Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Curvas Elípticas y Problemas Aritméticos

Trabajo de fin de grado

Grado en Matemáticas

Autor: Miguel Guijarro de la Hoz
Tutor: Enrique González Jiménez

Curso 2018-2019

Resumen

En este trabajo vamos a realizar un estudio sobre las curvas elípticas, con el fin de resolver algunos problemas aritméticos.

Las curvas elípticas se fundamentan en la geometría algebraica. En el primer capítulo veremos algunas nociones fundamentales sobre la geometría algebraica. Nos detendremos en el teorema de Bézout, uno de los teoremas más importantes en el ámbito de las curvas algebraicas.

En el segundo capítulo utilizaremos lo aprendido en el tema uno para poder definir las curvas elípticas. Estudiaremos la Ley de Grupo, y veremos su forma explicita.

La tercera parte del proyecto se fundamenta en el estudio de tres teoremas fundamentales en la teoría de las curvas elípticas. Estos teoremas nos ayudan a entender y a clasificar los puntos racionales de las curvas elípticas y los subgrupos de torsión.

En el cuarto capítulo estudiaremos algunos problemas aritméticos. Problemas con más de dos mil años de antigüedad que pueden ser resueltos con curvas elípticas. El problema del número congruente o el triángulo de Herón son los más reconocidos.

Por último finalizaremos el trabajo con un resumen del estudio realizado y las conclusiones sobre el proyecto.

Abstract

In this project we are going to carry out a study on the elliptic curves, in order to solve some arithmetic problems.

The elliptic curves are based on algebraic geometry. In the first chapter we will see some fundamental notions about algebraic geometry. We will dwell on Bézout's theorem, one of the most important theorems in the theory of algebraic curves.

In the second chapter we will use what we learned in topic one to be able to define elliptic curves. We will study the Group Law, and we will see it's explicit form.

The third part of the project is based on the study of three fundamental theorems in the theory of elliptic curves. These theorems help us understand and classify the rational points of elliptic curves and torsion subgroups.

In the fourth chapter we will study some arithmetic problems. Problems with more than two thousand years old that can be solved with elliptical curves. The problem of the congruent number or the triangle of Heron are the most recognized.

Finally, we will finish the work with a summary of the study and the conclusions about the project

Índice general

Introducción

Las curvas elípticas pueden ser consideradas erróneamente como objetos modernos, ya que muchas de sus propiedades solo han sido estudiadas en el último siglo, pero realmente surgen de manera implícita del trabajo de Diofanto de Alejandría en el siglo III d.C., considerado como el padre del álgebra. En su obra "Arithmetica", que solo se conserva parcialmente, presenta una serie de problemas de ecuaciones con variables que tiene un valor racional, llamadas en su honor "Ecuaciones diofánticas". Su trabajo permanece ignorado hasta el siglo XVII, con el revivir de la aritmética y los estudios de Bachet y Fermat. Solo en los años 50 del siglo pasado con el descubrimiento de las conexiones profundas entre la aritmética y el álgebra con el análisis complejo es cuando se convierten en uno de los objetos más fascinantes y más intensamente estudiados de las matemáticas. Las curvas elípticas juegan un papel fundamental y de importancia creciente en la teoría de los números y en otros campos relacionados como la criptografía. Y fueron imprescindibles en la demostración del ultimo teorema de Fermat por Andrew Wiles en 1995.

El objetivo principal de este trabajo es realizar un acercamiento a las curvas elípticas y estudiar su aplicación a la resolución de algunos problemas aritméticos escogidos.

Las curvas elípticas se fundamentan en la geometría algebraica. En el capítulo 1 veremos algunas nociones fundamentales sobre la geometría algebraica. Nos detendremos en el teorema de Bézout, uno de los teoremas más importantes en el ámbito de las curvas algebraicas.

En el capítulo 2 comenzaremos con el estudio de las curvas elípticas propiamente dichas, y analizaremos la Ley de Grupo y la forma explicita de esta ley. Esto nos permitirá resolver los problemas aritméticos del ultimo capítulo.

En el capítulo 3 presentaremos el teorema de Mordell, y estudiaremos teoremas para la clasificación de los subgrupos de torsión, y la morfología de los puntos de orden finito.

Finalmente, en el capítulo 4 abordaremos la resolución de problemas aritméticos elementales a partir de los resultados obtenidos hasta ese punto, y terminaremos con un capítulo con conclusiones.

CAPÍTULO 1
Nociones Básicas de Curvas Algebraicas

Antes de empezar con el estudio de las curvas elípticas debemos definir una serie de conceptos necesarios para el entendimiento de dichas curvas.

1.1. Nociones Básicas

Definición 1.1. Sea K un cuerpo, definimos el plano proyectivo como:

$$\mathbb{P}^2(K) = \{(X, Y, Z) \neq (0, 0, 0) : X, Y, Z \in K\}/\sim$$

La relación de equivalencia queda determinada por:

$$(X, Y, Z) \sim (X', Y', Z') \Leftrightarrow \exists \lambda \in K : \lambda(X, Y, Z) = (X', Y', Z').$$

Denotaremos por $[X : Y : Z]$ a las clases de equivalencia. Obsérvese que podemos pensar el plano afín $\mathbb{A}^2(K)$ contenido en $\mathbb{P}^2(K)$, mediante la identificación de la clase de $[X : Y : 1]$ en el punto (X, Y).

Necesitamos definir qué es un polinomio homogéneo para poder continuar.

Definición 1.2. Un polinomio $F \in K[X_1, \ldots, X_n]$ se dice homogéneo de grado d si $\forall \lambda \in K$ se tiene

$$F(\lambda X_1, \ldots \lambda X_n) = \lambda^d F(X_1, \ldots, X_n).$$

Usando la relación de equivalencia y la definición de polinomio homogéneo tenemos que para cualesquiera $X_1, \ldots, X_n, \lambda \in K$ se tiene que:

$$F(\lambda X_1, \ldots \lambda X_n) = 0 \Longleftrightarrow F(X_1, \ldots, X_n) = 0.$$

Esta conclusión será fundamental en la geometría algebraica.

Continuamos definiendo las curvas proyectivas planas.

Definición 1.3. Sea $F(X,Y,Z) \in K[X,Y,Z]$ un polinomio homogéneo. Definimos la curva proyectiva plana asociada a F como:

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

Como F está definida en K, decimos que la curva C_F está definida en K. Además, definimos los puntos K-racionales de C_F como:

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

Cuando estudiamos las curvas proyectivas, es imprescindible conocer los puntos singulares y su relación con dichas curvas.

Definición 1.4. Sea $F(X,Y,Z) \in K[X,Y,Z]$ un polinomio homogéneo. Decimos que un punto $P = [X_0 : Y_0 : Z_0] \in C_F$, es un punto singular si:

$$\nabla F(X_0, Y_0, Z_0) = (0,0,0).$$

Si nuestra curva no tiene puntos singulares, diremos que es una curva no singular o lisa.

Es necesario estudiar ciertas nociones acerca del género de una curva. Hablamos de género de una curva para aludir a un concepto algebraico referente a las curvas. Sin entrar en todo el detalle que sería preciso, principalmente nos interesa conocer la fórmula para calcular el género:

$$g = \frac{(d-1)(d-2)}{2} - s,$$

donde d es el grado de F y s es un número entero que tiene que ver con las singularidades de F. En caso de que no existan singularidades en la curva, se cumple que $s = 0$. En particular, si $d = 3$ y la curva no tiene singularidades tendríamos que $g = 1$.

1.2. Teorema de Bezout

Supongamos que estamos interesados en calcular el número de soluciones de un sistema de ecuaciones definido de la siguiente forma:

$$\begin{cases} F(X,Y,Z) = 0, \\ G(X,Y,Z) = 0. \end{cases}$$

donde $F(X,Y,Z)$ y $G(X,Y,Z)$ son polinomios (homogéneos).

Podemos conocer el número de soluciones de este sistema de una manera más general si nos ceñimos a la clausura algebraica.

Para hallar la solución a nuestro problema tenemos el Teorema de Bézout [4]. Discutiremos la respuesta al sistema planteado en términos de intersecciones de curvas.

Definamos las curvas asociadas a los polinomios F, G como:

$$\begin{cases} C : F(X,Y,Z) = 0, \\ D : G(X,Y,Z) = 0. \end{cases}$$

Vamos introducir someramente la multiplicidad de las intersecciones locales $I_P(C,D)$ para todo $P \in \mathbb{P}^2(\overline{K})$. Hay 3 tipos de intersección:

1. Si $P \notin C \cap D$ entonces $I_P(C,D) = 0$.
2. Si $P \in C \cap D$ con P un punto no singular de C y D, y además C y D tienen diferentes direcciones de tangencia en P, entonces $I_P(C,D) = 1$. En este supuesto se dice que C y D intersecan de manera transversal en P.
3. Si $P \in C \cap D$ y C, D no intersecan de manera transversal en P entonces $I_P(C,D) \geq 2$.

Una vez introducidas las intersecciones locales, podemos abordar el estudio de las intersecciones globales de ambas curvas.

Definición 1.5. Sean C y D dos curvas proyectivas tales que $C \cap D$ contiene solo un número finito de puntos $P_1, P_2, ..., P_n$. La multiplicidad de la intersección global será igual a:

$$\phi(C,D) = \sum_{k=1}^{n} I_{P_k}(C,D). \tag{1.1}$$

Dicho de otro modo, la multiplicidad de la intersección global es la suma de todas las multiplicidades de las intersecciones locales por todos los puntos de la intersección.

Como ya hemos referido con anterioridad, estamos considerando K como un cuerpo y todos nuestros polinomios tendrán sus coeficientes en K.

Estamos en disposición de poder enunciar el Teorema de Bézout.

Teorema de Bézout. *Si la intersección entre C y D tiene un conjunto finito de puntos, entonces $\phi(C,D)$ es exactamente el producto de los grados de los polinomios homogéneos que definen C y D.*

La demostración, que escapa de los objetivos de este trabajo, se puede consultar en [4].

En el siguiente capítulo comenzaremos con el estudio de las curvas elípticas.

CAPÍTULO 2
Curvas Elípticas

2.1. Primeros Resultados

Nuestras ecuaciones en forma de Weierstrass son

$$C = \{[X : Y : Z] \in \mathbb{P}^2(\overline{K}) : Y^2Z + a_1XYZ + a_3YZ^2 = x^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3\}. \tag{2.1}$$

Con $a_1, a_2, a_3, a_4, a_6 \in K$. Al determinar así la curva, vemos que el punto $\mathcal{O} = [0 : 1 : 0]$ siempre pertenece a nuestro conjunto. De hecho, es el único punto con $Z = 0$.

Para seguir con nuestros cálculos, consideramos que $Z \neq 0$. Este condición nos va a permitir realizar un cambio de coordenadas y pasar del plano proyectivo al plano afín.

Si realizamos un cambio con coordenadas no homogéneas:

$$\begin{cases} x = \dfrac{X}{Z}, \\ y = \dfrac{Y}{Z}. \end{cases}$$

Con este cambio pasamos de estudiar las curvas en el plano proyectivo a estudiarlas en el plano afín. Así, nuestra curva C quedaría definida por la ecuación:

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

Con lo que podríamos reescribir la ecuación (2.1) como:

$$C(K) = \{(x, y) \in \mathbb{A}^2(K) : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}.$$

Ahora bien, si $car(K) \neq 2$ podemos simplificar aun más nuestra ecuación si aplicamos el siguiente cambio:

$$\begin{cases} x = x, \\ y = \dfrac{1}{2}(y - a_1x - a_3). \end{cases}$$

Tras aplicar este cambio, la ecuación resultante es:

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2.2}$$

Donde b_2, b_4, b_6 quedarían:

$$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = 2a_4 + a_1a_3, \\ b_6 = a_3^2 + 4a_6. \end{cases}$$

Si tenemos que $car(K) \neq 3$, podemos realizar los siguientes cambios:

$$\begin{cases} x = \dfrac{x - 3b_2}{36}, \\ y = \dfrac{y}{108}. \end{cases}$$

Tras aplicar estos cambios, la ecuación (2.2) se simplifica, quedando de la siguiente forma:

$$y^2 = x^3 - 27c_4x - 54c_6$$

con c_4, c_6:

$$\begin{cases} c_4 = b_2^2 - 24b_4, \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{cases}$$

Llegando a la ecuación que queríamos de nuestra curva C:

$$y^2 = x^3 + Ax + B. \tag{2.3}$$

Donde A y B toman los siguientes valores:

$$\begin{cases} A = -27c_4, \\ B = -54c_6. \end{cases}$$

A la ecuación (2.3) la denominaremos forma corta de Weierstrass de la curva C. Homogeneizando de nuevo obtenemos que C esta definida por el siguiente polinomio:

$$F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3. \tag{2.4}$$

Necesitamos saber cuáles son las condiciones necesarias para que esta curva sea una curva no singular. Vamos a calcular los puntos singulares de nuestra curva C. Tenemos que el único punto con $Z = 0$ es el punto $\mathcal{O}$, que no es punto singular. Esto implica que todo se reduce a calcular el valor $[X : Y : 1]$ tal que $F(X, Y, 1) = 0$.

Sean las derivadas parciales de $F(X,Y,Z)$:

$$\begin{cases} \dfrac{\partial F}{\partial X} = -3X^2 - AZ^2 = 0, \\ \dfrac{\partial F}{\partial Y} = 2YZ = 0, \\ \dfrac{\partial F}{\partial Z} = Y^2 - 2AXZ - 3BZ^2 = 0, \end{cases}$$

Como se puede apreciar, nos queda que cualquier punto singular ha de cumplir que $Y = 0$, ya que $Z \neq 0$.

Con lo cual, podemos plantear el siguiente sistema de ecuaciones:

$$\begin{cases} -3X^2 - A = 0, \\ -2AX - 3B = 0. \end{cases}$$

Si despejamos X en la segunda ecuación nos queda.

$$\begin{aligned} 2AX + 3B &= 0, \\ X &= -\frac{3B}{2A}. \end{aligned}$$

En el caso de que A fuese cero tenemos que

$$\begin{aligned} -3X^2 &= 0, \\ 3B &= 0, \end{aligned}$$

Tendríamos que $B = 0$ y $X = 0$ ya que nos quedaría la ecuación $Y^2Z = X^3$, en la que el punto $[0:0:1]$ es singular.

Volviendo al caso general. Si sustituimos en la primera ecuación del sistema el resultado sería

$$\begin{aligned} 3\left(\frac{3B}{2A}\right)^2 + A^2 &= 0, \\ (27B^2 + 4A^3) &= 0. \end{aligned}$$

Viendo este resultado obtenemos que la condición necesaria y suficiente para que nuestra curva sea singular será:

$$\Delta = 4A^3 + 27B^2 = 0. \tag{2.5}$$

El discriminante de nuestra curva será Δ.

Ya estamos en condiciones de definir las curvas elípticas:

Definición 2.1. Sean $A, B \in K$ y $F(X,Y,Z) = ZY^2 - X^3 - AXZ^2 - BZ^3$. Sea C la curva proyectiva plana asociada al polinomio F. Diremos que C es una curva elíptica definida sobre K si y sólo si $\Delta \neq 0$.

De una forma más general, para definir que una curva C sea una curva elíptica sobre un cuerpo K se tienen que cumplir:

1. El género de C tiene que ser igual a uno.
2. $C(K) \neq \emptyset$.

Si definimos nuestra curva con la forma de Weierstrass corta, tenemos una ecuación algebraica de grado 3 definida sobre K con $a_1, a_2, a_3, a_4, a_6 \in K$. Además para todas las ecuaciones de ese tipo siempre está contenido el punto $[0 : 1 : 0] \in C(K)$. De acuerdo con lo anterior, nuestro tipo de curva cumpliría el punto 2. Veamos qué tiene que suceder para que se cumpla el punto 1.

Para que el género de la curva sea 1 tenemos que:

$$g(C) = \frac{(3-1)(2-1)}{2} - s = 1.$$

Que solo es posible si $s = 0$. Esto a su vez determina que la curva algebraica no tenga ningún punto singular. Para que nuestra curva no tenga puntos singulares su discriminante debe ser distinto de cero.

$$\Delta = 4A^3 + 27B^2 \neq 0.$$

Además, si el discriminante es no nulo, se tiene que la curva es lisa.

Se puede demostrar con técnicas más avanzadas que dada una curva definida sobre un cuerpo K de género 1 y con algún punto definido sobre K que dicha curva se pueda dar por un modelo de Weierstrass.

Una vez hemos estudiado algunas nociones básicas sobre las curvas elípticas, podemos continuar con la definición de ley de grupo en las curvas elípticas.

2.2. Ley de Grupo

Sea E una curva elíptica sobre un cuerpo K definida por un modelo corto de Weierstrass $y^2 = x^3 + Ax + B$. Empezamos definiendo las operaciones para la ley de grupo.

Sean dos puntos P y Q en $E(K)$. En primer lugar trazamos la recta que pasa por P y Q. Por el Teorema de Bezout sabemos que hay un tercer punto de corte, que se denotará $P * Q$. Además veamos que $P * Q \in E(K)$. Supongamos que $E(K)$ esta determinada por un polinomio homogéneo $F(X, Y, Z) \in K[X, Y, Z]$ de grado 3. Si $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ entonces si $y = mx + n$ es la recta que une a P y Q, entonces $m, n \in K$. Ahora $F(x, mx + n, 1)$ es un polinomio de grado 3 en la variable x con coeficientes en K cuyas raíces son x_1, x_2, x_3. Por lo tanto $x_3 \in K$, y de ahí obtenemos $y_3 \in K$. Concluyendo $P * Q \in E(K)$.

Un par de propiedades fundamentales de la operación $*$ son:

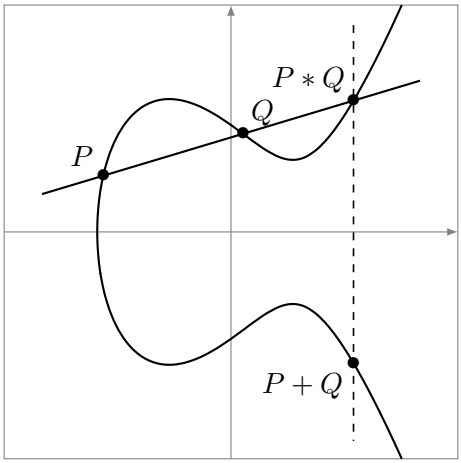


Figura 2.1: Operación + en una curva elíptica

1. $P * Q = Q * P$.
2. $(P * Q) * Q = P$.

Después de conseguir el punto $P * Q$ calculamos $P + Q$ con la recta paralela al eje y que pase por el punto ya definido. $P + Q$ será el corte de esa recta con nuestra curva elíptica. La ley de grupo quedará definido como

$$P + Q = (P * Q) * \mathcal{O}. \tag{2.6}$$

Definiremos el elemento neutro de nuestro grupo como $\mathcal{O} = [0 : 1 : 0]$.

Es importante ver que $P + Q = Q + P$ ya que

$$P + Q = (P * Q) * \mathcal{O} = (Q * P) * \mathcal{O} = Q + P. \tag{2.7}$$

Nos apoyaremos en esta propiedad mas adelante, con esto llegamos a la conclusión de que la operación + es conmutativa para cualquier $P, Q \in E(K)$. Veamos ahora la demostración de la ley de grupo. Para ello necesitamos que se cumplan las tres propiedades fundamentales de grupo.

1. **Elemento neutro:** $P + \mathcal{O} = P$.

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

   Utilizando las dos propiedades referidas anteriormente.

2. **Elemento inverso**: si definimos el elemento inverso para $P = (x, y) \in E(K)$ como $-P = (x, -y)$, que es el punto simétrico respecto al eje X, al hacer $P + (-P)$ obtenemos.

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

La prueba de la tercera propiedad de grupo, la propiedad asociativa

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

no es evidente. Por lo que será necesario un análisis más complejo que presentamos a continuación.

Para ello nos vamos a apoyar en el siguiente resultado.

Lema 2.2. *Sean $P_1, ..., P_8 \in \mathbb{P}^2(\overline{K})$, 8 puntos racionales en posición general: no hay cuatro puntos en linea recta ni 7 en una cónica. Entonces existe un noveno punto P_9 que pertenece a toda cúbica que pase por los 8 puntos anteriores.*

Demostración. Para empezar definimos una curva cúbica plana como:

$$E = \left\{[x, y, z] \in \mathbb{P}^2(\overline{K}) : F(x, y, z) = 0\right\}, \tag{2.8}$$

con $F(x, y, z) \in K[x, y, z]$ homogéneo de grado 3. Nuestra F será de la forma:

$$F(x, y, z) = a_1x^3+a_2y^3+a_3z^3+a_4x^2y+a_5x^2z+a_6xy^2+a_7y^2z+a_8xz^2+a_9yz^2+a_{10}xyz,$$

con $a_1, ..., a_{10} \in K$.
Por estar los 8 puntos en posición general, las condiciones lineales $F(P_i) = 0$ con $i = 1..,8$ sobre los coeficientes de F son independientes. Por tanto las cúbicas planas que pasan por $P_1, ..., P_8$ forman un espacio vectorial de dimensión 2 debido a la posición general de los puntos.

Definamos dos cúbicas E_1 y E_2, con polinomios homogéneos $F_1, F_2 \in K[x, y, z]$ independientes que cumplan que los ocho puntos definidos anteriormente pertenezcan a la intersección de ambas curvas. Cualquier cúbica que pase por esos 8 puntos quedará definida por un polinomio homogéneo del tipo:

$$F(x, y, z) = \alpha F_1(x, y, z) + \beta F_2(x, y, z) \tag{2.9}$$

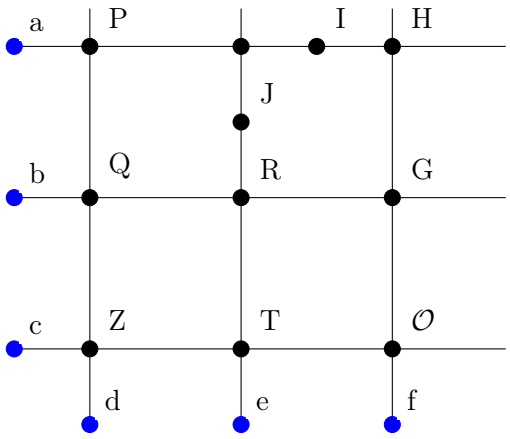
con $\alpha, \beta \in K$.

Si aplicamos el Teorema de Bézout, E_1 y E_2 tienen 9 puntos en común. Esto implica que $\exists P_9 \in E_1 \bigcap E_2$ tal que $P_9 \neq P_1, ..., P_8$ Quedando demostrado nuestro lema.

Para la realización de esta demostración me he apoyado en [2]. □

Demostrado el lema demostraremos la propiedad de la asociatividad.

Demostración de la Propiedad Asociativa. Para empezar la prueba, consideremos el siguiente gráfico:



Tenemos los puntos $P, Q, R \in E(K)$. Definimos los puntos de la figura como

$$\begin{aligned} Z &= P * Q \\ G &= Q * R \\ H &= Q + R = (Q * R) * \mathcal{O} \\ T &= P + Q = (P * Q) * \mathcal{O} \\ i &= H * P = (Q + R) * P \\ J &= T * R = (P + Q) * R \end{aligned}$$

Donde a, b, c, d, e, f son rectas que pasan por los puntos indicados. Obsérvese que todos los puntos pertenecen a $E(K)$. El objetivo de la prueba es ver que I y J son el mismo punto.

Para ello utilizaremos el lema anterior.

Definimos las cúbicas F_1 y F_2:

$$\begin{cases} F_1 = a \cdot b \cdot c, \\ F_2 = d \cdot e \cdot f. \end{cases}$$

Podemos apreciar que $P, Q, Z, R, T, H, G, \mathcal{O} \in F_1 \cap F_2$ y también que:

$$\begin{cases} I \in F_1, \\ J \in F_2. \end{cases}$$

Como hemos dicho antes, el objetivo de esta prueba es ver que $I = J$. Para demostrarlo lo probaremos por reducción al absurdo.

Supongamos $I \neq J$. En este caso, tendríamos que $I \in F_2$ y $J \in F_1$. Lo que nos conduce a afirmar que el número de puntos en el que intersecan ambas cúbicas son 10. Esto entraría en contradicción con el teorema de Bézout, que asegura que que el número máximo de puntos de intersección de ambas cúbicas tiene que ser 9. Por tanto $I \notin F_2$ ó $J \notin F_1$.

Comprobemos que $I = J$. Para realizar esta demostración usaremos el lema anteriormente explicado. Tenemos que los ocho puntos referidos pertenecen a la intersección de las cúbicas F_1 y F_2. Estos ocho puntos se encuentran en posición general ya que:

1. Si cuatro puntos se encuentran en una recta T, al pertenecer a E

$$\sum_{P \in T \cap E} I_P(E, T) = 3 < 4.$$

   Que supone una contradicción con el teorema de Bézout.

2. Si 7 puntos pertenecen a una cónica C, también pertenecerían a nuestra curva elíptica E. Esto también entraría en contradicción con el teorema de Bézout ya que:

$$\sum_{P \in C \cap E} I_P(E, C) = 2 \cdot 3 = 6 < 7.$$

Debido a estos resultados podemos afirmar que tenemos las condiciones del lema anterior. Por tanto, $I = J$ siendo el noveno punto en común. Acabamos de demostrar que

$$(P + Q) * R = P * (Q + R). \tag{2.10}$$

Usando esta ecuación con la propiedad (2.7) tenemos

$$(P+Q)+R = [(P+Q)*R)]*\mathcal{O} = [P*(Q+R)]*\mathcal{O} = (Q+R)+P = P+(Q+R) \tag{2.11}$$

Así quedaría demostrada la propiedad asociativa y por ende las 3 propiedades necesarias de un grupo. □

Se puede apreciar que este grupo es abeliano por (2.7). Con esta demostración podemos deducir el siguiente teorema.

Teorema 2.3. *Sea E una curva elíptica sobre un cuerpo K y sea $+$ la operación de grupo, entonces $(E(K), +)$ es un grupo abeliano.*

2.3. Forma Explícita de la Ley de Grupo

Veamos como construimos de forma explicita la Ley de Grupo estudiada en la sección 2.2.

Definimos $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$. Trazamos la recta que une ambos puntos y calculamos su intersección con nuestra curva elíptica. El punto de corte será $P_3 = (x_3, y_3)$.

Calculamos la recta que une P_1 y P_2.

$$\begin{cases} y = \lambda x + n, \\ \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, \\ n = y_1 - \lambda x_1 = y_2 - \lambda x_2. \end{cases} \tag{2.12}$$

Procedemos a sustituir en nuestra ecuación

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

Si operamos, nos queda:

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

Esta cúbica tiene como raíces x_1, x_2 y x_3.

$$x^3 - \lambda^2 x^2 + (A - 2\lambda n)x + B - n^2 = (x - x_1)(x - x_2)(x - x_3) = 0.$$

Si igualamos los coeficientes podemos calcular P_3

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda x_3 + n. \end{cases} \tag{2.13}$$

Si queremos la fórmula explicita nos quedaría

$$\begin{cases} x_3 = \left(\dfrac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 = \dfrac{y_2 - y_1}{x_2 - x_1} x_3 + n. \end{cases} \tag{2.14}$$

Sea el caso de $P_1 = P_2$. No podemos usar el mismo método que en el anterior caso. Para resolver este problema tendremos que utilizar la recta tangente al punto P_1. Si fijamos $y^2 = F(x) = x^3 + Ax + B$, derivando implícitamente la fórmula para calcular λ es:

$$\lambda = \frac{F'(x)}{2y} = \frac{3x^2 + A}{2y}.$$

Definimos $[2]P_1 = P_1 + P_1$ al punto que se calcula a partir de un único punto P_1. Nuestra recta será igual que la anterior $y = \lambda x + n$

$$\begin{aligned} x([2]P_1]) &= \lambda^2 - 2x_1, \\ y([2]P_1) &= \lambda x([2]P_1) + n. \end{aligned}$$

Y nuestra fórmula explícita quedaría como:

$$\begin{cases} x([2]P_1) = \dfrac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4x_1^3 + 4Ax_1 + 4B}, \\ y([2]P_1) = \left(\dfrac{3x_1^2 + A}{2y_1} x([2]P_1)\right) + y_1 - \left(\dfrac{3x_1^2 + A}{2y_1}\right) x_1. \end{cases}$$

Con este resultado terminamos nuestra revisión de los resultados básicos de curvas elípticas. En el siguiente apartado, estudiaremos el Teorema de Mordell y los subgrupos de torsión.

CAPÍTULO 3
Teorema de Mordell y Subgrupos de Torsión

En este capítulo haremos un estudio sobre la teoría fundamental de las curvas elípticas. Empezaremos enunciando el teorema de Mordell y continuaremos con los puntos de orden finito y el subgrupo que genera, denominado subgrupo de torsión. También estudiaremos teoremas para la clasificación del subgrupo de torsión y la morfología de los puntos de orden finito.

3.1. Teorema de Mordell

Para empezar, enunciaremos el Teorema de Mordell

Teorema de Mordell. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finítamente generado. Por tanto:*

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

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

Recordemos que si G es un grupo abeliano finitamente generado entonces podemos afirmar que G es isomorfo a la suma directa de grupos cíclicos primarios (elementos con orden finito) y grupos cíclicos infinitos (parte libre).

Definimos el subgrupo de torsión $E(\mathbb{Q})_{tors}$ compuesto por los puntos definidos sobre $\mathbb{Q}$ de orden finito pertenecientes a la curva y los puntos definidos sobre $\mathbb{Q}$ de orden infinito es isomorfa a $\mathbb{Z}^r$. Se puede profundizar en este tema en [8].

El cálculo del rango r es uno de los principales problemas en la actualidad, ya que no existe un algoritmo que permita calcularlo para cualquier curva elíptica. Está en relación con la conjetura de Birch y Swinnerton-Dyer.

3.2. Subgrupo de Torsión

Definición 3.1. Sea E una curva elíptica definida sobre un cuerpo K y sea $n \in \mathbb{Z}$ vamos a definir el subgrupo de n-torsión como

$$E[n] = \left\{ P \in E(\overline{K}) | nP = \mathcal{O} \right\},$$

donde K es un cuerpo y $\mathcal{O} = [0; 1; 0]$

Como ejercicio, vamos a proceder a calcular el subgrupo de 2-torsión y 3-torsión para cualquier curva elíptica $E : y^2 = x^3 + Ax + B$ en forma de Weierstrass.

Para que un punto $P = (x, y) \in E[2]$. Necesitamos que $[2]P = \mathcal{O}$, es decir, $P = -P = (x, -y)$.Concluyendo $y = 0$. Nuestro subgrupo de 2-torsión lo formarán los puntos de la curva que se encuentren en el eje de las X, ya que $y = 0$. Al tener una curva de la forma $y^2 = x^3 + Ax + B$ podemos observar que el número máximo que de puntos que cortan al eje Y son 3. Esto implica que nuestro subgrupo de 2-torsión estará formado como mucho por estos 3 puntos más el elemento neutro, que en este caso será el $\mathcal{O}$. Nuestro subgrupo de 2-torsión es

$$E[2] = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Para el subgrupo de 3-torsión, su definición formal será:

$$E[3] = \left\{ P \in E(\overline{K}) | 3P = \mathcal{O} \right\}.$$

Para este caso, necesitamos que

$$\begin{aligned} x([2]P_1) &= x(P_1), \\ y([2]P_1) &= -y(P_1). \end{aligned}$$

Si seguimos el razonamiento, tenemos:

$$\begin{aligned} \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4x_1^3 + 4Ax_1 + 4B} &= x_1, \\ x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2 &= 4x_1^4 + 4Ax_1^2 + 4Bx_1, \\ 3x_1^4 + 6Ax_1^2 + 12Bx - A^2 &= 0. \end{aligned}$$

Los puntos cuya coordenada en x cumpla esta condición serán los puntos de 3-torsión para cualquier curva en forma corta de Weierstrass.

Para calcular los puntos de torsión de una manera más general, podemos aplicar los polinomios de división. Se definen de forma recurrente:

$$\begin{cases} \Psi_0 = 0, \\ \Psi_1 = 1, \\ \Psi_2 = 2y, \\ \Psi_3 = 3x^4 + 6Ax^3 + 12Bx - A^2. \end{cases}$$

A partir de $m = 3$:

$$\begin{cases} \Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, \\ \Psi_{2m} = \left(\dfrac{\Psi_m}{\Psi_2}\right)(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2). \end{cases}$$

Las raíces de $\Psi_n(x)$ nos dan las x-coordenadas de los puntos de orden n (ver [8]).

Llegados a este punto, debemos ver uno de los teoremas más importantes para el cálculo del subgrupo de torsión, el teorema de Nagell-Lutz.

Teorema de Nagell-Lutz. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ con ecuación en forma de Weierstrass*

$$y^2 = x^3 + Ax + B,$$

con $A, B \in \mathbb{Z}$. Sea $P = (x(P), y(P)) \in E(\mathbb{Q})_{tors} \backslash \{\mathcal{O}\}$ Entonces:

1. *$x(P), y(P) \in \mathbb{Z}$.*
2. *Si P es de orden 2 entonces $y(P) = 0$.*
3. *Si P tiene un orden mayor que 2 entonces $y(P)^2 | 4A^3 + 27B^2$.*

Calcular la torsión es más fácil gracias a este teorema. Veamos un ejemplo de su aplicación.

Ejemplo 1. *Sea E la curva elíptica con el polinomio asociado $y^2 = x^3 - 1$. Vemos que el punto $P_1 = (1, 0)$ es un punto de 2-torsión. El discriminante de nuestra curva es $\Delta = 27$ y la coordenada y de un punto de torsión podría ser:*

$$0, \pm 1, \pm 3.$$

Para la coordenada $y = \pm 1$, tenemos que $x = 0$. Estos dos puntos, $P_2 = (0, -1)$ y $P_3 = (0, 1)$, son los puntos de 3-torsión. Si calculamos $x([2]P_2) = x(P_2)$ e $y([2]P_2) = -y(P_2)$, ocurre lo mismo con P_3.

Los puntos correspondientes a la coordenada $y = \pm 3$ serán $P_4 = (2, -3)$ y $P_5 = (2, 3)$ que vuelven a corresponder a puntos de torsión. En esto se puede ver que son de orden 6. Si añadimos el punto $\mathcal{O}$, tenemos nuestro subgrupo completo. El subgrupo de torsión será:

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}.$$

Contamos con un teorema que clasifica los tipos de subgrupos de torsión existentes, el teorema de Mazur.

Teorema de Mazur. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces el subgrupo de torsión será isomorfo a uno de los siguientes 15 grupos:*

$$\begin{array}{ll} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 10 \quad n = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & 1 \leq n \leq 4. \end{array}$$

Visto todo lo anterior con los teoremas estudiados, concluimos el capítulo dedicado a la teoría sobre las curvas elípticas. Toda la información de este capítulo se puede contrastar en [1], [6] y [8].

CAPÍTULO 4
Problemas Aritméticos Elementales

En este capítulo abordaremos algunos problemas aritméticos elementales empleando los conceptos y resultados presentados en los capítulos anteriores.

4.1. Un Problema en $\mathbb{Z}$

Hasta ahora hemos analizado los puntos racionales en las curvas elípticas. Para resolver problemas en $\mathbb{Z}$ necesitamos estudiar el siguiente teorema.

Teorema de Siegel. *Sea $E/\mathbb{Q}$ una curva elíptica de ecuación $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Entonces E tiene sólo un número finito de soluciones con coordenadas enteras.*

Para más información acerca del teorema de Siegel ver [6].

No existe ningún algoritmo para calcular todos los puntos racionales de una curva elíptica, pero sí existe dicho algoritmo aplicado a los puntos enteros. Veamos un problema clásico.

El problema que se plantea es: ¿Cuáles son los $n, n+1, n+2$ con $n \in \mathbb{Z}$ tales que, si multiplico esos tres y les sumo uno el resultado es un cuadrado perfecto?

Nuestra ecuación quedaría planteada del siguiente modo.

$$x \cdot (x+1) \cdot (x+2) + 1 = y^2. \tag{4.1}$$

Esta ecuación es una curva elíptica (podemos entenderla como una curva en forma de Weierstrass larga) y cumple que el punto $\mathcal{O}$ está contenido y es una curva lisa, lo que implica genero 1. Además el discriminante de esta curva es distinto de 0 (concretamente es -1664).

La solución del problema radica en encontrar las posibles soluciones enteras del problema. Emplearemos SAGE [7] para determinarlas:

```
sage: Z=EllipticCurve([0,3,0,2,1]); Z
Elliptic Curve defined by y^2 = x^3 + 3*x^2 + 2*x + 1 over Rational
    Field
sage: Z.rank()
1
```

```
sage: Z.torsion_subgroup()
Torsion Subgroup isomorphic to Trivial group associated to the Elliptic
    Curve defined by y^2 = x^3 + 3*x^2 + 2*x + 1 over Rational Field
sage: Z.S_integral_points([])
[(-2 : 1 : 1),
 (-1 : 1 : 1),
 (0 : 1 : 1),
 (2 : 5 : 1),
 (4 : 11 : 1),
 (55 : 419 : 1)]
```

Si analizamos el resultado anterior, observamos que los valores enteros que son solución son los siguientes:

$$\begin{cases} x = -2, y = 1, \\ x = -1, y = 1, \\ x = 0, y = 1, \\ x = 2, y = 5, \\ x = 4, y = 11, \\ x = 55, y = 419. \end{cases}$$

Nuestras tripletas serían $(2, 3, 4)$, $(4, 5, 6)$ y $(55, 56, 57)$, y las tres soluciones triviales, con lo que el problema quedaría resuelto.

En el caso general, nuestro problema quedaría definido por la siguiente ecuación:

$$y^2 = x(x + i)(x + 2i) + j, \tag{4.2}$$

con $i, j \in \mathbb{N}$.

Para obtener las soluciones enteras de la ecuación anterior, emplearemos de nuevo SAGE. Veamos el número de soluciones con $0 \leq i, j \leq 9$:

i \ j	0	1	2	3	4	5	6	7	8	9
0	-	3	1	1	1	1	0	0	4	5
1	3	6	0	1	7	0	1	1	0	7
2	3	11	0	1	7	0	1	1	0	6
3	3	9	0	0	3	0	1	1	3	6
4	3	15	0	0	8	0	1	0	0	3
5	5	13	0	0	3	0	0	2	0	3
6	8	14	0	0	6	0	0	0	0	8
7	4	17	0	1	3	0	0	0	0	3
8	3	26	0	0	14	0	0	0	0	3
9	3	12	0	0	3	0	1	0	1	14

Tabla 4.1: Soluciones Enteras para $i, j \leq 9$.

La casilla de la tabla con un $-$ no tienen resultado, ya que el polinomio con esas características no es una curva elíptica.

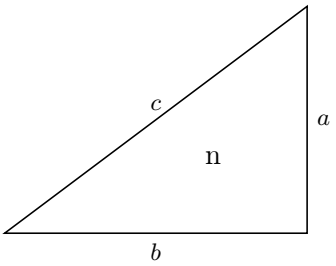
Como curiosidad podemos destacar que las soluciones de las columnas $j = 2, j = 3$ y $j = 5$ sólo tienen soluciones triviales.

4.2. Problemas en $\mathbb{Q}$

4.2.1. Problema del número congruente

El primer problema sobre $\mathbb{Q}$ que vamos a intentar resolver es el problema del número congruente.

Sea el triángulo rectángulo con catetos a y b y la hipotenusa c. El área del triángulo es n. El objetivo de este problema es determinar si existe un triángulo con área $n \in \mathbb{Q}$ y que cumpla que $a, b, c \in \mathbb{Q}$.



$$\begin{cases} a^2 + b^2 = c^2 \\ \dfrac{a \cdot b}{2} = n \end{cases}$$

Podemos plantear el problema mediante las siguientes dos ecuaciones:

$$(a \pm b)^2 = \quad a^2 + b^2 \pm 2ab = c^2 \pm 4n.$$

De aquí podemos hacer un cambio $x = \left(\dfrac{c}{2}\right)^2$. Esto implica:

$$\left(\frac{1}{2}(a \pm b)\right)^2 = x \pm n. \tag{4.3}$$

Al tomar este cambio sabemos que $x+n$ y $x-n$ son cuadrados de racionales, además $x = \left(\frac{c}{2}\right)^2$. Si son cuadrados de racionales, tenemos que: $\sqrt{x-n}, \sqrt{x}, \sqrt{x+n} \in \mathbb{Q}$. Por tanto:

$$\begin{cases} a = \sqrt{x+n} - \sqrt{x-n}, \\ b = \sqrt{x+n} + \sqrt{x-n}, \\ c = 2\sqrt{x}. \end{cases} \tag{4.4}$$

y se cumple que:

$$a^2 + b^2 = \left(\sqrt{x+n} - \sqrt{x-n}\right)^2 + \left(\sqrt{x+n} + \sqrt{x-n}\right)^2 = 4x = c^2.$$

También se cumple que:

$$\frac{1}{2}ab = \frac{1}{2}\left(\sqrt{x+n} - \sqrt{x-n}\right) * \left(\sqrt{x+n} + \sqrt{x-n}\right) = \frac{1}{2}2n = n.$$

Con estos resultados se infiere el siguiente teorema.

Teorema 4.1. *Dado $n \geq 0$ tal que $n \in \mathbb{Q}$, existe una biyección entre los triángulos rectángulos $(a, b, c) \in \mathbb{Q}$ de área n y los $(x-n, x, x+n)$ cuadrados de racionales.*

Planteamos la siguiente ecuación:

$$x(x-n)(x+n) = x^3 - n^2x.$$

Definamos la curva:

$$E_n : y^2 = x^3 - n^2x. \tag{4.5}$$

Esta curva cumple nuestra definición de curva elíptica. Es una curva en forma de corta de Weierstrass. El discriminante de nuestra curva es siempre distinto de cero ya que $\Delta = 4n^2 \neq 0$ porque $n \neq 0$.

Vamos a ver el subgrupo de torsión.

Los puntos de 2-torsión son aquellos para los que se cumple que $y = 0$. Para nuestra curva $y^2 = x^3 - n^2x$, tenemos que esos puntos son $(-n, 0), (0, 0), (n, 0)$. Ninguno de estos tres puntos racionales son solución para nuestro problema ya que:

1. Si $x = 0, y = 0$, tenemos que el triangulo tiene hipotenusa 0, lo que no tiene sentido.

2. Para los puntos $(n, 0), (-n, 0)$ tenemos que:

$$\begin{cases} a = \sqrt{2n}, \\ b = \sqrt{2n}, \\ c = 2\sqrt{n}. \end{cases}$$

   Si $\sqrt{2n} \in \mathbb{Q}$ entonces n tiene que ser de la forma $2^{2k+1}t$ con $k \in \mathbb{Z}$. Esto implica que $c = 2\sqrt{n} \notin \mathbb{Q}$ con lo cual no cumple las hipótesis iniciales.

De hecho se tiene el siguiente resultado:

Teorema 4.2. *Todas la familia de curvas elípticas E_n de la forma $y^2 = x^3 - n^2x$ con $n \in \mathbb{Q}$, cumplirán que*

$$E_n(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

La demostración de este teorema se encuentra en [5].

Recordemos, que el Teorema de Mordell nos dice en el caso particular de nuestra curva elíptica:

$$E_n(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^r,$$

donde r es el rango de $E_n(\mathbb{Q})$. De lo que se deduce:

Teorema 4.3. *Un número racional positivo es congruente si y solo si el rango de $E_n(\mathbb{Q})$ es no nulo.*

De este problema podemos deducir el siguiente teorema.

Teorema 4.4. *Ningún cuadrado de un número entero puede ser el área de un triángulo rectángulo con lados pertenecientes a $\mathbb{Q}$.*

Demostración. Supongamos que el área de nuestro triángulo rectángulo sea m^2 con $m \in \mathbb{Q}$. Nuestra curva elíptica quedará determinada por:

$$y^2 = x^3 - (m^2)^2 x.$$

Esto es idéntico a decir que:

$$y^2 = x^3 - m^4 x.$$

Llegados a este punto vamos a realizar un *twist*. Para ello tomaremos:

$$\begin{cases} x = m^2 x, \\ y = m^3 y. \end{cases}$$

Quedando nuestra curva elíptica como:

$$y^2 = x^3 - x.$$

```
sage: F= EllipticCurve([-1,0]);F
Elliptic Curve defined by y^2 = x^3 - x over Rational Field;
sage: f = F.torsion_subgroup(); f
Torsion Subgroup isomorphic to Z/2 + Z/2 associated to the Elliptic
    Curve defined by y^2 = x^3 - x over Rational Field
sage: ff = F.torsion_points(); ff
[(-1 : 0 : 1), (0 : 0 : 1), (0 : 1 : 0), (1 : 0 : 1)]
sage: fr = F.rank(); fr
0
```

Con estos resultados vemos que $E_{m^2}(\mathbb{Q}) = E_{m^2}(\mathbb{Q})_{tors}$. Esto implica que no existen triángulos con lados racionales y cuyo área sea el cuadrado de un entero.

□

Planteamos ahora el mismo problema pero cambiando el área del triángulo por 6 tenemos:

```
sage: E=EllipticCurve([-36,0]);E
Elliptic Curve defined by y^2 = x^3 - 36*x over Rational Field
sage: E.rank()
1
sage: F=E.torsion_subgroup();F
Torsion Subgroup isomorphic to Z/2 + Z/2 associated to the Elliptic
    Curve defined by y^2 = x^3 - 36*x over Rational Field
```

En esta situación, nuestra curva elíptica tiene rango 1, lo que conlleva que hay infinitas soluciones para nuestro polinomio. Para cada valor de x en los racionales, podemos realizar los cambios vistos anteriormente en (4.4) y calcular los lados del triángulo. Podemos conseguir una solución con $x = 25/4, y = 35/8$. Esta solución es el triángulo rectángulo con catetos 3 y 4 e hipotenusa 5.

4.2.2. Triángulos de igual perímetro y área

El objetivo de este problema es averiguar si existen triángulos con distintos lados pero mismos perímetro y área. Trataremos de averiguar si hay algún método general para hallar dichos triángulos.

Para ello vamos a intentar estudiar los triángulos desde otro punto de vista.

Cada triángulo tiene un círculo inscrito de radio r que cumple

$$A = rs. \tag{4.6}$$

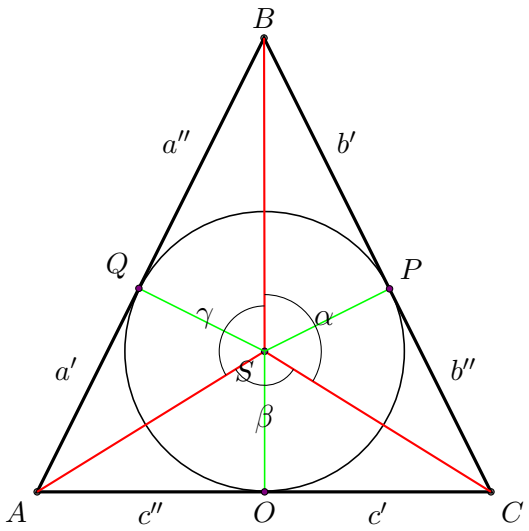


Figura 4.1: Triángulo de Herón

Donde A es el área y s es la mitad del perímetro, que a partir de ahora llamaremos semiperímetro.

Tomemos el vértice A de la figura. Si unimos A con el incentro nos quedan dos triángulos rectángulos simétricos con lados a', r y c'', r (la definición de incentro nos permite afirmar que ambos lados están a la misma distancia de la bisectriz). Si repetimos el proceso con los vértices restantes nos quedan seis triángulos. Podemos decir que el área de la figura 4.1 es la suma de las áreas de los seis triángulos que hemos generado. Nos quedaría:

$$\frac{ra' + ra'' + rb' + rb'' + rc' + rc''}{2} = r\frac{a' + a'' + b' + b'' + c' + c''}{2} = rs$$

Podemos ver el semiperímetro como:

$$s = r\left(tan\frac{\alpha}{2} + tan\frac{\beta}{2} + tan\frac{\gamma}{2}\right) \tag{4.7}$$

Esta formula se extrae del cálculo del incentro. Realizamos la intersección de las bisectrices. Una vez tenemos el baricentro, unimos con los puntos P, O, Q generando tres segmentos desde nuestro baricentro hasta P, O, Q con longitud r.

De cada Bisectriz se generan dos triángulos. Vamos a tomar uno por cada bisectriz, ya que el otro es simétrico. Fijémonos en el ángulo α. la bisectriz del ángulo es el radio de la circunferencia que tiene por centro al incentro. Nos queda un triangulo con ángulo $\alpha/2$ el cálculo de la tangente de $\alpha/2$ será el lado opuesto al que llamaremos b' entre el cateto contiguo, que es el radio r. Si multiplicamos por r tenemos el lado b'. Con cada bisectriz se generan dos triángulos simétricos. Si repetimos el proceso con a' y c'. nos queda la suma de 3 lados $a' + b' + c'$. Esto es el semiperímetro de nuestro triángulo. La suma de las tangentes cumple

$$tan\frac{\alpha}{2} + tan\frac{\beta}{2} + tan\frac{\gamma}{2} = \frac{s^2}{A}. \tag{4.8}$$

Tomamos los cambios $X = tan(\alpha/2)$ $Y = tan(\beta/2)$ $Z = tan(\gamma/2)$ y además se cumple que $\alpha + \beta + \gamma = 2\pi$. Es obvio que:

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

Realizamos los cambios anteriores y nos queda:

$$Z = tan\left(\pi - \frac{\alpha}{2} - \frac{\beta}{2}\right) = -tan\left(\frac{\alpha}{2} + \frac{\beta}{2}\right) = -\frac{tan(\alpha/2) + tan(\beta/2)}{1 - (tan(\alpha/2)tan(\beta/2)} = -\frac{X+Y}{1-XY}.$$

Tomamos $k = s^2/A$ y nos queda la ecuación

$$X + Y - \frac{X+Y}{1-XY} = k. \tag{4.9}$$

Que se puede reescribir como:

$$X^2Y + XY^2 = kXY - k.$$

Ahora homogeneizamos nuestra ecuación.

$$X^2Y + XY^2 = kXYZ - kW^3.$$

Considerando el cambio

$$\begin{cases} X = 1, \\ Y = -\dfrac{u}{k}, \\ W = \dfrac{v}{k}. \end{cases}$$

Nuestra curva queda así:

$$v^2 + kvu + kv = u^3. \tag{4.10}$$

Para seguir con la notación haremos el cambio,

$$\begin{cases} v = y, \\ u = x. \end{cases}$$

El resultado sería:

$$y^2 + kxy + ky = x^3 \tag{4.11}$$

Tenemos una ecuación de Weierstrass en forma general. Nuestra ecuación depende de k, donde $k = \frac{s^2}{A}$. Analicemos un ejemplo. Sea el triángulo de lados $3, 4, 5$ con área 6 y semiperímetro 6. Nuestra ecuación quedaría como:

$$y^2 + 6xy + 6y = x^3$$

Para buscar las soluciones tenemos que estudiar el grupo de Mordell-Weil. Veamos los resultados en SAGE

```
sage: f = EllipticCurve([6,0,6,0,0]);f
Elliptic Curve defined by y^2 + 6*x*y + 6*y = x^3 over Rational Field
sage: g= f.torsion_subgroup(); g
Torsion Subgroup isomorphic to Z/3 associated to the Elliptic Curve
    defined by y^2 + 6*x*y + 6*y = x^3 over Rational Field
p= f.torsion_points(); p
[(0 : -6 : 1), (0 : 0 : 1), (0 : 1 : 0)]
sage: h = f.rank(); h
1
```

El rango de nuestra curva es 1, los puntos de torsión no son solución ya que al realizar los cambios tenemos que para los tres puntos se tiene $\alpha + \beta + \gamma \neq 2\pi$. La solución de nuestro problema se encuentra en la parte libre. Al tener rango distinto de cero se pueden encontrar triángulos con lados distintos pero mismo perímetro y área, por ejemplo si tomamos el punto $(-35/9 : 343/27)$ tenemos el triángulo de lados $[41/15, 156/35, 101/21]$.

Podemos conjeturar por las diversas pruebas realizadas en SAGE que todos los subgrupos de torsión de esta familia de curvas son isomorfos a $\mathbb{Z}/3\mathbb{Z}$.

4.2.3. Problema de los 4 cuadrados en progresión aritmética

En este problema nuestro objetivo será demostrar si existe alguna cuaterna de números $a, b, c, d \in \mathbb{Q}$, tal que $a^2 + n = b^2$, $b^2 + n = c^2$, y $c^2 + n = d^2$. Observar si $n = 0$, la progresión constante a^2, a^2, a^2, a^2 es solución. Este caso corresponde a $\pm a, \pm a, \pm a, \pm a$, que llamaremos soluciones triviales.

Ahora, podemos plantear el problema como $a, b, c, d \in \mathbb{Q}$ que estén en la intersección de $a^2 + c^2 = 2b^2$ y $b^2 + d^2 = 2c^2$. Despejando b^2 en la segunda ecuación y sustituyendo en la primera ecuación, nos queda:

$$\begin{cases} a^2 + 2d^2 = 3c^2, \\ 2c^2 - d^2 = b^2. \end{cases} \tag{4.12}$$

Ahora tomamos la parametrización para la primera cónica:

$$(a, d, c) = (2t^2 - 4t - 1, 2t^2 + 2t - 1, 2t^2 + 1) \tag{4.13}$$

Si sustituimos los valores de la parametrización en nuestra segunda ecuación, nos queda:

$$T : b^2 = 4t^4 - 8t^3 + 8t^2 + 4t + 1.$$

Se puede demostrar [1] que nuestra curva T es de género 1 con algún punto racional, es decir, es una curva elíptica sobre $\mathbb{Q}$. En particular tiene un modelo de Weierstrass. De hecho se tiene que una forma corta de Weierstrass es:

$$E : y^2 = x(x-1)(x+3). \tag{4.14}$$

Hemos reducido el problema de encontrar progresiones aritméticas de cuatro cuadrados en el problema de calcular los puntos racionales de E.

Calculamos el grupo de Mordell-Weil de esta curva usando SAGE:

```
sage: RM=EllipticCurve([0,2,0,-3,0]); RM
Elliptic Curve defined by y^2 = x^3 + 2*x^2 - 3*x over Rational Field
sage: RM.rank()
0
sage: k=RM.torsion_subgroup();k
Torsion Subgroup isomorphic to Z/4 + Z/2 associated to the Elliptic
    Curve defined by y^2 = x^3 + 2*x^2 - 3*x over Rational Field
sage: RM.torsion_points()
[(-3 : 0 : 1),
 (-1 : -2 : 1),
 (-1 : 2 : 1),
 (0 : 0 : 1),
 (0 : 1 : 0),
 (1 : 0 : 1),
 (3 : -6 : 1),
 (3 : 6 : 1)]
```

Los puntos racionales de nuestra curva serán solo los del subgrupo de torsión, ya que el rango de nuestra curva es 0. Esto implica que $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Se puede demostrar [3] que los ocho puntos de torsión corresponden a las soluciones triviales a nuestro problema, que corresponden a progresiones constantes.

Así, podemos afirmar que no existe ninguna cuaterna de números pertenecientes a los racionales que cumpla que sus cuadrados forman una progresión aritmética de longitud 4 no constante.

[1] No vamos a demostrarlo en este trabajo, se puede consultar la demostración en [3]

CAPÍTULO 5
Conclusiones

En este trabajo nos planteábamos la aplicación de la teoría de curvas elípticas para la la resolución de una serie de problemas de aritmética. Para ello, como primer paso comenzamos estudiando algunas nociones básicas de geometría algebraica. Este estudio era imprescindible para poder trabajar con las curvas elípticas. Esta primera fase de estudio y familiarización ha sido la parte más laboriosa del proyecto dado que durante todo el grado no he tenido que estudiar ningún curso de geometría algebraica.

La segunda parte del trabajo se ha centrado en estudio de la ley de grupo y la teoría fundamental sobre curvas elípticas. Esta parte es la parte más importante del trabajo. Aquí he podido apreciar de primera mano la complejidad que tienen las curvas elípticas. Desde cosas tan sencillas a primera vista como la ley de grupo a temas tan complejos como la conjetura de Birch y Swinnerton-Dyer, que es uno de los problemas del milenio.

La parte final del trabajo ha sido la aplicación de todo lo estudiado en el capítulo anterior para la resolución de problemas clásicos. Problemas de más de dos mil quinientos años como el problema del número congruente. Esta parte ha sido mucho mas libre que las anteriores, la resolución de cada problema nos hacía ver diferente el siguiente problema o como enfocarlo.

Como colofón veo las curvas elípticas como un campo muy extenso, con muchas variantes que me gustaría poder investigar en un futuro, como por ejemplo el estudio de las curvas elípticas en cuerpos finitos y su aplicación con la criptografía.

Por último, me gustaría agradecer a mi tutor Enrique González su esfuerzo y dedicación. Me ha guiado por una rama de las matemáticas que desconocía y me ha facilitado las herramientas necesarias para poder realizar este trabajo.

Bibliografía

[1] Avner Ash y Robert Gross. *Elliptic Tales: Curves, Counting, and Number Theory.* Princeton University Press, 2012.

[2] John W. S. Cassels. *Lectures on Elliptic Curves, LMSST 24.* London Mathematical Society Student Texts. Cambridge University Press, 1991.

[3] Enrique González-Jiménez y Jorn Steuding. «Arithmetic progressions of four squares over quadratic fields». En: *Publicationes Mathematicae Debrecen 77/ 1-2 (2010), 125-138* 77 (2010).

[4] Frances Kirwan. *Complex Algebraic Curves.* London Mathematical Society Student Texts. Cambridge University Press, 1992.

[5] Ken Ono. «Euler's concordant forms». En: *Acta Arith* (1996), págs. 101-123.

[6] Joseph H. Silverman y John T. Tate. *Rational Points on Elliptic Curves.* 2nd. Springer Publishing Company, Incorporated, 2015.

[7] W. A Stein y col. *Sage Mathematics Software (Version 8.6).* The Sage Development Team, 2019.

[8] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition.* 2.ª ed. Chapman & Hall/CRC, 2008.