Sección de Matemáticas
Universidad de La Laguna

Daniel Montesdeoca del Pino

El Problema del Número Congruente

The Congruent Number Problem

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Marzo de 2024

Dirigido por
Evelia Rosa García Barroso

Evelia Rosa García Barroso
Departamento de Matemáticas,
Estadística e I.O.
Universidad de La Laguna
38200 La Laguna, Tenerife

Agradecimientos

A todos los profesores que me han acompañado durante mi aprendizaje y consiguieron que me enamorase un poco más de las matemáticas, en especial a mi tutora, Evelia.

A los amigos que hice durante la carrera, Javier y Gisela, por estar conmigo durante estos últimos años.

A mi familia, por darme siempre todo su apoyo y amor de manera incondicional.

Gracias.

Daniel Montesdeoca del Pino
La Laguna, 5 de marzo de 2024

Resumen · Abstract

Resumen

El problema del número congruente consiste en determinar qué números racionales pueden ser el área de un triángulo rectángulo cuyos tres lados son racionales, dichos números son llamados números congruentes. Para ello necesitaremos algunos resultados de la teoría de curvas elípticas.
En primer lugar, haremos una introducción al problema, se darán ejemplos conocidos tanto de números congruentes como de números no congruentes y se estudiarán diferentes perspectivas de nuestro problema original. A continuación, nos centraremos en la teoría de Curvas Elípticas, y en particular, demostraremos el Teorema de Nagell-Lutz, un teorema importante sobre los puntos de torsión racionales de curvas elípticas. Concluiremos el Capítulo 2 aplicando este teorema para conectar nuestro problema al estudio del rango de ciertos grupos abelianos finitamente generados. Por último, daremos una generalización de los números congruentes y probaremos que también está conectado al estudio de una familia de curvas elípticas.

Palabras clave: *Curvas elípticas – Puntos racionales – Teoría de Números.*

Abstract

The congruent number problem consists of determining which rational numbers can be the area of a right triangle with three rational sides, such numbers are called congruent numbers. For this purpose, we need some results from the theory of elliptic curves.
First of all, we will make an introduction to the problem, providing well-known examples of congruent numbers, as well as non-congruent numbers and we will study different approaches to our original problem. Next, we will focus on the theory of elliptic curves, in particular, we will prove the Nagell-Lutz Theorem, an important theorem about the rational torsion points of elliptic curves. We will finish Chapter 2 by applying this theorem to link our original problem to the study of the rank of certain finitely generated abelian groups. Finally, we will provide a generalization of congruent numbers and prove that it is also connected to the study of a family of elliptic curves.

Keywords: *Elliptic Curves – Rational Points – Number Theory.*

Contenido

Introducción

En matemáticas, y especialmente en Teoría de Números, es posible encontrar problemas que son fáciles en apariencia, y sin embargo, son realmente difíciles de resolver. El Problema del Número Congruente es uno de estos problemas. De hecho, se trata del problema aritmético más antiguo no completamente resuelto todavía.

Desde la antigua Grecia, y en particular desde *Arithmetica* de Diofanto en el siglo III D.C, se observa cierto interés por este tipo de números. Pero es el matemático persa Al-Karají (953-1029) quien después de leer las traducciones al árabe de Diofanto, formuló por primera vez el conocido como el Problema del Número Congruente.

Muchos matemáticos a lo largo del tiempo se han visto interesados en este problema, como por ejemplo Fibonacci o Fermat. Es más, uno de los resultados que dio Fermat sobre los números congruentes tiene como consecuencia un caso particular del famoso último teorema de Fermat.

Al ser un problema tan longevo, este problema se ha atacado desde varios campos de las matemáticas. Sin embargo, sin duda el más fructífero ha sido el campo de las curvas elípticas. El resultado más destacado que nos ha proporcionado este enfoque es el Teorema de Tunnell (1983), el cual nos da una condición necesaria para que un número sea congruente. Además, en caso de que la *Conjetura de Birch y Swinnerton-Dyer*, uno de los problemas del milenio, sea cierta entonces Tunnell demostró que la implicación era un si y solo si. De esta forma obtendríamos un algoritmo para determinar en un número finito de pasos si un número es congruente o no, resolviendo finalmente el Problema del Número Congruente.

Este trabajo de fin de grado está dividido en tres capítulos. En el primero se expone el Problema del Número Congruente, las secciones de este capítulo están dedicadas a formulaciones equivalentes de este, donde cada una nos ofrece diferentes herramientas para afrontar el problema original.

En el segundo capítulo, se da una introducción a la teoría de curvas elípticas. Más concretamente, se prueba el Teorema de Nagell-Lutz, necesario para

establecer una última posible formulación del problema, la cual busca encontrar el rango de una familia de grupos abelianos finitamente generados.

Finalmente, en el tercer capítulo, se propone una generalización del problema, y aprovechando resultados del segundo capítulo, encontramos una familia de curvas elípticas cuyo estudio es interesante a la hora de resolver este problema.

1

El Problema del Número Congruente

En este capítulo daremos una introducción del problema del número congruente, se proporcionarán algunos resultados clásicos y estableceremos algunas formas equivalentes de este problema. Hemos seguido principalmente [5], también se ha hecho uso de [4] y [8].

1.1. Ternas Pitagóricas

Definición 1.1 (Número Congruente). *Decimos que $n \in \mathbb{Q}$ es un número congruente si es el área de un triángulo rectángulo cuyos lados son racionales.*

Por lo tanto dado un cierto $n \in \mathbb{Q}$ buscamos si el siguiente sistema tiene solución:

$$\begin{cases} a^2 + b^2 = c^2 \\ \frac{ab}{2} = n \\ a, b, c \in \mathbb{Q}^+ \end{cases} \tag{1.1}$$

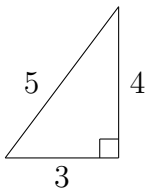
En esta memoria denotaremos por $a \mid b$, cuando a divide a b.

Si $n = p/q$ es congruente y a, b, c son los lados del correspondiente triángulo rectángulo entonces si tomamos $s_1 = max\{x \in \mathbb{Z} : x^2 \mid p\}$, $s_2 = max\{x \in \mathbb{Z} : x^2 \mid q\}$ y $s = q/(s_1 \cdot s_2)$, se tiene que ns^2 es un entero libre de cuadrados y sa, sb, sc forman los lados de un triángulo rectángulo de área ns^2. Así que en realidad el problema se reduce a encontrar los enteros libres de cuadrados n que cumplen (1.1).

Definición 1.2 (Ternas Pitagóricas). *Una terna pitagórica (a, b, c) consiste en tres enteros $a, b, c > 0$ que verifican $a^2 + b^2 = c^2$. Si además $\mathrm{mcd}(a, b, c) = 1$ entonces decimos que es una terna pitagórica primitiva, y el correspondiente triángulo rectángulo que determina es primitivo.*

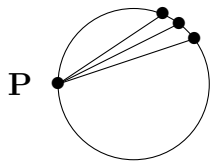
Ejemplo 1.3. La terna (3,4,5) son los lados de un triángulo rectángulo de área 6, por tanto 6 es un número congruente

Vamos a encontrar todas las ternas pitagóricas:



Teorema 1.4. *Toda terna pitagórica primitiva se puede escribir como* $(s^2 - r^2, 2rs, r^2 + s^2)$ *para ciertos enteros positivos* r, s *verificando* $\mathrm{mcd}(r, s) = 1$*, donde uno de ellos es par y el otro es impar.*

Demostración. Sea (a, b, c) una terna pitagórica primitiva, es decir, $\mathrm{mcd}(a, b, c) = 1$. De aquí se sigue que a, b y c no tienen factores en común entre sí, si por ejemplo un primo p dividiese a a y b entonces p^2 divide a c^2, de donde p divide a c. Sin embargo el triángulo rectángulo que determina (a, b, c) es primitivo. Así que a y b no pueden ser pares a la vez. Y tampoco pueden ser ambos impares, pues recordemos que el cuadrado de un impar es congruente a 1 mód 4. Y si a y b son impares $a^2 + b^2 \equiv 1 + 1 = 2$ mód 4, así que $c^2 \equiv 2$ mód 4 pero no hay nigún cuadrado congruente a 2 mód 4. Supongamos sin pérdida de generalidad que b es par y a es impar. Si definimos $u = a/c, v = b/c$, entonces (u, v) es un punto racional de la circunferencia $x^2 + y^2 = 1$ donde u y v son fracciones irreducibles. Además como $a, b, c > 0$, (u, v) está en el primer cuadrante.



Dada la circunferencia unidad cogemos el punto (-1,0) al que llamamos P y consideramos las rectas que pasan por P. Salvo la recta tangente a la circunferencia en P, el resto de rectas son de la forma $y = t(x + 1)$ para un cierto t e intersectará a la circunferencia en otro punto además de en P. Para hallar ese punto sustituimos la ecuación anterior en la ecuación de la circunferencia y obtenemos:

$$(1 + t^2)x^2 + 2t^2x + (t^2 - 1) = 0 \tag{1.2}$$

La raíz en $x = -1$ se corresponde con el punto P, mientras que la otra raíz de (1.2) se corresponde con el segundo punto de intersección y sus coordenadas son:

$$x(t) = \frac{1 - t^2}{1 + t^2}, \quad y(t) = \frac{2t}{1 + t^2}, \tag{1.3}$$

$(x(t), y(t))$ con $t \in \mathbb{R}$ parametriza todos los puntos de la circunferencia excepto (-1,0). Si $t \in \mathbb{Q}$ está claro que $x, y \in \mathbb{Q}$. Por otro lado, si $x, y \in \mathbb{Q}$ como $y = t(x+1)$ entonces $t \in \mathbb{Q}$ pues $x \neq -1$ para cualquier valor de t. Por lo tanto existe un valor de $t \in \mathbb{Q}$ tal que $(u, v) = (x(t), y(t))$. Escribimos $t = r/s$ donde r y s son

coprimos, y además para que $(x(t), y(t))$ esté en el primer cuadrante tenemos que imponer que $0 \leq t \leq 1$, por lo que $0 \leq r \leq s$. Nos queda que:

$$u = \frac{a}{c} = \frac{s^2 - r^2}{r^2 + s^2}, \quad v = \frac{b}{c} = \frac{2rs}{r^2 + s^2}. \tag{1.4}$$

Recordemos que a/c y b/c son fracciones irreducibles así que existirá un entero positivo λ tal que:

$$\lambda a = s^2 - r^2, \quad \lambda b = 2rs, \quad \lambda c = r^2 + s^2. \tag{1.5}$$

Como λ divide a $s^2 - r^2$ y a $r^2 + s^2$, λ divide a la suma $2s^2$ y a la diferencia $2r^2$, al ser r y s coprimos entonces λ divide a 2, lo que significa que $\lambda = 1$ o $\lambda = 2$. Supongamos que $\lambda = 2$. Como b es par y $\lambda b = 2rs$ tenemos entonces que 2 divide a rs y dado que r y s son coprimos la única opción es que uno de ellos sea par y el otro impar, lo que significa que entre r^2 y s^2 uno es par y el otro impar, de cualquier forma $r^2 + s^2$ es impar pero al ser $\lambda = 2$ se tiene que $2c = r^2 + s^2$ y esto es una contradicción. Concluimos que $\lambda = 1$.

Además si $r \equiv s$ mód 2, $s^2 - r^2$ y $r^2 + s^2$ serían pares, y por tanto $(s^2 - r^2, 2rs, r^2 + s^2)$ no sería una terna pitagórica primitiva.

Hemos concluido que todas las ternas pitagóricas de triángulos primitivos están generadas por $(s^2 - r^2, 2rs, r^2 + s^2)$ donde r y s son coprimos, donde uno de ellos es par y el otro es impar y $0 \leq r \leq s$. Si multiplicamos la anterior terna por un entero positivo podemos generar todas las ternas pitagóricas.

□

Lema 1.5. *Sean $a, b \in \mathbb{Z}^+$ coprimos.*

(a) Si $ab = k^n, k \in \mathbb{Z}^+$ entonces $a = r^n$ y $b = s^n$ para ciertos $r, s \in \mathbb{Z}^+$ coprimos.
(b) Si $ab = pk^n, k \in \mathbb{Z}^+$, p primo entonces $a = pr^n$ y $b = s^n$ o $a = r^n$ y $b = ps^n$ para ciertos $r, s \in \mathbb{Z}^+$ coprimos.
(c) $\mathrm{mcd}(a + b, a - b)$ *es 1 o 2.*
(d) $\mathrm{mcd}(a^2+b^2, a^2+4b^2) = 1$. *En particular la hipotenusa del triángulo rectángulo asociado a una terna pitagórica primitiva no es múltiplo de 3.*

Demostración. (a) Si a o b son 1 el resultado está claro. Sean $a, b > 1$. Escribimos a, b y k en función de sus factores primos:

$$a = p_1^{\alpha_1} \cdots p_m^{\alpha_m}, \quad b = p_1^{\beta_1} \cdots p_m^{\beta_m}, \quad k = p_1^{\gamma_1} \cdots p_m^{\gamma_m}, \tag{1.6}$$

donde $p_1, \ldots, p_m$ son primos y $\alpha_i,\ \beta_i,\ \gamma_i \in \mathbb{N}$. De la igualdad $ab = k^n$ obtenemos

$$p_1^{\alpha_1+\beta_1} \cdots p_m^{\alpha_m+\beta_m} = p_1^{n\gamma_1} \cdots p_m^{n\gamma_m}. \tag{1.7}$$

Esto quiere decir que $\alpha_i + \beta_i = n\gamma_i$ para todo $i \in \{1, \ldots, m\}$ y como a y b son coprimos se tendrá que $\alpha_i = 0$ o $\beta_i = 0$, por lo que los exponentes en la

factorización de a y b son todos múltiplos de n, de aquí concluimos que existen $r, s \in \mathbb{Z}^+$ coprimos verificando $a = r^n$ y $b = s^n$.
(b) Seguimos el mismo razonamiento que en (a), la única diferencia es que ahora $pk^n = p_1^{n\gamma_1} \cdots p_j^{n\gamma_j+1} \cdots p_m^{n\gamma_m}$ para un cierto j (el que verifique $p_j = p$), esto significa que $\alpha_j + \beta_j = n\gamma_j + 1$. De nuevo como a y b son coprimos se tiene que $\alpha_j = 0$ o $\beta_j = 0$. En el primer caso concluimos que $a = r^n$ y $b = ps^n$ y en el otro que $a = pr^n$ y $b = s^n$.
(c) Tenemos que $\mathrm{mcd}(a+b, a-b) = \mathrm{mcd}(a+b, (a-b)+(a+b)) = \mathrm{mcd}(a+b, 2a)$ que divide a $\mathrm{mcd}(2(a+b), 2a) = \mathrm{mcd}(2(a+b) - 2a, 2a) = 2\,\mathrm{mcd}(b, a) = 2$. Esto significa que $\mathrm{mcd}(a+b, a-b)$ debe ser 1 o 2.
(d) Observemos que $\mathrm{mcd}(a^2+b^2, a^2+4b^2) = \mathrm{mcd}(a^2+b^2, a^2+4b^2-(a^2+b^2)) = \mathrm{mcd}(a^2+b^2, 3b^2)$ que divide a $\mathrm{mcd}(3(a^2+b^2), 3b^2) = 3\,\mathrm{mcd}(a^2+b^2, b^2) = 3\,\mathrm{mcd}(a^2+b^2-b^2, b^2) = 3\,\mathrm{mcd}(a^2, b^2) = 3$, es decir que $\mathrm{mcd}(a^2+b^2, a^2+4b^2)$ es 1 o 3. Sabemos que dado $x \in \mathbb{Z}$, x^2 solo puede ser 0 mód 3 o 1 mód 3, por lo tanto si $a^2 + b^2 \equiv 0$ mód 3, necesariamente $a^2 \equiv 0$ mód 3 y $b^2 \equiv 0$ mód 3, pero entonces a y b no son coprimos. Concluimos que 3 no divide a $a^2 + b^2$ y de aquí que 3 no divide a la hipotenusa del triángulo asociado a una terna pitagórica primitiva, y también $\mathrm{mcd}(a^2+b^2, a^2+4b^2) = 1$.

□

Lema 1.6. *Sean $a, b \in \mathbb{Z}^+$.*

(a) Si $a^n \mid b^n$ entonces $a \mid b$.
(b) Si $a^2 \mid 2b^2$ entonces $a \mid b$.

Demostración. (a) Tomamos $c = b/a \in \mathbb{Q}$, como $a^n \mid b^n$ entonces $d := c^n \in \mathbb{Z}$ y c es raíz del polinomio mónico $x^n - d \in \mathbb{Z}[x]$, pero las raíces racionales de un polinomio mónico son enteras, así que $c \in \mathbb{Z}$, es decir, $a \mid b$.
(b) Podemos escribir a y b en términos de sus factores primos, $a = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, $b = 2^{\beta_0} p_1^{\beta_1} \cdots p_m^{\beta_m}$, donde $\alpha_i,\ \beta_i \in \mathbb{N}$ para todo $i \in \{1, \ldots, m\}$. Por hipótesis

$$2^{2\alpha_0} p_1^{2\alpha_1} \cdots p_m^{2\alpha_m} \mid 2^{2\beta_0+1} p_1^{2\beta_1} \cdots p_m^{2\beta_m}. \tag{1.8}$$

Esto quiere decir que $2\alpha_i \leq 2\beta_i$, en el caso $i = 0$ se tiene que $2\alpha_0 \leq 2\beta_0 + 1$, pero como $2\alpha_0 \neq 2\beta_0 + 1$ ya que $\alpha_0,\ \beta_0 \in \mathbb{N}$, en realidad $2\alpha_0 \leq 2\beta_0$. Concluimos entonces que para cada i, $\alpha_i \leq \beta_i$, es decir, $a \mid b$.

□

Fibonacci afirmó, pero no demostró, que el 1 no es un número congruente y durante mucho tiempo esta pregunta estuvo abierta, hasta que Fermat dio la primera demostración aceptada de este resultado.

Teorema 1.7 (Fermat). *El número 1 no es congruente.*

Demostración. Por reducción al absurdo supongamos que existen $x, y, z \in \mathbb{Q}^+$ verificando $x^2 + y^2 = z^2$ y $xy = 2$. Podemos escribir $x = a/d,\ y = b/d,\ z = c/d$ para ciertos $a, b, c, d \in \mathbb{Z}^+$. De esta forma se obtiene que:

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2d^2. \end{cases} \tag{1.9}$$

Sea $m = \text{mcd}(a, b)$. Como $m \mid a$ y $m \mid b$ y $a^2 + b^2 = c^2$ entonces $m^2 \mid c^2$ y de $ab = 2d^2$ se tiene $m^2 \mid 2d^2$. Aplicando el Lema 1.6 tenemos que $m \mid c$ y $m \mid d$. Podemos entonces dividir a, b, c, d por m de forma que se siguen cumpliendo las condiciones de (1.9) y además $\text{mcd}(a, b) = 1$. Demostraremos que no existen soluciones enteras positivas del sistema (1.9) con la condición de que a y b sean coprimos.
Para ello usaremos el método de descenso infinito de Fermat, a partir de una solución (a, b, c, d) de (1.9) donde $\text{mcd}(a, b) = 1$ construiremos una nueva solución de (1.9), digamos (a', b', c', d'), donde $\text{mcd}(a', b') = 1$ y $0 < c' < c$ y podríamos repetir este proceso indefinidamente. Sin embargo, no existen infinitos enteros positivos más pequeños que uno dado, esto nos dará la contradicción que buscamos.
Para ello notamos que como $ab = 2d^2$ por el Lema 1.5(b) y dado que a y b tienen un papel simétrico, podemos decir que existen $k, l \in \mathbb{Z}^+$ coprimos donde

$$a = 2k^2, \quad b = l^2. \tag{1.10}$$

Como a y b son coprimos se tendrá que b es impar y a es par, por lo tanto $c^2 = a^2 + b^2$ es impar, así que c es impar, de aquí sacamos que $c + b$ y $c - b$ son pares, entonces podemos reescribir $a^2 + b^2 = c^2$ como $4k^4 = (c - b)(c + b)$ y llegamos a que

$$k^4 = \frac{c - b}{2} \cdot \frac{c + b}{2}. \tag{1.11}$$

Si $p \mid b$ y $p \mid c$, como $c^2 - b^2 = a^2$, se tendría que $p^2 \mid a^2$ y por el Lema 1.6 (a) deducimos que $p \mid a$, sin embargo, $\text{mcd}(a, b) = 1$. Concluimos que b y c son coprimos y ahora aplicando el Lema 1.5 (c) se tiene que $\text{mcd}(\frac{c-b}{2}, \frac{c+b}{2}) = 1$. Volviendo a la ecuación (1.11) podemos aplicar el Lema 1.5 (a) de donde existen $r, s \in \mathbb{Z}^+$ coprimos tales que:

$$\frac{c + b}{2} = r^4, \quad \frac{c - b}{2} = s^4. \tag{1.12}$$

Resolviendo el sistema (1.12), obtenemos que $b = r^4 - s^4$ y $c = r^4 + s^4$. Además teníamos que $l^2 = b$, por lo que:

$$l^2 = r^4 - s^4 = (r^2 - s^2)(r^2 + s^2). \tag{1.13}$$

Como $b = l^2$ es impar, $r^2 - s^2$ y $r^2 + s^2$ son impares y al ser r y s coprimos, r^2 y s^2 también lo son. Aplicando el Lema 1.5(c) se tiene que $\text{mcd}(r^2 + s^2, r^2 - s^2) = 1$, por lo que podemos aplicar el Lema 1.5(a) de donde existen $u, t \in \mathbb{Z}^+$ coprimos que verifican:

$$r^2 + s^2 = t^2, \quad r^2 - s^2 = u^2. \tag{1.14}$$

Deducimos que t y u son impares, de aquí $u^2 \equiv 1$ mód 4, y como $r^2 - s^2 = u^2$, necesariamente r es impar y s es par. Resolviendo el sistema en (1.14) obtenemos

$$r^2 = \frac{t^2 + u^2}{2} = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2. \tag{1.15}$$

Por ser t y u impares tenemos que $(t \pm u)/2 \in \mathbb{Z}^+$. Tomamos ahora:

$$a' = \frac{t+u}{2}, \quad b' = \frac{t-u}{2}, \quad c' = r. \tag{1.16}$$

Por el Lema 1.5(c) y al ser t y u coprimos e impares, $\mathrm{mcd}(a', b') = 1$. Podemos además ver que $(a')^2 + (b')^2 = (c')^2$ y $a'b' = (t^2 - u^2)/4 = (2s^2)/4 = 2(s/2)^2$, tomando $d' = s/2 \in \mathbb{Z}$ pues s es par. Hemos encontrado (a', b', c', d') con $\mathrm{mcd}(a', b') = 1$ solución del sistema (1.9) donde $0 < c' = r < r^4 + s^4 = c$.

□

En 1659 Fermat envió a Huygens un resumen de algunos de sus trabajos, entre ellos afirmó que había demostrado mediante un método que él llama descenso infinito, que no existe un triángulo rectángulo con lados enteros cuya área sea el cuadrado de un entero. Fermat no dió los detalles de la demostración alegando que alargarían demasiado la carta, tan sólo dió la idea general del método, sin embargo, sí que escribió los detalles en los márgenes de su ejemplar de la *Arithmetica* de Diofanto.

Una consecuencia curiosa de este teorema es una demostración en una línea de la irracionalidad de $\sqrt{2}$, pues de ser $\sqrt{2}$ racional, el 1 sería un número congruente, ya que el triángulo rectángulo de lados $\sqrt{2}$, $\sqrt{2}$, 2 tiene área 1.

Corolario 1.8. *La ecuación $X^4 - Y^4 = Z^2$ no tiene soluciones enteras donde $XYZ \neq 0$.*

Demostración. Supongamos por reducción al absurdo que existen $x, y, z \in \mathbb{Z}$ con $xyz \neq 0$ y $x^4 - y^4 = z^2$. Sean $n = x^2$ y $m = y^2$. Tomamos

$$a = n^2 - m^2, \quad b = 2nm, \quad c = n^2 + m^2,$$

entonces a y b son los catetos y c la hipotenusa de un triángulo rectángulo cuya área es $(ab)/2 = nm(n^2 - m^2) = (xyz)^2$. Por lo tanto $(xyz)^2$ es un número congruente, pero entonces la parte libre de cuadrados también es un número congruente, es decir que 1 es un número congruente, lo cual es absurdo.

□

En particular si en el Corolario 1.8 tomamos $z = w^2$, con w una nueva variable, obtenemos que la ecuación

$$y^4 + w^4 = x^4 \tag{1.17}$$

no tiene soluciones enteras donde $xyw \neq 0$. Esta es la única evidencia escrita que llevó a Fermat a conjeturar su famoso último teorema de Fermat.

Lema 1.9. *Sean $u, v, x, y \in \mathbb{Z}^+$ tales que $uv = xy$.*

(a) Si $\mathrm{mcd}(u, x) = \mathrm{mcd}(v, y) = 1$ *entonces* $u = y,\ v = x$.
(b) Si $\mathrm{mcd}(u, v) = \mathrm{mcd}(x, y) = 1$ *entonces existen enteros* $\alpha, \beta, \gamma, \delta$ *coprimos dos a dos tales que* $u = \alpha\beta,\ v = \gamma\delta,\ x = \alpha\gamma$ *y* $y = \delta\beta$.

Demostración. (a) Vamos a demostrar que $u = y$. Dado que $uv = xy$ tenemos que $u \mid xy$ y que $y \mid uv$. Como $\mathrm{mcd}(u, x) = \mathrm{mcd}(v, y) = 1$, aplicando el Lema de Euclides tenemos que $u \mid y$ y $y \mid u$, de donde $u = y$. De forma análoga se demuestra que $v = x$.
(b) Sean $\alpha = \mathrm{mcd}(u, x)$ y $\delta = \mathrm{mcd}(v, y)$. Podemos dividir $uv = xy$ por α y δ y obtenemos $u'v' = x'y'$ para ciertos $u', v', x', y' \in \mathbb{Z}^+$, donde $\mathrm{mcd}(u', x') = \mathrm{mcd}(v', y') = 1$. Aplicamos el Lema 1.9 (a) y tenemos $u' = y' = \beta,\ v' = x' = \gamma$, concluyendo que $u = \alpha\beta$, $v = \gamma\delta$, $x = \alpha\gamma$, $y = \delta\beta$ donde $\alpha, \beta, \gamma, \delta$ son coprimos dos a dos.

□

Teorema 1.10. *No existen $a, b, c, d \in \mathbb{Z}^+$ tales que las ternas (a, b, c) y $(a, 2b, d)$ sean ambas pitagóricas.*

Demostración. Podemos suponer que (a, b, c) y $(a, 2b, d)$ son ternas pitagóricas primitivas. En caso contrario sea $g = \mathrm{mcd}(a, b) > 1$, como $a^2 + b^2 = c^2$ y $a^2 + 4b^2 = d^2$ tendremos que $g^2 \mid c^2$, $g^2 \mid d^2$ y del Lema 1.6 (a) $g \mid c$ y $g \mid d$, es decir, $(a, b, c) = (gA, gB, gC)$ y $(a, 2b, d) = (gA, 2gB, gD)$ para ciertos $A, B, C, D \in \mathbb{Z}^+$. Tenemos entonces ternas pitagóricas (A, B, C) y $(A, 2B, D)$ donde $\mathrm{mcd}(A, B) = 1$. Ahora distinguiremos dos casos.
Caso 1: A es impar. Si $\mathrm{mcd}(A, C) = p > 1$ y $\mathrm{mcd}(A, D) = p > 1$, de $A^2 + B^2 = C^2$ obtendríamos $p^2 \mid B^2$, y por el Lema 1.6 (a) $p \mid B$, sin embargo $\mathrm{mcd}(A, B) = 1$, es decir (A, B, C) es primitiva. Por otra parte, de $A^2 + 4B^2 = D^2$ obtenemos $p^2 \mid (2B)^2$ y por el Lema 1.6 (a) $p \mid (2B)$. Como A es impar, p es impar y del Lema de Euclides tenemos que $p \mid B$, pero $\mathrm{mcd}(A, B) = 1$, por lo que $(A, 2B, D)$ es primitiva.
Caso 2: A es par, entonces podemos escribir $A = 2A'$. Dado que $2 \mid A$ y $2 \mid 2B$, deducimos que $2 \mid D$, por lo tanto podemos escribir $D = 2D'$. De las ternas pitagóricas $(2A', B, C)$, $(2A', 2B, 2D')$, podemos obtener las nuevas ternas pitagóricas $(B, 2A', C)$ y (B, A', D'), donde $\mathrm{mcd}(A', B) = 1$. Recordemos que $\mathrm{mcd}(A, B) = 1$, por lo que B debe ser impar, y estamos en las condiciones de aplicar el caso 1, por lo que $(B, 2A', C)$ y (B, A', D') son ternas pitagóricas primitivas.
Supongamos entonces que (a, b, c) y $(a, 2b, c)$ son ternas pitagóricas primitivas. Usamos la parametrización de ternas pitagóricas primitivas que obtuvimos en el Teorema 1.4, por lo que existen $u, v, x, y \in \mathbb{Z}^+$, donde $\mathrm{mcd}(u, v) = 1 = \mathrm{mcd}(x, y)$ verificando que

$$a = v^2 - u^2, \quad b = 2uv, \quad a = y^2 - x^2, \quad 2b = 2xy. \tag{1.18}$$

Al analizar la expresión $v^2 - u^2$ mód 4, dado que un cuadrado módulo 4 puede ser congruente a 0 o a 1, obtenemos 3 posibilidades al descartar el caso $u^2 \equiv v^2 \equiv 0$ mód 4 ya que $\text{mcd}(u, v) = 1$. Llegamos a

$$\begin{aligned} &\text{caso 1: } v^2 \equiv 1 \text{ mód } 4,\ u^2 \equiv 0 \text{ mód } 4,\ a \equiv 1 \text{ mód } 4,\\ &\text{caso 2: } v^2 \equiv 0 \text{ mód } 4,\ u^2 \equiv 1 \text{ mód } 4,\ a \equiv 3 \text{ mód } 4,\\ &\text{caso 3: } v^2 \equiv 1 \text{ mód } 4,\ u^2 \equiv 1 \text{ mód } 4,\ a \equiv 0 \text{ mód } 4. \end{aligned}$$

Análogamente al analizar $y^2 - x^2$ mód 4, llegamos a los mismos casos que antes reemplazando (u, v) por (x, y). Por lo que necesariamente $u^2 \equiv x^2$ mód 4 y $v^2 \equiv y^2$ mód 4, lo cual implica que $u \equiv x$ mód 2 y $v \equiv y$ mód 2.

Suponemos que u, x son impares y que por tanto v, y son pares, el otro caso es similar. Como $uv = x(y/2)$ aplicamos el apartado b del Lema 1.9 para escribir $u = \alpha\beta$, $v = \gamma\delta$, $x = \alpha\gamma$, $y = 2\delta\beta$ donde $\alpha, \beta, \gamma, \delta$ son coprimos dos a dos, entonces $\delta = \text{mcd}(v, y/2)$ es par. Igualando a en (1.18) nos queda que $u^2 + y^2 = x^2 + v^2$ y de aquí:

$$\beta^2(\alpha^2 + 4\delta^2) = \gamma^2(\alpha^2 + \delta^2).$$

Y como $\text{mcd}(\beta, \gamma) = 1$, por el Lema 1.9 (a) llegamos a que $\alpha^2 + \delta^2 = \beta^2$ y $\alpha^2 + 4\delta^2 = \gamma^2$. Tenemos entonces dos ternas pitagóricas primitivas de la forma (α, δ, β) y $(\alpha, 2\delta, \gamma)$, donde en este caso δ es un entero positivo verficando $\delta \leq y/2 < y \leq b$. Por el método del descenso infinito llegamos a un absurdo concluyendo así la prueba.

□

1.2. Progresiones Aritméticas

El problema del número congruente admite formulaciones equivalentes, una de ellas es mediante progresiones aritméticas, veremos cómo se relacionan con el siguiente teorema.

Teorema 1.11. *Sea $n > 0$. Existe una aplicación biyectiva entre los triángulos rectángulos racionales de área n y las progresiones aritméticas de tres cuadrados con diferencia constante n.*

Demostración. Sean $a, b, c \in \mathbb{Q}$ tales que $(ab)/2 = n$ y $a^2 + b^2 = c^2$. Sumando o restando 4 veces la primera ecuación a la segunda obtenemos $(a \pm b)^2 = c^2 \pm 4n$, y dividiendo entre 4 nos queda

$$\left(\frac{c}{2}\right)^2 \pm n = \left(\frac{a \pm b}{2}\right)^2.$$

Recíprocamente, si $s^2 - r^2 = t^2 - s^2 = n$, para ciertos números racionales r, s, t, se tiene que $t^2 - r^2 = 2n$ y $t^2 + r^2 = 2s^2$. Escogemos $a = t - r$, $b = t + r$, $c = 2s$. Tenemos que

$$\frac{ab}{2} = \frac{t^2 - r^2}{2} = n \quad \text{y} \quad (t-r)^2 + (t+r)^2 = 2(t^2 + r^2) = 4s^2 = (2s)^2.$$

Entonces los conjuntos

$$A = \{(a,b,c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2, (1/2)ab = n\} \quad \text{y} \quad B = \{(r,s,t) \in \mathbb{Q}^3 : s^2 - r^2 = t^2 - s^2 = n\}$$

están en correspondencia mediante las aplicaciones

$$\begin{array}{ll} f : A \to B & g : B \to A \\ (a,b,c) \mapsto ((b-a)/2, c/2, (b+a)/2) & (r,s,t) \mapsto (t-r, t+r, 2s). \end{array} \tag{1.19}$$

Además se verifica que $f \circ g = id_B$ y $g \circ f = id_A$. Por lo tanto f es una aplicación biyectiva.

□

Ejemplo 1.12. Para $n = 6$, tenemos la terna pitagórica $(3, 4, 5)$, cuya imagen por la aplicación f de (1.19) es $(1/2, 5/2, 7/2)$, lo cual quiere decir que $(1/4, 25/4, 49/4)$ es una progresión aritmética de tres cuadrados cuya diferencia constante es 6.

Una vez el emperador Federico II visitó Pisa, Leonardo, también conocido como Fibonacci fue invitado a su corte y se sabe que Fibonacci fue retado a encontrar tres cuadrados racionales en progresión aritmética con diferencia común 5. La respuesta que encontró fue la siguiente

$$\left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2, \quad \left(\frac{41}{2}\right)^2 + 5 = \left(\frac{49}{12}\right)^2.$$

Fibonacci en su libro Liber Quadratorum en 1225 llamó *congruum* a los enteros n, para los que existe un racional x tal que $x^2 - n$ y $x^2 + n$ son cuadrados, este es el origen del nombre *número congruente*.

Proposición 1.13 (Fibonacci). *Un entero positivo n es un número congruente si y solo si existen enteros positivos a, b con $a > b$ tales que entre los cuatro números a, b, $a+b$, $a-b$ tres son cuadrados y el cuarto es n por un cuadrado.*

Demostración. Si n es congruente, tenemos que $\beta^2 \pm n$ son cuadrados para cierto $\beta \in \mathbb{Q}$. Podemos escribir $\beta = c/d$ y escogiendo $b = nd^2$, $a = c^2$, se verifica que $a, a + b$ y $a - b$ son cuadrados.
Recíprocamente, el triángulo rectángulo formado por los catetos $2ab$ y $a^2 - b^2$ y la hipotenusa $a^2 + b^2$, tiene área $ab(a + b)(a - b)$ que es por tanto un número congruente pero no es libre de cuadrados. Por lo visto anteriormente el correspondiente número libre de cuadrados es un número congruente.

□

Teorema 1.14. *El producto de cuatro enteros positivos distintos que forman una progresión aritmética no es un cuadrado, es decir, no hay $a, d, x \in \mathbb{Z}^+$ de forma que $a(a+d)(a+2d)(a+3d) = x^2$.*

Demostración. Supongamos por reducción al absurdo que existen $a, d, x \in \mathbb{Z}^+$ donde $a(a+d)(a+2d)(a+3d) = x^2$. Podemos suponer que a y d son coprimos, pues en caso contrario podríamos dividir la ecuación por $\text{mcd}(a,d)^4$. Tenemos que

$$x^2 = a(a+3d)(a+d)(a+2d) = (a^2+3ad)(a^2+3ad+2d^2) = (a^2+3ad+d^2)^2 - d^4.$$

Sea p un número primo tal que $p \mid (a^2+3ad+d^2)$ y $p \mid a^2$, en particular $p \mid a$, y como $p \mid (a^2+3ad+d^2)$, entonces $p \mid (a^2+3ad+d^2-(3d+a)a)$. Concluimos que p divide a a y d contradiciendo que a y d son coprimos. Esto significa que $(x, d^2, a^2+3ad+d^2)$ es una terna pitagórica primitiva.
Si suponemos que d es par, usando la parametrización encontrada en el Teorema 1.4, existen u,v con u par y v impar coprimos tales que $d^2 = 2uv$ y $a^2+3ad+d^2 = u^2+v^2$, es decir, $(u/2)v = (d/2)^2$. De aquí por el Lema 1.5 (a) existen s y t coprimos tales que $u = 2s^2$ y $v = t^2$ se sigue que

$$\left(a + \frac{3d}{2}\right)^2 = a^2 + 3ad + d^2 + \frac{5}{4}d^2 = 4s^2 + t^4 + 5s^2t^2 = (s^2+t^2)(4s^2+t^2).$$

Por el Lema 1.5 (d) $\text{mcd}(s^2+t^2, 4s^2+t^2) = 1$. Aplicamos el Lema 1.5 (a) de forma que para ciertos m, n enteros se verifica $n^2 = s^2+t^2$ y $m^2 = s^2+4t^2$, contradiciendo el Teorema 1.10. Supongamos que d es impar, de la parametrización dada en el Teorema 1.4 existen enteros coprimos u, v tales que $d^2 = v^2 - u^2$ y $a^3+3ad+d^2 = v^2+u^2$. Tenemos que

$$(2a+3d)^2 = 4(a^2+3ad+d^2) + 5d^2 = (4v^2+4u^2) + (5v^2-5u^2) = 9v^2 - u^2.$$

Esto significa que $(u, 2a+3d, 3v)$ es una terna pitagórica. Por el Lema 1.5 (d), se tendrá que 3 divide a u y $2a+3d$ y

$$(v-u)\left(v-\frac{u}{3}\right)\left(v+\frac{u}{3}\right)(v+u) = (v^2-u^2)\left(\frac{9v^2-u^2}{9}\right) = \left(\frac{d(2a+3d)}{3}\right)^2.$$

Por lo tanto tenemos cuatro enteros distintos en progresión aritmética cuyo producto es un cuadrado, sin embargo tienen diferencia constante dos a dos igual a $2u/3$ que es par, contradiciendo así la primera parte de la prueba.

□

Corolario 1.15. *No existen cuatro cuadrados racionales en progresión aritmética.*

Demostración. Supongamos que existen cuatro racionales cuadrados en progresión aritmética, entonces podríamos conseguir cuatro enteros cuadrados en progresión aritmética y su producto es un cuadrado contradradiciendo el Teorema 1.14

□

Definición 1.16. *Sean $a, p \in \mathbb{Z}, p$ primo. Definimos el simbolo de Legendre como:*

$$\left(\frac{a}{\bar{p}}\right) = \begin{cases} 0, & si\ a \equiv 0 \mod p \\ 1, & si\ x^2 \equiv a \mod p\ tiene\ solución \\ -1, & si\ x^2 \equiv a \mod p\ no\ tiene\ solución \end{cases}$$

Lema 1.17. *Sea p un entero primo impar entonces*

$$\left(\frac{-1}{\bar{p}}\right) \equiv (-1)^{\frac{p-1}{2}} \mod p.$$
$$\left(\frac{2}{\bar{p}}\right) \equiv (-1)^{\frac{p^2-1}{8}} \mod p.$$

La demostración de este lema se puede encontrar, por ejemplo, en el Theorem 9-5 de [1]. Como consecuencia directa se obtiene el siguiente corolario.

Corolario 1.18. *Si $p \equiv 3$ mód 8 con p número primo entonces $x^2 \equiv -1$ mód p y $x^2 \equiv 2$ mód p no tienen solución.*

Haciendo uso de estos resultados a continuación veremos una familia de números no congruentes.

Teorema 1.19. *Sea p número primo donde $p \equiv 3$ mód 8, entonces p no es un número congruente.*

Demostración. Supongamos que p es un número congruente. Entonces por el Teorema 1.11 existe una terna de racionales positivos x_i, que podemos escribir con denominador común q positivo,

$$x_1 = \frac{m_1}{q}, \quad x_2 = \frac{m_2}{q}, \quad x_3 = \frac{m_3}{q},$$

satisfaciendo $x_2^2 - p = x_1^2$, $x_2^2 + p = x_3^2$. De entre todas estas ternas de números racionales, elegimos aquella en las que q es mínimo. Se tiene que si $\mathrm{mcd}(m_1, m_2, m_3) = n$, sabemos que p es congruente si y solo si p/n^2 lo es. Escribiendo $p_i = m_i/n$, entonces

$$y_1 := \frac{p_1}{q}, \quad y_2 := \frac{p_2}{q}, \quad y_3 := \frac{p_3}{q},$$

verifican $y_2^2 - p/n^2 = y_1^2$, $y_2^2 + p/n^2 = y_3^2$, donde $\mathrm{mcd}(p_1, p_2, p_3) = 1$. Se cumple

$$\frac{2pq^2}{n^2} = p_3^2 - p_1^2, \quad 2p_2^2 = p_1^2 + p_3^2. \tag{1.20}$$

Dado que $p_3^2 - p_1^2$ es entero, tenemos que $n^2 \mid 2pq^2$. Si $n = 1$, entonces $n^2 \mid q^2$. Si $n > 1$, claramente n^2 no divide a $2p$ ya que p es un número primo impar, de donde $n^2 \mid q^2$.

Además, tomando la segunda ecuación en (1.20), podemos concluir que p_1, p_3 son coprimos, ya que si $l \mid p_1$ y $l \mid p_3$, entonces $l^2 \mid 2p_2^2$ y aplicando el Lema 1.6 (b), concluimos que $l \mid p_2$, sin embargo, $\mathrm{mcd}(p_1, p_2, p_3) = 1$.

Pasando la ecuación $2p_2^2 = p_1^2 + p_3^2$ a mód 2, deducimos que $p_1 \equiv p_3$ mód 2, por lo que aplicando el Lema 1.5 (c) concluimos que

$$t_1 = \frac{p_3 + p_1}{2}, \quad t_3 = \frac{p_3 - p_1}{2} \in \mathbb{Z},$$

donde t_1, t_3 son coprimos. Podemos entonces reescribir (1.20) como

$$p\left(\frac{q}{n}\right)^2 = 2t_1t_3, \quad p_2^2 = t_1^2 + t_3^2.$$

Al ser t_1, t_3 coprimos, $\mathrm{mcd}(t_1, t_3, p_2) = 1$, de donde (t_1, t_3, p_2) es una terna pitagórica primitiva. Del Teorema 1.4, tenemos que $(t_1, t_3, p_2) = (a^2 - b^2, 2ab, a^2 + b^2)$ para ciertos a, b coprimos, donde $a \not\equiv b$ mód 2, de modo que

$$p\left(\frac{q}{n}\right)^2 = 2t_1t_3 = 4ab(a+b)(a-b).$$

Dado que p es un número primo impar, de la anterior expresión deducimos que $4 \mid (q/n)^2$, es decir

$$p\left(\frac{q}{2n}\right)^2 = ab(a+b)(a-b). \tag{1.21}$$

Como a y b son coprimos y $a \not\equiv b$ mód 2, por el Lema 1.5 (c), se tiene que $\mathrm{mcd}(a+b, a-b) = 1$. Además $\mathrm{mcd}(a, a+b) = \mathrm{mcd}(a, a+b-a) = \mathrm{mcd}(a, b) = 1$. Análogamente, podemos concluir que los enteros a, b, $a+b$, $a-b$ son coprimos dos a dos. Ahora aplicando el Lema 1.5 (b) sobre la ecuación (1.21), se pueden presentar cuatro casos:

$$\begin{aligned}
&\text{caso 1: } a = pf^2, b = g^2, \ a+b = h^2, \ a-b = k^2,\\
&\text{caso 2: } a = f^2, \ b = pg^2, a+b = h^2, \ a-b = k^2,\\
&\text{caso 3: } a = f^2, \ b = g^2, \ a+b = ph^2, a-b = k^2,\\
&\text{caso 4: } a = f^2, \ b = g^2, \ a+b = h^2, \ a-b = pk^2,
\end{aligned}$$

con f, g, h, k enteros. En el caso 2,

$$z_1 \coloneqq \frac{k}{g}, \quad z_2 \coloneqq \frac{f}{g}, \quad z_3 \coloneqq \frac{h}{g},$$

cumplen $z_2^2 - p = z_1^2,\ z_2^2 + p = z_3^2$, pero

$$pq^2 = 4n^2ab(a+b)(a-b) = 4n^2f^2\left(pg^2\right)h^2k^2$$

de donde se deduce que $pg^2 < pq^2$ y por ello que $g < q$, pero esto contradice la minimalidad de q.

Para el caso 1, tenemos que $(a-b)(a+b) = h^2k^2$, es decir, $a^2 = b^2 + (hk)^2$, y además $\text{mcd}(a,b) = 1$ por lo que (b, hk, a) es una terna pitagórica primitiva. Empleando la parametrización obtenida en el Teorema 1.4, llegamos a que existen $r, s \in \mathbb{Z}^+$ coprimos tales que $a = (r^2 + s^2)$, además

$$2pf^2 = 2a = 2(r^2 + s^2) = (r+s)^2 + (r-s)^2,$$

si $\alpha \coloneqq (r+s)$ y $\beta \coloneqq (r-s)$. Entonces $0 \equiv \alpha^2 + \beta^2$ mód p, esto significa que $\alpha^2 \equiv -\beta^2$ mód p. Podría ser que $\alpha \equiv \beta \equiv 0$ mód p que es la solución trivial, pero por el Lema 1.5 (c), $\text{mcd}(r+s, r-s)$ es 1 o 2, por lo tanto p primo impar no divide a α y β.

Si existiese otra solución entonces -1 es un cuadrado en $\mathbb{Z}_p$, sin embargo, esto no puede ocurrir por el Corolario 1.18.

En el caso 3, vemos que $f^2 + g^2 = ph^2$ y llegamos a que $f^2 + g^2 \equiv 0$ mód p, por los mismos motivos que en el caso 1 obtenemos un absurdo.

En el caso 4, se tiene que $f^2 + g^2 = h^2$, de donde (f, g, h) es una terna pitagórica primitiva y por la parametrización del Teorema 1.4 existen $r, s \in \mathbb{Z}^+$ tales que $(f, g) = (r^2 - s^2, 2rs)$ o bien $(f, g) = (2rs, r^2 - s^2)$. Además $f^2 - g^2 = pk^2$, por lo que se tiene

$$\pm pk^2 = (r^2 - s^2)^2 - (2rs)^2 = (r^2 - 3s^2)^2 - 2(2s^2)^2,$$

si $\gamma \coloneqq (r^2 - 3s^2)$ y a $\delta \coloneqq 2s^2$. Entonces llegamos a que $0 \equiv \gamma^2 - 2\delta^2$ mód p.
Si $p \mid 2s^2$, del Lema de Euclides, al ser p un número primo impar, se tiene que $p \mid s^2$. Si además, $p \mid (r^2 - 3s^2)$, entonces $p \mid (r^2 - 3s^2 + 3s^2)$, pero entonces p divide tanto a r como a s contradiciendo que $\text{mcd}(r, s) = 1$. Concluimos que no puede ser la solución trivial $\gamma \equiv \delta \equiv 0$ mód p.

Si existiese otra solución entonces 2 es un cuadrado en $\mathbb{Z}_p$ llegando a un absurdo por el Corolario 1.18.

□

1.3. Puntos en Curvas Cúbicas

El problema del número congruente también es equivalente a encontrar los puntos racionales de una cierta familia de curvas cúbicas. Esta forma equivalente del problema es una de las más interesantes, ya que seremos capaces de aplicar algunos resultados que presentaremos en el Capítulo 2 sobre estas curvas.

Teorema 1.20. *Sea n entero positivo, entonces existe una aplicación biyectiva entre los siguientes conjuntos*

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

Demostración. Consideremos las correspondencias

$$\begin{aligned} f : A &\longrightarrow B & g : B &\longrightarrow A \\ (a,b,c) &\mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) & (x,y) &\mapsto \left(\frac{x^2-n^2}{y}, \frac{2nx}{y}, \frac{x^2+n^2}{y}\right). \end{aligned}$$

Primero demostramos que f es una aplicación. Sea $(a,b,c) \in A$, entonces

$$\left(\frac{nb}{c-a}\right)^3 - n^2\left(\frac{nb}{c-a}\right) = n^3 b\left(\frac{b^2-(c-a)^2}{(c-a)^3}\right) = n^3 b\left(\frac{b^2-a^2-c^2+2ac}{(c-a)^3}\right).$$

Usando que $a^2+b^2 = c^2$ y que $ab = 2n$ obtenemos

$$n^3 b\left(\frac{2ac-2a^2}{(c-a)^3}\right) = 4n^4\left(\frac{c-a}{(c-a)^3}\right) = \left(\frac{2n^2}{c-a}\right)^2,$$

y concluimos que f es aplicación. Además g también lo es ya que si $(x,y) \in B$ entonces

$$\left(\frac{x^2-n^2}{y}\right)^2 + \left(\frac{2nx}{y}\right)^2 = \left(\frac{x^4+2n^2x^2+n^4}{y^2}\right) = \left(\frac{x^2+n^2}{y}\right)^2,$$

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

Además $f \circ g = id_B$ y $g \circ f = id_A$, por lo que f es una aplicación biyectiva. □

Ejemplo 1.21. Si $a,d,x \in \mathbb{Z}^+$, entonces $a(a+d)(a+2d)(a+3d) = x^2$ no tiene solución por el Teorema 1.14 , si dividimos por a^4 y con el cambio de variable $y' = x/a^2$, $x' = d/a$ obtenemos que $y'^2 = (1+x')(1+2x')(1+3x')$, es decir, $6^2y'^2 = 6^3(x'+1)(x'+1/2)(x'+1/3)$, con el cambio de variable $v = 6y'$, $w = 6x'$, nos queda que $v^2 = (w+2)(w+3)(w+6)$ y finalmente mediante $u = w+4$, llegamos a la curva cúbica $v^2 = (u-1)(u^2-4)$.

Al final, $v = 6x/a^2$, $u = 6(d/a) + 4$, pero como $a, x, d \in \mathbb{Z}^+$, de existir una progresión aritmética de cuatro cuadrados, existiría un punto racional (u, v) con $u > 4$ y $v > 0$ en la curva $v^2 = (u-1)(u^2-4)$, es decir, también podemos entender este problema como puntos racionales de una cierta curva. Nótese que los siguientes puntos racionales

$$(1,0), \quad (2,0), \quad (-2,0), \quad (0,2), \quad (0,-2), \quad (4,6), \quad (4,-6),$$

están en dicha curva, sin embargo, no se corresponden con una solución de $a(a+d)(a+2d)(a+3d) = x^2$.

Ahora podemos generalizar el resultado que vimos en el Corolario 1.8. Consideramos la ecuación

$$x^4 - n^2y^4 = z^2 \tag{1.22}$$

Proposición 1.22. *Sea $n \in \mathbb{N}$, si la ecuación $x^4 - n^2y^4 = z^2$ tiene una solución entera donde $xyz \neq 0$, entonces n es un número congruente.*

Demostración. Consideremos $P = (x^2/y^2, xz/y^3)$, dado que $xyz \neq 0$, está claro que P es distinto de $(0,0)$, $(n,0)$, $(-n,0)$. Teniendo en cuenta que se verifica que $x^4 - n^2y^4 = z^2$, al multiplicar la anterior ecuación por x^2/y^6, se llega a que

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

Aplicando el Teorema 1.20 concluimos que n es un número congruente.

□

En 1878, el matemático francés Desboves, encontró soluciones de (1.22) haciendo uso de la siguiente expresión algebraica

$$\left(y^2+2xy-x^2\right)^4+\left(2x^3y+x^2y^2\right)(2x+2y)^4 = \left(x^4+y^4+10x^2y^2+4xy^3+12x^3y\right)^2. \tag{1.23}$$

Corolario 1.23. *Sea $m \in \mathbb{N}$ entonces $n = m(1+4m^2)$ es un número congruente.*

Demostración. Si en (1.23), tomamos $x = 1+4m^2$, $y = -8m^2$, llegamos a que

$$\begin{aligned}(-1-24m^2-16m^4)^4 - 16m^2(1+4m^2)^2(2(1-4m^2))^4 \\ = (1-80m^2-416m^4-1280m^6+256m^8)^2.\end{aligned}$$

Por lo que usando la Proposición 1.22, llegamos a que $4m(4m^2+1)$ es un número congruente, en particular, dado que 4 es un cuadrado, $m(4m^2+1)$ es un número congruente.

□

Ejemplo 1.24. Si tomamos $m = 23660^2$ en el Corolario 1.23, llegamos a un número cuya parte libre de cuadrados resulta ser el número primo 1119543881, que es por tanto un número congruente.

Hasta ahora hemos podido comprobar que el problema acepta varias formas equivalentes, las cuales podemos resumir en la siguiente proposición:

Proposición 1.25. *Sea $n \in \mathbb{Z}^+$. Son equivalentes:*

- *Existe un triángulo rectángulo de lados racionales A, B, C y área n.*
- *Existen cuadrados racionales α^2, β^2 y γ^2 en progresión aritmética de razón n.*
- *La curva $\mathcal{C}_n : Y^2 = X^3 - n^2X$ tiene un punto racional (x, y) con $y \neq 0$.*

Para ejemplificar este resultado y las correspondencias dadas en los Teoremas 1.20 y 1.11, en la Tabla 1.1 se recogen algunos ejemplos de números congruentes:

n	(A, B, C)	$(\alpha^2, \beta^2, \gamma^2)$	(x, y)
6	(3, 4, 5)	$\left(\left(\frac{1}{2}\right)^2, \left(\frac{5}{2}\right)^2, \left(\frac{7}{2}\right)^2\right)$	(12, 36)
7	$\left(\frac{35}{12}, \frac{24}{5}, \frac{337}{60}\right)$	$\left(\left(\frac{113}{120}\right)^2, \left(\frac{337}{120}\right)^2, \left(\frac{463}{120}\right)^2\right)$	$\left(\frac{112}{9}, \frac{980}{27}\right)$
13	$\left(\frac{780}{323}, \frac{323}{30}, \frac{106921}{4913}\right)$	$\left(\left(\frac{80929}{19380}\right)^2, \left(\frac{106921}{19380}\right)^2, \left(\frac{127729}{19380}\right)^2\right)$	$\left(\frac{4693}{289}, \frac{192660}{4913}\right)$
210	(20, 21, 29)	$\left(\left(\frac{1}{2}\right)^2, \left(\frac{29}{2}\right)^2, \left(\frac{41}{2}\right)^2\right)$	(490, 9800)

Tabla 1.1.

Ejemplo 1.26. La terna (3,4,5) se corresponde, por el Teorema 1.20, con el punto (12,36) de la curva $\mathcal{C} : y^2 = x^3 - 36x$. La recta tangente a la curva en este punto es $y = (11/2)x - 30$. Tal y como se puede observar en la Figura 1.1 esta recta corta a la curva $\mathcal{C}$ en un nuevo punto, en efecto, sustituyendo en la ecuación de la curva obtenemos $(x - 12)^2(x - 25/4) = 0$, es decir, (25/4,35/8) es un nuevo punto racional de la curva y se corresponde por el Teorema 1.20, con el triángulo rectángulo asociado a la terna pitagórica (7/10, 120/7, 1201/70), el cual tiene lados racionales y de nuevo área 6.

Usando el Teorema 1.11 la nueva terna pitagórica se corresponde con una nueva progresión aritmética de tres cuadrados racionales, que es

$$\left(\frac{1151}{140}\right)^2, \left(\frac{1201}{140}\right)^2, \left(\frac{1249}{140}\right)^2. \tag{1.24}$$

Comenzando con un triángulo rectángulo racional de área 6 hemos construido un nuevo triángulo rectángulo racional con la misma área y a partir de una progresión aritmética de tres cuadrados racionales con diferencia común 6 hemos construido una nueva que mantiene la misma diferencia común, esta forma de construir una nueva solución a partir de una previa no es nada evidente, a no ser que veamos las soluciones del problema como puntos en una curva cúbica.

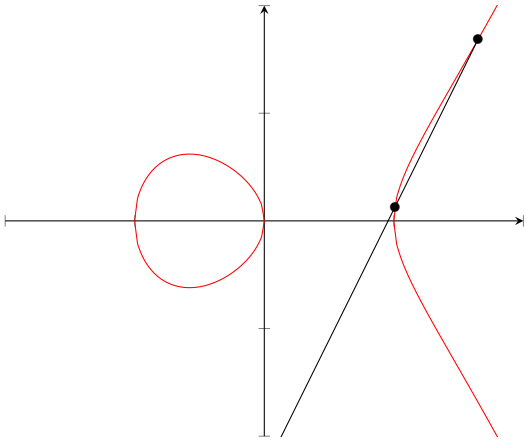


Figura 1.1.

2

Curvas elípticas

En este capítulo se introducirán varios conceptos de la teoría de curvas elípticas. También se proporcionará una prueba del Teorema de Nagell-Lutz, y emplearemos este para dar una última caracterización de los números congruentes. Para ello nos hemos basado en [7], [12], [2], [15], [16] y [3] .

2.1. Introducción a las curvas elípticas

Sean $\mathbb{K}$ cuerpo y $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{K}^3 \backslash (0,0,0)$, se define la siguiente relación de equivalencia:

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2), \text{ si y sólo si existe } \lambda \in \mathbb{K}\backslash\{0\} \text{ tal que } (x_1, y_1, z_1) = \lambda(x_2, y_2, z_2). \tag{2.1}$$

La clase de (x, y, z) se denota como $(x : y : z)$, es decir

$$(x : y : z) = \{(x', y', z') \in \mathbb{K}^3 \backslash (0,0,0) : (x, y, z) = \lambda(x', y', z'), \lambda \in \mathbb{K}\backslash\{0\}\}.$$

Definición 2.1. *El plano proyectivo sobre $\mathbb{K}$ se define como el conjunto de las clases de equivalencia dadas en (2.1) y se denota por $\mathbb{PK}^2$*

$$\mathbb{PK}^2 = \{(x : y : z) : (x, y, z) \in \mathbb{K}^3 \backslash (0,0,0)\}.$$

El plano proyectivo está en correspondencia con las rectas que pasan por el origen en $\mathbb{K}^3$, donde las rectas que están contenidas en el plano $z = 0$ son los que llamaremos puntos del infinito, por lo que en realidad lo que estamos haciendo es completar el plano afín con los puntos del infinito. Nótese además que el punto (0:0:0) no existe.

Definición 2.2. *Sea $F(x_1, \ldots, x_m) \in \mathbb{K}[x_1, \ldots, x_m]$, diremos que F es un polinomio homogéneo de grado n, si todos los términos son de grado n.*

Lema 2.3. *Sea $F(x_1,\ldots,x_m)\in\mathbb{K}[x_1,\ldots,x_m]$ un polinomio homogéneo de grado n y $\lambda\in\mathbb{K}$, entonces $F(\lambda x_1,\ldots,\lambda x_m)=\lambda^n F(x_1,\ldots,x_m)$.*

Demostración. Sea $F\left(x_1,\ldots,x_m\right)=\sum_{|\alpha|=n}a_\alpha x_1^{\alpha_1}\ldots x_m^{\alpha_m}$, donde $\alpha=(\alpha_1,\ldots,\alpha_m)$ y $|\alpha|=\sum_{i=1}^m\alpha_i$. Evaluando en $(\lambda x_1,\ldots,\lambda x_m)$, con $\lambda\in\mathbb{K}$:

$$F\left(\lambda x_1,\ldots,\lambda x_m\right)=\sum_{|\alpha|=n}a_\alpha(\lambda x_1)^{\alpha_1}\ldots(\lambda x_m)^{\alpha_m}=\sum_{|\alpha|=n}a_\alpha\lambda^n\,x_1^{\alpha_1}\ldots x_m^{\alpha_m}=$$
$$=\lambda^n\sum_{|\alpha|=n}a_\alpha x_1^{\alpha_1}\ldots x_m^{\alpha_m}=\lambda^n F\left(x_1,\ldots,x_m\right).$$

□

Lema 2.4 (Euler). *Sea $F(x,y,z)$ un polinomio homogéneo de grado n, entonces se tiene que*

$$x\frac{\partial F}{\partial x}+y\frac{\partial F}{\partial y}+z\frac{\partial F}{\partial z}=nF. \tag{2.2}$$

Demostración. Por ser F homogéneo de grado n se tiene que $F(\lambda x,\lambda y,\lambda z)=\lambda^n F(x,y,z)$, podemos derivar a ambos lados respecto de λ y escribiendo $\mathbf{x}=(x,y,z)$ obtenemos

$$\frac{\partial F(\lambda\mathbf{x})}{\partial\lambda}=\frac{\partial}{\partial\lambda}(\lambda^n F(\mathbf{x})),$$

aplicando la regla de la cadena en el lado izquierdo de la ecuación,

$$\frac{\partial F(\lambda\mathbf{x})}{\partial x}\frac{\partial}{\partial\lambda}(\lambda x)+\frac{\partial F(\lambda\mathbf{x})}{\partial y}\frac{\partial}{\partial\lambda}(\lambda y)+\frac{\partial F(\lambda\mathbf{x})}{\partial z}\frac{\partial}{\partial\lambda}(\lambda z),$$

mientras que en el lado derecho nos queda $n\lambda^{n-1}F(\mathbf{x})$, finalmente tomando $\lambda=1$ llegamos a la Ecuación (2.2)

□

Definición 2.5. *Se llama curva algebraica proyectiva de grado n a todo conjunto de la forma $\mathcal{C}_F=\{(a:b:c)\in\mathbb{PK}^2:F(a,b,c)=0\}$, donde $F(x,y,z)\in\mathbb{K}[x,y,z]$ es un polinomio homogéneo de grado n. Además, diremos que $\mathcal{C}_F$ es una cúbica proyectiva cuando $n=3$.*

Dado un polinomio $f(x,y)=\sum_{finita}a_{ij}x^iy^j\in\mathbb{K}[x,y]$ de grado d, podemos asociarle un polinomio homogéneo, mediante un proceso que llamamos homogeneización

$$F(x,y,z)=z^d f\left(\frac{x}{z},\frac{y}{z}\right)=\sum_{\text{finita}}z^d a_{ij}\left(\frac{x}{z}\right)^i\left(\frac{y}{z}\right)^j=\sum_{\text{finita}}a_{ij}x^iy^jz^{d-i-j}.$$

Definición 2.6. *Diremos que un punto P de una curva proyectiva $\mathcal{C}_F$ es singular si todas las derivadas parciales se anulan en ese punto, es decir, $F_x(P) = F_y(P) = F_z(P) = 0$. Si una curva no contiene puntos singulares, se dice que es una curva lisa.*

Definición 2.7. *Una curva elíptica es una curva proyectiva lisa en $\mathbb{PC}^2$.*

Ejemplo 2.8. Si $f(x, y) = y^2 - x^3 + n^2 x$ es la curva asociada al número congruente n, entonces su homogeneización es $F(x, y, z) = y^2 z - x^3 + n^2 x z^2$ de grado 3, si calculamos sus derivadas parciales e igualamos a 0 obtenemos

$$\begin{cases} F_x = -3x^2 + n^2 z^2 = 0 \\ F_y = 2yz = 0 \\ F_z = y^2 + 2n^2 xz = 0. \end{cases}$$

La unica solución de este sistema es (0,0,0), la cual no se corresponde con un punto en el plano proyectivo. Por todo esto concluimos que la curva proyectiva asociada al número congruente n es una curva elíptica.

Sea ϕ un isomorfismo lineal en $\mathbb{K}^3$

$$\begin{aligned} \phi : \quad & \mathbb{K}^3 \longrightarrow \mathbb{K}^3 \\ & (x, y, z) \longmapsto \phi(x, y, z) = A \begin{pmatrix} x \\ y \\ z \end{pmatrix} =: (X, Y, Z), \end{aligned}$$

donde $A \in \mathcal{M}_{3\times 3}(\mathbb{K})$ es no singular.

Definición 2.9. *Se llama transformación proyectiva en $\mathbb{PK}^2$ a toda a aplicación ϕ^* inducida por ϕ como sigue:*

$$\begin{aligned} \phi^* : \quad & \mathbb{PK}^2 \longrightarrow \mathbb{PK}^2 \\ & (x : y : z) \longmapsto \phi^*(x : y : z) = \phi(x, y, z) = (X : Y : Z). \end{aligned}$$

Definición 2.10. *Diremos que dos curvas proyectivas $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{PK}^2$ son proyectivamente equivalentes cuando existen un isomorfismo lineal ϕ en $\mathbb{K}^3$ y un escalar $\lambda \in \mathbb{K}\backslash\{0\}$ tales que $F(x, y, z) = \lambda G(\phi(x, y, z))$. En tal caso, se denota por $\mathcal{C}_F \cong \mathcal{C}_G$.*

Gran parte del trabajo realizado en el Capítulo 1 dependía de la parametrización encontrada en el Teorema 1.4, la cual encontramos mediante el estudio de los puntos racionales de una curva, en ese caso de la circunferencia unidad, de hecho fuimos capaces de encontrar una parametrización que nos permitía encontrar todos los puntos racionales. La pregunta natural es si podemos hacer algo similar para encontrar los puntos racionales de la curva asociada a un cierto número congruente.

Definición 2.11. *Sea f un polinomio irreducible en $\mathbb{K}^2$, la curva asociada a f es racional si existen funciones racionales $x(t),\ y(t)$ verificando*

(a) Salvo para un número finito de valores de t, las funciones $x(t),\ y(t)$ satisfacen $f(x(t), y(t)) = 0$.
(b) Salvo por un número finito de excepciones, para cualquier punto (x, y) satisfaciendo $f(x, y) = 0$ existe un único t para el cual $x = x(t),\ y = y(t)$.

Ejemplo 2.12. Si $f(x, y) = x^2 + y^2 - 1$, donde f es irreducible, encontramos en el Teorema 1.4 la siguiente parametrización racional

$$x(t) = \frac{1 - t^2}{1 + t^2}, \quad y(t) = \frac{2t}{1 + t^2},$$

que parametrizaba a todos los puntos de la circunferencia salvo (-1,0), por lo que la circunferencia unidad es racional.

Se puede extender la idea de curva racional al plano proyectivo de la siguiente forma:

Definición 2.13. *Sea $\mathcal{C}$ una curva proyectiva definida por un polinomio homogéneo $F(x, y, z) \in \mathbb{K}[x, y, z]$ de grado $n \geq 1$. Decimos que $\mathcal{C}$ es racional si existen $f, g, h \in \mathbb{K}[u, v]$ de grado $m \geq 1$ tales que $F(f, g, h) = 0$ idénticamente.*

Teorema 2.14. *Sean $\mathbb{K}$ un cuerpo algebraicamente cerrado y de característica 0 y $\mathcal{C}_F$ una curva proyectiva lisa donde $F(x, y, z) \in \mathbb{K}[x, y, z]$ de grado $n \geq 1$. Si $\mathcal{C}_F$ es racional entonces $n \leq 2$.*

Demostración. Supongamos que existen $f, g, h \in \mathbb{K}[u, v]$ homogéneos de grado $m \geq 1$ tales que $F(f, g, h) = 0$ y $\mathrm{mcd}(f, g, h) = 1$. Derivando respecto de u, v obtenemos el siguiente sistema matricial.

$$\begin{pmatrix} f_u & g_u & h_u \\ f_v & g_v & h_v \end{pmatrix} \begin{pmatrix} F_x(f, g, h) \\ F_y(f, g, h) \\ F_z(f, g, h) \end{pmatrix} = 0.$$

Vamos a demostrar que la matriz 2x3 anterior tiene rango 2, en caso contrario se tendría que $f_u g_v - f_v g_u = 0$. Además por el Lema de Euler (Lema 2.4)

$$mf = uf_u + vf_v, \quad mg = ug_u + vg_v.$$

Por lo tanto

$$0 = u(f_u g_v - f_v g_u) = m(f g_v - g f_v). \tag{2.3}$$

Como F es un polinomio homogéneo, podemos escribir

$$F(x,y,z) = x \cdot G(x,y,z) + y \cdot H(x,y,z) + c \cdot z^n,$$

para ciertos polinomios $G, H \in \mathbb{K}[x,y,z]$ de grado $n-1$ o nulos y $c \in \mathbb{K}$. Si $c \neq 0$ tenemos que

$$0 = F(f,g,h) = f \cdot G(f,g,h) + g \cdot H(f,g,h) + c \cdot h^n.$$

Sea $p := mcd(f,g)$. Si $p = 1$, ya estaría. Si $p \neq 1$, de la anterior expresión se deduce que $p \mid h^n$, contradiciendo $\text{mcd}(f,g,h) = 1$. Si $c = 0$, sea $f' = f/p$ y $g' = g/p$, podemos ver que

$$0 = F(f,g,h) = p^n \cdot F(f',g',h).$$

Al ser $\mathbb{K}[u,v]$ un dominio de integridad y dado que $\deg(p) \geq 1$ concluimos que $F(f',g',h) = 0$ veridicando las condiciones de la Definición 2.13, por lo que podemos suponer sin pérdida de generalidad que f y g son coprimos.

Tenemos que $m \neq 0$, así que de (2.3) se obtiene que $f \mid f_v$, pero $\deg(f_v) < \deg(f)$, entonces $f_v = 0$ y por el mismo razonamiento concluimos $f_u = 0$. Sin embargo, como $\mathbb{K}$ es un cuerpo de característica 0, esto solo es posible si $\deg f = 0$, lo cual es absurdo, de aquí concluimos que la matriz 2x3 tiene rango 2.

Ahora vamos a demostrar que $\text{mcd}(F_x, F_y, F_z) = 1$, en caso contrario como $\mathbb{K}$ es algebraicamente cerrado se tendría que F_x, F_y, F_z tienen un factor lineal $(u - cv)$ en común. Podemos tomar $x = f(c,1)$, $y = g(c,1)$ y $z = h(c,1)$, tenemos que $(x,y,z) \neq (0,0,0)$, pues en caso contrario f, g, h tendrían un factor común $(u - cv)$, sin embargo, $\text{mcd}(f,g,h) = 1$. Concluimos que $F_x(x,y,z) = F_y(x,y,z) = F_z(x,y,z) = 0$, de donde $(x : y : z)$ es un punto singular, lo cual es absurdo. Volviendo al sistema

$$\begin{pmatrix} f_u & g_u & h_u \\ f_v & g_v & h_v \end{pmatrix} \begin{pmatrix} P \\ Q \\ R \end{pmatrix} = 0, \tag{2.4}$$

su conjunto solución tiene dimensión 1 como subespacio del espacio vectorial $\mathbb{K}(u,v)^3$. Ahora consideramos las matrices

$$M = \begin{pmatrix} f_u & g_u & h_u \\ f_u & g_u & h_u \\ f_v & g_v & h_v \end{pmatrix} \quad \text{y} \quad N = \begin{pmatrix} f_v & g_v & h_v \\ f_u & g_u & h_u \\ f_v & g_v & h_v \end{pmatrix}.$$

Se tiene que $0 = \det M = f_u P + g_u Q + h_u R$ y $0 = \det N = f_v P + g_v Q + h_v R$, donde

$$P = \begin{vmatrix} g_u & h_u \\ g_v & h_v \end{vmatrix}, \quad Q = -\begin{vmatrix} f_u & h_u \\ f_v & h_v \end{vmatrix} \quad \text{y} \quad R = \begin{vmatrix} f_u & g_u \\ f_v & g_v \end{vmatrix}.$$

Por lo tanto hemos encontrado una solución del sistema (2.4) y como $P = F_x(f,g,h),\ Q = F_y(f,g,h),\ R = F_z(f,g,h)$ es otra solución y usando que el espacio solución tiene dimensión 1, podemos concluir que dichas soluciones son linealmente dependientes, es decir, que existe $p(u,v)/q(u,v)$ donde $p, q \in \mathbb{K}[u,v]$ son coprimos, de forma que

$$\begin{aligned} q(u,v)\,(h_u g_v - h_v g_u) &= p(u,v)F_x(f,g,h), \\ q(u,v)\,(f_u h_v - f_v h_u) &= p(u,v)F_y(f,g,h), \\ q(u,v)\,(g_u f_v - g_v f_u) &= p(u,v)F_z(f,g,h). \end{aligned} \tag{2.5}$$

Como p y q son coprimos, deducimos del Lema de Euclides que q divide a $F_x(f,g,h), F_y(f,g,h)$, y $F_z(f,g,h)$ por tanto divide a su máximo común divisor el cual es 1, deducimos por tanto que $\deg(q) = 0$. Ahora calculando el grado de la primera ecuación de (2.5) tenemos que

$$\deg(q\,(h_u g_v - h_v g_u)) = \deg\,(h_u g_v - h_v g_u) \leq 2(m-1),$$

y en el lado derecho,

$$\deg(p \cdot F_x(f,g,h)) \geq \deg F_x(f,g,h) = (n-1)m.$$

Donde la última igualdad se da porque $F(x,y,z)$ define una curva lisa y por tanto tiene que contener al menos un monomio que sea múltiplo de x. Comparando, obtenemos que $2m-2 \geq m(n-1)$, lo cual implica que $-2 \geq m(n-3)$ de donde necesariamente $n < 3$.

□

Ahora recordaremos el Teorema de Bézout.

Teorema 2.15. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado. Sean $\mathcal{C}_F, \mathcal{C}_G \subset \mathbb{PK}^2$ dos curvas proyectivas determinadas por los polinomios $F(x,y,z), G(x,y,z) \in \mathbb{K}[x,y,z]$, sin componentes en común, de grados n y m, respectivamente. Entonces, $\mathcal{C}_F$ y $\mathcal{C}_G$ tienen exactamente $n \cdot m$ puntos en común (contadas multiplicidades).*

Una demostración de este resultado se recoge en [10].

Definición 2.16. *El siguiente polinomio*

$$F(x,y,z) = a(x-\alpha z)(x-\beta z)(x-\gamma z) - y^2 z \in \mathbb{C}[x,y,z] \tag{2.6}$$

que determina una curva cúbica proyectiva $\mathcal{C}$, se denomina forma de Weierstrass de $\mathcal{C}$.

Lema 2.17. *Cualquier curva elíptica $\mathcal{C}' \subset \mathbb{PC}^2$ es proyectivamente equivalente a otra curva elíptica $\mathcal{C} \subset \mathbb{PC}^2$ que está determinada por una forma de Weierstrass.*

La demostración del Lema 2.17 se puede encontrar en el Lema 2.4 del Capítulo 2 de [9]. Gracias al Lema 2.17 podemos suponer que toda curva elíptica viene dada por una ecuación de la forma $\mathcal{C} : y^2z = x^3 + ax^2z + bxz^2 + cz^3$, que se obtiene al desarrollar la expresión en (2.6).

En la forma de Weierstrass, las curvas elípticas tienen un único punto en el infinito. En efecto, tomando $z = 0$ y sustituyendo en (2.6) obtenemos que necesariamente que $x = 0$, de donde $\mathcal{O} = (0 : 1 : 0)$ es el único punto en el infinito.

Observamos que $\mathcal{O}$ es el punto en el que intersectan todas las paralelas al eje Y. Además, es un punto racional.

El plano proyectivo resulta de completar el plano con puntos en el infinito. Por lo tanto deshomogeneizando la forma de Weierstrass de una curva elíptica $\mathcal{C}$, podemos definir el siguiente conjunto

Definición 2.18. *Dada una curva elíptica $\mathcal{C} : y^2z = x^3 + ax^2z + bxz^2 + cz^3$, y un cuerpo $\mathbb{K}$, tal que $\mathbb{K} \subseteq \mathbb{C}$, se denota por $\mathcal{C}(\mathbb{K})$ al conjunto de puntos de la curva $\mathcal{C}$ cuyas coordenadas están en $\mathbb{K}$, es decir*

$$\mathcal{C}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}.$$

Tomemos un par de puntos distintos $P, Q \in \mathcal{C}(\mathbb{C})$, gracias al Teorema de Bézout, sabemos que la recta que pasa por P y Q corta a la curva elíptica en tres puntos contando multiplicidades salvo que dicha recta sea una componente de la curva. Podemos entonces definir $P * Q$ como el tercer punto en común. En el caso particular de que $P = Q$, tomamos la recta tangente a P. La operación

$$\begin{aligned} * : \mathcal{C}(\mathbb{C}) \times \mathcal{C}(\mathbb{C}) &\longrightarrow \mathcal{C}(\mathbb{C}) \\ (P, Q) &\longmapsto P * Q \end{aligned}$$

no dota a las curvas elípticas de estructura de grupo puesto que $(\mathcal{C}(C), *)$ carece de elemento neutro. Sin embargo, sí la podemos usar para definir la siguiente operación, fijando un punto $O \in \mathcal{C}(\mathbb{C})$

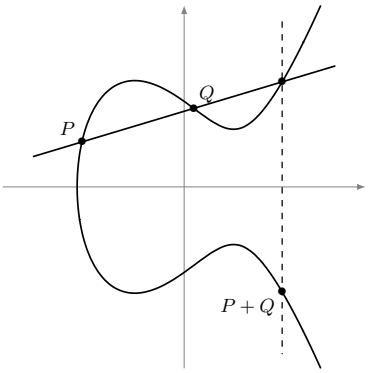
$$\begin{aligned} + : \mathcal{C}(\mathbb{C}) \times \mathcal{C}(\mathbb{C}) &\longrightarrow \mathcal{C}(\mathbb{C}) \\ (P, Q) &\longmapsto P + Q = (P * Q) * O. \end{aligned} \tag{2.7}$$

Teorema 2.19. *Sea $\mathcal{C}$ una curva elíptica, entonces $(\mathcal{C}(\mathbb{C}), +)$ es un grupo abeliano con elemento neutro O. Si además, $O \in \mathcal{C}(\mathbb{Q})$, entonces $(\mathcal{C}(\mathbb{Q}), +)$ es un subgrupo.*

El Teorema 2.19 se desvía del objetivo de esta memoria. Puede encontrarse una prueba en los Teoremas 2.10 y 2.15 del Capítulo 2 de [9] respectivamente.

Si el punto fijado en (2.7) es $O = \mathcal{O}$, la operación $+$ tiene un funcionamiento especial que simplifica los cálculos. Dados los puntos P y Q distintos de $\mathcal{O}$,

entonces para calcular $(P * Q) * \mathcal{O}$ se traza la recta paralela al eje Y que pasa por $P * Q$. Además como la curva es simétrica respecto al eje X, esto significa que $(P * Q) * \mathcal{O}$ es el simétrico con respecto al eje X de $P * Q$.



Si $P = (x, y)$, entonces $-P = (x, -y)$, ya que la recta que pasa por P y $-P$ es paralela al eje Y, intersectando a la curva en $\mathcal{O}$, de donde $P + (-P) = (P * (-P)) * \mathcal{O} = \mathcal{O} * \mathcal{O} = \mathcal{O}$.

Lema 2.20. *Un punto $P = (x, y)$ tiene orden 2 si y solo si $y = 0$.*

Demostración. Un punto es de orden 2, si y solo si, $P + P = \mathcal{O}$, o equivalentemente si $P = -P$, es decir, $(x, y) = (x, -y)$, esto solo es cierto si $y = 0$. □

Uno de los resultados más importantes de la teoría de curvas elípticas es el siguiente

Teorema 2.21 (Mordell-Weil). *Si $\mathcal{C}$ es una curva elíptica, entonces el grupo $\mathcal{C}(\mathbb{Q})$ está finitamente generado.*

La demostración de este resultado se puede encontrar en el capítulo 3 en [9]. Como $\mathcal{C}(\mathbb{Q})$ es un grupo finitamente generado entonces $\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}^r \bigoplus T$, donde T es un grupo finito conocido como el subgrupo de torsión de $\mathcal{C}(\mathbb{Q})$, el cual está formado por los elementos de orden finito. Por otro lado $r_{\mathbb{Q}}(\mathcal{C}) \coloneqq r$ es conocido como el rango de $\mathcal{C}$ sobre $\mathbb{Q}$.

2.2. Los puntos de orden finito tienen coordenadas enteras

A partir de ahora consideraremos que los coeficientes a, b, c de la forma de Weierstrass de una curva elíptica $\mathcal{C}$ son enteros, queremos demostrar que si (x, y) es un punto racional de orden finito de $\mathcal{C}$ entonces sus coordenadas son enteras.

Demostrar que (x, y) tiene coordenadas enteras es equivalente a demostrar que los denominadores de x y de y no son divisibles por ningún número primo, esta es la estrategia que vamos a seguir para demostrar este resultado.

Definición 2.22. *Para cada primo p se define el orden respecto a p de cualquier número racional z como el entero ν tal que $z = (m/n)p^\nu$, donde m, n son coprimos con p y m/n es una fracción irreducible, y lo denotaremos*

$$\operatorname{ord}_p\left(\frac{m}{n}p^\nu\right) = \nu.$$

Tenemos que p divide al denominador de un número racional si y solo si su orden es negativo, de la misma forma p divide al numerador si y solo si su orden es positivo. El orden es cero, si y solo si p no divide al denominador ni al numerador.

Proposición 2.23. *Sea (x, y) un punto racional de $\mathcal{C} : y^2 = x^3 + ax^2 + bx + c$. Si p divide al denominador de x o al denominador de y, entonces p divide al denominador de ambos. Es más, la potencia exacta que divide al denominador de x es $p^{2\nu}$ y en el caso del denominador de y es $p^{3\nu}$, para un cierto entero positivo ν.*

Demostración. Asumimos que p divide al denominador x. En el caso de que p divida al denominador de y se hace análogamente. Tenemos que

$$x = \frac{m}{np^\mu}, \quad e \quad y = \frac{u}{wp^\sigma},$$

donde $\mu > 0$, p no divide a m, n, u ni w y $\operatorname{mcd}(n, m) = \operatorname{mcd}(u, w) = 1$. Nuestro objetivo será demostrar que $\sigma > 0$. Sustituyendo en $\mathcal{C}$ obtenemos que

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Como $p \nmid u^2$ y $p \nmid w^2$ sabemos que

$$\operatorname{ord}_p\left(\frac{u^2}{w^2p^{2\sigma}}\right) = -2\sigma.$$

Además como, $\mu > 0$ y $p \nmid m$, deducimos que

$$p \nmid m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}.$$

De la misma forma, como $\operatorname{mcd}(n, m) = 1$, entonces $\operatorname{mcd}(n^3, m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}) = 1$, y también tenemos que $p \nmid n^3$, de donde

$$\operatorname{ord}_p\left(\frac{m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Entonces $2\sigma = 3\mu$. En particular $\sigma > 0$, por lo que p divide al denominador de y. También deducimos que $2 \mid \mu$ y $3 \mid \sigma$, por lo que $\mu = 2\nu$ y $\sigma = 3\nu$ para algún entero ν.

□

Se denota por $\mathcal{C}(p^\nu)$ al conjunto de puntos racionales (x, y) de $\mathcal{C}$ de manera que $p^{2\nu}$ divide al denominador de x y $p^{3\nu}$ divide al denominador de y, junto con el punto $\mathcal{O}$. Es decir,

$$\mathcal{C}(p^\nu) = \{(x, y) \in \mathcal{C}(\mathbb{Q}) : \mathrm{ord}_p(x) \leq -2\nu,\ \mathrm{ord}_p(y) \leq -3\nu\} \cup \{\mathcal{O}\}.$$

En particular $\mathcal{C}(p)$ es el conjunto de puntos $(x, y) \in \mathcal{C}(\mathbb{Q})$ donde p divide al denominador de x e y. Se tiene que

$$\mathcal{C}(\mathbb{Q}) \supset \mathcal{C}(p) \supset \mathcal{C}(p^2) \supset \mathcal{C}(p^3) \supset \ldots$$

Se denota por R_p al conjunto de los números racionales tales que p no divide al denominador, es decir

$$R_p = \left\{ \frac{n}{m} \in \mathbb{Q} : n \text{ y } m \text{ coprimos},\ p \nmid m \right\}.$$

Se tiene que R_p es un subanillo de $\mathbb{Q}$. Denotamos por $p^k R_p$, para $k \in \mathbb{N}$ y p número primo, a los subconjuntos

$$p^k R_p = \left\{ \frac{n}{m} \in \mathbb{Q} : n \text{ y } m \text{ coprimos},\ p \nmid m, p^k \mid n \right\}.$$

Lema 2.24.
(a) Si $\alpha \in p^k R_p$ entonces para cualquier $i \leq k$ se tiene que $\alpha \in p^i R_p$.
(b) Si $\alpha \in p^k R_p$ y $\beta \in p^l R_p$ entonces $\alpha + \beta \in p^i R_p$ donde $i = min\{k, l\}$.
(c) Si $\alpha \in p^k R_p$ y $\beta \in p^l R_p$ entonces $\alpha\beta \in p^{k+l} R_p$.
(d) Si $\alpha \in p^k R_p$ entonces $1 + \alpha \notin pR_p$.
(e) Si $\alpha \in p^k R_p$ y $\beta \notin pR_p$ entonces $\alpha/\beta \in p^k R_p$.

Demostración. Sean $\alpha = n/m,\ \beta = u/w$ donde $p^k \mid n$, $p^l \mid u$, $p \nmid m$ y $p \nmid w$.

(a) Claramente si p^k divide al numerador de α, p^i con $i \leq k$ divide también al numerador de α.

(b) Tenemos que $\alpha + \beta = (nw + um)/(mw)$ y además $p^i \mid (nw + um)$ y $p \nmid mw$, donde $i = min\{k, l\}$ y por tanto $\alpha + \beta \in p^i R_p$.

(c) Sabemos que $\alpha\beta = (nu)/(mw)$, donde $p^{k+l} \mid nu$ y $p \nmid mw$ por lo que $\alpha\beta \in p^{k+l} R_p$.

(d) Como $1 + \alpha = (m + n)/m$, dado que $p \mid n$ y $p \nmid m$, entonces $p \nmid (n + m)$, así que $1 + \alpha \notin pR_p$.

(e) En este caso consideramos $\alpha = n/m,\ \beta = u/w$ donde $p^k \mid n$, $p \nmid u$, $p \nmid m$ y $p \nmid w$. Entonces $\alpha/\beta = (nw)/(mu)$ y se tiene que $p \nmid mu$ y $p^k \mid nw$, concluimos que $\alpha/\beta \in p^k R_p$.

□

Obsérvese que $p^k R_p$ es un ideal de R_p para todo $k \in \mathbb{N}$ y p número primo.

Proposición 2.25. *Sean $\mathcal{C}$, $\mathcal{C}'$ dos curvas elípticas contenidas en $\mathbb{PC}^2$. Si $\mathcal{C}$ y $\mathcal{C}'$ son proyectivamente equivalentes, entonces sus grupos asociados son isomorfos. Un isomorfismo es $\phi^* : \mathcal{C} \longmapsto \mathcal{C}'$, siendo ϕ^* una transformación proyectiva verificando $\phi^*(O) = \phi^*(O')$ donde O y O' son los neutros de $\mathcal{C}$ y $\mathcal{C}'$ respectivamente.*

La demostración de la Proposición 2.25 se puede encontrar en la Proposición 2.12 del Capítulo 2 de [9].

La curva $\mathcal{C} \equiv \mathcal{C}_F : y^2z = x^3 + ax^2z + bxz^2 + cz^3$ es proyectivamente equivalente a $\mathcal{C}' \equiv \mathcal{C}_G : z^2y = x^3 + ax^2y + bxy^2 + cy^3$, ya que $F(x, y, z) = G(\phi(x, y, z))$, donde el isomorfismo lineal es $\phi(x, y, z) = (x, z, y)$.

Tomando como neutro en el grupo asociado a $\mathcal{C}'$ al origen (0,0), vemos entonces que los grupos asociados a $\mathcal{C}$ y $\mathcal{C}'$ son isomorfos, mediante $\phi^*(x : y : z) = (x : z : y)$, gracias a la Proposición 2.25.

Bajo esta transformación, el elemento neutro $\mathcal{O}$ de la curva $\mathcal{C}$ pasa a estar en el origen (0,0), y los puntos que verifican $y = 0$, es decir, los puntos de orden 2, pasan a ser puntos en el infinito de $\mathcal{C}'$. El resto de puntos (x, y) de $\mathcal{C}$ se corresponden biyectivamente con los puntos $(t, s) = (x/y, 1/y)$. Estos puntos se pueden recuperar mediante $(x, y) = (t/s, 1/s)$.

Sea $P \in \mathcal{C}$ un punto de orden distinto a 2, entonces $\phi^*(P) = (u, w)$, donde ϕ^* es la transformación inducida por $\phi(x, y, z) = (x, z, y)$. En lo que sigue denotaremos como $t(P)$ a la primera coordenada de $\phi^*(P)$ y como $s(P)$ a la segunda coordenada, es decir, $t(P) = u,\ s(P) = w$.

Proposición 2.26. *Sea $P \in \mathcal{C}$, entonces $P \in \mathcal{C}(p^\nu)$ si y solo si $t(P) \in p^\nu R_p$ y $s(P) \in p^{3\nu} R_p$.*

Demostración. Supongamos que $P \in \mathcal{C}(p^\nu)$ y $t = t(P),\ s = s(P)$, entonces los puntos $P = (x, y)$ tales que $y = 0$ no se encuentran en $\mathcal{C}(p^\nu)$, ya que si sustituimos $y = 0$ en $\mathcal{C}$, entonces $0 = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ que es un polinomio mónico, de donde las posibles raíces racionales deben ser enteras, y por tanto, no están en ningún $\mathcal{C}(p^\nu)$.
Si $P \neq \mathcal{O}$, entonces $P = (x, y)$ se puede escribir como

$$x = \frac{m}{np^{2(\nu+i)}}, \quad y = \frac{u}{wp^{3(\nu+i)}},$$

para cierto $i \geq 0$. Al ser (x, y) un punto tal que $y \neq 0$, se tiene que $Q = (t, s)$ donde

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+i} \quad \text{y} \quad y = \frac{1}{s} = \frac{w}{u}p^{3(\nu+i)}.$$

Concluimos que $t \in p^\nu R_p$ y $s \in p^{3\nu} R_p$, es decir, $(t, s) \in p^\nu R_p \times p^{3\nu} R_p$. Si $P = \mathcal{O}$, entonces $\phi^*(\mathcal{O}) = (0, 0) \in\ p^\nu R_p \times p^{3\nu} R_p$.

Por otro lado, supongamos que $Q = (t, s) \in p^\nu R_p \times p^{3\nu} R_p$, entonces Q se puede escribir como

$$t = \frac{n}{m}p^{(\nu+i)}, \quad s = \frac{w}{u}p^{3(\nu+i)},$$

para cierto $i \geq 0$. Si $Q \neq (0,0)$ entonces

$$x = \frac{t}{s} = \frac{nu}{mwp^{2(\nu+i)}} \quad \text{y} \quad s = \frac{1}{y} = \frac{u}{wp^{3(\nu+i)}},$$

por lo que $(x,y) \in \mathcal{C}(p^\nu)$. En el caso de que $Q = (0,0)$, este punto se corresponde con $\mathcal{O} \in \mathcal{C}(p^\nu)$.

□

Lema 2.27. *Sean $P, Q \in \mathcal{C}(p^\nu)$, $\nu \geq 1$, entonces $P = Q$ si y solo si $t(P) = t(Q)$.*

Demostración. Está claro que si $P = Q$ entonces $t(P) = t(Q)$. Supongamos que $t(P) = t(Q)$, si demostramos que $s(P) = s(Q)$ tendríamos que $P = Q$.

Vamos a demostrar que $s(P) - s(Q) \in p^k R_p$ para cualquier $k \geq 1$, $k \in \mathbb{N}$. Procederemos por inducción sobre k. Como $P, Q \in \mathcal{C}(p^\nu)$ sabemos por la Proposición 2.26 que $s(P), s(Q) \in p^{3\nu}R_p$ y $t(P) \in p^\nu R_p$, en particular $s(P), s(Q), t(P) \in pR_p$, de donde, $s(P) - s(Q) \in pR_p$ demostrando así el caso $k = 1$.

Tenemos que $(t(P), s(P)), (t(Q), s(Q)) \in \mathcal{C}'$, por lo tanto

$$\begin{cases} s(P) = t(P)^3 + at(P)^2 s(P) + bt(P)s(P)^2 + cs(P)^3 \\ s(Q) = t(Q)^3 + at(Q)^2 s(Q) + bt(Q)s(Q)^2 + cs(Q)^3. \end{cases}$$

Usando que $t(P) = t(Q)$, al restar las ecuaciones anteriores obtenemos que

$$s(P) - s(Q) = at(P)^2(s(P) - s(Q)) + bt(P)(s(P)^2 - s(Q)^2) + c(s(P)^3 - s(Q)^3). \tag{2.8}$$

Supongamos que $s(P) - s(Q) \in p^k R_p$ y demostraremos que $s(P) - s(Q) \in p^{k+1}R_p$. Como $s(P), s(Q), t(P) \in pR_p$, del Lema 2.24 tenemos que $s(P) + s(Q) \in pR_p$ y $s(P)^2 + s(P)s(Q) + s(Q)^2 \in pR_p$. Por lo tanto de nuevo por el Lema 2.24

$$\begin{cases} s(P)^2 - s(Q)^2 = (s(P) - s(Q))(s(P) + s(Q)) \in p^{k+1}R_p \\ s(P)^3 - s(Q)^3 = (s(P) - s(Q))(s(P)^2 + s(P)s(Q) + s(Q)^2) \in p^{k+1}R_p \\ t(P)^2(s(P) - s(Q)) \in p^{k+1}R_p. \end{cases}$$

Retomando la ecuación (2.8), el lado derecho es una suma de elementos de $p^{k+1}R_p$ por lo que al aplicar el Lema 2.24 concluimos que el lado izquierdo es un elemento de $p^{k+1}R_p$, es decir, $s(P) - s(Q) \in p^{k+1}R_p$, concluyendo así la demostración por inducción.

Si $s(P) - s(Q) \in p^k R_p$ para cualquier $k \geq 1$, esto quiere decir que el numerador de $s(P) - s(Q)$ es divisible por p^k, siendo k arbitrariamente grande, de donde necesariamente $s(P) - s(Q) = 0$. Concluyendo así que $P = Q$.

□

Proposición 2.28. *Se tiene que* $(\mathcal{C}(p^\nu),+)$ *es un subgrupo de* $(\mathcal{C}(\mathbb{Q}),+)$ *para cualquier* $\nu \geq 1$. *Además si* $P_1, P_2 \in \mathcal{C}(p^\nu)$, *entonces* $t(P_1)+t(P_2)-t(P_1+P_2) \in p^{3\nu}R_p$.

Demostración. Si $P=(x,y) \in \mathcal{C}(p^\nu)$, tenemos que $-P=(x,-y)$, claramente $\mathrm{ord}_p(-y)=\mathrm{ord}_p(y) \leq -3\nu$. Por lo tanto $-P \in \mathcal{C}(p^\nu)$.

Sean $P_1, P_2 \in \mathcal{C}(p^\nu)$ tales que $P_1+P_2=P_3$, tenemos que $\phi^*(P_1+P_2)=\phi^*(P_3)$, al ser ϕ^* un homomorfismo, $\phi^*(P_1)+\phi^*(P_2)=\phi^*(P_3)$. Tomamos $Q_i=\phi^*(P_i)=(t_i,s_i)$, $i=1,2,3$. Se tiene que $Q_1+Q_2=(Q_1*Q_2)*(0,0)$, supongamos que la recta que pasa por Q_1 y Q_2 corta a $\mathcal{C}'$ en $Q_3'=(t_3',s_3')$, es fácil comprobar sustituyendo en la ecuación de $\mathcal{C}'$ que si $(t_3',s_3') \in \mathcal{C}'$ entonces $(-t_3',-s_3')$ también está en $\mathcal{C}'$.

La recta que pasa por (t_3',s_3') y $(-t_3',-s_3')$ también pasa por $(0,0)$, por lo tanto $Q_3'*(0,0)=(-t_3',-s_3')$, como $(-t_3',-s_3')=Q_1+Q_2=Q_3=(t_3,s_3)$, concluimos que $t_3=-t_3'$ y $s_3=-s_3'$.

Supongamos que $P_1 \neq P_2$, por el Lema 2.27 sabemos que $t(P_1) \neq t(P_2)$, es decir $t_1 \neq t_2$. Sea $s=\alpha t+\beta$ la recta que pasa por Q_1 y Q_2, la pendiente α viene dada por

$$\alpha=\frac{s_2-s_1}{t_2-t_1}.$$

Como los puntos $Q_1, Q_2 \in \mathcal{C}'$, entonces satisfacen la ecuación de $\mathcal{C}'$, es decir, $s=t^3+at^2s+bts^2+cs^3$. Restamos la ecuación de Q_1 a la ecuación de Q_2 y factorizamos:

$$\begin{aligned} s_2-s_1 &= \left(t_2^3-t_1^3\right)+a\left(t_2^2s_2-t_1^2s_1\right)+b\left(t_2s_2^2-t_1s_1^2\right)+c\left(s_2^3-s_1^3\right) \\ &= \left(t_2^3-t_1^3\right)+a\left(\left(t_2^2-t_1^2\right)s_2+t_1^2\left(s_2-s_1\right)\right)+b\left(\left(t_2-t_1\right)s_2^2+t_1\left(s_2^2-s_1^2\right)\right) \\ &\quad +c\left(s_2^3-s_1^3\right). \end{aligned}$$

Algunos de los términos son divisibles por s_2-s_1 y otros lo son por t_2-t_1. Podemos agruparlos de la siguiente forma

$$(s_2-s_1)(1-at_1^2-bt_1(s_2-s_1)-c(s_2^2+s_1s_2+s_1^2))=(t_2-t_1)(t_2^2+t_1t_2+t_1^2+a(t_2+t_1)s_2+bs_2^2).$$

Por lo que finalmente

$$\alpha=\frac{s_2-s_1}{t_2-t_1}=\frac{t_2^2+t_1t_2+t_1^2+a(t_2+t_1)s_2+bs_2^2}{1-at_1^2-bt_1(s_2-s_1)-c(s_2^2+s_1s_2+s_1^2)}. \tag{2.9}$$

De manera similar, si $P_1=P_2$, tendríamos que $Q_1=\phi^*(P_1)=\phi^*(P_2)=Q_2$, por lo tanto la pendiente α de la recta tangente a Q_1 viene dada por

$$\alpha = \frac{ds}{dt}(Q_1) = \frac{3t_1^2 + 2at_1s_1 + bs_1^2}{1 - at_1^2 - 2bt_1s_1 - 3cs_1^2}.$$

Notamos que esta pendiente es la que se obtiene en (2.9), si $t_1 = t_2$ y $s_1 = s_2$. Por lo tanto, en lo que sigue podemos usar la expresión en (2.9).

Dado que $t_1, t_2, s_1, s_2 \in p^\nu R_p$, sabemos por el Lema 2.24 que $t_2^2 + t_1t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2 \in p^{2\nu}R_p$ y $1 - at_1^2 - bt_1(s_2 - s_1) - c(s_2^2 + s_1s_2 + s_1^2) \notin pR_p$, y concluimos que $\alpha \in p^{2\nu}R_p$.

Además como $s_1 \in p^{3\nu}R_p$, $\alpha \in p^{2\nu}R_p$ y $t_1 \in p^\nu R_p$, de $\beta = s_1 - \alpha t_1$ se deduce, de nuevo por el Lema 2.24, que $\beta \in p^{3\nu}R_p$. Ahora como Q_3' es el tercer punto de intersección de la curva C' con la recta $s = \alpha t + \beta$. Para obtener los puntos de intersección podemos sustituir $s = \alpha t + \beta$ en la ecuación de la curva,

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3.$$

Al multiplicar y agrupar en potencias de t, podemos reescribir la ecuación anterior como

$$0 = (1 + a\alpha + b\alpha^2 + c\alpha^3)t^3 + (\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta)t^2 + \ldots,$$

que tiene raíces t_1, t_2, t_3' que se corresponden con los puntos Q_1, Q_2, Q_3', por lo que el lado derecho será $k(t - t_1)(t - t_2)(t - t_3')$ para cierta constante $k \neq 0$. Además como,

$$k(t - t_1)(t - t_2)(t - t_3') = kt_1^3 + (k(-t_1 - t_2 - t_3'))t^2 + \ldots$$

Comparando coeficientes concluimos que

$$t_1 + t_2 + t_3' = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}.$$

Dado que $\alpha \in p^{2\nu}R_p$ y $\beta \in p^{3\nu}R_p$, aplicando el Lema 2.24, tenemos que el numerador de $t_1 + t_2 + t_3'$ se encuentra en $p^{3\nu}R_p$ mientras que el denominador está en R_p pero no en pR_p y finalmente deducimos que $t_1 + t_2 + t_3' \in p^{3\nu}R_p$.

Como $t_1, t_2 \in p^\nu R_p$ y $t_1 + t_2 + t_3' \in p^{3\nu}R_p$, entonces $t_3' \in p^\nu R_p$, además tenemos que $s_3' = \alpha t_3' + \beta$ y por el Lema 2.24 observamos que $s_3' \in p^{3\nu}R_p$. Por lo tanto, $-t_3' \in p^\nu R_p$ y $-s_3' \in p^{3\nu}R_p$.

Recordamos que $(t_3, s_3) = (-t_3', -s_3') \in p^\nu R_p \times p^{3\nu}R_p$, como $t(P_3) = t_3$ y $s(P_3) = s_3$, usando la Proposición 2.26, concluimos que $P_3 \in \mathcal{C}(p^\nu)$, esto demuestra que $+$ es ley de composición interna en $\mathcal{C}(p^\nu)$.

□

Proposición 2.29. *Se tiene que $R_p/p^{3\nu}R_p$ es un anillo, y si $[m] \in R_p/p^{3\nu}R_p$, donde $m \in \mathbb{Z}$ tal que $p \nmid m$, entonces $[m]$ es una unidad en $R_p/p^{3\nu}R_p$.*

Demostración. Como R_p es un subanillo de $\mathbb{Q}$ y por el Lema 2.24 sabemos que $p^{3\nu}R_p$ es un ideal de R_p, entonces $R_p/p^{3\nu}R_p$ es un anillo.

Dado que $p \nmid m$, tenemos que m mód $p^{3\nu}$ es una unidad en $\mathbb{Z}_{p^{3\nu}}$, es decir, existe $k \in \mathbb{Z}$ tal que $mk - 1 \in p^{3\nu}\mathbb{Z}$. En particular, esto significa que $mk - 1 \in p^{3\nu}R_p$ por lo que $[m]$ es unidad en $R_p/p^{3\nu}R_p$.

□

Lema 2.30. *Si denotamos por $\bar{P}$ a las clases de equivalencia que conforman el grupo cociente $\mathcal{C}(p^\nu)/\mathcal{C}(p^{3\nu})$ y de la misma forma, denotamos por $[Q]$ a las clases del anillo cociente $R_p/p^{3\nu}R_p$. Tenemos que*

$$\begin{aligned} h : \mathcal{C}(p^\nu)/\mathcal{C}\left(p^{3\nu}\right) &\to R_p/p^{3\nu}R_p \\ \bar{P} &\mapsto [t(P)] \end{aligned}$$

es un homomorfismo de grupos inyectivo.

Demostración. Veamos que h es aplicación. Está claro que si $P \in \mathcal{C}(p^\nu)$, entonces por la Proposición 2.26 $t(P) \in p^\nu R_p$, de donde, $[t(P)] \in R_p/p^{3\nu}R_p$.

Supongamos que $\bar{P} = \bar{Q}$, entonces $P - Q \in \mathcal{C}(p^{3\nu})$ y por la Proposición 2.26, necesariamente $t(P - Q) \in p^{3\nu}R_p$. Ahora por la Proposición 2.28, como $P, Q \in \mathcal{C}(p^\nu)$, se tiene que $t(P) + t(-Q) - t(P - Q) \in p^{3\nu}R_p$.

Recordemos que si $Q = (x, y)$ entonces $-Q = (x, -y)$, por lo que, $t(-Q) = -t(Q)$. Podemos concluir que $t(P) - t(Q) \in p^{3\nu}R_p$, y finalmente que $[t(P)] = [t(Q)]$. Se tiene que h es homomorfismo como consecuencia directa de la Proposición 2.28.

Demostremos la inyectividad de h. Sea $P \in \mathcal{C}(p^\nu)$, por la Proposición 2.26, $s(P) \in p^{3\nu}R_p$. Supongamos que $h(\bar{P}) = [0]$, esto es que, $t(P) \in p^{3\nu}R_p$. Ahora sabemos que $t(P)$ y $s(P)$ están relacionados por la siguiente fórmula

$$s(P) = t(P)^3 + at(P)^2 s(P) + bt(P)s(P)^2 + cs(P)^3.$$

En el lado derecho cada sumando se encuentra en $p^{9\nu}R_p$, por lo que $s(P) \in p^{9\nu}R_p$, juntándolo con el hecho de que $t(P) \in p^{3\nu}R_p$ y usando la Proposición 2.26, concluimos que $P \in \mathcal{C}(p^{3\nu})$.

□

Teorema 2.31. *Para todo número primo p, el único punto de orden finito en el grupo $\mathcal{C}(p)$ es $\mathcal{O}$.*

Demostración. Por reducción al absurdo, supongamos que existe un número primo p tal que $P = (x, y) \in \mathcal{C}(p)$. Dado que los denominadores de x e y no pueden ser divisibles por potencias arbitrariamente grandes de p concluimos que para cierto $\nu \geq 1$, $P \in \mathcal{C}(p^\nu)$ y $P \notin \mathcal{C}(p^{\nu+1})$.

Tenemos que P es un punto de orden finito distinto de $\mathcal{O}$, es decir, existe $m \geq 1$ tal que

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ sumandos}} = \mathcal{O}.$$

Por un lado, si $p \nmid m$, entonces haciendo uso del homomorfismo h definido en el Lema 2.30, obtenemos que $h(\bar{P}) + \cdots + h(\bar{P}) = [0]$, es decir, $[m]h(\bar{P}) = [0]$ y aplicando la Proposición 2.29 como $[m]$ es unidad, deducimos que $h(\bar{P}) = [0]$. Ahora como h es inyectivo, necesariamente $P \in \mathcal{C}(p^{3\nu})$, contradiciendo que $P \notin \mathcal{C}(p^{\nu+1})$.

Por otro lado, si $p \mid m$, entonces para cierto $n \in \mathbb{Z}$, se tiene que $m = pn$, podemos entonces considerar $P' = nP$. Dado que $P \in \mathcal{C}(p)$ y $\mathcal{C}(p)$ es un subgrupo de $\mathcal{C}(\mathbb{Q})$, vemos que $P' \in \mathcal{C}(p)$, y de la misma forma que antes para cierto $\nu \geq 1$, $P' \in \mathcal{C}(p^{\nu})$ y $P' \notin \mathcal{C}(p^{\nu+1})$.

En este caso, usando el homomorfismo h obtenemos que $[t(pP')] = [0]$, por lo que $pt(P') \in p^{3\nu}R_p$, por lo tanto, $t(P') \in p^{3\nu-1}R_p$, en particular $t(P') \in p^{\nu+1}R_p$, y dado que $P' \in \mathcal{C}(p^{\nu})$, tenemos, por la Proposición 2.26 que $s(P') \in p^{3\nu}R_p$. Usando la relación entre $t(P')$ y $s(P')$

$$s(P') = t(P')^3 + at(P')^2 s(P') + bt(P')s(P')^2 + cs(P')^3,$$

donde cada sumando se encuentra en $p^{3\nu+3}R_p$. Por tanto $s(P') \in p^{3\nu+3}R_p$ y finalmente por la Proposición 2.26 podemos concluir que $P' \in \mathcal{C}(p^{\nu+1})$ llegando a una contradicción.

□

Corolario 2.32. *Sea $P = (x, y) \in \mathcal{C}(\mathbb{Q})$ un punto racional de orden finito. Entonces x e y son enteros.*

Demostración. Sabemos por el Teorema 2.31 que $P \notin \mathcal{C}(p)$ para cualquier primo p. Por lo tanto los denominadores de x e y no son divisibles por ningún primo, o lo que es lo mismo, x e y son números enteros.

□

Ejemplo 2.33. En el Ejemplo 1.26, vimos que $P = (12, 36)$ era un punto de la curva $\mathcal{C} : y^2 = x^3 - 36x$, al ser un punto con coordenadas enteras, podríamos pensar que tiene orden finito. Sin embargo, en el Ejemplo 1.26 también calculamos $2P = (25/4, 35/8)$, aplicando el Corolario 2.32, se ve claramente que $2P$ no tiene orden finito, esto significa que necesariamente P tampoco tiene orden finito.

De esta forma también hemos demostrado que existen infinitos puntos racionales en la curva $\mathcal{C}$, es decir, existen infinitos triángulos rectángulos cuyos lados sean racionales y su área sea 6.

2.3. El Teorema de Nagell-Lutz

Una vez probado que los puntos de orden finito tienen coordenadas enteras, podemos ir un poco más allá y proporcionar un método para encontrar dichos puntos, a través del Teorema de Nagell-Lutz, el cual nos permite calcular en un número finito de pasos el subgrupo de torsión del grupo de puntos racionales asociado a una curva elíptica.

Definición 2.34. *Sea $y^2 = f(x) = x^3 + ax^2 + bx + c$, donde $a, b, c \in \mathbb{Z}$. Se define el discriminante como*

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Lema 2.35. *Sea $f(x) \in \mathbb{Z}[x]$ mónico. El discriminante de $f(x)$ está en el ideal generado por $f(x)$ y $f'(x)$ en $\mathbb{Z}[x]$.*

Demostración. Si tomamos los siguientes polinomios

$$\begin{cases} p(x) = (18b - 6a^2)x - (4a^3 - 15ab + 27c) \\ q(x) = (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2), \end{cases}$$

Se verifica que $\Delta = p(x)f(x) + q(x)f'(x)$, y por tanto Δ está en el ideal generado por $f(x)$ y $f'(x)$.

□

Lema 2.36. *Sea $\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx + c$. Dado un punto $P = (x_0, y_0) \in \mathcal{C}(\mathbb{Q})$, $y_0 \neq 0$ si $2P = (x_1, y_1)$, entonces $2x_0 + x_1 = \lambda^2 - a$, donde $\lambda = f'(x_0)/2y_0$.*

Demostración. Para hallar $2P$, debemos encontrar la recta tangente a la curva en P, usando que $y^2 = f(x)$. Al derivar encontramos que la pendiente de dicha recta es justamente $\lambda = f'(x_0)/2y_0$. Por lo tanto buscamos los puntos de intersección de $y^2 = f(x)$ con $y = \lambda x + k$. Para ello sustituimos en la ecuación de la curva

$$x^3 + ax^2 + bx + c = y^2 = (\lambda x + k)^2 = \lambda^2 x^2 + 2\lambda x + k^2,$$

despejando obtenemos

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda) + c - k^2 = 0. \tag{2.10}$$

Sabemos que el anterior polinomio tiene una raíz doble en x_0 y la raíz restante es x_1, es decir, el polinomio en (2.10) es $(x - x_0)^2(x - x_1)$. El coeficiente de x^2 en este último es $-x_1 - 2x_0$, al igualarlo con el coeficiente de x^2 en (2.10), llegamos a que $2x_0 + x_1 = \lambda^2 - a$.

□

Teorema 2.37 (Nagell-Lutz). *Sea $\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx + c$ una curva elíptica donde $a, b, c \in \mathbb{Z}$ y sea Δ su discriminante. Si $P = (x_0, y_0)$ es un punto racional de orden finito, entonces tanto x_0 como y_0 son enteros. Además, $y_0 = 0$, o bien, $y_0 \mid \Delta$.*

Demostración. Por el Corolario 2.32 sabemos que x_0 e y_0 son enteros. Supongamos que $y_0 \neq 0$, esto significa por el Lema 2.20 que $2P \neq \mathcal{O}$, por lo que $2P = (x_1, y_1)$ que es un punto de orden finito y por el Corolario 2.32 debe darse que $x_1, y_1 \in \mathbb{Z}$.

Ahora bien por el Lema 2.36, necesariamente $2x_0 + x_1 = \lambda - a$, donde $\lambda = f'(x_0)/2y_0$. Usando que $x_0, x_1, a \in \mathbb{Z}$ concluimos que $\lambda \in \mathbb{Z}$, y como $y_0, f'(x_0) \in \mathbb{Z}$, esto es que $2y_0 \mid f'(x_0)$, y en particular que $y_0 \mid f'(x_0)$. Recordemos que $y_0^2 = f(x_0)$, por lo que también $y_0 \mid f(x_0)$.

Por el Lema 2.35, es posible escribir $\Delta = p(x_0)f(x_0) + q(x_0)f'(x_0)$ para ciertos polinomios $p, q \in \mathbb{Z}[x]$. Finalmente, usando que $y_0 \mid f(x_0)$ y $y_0 \mid f'(x_0)$, se concluye que $y \mid \Delta$.

□

Ejemplo 2.38. Supongamos que queremos encontrar los puntos de orden finito de la curva $\mathcal{C} : y^2 = x^3 - x$, cuyo determinante es -4. Por el Teorema de Nagell-Lutz, existen 4 posibilidades, $y_0 = 0,\ y_1 = 1,\ y_2 = 2,\ y_3 = 4$, ya que podemos descartar los valores negativos de y por ser la curva simétrica respecto al eje X. Buscamos por lo tanto las soluciones de

$$\begin{cases} x_0^3 - x_0 = 0 \\ x_1^3 - x_1 = 1 \\ x_2^3 - x_2 = 4 \\ x_3^3 - x_3 = 16. \end{cases}$$

De entre todas, solo la primera produce soluciones racionales, que son $(0,0), (1,0)$ y $(-1,0)$; lo que nos permite concluir que la curva $\mathcal{C}$ tiene únicamente 4 puntos racionales de orden finito contando con $\mathcal{O}$. Sin embargo, esto ya lo sabíamos, pues en el Teorema 1.7 demostramos que 1 no es un número congruente, y dado que $\mathcal{C}$ es la curva asociada a este, necesariamente $(0,0), (1,0), (-1,0)$ y $\mathcal{O}$ son los únicos puntos racionales de esta curva.

Teorema 2.39. *Sea $\mathcal{C}_n : y^2 = x^3 - n^2x, n \in \mathbb{N}$. Se tiene que n es un número congruente si y solo si el rango de $\mathcal{C}_n$ sobre $\mathbb{Q}$ es positivo.*

Demostración. Supongamos que el rango de $\mathcal{C}_n$ sobre $\mathbb{Q}$ es positivo, esto significa en particular que existe un punto $P = (x, y)$ en $\mathcal{C}_n$ de orden infinito, por lo que $y \neq 0$, ya que de otra forma P tendría orden 2. Aplicando ahora el Teorema 1.20, concluimos que n es un número congruente.

Por otro lado, supongamos ahora que n es un número congruente, sabemos entonces por el Teorema 1.11, que existen $r, s, t \in \mathbb{Q}$ tales que $s^2 - r^2 = t^2 - s^2 = n$. Podemos encontrar $y \in \mathbb{Z}$, con $y > 0$ tal que $x, z, u \in \mathbb{Z}$, donde $x = sy,\ z = ry,\ u = ty$, se tiene entonces que

$$\begin{cases} x^2 - ny^2 = z^2 \\ x^2 + ny^2 = u^2. \end{cases} \tag{2.11}$$

Podemos suponer además que x e y son coprimos, ya que si $m = \text{mcd}(x, y) > 1$, dado que $m \mid x$ y $m \mid y$, del par de ecuaciones en (2.11), se tiene que $m^2 \mid z^2$ y $m^2 \mid u^2$. Aplicando el Lema 1.6 (a) podemos concluir que $m \mid z$ y $m \mid u$. Dividiendo por m en (2.11) obtenemos

$$\begin{cases} x'^2 - ny'^2 = z'^2 \\ x'^2 + ny'^2 = u'^2, \end{cases}$$

donde $x', y', z', u' \in \mathbb{Z}$ y $\text{mcd}(x', y') = 1$.

Multiplicando las ecuaciones en (2.11) deducimos que $x^4 - n^2y^4 = (zu)^2$, y al multiplicar esta última por x^2/y^6 llegamos a que

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

Por lo tanto, hemos encontrado un punto de $\mathcal{C}_n$, $P = (x^2/y^2, zux/y)$, teniendo en cuenta que x e y son coprimos está claro que $x^2/y^2 \notin \mathbb{Z}$, y del Teorema de Nagell-Lutz podemos concluir que P tiene orden infinito, demostrando así que el rango de $\mathcal{C}_n$ sobre $\mathbb{Q}$ es positivo.

□

Gracias al Teorema 2.39, podemos ver que, si fuesemos capaces de calcular el grupo asociado a una cierta curva elíptica, o en particular, si pudiesemos calcular el rango de $\mathcal{C}_n$ sobre $\mathbb{Q}$, el Problema del Número Congruente estaría cerrado. Sin embargo, este no es el caso, el problema de determinar el rango resulta ser muy complejo.

No obstante, ahora los Teoremas 1.7 y 1.19 adquieren un nuevo valor, ya que junto con el Teorema 2.39, podemos ver que los grupos asociados a las curvas $\mathcal{C}_1 : y^2 = x^3 - x$ y $\mathcal{C}_p : y^2 = x^3 - p^2x$ con p número primo y $p \equiv 3$ mód 8, tienen rango 0, de hecho sus grupos asociados estan formados por $\mathcal{O}$ y tres puntos de orden 2, de donde podemos deducir que sus grupos son isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

En [14], se encuentra una base de datos sobre si los números del 1 al 1.000.000 son congruentes o no. Además, proporciona el rango del grupo asociado, y si el número es congruente, los lados de uno de los infinitos triángulos posibles.

3

Los números θ-congruentes

El objetivo de este capítulo será el de introducir una generalización a los números congruentes. Veremos que este problema más general también se puede entender mediante los puntos racionales de una cierta familia de curvas elípticas, para ello nos hemos basado en [6] y [11].

Si $X, Y, Z \in \mathbb{Q}$ son los lados de un triángulo y θ es uno de los tres ángulos de dicho triángulo, entonces al tener lados racionales deducimos que $\cos\theta = s/r$ es racional, donde $\text{mcd}(s, r) = 1$. Por lo tanto $\operatorname{sen}\theta = \alpha_\theta/r$ donde $\alpha_\theta = \sqrt{r^2 - s^2}$.

Definición 3.1. *Si $n \in \mathbb{Z}^+$, decimos que n es θ-congruente si existe un triángulo verificando que*

(1) Sus tres lados son racionales.
(2) Uno de sus ángulos es θ.
(3) Su área es $n\alpha_\theta$.

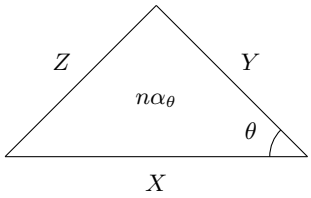


Figura 3.1. Triángulo verificando las condiciones de la Definición 3.1.

Ejemplo 3.2. El número 1 es $\pi/3$-congruente, ya que $\alpha_{\pi/3} = \sqrt{3}$, y el triángulo equilátero donde $X = Y = Z = 2$, tiene área $\sqrt{3}$. Un ejemplo algo más complicado es que el 11 es $\pi/3$-congruente ya que $11\sqrt{3}$ es el área de un triángulo con lados $X = 55/12,\ Y = 48/5,\ Z = 499/60$.

Sea T un triángulo de lados $X,\ Y,\ Z$. Supongamos sin pérdida de la generalidad que θ es el ángulo que se forma entre X e Y. Tenemos que n es θ-congruente

si y solo si el área del triángulo es $n\alpha_\theta = (XY\sin\theta)/2$, y además por la Ley del Coseno $Z^2 = X^2 + Y^2 - 2XY\cos\theta$. Por lo tanto n es θ-congruente si y solo si

$$XY = 2rn, \quad \text{y} \quad Z^2 = X^2 + Y^2 - \frac{2sXY}{r}, \quad X, Y, Z \in \mathbb{Q}. \tag{3.1}$$

Proposición 3.3. *Los triángulos que satisfacen* (3.1) *están en correspondencia biyectiva con los números racionales x tales que $x, x+(r+s)n$ y $x-(r-s)n$ son cuadrados de racionales.*

Demostración. Definimos los siguientes conjuntos

$$A = \left\{(X, Y, Z) \in \mathbb{Q}^3 : XY = 2rn,\ Z^2 = X^2 + Y^2 - \frac{2sXY}{r}\right\} y$$

$$B = \{(a, b, c) \in \mathbb{Q}^3 : a^2 = x,\ b^2 = x + (r+s)n,\ c^2 = x - (r-s)n\}.$$

Sean $X, Y, Z \in \mathbb{Q}$ verificando (3.1). Usando que $n = (XY)/(2r)$, dividiendo por 4 y sumando $(r+s)n$ obtenemos que

$$\left(\frac{Z}{2}\right)^2 + (r+s)n = \frac{X^2}{4} + \frac{Y^2}{4} - \frac{sXY}{2r} + \frac{(r+s)XY}{2r} = \left(\frac{X+Y}{2}\right)^2.$$

Si ahora, en su lugar restamos por $(r-s)n$ nos queda

$$\left(\frac{Z}{2}\right)^2 - (r-s)n = \frac{X^2}{4} + \frac{Y^2}{4} - \frac{sXY}{2r} - \frac{(r-s)XY}{2r} = \left(\frac{X-Y}{2}\right)^2.$$

Entonces hemos encontrado una aplicación de A en B, $x = (Z/2)^2$.

Sean ahora $a = \sqrt{x}$, $b = \sqrt{x + (r+s)n}$ y $c = \sqrt{x - (r-s)n} \in \mathbb{Q}$. Por un lado tenemos que

$$(b-c)(b+c) = b^2 - c^2 = 2rn,$$

y por otro que

$$(b-c)^2 + (b+c)^2 - \frac{2s(b-c)(b+c)}{r} = \frac{2((r-s)b^2 + (r+s)^2)}{r} = 4x = (2a)^2.$$

Por lo que hemos encontrado una aplicación de B en A, $X = b - c$, $Y = b + c$, $Z = 2a$. Se puede comprobar que además estas aplicaciones son una la inversa de la otra.

□

Sea $\mathcal{C}$ una curva elíptica, se denota por $2\mathcal{C}(\mathbb{Q})$ al conjunto formado por $2Q$ donde $Q \in \mathcal{C}(\mathbb{Q})$.

Lema 3.4. *Si $\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx + c$ es una curva elíptica y T una traslación siendo $(a, 0)$ con $a \in \mathbb{Q}$ el vector que define la traslación, entonces $P \in 2\mathcal{C}(\mathbb{Q}) - \{\mathcal{O}\}$ si y solo si $T(P) \in 2\mathcal{C}'(\mathbb{Q}) - \{\mathcal{O}\}$, donde $\mathcal{C}' = T(\mathcal{C})$.*

Demostración. Vamos a probar que si $P \in 2\mathcal{C}(\mathbb{Q}) - \{\mathcal{O}\}$ entonces $T(P) \in 2\mathcal{C}'(\mathbb{Q}) - \{\mathcal{O}\}$, la demostración en el otro sentido es análoga. Sea $Q = (u, v) \in \mathcal{C}(\mathbb{Q})$ tal que $2Q = P$, entonces $T(Q) = (u + a, v)$, para un cierto $a \in \mathbb{Q}$ y la curva trasladada será $\mathcal{C}' : y^2 = f(x - a)$, claramente $T(Q) \in \mathcal{C}'(\mathbb{Q})$.

Si $\mathcal{L} : y = mx + n$ es la recta tangente a $\mathcal{C}$ en Q y $\mathcal{L}' : y = m'x + n'$ es la recta tangente a $\mathcal{C}'$ en Q', como $\mathcal{C} : y^2 = f(x)$ sabemos que m es $f'(x)/2y$ evaluado en (u, v) y como $\mathcal{C}' : y^2 = f(x - a)$ tenemos que $m' = f'(x - a)/2y$ evaluado en $(u + a, v)$. Obtenemos por tanto que $m = m'$.

Al trasladar la recta $\mathcal{L}$ mantendrá su pendiente, y además pasará por el punto $T(Q)$, como hemos demostrado que $\mathcal{L}$ trasladada y $\mathcal{L}'$ pasan por el mismo punto y tienen la misma pendiente, hemos demostrado que son iguales. Tenemos que $-P = (s, -t)$ está en $\mathcal{L}$ porque $2Q = P$, entonces $T(-P) = (s + a, -t) = -T(P) \in \mathcal{C}'(\mathbb{Q}) - \{\mathcal{O}\}$ está en $\mathcal{L}'$, de donde $2T(Q) = T(P)$, lo que demuestra que $T(P) \in 2\mathcal{C}'(\mathbb{Q}) - \{\mathcal{O}\}$.

□

Lema 3.5. *Sea $\mathcal{C} : y^2 = f(x) = x^3+ax^2+bx+c$ una curva elíptica y $P = (x_1, y_1)$ un punto de la curva distinto de $\mathcal{O}$, entonces existe $Q = (x_0, y_0) \in \mathcal{C}(\mathbb{C})$ tal que $2Q = P$.*

Demostración. Si $2Q = P$, esto significa que la recta tangente a $\mathcal{C}$ en Q corta a $\mathcal{C}$ en $-P = (x_1, -y_1)$. Llamamos $\mathcal{L}$ a dicha recta. Si suponemos que $x_0 = x_1$, entonces $\mathcal{L}$ debe ser $x = x_0$, pues es la única recta que pasa por $-P$ y Q. Como $\mathcal{L}$ es una recta paralela al eje Y, corta a $\mathcal{C}$ en $\mathcal{O}$, de donde $2Q = \mathcal{O}$, por lo que $P = \mathcal{O}$, lo cual es absurdo.

Por lo tanto como la recta $\mathcal{L}$ pasa por (x_0, y_0) y $(x_1, -y_1)$, donde $x_0 \neq x_1$, entonces la pendiente de la recta viene dada por

$$m = \frac{-y_1 - y_0}{x_1 - x_0}.$$

Como $\mathcal{C} : y^2 = f(x)$, al derivar encontramos que la pendiente de la recta tangente a $\mathcal{C}$ en (x_0, y_0) debe ser $m = f'(x_0)/2y_0$. Por lo que una condición sobre el punto (x_0, y_0) que estamos buscando es que

$$\frac{f'(x_0)}{2y_0} = \frac{-y_1 - y_0}{x_1 - x_0},$$

o equivalentemente $f'(x_0)(x_1 - x_0) - 2y_0(-y_1 - y_0) = 0$. Como $f(x)$ es un polinomio de grado 3, tenemos que la ecuación anterior define una cúbica sobre las variables x_0, y_0. Homogeneizando el anterior polinomio obtenemos

$$F(x_0, y_0, z_0) = -3x_0^3 + (3x_1 - 2a)x_0^2 z_0 + (2ax_1 - b)x_0 z_0^2 + 2y_1 y_0 z_0^2 + 2y_0^2 z_0.$$

Podemos ver que $\mathcal{O} = (0 : 1 : 0)$ es un punto de la curva $\mathcal{C}_F$ definida por F. Ahora bien, la derivada de F con respecto a z_0 es

$$\frac{\partial F}{\partial z_0} = (3x_1 - 2a)x_0^2 + (4ax_1 - 2b)x_0 z_0 + 4y_1 y_0 z_0 + 2y_0^2,$$

y al sustituir $(x_0 : y_0 : z_0)$ por $(0 : 1 : 0)$ en la expresión anterior obtenemos 2, por lo que $\mathcal{O}$ no es un punto singular de $\mathcal{C}_F$.

La otra condición que debemos imponer al punto (x_0, y_0) es que se encuentre en $\mathcal{C}$. Así que buscamos los puntos de intersección entre $\mathcal{C}_F$ y $\mathcal{C}$.

Al ser la intersección entre dos cúbicas proyectivas en $\mathbb{PC}^2$, podemos deducir como consecuencia del Teorema de Bézout que se intersectarán en 9 puntos contando multiplicidades, o bien en infinitos, en el caso de que tengan componentes en común.

Vimos que $\mathcal{O}$ es un punto que se encuentra tanto en $\mathcal{C}$ como en $\mathcal{C}_F$, pero tiene multiplicidad 1 dado que $\mathcal{O}$ no es un punto singular de $\mathcal{C}_F$ ni de $\mathcal{C}$, de donde deducimos que existe al menos un punto de intersección $R = (x' : y' : z') \in \mathbb{PC}^2$, $R \neq \mathcal{O}$.

Recordemos que el único punto en el infinito de $\mathcal{C}$ es $\mathcal{O}$, por lo que necesariamente R no es un punto en el infinito, y esto significa que hemos encontrado $Q = (x'/z', y'/z') \in \mathcal{C}(\mathbb{C})$ que verifica $2Q = P$.

□

Proposición 3.6. *Sea $\mathcal{C} : y^2 = (x - e_1)(x - e_2)(x - e_3)$ una curva elíptica con $e_1, e_2, e_3 \in \mathbb{Q}$ distintos entre sí y sea $P = (x_0, y_0) \in \mathcal{C}(\mathbb{Q})$, $P \neq \mathcal{O}$. Entonces $P \in 2\mathcal{C}(\mathbb{Q}) - \{\mathcal{O}\}$ si y solo si $x_0 - e_1$, $x_0 - e_2$ y $x_0 - e_3$ son cuadrados de números racionales.*

Demostración. Sin pérdida de la generalidad, podemos suponer que $x_0 = 0$, ya que podemos considerar la traslación $x' = x - x_0$. La curva $\mathcal{C}$ al ser trasladada pasa a ser $\mathcal{C}' : y^2 = (x - e_1')(x - e_2')(x - e_3')$, donde $e_i' = e_i - x_0$. Si $P' = (0, y_0)$, por el Lema 3.4 tenemos que $P \in 2\mathcal{C}(\mathbb{Q}) - \{\mathcal{O}\}$ si y solo si $P' \in 2\mathcal{C}'(\mathbb{Q}) - \{\mathcal{O}\}$. Además, $x_0 - e_i$ son cuadrados si y solo si $-e_i'$ lo son. Por lo que probaremos la proposición para $x_0 = 0$.

Nótese que si existe $Q \in \mathcal{C}(\mathbb{Q})$ tal que $2Q = P$, entonces podemos considerar $Q_i = Q + (e_i, 0)$, debido a que $(e_i, 0) \in \mathcal{C}(\mathbb{Q})$ es un punto de orden 2 gracias al Lema 2.20, sabemos que $2Q_i = P$, por lo que en realidad existirían 4 puntos verificando dicha condición.

Sabemos por el Lema 3.5 que existe un punto $Q \in \mathcal{C}(\mathbb{C})$ verificando que $2Q = P$, queremos ver bajo qué condiciones podemos garantizar que dicho punto

es racional. Nuestra estrategia a seguir será demostrar que Q es un punto racional si y solo si la pendiente de la recta de $-P$ a Q es racional, y luego demostrar que dicha pendiente es racional si y solo si $-e_1$, $-e_2$ y $-e_3$ son cuadrados.

Sea $Q = (x_1, y_1)$ y $-P = (0, -y_0)$. Notamos que $x_1 \neq 0$, pues de no ser así $x = 0$ sería la recta que corta a Q y $-P$, que también corta en $\mathcal{O}$, de donde $P = \mathcal{O}$, lo cual es absurdo. Por lo que la recta que pasa por Q y $-P$ vendrá dada por $\mathcal{L} : y = mx - y_0$.

Por un lado, si suponemos que Q es un punto racional, tenemos que $m = (y_1 + y_0)/x_1$ y por lo tanto m es racional. Por otro lado, si suponemos que m es racional, al sustituir en la ecuación que define $\mathcal{C}$ entonces x_1 es la raíz doble del polinomio $(mx - y_0)^2 - (x - e_1)(x - e_2)(x - e_3)$, además 0 es una raíz puesto que $-P$ es un punto de intersección, por lo que el anterior polinomio es $x(x - x_1)^2 \in \mathbb{Q}[x]$. Deducimos así que x_1 es racional, y como $y_1 = mx_1 - y_0$, también y_1 lo es, por consiguiente Q es racional.

Tenemos que m será la pendiente de una recta que pasa por $-P$ y es tangente a $\mathcal{C}$ en un punto si y solo si la siguiente ecuación tiene una raíz doble:

$$(mx - y_0)^2 = (x - e_1)(x - e_2)(x - e_3) = x^3 + ax^2 + bx + c, \tag{3.2}$$

con

$$a = -e_1 - e_2 - e_3, \quad b = e_1e_2 + e_1e_3 + e_2e_3, \quad c = -e_1e_2e_3 = y_0^2, \tag{3.3}$$

donde la última igualdad $c = y_0^2$ es debida a que $(0, y_0)$ es un punto de la curva $y^2 = x^3 + ax^2 + bx + c$. Si simplificamos (3.2) y sacamos factor común x, la condición en (3.2) se convierte en que la siguiente ecuación cuadrática tenga una raíz doble:

$$x^2 + (a - m^2)x + (b + 2my_0) = 0.$$

Esto es equivalente a que el discriminante del anterior polinomio sea 0, es decir,

$$(a - m^2)^2 - 4(b + 2my_0) = 0. \tag{3.4}$$

Por lo tanto nuestra tarea es determinar cuando las raíces del anterior polinomio de grado 4 son racionales, veremos que es equivalente a que $-e_1$, $-e_2$, $-e_3$ sean cuadrados. Sea $f_i = +\sqrt{-e_i}$, dado que e_1, e_2, e_3 son racionales distintos, al menos dos de ellos son distintos de 0, de donde

$$(f_1, f_2, f_3), \quad (-f_1, -f_2, f_3), \quad (f_1, -f_2, -f_3), \quad (-f_1, f_2, -f_3),$$

son cuatro ternas distintas. Tomamos (g_1, g_2, g_3) una de las ternas anteriores. Tenemos que $g_i^2 = f_i^2 = -e_i$. Definimos $s_1 = g_1 + g_2 + g_3$, $s_2 = g_1g_2 + g_1g_3 + g_2g_3$ y $s_3 = g_1g_2g_3$. Entonces, recordando (3.3)

$$\begin{aligned} &a = g_1^2 + g_2^2 + g_3^2 = s_1^2 - 2s_1 \ ; \\ &b = g_1^2g_2^2 + g_1^2g_3^2 + g_2^2g_3^2 = s_2^2 - 2s_1s_3 \ ; \\ &y_0 = s_3. \end{aligned}$$

La ecuación (3.4) pasa a ser

$$\begin{aligned} 0 &= (m^2 - s_1^2 + 2s_2)^2 - 4(s_2^2 - 2s_1s_3 + 2ms_3) \\ &= (m^2 - s_1^2)^2 + 4s_2(m^2 - s_1^2) - 8s_3(m - s_1). \end{aligned}$$

El polinomio anterior es divisible por $(m - s_1)$, es decir, $m = s_1 = g_1 + g_2 + g_3$ es una raíz. Como toda esta discusión ha sido independiente de la elección de (g_1, g_2, g_3), en realidad hemos encontrado las cuatro raíces del polinomio que son:

$$\begin{aligned} m_1 &= f_1 + f_2 + f_3, \quad & m_2 &= -f_1 - f_2 + f_3, \\ m_3 &= f_1 - f_2 - f_3, \quad & m_4 &= -f_1 + f_2 - f_3. \end{aligned}$$

Está claro que si $f_1,\ f_2,\ f_3$ son racionales entonces también lo son $m_1,\ m_2,\ m_3,\ m_4$. Por otro lado si suponemos que las pendientes son racionales, tenemos que $f_1 = (m_1 + m_3)/2,\ f_2 = (m_1 + m_4)/2$ y $f_3 = (m_1 + m_2)/2$ son racionales. En conclusión un punto Q tal que $2Q = P$ es racional si y solo si los $f_i = \sqrt{-e_i}$ son racionales.

□

Introducimos ahora la siguiente curva asociada a n y θ, donde recordemos que los valores de r y s están determinados por θ.

$$\mathcal{C}_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n).$$

Proposición 3.7. *La curva $\mathcal{C}_{n,\theta}$ es elíptica.*

Demostración. Al homogeneizar el polinomio que define la curva $\mathcal{C}_{n,\theta}$ obtenemos $F(x, y, z) = x^3 + 2nsx^2z - n^2(r^2 - s^2)xz^2 - zy^2$. Para demostrar que es una curva elíptica tenemos que garantizar que no tiene puntos singulares, es decir, que el siguiente sistema no tiene solución.

$$\begin{cases} \frac{\partial F}{\partial x} = 3x^2 + 4nsxz - n^2(r^2 - s^2)z^2 = 0 \\ \frac{\partial F}{\partial y} = -2yz = 0 \\ \frac{\partial F}{\partial z} = 2nsx^2 - 2n^2(r^2 - s^2)xz - y^2 = 0. \end{cases} \tag{3.5}$$

De la segunda ecuación en (3.5), podemos deducir que $z = 0$ o $y = 0$, si suponemos lo primero, la primera ecuación se reduce a $3x^2 = 0$, de donde $x = 0$, y finalmente de la tercera ecuación obtenemos que $y^2 = 0$, pero $(0 : 0 : 0)$ no es un punto del plano proyectivo.

Por lo tanto, nos queda estudiar el caso $y = 0$. Podemos sacar factor común x en la tercera ecuación de (3.5), de modo que $x(2nsx - 2n^2(r^2 - s^2)z) = 0$, de aquí podemos decir que $x = 0$, o $nsx - n^2(r^2 - s^2) = 0$.

Al suponer que $x = 0$, como también $y = 0$, la primera ecuación de (3.5) se reduce a $n^2(r^2 - s^2)z^2 = 0$, sabemos que $n \neq 0$ y además que $r^2 \neq s^2$, ya que

de otra forma $\cos\theta = s/r = \pm 1$, y esto no puede ser pues θ es el ángulo de un triángulo y verifica que $0 < \theta < \pi$. Esto quiere decir que $z = 0$, y de nuevo no obtenemos un punto del plano proyectivo.

Nos falta ver qué ocurre si $nsx - n^2(r^2 - s^2)z = 0$, ya que como vimos antes $n^2(r^2 - s^2) \neq 0$, entonces $z = (sx)/(n(r^2 - s^2))$. Al sustituir esto en la primera ecuacion de (3.5), nos queda

$$0 = 3x^2 + \frac{4(sx)^2}{(r^2 - s^2)} - \frac{(sx)^2}{(r^2 - s^2)} = x^2\left(3 + \frac{3s^2}{r^2 - s^2}\right).$$

El caso $x = 0$, ya habíamos visto que no conducía a ninguna solución, por lo que llegamos a que $3s^2 = -3(r^2 - s^2)$, es decir, $r = 0$, esto es absurdo ya que $\cos\theta = s/r \in \mathbb{Q}$.

□

Teorema 3.8. *El número n es θ-congruente si y solo si $\mathcal{C}_{n,\theta}$ tiene un punto racional de orden mayor que 2.*

Demostración. Por la Proposición 3.3, n es θ-congruente si y solo si existe un número racional x tal que $x,\ x+(r+s)n,\ x-(r-s)n$ son cuadrados de racionales. Ahora, por la Proposición 3.6 aplicada a $\mathcal{C}_{n,\theta}$ esto implica que n es θ-congruente si y solo si existe un punto P en $2\mathcal{C}_{n,\theta}(\mathbb{Q}) - \{\mathcal{O}\}$, esto es si y solo si existe un punto de $\mathcal{C}_{n,\theta}(\mathbb{Q})$ de orden mayor que 2.

□

Ejemplo 3.9. Tal y como vimos en el Ejemplo 3.2, 1 es $\pi/3$-congruente. Ahora intentaremos demostrarlo mediante el Teorema 3.8: la curva asociada es $\mathcal{C}_{1,\pi/3}$: $y^2 = x(x-1)(x+3)$. Apliquemos el Teorema de Nagell-Lutz para encontrar los puntos de orden finito.

El discriminante de la ecuación de la curva $\mathcal{C}_{1,\pi/3}$ es $\Delta = 100$. Si probamos con $y = 2 \mid \Delta$, podemos ver $4 = x(x-1)(x+3)$ tiene una raíz racional $x = -1$, por lo tanto el punto $P = (-1, 2)$ es candidato a ser un punto de orden finito. De hecho la recta tangente a $\mathcal{C}_{1,\pi/3}$ en P es $y = -x + 1$ que corta a $\mathcal{C}_{1,\pi/3}$ en $(1, 0)$ el cual es un punto de orden 2, de donde concluimos que P es un punto de orden 4, y necesariamente que 1 es $\pi/3$-congruente.

De hecho podemos consultar [13], para ver que $\mathcal{C}_{1,\pi/3}(\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. Por lo que en realidad, al contrario de lo que ocurría con los números congruentes o $\pi/2$-congruentes, el rango de esta curva sobre $\mathbb{Q}$ es 0.

Conclusiones

A lo largo del Capítulo 1 hemos estudiado el Problema del Número Congruente, estableciendo algunos criterios para encontrar números congruentes y no congruentes. En particular, se relacionó a los números congruentes con la existencia de puntos racionales de una cierta curva elíptica.

En el Capítulo 2 profundizamos en el estudio de las curvas elípticas, lo que nos permitió establecer una relación con el rango de ciertos grupos abelianos finitamente generados. Si bien es posible calcular los puntos de torsión de estos grupos en un número finito de pasos, y parte del segundo capítulo se dedica a esto, no ocurre lo mismo con el rango. Sin embargo, existen algunos métodos para calcularlo, en [16] se recogen algunos ejemplos.

Es posible continuar el estudio del problema del número congruente en [11], donde se encuentra uno de los resultados más importantes de este problema, el Teorema de Tunnell, que provee una condición necesaria para que un número sea congruente, pero que en el caso de que la *Conjetura de Birch y Swinnerton-Dyer*, uno de los problemas del milenio, sea cierta, nos permitiría determinar en un número finito de pasos si un número es congruente.

Bibliografía

[1] ANDREWS, G.E. Number Theory, Courier Corporation, 1994.

[2] CANO WALL, P. El teorema de Nagell-Lutz. TFG, Universidad de Sevilla, 2023.

[3] CHAHAL, J.S. Congruent Numbers and Elliptic Curves *The American Mathematical Monthly*, 2006, vol. 113, pp. 308–317.

[4] COATES, J.H. Congruent Number Problem. *Pure and Applied Mathematics Quarterly*, 2005, vol. 1, pp. 14–27.

[5] CONRAD, K. *The Congruent number problem*. Disponible en https://kconrad.math.uconn.edu/articles/congruentnumber.pdf.

[6] FUJIWARA, M. θ-Congruent Numbers, Number Theory K. Győry, A. Pethő and V. Sós (eds.), de Gruyter 235–241 (1997)

[7] GIBSON, C.G. Elementary Geometry of Algebraic Curves, Cambridge University Press, 1998.

[8] GORDON, R.A y GRAHAM, S.L. Comments on proofs that there are no four squares in arithmetic progression. *Fibonacci Quarterly*, 2015, vol. 53, pp. 68–73.

[9] HERNÁNDEZ YANES, W. G. Grupos en Curvas Elípticas. TFG, Universidad de La Laguna, 2022.

[10] HILMAR, J. y SMYTH, C. Euclid meets Bézout: Intersecting Algebraic Plane Curves with the Euclidean Algorithm, *The American Mathematical Monthly*, Vol. 117, No.3 (March 2010), pp. 250-260.

[11] KOBLITZ, N. Introduction to Elliptic Curves and Modular Forms. Springer, New York (1993).

[12] LEMMERMEYER, F. Parametrization of Algebraic Curves from a Number Theorist's Point of View *The American Mathematical Monthly*, 2012, vol. 119, pp. 573–583.

[13] LMFDB. Disponible en https://www.lmfdb.org/EllipticCurve/Q/.

[14] LMFDB. Disponible en https://www.lmfdb.org/EllipticCurve/Q/CongruentNumbers.

[15] SILVERMAN, J. H. y TATE, J. Rational Points on Elliptic Curves, 2nd edition, Springer-Verlag New York, INC, 1992.
[16] WASHINGTON, L. C. Elliptic Curves, Number Theory and Cryptography, 2nd edition, Chapman and Hall, 2008.

The Congruent Number Problem

Daniel Montesdeoca del Pino
Facultad de Ciencias • Sección de Matemáticas
Universidad de La Laguna
alu0101363394@ull.edu.es

Abstract

The congruent number problem consists of determining which numbers can be the area of a right triangle with three rational sides, such numbers are called congruent numbers. For this purpose, we need some results from the theory of elliptic curves.

1. Introduction

Definition. A number $n \in \mathbb{Q}$ is said to be congruent if there exist $A, B, C \in \mathbb{Q}^+$ such that

$$\begin{cases} A^2 + B^2 = C^2 \\ \frac{AB}{2} = n. \end{cases}$$

The congruent number problem asks which positive rational numbers are congruent numbers. One can show that the question reduces to finding which squarefree integers are congruent numbers.

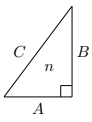


Figure 1: Right Triangle

Proposition. Let $n \in \mathbb{Z}^+$. The following statements are equivalent:

- There exists a right triangle with rational sides A, B, C and area n.
- There exist rational squares α^2, β^2, γ^2 which are in arithmetic progression with common difference n.
- The curve $\mathcal{C}_n : Y^2 = X^3 - n^2X$ has a rational point (x, y) with $y \neq 0$.

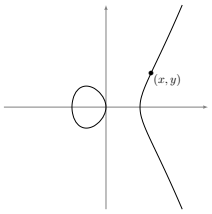


Figure 2: $\mathcal{C}_n : Y^2 = X^3 - n^2X$

2. Elliptic Curves

Definition. A projective elliptic curve $\mathcal{C} \subset \mathbb{PC}^2$ is a non-singular cubic.
There exists a binary operation $+$ such that the rational points of an elliptic curve form a finitely generated abelian group.

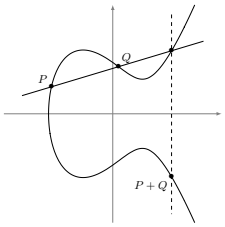


Figure 3: Binary operation $+$ on an Elliptic Curve

Definition. Let $\mathcal{C} : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve. The discriminant is defined to be

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Nagell-Lutz Theorem. Let $\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx + c$ be an elliptic curve, where $a, b, c \in \mathbb{Z}$. If $P = (x_0, y_0)$ is a rational torsion point then $x_0, y_0 \in \mathbb{Z}$ and $y_0 = 0$ or y_0 divides Δ.
Theorem. A number $n \in \mathbb{Z}^+$ is congruent if and only if the group associated to the rational points of the elliptic curve $\mathcal{C}_n$ has a positive rank.

3. θ-congruent numbers

Let X, Y, Z be the rational sides of a triangle and θ the angle between X and Y, then $\cos(\theta)$ is necessarily rational. Thus $\cos(\theta) = s/r$, where $\gcd(r, s) = 1$. We can define $\alpha_\theta = \sqrt{r^2 - s^2}$.
Definition. A number $n \in \mathbb{Z}^+$ is a θ-congruent number if there exists a triangle such that

- three sides are rational.
- one angle is θ.
- the area is $n\alpha_\theta$.

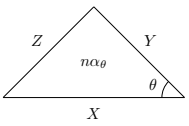


Figure 4: A triangle meeting all of the conditions above.

One can show that the following curve attached to n and θ is an elliptic curve

$$\mathcal{C}_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n).$$

Theorem. A number n is θ-congruent if and and only if there exists a rational point $(x_0.y_0)$ with $y_0 \neq 0$ in the elliptic curve $\mathcal{C}_{n,\theta}$.

References

[1] CONRAD, K. *The Congruent number problem*. URL: https://kconrad.math.uconn.edu/articles/congruentnumber.pdf.
[2] FUJIWARA, M. θ-Congruent Numbers, Number Theory K. Győry, A. Pethő and V. Sós (eds.), de Gruyter 235-241 (1997).
[3] SILVERMAN, J. H. y TATE, J. Rational Points on Elliptic Curves, 2nd edition, Springer-Verlag New York, INC, 1992.