $\mathbb{K}$-racionales)*: Sea $\mathbb{K}$ un cuerpo y $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$ un polinomio homogéneo. Los puntos $\mathbb{K}$-racionales de la curva asociada a la curva C definida por F es el conjunto

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

Definición 1.6. *(Forma de Weierstrass)*: Una curva plana sobre $\mathbb{K}$ está en forma de Weierstrass cuando viene dada por una ecuación del tipo

$$W \,:\, y^2 = x^3 + ax + b$$

con $a, b \in \mathbb{K}$.

La ecuación de Weierstrass homogeneizada de nuestra curva es

$$W \,:\, Y^2Z = X^3 + AXZ^2 + BZ^3$$

y tomemos su intersección con la *recta en el infinito*, $Z = 0$. Podemos ver entonces que hay un único punto de intersección en $X = 0$, y este punto es el $[0, Y, 0]$ para cualquier Y. Sin embargo, este punto es equivalente a tomar el $[0, 1, 0]$ (pertenecen a la misma clase de equivalencia).

Por lo tanto, el punto $\mathcal{O} = [0, 1, 0]$ es el único punto de intersección de la curva con la *recta en el infinito*. En particular para cualquier cuerpo $\mathbb{K}$ se tiene que $\mathcal{O} \in W(\mathbb{K})$. Así se tiene

$$W(\mathbb{K}) = \{(x, y) \in \mathbb{A}^2(\mathbb{K}) \,:\, y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}. \tag{1.1}$$

1.2. Puntos singulares

Definición 1.7. *(Punto Singular)*: Un *punto singular* de una curva proyectiva plana definida por un polinomio $F(X, Y, Z)$ es un punto $P \in C$ tal que $\nabla F(P) = (0, 0, 0)$. Una *curva singular* es aquella que tiene algún *punto singular*. En caso contrario, hablaremos de *curvas lisas* o *no singulares*.

Obsevación 1.8. *Un punto $P = [x_0 : y_0 : 1] \in C$ es singular si*

$$f(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0,$$

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

Vamos a estudiar cuándo una curva dada por una forma de Weierstrass tiene puntos singulares. Supongamos ahora que nuestra curva W viene dada por el polinomio $F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 + bZ^3$. Hemos visto en la sección anterior que el único punto en el infinito de W es $\mathcal{O}$. Se tiene $\frac{\partial F}{\partial Z}(\mathcal{O}) = 1$, por lo tanto $\mathcal{O}$ no es singular. Así que si W tiene un punto singular, será de la forma $(x_0, y_0) \in \mathbb{A}^2(\overline{\mathbb{K}})$. Por tanto si $f(x, y) = F(X, Y, 1)$ se tendrá $f(x_0, y_0) = 0$,

$$\frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0 \qquad y \qquad \frac{\partial f}{\partial x}(x_0, y_0) = g'(x_0) = 0,$$

donde $g(x) = x^3 + ax + b$. Supongamos que $\mathrm{char}(\mathbb{K}) \neq 2$, entonces como $g(x_0) = y_0^2 = 0$ y $g'(x_0) = 0$, x_0 es raíz tanto de $g(x)$ como de $g'(x)$, por lo que es raíz doble de $g(x)$.

En conclusión, en el caso que nos atañe, $\mathrm{char}(\mathbb{K}) \neq 2$, sabemos que una curva en forma de Weierstrass tiene puntos singulares sí y solo sí tiene alguna raíz múltiple.

Por lo tanto, otra forma de comprobar si una curva dada por una forma de Weierstrass es singular o no, es mediante su discriminante: existen raíces múltiples (hay puntos singulares) sí y solo sí el discriminante del polinomio $g(x)$ es nulo. Esto es así porque el discriminante de $P(x) = a_n x^n + (n-1)a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ puede expresarse en función de sus raíces como

$$Disc_x(P) = a_n^{2n-2} \prod_{i<j} (r_i - r_j)^2$$

Proposición 1.9. Una curva algebraica sobre un cuerpo K con $char(\mathbb{K}) \neq 2$, expresada por una forma de Weierstrass $y^2 = x^3 + ax + b$ es singular sí y solo sí

$$4a^3 + 27b^2 = 0$$

Demostración. Tomemos de nuevo la misma expresión de nuestra curva

$$y^2 = g(x) = x^3 + ax + b,$$

y supongamos que tiene un punto singular en (x_0, y_0) y, por tanto, una raíz doble de $g(x)$ en x_0. Esto implica que

$$g'(x_0) = 3x_0^2 + a = 0.$$

Resolviendo,

$$x_0 = \pm\sqrt{-\frac{a}{3}}.$$

Por lo que

$$g(x_0) = \left(\pm\sqrt{-\frac{a}{3}}\right)^3 \pm a\sqrt{-\frac{a}{3}} + b = \pm\frac{2a}{3}\sqrt{-\frac{a}{3}} + b = 0.$$

Esto es cierto sí y solo sí

$$\pm 2a\sqrt{-a} + 3\sqrt{3}b = 0,$$

$$(3\sqrt{3}b + i2a\sqrt{a}) \cdot (3\sqrt{3}b - i2a\sqrt{a}) = 0,$$

$$4a^3 + 27b^2 = 0.$$

Finalmente, podemos concluir que una curva en forma de Weierstrass es singular sí y solo sí

$$4a^3 + 27b^2 = 0.$$

□

1.3. Puntos de inflexión

Definición 1.10. Sean C y L curvas algebraicas planas y P un punto de intersección de ambas, llamaremos $I_P(C, L)$ a la multiplicidad de dicha intersección.

Definición 1.11. *(Punto de Inflexión)*: Sea C una curva plana, $P \in C$ y L la tangente a C en el punto P, diremos que P es un *punto de inflexión* si

$$I_P(C, L) \geq 3.$$

Proposición 1.12. Sea $W : y^2 = x^3 + Ax + B$ una curva dada por una forma de Weierstrass. Entonces la recta $Z = 0$ es tangente a W en el punto $\mathcal{O}$ y corta tres veces con la curva en dicho punto. En particular $\mathcal{O}$ es un punto de inflexión.

Demostración. Comenzamos tomando la ecuación homogénea de nuestra curva

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

La idea es escoger una carta hacia el plano afín que contenga al punto $\mathcal{O}$. Por lo tanto, en vez de fijar $Z = 1$, vamos a fijar $Y = 1$. Esto quiere decir que

$$\begin{cases} [a/b : 1 : c/b] = (a/b, c/b) \in \mathbb{A}^2 \ si \ b \neq 0, \\ [a : 0 : c] = \begin{cases} [1 : 0 : c/a] \in \mathbb{P}^1 \ si \ b = 0 \ y \ a \neq 0, \\ [0 : 0 : 1] \in \mathbb{P}^1 \ si \ b = a = 0. \end{cases} \end{cases}$$

Y, como inversa, tenemos

$$\begin{cases} x \mapsto \frac{X}{Y}, \\ z \mapsto \frac{Z}{Y}. \end{cases}$$

Ahora, nuestra ecuación afín sería

$$z = x^3 + Ax^2z + Bz^3$$

y el punto sería $\mathcal{O} = (0, 0)$. A continuación, queremos ver cuánto vale $I_{\mathcal{O}}(C, L)$, siendo C nuestra curva y L la tangente en el punto $\mathcal{O}$.

$$f(x, z) = x^3 + Axz^2 + Bz^3 - z,$$

$$\nabla f(\mathcal{O})(x - 0, z - 0) = 0,$$

$$(0, -1)(x, z) = 0,$$

Una vez tenemos la tangente, $Z = 0$, vemos su intersección con la curva

$$\{x^3 = 0\} = \{\mathcal{O}\}$$

Por lo tanto, $I_{\mathcal{O}}(C, L) = 3$.

□

CAPÍTULO 2
Curvas elípticas

2.1. Introducción

Hasta ahora, hemos definido las curvas algebraicas sobre un cuerpo $\mathbb{K}$. De aquí en adelante, vamos a centrarnos únicamente en el cuerpo $\mathbb{Q}$ de los números racionales, puesto que es el que más nos interesa estudiar en este caso.

Definición 2.1. *(Curva Elíptica)*: Una curva elíptica E definida sobre $\mathbb{Q}$ es una curva algebraica plana no singular definida por una forma de Weierstrass. Esto es, dados $a, b \in \mathbb{Q}$ tal que $4a^3 + 27b^2 \neq 0$ se tiene

$$E \,:\, y^2 = x^3 + ax + b.$$

Por la ecuación (1.1) se tiene

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

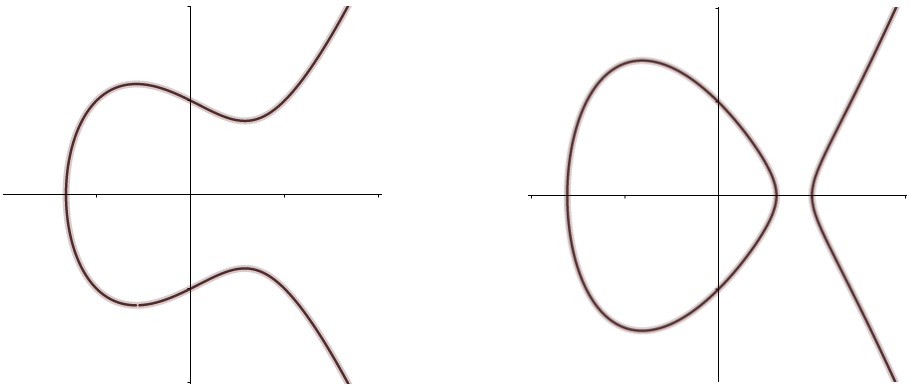

Figura 2.1: Suma en curvas elípticas

Obsevación 2.2. *Nótese que la ecuación que define una curva elíptica es simétrica respecto al eje $y = 0$.*

En este capítulo vamos a dar estructura de grupo al conjunto de puntos racionales de una curva elíptica.

2.2. Ley de Grupo

A continuación vamos a tratar una de las propiedades más importantes de las curvas elípticas: su Ley de Grupo. Y es que vamos a demostrar que el conjunto de los puntos racionales $E(\mathbb{Q})$ conforman un grupo con una operación "suma" un tanto peculiar.

Obsevación 2.3. *Nótese que una recta y una cúbica intersecan en, a lo sumo, tres puntos. Basta tomar la ecuación de una recta $y = ax + b$ y la de una cúbica $y^2 = x^3 + cx + d$ y comprobar su intersección $(ax + b)^2 = x^3 + cx + d$. Al tratarse de un polinomio de grado 3, por el Teorema Fundamental del Álgebra sabemos que tiene exactamente tres raíces en $\mathbb{C}$, de las cuales o bien todas son reales, o bien exactamente dos pertencen a $\mathbb{C} \setminus \mathbb{R}$ (puesto que las soluciones complejas aparecen siempre en pares conjugados).*

Operación Suma: *Si tenemos dos puntos $P, Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ y trazamos la recta que los une, por la observación anterior sabremos que dicha recta va a cortar a nuestra curva en un tercer punto en $E(\mathbb{Q})$, que vamos a denominar $P * Q = (x_0, y_0)$. Ya mencionamos que una curva elíptica es simétrica respecto al eje $Y = 0$, por lo que podemos tomar $P + Q = (x_0, -y_0)$ como la reflexión de $P * Q$ sobre dicho eje.*

Obsevación 2.4. *En el apartado 2.2.1 comprobamos que, al definir esta operación de forma explícita a partir de dos puntos de una curva $P, Q \in E(\mathbb{Q})$, efectivamente la suma existe y es un punto racional perteneciente a la misma curva.*

Si, en su lugar, queremos calcular $P+P$, entonces tomamos la tangente a la curva en el punto P. Esto es así porque la tangente tendrá una intersección doble con la curva en dicho punto.

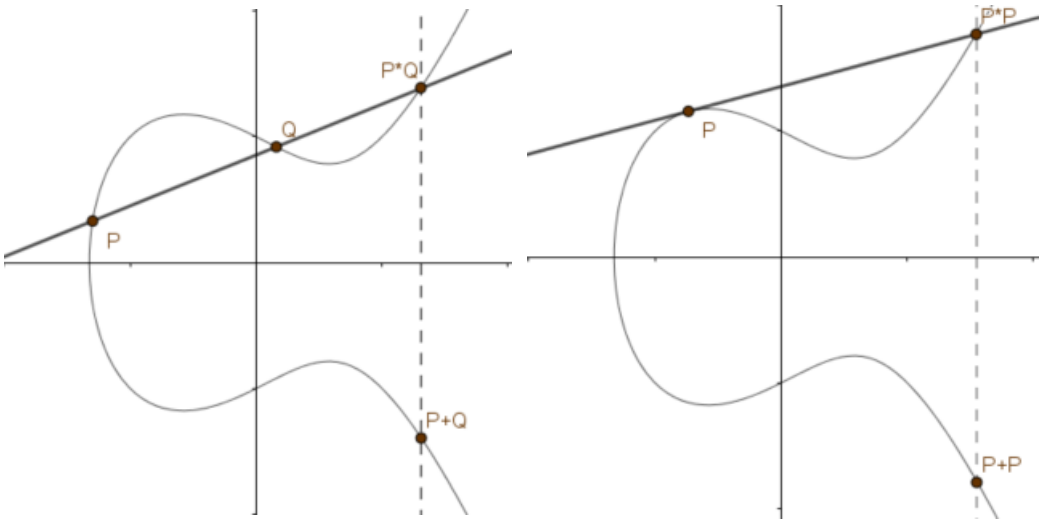

Figura 2.2: Suma en curvas elípticas

Obsevación 2.5. *De la misma definición de la operación se deduce la conmutatividad.*

En el capítulo 1 vimos que el punto $\mathcal{O}$ es el único punto de intersección de la curva con la recta en el infinito. En concreto, tal y como explicamos en el capítulo anterior, el punto $\mathcal{O}$ es también el punto de intersección de todas las paralelas con pendiente infinita, es decir, todas las rectas $X = \alpha$ para todo α.

Si ahora regresamos a la operación suma definida para curvas elípticas, veremos que al obtener $P+Q$ como la reflexión sobre el eje X del punto $P*Q$, lo que realmente estamos haciendo es trazar la recta que une $\mathcal{O}$ con $P*Q$, que será una recta vertical, y tomar la tercera intersección con la curva (la reflexión mencionada). En definitiva tenemos

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

Entonces podemos atender al último caso de nuestra operación suma: aquel en el que uno de los puntos es $\mathcal{O}$. En ese caso, tendríamos

$$P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O}.$$

Supongamos en primer lugar que $P \neq \mathcal{O}$. En la observación 2.3 mencionamos que una recta y una cúbica intersecan en, a lo sumo, tres puntos. Por lo tanto, la recta que une P y $\mathcal{O}$, o bien corta con la curva en un tercer punto, Q, o bien sólo corta en P y en $\mathcal{O}$. En el primer caso, si trazamos de nuevo la recta que une Q y $\mathcal{O}$, veremos que la tercera intersección vuelve a ser P. Es decir, $P + \mathcal{O} = P$. El segundo caso se produce cuando hay una intersección doble en el punto P (la única recta que corta más de una vez en $\mathcal{O}$ es la recta en el infinito, como hemos visto en el capítulo anterior). Por lo tanto, $P * \mathcal{O} = P$ y $P + \mathcal{O} = P$.

Por último si $P = \mathcal{O}$ se tiene $\mathcal{O} + \mathcal{O} = (\mathcal{O} * \mathcal{O}) * \mathcal{O} = \mathcal{O}$, por la proposición 1.12.

Por lo tanto hemos demostrado el siguiente resultado.

Proposición 2.6. Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces para $P, Q \in E(\mathbb{Q})$ se tiene $P + Q \in E(\mathbb{Q})$ y $P + \mathcal{O} = P$. Es decir, la operación $+$ es cerrada en $E(\mathbb{Q})$ y $\mathcal{O}$ es neutro de la operación.

El objetivo de este capítulo es la demostración del siguiente teorema.

Teorema 2.7. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces $(E(\mathbb{Q}), +)$ es un grupo abeliano.*

2.2.1. Operación explícita

Para poder trabajar fácilmente con la operación que hemos definido, vamos a estudiar las fórmulas explícitas correspondientes.

Inicialmente, vamos a suponer el caso $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ tal que $x_P \neq x_Q$ y $P + Q = (x_R, -y_R)$, donde $R = (x_R, y_R) = P * Q$. Trazamos la recta que pasa por los dos puntos, que será $y = \lambda x + \nu$, con $\lambda = \frac{y_Q - y_P}{x_Q - x_P}$ y $\nu = y_P - \lambda x_P = y_Q - \lambda x_Q$.

$$y^2 = (\lambda x + \nu)^2 = x^3 + Ax + B$$

que poniéndolo todo al mismo lado

$$0 = x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)x + (B - \nu^2).$$

Obtenemos entonces una ecuación cúbica que, por el Teorma Fundamental del Álgebra, sabemos que va a tener tres raíces en $\mathbb{C}$. Dos de ellas, en concreto, serán x_P y x_Q, ya que la ecuación representa la intersección entre la recta que pasa por P y Q, y nuestra curva.

Entonces podemos reescribir la ecuación como

$$x^3 - \lambda^2 x^2 + (A - 2\lambda\nu)x + (B - \nu^2) = (x - x_P)(x - x_Q)(x - x_R)$$

pero

$$(x-x_P)(x-x_Q)(x-x_R) = x^3+(-x_P-x_Q-x_R)x^2+(x_Px_R+x_Px_Q+x_Rx_Q)x-x_Px_Qx_R$$

De aquí podemos deducir que

$$\lambda^2 = x_P + x_Q + x_R$$

y, por tanto,

$$x_R = \lambda^2 - x_P - x_Q$$

$$-y_R = -\lambda x_R - \nu = -y_P - \lambda(x_R - x_P)$$

Sin embargo, cuando $P = Q = (x_P, y_P)$ no podemos aplicar la fórmula anterior. Tal y como definimos nuestra operación, tomaremos la recta tangente a la curva en el punto P, obteniendo

$$\lambda = \frac{\partial y}{\partial x}\Big|_P = \frac{f'(x_P)}{2y_P} = \frac{3x_P^2 + A}{2y_P}.$$

Por el mismo procedimiento, tenemos que

$$x_R = \lambda^2 - 2x_P$$

$$-y_R = -\lambda x_R - \nu = -y_P - \lambda(x_R - x_P)$$

Por último el caso en el que $P \neq Q$ y $x_P = x_Q$. Por la simetría de la ecuación de E se tiene $y_Q = -y_P$. La recta que pasa por P y Q tiene por ecuación $x = x_P$, por lo que está corta a E en el punto $\mathcal{O}$. Por lo tanto $P + Q = \mathcal{O} * \mathcal{O} = \mathcal{O}$.

2.2.2. Elemento neutro

Proposición 2.8. El punto $\mathcal{O} \in E(\mathbb{Q})$ es el único neutro para la operación definida.

Demostración. Vamos a proceder por reducción al absurdo, suponiendo únicamente que $\mathcal{O}$ es neutro, y que la operación es conmutativa.

Suponemos que existe un segundo neutro, $\mathcal{O}_2$. En ese caso, por definición de neutro, tendríamos que $P + \mathcal{O}_2 = \mathcal{O}_2 + P = P$ para todo P punto en la curva. En concreto, $\mathcal{O}$ es un punto en la curva, por lo que tendríamos

$$\mathcal{O} + \mathcal{O}_2 = \mathcal{O}_2.$$

y, como $\mathcal{O}$ es también neutro

$$\mathcal{O}_2 + \mathcal{O} = \mathcal{O}.$$

Como la suma es conmutativa, sabemos que $\mathcal{O}_2 + \mathcal{O} = \mathcal{O} + \mathcal{O}_2$ y, por tanto, $\mathcal{O}_2 = \mathcal{O}$.

□

2.2.3. Elemento inverso

Proposición 2.9. Dado un punto $P = (x_0, y_0) \in E(\mathbb{Q})$, existe un único inverso. Dicho inverso es $-P = (x_0, -y_0)$.

Demostración. En la descripción explícita de la suma hemos visto que $P + (-P) = \mathcal{O}$ y que la única posibilidad para que $P + Q = \mathcal{O}$ es $Q = -P$. □

2.2.4. Asociatividad

La prueba de la asociatividad en $E(\mathbb{Q})$ requiere de varios cálculos y resultados previos, basados en los artículos de Friedl[4] y Théry[9]. En primer lugar, probaremos tres casos específicos por computación explícita utilizando *Sage*[7]:

Lema 2.10. *Sean* $P, Q, R \in E(\mathbb{Q}) \setminus \mathcal{O}$. *Si* $P \neq \pm Q, Q \neq \pm R, P + Q \neq \pm R$ *y* $Q + R \neq \pm P$, *entonces*

$$P + (Q + R) = (P + Q) + R.$$

Demostración. Demostración en el apéndice A.1. □

Lema 2.11. *Sean* $P, Q \in E(\mathbb{Q}) \setminus \mathcal{O}$. *Si* $P \neq -P, P \neq \pm Q, P + P \neq \pm Q$ *y* $P + Q \neq \pm P$, *entonces*

$$(P + P) + Q = P + (P + Q).$$

Demostración. Demostración en el apéndice A.2. □

Lema 2.12. *Sea* $P \in E(\mathbb{Q}) \setminus \mathcal{O}$. *Si* $P \neq -P, P + P \neq -(P + P), (P + P) + P \neq \pm P$ *y* $P + P \neq \pm P$, *entonces*

$$(P + P) + (P + P) = P + (P + (P + P)).$$

Demostración. Demostración en el apéndice A.3. □

A continuación probaremos algunas propiedades de la asociatividad.

Teorema 2.13 (Suma de Opuestos)**.** *Sean $P, Q \in E(\mathbb{Q})$, entonces*

$$-(P+Q) = (-P) + (-Q).$$

Demostración. Teniendo en cuenta que los puntos de $E(\mathbb{Q})$ son simétricos respecto al eje $y = 0$, esta prueba se deduce fácilmente de la definición de nuestra operación. Basta pensar que la recta que pasa por P y Q va a ser simétrica a la que pase por $(-P)$ y $(-Q)$ y, por tanto, el tercer punto de intersección de la primera recta, $(P+Q)$, será el simétrico al tercer punto de intersección de la segunda recta, $-(P+Q)$. □

Teorema 2.14. *Sean $P, Q \in E(\mathbb{Q})$, si $P+Q = P-Q$ y $P \neq -P$, entonces $Q = -Q$.*

Demostración. Pueden darse los siguientes casos:

1. $P = \mathcal{O}$ es imposible, porque entonces $P = -P$.
2. Si $Q = \mathcal{O}$, $\mathcal{O} = -\mathcal{O}$.
3. Si $P = Q$, tenemos $P + Q = P - Q = P - P = \mathcal{O}$. Entonces, $P = -Q$ (por unicidad del opuesto) y $P = -P$, lo que contradice la hipótesis.
4. Si $P = -Q$, tenemos $P + Q = -Q + Q = \mathcal{O} = P - Q = P + P$ y, por unicidad del opuesto, llegamos a que $P = -P$, lo que contradice la hipótesis.
5. Si $P = (x_P, y_P), Q = (x_Q, y_Q)$, con $x_P \neq x_Q$, podemos tomar la componente x en ambos extremos de la ecuación de la hipótesis:

$$\frac{(y_Q - y_p)^2}{(x_Q - x_P)^2} - x_P - x_Q = \frac{(-y_Q - y_p)^2}{(x_Q - x_P)^2} - x_Q - x_P$$

   Así que $4y_P y_Q = 0$. Como $P \neq -P$, $y_P \neq 0$. Por tanto, $y_Q = 0$, por lo que $Q = -Q$.

□

Teorema 2.15. *Sea $P \in E(\mathbb{Q})$, si $P \neq -P$ y $(P+P) \neq -P$, entonces*

$$(P+P) - P = P.$$

Demostración. Pueden darse los siguientes casos:

1. Si $P + P = \mathcal{O}$, por unicidad del opuesto se contradice la hipótesis $P \neq -P$.
2. Si $P = \mathcal{O}$, también se contradice la hipótesis.
3. Si $P + P = P$, por unicidad del neutro, tenemos que $P = \mathcal{O}$.

4. Si $P = (x, y)$ y $P + P = (x_2, y_2)$ con $x \neq x_2$, entonces tenemos que, para $\lambda = \frac{3x^2+A}{2y}$, se cumple $x_2 = \lambda^2 - 2x$ y $y_2 = -y - \lambda(x_2 - x)$. Si tomamos la componente x de la ecuación $(P + P) - P = (x_R, y_R)$, con $\lambda_R = \frac{(y_2-y)}{(x_2-x)}$, llegamos a que
$$x_R = x \tag{2.1}$$
(la demostración de este paso se incluye en el apéndice A.4).

   Por tanto, tenemos que $(P + P) - P = \pm P$. Sin embargo, si fuese igual a $-P$, por unicidad del neutro, llegaríamos a que $P + P = \mathcal{O}$.

□

Teorema 2.16. *Sean $P, Q \in E(\mathbb{Q})$ con $P + Q = -P$, entonces $Q = (-P) + (-P)$.*

Demostración. El caso $P = -P$ resulta trivial, puesto que $P + Q = P$, lo que implica $Q = \mathcal{O}$ y, por tanto, $Q = \mathcal{O} = P + (-P) = (-P) + (-P)$. Vamos a suponer $P \neq -P$ y a tratar cada caso por separado:

1. Si $Q = \mathcal{O}$, entonces $P = -P$ volvemos al caso anterior.
2. Si $P = -Q$, entonces $\mathcal{O} = P + Q = -P = P$. De nuevo, estamos en el caso previo.
3. Si $P = Q$, entonces $P + P = P + Q = -P = -Q$, por lo que $Q = -(P + P) = (-P) + (-P)$, usando el teorema 2.13.
4. Si $P = (x_P, y_P), Q = (x_Q, y_Q)$, con $x_P \neq x_Q$, tenemos $-P = P + Q$. Tomando la componente x a cada lado, llegamos a que
$$x_P = \frac{(y_Q - y_P)^2}{(x_Q - x_P)^2} - x_P - x_Q$$
   Operando los cuadrados y sustituyendo $y^2 = x^3 + Ax + B$ (la ecuación de la curva), obtenemos
$$2y_P y_Q = Ax_Q + 3x_Q x_P^2 + Ax_P - x_P^3 + 2B.$$
   Elevando al cuadrado y volviendo a sustituir con $y^2 = x^3 + Ax + B$
$$-x_P^6 + 6x_P^5 x_Q^2 Ax_P^4 - 9x_P^4 x_Q^2 + 8Bx_P^3$$
$$+4x_P^3 x_Q^3 - A_2 x_P^2 - 6Ax_P^2 x_Q^2 - 12Bx_P^2 x_Q +$$
$$2A^2 x_P x_Q + 4Ax_P x_Q^3 - A^2 x_2^2 + 4Bx_2^3 = 0.$$
   Que es la misma ecuación que la obtenida de sustituir $y^2 = x^3 + Ax + B$ en la fórmula
$$(x_Q - \left(\frac{3x_P^2 + A}{-2y_P}\right)^2 + 2x_P)(x_Q - x_P)^2 = 0.$$

Como sabemos que $x_P \neq x_Q$, podremos deducir que

$$x_Q = \left(\frac{3x_P^2 + A}{-2y_P}\right)^2 - 2x_P.$$

Así llegamos a que $Q = \pm((-P) + (-P))$. Suponiendo el caso

$$Q = -((-P) + (-P)),$$

llegamos a que $Q = P + P$, usando el teorema 2.13.

a) Si $P + P = -P$, llegamos a que $Q = P + P = -P = P + Q$, por lo que $P = \mathcal{O} = Q$.

b) Si $P + P \neq -P$, tenemos que $P - Q = P - (P + P) = -((P + P) - P)$. Si usamos el teorema 2.15, obtenemos $P - Q = -P = P + Q$ y, usando el teorema 2.14, $Q = -Q$. En conclusión, $Q = -Q = -(P + P) = (-P) + (-P)$.

□

Teorema 2.17. *Sean $P, Q, R \in E(\mathbb{Q})$, si $P + Q = P + R$, entonces $Q = R$.*

Demostración. Los casos $P = \mathcal{O}, Q = \mathcal{O}, R = \mathcal{O}, P = -Q, P = -R$ resultan triviales (gracias a la unicidad del opuesto y del neutro). Así que nos vamos a concentrar en el caso $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3), P + Q = (x_4, y_4) = P + R$. Tomando la componente y en ambos lados de la ecuación explícita $P + Q = P + R$, llegamos a

$$-y_1 - \lambda_{12}(x_4 - x_1) = -y_1 - \lambda_{13}(x_4 - x_1),$$

donde λ_{12} es la pendiente de la recta que une los puntos P y Q, y λ_{13}, la de la recta que une P y R. En concreto, tenemos

$$(\lambda_{12} - \lambda_{13})(x_4 - x_1) = 0.$$

Esta igualdad da lugar a dos casos:

1. $(\lambda_{12} - \lambda_{13}) = 0$: En este caso, tomando la componente x de la igualdad $P + Q = P + R$ obtenemos
$$\lambda_{12}^2 - x_1 - x_3 = \lambda_{13}^2 - x_1 - x_2.$$
Lo que nos lleva a que $x_2 = x_3$. De modo que, o bien $Q = R$, o bien $Q = -R$. Esto nos deja únicamente con el segundo caso por explorar (el primero ya cumple el enunciado). Si $Q = -R$, entonces $P + Q = P + R = P - Q$ lo que, por el teorema 2.14 nos dice que $Q = -Q$ y, como además $Q = -R$, también tenemos que $Q = R$. Sin embargo, para poder aplicar el teorema 2.14 necesitamos que $P \neq -P$. Pero si $P = -P$, entonces como ya sabemos que $P \neq -Q$ y que $P \neq -R$, también tenemos que $R \neq P \neq Q$. Por tanto, podemos escribir

$\lambda_{12} = (x_2 - x_1)/(y_2 - y_1)$ y $\lambda_{13} = (x_3 - x_1)/(y_3 - y_1)$. Obtenemos así la igualdad (por hipótesis):

$$(x_2 - x_1)/(y_2 - y_1) = (x_3 - x_1)/(y_3 - y_1).$$

Como $Q = -R$, entonces $x_2 = x_3$ y, por tanto, $y_2 = y_3 = 0$. Entonces $Q = R$.

2. $x_4 = x_1$: Esta vez, o bien $P + Q = P$, o bien $P + Q = -P$. En el primer caso, como $P + Q = P + R = P$, por unicidad del neutro sabemos que $Q = R = \mathcal{O}$. En el segundo, como $P + Q = P + R = -P$, usando el teorema 2.16 obtenemos que $Q = (-P) + (-P) = R$.

□

Teorema 2.18. *Sean $P, Q \in E(\mathbb{Q})$, entonces $(P + Q) - Q = P$*

Demostración. Si $P + Q = -Q$, entonces usando el teorema 2.16 tenemos que $P = (-Q) + (-Q)$. Por tanto, $(P + Q) - Q = (-Q) + (-Q) = P$.

Si $P + Q \neq -Q$, entonces tenemos varios casos.

1. Los casos $P = \mathcal{O}, Q = \mathcal{O}, P = -Q$ son triviales.
2. Si $P = Q$, entonces $(P + Q) - Q = (Q + Q) - Q = Q$ por el teorema 2.15.
3. Si $Q = P + Q$, entonces $P = \mathcal{O}$ por unicidad del neutro.
4. Nos queda el caso $(P + Q) - Q = P$ que se prueba por computación en el apéndice A.5.

□

Teorema 2.19. *Sean $P, Q, R \in E(\mathbb{Q})$, si $P + Q = R$ entonces $P = R - Q$.*

Demostración. Sabemos que $R = (R - Q) + Q$ por el teorema 2.18. Por tanto, aplicando 2.17 sobre $P + Q = (R - Q) + Q$, obtenemos $P = R - Q$. □

Teorema 2.20 (Asociatividad para casos degenerados)**.** *Sean $P, Q, R \in E(\mathbb{Q})$ tales que $(P = \mathcal{O} \vee Q = \mathcal{O} \vee R = \mathcal{O}) \vee (P = -Q \vee Q = -R) \vee (-P = Q + R \vee -R = P + Q)$, entonces $P + (Q + R) = (P + Q) + R$.*

Demostración. Vamos a ver cada uno de los casos por separado.

1. Si $P = \mathcal{O}$, entonces $P + (Q + R) = Q + R = (\mathcal{O} + Q) + R = (P + Q) + R$. Los casos $Q = 0$ y $R = 0$ son similares.
2. Si $P = -Q$, usando el teorema 2.18 tenemos que $-Q + (Q + R) = R$. Además, $(P + Q) + R = R$. Por tanto, $(P + Q) + R = -Q + (Q + R) = P + (Q + R)$.
3. Si $Q = -R$, estamos ante un caso similar.

4. Si $P + Q = -R$, entonces por el teorema 2.18 tenemos que $Q - (P + Q) = ((-P) + (-Q)) - (-Q) = -P$. Por tanto, $P + (Q + R) = P + (Q - (P + Q)) = P - P = \mathcal{O} = (P + Q) - (P + Q) = (P + Q) + R$

5. Si $Q + R = -P$ nos encontramos ante un caso similar al anterior.

□

Teorema 2.21. *Sean $P, Q \in E(\mathbb{Q})$, entonces $P + (P + Q) = (P + P) + Q$.*

Demostración. Gracias al teorema anterior, podemos reducir al caso no degenerado, en el que $P, Q \neq \mathcal{O}$ y $P \neq Q$ (si $P = Q$, resulta trivial aplicando la conmutatividad de la operación).

Si, por otro lado, $P = Q + Q$, tendremos que probar

$$(Q + Q) + (Q + Q) = ((Q + Q) + Q) + Q.$$

Es fácil ver, por unicidad del neutro, que $Q \neq Q + Q$. De forma similar, podemos ver que $Q \neq (Q + Q) + Q$. En este punto, nos encontramos en situación de aplicar el lema 2.12.

Si $Q = P + Q$, tendríamos que $P = \mathcal{O}$ por unicidad del neutro (contradicción).

El caso restante es exactamente el que se recoge en el lema 2.11. □

Teorema de Asociatividad. *Sean $P, Q, R \in E(\mathbb{Q})$, entonces $P + (Q + R) = (P + Q) + R$.*

Demostración. Podemos restringirnos a los casos no degenerados, gracias al teorema 2.21.

1. Si $Q = R$ o $P = Q$, aplicamos el teorema 2.21.

2. Si $P = Q + R$ tenemos $((Q + R) + (Q + R)) + (-R)$ que, por el teorema 2.21 es igual a $(Q + R) + ((Q + R) + (-R))$. Por el teorema 2.18 tenemos que es igual a $(Q + R) + Q$ que, a su vez, es igual a $(((Q + R) + Q) + R) + (-R)$. Ahora tenemos la igualdad

   $$((Q + R) + (Q + R)) + (-R) = (((Q + R) + Q) + R) + (-R)$$

   Y, por el teorema 2.17, llegamos a que

   $$(Q + R) + (Q + R) = ((Q + R) + Q) + R$$

   Y, por tanto

   $$P + (Q + R) = (P + Q) + R$$

3. El caso $R = P + Q$ es similar.

4. El caso restante es, por tanto, exactamente el que se especifica en el lema 2.10.

□

CAPÍTULO 3
Grupo de Mordell

En este capítulo vamos a presentar una serie de teoremas que nos serán de gran utilidad en lo que resta. El objetivo principal es el de caracterizar el grupo de los puntos racionales de la curva.

Sin embargo, no vamos a aportar ninguna demostración de estos teoremas más allá de alguna observación puntual, ya que preferimos centrarnos en otros apartados más relevantes.

3.1. Teorema de Mordell

A continuación enunciamos la que probablemente sea nuestra mejor herramienta a la hora de estudiar los puntos racionales de una curva elíptica y los triángulos de Herón. El teorema de Mordell afirma que el conjunto de puntos racionales forma un grupo abeliano finitamente generado.

Teorema de Mordell. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces el grupo de puntos racionales $E(\mathbb{Q})$ de la curva es un* ***grupo abeliano finitamente generado****, que denominaremos* ***Grupo de Mordell****. Además, por el Teorema de Estructura de grupos abelianos finitamente generados (ver apéndice B), sabemos que tendrá la siguiente forma:*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}, \quad 1 < d_1|d_2|...|d_s.$$

Al grupo $\mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_s\mathbb{Z}$ se le denomina ***subgrupo de torsión****.*

El exponente r se conoce como ***rango*** *del Grupo de Mordell o rango de la curva elíptica. En el caso concreto en el que $r = 0$, vemos que el Grupo de Mordell tiene orden finito y, por lo tanto, será posible calcular todos los puntos del grupo. En caso contrario, sigue siendo posible dar un conjunto de generadores.*

En el resto del documento, obtendremos el rango de una curva haciendo uso de la función rank() de Sage.

3.2. Subgrupo de torsión

Lema 3.1. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces existen $A, B \in \mathbb{Z}$ tales que $E : y^2 = x^3 + Ax + B$.*

Demostración. Partiendo de la curva $y^2 = x^2 + Ax + B$ con $A, B \in \mathbb{Q}$, basta tomar m como el mínimo comúno divisor de A y B y hacer el cambio $x \mapsto \frac{1}{m^2}x$, $y \mapsto \frac{1}{m^3}y$. □

3.2.1. Teorema de Nagell-Lutz

El siguiente teorema, probado por Trygve Nagell y Élisabeth Lutz de forma independiente, da un algoritmo para determinar todos los puntos de orden finito.

Teorema de Nagell-Lutz. *Sea E una curva elíptica en forma de Weierstrass con coeficientes enteros a, b, y sea $P = (x, y) \in E(\mathbb{Q})$ un punto racional de orden finito, entonces $x, y \in \mathbb{Z}$ y, o bien $y = 0$, o bien y^2 divide al discriminante $\Delta = -4a^3 - 24b^2$.*

3.2.2. Teorema de Mazur

El teorema de Mazur (o teorema de torsión de Mazur), probado en 1977 por el matemático del mismo nombre, es una de las principales herramientas de las que disponemos para estudiar los puntos racionales de una curva elíptica. En concreto, aporta una caracterización de su grupo de torsión.

Teorema de Mazur. *Sea E una curva cúbica racional tal que $E(\mathbb{Q})$ contiene al menos un punto de orden finito, entonces el subgrupo de torsión de $E(\mathbb{Q})$ es isomorfo a uno de los siguientes grupos:*

- $\mathbb{Z}/n\mathbb{Z}$, *con* $1 \leq n \leq 10$, *o* $n = 12$.
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *con* $1 \leq n \leq 4$.

3.2.3. No hay puntos de orden 11, 14 ni 15 sobre $\mathbb{Q}$.

Vamos a estudiar por qué el Teorema de Mazur expone que no existen puntos racionales de orden 11, 14 ni 15. La siguiente demostración, para el caso de orden 11, está basada en el artículo de Woodbury (capítulo 4) [10], el cual a su vez se basa en el artículo de Billing y Mahler [2].

Los casos de orden 14 y orden 15, por su semejanza con el caso actual, se recogen en el apéndice C, secciones C.2 y C.3.

En primer lugar, suponemos que existe un punto racional de orden 11. Por lo tanto, el elemento $\mathcal{O}$ será el neutro, y llamaremos P al generador del grupo cíclico. Por lo tanto, $\mathcal{O}, P, 2P, 3P, ..., 10P$ serán puntos distintos.

Observemos que tres puntos P, Q y R de una curva elíptica pertenecen a la misma recta sí y solo sí $P + Q + R = \mathcal{O}$.

Si partimos de cinco puntos $\mathcal{O}, P, 2P, 3P, 4P$, todos los demás se pueden sacar intersecando rectas, empleando la observación anterior. Por ejemplo, observamos que $\mathcal{O} + P + (-P) = \mathcal{O}$, por lo que los tres puntos pertenecen a la misma recta y, más concretamente, $-P \in \overline{\mathcal{O}P}$ (la recta que une $\mathcal{O}$ y P). De la misma manera, podemos ver que $-P \in \overline{(-3P)\ 4P}$. En consecuencia, tenemos que

$$10P = -P = \overline{\mathcal{O}P} \cap \overline{(-3P)\ 4P}.$$

Siguiendo el mismo procedimiento, llegamos a

$$9P = -2P = \overline{\mathcal{O}\ 2P} \cap \overline{(-P)\ 3P},$$

$$8P = -3P = \overline{\mathcal{O}\ 3P} \cap \overline{P\ 2P},$$

$$7P = -4P = \overline{\mathcal{O}\ 4P} \cap \overline{P\ 3P},$$

$$6P = -5P = \overline{P\ 4P} \cap \overline{2P\ 3P},$$

$$5P = \overline{(-P)\ (-4P)} \cap \overline{(-2P)\ (-3P)}.$$

A continuación, nos remitimos al apéndice C para comprobar que podemos hacer un cambio a proyectivas que envíe el punto $\mathcal{O}$ al $[1:1:1]$ y los puntos $P, 2P, 3P$ y $4P$ a $[1:0:0], [0:1:0], [0:0:1], [x:y:z]$ de forma única.

Este cambio genera los siguientes puntos (ver apéndice C):

$$-P = [x - y + z : z : z],$$

$$-2P = [x - y + z : z : x - y + z],$$

$$-3P = [1:1:0],$$

$$-4P = [x - y : 0 : z - y],$$

$$-5P = [0 : y : z],$$

$$5P = [xy + xz - y^2 : xz : y(x - y + z)],$$

$$6P = [(x-y+z)(x^2y-xy^2+y^2z-xz^2) : z(y-z)(xy+xz-y^2) : xz(y-z)(x-y+z)].$$

Como $11P = \mathcal{O}$, tenemos $6P = -5P$ y la siguiente igualdad

$$(x - y + z)(x^2y - xy^2 - xz^2 + y^2z) = 0.$$

Ahora bien, si $x - y + z = 0$, entonces $2P = -2P$, lo cual sabemos que es falso. Por lo tanto, necesariamente

$$x^2y - xy^2 - xz^2 + y^2z = 0. \tag{3.1}$$

Usando el siguiente código en Magma,

Código 3.1: Definición de las rectas

```
P2<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(P2,x^2*y - x*y^2 - x*z^2 + y^2*z);
pt:=C![0,0,1];
E,map:=EllipticCurve(C,pt);
We,map2:=WeierstrassModel(E);
We;
Elliptic Curve defined by y^2 = x^3 - 6912*x + 525312 over Rational Field

G,mw:=MordellWeilGroup(We);
pts:={};
pss:={};
for p in {mw(g) : g in G} do
        pts:={pt : pt in RationalPoints(p @@ map2 @@ map)} join pts;
        pss:={p} join pss;
end for;

pss;
{ (0 : 1 : 0), (-48 : -864 : 1), (96 : -864 : 1), (-48 : 864 : 1), (96 : 864 :1) }

pts;
{ (1 : 1 : 1), (0 : 1 : 0), (0 : 0 : 1), (1 : 0 : 0), (1 : 1 : 0) }


Rank(E);
# 0
```

obtenemos la curva elíptica que trae por ecuación $y^2 = x^3 - 6912x + 525312$. Podemos ver que el grupo de Mordell es isomorfo a $\mathbb{Z}/5\mathbb{Z}$ y que, como el rango de la curva es cero, los únicos puntos racionales serán por tanto, los siguientes cinco:

$$[0:1:0], [-48:-864:1], [96:-864:1], [-48:864:1], [96:864:1]$$

que, obteniendo sus preimágenes, se corresponden con

$$\mathcal{O} = [1:1:1],\ 2P = [0:1:0],\ 3P = [0:0:1],\ P = [1:0:0],\ -3P = [1:1:0].$$

Teorema 3.2. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces no existe $P \in E(\mathbb{Q})$ de orden 11.*

Demostración. Utilizando todo lo que hemos tratado en este punto, vemos que $\mathcal{O}, P, 2P$ y $3P$ se pueden tomar como $[1:1:1], [0:0:1], [0:1:0], [1:0:0]$. Además ya sabíamos que $-3P = [1:1:0]$. Por otro lado, $4P = [x:y:z]$ tiene que ser un punto distinto de los cinco anteriores que además satisfaga la ecuación $x^2y - xy^2 - xz^2 + y^2z = 0$. Sin embargo, hemos probado que los únicos puntos racionales que viven en esta curva son dichos cinco, alcanzando así una contradicción. □

Teorema 3.3. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces no existe $P \in E(\mathbb{Q})$ de orden 14 ni 15.*

Demostración. Se prueba en el apéndice C, secciones C.2 y C.3. □

3.3. Rango

Obtener el rango de una curva es una tarea bastante compleja. En esta sección vamos a tratar superficialmente uno de los métodos empleados para ello aunque, al no tratarse del objetivo principal de este proyecto, no entraremos en demostraciones ni profundizaremos en la teoría presentada.

Proposición 3.4. Sea E una curva elíptica definida por

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

y sea

$$E_p : y^2 = x^3 + A_p x + B_p$$

su reducción módulo p, donde p es un primo que no divide al discriminante $\Delta = -4a^3 - 24b^2$, (denotamos $A_p = A \ (mod\, p)$ y $B_p = B \ (mod\, p)$), se tiene entonces que E_p es una curva elíptica sobre $\mathbb{F}_p$.

Tomamos ahora $a_p = p + 1 - |E(\mathbb{F}_p)|$ para definir la función

$$L_E(s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Esta función $L_E(s)$ se conoce como **función L de Hasse-Weil de la curva elíptica** E. Recordamos que el primo p no divide al discriminante Δ de la curva (se dice que p es de *buena reducción*, o que E tiene *buena reducción* en p), por lo que únicamente falta un número finito de factores (los que sí dividen al discriminante).

Esta función es holomorfa para $Re(s) > 2/3$. De hecho, está demostrado que la función $L_E(s)$ puede ser continuada analíticamente en el plano complejo como una función meromorfa con un polo en $s = 1$.

3.3.1. Conjetura de Birch y Swinnerton-Dyer

Llegados a este punto podemos presentar la conjetura de Birch y Swinnerton-Dyer que busca aportar información sobre el rango de una curva elíptica.

Conjetura de Birch y Swinnerton-Dyer (débil). El rango de una curva elíptica definida sobre los racionales, $E(\mathbb{Q})$, es igual al orden del polo de la función $L_E(s)$ para $s = 1$.

Esta conjetura fue enunciada en 1965 por Bryan Birch y Peter Swinnerton-Dyer y, actualmente, es uno de los famosos siete problemas del milenio, cuya solución está premiada con un millón de dólares por el Instituto Clay de Matemáticas. Para llegar a esta conclusión, se calculó el número de puntos módulo p para un número muy grande de primos p sobre curvas elípticas cuyo rango era conocido.

CAPÍTULO 4
Triángulos de Herón

En este último capítulo vamos a aportar una aplicación práctica de la teoría de curvas elípticas tratada hasta el momento, que es la resolución de problemas relacionados con **triángulos de Herón**.

Los triángulos de Herón, llamados así por el famoso matemático Herón de Alejandría, son triángulos cuyas longitudes de lado y área son números enteros. Esta definición se suele extender también a los números racionales, ya que estos se pueden reescalar multiplicando por un múltiplo común para obtener dimensiones enteras. De hecho, es esta segunda definición con la que vamos a trabajar de ahora en adelante.

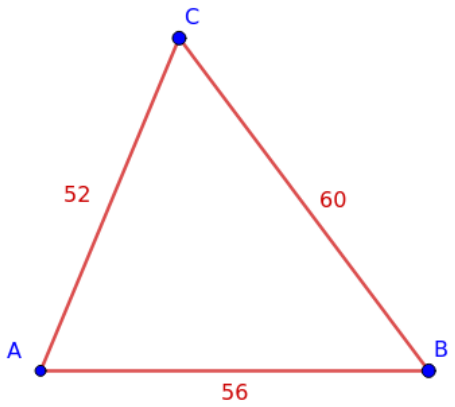

Figura 4.1: Ejemplo de triángulo de Herón

Una de las principales aportaciones de Herón al estudio de los triángulos es la **fórmula de Herón**, que permite hallar el área de un triángulo dadas las longitudes de sus tres lados.

Proposición 4.1. (Fórmula de Herón) El área de un triángulo viene dada por la siguiente fórmula:

$$A = \sqrt{s(s-a)(s-b)(s-c)}$$

donde s es el semiperímetro del triángulo, y a, b y c las longitudes de sus lados.

Al tratarse de un resultado clásico y de menor interés en este proyecto, la demostración se incluye en el apéndice D.

4.1. Triángulos Congruentes

Si dos triángulos tienen el mismo perímetro y el mismo área, ¿son congruentes?

El primer problema que vamos a tratar busca dar con una respuesta a la pregunta anterior, para lo que nos hemos basado en el artículo de Cuoco y McCallum [3]. Entendemos que dos triángulos son congruentes si existe un isomorfismo entre ellos. Esto se traduce en que sean iguales, salvo movimientos rígidos en $\mathbb{R}^2$.

Tal y como se ve en la siguiente imagen, vamos a llamar a, b y c a las longitudes de los lados, y α, β y γ a los ángulos generados por la intersección de las alturas de los tres triángulos interiores, que resulta ser el incentro de la circunferencia circunscrita.

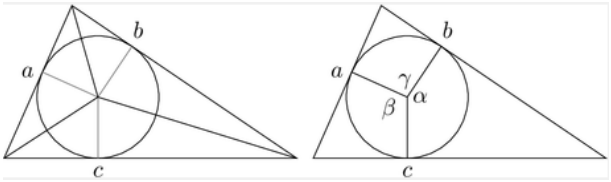

Figura 4.2: Circunferencia circunscrita

La primera observación que haremos, es que, siendo r el radio de la circunferencia circunscrita, A el área del triángulo y s su semiperímetro, entonces se cumple la siguiente relación:

$$A = rs.$$

Esta fórmula se obtiene de forma sencilla si nos damos cuenta de que la altura de cada uno de los tres triángulos interiores es igual al radio r. Por lo tanto, el área del triángulo exterior se hallaría como:

$$A = \frac{1}{2}r(a + b + c) = rs.$$

A continuación, vamos a expresar el semiperímetro en función de los ángulos. Para ello, observamos primero que los segmentos que unen los vértices al incentro bisecan cada uno de los tres ángulos. Por lo tanto, podemos expresar el perímetro como:

$$P = 2r \tan\frac{\alpha}{2} + 2r \tan\frac{\gamma}{2} + 2r \tan\frac{\gamma}{2}.$$

En consecuencia:

$$s = r(\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2}).$$

Y usando la relación $A = rs$

$$\tan\frac{\alpha}{2} + \tan\frac{\beta}{2} + \tan\frac{\gamma}{2} = \frac{s}{r} = \frac{s^2}{A}. \tag{4.1}$$

Como $\alpha + \beta + \gamma = 2\pi$, entonces:

$$\frac{\gamma}{2} = \pi - \frac{\alpha}{2} - \frac{\beta}{2}.$$

Hacemos el cambio de variable $u = \tan\frac{\alpha}{2}, v = \tan\frac{\beta}{2}, w = \tan\frac{\gamma}{2}$ y obtenemos la siguiente relación:

$$w = \tan\left(\frac{\gamma}{2}\right) = \tan\left(\pi - \frac{\alpha}{2} - \frac{\beta}{2}\right) = -\tan\left(\frac{\alpha}{2} + \frac{\beta}{2}\right) =$$

$$= -\frac{\tan\left(\frac{\alpha}{2}\right) + \tan\left(\frac{\beta}{2}\right)}{1 - \tan\left(\frac{\alpha}{2}\right)\tan\left(\frac{\beta}{2}\right)} = -\frac{u+v}{1-uv}.$$

Volviendo a la ecuación (4.1), tenemos:

$$u + v + w = \frac{s^2}{A} = k,$$

donde k es la constante que representa a $\frac{s^2}{A}$. Ahora sustituimos w por la relación anterior:

$$u + v - \frac{u+v}{1-uv} = k. \tag{4.2}$$

Y multiplicando por el denominador,

$$u^2v + uv^2 - kuv + k = 0. \tag{4.3}$$

Procedemos a aplicar una serie de cambios de variable para obtener una expresión en forma de Weierstrass y ver así que nos encontramos ante la ecuación de una curva elíptica. En primer lugar, homogeneizamos la ecuación (4.3). Hacemos el cambio $u \longmapsto X$, $v \longmapsto Y$:

$$X^2Y + XY^2 - kXYZ = -kZ^3. \tag{4.4}$$

Y aplicamos el cambio $X \longmapsto 1$, $Y \longmapsto -\frac{1}{216k}\left(y + 3k(x - 3k^2) + 108k\right)$, $Z \longmapsto \frac{3k^2-x}{36k}$, obteniendo la forma de Weierstrass:

$$E_k : y^2 = x^3 - 27(k^4 - 24k^2)x + 54k^6 - 1944k^4 + 11664k^2. \tag{4.5}$$

La curva E_k parametriza los triángulos tales que $s^2/A = k$. Volviendo a la pregunta inicial, podemos demostrar ahora que dos triángulos con el mismo área y perímetro

no son necesariamente congruentes. Basta con tomar dos puntos de la curva que correspondan a dos triángulos distintos. Veamos un ejemplo para $k = 6$.

En este caso, la ecuación de la curva sería la siguiente:

$$E_6 : y^2 = x^3 - 11664x + 419904. \tag{4.6}$$

Utilizando Sage, vemos que el subgrupo de torsión es isomorfo a $\mathbb{Z}/3\mathbb{Z}$ y contiene los puntos $\mathcal{O}, (108, 648)$ y $(108, -648)$. Además, el rango de la curva es 1, por lo que el Grupo de Mordell es:

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Código 4.1: Grupo de Mordell

```
E = EllipticCurve([-11664, 419904])
G = E.torsion_subgroup()
print G
# Torsion Subgroup isomorphic to Z/3
# associated to the Elliptic Curve defined
# by y^2 = x^3 - 11664*x + 419904 over Rational Field

print [E(p) for p in G]
# [(0 : 1 : 0), (108 : 648 : 1), (108 : -648 : 1)]

print "Rank:" + str(E.rank())
# Rank: 1

print "Generators:" + str(E.gens())
# Generators: [(-108 : 648 : 1)]
```

El generador de la parte libre del Grupo de Mordell es, por lo tanto, $(-108, 648)$.

Recordamos ahora que la pregunta con la que partíamos en este apartado era la de comprobar si todo par de triángulos con el mismo perímetro y el mismo área eran congruentes.

Para ello, vamos a definir una función que, dado un punto en la curva elíptica obtenida, deshaga los cambios de variable realizados hasta obtener la longitud de sus lados. Es decir, la función va a deshacer los cambios hasta obtener los ángulos α, β y γ.

En este punto, las longitudes de los lados del triángulo se calcularían como $a = r\ tan\frac{\alpha}{2}$, $b = r\ tan\frac{\beta}{2}$, $c = r\ tan\frac{\gamma}{2}$. Sin embargo, si dos triángulos son congruentes, entonces el radio r de la circunferencia circunscrita es el mismo. Por lo tanto, podemos tomar $r = 1$ para comprobar si dos puntos de la curva corresponden a triángulos congruentes entre sí.

Código 4.2: Función getTriangleSides()

```
def getTriangleSides(x, y, k):
    x1 = (x - 3*k^2)/36
    y1 = y/108

    x0 = x1
    y0 = 1/2*(y1 + k*x1 + k)

    X=1
    Y=-y0/k
    Z=-x0/k

    X=X/Z
    Y=Y/Z

    u=X
    v=Y
    w=-(u+v)/(1-u*v)

    a = u + v
    b = v + w
    c = u + w

    print "(" + str(a) + ", " + str(b) + ", " + str(c) + ")"
```

Ahora podemos comprobar que, para $k = 6$, el punto de la curva $(-32, 872)$ corresponde con el triángulo de lados $(41/15, 156/35, 101/21)$, cuyo perímetro es 12, por tanto, su área es 6. Por otro lado, el punto de la curva $(0, 648)$ se corresponde con un triángulo de lados $(3, 4, 5)$, cuyo perímetro vuelve a ser 12.

Por lo tanto, hemos encontrado un contraejemplo claro en el que dos triángulos que comparten perímetro y área tienen longitudes de lado diferentes y, por lo tanto, no son congruentes.

4.2. Un problema de triángulos rectángulos

¿Es posible encontrar dos triángulos rectángulos con lados enteros y la misma base, tales que sus alturas mantengan una relación $n : 1$?

Para responder a esta pregunta, recurrimos a un argumento ideado por A. J. Macleod [5] para trasladar este problema a uno equivalente sobre curvas elípticas.

Los triángulos sobre los que trabajaremos serán los siguientes:

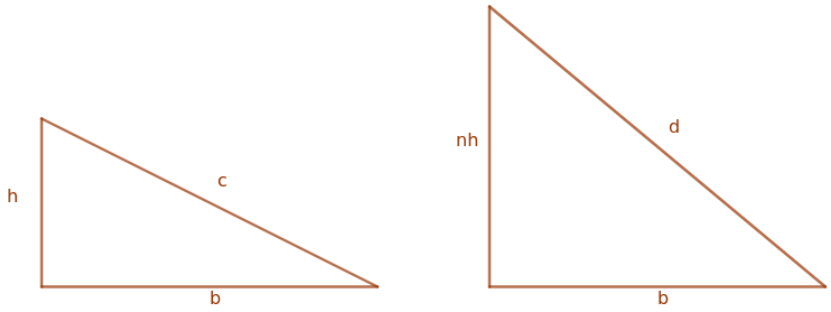

Figura 4.3: Triángulos rectángulos con alturas h y nh.

Por lo tanto, aplicando el Teorema de Pitágoras obtendríamos la siguiente relación:

$$b^2 + h^2 = c^2 \tag{4.7}$$

$$b^2 + (nh)^2 = d^2 \tag{4.8}$$

El problema se reduce a encontrar triángulos con lados racionales, ya que estos se pueden escalar a triángulos enteros manteniendo la relación entre las alturas.

Buscamos ahora una parametrización de un triángulo rectángulo tal que $a^2+b^2 = c^2$. Vemos que $(a/c)^2 + (b/c)^2 = 1$, por lo que tomamos $X = a/c$, $Y = b/c$, llegando a la circunferencia

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

con $(X, Y) \in \mathbb{Q}^2$. Se tiene que el punto $(1, 0)$ pertenece a la circunferencia. Por lo tanto, trazando una recta que pase por dicho punto, con pendiente $t \in \mathbb{Q}$, parametrizamos la segunda coordenada como $Y = t(X - 1)$ y llegamos a la siguiente ecuación

$$X^2 + t^2(X - 1)^2 = 1.$$

Que tiene como soluciones $X = 1$ y $X = (t^2 - 1)/(t^2 + 1)$. En el primer caso, $Y = 0$ y, en el segundo, $Y = -2t/(t^2 + 1)$. Como el punto $(1, 0)$ no se corresponde con un triángulo, solo tiene sentido ver el caso $(\frac{t^2-1}{t^2+1}, \frac{-2t}{t^2+1})$.

Deshaciendo el cambio de coordenadas inicial, llegamos a que

$$\frac{a}{c} = X = \frac{t^2 - 1}{t^2 + 1}.$$

Por lo que $a = \lambda(t^2 - 1)$ y $c = \lambda(t^2 + 1)$, para un cierto $\lambda \in \mathbb{Q}$. Por otro lado,

$$\frac{b}{c} = Y = \frac{-2t}{t^2 + 1}.$$

Por lo tanto, $b = -2t\lambda$. Podemos asumir que $t < 0$ y tomar $r = -t$ para llegar a $a = \lambda(r^2 - 1)$, $b = 2r\lambda$ y $c = \lambda(r^2 + 1)$ con $r > 0$.

Usando esta parametrización en las ecuaciones (4.7) y (4.8), tomamos ahora $g, f, \lambda, \nu \in \mathbb{Q}$ tales que $b = \lambda(f^2-1) = \nu(g^2-1)$, $h = 2\lambda f$ y $nh = 2\nu g$. Despejando en la primera ecuación, obtenemos

$$\lambda = \frac{b}{f^2-1}$$

$$\nu = \frac{b}{g^2-1}.$$

Nótese que $f, g \neq \pm 1$, puesto que la base del triángulo tiene que ser mayor que cero y, por el mismo motivo, $\lambda, \nu \neq 0$. Además, como la altura no puede ser nula, $f, g \neq 0$. Y, por tanto, tenemos

$$n = \frac{\nu g}{\lambda f} = \frac{(f^2-1)g}{(g^2-1)f}.$$

Con el siguiente cambio de coordenadas, $f \mapsto X/Z$ y $g \mapsto Y/Z$, obtenemos la siguiente ecuación:

$$Y(X^2 - Z^2) = nX(Y^2 - Z^2).$$

Usando ahora $X \mapsto 16n^2y$, $Y \mapsto -4nxy$, $Z \mapsto 8n^2x^2 + 32n^2x$, obtenemos lo siguiente:

$$(4n^2x^2 + 16n^2x + x^3 + 4x^2 - y^2)(x+4)xy = 0.$$

En los casos $x = -4$ y $x = 0$ llegamos a que $Z = 0$, lo cual, por cómo está definido el cambio de coordenadas ((f, g) pertenece al plano afín), no tiene sentido. En el caso $y = 0$, f y g valdrían 0 también, lo que implica que al altura de los triángulos, que viene dada por la ecuación $h = 2\lambda f = \frac{2\nu g}{n}$, sería nula.

Por lo tanto, el único caso que tiene sentido es

$$E_n : y^2 = x^3 + 4(n^2+1)x^2 + 16n^2x. \tag{4.9}$$

Obtenemos así la ecuación de una familia de curvas elípticas E_n que parametrizan el conjunto de triángulos con la misma base b y altura nh. Es decir, si tomamos un punto de la curva E_1 y un punto de la curva E_4, sus triángulos asociados tendrán la misma base y alturas con una relación 1:4.

Vamos a analizar ahora los puntos de orden dos, que son aquellos tales que $y = 0$ (puesto que, como $2P = 0$, es necesario que $P = -P$). Estos puntos vienen dados por la ecuación

$$x^3 + 4(n^2+1)x^2 + 16n^2x = 0. \tag{4.10}$$

que tiene soluciones $(0,0)$, $(-4,0)$ y $(-4n^2, 0)$. El Teorema de Mazur nos dice que el grupo de torsión es isomorfo, o bien a $\mathbb{Z}/n\mathbb{Z}$ para $1 \leq n \leq 10$, o $n = 12$, o bien a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ para $1 \leq n \leq 4$. Como no hay ningún grupo cíclico de los mencionados que tenga tres puntos de orden 2, necesariamente el grupo de torsión será $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$.

Veamos ahora que existen puntos de orden 4, descartando así el caso $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Sea P un punto de orden 4, entonces $2P$ tendrá orden 2. Si P tiene coordenadas (u, v), usando la fórmula explícita de la suma llegaríamos a que la primera coordenada

del punto $2P$ sería $(u^2-16n^2)^2/4v^2$, que es mayor o igual que 0. Por lo tanto, el único punto de los anteriores que puede obtenerse de esta forma sería el $(0,0)$. Tendríamos

$$u^2 - 16n^2 = 0.$$

Es decir, un punto $P = (u, v)$ tiene orden 4 sí y solo sí cumple $u = \pm 4n$. Esto nos lleva a cuatro posibles puntos: $(4n, \pm 8n(n+1))$, $(-4n, \pm 8n(n-1))$. Como estos cuatro puntos son racionales, también pertenecen al grupo de torsión. Por lo tanto tenemos, por lo menos, 8 puntos de torsión. Como, además, existen únicamente cuatro puntos de orden 4, sabemos que el grupo de torsión será isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ o a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

Falta ver, entonces, si existen o no puntos de orden 8.

De nuevo, si $P = (u, v)$ tiene orden 8, entonces $2P$ tendrá orden 4 y será uno de los cuatro posibles puntos obtenidos anteriormente. Usando la fórmula explícita, tendríamos

$$\frac{(u^2-16n^2)^2}{4v^2} = \frac{(u^2-16n^2)^2}{4(u^3+4(n^2+1)u^2+16n^2u)} = \pm 4n.$$

Como la parte izquierda de la ecuación es positiva, sólo tiene sentido estudiar el caso

$$\frac{(u^2-16n^2)^2}{4(u^3+4(n^2+1)u^2+16n^2u)} = 4n.$$

Esto se cumple sí y solo sí $n = k^2$, por lo que podemos reescribirlo como

$$\frac{(u^2-16k^4)^2}{4(u^3+4(k^4+1)u^2+16k^4u)} = 4k^2.$$

Las únicas soluciones serían, entonces:

$$u = 4(-k^3 + k^2 \pm \sqrt{k^6 - 2k^5 + 2k^4 - 2k^3 + k^2} - k)$$

y

$$u = 4(k^3 + k^2 \pm \sqrt{k^6 + 2k^5 + 2k^4 + 2k^3 + k^2} + k).$$

En el primer caso, para que u sea racional, $\sqrt{k^6 - 2k^5 + 2k^4 - 2k^3 + k^2} = m^2$ para algún m entero. Pero $\sqrt{k^6 - 2k^5 + 2k^4 - 2k^3 + k^2} = \sqrt{k^2(k^2+1)(k-1)^2}$. Sin embargo, es imposible que $\sqrt{(k^2+1)} = m'$ para m' entero y $k \geq 1$ (puesto que $n = k^2$ y $n \geq 1$).

El segundo caso es similar. Como $\sqrt{k^6 + 2k^5 + 2k^4 + 2k^3 + k^2} = \sqrt{k^2(k^2+1)(k+1)^2}$, también es imposible que u sea racional.

Por tanto, no existen puntos de orden 8, y el grupo de torsión es isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, siendo sus elementos los 7 puntos que hemos obtenido, más el punto $\mathcal{O}$.

El problema viene cuando tratamos de encontrar el triángulo asociado a cada uno de estos puntos.

En los de orden 2, si $x = 0$ o $x = -4$, entonces f no está definido según nuestro cambio de coordenadas. En el caso $x = -4n^2$, tendríamos que tanto f como g serían iguales a 0 y, por lo tanto, la altura sería nula, así que no daría lugar a un triángulo.

En los puntos de orden 4, el hecho de que $x = 4n$ implica $X = -Y$, deshaciendo el cambio, por lo que $n = -1$ (lo cual no tiene sentido). Si, por otro lado, $x = -4n$, entonces $X = Y$ y $Z = 128n^3(n-1)$, por lo que $f = g$. En este caso, como $n = \frac{(f^2-1)g}{(g^2-1)f}$, $n = 1$. Sin embargo, esto llevaría a que $Z = 0$ y entonces el cambio no estaría definido.

Teorema 4.2. *Existen dos triángulos rectángulos con lados enteros y la misma base tales que sus alturas mantienen una relación $n : 1$ sí y solo sí el rango de $E_n(\mathbb{Q}) \neq 0$.*

Para ver algunos ejemplos, hemos calculado el rango de E_n para $2 \leq n \leq 50$ usando el siguiente código en *Magma*[6].

Código 4.3: Cálculo de rangos para n entre 2 y 50

```
for n in [2 .. 50] do
    E:=EllipticCurve([0, 4*(n^2 + 1), 0, 16*n^2, 0]);
    R:=Rank(E);
    printf "n: %o, rank: %o\n", n, R;
end for;
```

Los resultados son los siguientes:

n	Rango	n	Rango	n	Rango	n	Rango
2	0	3	0	4	0	5	0
6	0	7	1	8	0	9	0
10	1	11	1	12	1	13	0
14	1	15	0	16	0	17	1
18	0	19	1	20	0	21	0
22	1	23	1	24	0	25	0
26	0	27	1	28	1	29	1
30	1	31	0	32	0	33	1
34	0	35	0	36	0	37	0
38	1	39	1	40	1	41	2
42	1	43	0	44	1	45	1
46	0	47	1	48	1	49	0
50	0						

Tabla 4.1: Tabla del rango de E_n.

Tomamos ahora, por ejemplo, la curva E_{44}, que tiene rango 1. Usando la función *gens*() de Sage, vemos que el generador de la parte libre es el punto $(5776, 671840)$. Queremos hallar ahora dos triángulos con la misma base, digamos $b = 10$, lados racionales y alturas con una proporción $1 : 44$. Para eso, deshacemos los cambios hasta obtener los parámetros f y g y calculamos la altura y la hipotenusa c del triángulo. De ese modo, obtenemos los triángulos de lados $(10, 4199/5208, 52249/5208)$ y $(10, 46189/1302, 47989/1302)$, que cumplen con las condiciones del problema (las coordenadas representan base, altura e hipotenusa, respectivamente). Para obtener

triángulos de lados enteros, basta multiplicar cada coordenada por el máximo común divisor.

La siguiente función en Sage permite calcular pares de triángulos en estas condiciones, dadas las coordenadas (x, y) de un punto de orden infinito, la proporción n entre las alturas, y una base b.

Código 4.4: Obtención de soluciones racionales del problema

```
def getProportionalTriangles(x, y, n, b):
    X = 16*n^2*y
    Y = -4*n*x*y
    Z = 8*n^2*x^2 + 32*n^2*x

    f = X / Z
    g = Y / Z

    lda = b / (f^2 - 1)
    nu = n*lda

    h = abs(2*lda*f)
    c = sqrt(b^2 + h^2)

    nh = n*h
    nc = sqrt(b^2 + nh^2)

    print "(" + str(b) + ", " + str(h) + ", " + str(c) + ")"
    print "(" + str(b) + ", " + str(nh) + ", " + str(nc) + ")"

    return

x = 5776
y = 671840
n = 44
b = 10

getProportionalTriangles(x,y,n,b)
# (10, 4199/5208, 52249/5208)
# (10, 46189/1302, 47989/1302)
```

4.3. El problema del número congruente

Se dice que un número $n \in \mathbb{Z}$ es congruente si se corresponde con el área de un triángulo rectángulo de Herón (con lados racionales). En esta sección vamos a resolver el conocido como "Problema del Número Congruente":

Dado un entero positivo n, encuentra un triángulo rectángulo con lados racionales tal que su área sea igual a n.

Se trata de uno de los problemas matemáticos más antiguos de la teoría de números. El primer resultado relevante acerca de los números congruentes se remonta al siglo XVII, cuando Fermat demostró que 1 no es un número congruente. Aun-

que también se pueden encontrar referencias a estos números en obras como el *Liber Quadratorum*, de Fibonacci, publicado en 1225 e incluso en manuscritos arábicos que datan del siglo X, como el manuscrito de al-Kazin (en la Biblioteca Nacional de París) ya incluían tablas de números congruentes.

Obsevación 4.3. *Asumiremos en todo momento que n es un entero positivo libre de cuadrados, puesto que si (a, b, c) es un triángulo rectángulo con área n, entonces (as, bs, cs) es también un triángulo rectángulo con área ns^2. Por lo tanto, basta demostrar que n es congruente para ver que ns^2 también lo es.*

El número n, por tanto, será congruente sí y solo sí existen $a, b, c \in \mathbb{Q}$ tales que:

$$\begin{cases} a^2 + b^2 = c^2, \\ \frac{ab}{2} = n. \end{cases} \tag{4.11}$$

Queremos analizar ahora este sistema de ecuaciones. Tomamos $c = t + a$ en la primera ecuación, obteniendo:

$$2at = b^2 - t^2. \tag{4.12}$$

Por otro lado, como $\frac{ab}{2} = n$ y $n \neq 0$, tanto a como b con distintos de 0 y entonces $a = \frac{2n}{b}$. Sustituyendo ahora en la ecuación anterior:

$$\frac{4nt}{b} = b^2 - t^2. \tag{4.13}$$

Multiplicando ahora ambos lados por $\frac{bn^3}{t^3}$ obtenemos:

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{nb}{t}\right)^3 - n^2\left(\frac{nb}{t}\right). \tag{4.14}$$

Finalmente, si sustituimos $x = \frac{nb}{t} = \frac{nb}{c-a}$, $y = \frac{2n^2}{t} = \frac{2n^2}{c-a}$, obtendremos la ecuación de una familia de curvas elípticas que parametrizan el conjunto de triángulos rectángulos con área n:

$$E_n : y^2 = x^3 - n^2 x. \tag{4.15}$$

Por lo tanto, el problema del número congruente queda reducido a encontrar un punto racional en la curva E_n. Queremos ver, entonces, cómo es el grupo de Mordell de la curva.

Al igual que en el problema anterior, comenzamos analizando los puntos de orden 2, que son aquellos tales que $y = 0$. La ecuación resultante, $x^3 - n^2 x = 0$, tiene tres soluciones: $(0, 0)$, $(n, 0)$ y $(-n, 0)$. Estos serán los únicos puntos de orden dos en E_n.

De nuevo, recurrimos al Teorema de Mazur para estudiar el subgrupo de torsión. Como no hay ningún grupo cíclico de orden $1 \leq n \leq 10$ o $n = 12$ con tres puntos de orden dos, necesariamente el grupo de torsión será $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, con $1 \leq n \leq 4$.

Veamos ahora que no existen puntos de 3-torsión ni de 4-torsión.

Supongamos que $P = (u, v)$ es un punto de orden 4, por lo que $2P$ será un punto de orden 2. En ese caso, usando la fórmula explícita de la suma, llegamos a que la primera coordenada del punto $2P$ será $(u^2 + n^2)^2/4v^2$, que es mayor o igual que cero. Por tanto, $2P$ tendría que ser igual a $(0, 0)$ o a $(n, 0)$.

En el primer caso, tendríamos la ecuación

$$u^2 + n^2 = 0,$$

lo cual es imposible, puesto que $n > 0$.

En el segundo caso, tendríamos

$$\frac{(u^2 + n^2)^2}{4v^2} = \left(\frac{u^2 + n^2}{2v}\right)^2 = n$$

lo que significa que n es un cuadrado, pero desde el principio hemos asumido que n es un entero libre de cuadrados. Por lo tanto, este caso también es imposible.

Suponemos ahora que $P = (u, v)$ es un punto de orden 3, lo que significa que $2P = -P$. Si observamos que la primera coordenada de P es igual a la primera coordenada de $-P$, y que la primera coordenada de $2P$ es, de nuevo, $(u^2 + n^2)^2/4v^2$, obtenemos la siguiente ecuación:

$$\frac{(u^2 + n^2)^2}{4v^2} = \frac{(u^2 + n^2)^2}{4(u^3 - n^2u)} = u.$$

Si la resolvemos sobre n, obtenemos $n = u\sqrt{-3 \pm 2\sqrt{3}}$ o $n = -u\sqrt{-3 \pm 2\sqrt{3}}$ que en ningún caso puede ser un número racional, y mucho menos un número entero. Por lo tanto, esta situación también es imposible.

Hemos probado que no existen puntos de orden 3 ni puntos de orden 4, además de que existen tres puntos de orden 2. Por tanto, podemos afirmar que el subgrupo de torsión es isomorfo a $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ y está formado por los puntos $\{\mathcal{O}, (0, 0), (n, 0), (-n, 0)\}$.

Ahora bien, si recordamos los cambios de coordenadas $x = \frac{nb}{c-a}$, $y = \frac{2n^2}{c-a}$ que nos han traido hasta aquí, observaremos que ninguno de estos puntos de orden 2 se corresponde con un triángulo. Esto es porque su segunda coordenada es, en todos los casos, igual a cero, lo que implicaría $0 = \frac{2n^2}{c-a}$ y, por tanto, $n = 0$ (no existen triángulos de área 0).

En conclusión, ningún punto de orden finito (perteneciente al subgrupo de torsión) está asociado a un triángulo con las características que buscamos. Por lo tanto, podemos enunciar el siguiente teorema:

Teorema 4.4. *Un número entero positivo n es congruente sí y solo sí la curva*

$$E_n : y^2 = x^3 - n^2x$$

tiene puntos de orden infinito, es decir, tiene rango mayor que 0.

Hemos obtenido así un método que nos permite saber cuándo un número n es congruente y, por tanto, es equivalente al área de un triángulo de Herón.

Apéndices

APÉNDICE A
Demostraciones complementarias de asociatividad

En este apéndice se incluyen las demostraciones pendientes de ciertas propiedades tratadas en la sección 2.2.4. Estas pruebas se han realizado utilizando el software *SageMath*, que emplea *Python3* y, por tanto, tiene sintaxis similar.

En primer lugar, definimos la operación sobre dos puntos de una curva elíptica:

Código A.1: Definición de la operación suma

```
def suma(xa, ya, xb, yb):
    if xa != xb:
        alpha = (yb-ya)/(xb-xa)
    else:
        alpha = (3*xa^2 + a)/(2*ya)
    x = alpha^2 - xa - xb
    y = -ya + alpha*(xa - x)

    return {'x': x, 'y':y}
```

A.1. Lema 2.10

Sean $P, Q, R \in E(\mathbb{Q}) \setminus \mathcal{O}$. Si $P \neq \pm Q, Q \neq \pm R, P + Q \neq \pm R$ y $Q + R \neq \pm P$, entonces

$$P + (Q + R) = (P + Q) + R.$$

Demostración. Se establece que los pares *(xp, yp), (xq, yq), (xr, yr)* satisfacen la ecuación $y^2 - x^3 - ax - b = 0$ y, por tanto, viven en la curva establecida. Para ello se define un anillo polinómico sobre $\mathbb{Z}$ extendido con todas las variables que necesitamos.

Código A.2: Definición del cociente

```
Z = IntegerRing()
R.<xp,xq,xr,yp,yq,yr,a,b>=PolynomialRing(Z,8)
I = R.ideal(yp^2-xp^3-a*xp-b, yq^2-xq^3-a*xq-b, yr^2-xr^3-a*xr-b)
RI = R.quotient(I)
```

Utilizando la función suma definida anteriormente, y trabajando sobre el anillo cociente (*Código A.2*), vemos que las coordenadas del punto $(P+Q)+R$ son iguales a las del punto $P+(Q+R)$.

Las condiciones enunciadas en el lema son necesarias para garantizar que no existan ceros ni polos en los polinomios empleados en estos cálculos, permitiendo así su automatización mediante cálculo simbólico.

Código A.3: Demostración del lema 2.10

```
res_pq = suma(xp, yp, xq, yq) # P + Q
res_qr = suma(xq, yq, xr, yr) # Q + R

res1 = suma(res_pq['x'], res_pq['y'], xr, yr) # (P + Q) + R
res2 = suma(xp, yp, res_qr['x'], res_qr['y']) # P + (Q + R)

resta_x = res1['x']-res2['x']
print('Numerador: ' + str(RI(resta_x.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_x.denominator() != 0))))
# Numerador: 0
# Denominador != 0: True

resta_y = res1['y'] - res2['y']
print('Numerador: ' + str(RI(resta_y.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_y.denominator() != 0))))
# Numerador: 0
# Denominador != 0: True
```

□

A.2. Lema 2.11

Sean $P, Q \in E(\mathbb{Q}) \setminus \mathcal{O}$. Si $P \neq -P, P \neq \pm Q, P+P \neq \pm Q$ y $P+Q \neq \pm P$, entonces

$$(P+P)+Q = P+(P+Q).$$

Demostración. De nuevo, se establece que los pares *(xp, yp), (xq, yq)* satisfacen la ecuación $y^2 - x^3 - ax - b = 0$.

Código A.4: Definición del cociente

```
Z = IntegerRing()
R.<xp,xq,yp,yq,a,b>=PolynomialRing(Z,6)
I = R.ideal(yp^2-xp^3-a*xp-b, yq^2-xq^3-a*xq-b)
RI = R.quotient(I)
```

A continuación, al igual que en el lema anterior, se comprueba mediante cálculo simbólico que las coordenadas del punto $(P+P)+Q$ son iguales a las del $P+(P+Q)$.

Código A.5: Demostración del lema 2.11

```
res_pp = suma(xp, yp, xp, yp) # (P + P)
res1 = suma(res_pp['x'], res_pp['y'], xq, yq) # (P + P) + Q

res_pq = suma(xp, yp, xq, yq) # P + Q
res2 = suma(xp, yp, res_pq['x'], res_pq['y']) # P + (P + Q)

resta_x = res1['x'] - res2['x']
print('Numerador: ' + str(RI(resta_x.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_x.denominator() != 0))))
# Numerador: 0
# Denominador!= 0: True

resta_y = res1['y'] - res2['y']
print('Numerador: ' + str(RI(resta_y.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_y.denominator() != 0))))
# Numerador: 0
# Denominador!= 0: True
```

□

A.3. Lema 2.12

Sea $P \in E(\mathbb{Q}) \setminus \mathcal{O}$. Si $P \neq -P, P+P \neq -(P+P), (P+P)+P \neq \pm P$ y $P+P \neq \pm P$, entonces

$$(P+P)+(P+P) = P+(P+(P+P)).$$

Demostración. Esta vez tomamos el siguiente cociente:

Código A.6: Definición del cociente

```
Z = IntegerRing()
R.<xp,yp,a,b>=PolynomialRing(Z,4)
I = R.ideal(yp^2-xp^3-a*xp-b)
RI = R.quotient(I)
```

A continuación, comprobamos que las coordenadas del punto $(P+P)+(P+P)$ coinciden con las del punto $P+(P+(P+P))$.

Código A.7: Demostración del lema 2.12

```
res_pp = suma(xp, yp, xp, yp) # P + P
res1 = suma(res_pp['x'], res_pp['y'], res_pp['x'], res_pp['y']) # (P+P)+(P+P)

res_ppp = suma(xp, yp, res_pp['x'], res_pp['y']) # P + (P + P)
res2 = suma(xp, yp, res_ppp['x'], res_ppp['y']) # P + (P + (P + P))

resta_x = res1['x'] - res2['x']
print('Numerador: ' + str(RI(resta_x.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_x.denominator() != 0))))
# Numerador: 0
# Denominador!= 0: True

resta_y = res1['y'] - res2['y']
print('Numerador: ' + str(RI(resta_y.numerator())))
print('Denominador != 0: ' + str(bool(RI(resta_y.denominator() != 0))))
# Numerador: 0
# Denominador!= 0: True
```

□

A.4. Cálculos del Teorema 2.15

Sea $P \in E(\mathbb{Q})$, si $P \neq -P$ y $(P+P) \neq -P$, entonces $(P+P)-P = P$.

Demostración. Para obtener la ecuación (2.1) hemos empleado cálculo simbólico en *Sage*.

En el caso $P = (x, y)$ y $P+P = (x_2, y_2)$ con $x \neq x_2$, se tiene que, para $\lambda = \frac{3x^2+A}{2y}$, entonces $x_2 = \lambda^2 - 2x$ y $y_2 = -y - \lambda(x_2 - x)$. Ha sido necesario reescribir estas relaciones, multiplicando por el denominador de λ, para poder generar el ideal con *Sage*. La primera quedaría como

$$4y^2(x_2 + 2x) - (3x^2 + A)^2$$

Y la segunda:

$$2yy_2 + 2y^2 + (3x^2 + A)(x_2 - x)$$

Ahora, empleando la función suma definida anteriormente, calculamos la primera coordenada de $(P+P)-P$ y comprobamos que es igual a x.

Código A.8: Obtención de la ecuación (2.1)

```
Z = IntegerRing()
R.<x,y,x2,y2,a,b>=PolynomialRing(Z,6)
I = R.ideal(y^2-x^3-a*x-b, y2^2-x2^3-a*x2-b, 4*y^2*(x2+2*x) -
(3*x^2 + a)^2, 2*y*y2 + 2*y^2 + (3*x^2 + a)*(x2-x))
# Ecuaciones de la curva, de x2 y de y2
RI = R.quotient(I)

# P = (x,y)
# P + P = (x2, y2)
objetivo = suma(x2,y2,x,-y)['x'] - x
# Primera coordenada de (P + P) - P menos x

print("Numerador: " + str(RI(objetivo.numerator())))
print("Denominador: " + str(RI(objetivo.denominator())))
# Numerador: 0
# Denominador: xbar^2 - 2*xbar*x2bar + x2bar^2
```

Concluimos, por tanto, que

$$x_2 = x$$

□

A.5. Teorema 2.18

Sean $P, Q \in E(\mathbb{Q})$, entonces $(P+Q)-Q = P$.

Demostración. Falta por probar el caso en el que $P+Q \neq -Q$, $P \neq \mathcal{O}$, $Q \neq \mathcal{O}$, $P \neq -Q$, $P \neq Q$ y $Q \neq P+Q$. Se empleará cálculo simbólico, por lo que las condiciones anteriores son necesarias para que no se produzca ninguna anulación en el cálculo.

Fijamos entonces un anillo cociente en el que (xp, yp) representan las coordenadas del punto P y (xq, yq), las del punto Q. Vamos a calcular $(P+Q)-Q$ usando la función suma definida anteriormente, y a comprobar que las coordenadas resultantes coinciden con las del punto P.

Código A.9: Demostración del Teorema 2.18

```
Z = IntegerRing()
R.<xp,yp,xq,yq,a,b>=PolynomialRing(Z,6)
I = R.ideal(yp^2-xp^3-a*xp-b, yq^2-xq^3-a*xq-b) # Ecuaciones de las curvas
RI = R.quotient(I)

# P = (xp, yp)
# Q = (xq, yq)
# P + Q = R = (xr, yr)
PQ = suma(xp,yp,xq,yq)
xr = PQ['x']
yr = PQ['y']

# (P + Q) - Q
res = suma(xr,yr,xq,-yq)
resx = res['x']
resy = res['y']

objetivox = resx - xp
print("Numerador primera coordenada: " + str(RI(objetivox.numerator())))
print("Denominador primera coordenada: " + str(RI(objetivox.denominator())))
# Numerador primera coordenada: 0
# Denominador primera coordenada: 1

objetivoy = resy - yp
print("Numerador segunda coordenada: " + str(RI(objetivoy.numerator())))
print("Denominador segunda coordenada: " + str(RI(objetivoy.denominator())))
# Numerador segunda coordenada: 0
# Denominador segunda coordenada: 1
```

□

APÉNDICE B

Teorema de Estructura para grupos abelianos finitamente generados

El objetivo de este apéndice es estudiar la estructura de los grupos abelianos finitamente generados tal y como se explica en los apuntes de Estructuras Algebraicas del Departamento de Álgebra de la Facultad de Ciencias de la Universidad de Sevilla [1] en los que nos hemos basado.

Vamos a presentar una serie de teoremas y proposiciones que nos llevarán a demostrar el resultado principal del apartado.

B.1. Teoremas previos

Definición B.1. Sea G un grupo y S un conjunto finito, se dice que G es **finitamente generado** si $G = \langle S \rangle$. En concreto, en esta sección nos centraremos en los grupos abelianos finitamente generados.

Definición B.2. Se dice que el conjunto $\mathcal{B} = \{u_1, ..., u_n\} \subset \mathbb{Z}^n$ es una **base de** $\mathbb{Z}^n$ si es un conjunto generador de todo el espacio y, además, todos sus componentes son linealmente independientes.

Teorema B.3. *Sea $\{u_1, ..., u_n\}$ una base de $\mathbb{Z}^n$, G un grupo abeliano de n elementos $\alpha_1, ...\alpha_n \in G$, existe un único homomorfismo de grupos*

$$f : \mathbb{Z}^n \longrightarrow G$$

tal que $f(u_i) = \alpha_i$ para todo $i = 1, ..., n$.

Demostración. Si tomamos $a \in \mathbb{Z}^n$, sabemos que existen $m_1, ..., m_n$ tales que $a = m_1u_1 + ... + m_nu_n$. Sea $f : \mathbb{Z}^n \longrightarrow G$, la condición de que f sea un homomorfismo y, además, $f(u_i) = \alpha_i$, nos lleva a definir f como $f(a) = m_1f(\alpha_1) + ... + m_nf(\alpha_n) = m_1\alpha_1 + ... + m_n\alpha_n$.

Esta aplicación está bien definida, es claramente un homomorfismo y, además, es necesariamente la única que cumple las condiciones especificadas. □

Teorema B.4. *Todo grupo abeliano finitamente generado es isomorfo a un cociente de $\mathbb{Z}^n$.*

Demostración. Sea $G = \langle \alpha_1, ..., \alpha_n \rangle$, tomamos el homomorfismo $f : \mathbb{Z}^n \longrightarrow G$ resultado del teorema anterior. Dicho homomorfismo es sobreyectivo, ya que $\alpha_1, ..., \alpha_n \in Im(f)$ y $\langle \alpha_1, ..., \alpha_n \rangle = G$.

Por tanto, podemos aplicar el primer teorema de isomorfía:

$$\mathbb{Z}^n \Big/ ker(f) \cong Im(f) = G.$$

Donde es claro que $ker(f) \leq \mathbb{Z}^n$ □

Gracias a este teorema, vemos que estudiar los grupos abelianos finitamente generados es equivalente a estudiar los grupos cocientes de la forma $\mathbb{Z}^n/H$.

Teorema B.5. *Todo subgrupo $H \leq \mathbb{Z}^n$ es finitamente generado y admite un sistema de generadores con un máximo de n elementos.*

Demostración. En el caso $n = 1$, ya sabemos que $H = \langle m \rangle$ para cierto entero m. Vamos a proceder por inducción, suponiendo $n > 1$ y que el teorema es cierto para $n - 1$.

Tomamos $\pi_1 : \mathbb{Z}^n \longrightarrow \mathbb{Z}$ como la proyección sobre la primera coordenada. En concreto, dados $a, b \in \pi_1(H)$, existen $(a, a_2, ..., a_n)$, $(b, b_2, ..., b_n) \in H$. Entonces $(a - b, a_2 - b_2, ..., a_n - b_n) \in H$, por lo que $a - b \in \pi_1(H)$, y $\pi_1(H) \leq \mathbb{Z}$.

Por lo tanto, $\pi_1(H) = \langle a \rangle$ para cierto $a \in \mathbb{Z}$, y debe existir un elemento $u_0 = (a, a_2, ..., a_n) \in H$.

Vemos también que $ker(\pi_1) = \{(0, a_2, ..., a_n) \in \mathbb{Z}^n\}$ es isomorfo a $\mathbb{Z}^{n-1}$, y que $H \cap ker(\pi_1) \leq ker(\pi_1)$. Por tanto, $H \cap ker(\pi_1)$ es isomorfo a un subgrupo de $\mathbb{Z}^{n-1}$.

Por hipótesis de inducción, sabemos que $H \cap ker(\pi_1)$ es finitamente generado y, entonces, $H \cap ker(\pi_1) = \langle u_1, ..., u_r \rangle$ con $r \leq n - 1$.

Ahora tomamos un elemento $u = (ma, c_2, ..., c_n) \in H$ genérico. Tendremos que $u - mu_0 = (0, c_2 - ma, ..., c_n - ma) \in H \cap ker(\pi_1)$, luego $u \in \langle u_0, u_1, ..., u_r \rangle$ para todo $u \in H$. Entonces $H = \langle u_0, u_1, ..., u_r \rangle$. Además, como $r \leq n - 1$, tenemos que el número de generadores de H será $r + 1 \leq n$, justo como pretendíamos. □

B.2. Forma Normal de Smith

Queremos demostrar que todo subgrupo $H \leq \mathbb{Z}^n$ puede escribirse como $H = \langle a_1, ..., a_s \rangle$, donde representaremos a_i como $a_i = (a_{1i}, ..., a_{ni})$. Usaremos la matriz

$$A = \begin{pmatrix} a_{11} & ... & a_{1s} \\ ... & ... & ... \\ a_{n1} & ... & a_{ns} \end{pmatrix}.$$

Definición B.6. Una **transformación elemental por columnas** de una matriz A, consiste en realizar una de las siguientes acciones:

1. Intercambiar dos columnas,
2. cambiar una columna de signo,
3. sumar a una columna un múltiplo de otra.

Aplicar una de estas transformaciones se consigue multiplicando A por una matriz elemental $E_{i,j}$, $E_i(-1)$ o $E_{i,j}(m)$, respectivamente, por la derecha. Estas matrices elementales tendrán determinante ± 1.

Además, al aplicar una transformación de este tipo, simplemente estamos cambiando el sistema de generadores de H.

Definición B.7. Una **transformación elemental por filas** de una matriz A, consiste en realizar una de las siguientes acciones:

1. Intercambiar dos filas,
2. cambiar una fila de signo,
3. sumar a una fila un múltiplo de otra.

En este caso, la transformación equivale a multiplicar por la derecha por las mismas matrices elementales, de nuevo con determinante ± 1.

Aplicar una transformación elemental por filas implica realizar un cambio de base.

En conclusión, podemos modificar la matriz A usando tantas de estas transformaciones como queramos, obteniendo como resultado un sistema de generadores de H, en cierta base de $\mathbb{Z}^n$.

Teorema B.8. *(Forma normal de Smith). Sea A una matriz como la definida anteriormente, existe una única matriz S de la forma*

$$S = \begin{pmatrix} d_1 & ... & 0 & 0 & ... & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & ... & d_r & 0 & ... & 0 \\ 0 & ... & 0 & 0 & ... & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & ... & 0 & 0 & ... & 0 \end{pmatrix}.$$

Donde $r \leq s$, $d_1, ..., d_r > 0$ y $d_i | d_{i+1}$ para todo $i = 1, ..., r-1$, tal que S se obtiene a partir de A mediante transformaciones elementales por filas y columnas.

Demostración. Comenzamos demostrando la existencia, para lo que vamos a aportar un procedimiento para calcular S.

1. Tomamos A y permutando filas y columnas, colocamos el número de menor valor absoluto, m, en la posición $(1,1)$, cambiando el signo de su columna para $m > 0$.

2. Si un elemento $a_{1,j}$ de la primera fila no es múltiplo de m, sabremos que $a_{1j} = qm + m'$, donde $0 < m' < m$. En ese caso, restamos a la columna j q veces la columna 1 y las permutamos, obteniendo ahora el elemento $m' < m$ en la posición $(1,1)$.

3. De forma análoga, podemos repetir el mismo procedimiento si hay algún elemento en la primera columna que no sea múltiplo de m.

4. Repetimos este procedimiento hasta que no haya múltiplos de m ni en la primera fila, ni en la primera columna y, sumando y restando múltiplos de las demás filas y columnas, obtenemos la matriz

$$\begin{pmatrix} m & 0 & ... & 0 \\ 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{pmatrix}.$$

5. Si hay algún elemento en una posición (i,j) que no sea múltiplo de m, se le suma la fila i a la fila 1, encontrándonos de nuevo en el caso de que un elemento de la primera fila no es múltiplo de m, y podremos reducirlo como antes. Repetimos este proceso hasta que m no se pueda reducir más, obteniendo la matriz

$$\begin{pmatrix} d_1 & 0 & ... & 0 \\ 0 & & & \\ \vdots & & M_1 & \\ 0 & & & \end{pmatrix},$$

donde d_1 divide a todo elemento de la matriz M_i.

6. Repetimos el mismo procedimiento sobre la matriz M_i, hasta obtener una matriz de la forma

$$\begin{pmatrix} d_1 & ... & 0 & 0 & ... & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & ... & d_r & 0 & ... & 0 \\ 0 & ... & 0 & 0 & ... & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & ... & 0 & 0 & ... & 0 \end{pmatrix},$$

donde $d_1, d_r > 0$. Además, como cada d_i divide a toda la matriz M_i, por la naturaleza de las transformaciones aplicadas, también va a dividir a todos los d_j con $j > i$. Por tanto, se cumple también que $d_i | d_{i+1}$ para todo $i = 1, ..., r-1$.

Faltaría por ver la unicidad de dicha matriz. Una primera observación es que r es el rango de A, puesto que las transformaciones aplicadas no alteran el rango.

Definimos $\Delta_i(A) = mcd(\{menores\ de\ orden\ i\ de\ A\})$

Observemos primero que aplicar una transformación elemental preserva el mcd de los menores de orden i de una matriz. Por lo tanto, $\Delta_i(A) = \Delta_i(S)$. Resulta sencillo comprobar que $\Delta_i(S) = d_1 \cdots d_i$.

Por tanto, los elementos $d_1, ..., d_r$ vienen determinados de forma única por la matriz A. □

Corolario B.9. *Dado un subgrupo $H \leq \mathbb{Z}^n$, existe una base $\mathcal{B} = \{u_1, ..., u_n\}$ de $\mathbb{Z}^n$ y unos enteros positivos $d_1|...|d_r$ tales que $H = \langle d_1u_1, ..., d_ru_r\rangle$.*

Demostración. Por el Teorema B.4 sabemos que todo subgrupo de $\mathbb{Z}^n$ es finitamente generado y admite un sistema de generadores con un máximo de n elementos. Tomamos entonces la matriz A como la formada por ese sistema de generadores de H sobre una base cualquiera $\mathcal{B}$ de $\mathbb{Z}^n$, y obtenemos su Forma Normal de Smith, que nos va a aportar r enteros $d_1|...|d_r$ que, además, cumplen $H = \langle d_1u_1, ..., d_ru_r\rangle$. □

B.3. Teorema de Estructura

Proposición B.10. En las condiciones anteriores,

$$\mathbb{Z}^n/_H \cong \mathbb{Z}/_{d_1\mathbb{Z}} \times \mathbb{Z}/_{d_2\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{d_r\mathbb{Z}} \times \mathbb{Z}^{n-r}.$$

Demostración. Procederemos empleando el primer teorema de isomorfía, para lo que vamos a definir la siguiente aplicación:

$$f : \mathbb{Z}^n \longrightarrow \mathbb{Z}/_{d_1\mathbb{Z}} \times \mathbb{Z}/_{d_2\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{d_r\mathbb{Z}} \times \mathbb{Z} \times \overset{n-r}{\cdots} \times \mathbb{Z}$$
$$(m_1, ..., m_n)_{\mathcal{B}} \longmapsto (\overline{m_1}, ..., \overline{m_r}, m_{r+1}, ..., m_n)$$

Obsevamos que la aplicación f está bien definida, y además es un homomorfismo de grupos sobreyectivo.

Además, $f((m_i)_{\mathcal{B}}) = 0 \iff m_i = k_id_i\ \forall i = 1, ..., r,\ m_i = 0\ \forall i = r+1, ..., n.$

Por tanto,

$$ker(f) = \{(k_1d_1, ..., k_rd_r, 0, ..., 0)_{\mathcal{B}};\ k_1, ..., k_r \in \mathbb{Z}\} = \langle d_1u_1, ..., d_ru_r\rangle = H.$$

Finalmente, por el primer teorema de isomorfía:

$$\mathbb{Z}^n/_H = \mathbb{Z}^n \Big/ ker(f) \cong Im(f) = \mathbb{Z}^n/_{d_1\mathbb{Z}} \times \mathbb{Z}^n/_{d_2\mathbb{Z}} \times \cdots \times \mathbb{Z}^n/_{d_r\mathbb{Z}} \times \mathbb{Z}^{n-r}$$

□

Teorema de Estructura de Grupos Abelianos Finitamente Generados. *Todo grupo abeliano finitamente generado es isomorfo a un único grupo de la forma*

$$\mathbb{Z}/_{d_1\mathbb{Z}} \times \mathbb{Z}/_{d_2\mathbb{Z}} \times \cdots \times \mathbb{Z}/_{d_s\mathbb{Z}} \times \mathbb{Z}^r$$

con $r \geq 0$ y $1 < d_1|d_2|...|d_s$.

Demostración. Ya sabemos que todo grupo abeliano finitamente generado es isomorfo a $\mathbb{Z}^n/H$ para algún $H \leq \mathbb{Z}^n$ y para cierto $n \in \mathbb{N}$. Basta con aplicar el Teorema B.10 concluir la demostración. La unicidad procede de la unicidad de la Forma Normal de Smith. □

APÉNDICE C
Relativo a la torsión

En este apéndice se encuentran las demostraciones pendientes la sección 3.2.3, en el que tratábamos de aclarar por qué no hay puntos de torsión de orden 11, 14 ni 15.

Proposición C.1. Sean P_1, P_2, P_3, P_4 puntos en el plano proyectivo tales que ninguno de ellos pertenece a la misma recta, entonces existe una única transformación proyectiva que los envía a $[1:0:0], [0:1:0], [0:0:1], [1:1:1]$, respectivamente.

Demostración. Una transformación proyectiva viene dada por una matriz $A_{3\times 3} = (a_{i,j})$ invertible, de forma que envíe el punto $P_1 = [x_1 : y_1 : z_1]$ al $[1:0:0]$ sí y solo sí existe un α_1 sobre el cuerpo tal que

$$\alpha_1(x_1, y_1, z_1) = (1, 0, 0)A = (a_{11}, a_{12}, a_{13}).$$

De esta forma, la primera fila de la matriz A queda determinada por un factor α_1 no nulo, multiplicando a un vector $P_1 = (x_1, y_1, z_1)$. De manera similar, la segunda y tercera filas quedarán determinadas por α_2 y α_3, respectivamente, multiplicando a los vectores P_2 y P_3.

Ahora nos fijamos en el punto P_4, que queremos mandarlo al punto $[1:1:1]$. En ese caso, por la propiedad de linealidad de nuestra transformación, nos encontramos con

$$\alpha_4(x_4, y_4, z_4) = (1, 1, 1)A = (1, 0, 0)A + (0, 1, 0)A + (0, 0, 1)A.$$

Podemos suponer libremente que $\alpha_4 = 1$, obteniendo así la igualdad

$$P_4 = \alpha_1 P_1 + \alpha_2 P_2 + \alpha_3 P_3.$$

Como los vectores P_1, P_2 y P_3 son linealmente independientes, tenemos una solución única para este sistema $(\alpha_1, \alpha_2, \alpha_3)$. Como, además, P_4 es linealmente independiente con cada par de vectores $(P_1, P_2), (P_1, P_3), (P_2, P_3)$, podemos garantizar que los α_i son todos distintos de cero.

De esta forma hemos determinado una matriz A en la que sus filas vendrán dadas por $\alpha_i P_i$. Dicha matriz será invertible, y única salvo para valores $\alpha_4 \neq 1$. Pero como A es una matriz sobre el plano proyectivo, cualquier reescalado de α_4 es equivalente a 1. □

Supongamos ahora un punto $P \in E(\mathbb{Q})$ tal que $11P = \mathcal{O}$.

Corolario C.2. *Se puede hace una transformación proyectiva que envíe el punto* $\mathcal{O}$ *a* $[1:1:1]$ *y los puntos* $P, 2P$ *y* $3P$ *a* $[1:0:0], [0:1:0]$ *y* $[0:0:1]$.

Demostración. Basta tomar $P_1 = \mathcal{O}, P_2 = P, P_3 = 2P$ y $P_4 = 3P$ en la proposición C.1. □

Ahora podemos tomar los puntos $\mathcal{O} = [1:1:1], P = [1:0:0], 2P = [0:1:0], 3P = [0:0:1]$ y $4P = [x:y:z]$ y calcular todos los demás elementos del grupo como puntos de intersección de las rectas mencionadas en la sección.

C.1. Cálculos explícitos para los Teoremas 3.2 y 3.3

C.1.1. Punto 8P

Demostración.

$$8P = -3P = \overline{\mathcal{O}\ 3P} \cap \overline{P\ 2P}$$

La recta que pasa por los puntos

$$\begin{cases} \mathcal{O} = [1:1:1] \\ 3P = [0:0:1] \end{cases}$$

viene dada por las ecuaciones

$$\begin{cases} a+b+c=0 \\ c=0 \end{cases} \longrightarrow a = -b \longrightarrow a\mathbf{X} + b\mathbf{Y} = a\mathbf{X} - a\mathbf{Y} = 0 \longrightarrow \mathbf{X} = \mathbf{Y}$$

$$\begin{cases} P = [1:0:0] \\ 2P = [0:1:0] \end{cases} \longrightarrow \begin{cases} a = 0 \\ b = 0 \end{cases} \longrightarrow a\mathbf{X} + b\mathbf{Y} + c\mathbf{Z} = c\mathbf{Z} = 0 \longrightarrow \mathbf{Z} = 0.$$

Podemos calcular entonces el punto $8P$ como la intersección de las dos rectas anteriores.

$$8P = \{\mathbf{X} = \mathbf{Y}\} \cap \{\mathbf{Z} = 0\} \longrightarrow 8P = [1:1:0]$$

□

C.1.2. Punto 10P

Punto 10P

Demostración.

$$10P = -P = \overline{\mathcal{O}\ P} \cap \overline{(-3P)\ 4P}$$

$$\begin{cases} \mathcal{O} = [1:1:1] \\ P = [1:0:0] \end{cases} \longrightarrow \begin{cases} a+b+c=0 \\ a=0 \end{cases} \longrightarrow b = -c \longrightarrow b\mathbf{Y} + c\mathbf{Z} = b\mathbf{Y} - b\mathbf{Z} = 0 \longrightarrow \mathbf{Y} = \mathbf{Z}$$

$$\begin{cases} -3P = [1:1:0] \\ 4P = [x:y:z] \end{cases} \longrightarrow \begin{cases} a+b=0 \\ ax+by+cz=0 \end{cases} \longrightarrow \begin{cases} a=-b \\ ax-ay+cz=0 \end{cases} \longrightarrow c = a\left(\frac{y-x}{z}\right)$$

$$\longrightarrow a\mathbf{X}+b\mathbf{Y}+c\mathbf{Z} = a\mathbf{X}-a\mathbf{Y}+a\left(\frac{y-x}{z}\right)\mathbf{Z} = a\mathbf{X}-a\mathbf{Y}+a\left(\frac{y-x}{z}\right)\mathbf{Z} = 0$$

$$10P = \{\mathbf{Y}=\mathbf{Z}\} \cap \{\mathbf{X}-\mathbf{Y}+\left(\frac{y-x}{z}\right)\mathbf{Z}=0\} \longrightarrow \mathbf{X} = \left(1-\frac{y-x}{z}\right)\mathbf{Z}$$

$$\longrightarrow 10P = [x-y+z:z:z]$$

□

C.1.3. Puntos 9P, 7P y 5P

Como el cálculo de estos dos puntos es muy similar al de los dos anteriores y el resultado no es de mayor relevancia, no vamos a entrar en su contenido.

C.1.4. Punto -5P

Demostración.

$$-5P = \overline{P\ 4P} \cap \overline{2P\ 3P}$$

$$\begin{cases} 2P = [0:1:0] \\ 3P = [0:0:1] \end{cases} \longrightarrow \mathbf{X} = 0$$

$$\begin{cases} P = [1:0:0] \\ 4P = [x:y:z] \end{cases} \longrightarrow \begin{cases} a=0 \\ ax+by+cz=0 \end{cases} \longrightarrow by+cz=0$$

$$\longrightarrow \begin{cases} b = -\frac{z}{y}c & \text{si } y \neq 0 \\ c = -\frac{y}{z}b & \text{si } z \neq 0 \end{cases}$$

Sabemos que uno de los dos casos anteriores se va a dar, puesto que si $y = z = 0$, entonces $4P = [1:0:0] = P$.

Ahora calculamos la intersección con $\{\mathbf{X}=0\}$.

En el caso $y \neq 0$:

$$b\mathbf{Y}+c\mathbf{Z} = -\frac{z}{y}c\mathbf{Y}+c\mathbf{Z} = 0 \longrightarrow \mathbf{Z} = \frac{z}{y}\mathbf{Y} \longrightarrow -5P = [0:1:\frac{z}{y}] = [0:y:z]$$

En el caso $z \neq 0$:

$$b\mathbf{Y}+c\mathbf{Z} = b\mathbf{Y}-\frac{y}{z}\mathbf{Z} = 0 \longrightarrow \mathbf{Y} = \frac{y}{z}\mathbf{Y} \longrightarrow -5P = [0:\frac{y}{z}:1] = [0:y:z]$$

□

C.1.5. Punto 6P

Demostración. Este caso es bastante más complejo, por lo que vamos a utilizar *Sage* para tratarlo. En primer lugar, al igual que en los casos anteriores, observamos lo siguiente:

$$6P = \overline{(-P)\ (-5P)} \cap \overline{(-2P)\ (-4P)}$$

A continuación, vamos a declarar en Sage las variables utilizadas y los puntos necesarios:

Código C.1: Declaración de variables

```
var('a b c x y z X Y Z')

Pmenos = [x-y+z,z,z]
P2menos = [x-y+z,z,x-y+z]
P4menos = [x-y,0,z-y]
P5menos = [0,y,z]
```

El siguiente paso es definir las funciones que vamos a utilizar. En este caso, *line_points(p1,p2)* calculará la recta que une dos puntos, mientras que *intersection(R1,R2)* devolverá la intersección entre dos rectas.

Código C.2: Declaración de funciones

```
# Devuelve la recta que une dos puntos
def line_points(p1,p2):
    f1 = a*p1[0] + b*p1[1] + c*p1[2] == 0
    f2 = a* p2[0] + b*p2[1] + c*p2[2] == 0
    sols = solve([f1,f2], [a,b,c], solution_dict=True,\
                 explicit_solutions=True)
    if sols[0][a] == 0 and sols[0][b] == 0 and sols[0][c] == 0 \
    and len(sols) > 0:
        sols = sols[1]
    else:
        sols = sols[0]
    F = sols[a]*X + sols[b]*Y + sols[c]*Z == 0
    print solve(F, [X,Y,Z])[0]


# Devuelve la interseccion entre dos rectas
def intersection(R1,R2):

    s = solve([R1,R2], [X,Y,Z], solution_dict=True)[0]
    print 'X: ' + str(s[X].simplify_full().factor())
    print 'Y: ' + str(s[Y].simplify_full().factor())
    print 'Z: ' + str(s[Z].simplify_full().factor())
    return {
        'X': s[X].simplify_full().factor(),
        'Y': s[Y].simplify_full().factor(),
        'Z': s[Z].simplify_full().factor()
    }
```

A continuación podemos hallar las rectas $\overline{(-P)\ (-5P)}$ y $\overline{(-2P)\ (-4P)}$.

Código C.3: Declaración de funciones

```
line_points(Pmenos, P5menos)
# [X == (r130*x*y-r130*y^2-r131*z^2-(r131*x-(r130+r131)*y)*z)/(y*z-z^2),
# Y == r131,
# Z == r130]

line_points(P2menos, P4menos)
# [X == (r134*x^2-r134*x*y-r134*z^2-(r133*x-(r133+r134)*y)*z)/(y*z-z^2),
# Y == r134,
# Z == r133]
```

Llegados a este punto, debemos hacer una interpretación de los resultados. Vemos que tanto Y como Z equivalen a unas constantes arbitrarias que también aparecen dentro de X. Esto implica que podemos definir las rectas como:

Código C.4: Definición de las rectas

```
# Recta entre -P y -5P
R1 = X == (Z*x*y - Z*y^2 - Y*z^2 - (Y*x - (Z + Y)*y)*z)/(y*z - z^2)

# Recta entre -2P y -4P
R2 = X == (Y*x^2 - Y*x*y - Y*z^2 - (Z*x - (Z + Y)*y)*z)/(y*z - z^2)
```

Por último, hallamos la intersección entre ambas rectas y analizamos el resultado:

Código C.5: Definición de las rectas

```
res = intersection(R1,R2)

# X: (x^2*y-x*y^2+y^2*z-x*z^2)*r135*(x-y+z)/((x*y-y^2+x*z)*(y-z)*z)
# Y: r135
# Z: r135*(x - y + z)*x/(x*y - y^2 + x*z)
```

En este caso, debemos interpretar el resultado como lo que es: un punto en el plano proyectivo. Es decir, tendríamos el equivalente a:

$$P6 = \left[\frac{(x^2y - xy^2 + y^2z - xz^2)(x - y + z)\cdot r135}{(xy - y^2 + xz)(y - z)z} : r135 : \frac{r135\cdot(x - y + z)x}{xy - y^2 + xz}\right]$$

Si dividimos todo entre la constante arbitraria y multiplicamos hasta obtener un denominador común, obtenemos el siguiente punto:

$$P6 = \left[(x^2y - xy^2 + y^2z - xz^2)(x - y + z) : (xy - y^2 + xz)(y - z)z : (x - y + z)(y - z)xz\right]$$

□

C.2. Prueba para el caso de orden 14

Al igual que en el caso de orden 11, procedemos por reducción al absurdo, suponiendo que, efectivamente, hay un punto de torsión de orden 14. En ese caso se cumplirá que $\mathcal{O}, P, 2P, ..., \ 13P$ son todos puntos distintos, y $14P = \mathcal{O}$.

Análogamente, tomamos los puntos $\mathcal{O} = [1:1:1], P = [1:0:0], 2P = [0:1:0], 3P = [0:0:1]$ y $4P = [x:y:z]$ con sus respectivos cambios a proyectivas.

Utilizando el mismo razonamiento que antes, que tres puntos de una curva pertenecen a la misma recta sí y solo sí $P+Q+R = \mathcal{O}$, obtendremos los demás puntos de la curva a partir de los cinco iniciales.

Comenzamos por el punto $-3P$, puesto que depende únicamente de los puntos ya conocidos.

$$11P = -3P = \overline{\mathcal{O}\ 3P} \cap \overline{P\ 2P}.$$

A partir de ahí, podemos obtener los demás (el orden en el que aparecen deja patente la dependencia de los puntos previos):

$$13P = -P = \overline{\mathcal{O}P} \cap \overline{(-3P)\ 4P},$$

$$12P = -2P = \overline{\mathcal{O}\ 2P} \cap \overline{(-P)\ 3P},$$

$$10P = -4P = \overline{\mathcal{O}\ 4P} \cap \overline{P\ 3P},$$

$$9P = -5P = \overline{P\ 4P} \cap \overline{2P\ 3P},$$

$$5P = \overline{(-P)\ (-4P)} \cap \overline{(-2P)\ (-3P)},$$

$$8P = -6P = \overline{P\ 5P} \cap \overline{2P\ 4P},$$

$$6P = \overline{(-P)\ (-5P)} \cap \overline{(-2P)\ (-4P)},$$

$$7P = \overline{(-P)\ (-6P)} \cap \overline{(-2P)\ (-5P)}.$$

De forma explícita, los puntos que obtenemos al hallar las intersecciones son los siguientes:

$$-P = [x-y+z : z : z]$$

$$-2P = [x-y+z : z : x-y+z]$$

$$-3P = [1:1:0]$$

$$-4P = [x-y : 0 : z-y]$$

$$-5P = [0 : y : z]$$

$$-6P = [(x-y+z)yx : z^2x : (x-y+z)yz]$$

$$-7P = [x(xy-y^2+xz) : y(xy-y^2+xz) : (x-y+z)xy]$$

$$5P = [xy - y^2 + xz : xz : y(x - y + z)]$$

$$6P = [(x-y+z)(x^2y-xy^2+y^2z-xz^2) : z(y-z)(xy+xz-y^2) : xz(y-z)(x-y+z)]$$

$$7P = [(-y^2 + xz)(x - y + z) : (-x^2y + xy^2 - y^2z + xz^2) : (-xy + y^2 - xz)(y - z)]$$

Como suponemos que el grupo tiene orden 14, se tiene que cumplir que $-7P = 7P$. Además, sabemos que $x - y + z \neq 0$, $x \neq 0$, $y \neq 0$, puesto que esos casos nos llevaría a contradicción tal y como están definidos los múltiplos de P. Por tanto, ver que dos puntos son iguales, $[X : Y : Z] = [U : V : W]$, sabiendo que $Z \neq 0$, equivale a comprobar $(X/Z, Y/Z) = (U/W, V/W)$ que, en el plano afín, significa que las coordenadas sean iguales una a una.

Obtenemos de esta manera las siguientes ecuaciones:

$$-\frac{(-x+y)z(-x^2y+y^3-xyz-y^2z+xz^2)}{y(y-z)(-x+y-z)(-xy+y^2-xz)} = 0, \tag{C.1}$$

$$\frac{(x-y)^2(x^2y-y^3+xyz+y^2z-xz^2)}{x(y-z)(x-y+z)(xy-y^2+xz)} = 0. \tag{C.2}$$

Esto implica

$$x^2y - y^3 + xyz + y^2z - xz^2 = 0 \tag{C.3}$$

ya que si $x = y$, entonces $-P = [1 : 1 : 1] = \mathcal{O}$; si $z = 0$, entonces $-P = P$; si $y = z$, entonces $-4P = P$. Por otro lado, ya sabemos que $x - y + z \neq 0$, $x \neq 0$, $y \neq 0$. Además, si $xy - y^2z + xz = 0$, entonces la tercera coordenada de $7P$ sería igual a 0, y la primera coordenada de $-7P$ también sería igual a cero. Eso implica que la primera coordenada de $7P$ también sea 0 (el que los puntos $[X : Y : Z] = [U : V : W]$ sean iguales, implica que $X = aU$, $Y = aV$, $Z = aW$, con $a \in \mathbb{Q}$ y, puesto que $U = 0$, sabemos que $X = 0$). En ese caso, $7P = [0 : 1 : 0] = 2P$, lo que de nuevo es una contradicción.

Usando el siguiente código en Magma,

Código C.6: Obtención de la curva elíptica

```
P2<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(P2,x^2*y - y^3 + x*y*z + y^2*z - x*z^2);
pt:=C![0,0,1];
E,map:=EllipticCurve(C,pt);
We,map2:=WeierstrassModel(E);
We;
# Elliptic Curve defined by y^2 = x^3 - 10800*x + 874368 over Rational Field

G,mw:=MordellWeilGroup(We);
pts:={};
pss:={};
for p in {mw(g) : g in G} do
        pts:={pt : pt in RationalPoints(p @@ map2 @@ map)} join pts;
        pss:={p} join pss;
end for;

pss;
# { (12 : 864 : 1), (0 : 1 : 0), (156 : 1728 : 1), (156 : -1728 : 1), (-132 : 0 :1),
# (12 : -864 : 1) }

pts;
# { (1/2 : 1/2 : 1), (0 : 0 : 1), (0 : 1 : 1), (1 : 0 : 0), (1 : 1 : 0),
# (-1 : 1 : 0) }

Rank(E);
# 0
```

vemos que la ecuación anterior equivale a la curva

$$W : y^2 = x^3 - 10800x + 874368$$

cuyo grupo de Mordell es isomorfo a $\mathbb{Z}/6\mathbb{Z}$ y contiene los puntos $[12 : 864 : 1], [0 : 1 : 0], [156 : 1728 : 1], [156 : -1728 : 1], [-132 : 0 : 1], [12 : -864 : 1]$. Además, como su rango es 0, sabemos que los únicos puntos racionales en la curva son estos seis. Por otro lado, si obtenemos las preimágenes de estos seis puntos, nos encontramos con que se corresponden con $[1/2 : 1/2 : 1], [0 : 0 : 1], [0 : 1 : 1], [1 : 0 : 0], [1 : 1 : 0], [-1 : 1 : 0]$. Podemos enunciar entonces el siguiente teorema.

Teorema C.3. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces no existe $P \in E(\mathbb{Q})$ de orden 14.*

Demostración. Sabemos que, en el caso de que exista un punto racional de orden 14, es necesario que las variables $x, y, z \in \mathbb{Q}$ satisfagan la ecuación $x^2y+y^2z+xyz-y^3-xz^2 = 0$. Esto ocurre sí y solo sí el punto $4P = [x : y : z]$ se correponde con uno de los seis puntos racionales de la curva W. Ya sabemos que $P = [1 : 0 : 0]$, $3P = [0 : 0 : 1]$ y $-3P = [1 : 1 : 0]$. Por lo tanto, $4P$ tendrá que ser igual a uno de los puntos $[1/2 : 1/2 : 1]$, $[0 : 1 : 1]$, $[-1 : 1 : 0]$.

Del primer caso se obtiene $x = y = 1/2$, $z = 1$, lo que implicaría $-P = [1 : 1 : 1] = \mathcal{O}$. Por lo tanto, este caso no es posible.

Si $4P = [0 : 1 : 1]$, entonces $x = 0$, $y = z = 1$. Esto conllevaría $-P = [0 : 1 : 1] = 4P$. De nuevo es imposible, puesto que hemos supuesto que P tiene orden 14.

Finalmente, si $4P = [-1 : 1 : 0]$, entonces $x = -y$, $z = 0$. En este caso tendríamos $-P = [1 : 0 : 0] = P$, lo que resulta imposible por el mismo motivo.

Por lo tanto, no existen $x, y, z \in \mathbb{Q}$ que satisfagan la ecuación $x^2y + y^2z + xyz - y^3 - xz^2 = 0$. En conclusión, no puede existir un punto racional de orden 14. □

C.3. Prueba para el caso de orden 15

El procedimiento en este caso es análogo al del caso anterior. Suponemos que P es un punto de orden 15, por lo que $\mathcal{O}, P, 2P, ..., 14P$ son puntos distintos y $14P = \mathcal{O}$. De nuevo, tomamos $\mathcal{O} = [1 : 1 : 1], P = [1 : 0 : 0], 2P = [0 : 1 : 0], 3P = [0 : 0 : 1]$ y $4P = [x : y : z]$.

Al igual que en el caso de orden 14, a partir de estos 4 puntos podemos obtener todos los demás trazando rectas y hallando intersecciones. En concreto, nos interesan los puntos

$$8P = \overline{(-P)\ (-7P)} \cap \overline{(-2P)\ (-6P)},$$
$$-7P = \overline{P\ 6P} \cap \overline{2P\ 5P}.$$

De forma explícita, estos dos puntos se corresponden con

$$8P = [-(x^2y^2 - xy^3 + y^3z - xyz^2 - y^2z^2 + xz^3) : (y^2 - xz)z^2 : (x^2y - xy^2 + y^2z - xz^2)z],$$

$$-8P = [(x^2y - xy^2 + y^2z - xz^2)(xy - y^2 + xz) : (x^2y - xy^2 + y^2z - xz^2)xz : (xy - y^2 + xz)(y - z)xz]$$
$$-7P = [x(xy - y^2 + xz) : y(xy - y^2 + xz) : (x - y + z)xy].$$

Como el punto P tiene orden 15, es necesario que $8P$ sea igual a $-7P$.

Sabemos que $x \neq 0$, $y \neq 0$ y $x - y + z \neq 0$ (en caso contrario, llegaríamos a contradicciones con los puntos tal y como los hemos definido en el caso de orden 14). Queremos ver que dos puntos son iguales, $[X : Y : Z] = [U : V : W]$, y sabemos que $Z \neq 0$. Por tanto, resulta equivalente comprobar $(X/Z, Y/Z) = (U/W, V/W)$ que, sobre el plano afín, implica que cada una de las coordenadas sean iguales.

La igualdad entre las primeras coordenadas nos da la ecuación

$$-\frac{(-xy + y^2 - yz + z^2)(-x^2y^2 + xy^3 - x^2yz + xy^2z - y^3z - x^2z^2 + xyz^2)}{yz(-x + y - z)(-x^2y + xy^2 - y^2z + xz^2)} = 0. \tag{C.4}$$

Por otro lado, la igualdad entre las segundas coordenadas nos lleva a

$$-\frac{(x - y)(x^2y^2 - xy^3 + x^2yz - xy^2z + y^3z + x^2z^2 - xyz^2)}{x(x - y + z)(x^2y - xy^2 + y^2z - xz^2)} = 0. \tag{C.5}$$

Esto implica

$$x^2y^2 - xy^3 + x^2yz - xy^2z + y^3z + x^2z^2 - xyz^2 = 0, \tag{C.6}$$

porque si $x = y$, entonces $-P = [1 : 1 : 1] = \mathcal{O}$; si $z = 0$, entonces $-P = P$. Por otro lado, ya sabíamos que $x \neq 0$, $y \neq 0$ y $x - y + z \neq 0$. Si $x^2y - xy^2 + y^2z - xz^2 = 0$, entonces tanto la primera coordenada de $-8P$ como la tercera coordenada de $8P$ serían iguales a 0. De forma análoga al caso de orden 14, si esto ocurriese entonces la primera coordenada de $-8P$ también sería igual a 0 y, por tanto, $-8P = 2P$. Lo cual es una contradicción. La ecuación (C.5) nos confirma entonces que la ecuación (C.6) es correcta.

Usando el siguiente código en Magma,

Código C.7: Obtención de la curva elíptica

```
P2<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(P2,x^2*y^2 - x*y^3 + x^2*y*z - x*y^2*z + y^3*z + x^2*z^2 - x*y*z^2);
pt:=C![0,0,1];
E,map:=EllipticCurve(C,pt);
We,map2:=WeierstrassModel(E);
We;
# Elliptic Curve defined by y^2 = x^3 - 27*x + 8694 over Rational Field

G,mw:=MordellWeilGroup(We);
pts:={};
pss:={};
for p in {mw(g) : g in G} do
        pts:={pt : pt in RationalPoints(p @@ map2 @@ map)} join pts;
        pss:={p} join pss;
end for;

pss;
# { (-21 : 0 : 1), (15 : 108 : 1), (0 : 1 : 0), (15 : -108 : 1) }

pts;
# { (0 : 1 : 0), (0 : 0 : 1), (1 : 0 : 0), (1 : 1 : 0) }

Rank(E);
# 0
```

vemos que la curva elíptica asociada a esa ecuación es

$$W : y^2 = x^2 - 27x + 8594.$$

Esta curva tiene rango igual a cero, por lo que sus únicos puntos racionales son los cuatro que forman el subgrupo de torsión: $[-21 : 0 : 0], [15 : 108 : 1], [0 : 1 : 0], [15 : -108 : 1]$. Si deshacemos los cambios, obtenemos la siguiente correspondencia entre puntos de la curva y múltiplos de P:

$$[-21 : 0 : 0)] \mapsto [0 : 1 : 0] = 2P,$$

$$[15 : 108 : 1] \mapsto [0 : 0 : 1] = P,$$

$$[0 : 1 : 0] \mapsto [1 : 0 : 0] = 3P,$$

$$[15 : -108 : 1] \mapsto [1 : 1 : 0] = -3P.$$

Teorema C.4. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces no existe $P \in E(\mathbb{Q})$ de orden 15.*

Demostración. Sabemos que, en caso de que exista un punto racional de orden 15, es necesario que las variables $x, y, z \in \mathbb{Q}$ satisfagan la ecuación (C.6), lo que ocurres sí y solo sí el punto $4P = [x : y : z]$ se correspodne con un punto racional de la curva W. Sin embargo, los únicos puntos racionales de dicha curva son los que se corresponden con P, $2P$, $3P$ y $-3P$. Por lo tanto, es imposible que $4P$ sea un punto racional, y es imposible que exista un punto racional de orden 15. □

APÉNDICE D
Fórmula de Herón

En el capítulo 4 se enuncia la fórmula de Herón (proposición 4.1). En este apéndice se incluye su demostración.

Para la demostración, haremos referencia al siguiente triángulo:

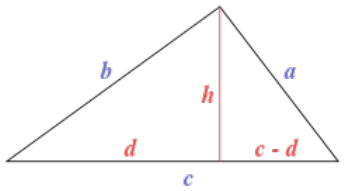

Figura D.1: Triángulo de herón con altura h

Su área, por tanto, será $A = \frac{1}{2}ch$. Resulta entonces equivalente probar la igualdad

$$(ch)^2 = 4s(s-a)(s-b)(s-c).$$

Sin embargo, usando el Teorema de Pitágoras sabemos que $h^2 = b^2 - d^2$, y entonces $(ch)^2 = c^2(b^2 - d^2)$.

Por otro lado,

$$4s(s-a)(s-b)(s-c) = (s(s-a) + (s-b)(s-c))^2 - (s(s-a) - (s-b)(s-c))^2.$$

Basta demostrar entonces lo siguiente:

$$cb = s(s-a) + (s-b)(s-c)$$

y

$$cd = s(s-a) - (s-b)(s-c).$$

En el primer caso,

$$s(s-a) + (s-b)(s-c) = 2s^2 - s(a+b+c) + cb.$$

Pero sabemos que $2s = a + b + c$, por lo que podemos sustituir obteniendo $s(s-a) + (s-b)(s-c) = cb$.

En el segundo caso, de nuevo extendemos la ecuación para obtener:

$$cd = -bc + s(b + c - a).$$

Si ahora sustituimos $s = \frac{a+b+c}{2}$, obtendremos:

$$cd = \frac{b^2 + c^2 - a^2}{2}.$$

Usando ahora el Teorema de Pitágoras, sustituimos $b^2 = d^2 + h^2$ y $a^2 = h^2 + (c-d)^2$ y obtenemos que, efectivamente, la fórmula equivale a cd.

Queda demostrada así la validez de la fórmula de Herón.

Bibliografía

[1] Apuntes de la asignatura de Estructuras Algebraicas del Departamento de Álgebra de la Facultad de Matemáticas de la Universidad de Sevilla, curso 2015/2016. Disponible en:
`http://rodas5.us.es/file/0125a68f-b30b-40e8-abc0-b5b82e0c5a8c/1/Apuntes_T2.pdf`

[2] Billing, G., Mahler, K. *On Exceptional Points on Cubic Curves*. London Journal of Mathematics, 15 (1940), 32-43.

[3] Cuoco A., McCallum W. *The Double Continuity of Algebra*. In: Kaiser G., Forgasz H., Graven M., Kuzniak A., Simmt E., Xu B. (eds) Invited Lectures from the 13th International Congress on Mathematical Education. ICME-13 Monographs. Springer, Cham, 2018.

[4] Friedl, S. *An Elementary Proof of the Group Law for Elliptic Curves*. Groups Complex, Cryptol, 9 (2017), no.2, 117-123.

[5] MacLeod, A. J. *On a problem of John Leech*. Expositiones Mathematicae, 23 (2005), 271–279.

[6] Bosma W., Cannon J., Playoust C. *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265

[7] *SageMath, the Sage Mathematics Software System (Version 8.1)*, The Sage Developers, 2017, `https://www.sagemath.org`.

[8] Silverman, J.H., Tate, J. *Rational Points on Elliptic Curves*. Springer, New York, 1992.

[9] Théry, L. *Proving the group law for elliptic curves formally*. Projet Marelle, 0330, 2007.
`https://hal.inria.fr/inria-00129237/document`

[10] Woodbury, M.C. *Finite Groups on Elliptic Curves*. University of Utah, 2003.
`https://www.math.utah.edu/∼woodbury/research/files/ellipticwriteup.pdf`