Números Congruentes: de Pitágoras a la Conjetura de Birch y Swinnerton-Dyer

Uxue Gallego Ruiz

Trabajo de fin de grado de Matemáticas
Universidad de Zaragoza

Director del trabajo: Carlos de Vera Piquero
12 de junio de 2024

Abstract

The purpose of this work is to study the *congruent number problem*. The discussion begins with the simple definition of what a congruent number is and proceeds to explain the relationship between the problem and the broad field of elliptic curves. This ultimately leads us to state the Birch and Swinnerton-Dyer Conjecture.

Congruent numbers are defined as integers that can be represented as the area of a right triangle with rational sides. This definition is followed by the result discovered by Arab students in the 10th century, which establishes a relationship between congruent numbers and rational numbers x satisfying that $x-n$, x, and $x+n$ are each the square of a rational number. This relationship is the reason why these numbers are called congruent, as $x-n$, x, and $x+n$ are congruent modulo n.

Using this correspondence, the paper proceeds to derive a cubic equation related to the problem. This equation is

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

Moreover, it is proved that there is a bijective mapping between right triangles with rational sides and area n, and rational solutions of the above cubic equation with $y \neq 0$. Thus, the problem of finding congruent numbers is translated into solving this cubic equation.

This cubic equation happens to be an elliptic curve. For this reason, the necessary background about them is discussed. The most relevant result is that if we define a certain group operation for the elliptic curve in the projective space, we give the curve the structure of an abelian group. Therefore, we are able to talk about the order of the points in the elliptic curve.

By using techniques from the study of elliptic curves over $\mathbb{C}$ and combining a reduction modulo prime argument with a theorem of Dirichlet, it is proved that there are only 4 points of finite order in the elliptic curve E_n over the rationals. With this, Mordell's theorem allows us to reformulate our problem as follows:

An integer $n > 0$ is a congruent number if and only if $E_n(\mathbb{Q})$ is infinite.

Finally, the modern Birch and Swinnerton-Dyer Conjecture is stated in order to provide a criterion to decide whether $E_n(\mathbb{Q})$ has infinite points or not.

Índice general

Capítulo 1

Introducción

Determinar si un número entero puede ser el área de un triángulo rectángulo de lados racionales ha sido un problema ampliamente estudiado a lo largo de muchos siglos. Desde el siglo X, cuando estuadiantes árabes reformularon el problema mediante una correspondencia entre dichos triángulos y números racionales x tal que $x-n$, x y $x+n$ son cada uno el cuadrado de un número racional. Hasta el día de hoy que es una cuestión que sigue abierta. El objetivo de este trabajo es estudiar estos números llamados congruentes.

Para ello, en el primer capítulo se presentan las primeras definiciones necesarias sobre el problema. A continuación, se observa que la cuestión no es tan sencilla como su planteamiento a través de un algoritmo paramétrico ineficiente. Con el objetivo de encontrar otra manera en la que abordar la cuestión, se desarrolla en profundidad la equivalencia ya mencionada que fue planteada por los estudiantes árabes. Esta equivalencia da nombre al problema, ya que $x-n$, x y $x+n$ son congruentes módulo n desde la perspectiva habitual. Después, para completar la explicación se demuestra el Teorema de Fermat. Este teorema es un resultado clásico que dice que el número 1 no es congruente y en consecuencia demuestra que ningún cuadrado perfecto lo es. Para finalizar el capítulo, se introduce una ecuación cúbica que resulta ser de gran importancia:

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

De hecho, demostramos que hay una aplicación biyectiva entre las soluciones racionales de esta ecuación E_n con $y \neq 0$ y los tríos racionales que forman un triángulo rectángulo y cuya área es n.

La ecuación anterior define una curva elíptica y por ello dedicamos el segundo capítulo al estudio de esas curvas. En primer lugar, se da la definición de curva elíptica y se presentan la ecuación de Weierstrass simplificada y su forma generalizada. A continuación, definimos una ley de grupo en el conjunto de soluciones racionales de la curva. Para ello, es necesario homogeneizar la ecuación anterior y considerar así la curva proyectiva asociada a E_n. En este proceso, 'ganamos' una solución adicional representada por el único punto de la curva proyectiva que corta la recta del infinito. Este punto, que denotaremos O_{E_n}, juega un papel fundamental en la ley de grupo: es el elemento neutro de la operación. Esta operación resulta que dota a las curvas elípticas de estructura de grupo abeliano. Además, también nos permite hablar sobre el orden de cada punto. Esto es importante para el problema porque resulta que hay una estrecha relación entre los números congruentes n y las soluciones infinitas de la ecuación cúbica E_n. Paradójicamente, el estudio de los puntos de orden infinito es abordado a través de los resultados sobre los puntos de orden finito. Para el estudio de estos puntos, juegan un papel fundamental técnicas que se obtienen estudiando las curvas elípticas sobre los números complejos. Por eso, se introducen las definiciones y resultados necesarios en $\mathbb{C}$ para facilitar el estudio de dichos puntos de orden finito. Al final de este capítulo, conseguimos demostrar un importante resultado que dice que para nuestra curva elíptica concreta E_n solo hay cuatro puntos de orden finito. Es decir, el subgrupo de torsión de $E_n(\mathbb{Q})$ tiene cardinal 4:

$$\#E_n(\mathbb{Q})_{\text{tors}} = 4.$$

Notemos que este resultado es independiente de n. De hecho, los cuatro puntos que forman $E_n(\mathbb{Q})_{\text{tors}}$ son el punto O_{E_n} junto con las soluciones obvias $(0,0),(0,\pm n)$ de la ecuación afín que define E_n (que son

precisamente aquellas en las que $y = 0$).

En el último capítulo, somos capaces de reformular nuestro problema gracias al estudio realizado en los anteriores capítulos. Empezamos presentando el Teorema de Mordell, que plantea que el conjunto de soluciones racionales de una curva elíptica definida sobre ese mismo cuerpo es un grupo abeliano finitamente generado. En consecuencia, relacionando la correspondencia que aparece al final del primer capítulo con la conclusión del tercer capítulo sobre los puntos de orden finito, se obtiene que:

n es congruente si y solo si $E_n(\mathbb{Q})$ *es infinito.*

Finalmente, se presenta de forma breve la conjetura de Birch y Swinnerton-Dyer, que propone un criterio para decidir cuándo el grupo de puntos racionales $E(\mathbb{Q})$ de una curva elíptica E definida sobre $\mathbb{Q}$ es infinito.

Capítulo 2

Números congruentes

En este capítulo se introducen las definiciones necesarias para el problema de los números congruentes, así como una aproximación al problema mediante un algoritmo paramétrico y correspondencias que relacionan el problema con curvas elípticas. Además, ofrecemos la demostración del Teorema de Fermat que asegura que 1 no es congruente. Para este desarrollo se ha seguido el artículo *Congruent Numbers* de K. Conrad [2] y el primer capítulo del libro *Introduction to Elliptic Curves and Modular Forms* de N. Koblitz [1].

2.1. Definiciones

Definición. Sea $n \in \mathbb{Q}^+$. Se dice que n es un *número congruente* si existe un triángulo rectángulo cuyos lados son racionales y tiene área n.

Nota: Supongamos que $r \in \mathbb{Q}^+$ es el área de un triángulo rectángulo con lados $X, Y, Z \in \mathbb{Q}$. Entonces, podemos encontrar un $s \in \mathbb{Q}^+$ tal que $s^2 r$ es un *entero* libre de cuadrados. En este caso, el área del triángulo de lados sX, sY y sZ es $s^2 r$. Por lo tanto, podemos asumir que $r = n$ es un número natural libre de cuadrados sin perder generalidad. De esta manera, probar que 1 no es congruente, resultado que veremos más adelante, demuestra que ningún racional que sea cuadrado es congruente.

Por ejemplo, 6 es el área del triángulo rectángulo de lados 3, 4 y 5 por lo que es un número congruente.

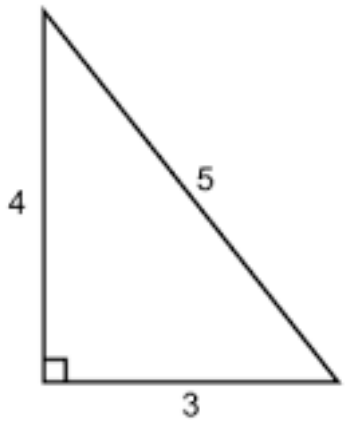

Figura 2.1: Triángulo rectángulo de área 6.

2.2. Algoritmo paramétrico

Es sencillo de observar que los triángulos rectángulos con lados racionales con catetos X, Y e hipotenusa Z están en biyección con las soluciones racionales de $X^2+Y^2=Z^2$, ya que cada triángulo rectángulo debe cumplir esa ecuación y cada trío de números que la cumple puede ser representado como triángulo rectángulo. Sin embargo, si tomamos (a,b,c) una solución sin ninguna restricción, el área $n=ab/2$ del correspondiente triángulo rectángulo no será necesariamente libre de cuadrados como se requiere en la nota anterior. Por eso, se presenta la siguiente definición.

Definición. Llamamos ternas de Pitágoras *primitivas* a las ternas de números enteros positivos (a,b,c) que verifican la igualdad $a^2+b^2=c^2$ y cuyo máximo común divisor es 1.

De esta forma, nos aseguramos de que el área de los triángulos rectángulos correspondientes sea libre de cuadrados. Por eso, será suficiente con limitarnos a ternas de Pitágoras primitivas.

Es bien sabido que existe una manera paramétrica de expresarlas:

$$(k^2-\ell^2,\quad 2k\ell,\quad k^2+\ell^2)$$

donde $k>\ell>0$, $\text{mcd}(k,\ell)=1$ y $k\not\equiv\ell \pmod 2$.

Cuadro 2.1: Tabla de correspondencia

k	ℓ	(a,b,c)	$(1/2)ab$	Parte libre de cuadrados
2	1	(3, 4, 5)	6	6
4	1	(15, 8, 17)	60	15
3	2	(5, 12, 13)	30	30
6	1	(35, 12, 37)	210	210
5	2	(21, 20, 29)	210	210
4	3	(7, 24, 25)	84	21
8	1	(63, 16, 65)	504	126
7	2	(45, 28, 53)	630	70
5	4	(9, 40, 41)	180	5

Sin embargo, de este modo no se puede prever cuánto hay que esperar para encontrar algún número concreto, por lo que se descarta como una herramienta efectiva para encontrar números congruentes o para decidir si un número dado es congruente o no. Por ejemplo, el número 53 es congruente pero no aparece hasta que $k=1873180325$ y $\ell=1158313156$.

2.3. Primera correspondencia

A pesar de que el estudio del problema de los números naturales que resultan ser el área de triángulos rectángulos con lados racionales fue de gran interés para los griegos, se tiene constancia de que estudiantes árabes estudiaron por primera vez, en el siglo X, la cuestión de los números congruentes. Estos estudiantes reformularon el problema mediante la equivalencia recogida en la siguiente proposición:

Proposición 1. *Sea n un entero positivo libre de cuadrados. Sean X,Y,Z números racionales positivos, con $X<Y<Z$. Existe una correspondencia uno a uno entre triángulos rectángulos con catetos X e Y, hipotenusa Z y área n y números racionales x para los cuales $x-n$, x, y $x+n$ son cada uno el cuadrado de un número racional. La correspondencia es:*

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

$$x\longrightarrow (X,Y,Z)=(\sqrt{x+n}-\sqrt{x-n},\quad \sqrt{x+n}+\sqrt{x-n},\quad 2\sqrt{x})$$

En particular, n es un número congruente si y solo si existe $x \in \mathbb{Q}$ tal que $x-n$, x, y $x+n$ son cuadrados de números racionales.

Demostración. Supongamos primero que X, Y, Z es una terna con las propiedades deseadas: $X^2+Y^2 = Z^2$, $\frac{XY}{2} = n$. Si sumamos o restamos cuatro veces la segunda ecuación de la primera, obtenemos:

$$(X \pm Y)^2 = Z^2 \pm 4n \tag{2.1}$$

Si luego dividimos ambos lados por cuatro, vemos que $x = \left(\frac{Z}{2}\right)^2$ tiene la propiedad de que los números $x \pm n$ son los cuadrados de $\frac{X \pm Y}{2}$.

Recíprocamente, dado x con las propiedades deseadas, es fácil ver que los tres números racionales positivos $X < Y < Z$ dados por las fórmulas de la proposición satisfacen:

$$XY = 2n \quad \text{y} \quad X^2+Y^2 = 4x = Z^2.$$

Finalmente, para establecer la correspondencia biunívoca, vemos que dos ternas diferentes no pueden llevar a la misma x. Supongamos que $(X_1, Y_1, Z_1) \neq (X_2, Y_2, Z_2)$ pero que para ambas se cumple que

$$x_1 = \left(\frac{Z_1}{2}\right)^2 = \left(\frac{Z_2}{2}\right)^2 = x_2.$$

Entonces como Z_1 y Z_2 son positivos deducimos que tienen que ser iguales. Además, como

$$X_1 = \sqrt{x_1+n} - \sqrt{x_1} \text{ y } X_2 = \sqrt{x_1+n} - \sqrt{x_1},$$

$$Y_1 = \sqrt{x_1+n} + \sqrt{x_1} \text{ y } Y_2 = \sqrt{x_1+n} + \sqrt{x_1},$$

podemos observar que necesariamente $X_1 = X_2$ y $Y_1 = Y_2$ lo que contradice nuestra suposición de que las ternas son diferentes. □

Se dice que esta correspondencia para números congruentes es una de las razones por las que a estos números se les llama congruentes, ya que $x-n$, x, $x+n$ son congruentes entre ellos módulo n.

2.4. Teorema de Fermat

Siglos después de que los estudiantes árabes investigaran el problema, renombrados matemáticos han contribuido al avance del conocimiento en este ámbito. Como, por ejemplo, Fibonacci, que descubrió que 7 es congruente y planteó que 1 no lo era en el siglo XIII. La primera demostración válida de que 1 no es congruente se conoce gracias a Fermat.

Teorema 2.1 (Fermat, 1640)**.** *El número 1 no es congruente.*

Demostración. Para esta prueba utilizaremos el método de descenso. Este método es particular por contradicción y se emplea para demostrar que una hipótesis no se puede cumplir para ningún número, probando que si se cumpliera, entonces también se cumpliría para números aún más pequeños, generando así un descenso hasta llegar a la contradicción que se obtiene por el principio de conjuntos ordenados.

Supongamos que un triángulo rectángulo de lados racionales tiene área 1. Denotemos los lados como a/d, b/d, y c/d, donde a, b, c, y d son enteros positivos, de modo que $a^2+b^2 = c^2$ y $\frac{1}{2}ab = d^2$. Al quitar el denominador de la segunda ecuación, obtenemos:

$$\begin{aligned} a^2+b^2 &= c^2, \\ ab &= 2d^2. \end{aligned} \tag{2.2}$$

Mostraremos que la ecuación anterior no tiene soluciones en enteros positivos.

Supongamos que existe una solución en enteros positivos para (2.2). Demostraremos que entonces existe una solución donde a y b son primos entre sí. Sea $g = \text{mcd}(a,b)$, entonces $g|a$ y $g|b$. Luego, $g^2|c^2$

y $g^2|2d^2$, por lo tanto, $g|c$ y $g|d$. Dividiendo a, b, c, y d por g, obtenemos otra cuádrupla de enteros positivos que satisface la ecuación anterior con $mcd(a,b) = 1$. Por lo tanto, bastará demostrar que (2.2) no tiene solución en enteros positivos que cumplen que $mcd(a,b) = 1$.

Utilizaremos ahora el método de descenso de Fermat. Para ello, construiremos una 4-tupla de enteros positivos (a',b',c',d') que satisfaga (2.2) con $mcd(a',b') = 1$ y $0 < c' < c$. Repitiendo esto las suficientes veces, llegamos a una contradicción. En el proceso de descenso, utilizaremos lo siguiente: dos enteros positivos relativamente primos cuyo producto es un cuadrado perfecto deben ser cada uno cuadrados perfectos.

Ahora comenzamos el descenso. Dado que $ab = 2d^2$ y a y b son relativamente primos, a o b es par pero no ambos. Entonces $c^2 = a^2 + b^2$ es impar, por lo que c es impar. Dado que ab es el doble de un cuadrado, $mcd(a,b) = 1$, y a y b son positivos, uno es un cuadrado y el otro es el doble de un cuadrado. Los roles de a y b son simétricos, por lo que sin pérdida de generalidad, asumiremos que a es par y b es impar. Entonces $a = 2k^2$, $b = \ell^2$ para algunos enteros positivos k y ℓ, con ℓ impar (porque b es impar). La primera ecuación (2.2) ahora se ve así: $4k^4 + b^2 = c^2$, por lo que:

$$\frac{c+b}{2} \cdot \frac{c-b}{2} = k^4$$

Dado que b y c son ambos impares y relativamente primos, $\frac{c+b}{2}$ y $\frac{c-b}{2}$ son enteros relativamente primos. Por lo tanto:

$$\frac{c+b}{2} = r^4, \quad \frac{c-b}{2} = s^4$$

para algunos enteros positivos relativamente primos r y s. Resolviendo para b y c sumando y restando estas ecuaciones:

$$b = r^4 - s^4, \quad c = r^4 + s^4,$$

Entonces:

$$\ell^2 = b = (r^2 + s^2)(r^2 - s^2).$$

Los factores $r^2 + s^2$ y $r^2 - s^2$ son relativamente primos: cualquier factor común sería impar (ya que ℓ es impar) y divide la suma $2r^2$ y la diferencia $2s^2$, por lo tanto, es un factor de $mcd(r^2, s^2) = 1$. Dado que el producto de $r^2 + s^2$ y $r^2 - s^2$ es un cuadrado impar y uno de ellos es positivo, el otro también es positivo y

$$r^2 + s^2 = t^2, \quad r^2 - s^2 = u^2 \tag{2.3}$$

para enteros positivos impares t y u que son primos entre sí. Dado que $u^2 \equiv 1 \pmod 4$, $r^2 - s^2 \equiv 1 \pmod 4$, lo que obliga a que r sea impar y s sea par. Resolviendo para r^2 en (2.2):

$$r^2 = t^2 + u^2 = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2,$$

donde $\frac{t \pm u}{2} \in \mathbb{Z}$ ya que t y u son impares. La ecuación anterior nos dará una versión más pequeña de (2.2).

Estableciendo $a' = \frac{t+u}{2}$, $b' = \frac{t-u}{2}$, $c' = r$, tenemos $a'^2 + b'^2 = c'^2$. A partir de $mcd(t,u) = 1$ obtenemos $mcd(a',b') = 1$. Además, utilizando (2.3),

$$a'b' = \frac{t^2 - u^2}{4} = \frac{2s^2}{4} = 2\left(\frac{s}{2}\right)^2.$$

Sea $d' = \frac{s}{2} \in \mathbb{Z}$, entonces tenemos una nueva solución (a',b',c',d') . Dado que $0 < c' = r \leq r^4 < r^4 + s^4 = c$, por descenso llegamos a una contradicción. □

Más tarde, Fermat demostraría que el 2 y el 3 no son congruentes. Se sabe de hecho que 5, 6 y 7 son los números conguentes más pequeños.

2.5. Ecuación cúbica

En la demostración de la Proposición 1, llegamos a las ecuaciones

$$\left(\frac{(X \pm Y)}{2}\right)^2 = \left(\frac{Z}{2}\right)^2 \pm n$$

siempre que X, Y, Z sean los lados de un triángulo con área n. Si multiplicamos estas dos ecuaciones, obtenemos

$$\left(\frac{(X^2 - Y^2)}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2.$$

Esto muestra que la ecuación

$$u^4 - n^2 = v^2$$

tiene una solución racional con

$$u = \frac{Z}{2} \text{ y } v = \frac{(X^2 - Y^2)}{4}.$$

Luego multiplicamos por u^2 para obtener

$$u^6 - n^2u^2 = (uv)^2.$$

Si establecemos

$$x = u^2 = \left(\frac{Z}{2}\right)^2$$

obtenemos el mismo x que en la Proposición 1, y establecemos

$$y = uv = \frac{(X^2 - Y^2)Z}{8}$$

entonces tenemos un par de números racionales (x, y) que satisfacen la ecuación cúbica:

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

En resumen, dado un triángulo rectángulo con lados racionales X, Y, Z y área n, obtenemos un punto (x, y) en el plano xy con coordenadas racionales y que yace en la curva

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

Por lo tanto, que un entero positivo n sea congruente o no, que está relacionado con la solubilidad de las ecuaciones $a^2 + b^2 = c^2$ y $\frac{ab}{2} = n$ con $a, b, c \in \mathbb{Q}$, se puede reinterpretar en términos de la solubilidad de la ecuación cúbica $y^2 = x^3 - n^2x$ sobre los racionales.

Esta ecuación tiene tres soluciones racionales obvias: $(0,0)$, $(n,0)$, y $(-n,0)$. Sin embargo, nos interesan las soluciones con $y \neq 0$.

Teorema 2.2. *Sea n un número entero positivo. Existe una correspondencia uno a uno entre los dos conjuntos siguientes:*

$$\{(a,b,c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2, \frac{ab}{2} = n\}, \quad \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2x, y \neq 0\}.$$

Las correspondencias mutuamente inversas entre estos conjuntos son:

$$(a,b,c) \overset{f}{\mapsto} \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \quad (x,y) \overset{g}{\mapsto} \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

Demostración. Para demostrar que la correspondencia es biyectiva, veremos que f y g están bien definidas, que f es inyectiva y que g es la inversa de f.

Primero vamos a comprobar que los puntos en la imagen de f cumplen $y^2 = x^3 - n^2x$, $y \neq 0$. Para ello, dados (a,b,c) que cumplen $a^2+b^2=c^2$, $\frac{ab}{2}=n$ vemos que si

$$f(a,b,c) = (x,y) = \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right),$$

entonces, $y \neq 0$ dado que $n > 0$. Además, observamos que el denominador $c-a$ no se anula. Esto se cumple porque c representa la hipotenusa de un triángulo y a el cateto del mismo triángulo. Por eso, si tuvieramos $c = a$ sustituyéndolo en la condición $a^2+b^2=a^2$ obtenemos que $b=0$ y entonces $\frac{a0}{2}=0=n$ y esto es contradictorio.

A continuación, comprobamos que se cumple la condicíon $y^2 = x^3 - n^2x$. Por un lado,

$$x^3 - n^2x = \frac{n^3b^3}{(c-a)^3} - \frac{n^3b}{c-a} = \frac{n^3b^3 - n^3b(c-a)^2}{(c-a)^3}$$

Simplificamos la fracción:

$$x^3 - n^2x = \frac{n^3(b^3 - b(c^2-2ca+a^2))}{(c-a)^3} = \frac{n^3(b^3 - bc^2 + 2bca - ba^2)}{(c-a)^3}$$

Sustituimos $c^2 = a^2+b^2$:

$$x^3 - n^2x = \frac{n^3(b^3 - b(a^2+b^2) + 2bca - ba^2)}{(c-a)^3} = \frac{n^3(b^3 - ba^2 - b^3 + 2bca - ba^2)}{(c-a)^3}$$

$$= \frac{n^3(-2ba^2+2bca)}{(c-a)^3} = \frac{2n^3ba(c-a)}{(c-a)^3} = \frac{2n^3ba}{(c-a)^2}$$

Dado que $ab = 2n$:

$$x^3 - n^2x = \frac{4n^4}{(c-a)^2} = \left(\frac{2n^2}{(c-a)}\right)^2 = y^2.$$

Lo que demuestra que se cumple la condición. Por lo tanto, queda demostrado que f está bien definida.

A continuación demostraremos que f es inyectiva. Supongamos que hay dos tríos (a_1,b_1,c_1) y (a_2,b_2,c_2) diferentes, cuya imagen por la correspondencia es igual:

$$\left(\frac{nb_1}{c_1-a_1}, \frac{2n^2}{c_1-a_1}\right) = \left(\frac{nb_2}{c_2-a_2}, \frac{2n^2}{c_2-a_2}\right)$$

Esto implica que:

$$\frac{nb_1}{c_1-a_1} = \frac{nb_2}{c_2-a_2} \quad \text{y} \quad \frac{2n^2}{c_1-a_1} = \frac{2n^2}{c_2-a_2}.$$

La segunda ecuación nos da $c_1 - a_1 = c_2 - a_2$. Luego, usando esta igualdad en la primera ecuación, obtenemos $b_1 = b_2$.

Dado que a_1,b_1,c_1 y a_2,b_2,c_2 deben satisfacer

$$a_1^2 + b_1^2 = c_1^2 \text{ y } a_2^2 + b_2^2 = c_2^2,$$

es necesario que $a_1 = a_2$ y $c_1 = c_2$. Por lo tanto,

$$(a_1,b_1,c_1) = (a_2,b_2,c_2),$$

lo que muestra que necesariamente las imagenes tiene que provenir de un trío idéntico, lo que verifica la inyectividad.

Continuamos comprobando que g está bien definida. Consideremos un par (x,y) tal que $y^2 = x^3 - n^2x$ y $y \neq 0$. Necesitamos verificar que la imagen por la correspondecia esté dentro del primer conjunto.

Para ello, vamos a comprobar que si tomamos:

$$a = \frac{x^2-n^2}{y}, \quad b = \frac{2nx}{y}, \quad c = \frac{x^2+n^2}{y}$$

satisfacen $a^2+b^2 = c^2$ y $(1/2)ab = n$.

Primero, verificamos que $a^2+b^2 = c^2$:

$$\begin{aligned} a^2+b^2 &= \left(\frac{x^2-n^2}{y}\right)^2 + \left(\frac{2nx}{y}\right)^2 = \frac{(x^2-n^2)^2+(2nx)^2}{y^2} = \frac{x^4-2n^2x^2+n^4+4n^2x^2}{y^2} \\ &= \frac{x^4+2n^2x^2+n^4}{y^2} = \frac{(x^2+n^2)^2}{y^2} = \left(\frac{x^2+n^2}{y}\right)^2 = c^2. \end{aligned}$$

Ahora, verificamos que $\frac{ab}{2} = n$:

$$\frac{ab}{2} = \frac{1}{2}\left(\frac{x^2-n^2}{y}\right)\left(\frac{2nx}{y}\right) = \frac{nx(x^2-n^2)}{y^2} = \frac{n(x^3-n^2x)}{y^2} = \frac{ny^2}{y^2} = n.$$

Por lo tanto, hemos mostrado que g está bien definida.

Para acabar, vamos a comprobar si $g = f^{-1}$. Para ello, comprobamos que $g \circ f = id$.

$$g(f(a,b,c)) = g\left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) = \left(\frac{\left(\frac{nb}{c-a}\right)^2 - n^2}{\frac{2n^2}{c-a}}, \frac{2n\frac{nb}{c-a}}{\frac{2n^2}{c-a}}, \frac{\left(\frac{nb}{c-a}\right)^2 + n^2}{\frac{2n^2}{c-a}}\right)$$

Desarrollando la primera coordenada, vemos que

$$\frac{\frac{n^2b^2-n^2(c-a)^2}{(c-a)^2}}{\frac{2n^2}{c-a}} = \frac{n^2b^2-n^2a^2-n^2b^2-n^2a^2+2n^2ca)}{2n^2(c-a)} = \frac{2n^2a(c-a)}{2n^2(c-a)} = a.$$

La segunda claramente se simplifica a b, mientras que para la tercera y última coordenada

$$\frac{\frac{n^2b^2+n^2(c-a)^2}{(c-a)^2}}{\frac{2n^2}{c-a}} = \frac{n^2b^2+n^2a^2+n^2b^2+n^2a^2-2n^2ca)}{2n^2(c-a)} = \frac{2n^2(b^2+a^2-ca)}{2n^2(c-a)} = \frac{2n^2c(c-a)}{2n^2(c-a)} = c.$$

Por lo tanto, queda demostrado que hay una correspondencia uno a uno entre los conjuntos dados. □

Capítulo 3

Curvas elípticas

Nuestro propósito es reformular el problema clásico inicial de los números congruentes. Para ello, en este capítulo se desarrolla la teoría necesaria sobre curvas elípticas viendo algunas nociones generales y algunos resultados concretos sobre la curva elíptica en función de n que hemos obtenido en el anterior capítulo.

3.1. Curvas elípticas

Introducimos en este apartado las definiciones generales necesarias para desarrollar el problema. Con ese próposito, se ha usado principalmente el segundo capítulo del libro *Elliptic Curves: Number Theory and Cryptography* de L. C. Washington [6].

Por conveniencia, en este trabajo tomaremos la siguiente definición de curva elíptica:

Definición. Sea K un cuerpo con característica distinta a 2 y 3. Una *curva elíptica* E definida sobre K es una curva algebraica plana dada por una ecuación de la forma

$$y^2 = x^3 + ax + b, \tag{3.1}$$

donde $a, b \in K$ tal que $4a^3 + 27b^2 \neq 0$.

La condición $4a^3 + 27b^2 \neq 0$ garantiza que la curva no será singular. La ecuación (3.1) se llama *ecuación de Weierstrass simplificada* o *forma normal de Weierstrass*. En general y sin restringir la característica del cuerpo K, la definición de curva elíptica puede darse mediante su forma más general llamada la forma generalizada de Weiestrass:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3.2}$$

donde ahora se requiere que los coeficientes $a_1, ..., a_6 \in K$ verifiquen

$$-b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0, \tag{3.3}$$

con

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

La condición (3.3) es la análoga a la condición $4a^3 + 27b^2 \neq 0$ en el caso de la forma normal de Weierstrass, y asegura en este caso que la curva plana definida por la ecuación (3.2) sea no singular.

Sin embargo, con la hipótesis $char(K) \neq 2, 3$ podemos realizar un cambio de variables adecuado que nos permite usar la forma reducida (3.1). El desarrollo de este cambio de variables puede encontrarse en la primera sección del Capítulo III del libro *The Arithmetic of Elliptic Curves* de J. H. Silverman [3].

Por otro lado, para poder definir una operación de grupo en la curva elíptica es conveniente introducir la proyectivización de dicha curva. Es decir, consideraremos la curva proyectiva plana dada por la homogeneización de la ecuación de Weierstrass simplificada (3.1). Para ello, recordaremos alguna definición útil para nuestro cometido.

Definición. Llamamos *grado total de un monomio* $x^i y^j$ a la suma de sus potencias $i+j$.

Definición. Llamamos *grado total de un polinomio* $f(x,y)$ al máximo grado total de los monomios que tienen coeficientes distintos de cero.

Por ello, si $f(x,y)$ tiene grado total n, definimos el polinomio *homogéneo* correspondiente $F(X,Y,Z)$ de tres variables como el que se obtiene multiplicando cada monomio $x^i y^i$ en $f(x,y)$ por Z^{n-i-j} para que su grado total en las variables X,Y,Z sea n. Es decir,

$$F(X,Y,Z) = Z^n f\left(\frac{X}{Z}, \frac{Y}{Z}\right)$$

En el caso de las curvas elípticas que nos concierne, partimos de una ecuación de la forma

$$f(x,y) = 0 \text{ con } f(x,y) = y^2 - (x^3 + ax + b).$$

Homogeneizando, obtenemos la ecuación $F(X,Y,Z) = 0$ con

$$F(X,Y,Z) = Y^2Z - (X^3 + aXZ^2 + bZ^3).$$

Nótese que $f(x,y) = F(x,y,1)$. De esta forma, las soluciones de la ecuación homogénea de la forma $(X,Y,1)$ recuperan las soluciones de la ecuación inicial.

Supongamos que nuestros polinomios tienen coeficientes en un cuerpo K, y que estamos interesados en tríos $X,Y,Z \in K$ tales que $F(X,Y,Z) = 0$. Entonces, debemos reparar en lo siguiente:

1. Para cualquier $\lambda \in K$ escalar, $F(\lambda X, \lambda Y, \lambda Z) = \lambda^n F(X,Y,Z)$, siendo n el grado total de F.
2. Para cualquier $\lambda \neq 0$ en K, $F(\lambda X, \lambda Y, \lambda Z) = 0$ si y solo si $F(X,Y,Z) = 0$.

En particular, para $Z \neq 0$ tenemos que $F(X,Y,Z) = 0$ si y solo si $F(X/Z, Y/Z, 1) = 0$.

Debido a el segundo punto (2), es natural considerar clases de equivalencia de tríos $X,Y,Z \in K$, donde decimos que dos tríos (X,Y,Z) y (X',Y',Z') son equivalentes si existe un $\lambda \neq 0 \in K$ tal que $(X',Y',Z') = \lambda(X,Y,Z)$. Omitimos el trío trivial $(0,0,0)$, y entonces, definimos el *plano proyectivo* $\mathbb{P}^2$ como el conjunto de todas las clases de equivalencia de tríos no triviales. Escribiremos las clases de equivalencia en el plano proyectivo con la notación $[X : Y : Z]$.

Retomando nuestro problema, la homogeneización de la forma normal de Weierstrass (3.1) nos proporciona la ecuación homogénea

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Observamos que partiendo de nuestro polinomio homegeneizado en el plano proyectivo, para recuperar (3.1) tenemos que dividir entre la variable Z. Esto nos dará problemas en la recta $Z = 0$ a la que llamamos recta del infinito. De hecho, esta es la recta que estamos ganando al pasar del plano afín al homegeneizar nuestro polinomio y verlo en el plano proyectivo. Si sustituímos $Z = 0$ en nuestra ecuación en el plano proyectivo, tenemos lo siguiente:

$$0 = X^3. \tag{3.4}$$

Es decir, que los puntos sobre la curva proyectiva que se encuentran en la recta del infinito $Z = 0$ son de la forma $(0,Y,0)$. Pero debido a la relación de equivalencia introducida anteriormente, tenemos que esos puntos representan en definitiva un único punto: $[0 : 1 : 0]$. Este punto, que es el único en el que la curva elíptica corta a la recta del infinito, tendrá un rol indispensable en la operación de grupo que definiremos más tarde.

Reparamos, además, en que este punto no depende de los coeficientes $a, b \in K$ concretos que definen la curva elíptica, lo que significa que llegaremos a él con este proceso independientemente de la elección concreta de nuestra curva elíptica. Teniendo esto en cuenta podemos dar la siguiente definición que incluye este punto.

Definición. Sean E una curva elíptica definida sobre un cuerpo K y K' una extesión de dicho cuerpo. Llamamos conjunto de puntos K'-racionales de E al conjunto

$$E(K') = \{(x,y) \in K' \times K' | y^2 = x^3 + ax + b\} \cup \{O_E = [0:1:0]\}.$$

Una característica del punto O_E que será indispensable para la ley de grupo es que corta a todas las rectas verticales. En el plano afín, una recta vertical se escribe como $x = c$ para alguna constante. Si homogeneizamos esta ecuación, tenemos que $X = Zc$. Si calculamos la intersección de esta recta (que proviene de una vertical en el plano afín) con la recta del infinito $Z = 0$ tenemos lo siguiente:

$$X = 0c = 0 \text{ y } Z = 0.$$

Por lo tanto, la intersección son los puntos de la forma $[0:Y:0]$, que como hemos explicado representan la clase de $O_E = [0:1:0]$. Nótese que este resultado es independiente de la constante c. Esto verifica que todas las rectas verticales del plano afín (o mejor dicho, sus proyectivizaciones) intersecan el punto O_E.

Además presentamos el siguiente teorema que se necesitará en la siguiente sección.

Teorema 3.1 (Bézout)**.** *Sean $F(X,Y,Z)$ y $G(X,Y,Z)$ polinomios homogéneos de grado m y n, respectivamente, sobre un cuerpo algebraicamente cerrado K. Supongamos que F y G no tienen ningún factor polinomial en común. Entonces, las curvas definidas por F y G tienen mn puntos de intersección, contando multiplicidades.*

Se encuentran más detalles sobre la multiplicidad de intersección y una prueba del teorema de Bézout, por ejemplo, en el libro de R. J. Walker *Algebraic Curves* [7].

3.2. Operación de grupo

En esta sección veremos que podemos definir una operación que llamaremos suma y representaremos como $+$, que dota a las curvas elípticas de una estructura de grupo (abeliano). Es decir, dados dos puntos P y Q en una curva elíptica E, definiremos cómo obtener un tercer punto en la curva, que denotaremos $P+Q$, y comprobaremos que la operación $(P,Q) \to P+Q$ es asociativa, que posee elemento identidad, que todo punto tiene un inverso y que es conmutativa.

Para la descripción del punto $P+Q$, daremos primero la idea geométrica detrás de la construcción y, a continuación, la manera explícita para obtenerlo mediante fórmulas.

Dados P y $Q \in E$, para calcular $P+Q$ se siguen dos pasos:

(1º) Trazamos la recta que pasa por P y Q. Gracias al Teorema de Bézout, como nuestra curva tiene grado 3 y la recta tiene grado 1, sabemos que su intersección contará con $3 \times 1 = 3$ puntos de intersección (contados con multiplicidad). Como P y Q ya están en la intersección de la curva y la recta, existirá un tercer punto R por el que la recta corta con la curva.

(2º) Trazamos la recta que une O_E con R. De esta manera obtendremos una recta que, de nuevo por el Teorema de Bézout, cortará a la curva elíptica en el punto del infinito O_E, en R y en un tercer punto que llamamos[1] $-R$. Dicho punto es por definición $P+Q$.

[1] El motivo de denotar por $-R$ a este punto es que, como veremos más adelante, se trata precisamente del inverso de R. Así, la relación entre P, Q y R es de hecho $P+Q+R = O_E$.

Para que esta construcción tenga consistencia, tenemos que reparar en que si $P = Q$ tenemos que 'la recta que pasa por P y Q' será *la recta tangente* a la curva elíptica en P. De este modo, si dicha recta tangente corta a la curva elíptica en otro punto (distinto) R, obtendremos $-R$ como se explica en el segundo paso y ese será el resultado de hacer $P+P$. Si por el contrario la recta tangente a P no corta a la curva en otro punto del plano afín, entonces dicha recta es vertical, con lo cual el tercer punto en la intersección con la curva elíptica que garantiza el Teorema de Bézout es el punto del infinito O_E. En este caso, el segundo paso requiere trazar la recta *tangente* por O_E. Dicha recta es la recta del infinito $Z = 0$, y como hemos observado en la sección anterior su intersección con la curva elíptica es (3.4), que nos muestra que $Z = 0$ corta la curva elíptica en O_E con multiplicidad 3. Es decir, el punto $-O_E$ que obtendríamos en el segundo paso es de nuevo O_E, concluyendo así que en este caso $P+P = O_E$.

Para completar la definición de la operación vamos a explicar qué ocurre cuando alguno de los puntos P, Q es O_E.

- Si $P = (x,y)$ es un punto afín de E y $Q = O_E$, cuando trazamos la recta que pasa por P y O_E obtenemos una recta vertical, que cortará a la curva en el punto $-P = (x,-y)$. Al ejecutar el segundo paso, observemos que se vuelve a tomar la misma recta, recuperando el punto $P = (x,y)$ de nuevo:
$$P + O_E = P.$$
Esto nos verifica que O_E tendrá el papel de elemento neutro en la suma (a falta de verificar que ocurre lo mismo para $P = O_E$, que se verá justo a continuación). El argumento con $P = O_E$ y $Q \neq O_E$ es análogo por simetría.
- Si $P = Q = O_E$, la recta tangente a O_E corta por tercera vez en el mismo punto O_E, como ya hemos observado antes. De nuevo, al realizar en el segundo paso la recta tangente por O_E el tercer punto de intersección es O_E. Por lo tanto:
$$O_E + O_E = O_E.$$

Con esta idea geométrica de la suma podemos calcular las ecuaciones de las rectas y las intersecciones con la curva para obtener una fórmula generalizada que involucra únicamente las coordenadas de los puntos. Para retomar toda la casuística, resumimos la ley de grupo

$$(P,Q) \longmapsto P+Q$$

de la siguiente forma:

(1) En caso de que uno de los puntos P,Q sea el punto del infinito, sin perderder generalidad escogemos $P = O_E$; entonces
$$P + Q = Q.$$

(2) Si P, $Q \neq O_E$, $P = (x,y)$ y $Q = -P = (x,-y)$, entonces
$$P + Q = O_E.$$

(3) Si $P,Q \neq O_E$ y $Q \neq -P$, entonces podemos escribir la operación con coordenadas afines. Tomando
$$P = (x_1,y_1) \text{ y } Q = (x_2,y_2),$$
el resultado de la suma
$$P + Q = (x_1,y_1) + (x_2,y_2) =: (x_3,y_3)$$
se puede obtener mediante la resolución de intersecciones entre la ecuación cúbica y las rectas correspondientes, obteniendo
$$x_3 = s^2 - x_1 - x_2, \qquad y_3 = s(x_1 - x_3) - y_1,$$
donde
$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} & \text{si } P = Q. \end{cases}$$

Teorema 3.2. *La suma de puntos en una curva elíptica E satisface las siguientes propiedades:*

1. *(Conmutatividad) $P+Q=Q+P$ para todos los puntos $P,Q\in E$.*
2. *(Existencia de la identidad) $P+O_E=P$ para todos los puntos $P\in E$.*
3. *(Existencia de inversos) Dado P en E, existe P' en E tal que $P+P'=O_E$. Anteriormente nos hemos referido a P' como $-P$.*
4. *(Asociatividad) $(P+Q)+R=P+(Q+R)$ para todos los $P,Q,R\in E$.*

En otras palabras, los puntos en E forman un grupo abeliano aditivo con O_E como el elemento identidad.

Demostración. La conmutatividad es obvia, ya sea desde las fórmulas o desde el hecho de que la recta que pasa por P y Q es obviamente la misma que la recta que pasa por Q y P. El hecho que O_E actúa como elemento identidad ya se ha visto en la descripción de la operación $+$. La existencia de inversos también se ha visto en la discusión anterior; simplemente notar que si $P\neq O_E$, entonces $-P$ es la reflexión de P a través del eje x. Finalmente, quedará por demostrar la asociatividad. Esta es, con diferencia, la propiedad más sutil y no evidente a partir de la definición de la suma en E. Es posible definir muchas leyes de composición que satisfagan las tres primeras condiciones para puntos en E, ya sean más simples o más complicadas que la que se ha descrito. Pero es muy improbable que tal ley sea asociativa. De hecho, es bastante sorprendente que la ley de composición que hemos definido lo sea. Después de todo, comenzamos con dos puntos P y Q y realizamos un cierto procedimiento para obtener un tercer punto $P+Q$. Luego repetimos el procedimiento con $P+Q$ y R para obtener $(P+Q)+R$. Si en cambio comenzamos agregando Q y R, luego calculamos $P+(Q+R)$, no parece haber una razón obvia para que esto dé el mismo punto que el otro cálculo. Esta demostración se puede encontrar en el capítulo II, sección 2.4 del libro *Elliptic Curves: Number Theory and Cryptography* de L. C. Washington [6]. □

3.3. Curvas elípticas sobre $\mathbb{C}$

Más adelante en el trabajo veremos que existe una relación estrecha entre los números congruentes y los puntos de orden infinito. Para decidir si hay tales puntos, es útil entender los puntos m-torsión que se introducirán en la siguiente sección. A su vez, para poder entender mejor los puntos de orden finito es útil ver nuestra curva elíptica que está en principio definida en $\mathbb{Q}$, definida en $\mathbb{C}$. Para eso, introducimos curvas elípticas sobre los complejos. En este apartado se ha usado de referencia principal el Capítulo I del libro *Introduction to Elliptic Curves and Modular Forms* de Koblitz [1] y las notas del curso de A. Sutherland [5], que utilizan las secciones 2 y 3 del Capítulo VI del libro *The Arithmetic of Elliptic Curves* de Silverman [3].

Definición. Sean $\omega_1,\omega_2\in\mathbb{C}$ dos números complejos que no están en la misma recta que pasa por el origen. Llamamos *retículo* al conjunto de todas las combinaciones lineales *enteras* de ω_1 y ω_2, y lo denotamos $L=[\omega_1,\omega_2]$. Es decir,

$$L=[\omega_1,\omega_2]:=\{m\omega_1+n\omega_2 : m,n\in\mathbb{Z}\}\subset\mathbb{C}.$$

Por ejemplo, si $\omega_1=i$ y $\omega_2=1$, obtenemos el retículo de los enteros gaussianos,

$$\mathbb{Z}[i]=\{m+ni : m,n\in\mathbb{Z}\}.$$

Definición. Llamamos *paralelogramo fundamental* para ω_1 y ω_2 a cualquier subconjunto de $\mathbb{C}$ de la forma

$$\Pi_\alpha=\{\alpha+a\omega_1+b\omega_2 : a,b\in\mathbb{R},\,0\leq a,b\leq 1\},\qquad \alpha\in\mathbb{C}.$$

Nos limitaremos a $\Pi = \Pi_0$ (es decir, $\alpha = 0$) ya que el resto serán traslaciones de éste.

Dado que ω_1 y ω_2 forman una $\mathbb{R}$-base para $\mathbb{C}$, cualquier número $x \in \mathbb{C}$ se puede escribir en la forma $x = a\omega_1 + b\omega_2$ para algunos $a, b \in \mathbb{R}$. Entonces, x se puede escribir como la suma de un elemento en el retículo $L = [\omega_1, \omega_2]$ y un elemento en Π, y esta representación es única a menos que a o b sean enteros, en cuyo caso el elemento de Π está en la frontera de Π.

Elegimos por convenio tomar ω_1 y ω_2 en orden de las agujas del reloj; es decir, asumiremos que ω_1/ω_1 tiene la parte imaginaria positiva.

Introducimos definiciones sobre análisis complejo que se utilizarán más adelante.

Definición. Dado un retículo L, decimos que una función meromorfa $f(z)$ en $\mathbb{C}$ es una *función elíptica* de L si $f(z+l) = f(z)$ para todo $l \in L$. Llamamos al conjunto de estas funciones elípticas $\mathscr{E}_L$.

Si $L = [\omega_1, \omega_2]$, basta con verificar esta propiedad para $l = \omega_1$ y $l = \omega_2$. En otras palabras, una función elíptica es periódica con dos períodos ω_1 y ω_2. Tal función está determinada por sus valores en el paralelogramo fundamental Π, y sus valores en puntos opuestos de la frontera de Π son iguales, es decir:

$$f(a\omega_1 + \omega_2) = f(a\omega_1), \quad f(\omega_1 + b\omega_2) = f(b\omega_2), \qquad \forall a, b \in \mathbb{R}, 0 \leq a, b \leq 1.$$

Así, se puede pensar una función elíptica $f(z)$ como una función en el conjunto Π con lados opuestos pegados entre sí; es decir, como una función en el cociente $\mathbb{C}/L$. Nótese que, por construcción, este conjunto es un *toro complejo*.

A continuación, damos una definición relacionada con las funciones complejas meromorfas que utilizaremos más adelante.

Definición. Sea $f(z)$ una función compleja no nula que es meromorfa en un entorno abierto de un punto $z_0 \in \mathbb{C}$. Definimos

$$\operatorname{ord}_{z_0}(f) := \begin{cases} n & \text{si } f \text{ tiene un cero de orden } n \text{ en } z_0, \\ -n & \text{si } f \text{ tiene un polo de orden } n \text{ en } z_0, \\ 0 & \text{en otro caso.} \end{cases}$$

Definimos lo que será un ejemplo clave de una función elíptica en relación con un retículo $L = [\omega_1, \omega_2]$. Dicha función se llama *función de Weierstrass* $\wp$, y se denota $\wp(z; L)$ o $\wp(z; \omega_1, \omega_2)$, o simplemente $\wp(z)$ si el retículo es conocido. Se define como sigue:

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{\substack{l \in L \\ l \neq 0}} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right). \tag{3.5}$$

Presentamos a continuación resultados sobre la función (3.5) que se demuestran en la sección 4 del Capítulo I del libro *Introduction to Elliptic Curves and Modular Forms* de Koblitz mencionado antes [1].

Proposición 2. *La suma* (3.5) *converge absoluta y uniformemente para z en cualquier subconjunto compacto de $\mathbb{C} - L$.*

Proposición 3. *$\wp(z) \in \mathscr{E}_L$ y sus únicos polos son polos dobles en cada punto del retículo.*

Presentamos también su derivada, que tendrá un papel fundamental a continuación:

$$\wp'(z) = -2 \sum_{\substack{l \in L \\ l \neq 0}} \frac{1}{(z-l)^3}.$$

La función $\wp$ cumple una ecuación diferencial con dos constantes que se obtienen mediante las llamadas series de Eisenstein. Por ello, vemos la definición de estas series:

Definición. Sea L un retículo en $\mathbb{C}$ y $k > 2$ un entero. La *serie de Eisenstein* de peso k para L se define como la suma

$$G_k(L) = \sum_{\omega \in L^*} \frac{1}{\omega^k},$$

donde $L^* = L - \{0\}$.

Observación. Si k es impar, entonces $G_k(L) = 0$ para cualquier retículo L, ya que los términos $\frac{1}{\omega^k}$ y $\frac{1}{(-\omega)^k}$ en la suma se cancelan.

Lema 1. *Para cualquier retículo L, la suma* $\sum_{\omega \in L^*} \frac{1}{\omega^k}$ *converge absolutamente para todo* $k > 2$.

Teniendo en mente las definiciones y propiedades que acabamos de presentar, podemos enunciar el teorema que relaciona la función (3.5) con una ecuación cúbica.

Teorema 3.3. *La función* $\wp(z) = \wp(z;L)$ *satisface la ecuación diferencial*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$

donde

$$g_2(L) := 60G_4(L), \quad g_3(L) := 140G_6(L). \tag{3.6}$$

Además, con $y = \wp'(z)$ y $x = \wp(z)$, observamos que la ecuación diferencial anterior nos recuerda a la forma de ecuación de Weierstrass simplificada de una curva elíptica:

$$y^2 = 4x^3 - g_2(L)x - g_3(L). \tag{3.7}$$

En efecto, esta ecuación puede ser puesta en forma de Weierstrass escribiendo $g_2(L) = -4A$ y $g_3(L) = -4B$, así que cada retículo L nos da una ecuación que podemos usar para definir una curva elíptica sobre $\mathbb{C}$, siempre y cuando podamos demostrar que la curva proyectiva definida por (3.7) no es singular.

Para comprobar que no sea singular vemos que basta comprobar la condición de que $(g_2)^3(L) - 27(g_3)^2 \neq 0$. Así que mientras $\Delta(L) := g_2(L)^3 - 27g_3(L)^2$ sea distinto de cero, la ecuación (3.7) define una curva elíptica sobre $\mathbb{C}$.

Para poder demostrar que dicho discriminante es no nulo, debemos introducir algunos resultados sobre análisis complejo. Comenzamos recordando la fórmula del residuo ya vista y conocida ampliamente, cuya demostración no se da por ese motivo.

Teorema 3.4 (Fórmula del residuo)**.** *Sea* γ *una curva cerrada simple con orientación positiva y sea* $f(z)$ *una función que es meromorfa en un conjunto abierto que contiene a* γ *y su interior sin polos en* γ*. Sean* $z_1, \ldots, z_N$ *los polos de* $f(z)$ *que se encuentran en el interior de* γ*. Entonces*

$$\oint_\gamma f(z)\,dz = 2\pi i \sum_{k=1}^{N} \operatorname{res}_{z_k}(f).$$

Utilizando la fórmula del residuo probamos el siguiente resultado:

Teorema 3.5. *Sea* γ *una curva cerrada simple con orientación positiva, sea* $f(z)$ *una función meromorfa en un conjunto abierto* Ω *que contiene a* γ *y su interior* Γ*, sin ceros ni polos en* γ*, y sea* $g(z)$ *una función no nula que es holomorfa en* Ω*.*

$$\frac{1}{2\pi i}\int_\gamma g(z)\frac{f'(z)}{f(z)}\,dz = \sum_{w \in \Gamma} g(w)ord_w(f).$$

Cuando $g(z) = 1$*, el lado derecho es la diferencia entre el número de ceros y polos que* $f(z)$ *tiene en* Γ *(contados con multiplicidad), lo cual es el principio del argumento usual.*

Demostración. Para cualquier $z_0 \in \Gamma$ que sea un cero o un polo de $f(z)$, consideramos las expansiones en series de Laurent

$$f(z) = \sum_{n \geq n_0} a_n (z - z_0)^n, \quad g(z) = \sum_{n \geq 0} b_n (z - z_0)^n,$$

donde $n_0 = \text{ord}_{z_0}(f)$ es elegido de modo que $a_{n_0} \neq 0$ y notamos que $g(z_0) = b_0$. Entonces

$$f'(z) = \sum_{n \geq n_0} n a_n (z - z_0)^{n-1},$$

y tenemos

$$\frac{f'(z)}{f(z)} = \frac{n_0 (z - z_0)^{-1} + h_1(z)}{g(z)\frac{f'(z)}{f(z)}} = b_0 n_0 (z - z_0)^{-1} + h_2(z),$$

donde $h_1(z)$ y $h_2(z)$ denotan funciones que son holomorfas en un entorno abierto de z_0. Así,

$$g(z)\frac{f'(z)}{f(z)}$$

tiene un simple polo con residuo

$$b_0 n_0 = g(z_0)\text{ord}_{z_0}(f)$$

en cada cero o polo z_0 de $f(z)$, y en ningún otro lugar. El teorema sigue de la fórmula del residuo. □

Aplicando el Teorema 3.5 con $g(z) = 1$ a una función elíptica $f(z)$ se obtiene lo siguiente.

Teorema 3.6. *Sea $f(z)$ una función elíptica no nula para un retículo L. Contando con multiplicidad, el número de ceros de $f(z)$ en cualquier paralelogramo fundamental Π_α para L es igual al número de polos de $f(z)$ en Π_α.*

Demostración. Primero notamos que, debido a la periodicidad de $f(z)$, es suficiente probar esto para cualquier paralelogramo fundamental Π_α. Los ceros y polos de $f(z)$ son discretos (nótese que $1/f(z)$ también es una función meromorfa), por lo que podemos elegir un α para el cual el contorno ∂ de Π_α no contenga ningún cero o polo de $f(z)$. Ahora consideramos la integral de contorno

$$\oint_{\partial \Pi_\alpha} \frac{f'(z)}{f(z)} dz,$$

donde la curva cerrada simple $\partial\Pi_\alpha$ está orientada positivamente. El hecho de que $f(z)$ sea periódica con respecto a L implica que $f'(z)$ también es periódica con respecto a L, al igual que $f'(z)/f(z)$, y de ello se deduce que la suma de la integral de $f'(z)/f(z)\,dz$ a lo largo de lados opuestos del paralelogramo $\partial\Pi_\alpha$ es cero, ya que $f'(z)/f(z)$ toma los mismos valores en ambos lados (debido a que es periódica) pero la curva orientada $\partial\Pi\alpha$ los recorre en direcciones opuestas. Tenemos así

$$\frac{1}{2\pi i} \oint_{\partial \Pi_\alpha} \frac{f'(z)}{f(z)} dz = 0,$$

y el teorema se deduce entonces del Teorema 3.5. □

Finalmente, el último lema necesario para lograr demostrar que el discriminante es diferente de 0 es el siguiente:

Lema 2. *Un punto $z \notin L$ es una raíz de $\wp'(z;L)$ si y solo si $2z \in L$.*

Demostración. Supongamos que $2z \in L$ para algún $z \notin L$. Entonces

$$\wp'(z) = \wp'(z - 2z) = \wp'(-z) = -\wp'(z) = 0,$$

donde hemos usado el hecho de que $\wp'(z)$ es tanto periódica con respecto a L como una función impar. Si $L = [\omega_1, \omega_2]$, entonces

$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2}, \quad \frac{\omega_1 + \omega_2}{2}$$

son los únicos puntos $z \in \Pi$ que no están en L y también satisfacen $2z \in L$. Dado que $\wp'(z)$ es una función elíptica de orden 3, tiene sólo estos tres ceros en Π, según el Teorema (3.6). Por lo tanto, para cualquier $z \notin L$ tenemos que $\wp'(z) = 0$ si y sólo si $2z \in L$. □

En términos de la operación de grupo en la curva elíptica, este lema nos dice que los puntos de orden 2 son precisamente los puntos de la forma $(x,y) = (\wp(z), \wp'(z))$ con $y = \wp'(z) = 0$. La condición de que $z \notin L$ significa que su clase no es trivial en $\mathbb{C}/L$.

Teorema 3.7. *Para cualquier retículo L, el discriminante* $\Delta(L)$ *es distinto de cero.*

Demostración. Sea $L = [\omega_1, \omega_2]$ y pongamos

$$r_1 := \frac{\omega_1}{2}, \quad r_2 := \frac{\omega_2}{2}, \quad r_3 := \frac{\omega_1 + \omega_2}{2}.$$

Entonces $r_i \notin L$ y $2r_i \in L$ para $i = 1,2,3$. Entonces $\wp'(r_i) = 0$ por el Lema 2. De (3.7) vemos que $\wp(r_1), \wp(r_2)$ y $\wp(r_3)$ son las raíces del cúbico $f(x) = 4x^3 - g_2(L)x - g_3(L)$. Ahora, el discriminante $\Delta(f)$ de $f(x)$ es igual a $16\Delta(L)$, por lo tanto

$$\Delta(L) = \frac{1}{16} \prod_{i<j} (\wp(r_i) - \wp(r_j))^2,$$

y es suficiente demostrar que los $\wp(r_i)$ son distintos.

Sea $g_i(z) = \wp(z) - \wp(r_i)$. Entonces $g_i(z)$ es una función elíptica de orden 2 (sus polos son los polos de $\wp(z)$), por lo que tiene exactamente 2 ceros, según el Teorema 3.6. Ahora r_i es un cero doble porque $g_i'(z) = \wp'(r_i) = 0$, por el Lema 2. Por lo tanto $g_i(z)$ no tiene otros ceros, y por lo tanto $\wp(r_j) \neq \wp(r_i)$ para $i \neq j$. □

En conclusión, este resultado nos demuestra que cada retículo del plano complejo L tiene asociada una curva elíptica. Observamos esta relación mediante la siguiente parametrización:

$$\phi : \mathbb{C} \longrightarrow E_L(\mathbb{C}) \tag{3.8}$$

$$z \longmapsto \phi(z) = \begin{cases} [\wp(z) : \wp'(z) : 1] & \text{si } z \notin L \\ [0:1:0] = O_E & \text{si } z \in L \end{cases} \tag{3.9}$$

Para poder comprender mejor cómo funciona esta parametrización presentamos un ejemplo de otra parametrización (más sencilla y conocida) con el que poder hacer un paralelismo. Considerando $\mathbb{R}$ como grupo abeliano (con la suma), $\mathbb{Z} \subset \mathbb{R}$ es un subgrupo y podemos formar el grupo cociente

$$\mathbb{R}/\mathbb{Z} = \{x + \mathbb{Z} : x \in \mathbb{R}\} = \{x + n : n \in \mathbb{Z}\}.$$

Notemos que $\mathbb{Z}$ es el núcleo del homomorfismo de grupos

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{C} \\ x &\longmapsto f(x) = e^{2\pi i x} \end{aligned}$$

y por tanto, por el Primer Teorema de Isomorfía tenemos que

$$\mathbb{R}/\mathbb{Z} \cong Imf = \mathbb{S}^1.$$

En consecuencia, conseguimos una parametrización del círculo unidad a través de $\mathbb{R}/\mathbb{Z}$. Además, observamos que el subgrupo por el que cocientamos es precisamente el subgrupo que consiste de los períodos de las funciones (reales) que proporcionan la parametrización:

$$\begin{aligned} \mathbb{R}/\mathbb{Z} &\longrightarrow \mathbb{S}^1 \subset \mathbb{C} \cong \mathbb{R}^2 \\ t &\longmapsto e^{2\pi it} \mapsto (x,y) = (cos(2\pi t), sen(2\pi t)). \end{aligned}$$

De manera similar a lo que ocurre en este ejemplo, las funciones $\wp$ y $\wp'$ proporcionan una parametrización (compleja) de la curva elíptica sobre $\mathbb{C}$ asociada a un retículo L, que hemos denotado $E_L(\mathbb{C})$. Esto nos explica la relación estrecha que hay entre las curvas elípticas sobre $\mathbb{C}$ y las funciones de Weierstrass asociadas a retículos.

En particular, $E_L(\mathbb{C})$ puede ser visto como curva algebraica y como grupo abeliano. La función dada en (3.8) es un homomorfismo de grupos cuyo núcleo es L. Por lo tanto, por el Primer Teorema de Isomorfía tenemos que

$$\mathbb{C}/L \cong E_L(\mathbb{C}).$$

En particular, la suma en la curva elíptica $E_L(\mathbb{C})$ se corresponde a través de este isomorfismo con la suma habitual en $\mathbb{C}$. Como en ejemplo anterior, nótese que el subgrupo por el que hemos concientado es de nuevo el periodo de la función. De hecho, puede probarse que el isomorfismo anterior es un isomorfismo de curvas algebraicas (cosa que queda fuera del alcance de este trabajo).

Además, dada E una curva elíptica sobre $\mathbb{C}$ se puede demostrar que existe un retículo L tal que $E_L \cong E$. No entraremos en esta demostración porque requiere técnicas y resultados que se escapan del alcance de este trabajo. El desarrollo de este resultado está en el Capítulo V de *Advanced Topics in the Arithmetic of Elliptic Curves* de Silverman [4].

3.4. Puntos de orden finito

En cualquier grupo, hay una distinción básica entre elementos de orden finito y elementos de orden infinito. En un grupo abeliano, el conjunto de elementos de orden finito forma un subgrupo llamado *subgrupo de torsión*. Para el desarrollo de ésta sección se utiliza el Capítulo I de *Introduction to Elliptic Curves and Modular Forms* de Koblitz [1].

Definición. Sea E una curva elíptica definida sobre un cuerpo K de característica distinta a 2 y 3. Si K' es una extensión de K, llamamos *subgrupo de torsión* (de $E(K')$) al siguiente conjunto:

$$E(K')_{\text{tors}} = \{P \in E(K') : mP = O_E \text{ para algún } m \geq 1\}.$$

Es inmediato comprobar que efectivamente $E(K')_{\text{tors}}$ es un *subgrupo* de $E(K')$. Es útil también introducir la noción del conjunto de puntos en la clausura algebraica de K de orden divisor de m, llamados *subgrupos de m-torsión*.

Definición. Con las condiciones de la definición anterior, sea m un entero positivo. Llamamos *subgrupo de m-torsión* al siguiente conjunto,

$$E[m] = \{P \in E(\bar{K}) \mid mP = O_E\}.$$

Observamos que existe una relación estrecha entre estos subgrupos. Sin ir más lejos tenemos que:

$$E(\bar{K})_{\text{tors}} = \bigcup_{m \geq 1} E[m].$$

Por lo tanto, para conocer el subgrupo de torsión debemos conocer cada uno de los subgrupos de m-torsión. A continuación, vamos a familiarizarnos con los ejemplos concretos de $m = 2, 3$, ya que son

sencillos de calcular, y posteriormente veremos un resultado general. Como la característica del cuerpo no es 2, $E[2]$ se obtiene de la siguiente manera. Supongamos que la ecuación de E puede escribirse como $y^2 = (x-e_1)(x-e_2)(x-e_3)$, con $e_1, e_2, e_3 \in \bar{K}$, la clausura algebraica de K. Un punto P satisface $2P = O_E$ si y solo si la recta tangente en P es vertical. Esto significa que $y = 0$, así que $E[2] = \{O_E, (e_1,0), (e_2,0), (e_3,0)\}$. Como grupo abstracto, es isomorfo a $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Ahora veamos $E[3]$. De nuevo, como se ha visto en la primera sección, tenemos que la ecuación puede darse como $y^2 = x^3 + ax + b$ gracias a la hipótesis sobre la característica. Por eso, un punto P satisface $3P = O_E$ si y solo si $2P = P + P = -P$. Esto significa que la coordenada x de $2P$ es igual a la coordenada x de P (las coordenadas y, por supuesto, difieren en signo; por supuesto, si fueran iguales, entonces $2P = P$, por lo tanto, $P = O_E$). Cuando introducimos la anterior igualdad en las fórmulas dadas para el cálculo de la suma, obtenemos una ecuación de grado 4 para la coordenada x, por lo que concluimos que hay 4 valores distintos de $x \in \bar{K}$, y cada x produce dos valores de y, por lo que tenemos ocho puntos de orden 3. Dado que O_E también está en $E[3]$, vemos que $E[3]$ es un grupo de orden 9 en el que cada elemento es de orden 3. Se cumple por lo tanto que $E[3]$ es $\mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Para estudiar el caso de un m arbitrario, nos limitamos al caso en que E está definida sobre $\mathbb{Q}$. Viendo la curva elíptica sobre los complejos, por el apartado anterior sabemos que $E(\mathbb{C})$ es isomorfo a $\mathbb{C}/L$ para algún retículo $L = [\omega_1, \omega_2]$. Con esto, a través del isomorfismo (3.8), un punto $P_z = \phi(z) \in E(\mathbb{C})$ tiene orden divisor de m si y solo si $mz \in L$. Notemos que si $z \in \mathbb{C}$, existen dos números reales $x, y \in \mathbb{R}$ tales que $z = x\omega_1 + y\omega_2$. Por lo tanto, la condición de que $mz = mx\omega_1 + my\omega_2 \in L$ es equivalente a que los coeficientes sean enteros, es decir, $mx, my \in \mathbb{Z}$. En ese caso, el menor m para el cual se cumpla la condición, que será concretamente el mínimo común denominador de los coeficientes de ω_1 y ω_2, es el orden exacto de P_z. Por lo tanto, esto se cumplirá si $x, y \in \frac{1}{m}\mathbb{Z} \subset \mathbb{Q}$. Este argumento muestra que

$$E[m](\mathbb{C}) \cong \mathbb{Z}_m \oplus \mathbb{Z}_m.$$

Sobre $\mathbb{Q}$, podemos deducir el siguiente resultado:

Teorema 3.8. *Sea E una curva elíptica sobre $\mathbb{Q}$. Dado un número entero positivo m cualquiera,*

$$E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m.$$

Demostración. Como $\mathbb{Q} \subset \mathbb{C}$, podemos ver la curva elíptica dada E como una curva definida sobre $\mathbb{C}$. Por lo que hemos visto en el apartado anterior, tenemos que

$$E[m](\mathbb{C}) \cong \mathbb{Z}_m \oplus \mathbb{Z}_m.$$

Además por la definición que hemos dado,

$$E[m] = E[m](\bar{\mathbb{Q}}) = \{P \in E(\bar{\mathbb{Q}}) \mid mP = O_E\}$$

Como $\bar{\mathbb{Q}} \subset \mathbb{C}$ tenemos que $E[m] \subset E[m](\mathbb{C})$. Pero cualquier $P = (x,y) \in E[m](\mathbb{C})$ cumple la ecuación $mP = O_E$. Si reparamos en las fórmulas dadas para el cálculo de la suma en la curva elíptica, vemos que todos los coeficientes de la ecuación $mP = O_E$ están en $\mathbb{Q}$ porque la curva elíptica está definida sobre $\mathbb{Q}$. Por lo tanto, las soluciones tendrán coordenadas algebraicas, por lo que se concluye que $P \in E(\bar{\mathbb{Q}})$. Por lo tanto, $E[m](\bar{\mathbb{Q}}) = E[m](\mathbb{C}) \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$. □

De este resultado obtenemos que los puntos del grupo de m-torsión en los que estamos interesados, que son los racionales, tendrán que ser un subgrupo de los puntos en la clausura algebraica, lo que nos deja con que:

$$E[m](\mathbb{Q}) \leq E[m](\bar{\mathbb{Q}}) = \mathbb{Z}_m \oplus \mathbb{Z}_m$$

A continuación, vamos a ver un resultado que nos muestra cuál será la cardinalidad de los subgrupos de torsión (con coordenadas en $\mathbb{Q}$) de las curvas elípticas de nuestro problema principal $E_n : y^2 = x^3 - n^2x$. Para comenzar, necesitamos dos resultados que luego se usarán en la demostración del teorema sobre esa cardinalidad.

Teorema 3.9 (Dirichlet)**.** *Sean q y ℓ dos números enteros positivos coprimos. Entonces hay infinitos números primos de la forma $\ell + kq$ con $k \in \mathbb{Z}$.*

La demostración de este teorema requiere la introducción de herramientas y conceptos que se escapan del objetivo de este trabajo. El desarrollo completo de su demostración puede encontrarse en los libros *Algebraic Number Theory* de Neukirch [8] y en *A Course in Arithmetic* de Serre [9].

A continuación, tras haber estudiado las posibles formas que tiene $E[m]$ y particularmente el subgrupo de 2-torsión, tenemos como objetivo demostrar que $E_n(\mathbb{Q})_{tors}$ contiene solamente esos 4 puntos obvios. Para ello, emplearemos la reducción módulo p de la ecuación, notando que exceptuando el caso $p = 2$ y los casos en que $p \mid n$, dicha reducción proporciona una curva elíptica.

Proposición 4. *Sea p un número primo tal que $p \nmid 2n$, y sea $q = p^r$, $r \geq 1$. Supongamos que $q \equiv 3$ (mód 4). Entonces hay $q+1$ puntos $\mathbb{F}_q$-racionales en la (reducción módulo p de la) curva elíptica $y^2 = x^3 - n^2 x$.*

Demostración. En primer lugar, vamos a comprobar que define una curva elíptica no singular. Para ello, sustituimos nuestros valores en $4a^3 + 27b^2 \neq 0$ y obtenemos la condición

$$4(-n^2)^3 = -4n^2 \not\equiv 0 \pmod{p}.$$

Esta condición se cumplirá siempre y cuando p no divida a 2 ni a n, lo cual tenemos garantizado por hipótesis. Por lo tanto la curva elíptica sobre $\mathbb{F}_p$ que se obtiene por reducción módulo p será no singular. Sabemos que hay cuatro puntos de orden 2: el punto en el infinito, $(0,0)$ y $(\pm n, 0)$. Ahora tendremos en cuenta todos los pares (x,y) donde $x \neq 0, n, -n$. Organizamos estos $q-3$ valores de x en pares $\{x,-x\}$. Dado que $f(x) = x^3 - n^2 x$ es una función impar y -1 no es un cuadrado en $\mathbb{F}_q$ ya que por hipótesis $q \equiv 3$ (mód 4), se sigue que exactamente uno de los dos elementos $f(x)$ y $f(-x) = -f(x)$ es un cuadrado en $\mathbb{F}_q$. Recordemos que en el grupo multiplicativo de un cuerpo finito, los cuadrados son un subgrupo de índice 2, y así el producto de dos no cuadrados es un cuadrado, mientras que el producto de un cuadrado y un no cuadrado es un no cuadrado. Sea cual sea el elemento en $\{x,-x\}$ que proporciona un cuadrado, obtenemos exactamente dos puntos: o bien $(x, \pm\sqrt{f(x)})$ o bien $(-x, \pm\sqrt{f(-x)})$. Así, los $(q-3)/2$ pares nos dan $q-3$ puntos. Junto con los cuatro puntos de orden dos, tenemos en total $q+1$ puntos $\mathbb{F}_q$-racionales, lo que pueba la proposición. □

Habiendo demostrado este resultado, finalmente podemos presentar la proposición que teníamos como objetivo.

Proposición 5. $\#E_n(\mathbb{Q})_{tors} = 4$.

Demostración. La idea de la demostración es construir homomorfismos de grupos de $E_n(\mathbb{Q})_{\text{tors}}$ a $E_n(\mathbb{F}_p)$ que sean inyectivos para una infinitud de primos p. Eso implicará que el orden de $E_n(\mathbb{Q})_{\text{tors}}$ divide el orden de $E_n(\mathbb{F}_p)$ para tales p. Pero ningún número mayor que 4 podría dividir todos esos números $\#E_n(\mathbb{F}_p)$, porque sabemos que $\#E_n(\mathbb{F}_p)$ recorre todos los enteros de la forma $p+1$ para p un número primo congruente a 3 módulo 4 por el teorema anterior.

Comenzamos construyendo una aplicación de 'reducción módulo p' $\mathbb{P}^2_{\mathbb{Q}} \to \mathbb{P}^2_{\mathbb{F}_p}$, que nos permitirá definir un homomorfismo de $E_n(\mathbb{Q})$ a $E_n(\mathbb{F}_p)$. Para ello, elegimos tríos $[x:y:z]$ para un punto en $\mathbb{P}^2_{\mathbb{Q}}$ de tal manera que x,y,z sean enteros sin ningún factor común. Salvo multiplicaciones por ± 1, hay un único trio con esas características en su clase de equivalencia. Para cualquier primo fijo p, definimos la imagen $\bar{P}$ de $P = [x:y:z] \in \mathbb{P}^2_{\mathbb{Q}}$ como el punto $\bar{P} = [\bar{x}:\bar{y}:\bar{z}] \in \mathbb{P}^2_{\mathbb{F}_p}$, donde la barra denota la reducción de un entero módulo p. Nótese que $\bar{P}$ no es el triple idénticamente cero, porque p no divide los tres enteros x,y,z por la condición que hemos pedido. También se debe notar que podríamos haber reemplazado el trio $[x:y:z]$ por cualquier múltiplo de un entero coprimo con p sin afectar a $\bar{P}$.

Es fácil ver que si $P = [x:y:z]$ resulta estar en $E_n(\mathbb{Q})$, es decir, si $y^2z = x^3 - n^2xz^2$, entonces $\bar{P}$ está en $E_n(\mathbb{F}_p)$. Además, la imagen de $P_1 + P_2$ bajo esta aplicación es $\bar{P}_1 + \bar{P}_2$, porque es lo mismo aplicar las fórmulas de la ley de grupo para obtener la suma y luego reducir módulo p que primero reducir módulo

p y luego usar las fórmulas de la ley de grupo. En otras palabras, nuestra aplicación es un homomorfismo de $E_n(\mathbb{Q})$ a $E_n(\mathbb{F}_p)$ para cualquier primo p que no divida $2n$.

Supongamos que nuestra proposición es falsa y $E_n(\mathbb{Q})$ contiene un punto de orden finito mayor a 2. Entonces, o contiene un elemento de orden impar o el grupo de puntos de orden 4 (o divirsor de cuatro) contiene o 8 o 16 elementos. En cualquiera de los casos, tenemos un subgrupo $S = \{P_1, ..., P_\ell\} \subset E_n(\mathbb{Q}_{\text{tors}})$, donde $\ell = \#S$ es 8 o un número impar.

Se puede demostrar que la aplicación de reducción módulo p de S en $E_n(\mathbb{F}_p)$ es inyectiva. Pero esto significa que para todos, excepto para un número finito de p primos congruentes a 3 módulo 4, por la proposición anterior, el número ℓ debe dividir $\#E_n(\mathbb{F}_p)$, porque la imagen de S es un subgrupo de orden ℓ. Esto quiere decir que, para todos excepto para un número finito de primos congruentes a 3 módulo 4, se tiene que $p \equiv -1 \pmod{\ell}$. Pero esto contradice el teorema de Dirichlet sobre primos en una progresión aritmética. Es decir, si $\ell = 8$ esto significaría que hay solo un número finito de primos de la forma $8k+3$. Si ℓ es impar, significaría que hay solo un número finito de primos de la forma $4\ell k+3$ (si $3 \nmid \ell$), y que hay solo un número finito de primos de la forma $12k+7$ si $3 \mid \ell$. En todos los casos, el teorema de Dirichlet nos dice que hay infinitos primos del tipo dado. Por lo tanto concluímos que $\#E_n(\mathbb{Q})_{\text{tors}}$ no puede ser otro que 4. □

Para acabar este capítulo vamos a presentar un resultado sobre las posibles formas que presenta $E(\mathbb{Q})_{\text{tors}}$. El teorema fue enunciado en 1977 por el matemático estadounidense Barry Mazur en el artículo *Modular curves and the Eisenstein ideal* [11].

Teorema 3.10 (Mazur)**.** *Sea $E/\mathbb{Q}$ una curva elíptica. Entonces $E(\mathbb{Q})_{tors}$ es isomorfo a uno de los siguientes:*

(*i*) $\mathbb{Z}/N\mathbb{Z}$ *para* $1 \leq N \leq 10$ *o* $N = 12$

(*ii*) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ *para* $1 \leq N \leq 4$

Este teorema es muy relevante ya que nos reduce las posibilidades de la forma de los subgrupos de torsión a simplemente 15 opciones.

Capítulo 4

Reformulación del problema original

Al final del primer capítulo, se expone una correspondecia entre triángulos rectángulos de lados racionales con área n y soluciones a la curva elíptica $y^2 = x^3 - nx$ con $y \neq 0$. Y en el capítulo anterior, hemos visto que precisamente los puntos de la curva cuya coordenada y es nula son los de 2-torsión: $(0,0), (n,0), (-n,0)$ y O_E.

Además, por estar definida en $\mathbb{Q}$, hemos visto que éstos son los únicos puntos de orden finito que hay en la curva. Por ello, gracias a la correspondencia biunívoca concluimos que existirán triángulos rectángulos de lados racionales con área n siempre y cuando haya al menos alguna solución de nuestra curva elíptica con $y \neq 0$ y por lo tanto de orden infinito.

El matématico L. J. Mordell presentó el resultado que enunciamos a continuación, cuya demostración puede leerse en su libro *Diophantine Equations* [12]. Este resultado nos ayudará a entender cuando nuestra curva elíptica es infinita.

Teorema 4.1 (Mordell)**.** *Sea $E/\mathbb{Q}$ una curva elíptica definida sobre los números racionales. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

Esto permite una descomposición $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$. Dependiendo de si r es positivo o 0, vemos que $E(\mathbb{Q})$ será infinito o finito, respectivamente. Al entero r se le llama *rango de la curva elíptica*.

En otras palabras, el Teorema de Mordell afirma que existe un número finito de puntos que generan $E(\mathbb{Q})$ usando la ley de grupo explicada en el capítulo 2:

$$\exists P_1, ..., P_s \in E(\mathbb{Q}) \text{ tal que } \forall Q \in E(\mathbb{Q}), Q = a_1P_1 + ... + a_sP_s \text{ con } a_i \in \mathbb{Z}.$$

Este resultado nos muestra que no hay infinitos puntos de orden finito. En un principio, para cada entero m, $E[m](\mathbb{Q})$ podría contener algún punto no trivial. Sin embargo, este teorema nos asegura que solo hay un número finito de m's para los cuales el subgrupo de m-torsión no es trivial.

Por este teorema y por la argumentación explicada al comienzo del capítulo obtenemos lo siguiente.

Proposición 6. *n es un número congruente si y solo si el rango de $E_n(\mathbb{Q})$ es mayor a 0.*

Demostración. Supongamos que n es un número congruente. En el primer capítulo hemos visto que la existencia de un triángulo rectángulo de lados racionales y área n nos lleva a un punto de la curva elíptica $y^2 = x^3 - n^2x$ con $y \neq 0$. Por lo que hemos visto en el apartado del segundo capítulo sobre puntos de orden finito, tenemos que los puntos con coordenada y nula son precisamente los únicos puntos de orden finito de la curva. Por lo tanto, los puntos que obtenemos de la curva tendrán orden infinito lo que implica que nuestra curva tendrá un rango estrictamente positivo.

Por otro lado, si suponemos que nuestra curva tiene puntos de orden infinito, necesariamente estos tendrán $y \neq 0$, porque de lo contrario estarían en el subgrupo de 2-torsión por lo que hemos visto en el apartado de puntos de orden finito. De nuevo, por la correspondecia biyectiva que hemos visto al final del primer capítulo, la existencia de soluciones de la curva elíptica con $y \neq 0$ nos da un trío (a,b,c) de números racionales que cumplen ser los lados de un triángulo rectángulo de área n, lo que asegura que n es congruente. □

Ahora que hemos conseguido reformular el problema de los números congruentes gracias al último resultado, la pregunta natural que nos hacemos es cómo determinar el rango de la curva elíptica $E_n(\mathbb{Q})$. Resulta que este problema es muy complicado y de hecho es un problema que sigue abierto actualmente.

Para abordar el problema vamos a introducir la conjentura de Birch y Swinnerton-Dyer. Lamentablemente, esta conjetura está sujeta a una función de variable compleja cuyo manejo es complicado. Por ello, se dará principalmente la idea detrás de la conjetura más que el desarrollo completo siguiendo las secciones 1.3 y 1.4 del Capítulo I del libro *Rational Points on Modular Elliptic Curves* de H. Darmon [10].

Por simplicidad y conveniencia por las características de nuestro problema, nos restringimos a las curvas definidas en $\mathbb{Q}$. Además, pese a haber usado durante el trabajo la ecuación simplificada de Weiestrass, $y^2 = x^3 + ax + b$ para esta construcción nos interesa utilizar la forma generalizada. Usando esta forma, cuando trabajamos sobre $\mathbb{Q}$, existe la llamada *ecuación mínima de Weiestrass* para cada curva E. Dicha ecuación tiene la ventaja de que sus coeficientes son enteros y su discriminante (que será por tanto un entero) será *mínimo* (en valor absoluto) entre todas las ecuaciones de este tipo que definen la misma curva E. En particuar, tendremos una ecuación de la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.1}$$

$$\text{con } a_1, ..., a_6 \in \mathbb{Z}.$$

Aquí, recordamos que su discriminante se define de la siguiente forma:

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0,$$

donde

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

La condición $\Delta \neq 0$ asegura que la curva sea no singular. Además, si p es un número primo que no divide a Δ, entonces puede probarse que la ecuación (4.1) reducida módulo p define una curva elíptica sobre $\mathbb{F}_p$.

Definición. Sean $E/\mathbb{Q}$ una curva elíptica y p un número primo. Decimos que E tiene *buena reducción* en p si p no divide Δ, el discriminante de E.

Definición. Sea $E/\mathbb{Q}$ una curva elíptica con buena reducción en p. Denotamos por N_p el cardinal del grupo $E(\mathbb{F}_p)$:

$$N_p = |E(\mathbb{F}_p)|.$$

Es decir, N_p será el número de puntos de (la reducción módulo p de) E con coordenadas en $\mathbb{F}_p$. Un argumento heurístico sencillo muestra que N_p debería ser 'cercano' a $p+1$. De hecho, escribiendo

$$N_p = p + 1 - a_p,$$

el 'término de error' a_p satisface la desigualdad de Hasse (capítulo V de [3]).

$$|a_p| \leq 2\sqrt{p}.$$

La idea detrás de la conjetura de Birch y Swinnerton-Dyer es que el rango de $E(\mathbb{Q})$ debería verse reflejado en el comportamiento asíntotico de las cantidades N_p cuando p tiende a infinito, y que por lo tanto, un rango grande, que supone una mayor cantidad de puntos racionales en $E(\mathbb{Q})$, debería tender a hacer de media N_p mayor que $p+1$.

Basados en experimentos numéricos, Birch y Swinnerton-Dyer propusieron la siguiente conjetura:

Conjetura 1 (Birch y Swinnerton-Dyer)**.** *Existe una constante C_E que depende solamente de E tal que*

$$\prod_{\substack{p\leq X,\\ p\nmid N}} \frac{N_p}{p} \sim C_E(\log X)^r,$$

donde r es el rango de $E(\mathbb{Q})$.

Aquí con el símbolo $\sim$ queremos expresar que el cociente de las expresiones que aparecen a ambos lados tiende a 1 cuando X tiende a infinito.

Una de las dificultades de esta conjetura es que el producto de la izquierda, que involucra los N_p definidos de manera aritmética, es complicado de analizar analíticamente. Debido a esa complejidad, se obtiene una mayor comprensión conceptual de la conjetura de Birch y Swinnerton-Dyer reformulándola en términos de la L-función de $E/\mathbb{Q}$ que introducimos a continuación.

Para comenzar, es necesario extender la definición que tenemos de los coeficientes a_p. Como hemos visto, éstos solo están definidos para aquellos primos p que no dividen a Δ. Por lo tanto, debemos externder la definición a aquellos primos (que son solo un número finito) que dividen a Δ. La extensión se hace dependiendo de cuál es la singularidad de E en $\mathbb{F}_p$. Pero, debido a que es una cuestión técnica que involucra conceptos que no se han desarrollado a lo largo del trabajo, no se explicará explícitamente esta extensión (se puede consultar en la referencia dada [10]).

Con esa extensión, la función L de E se define como el producto de Euler infinito

$$L(E,s) = \prod_{p\nmid N} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1} \prod_{p|N} \left(1 - a_p p^{-s}\right)^{-1} = \sum_{n=1}^{\infty} a_n n^{-s},$$

en el cual la expresión de $L(E,s)$ como una serie de Dirichlet proporciona la definición del coeficiente a_n cuando n no es primo.

Al evaluar el producto de Euler formalmente en $s = 1$ da

$$L(E,1)\text{”} = \text{”}\prod_p \frac{p}{N_p}, \tag{4.2}$$

donde N_p es la cardinalidad del grupo de puntos no singulares en $E(\mathbb{F}_p)$. Esta igualdad es solo formal, ya que el producto de Euler que define $L(E,s)$ solo converge en la mitad derecha del plano $\mathrm{Re}(s) > 3/2$.

Pero precisamente, se cree que el comportamiento de $L(E,s)$ en $s = 1$, asumiendo que podamos darle sentido a esa evaluación, debería reflejar la tendencia asintótica del producto $\prod_{p\nmid N} \frac{N_p}{p}$ que aparece en la primera versión de la conjetura de Birch y Swinnerton-Dyer que se ha dado. Por lo tanto, se puede reformular la conjeutra con la función $L(E,s)$.

Conjetura 2 (Birch y Swinnerton-Dyer)**.** *La función $L(E,s)$ se extiende a una función entera sobre $\mathbb{C}$ y el rango r de $E(\mathbb{Q})$ es igual al orden de anulación de $L(E,s)$ en $s = 1$.*

Asumiendo esta conjetura, vemos por ejemplo que si la función $L(E_n,s)$ no se anula en $s = 1$, el rango de $E_n(\mathbb{Q})$ es 0 y por lo tanto podemos descartar que n sea congruente. De hecho:

Corolario 1. *Asumiendo la Conjetura de Birch y Swinnerton-Dyer, un número entero $n > 0$ es congruente si y solo si $L(E_n,1) = 0$.*

Bibliografía

[1] N. KOBLITZ, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics 97 Springer, 1984.

[2] K. CONRAD, *Congruent Numbers*, Disponible online en: `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf`.

[3] J. H. SILVERMAN, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, 2nd Edition, Springer, 2009.

[4] J. H. SILVERMAN, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer, 1994.

[5] A. SUTHERLAND, *Elliptic Curves*, Notas de un curso en MIT (Massachusetts Institute of Technology), disponibles electrónicamente en `https://math.mit.edu/classes/18.783/2023/lectures.html`.

[6] L. C. WASHINGTON, *Elliptic Curves: Number Theory and Cryptography,* ,Second Edition, Chapman & Hall/CRC, 2008.

[7] R. J. WALKER, *Algebraic Curves*, Springer, 1978.

[8] J. NEUKIRCH, *Algebraic Number Theory*, Springer, 1999.

[9] J.P. SERRE, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer, 1973.

[10] H. DARMON, *Rational Points on Modular Elliptic Curves*, Department of Mathematics, McGill University, 1991.

[11] B. MAZUR, Modular curves and the Eisenstein ideal, With an appendix by B. Mazur and M. Rapoport *Inst. Hautes Études Sci. Publ. Math.*(1977), no. 47, 33–186.

[12] L. J. MORDELL, *Diophantine Equations*, Academic Press, 1969.

[13] B. J. BIRCH, W. KUYK (EDS.), *Modular Functions of One Variable IV*, Lecture Notes in Math. 476, Springer, Berlín, 1975.