Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

El problema del número congruente y generalizaciones

Trabajo de fin de grado

Grado en Matemáticas

Autor: Ana Torres López
Tutor: Enrique González Jiménez

Curso 2019-2020

Resumen

En este trabajo atacaremos el problema del número congruente desde el campo de las curvas elípticas.

Empezaremos con una introducción a este área de estudio, donde daremos varias definiciones y resultados importantes, como puede ser el 'Teorema de Bezout'. A continuación, estudiaremos el grupo que forman los puntos racionales de una curva elíptica ayudándonos del 'Algoritmo de Weierstrass' y de otros enunciados entre los que se encuentran el 'Teorema del descenso', el 'Teorema de Mordell' y el 'Teorema de Nagell-Nutz'. De todos ellos se dará una demostración. Por último, aplicaremos estos resultados a una curva elíptica estrechamente relacionada con el problema del número congruente, llegando a una formulación equivalente del mismo.

Al final del trabajo, daremos algunas generalizaciones del problema y enunciaremos el 'Teorema de Tunnell'.

Abstract

In this work the congruent number problem is tackled from the elliptic curve field point of view.

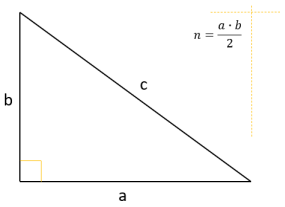
As an introduction, some definitions and important results, such as 'Bezout's Theorem', are presented. Then, the group formed by the set of rational points of an elliptic curve is studied with help of the 'Weierstrass Algorithm' and other statements among which are 'Descent Theorem', 'Mordell's Theorem' and 'Nagell-Lutz's Theorem'. Proof is provided for all of them. Lastly, all these results are applied to an elliptic curve that is closely related to the congruent number problem in order to get an equivalent formulation of the latter.

At the end of the work, some generalizations of the problem are exposed and 'Tunnell's Theorem' is stated.

Índice general

Introducción

Dado un $n \in \mathbb{N}$ ¿Existe un triángulo rectángulo de lados racionales (a,b,c) tal que su área sea n?



Este es el problema que nos atañe y por el que tiene existencia este trabajo.

El problema del número congruente es un problema con un enunciado corto, simple y sencillo que en absoluto requiere un basto conocimiento matemático para poder comprenderlo. Pero, cuidado, que las apariencias no nos engañen: este problema, al igual que muchos otros de afable enunciado, ha sido, y sigue siendo, un verdadero quebradero de cabeza para los matemáticos.

Este problema no siempre fue formulado de esta forma, con el paso del tiempo su caracterización ha ido cambiando. La primera de la que se tiene constancia es:

Sea n un número natural, decimos que n es congruente si existen cuadrados racionales α^2, β^2 y γ^2 en progresión aritmética tal que n sea su razón.

Y esta evolucionó con el paso del tiempo al enunciado, equivalente, que expusimos al principio.

Ya desde la *Aritmética* de Diofanto, siglo III D.C, se observa cierto interés por este tipo de números, también pueden encontrarse referencia a estos en manuscritos chinos del siglo VIII D.C y manuscritos árabes que datan de 972 D.C. Es considerado el problema no resuelto más longevo de la teoría de números. Por ejemplo:

- Tian Ye, 2014: Para cada $k \geq 0$ existen infinitos $n \equiv 5, 6, 7 (\text{mod } 8)$, con n libre de cuadrados, congruentes con exactamente $k + 1$ factores primos impares (ver [12]).

Uno de los resultados más importantes es el que dio Fermat en 1659:

1, 2 y 3 no son números congruentes.

La importancia de este enunciado radica no solo en que el hecho de que 1 no sea congruente demuestra la conjetura de Fermat para $n = 4$, si no en el hecho de que Fermat utilzó por primera vez el método del descenso infinito para resolver el caso de $n = 1$. Este método fue, y es, muy utilizado y supuso una revolución en la aritmética de la época.

Como se puede intuir por la longevidad de este problema, este ha sido atacado desde distintos campos de la matemáticas. En este trabajo optaremos por estudiarlo desde el campo de las curvas elípticas. Como veremos en el capítulo 5, a través de una serie de operaciones elementales pero no triviales, podemos obtener un problema equivalente al nuestro en dicho campo:

n, libre de cuadrados, es congruente.	$\Leftrightarrow$	*La curva* $E_n: \ y^2 = x^3 - n^2x$ *tiene un* $P = (x, y) \ \ con \ \ x, y \in \mathbb{Q} \ \ e \ \ y \neq 0.$

No hay inconveniente en el hecho de suponer que n es libre de cuadrados ya que, como veremos, para $n, n', s \in \mathbb{N}$ si $ns^2 = n'$ con n libre de cuadrados, entonces n es congruente si y solo si lo es n'. Desarrollaremos la teoría de curvas elípticas para ver qué resultado podemos conseguir sobre la curva elíptica, E_n, asociada al problema del número congruente. Este desarrollo estará distribudo de la siguiente forma:

- **Capítulo 1:** Daremos varias definiciones básicas, necesarias para desarrollar la teoría de curvas elípticas. Además, veremos varios resultados importantes. Entre ellos estará 'El Teorema de Bezout', cuya demostración, por falta de espacio, está en el Apéndice A.
- **Capítulo 2:** Veremos que toda curva proyectiva plana de grado 3 sobre un cuerpo K, con $char(K) \neq 2, 3$, es isomorfa a otra que está en su forma corta de Weierstrass. Dicha demostración está en Apéndice B por falta de espacio. Además, se verá que el conjunto de puntos racionales, $E(\mathbb{Q})$, de una curva elíptica E, con una cierta operación que definiremos en dicho apartado, tiene una estructura de grupo.
- **Capítulo 3:** Daremos enunciado a teoremas muy importantes en la teoría de curvas elípticas como pueden ser: 'El Teorema del descenso', 'El Toerema Débil de Mordell' o 'El Teorema de Mordell'. Todos estos teoremas, y resultado previos, están demostrados entre el Capítulo 3 y el Apéndice C, por falta de espacio.
- **Capítulo 4:** Veremos qué es la filtación p-ádica y varios resultados relacionados con ella, como puede ser el 'Teorema de Nagell-Lutz'. Lo más importante de este capítulo será demostrar que, bajo algunas condiciones, existe un homomorfismo inyectivo entre el grupo de torsión de curva elíptica E y el grupo $E_p(\mathbb{F}_p)$. Así como utilizar este resultado para demostrar que el subgrupo de torsión de $E_n(\mathbb{Q})$, con n libre de cuadrados, es isomorfo a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.
- **Capítulo 5:** Utilizaremos el hecho de que $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ es isomorfo al grupo de torsión de $E_n(\mathbb{Q})$ para ver que n, libre de cuadrados, es congruente si y solo si el rango de $E_n(\mathbb{Q})$ es estrictamente mayor que 0.

CAPÍTULO 1

Curvas: de lo intuitivo a la definición.

Comencemos por definir los conceptos más importantes de este trabajo y sobre los que se cimentará todo.

Definición 1.1. *Dado un polinomio* ***F(x,y,z)****, homogéneo de grado* $d > 0$*, definido sobre un cuerpo* ***k****. Se define* ***la curva proyectiva plana****,* ***C****, dada por* ***F*** *como:*

$$C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = 0\}.$$

De la misma forma que tenemos grados e irreducibilidad para los polinomios, también los tenemos para las curvas proyectivas planas.

Definición 1.2. *El grado de una curva proyectiva plana* ***C*** *se define como el grado de* ***F****.*

Definición 1.3. *Se dice que la curva proyectiva plana* ***C*** *es* ***irreducible****, si* ***F*** *es un polinomio irreducible.*

Definición 1.4. *Decimos que* $P = [x_1, y_1, z_1]$ *es un* ***punto singular*** *de* ***C****, si* $P \in C$ *y*

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0,$$

con las parciales como la derivada formal con respecto a la variable correspondiente. Además, decimos que C es ***lisa o no singular*** *si no tiene puntos singulares.*

Definimos, de igual manera que en *Análisis Matemático*, el plano (en nuestro caso será recta pues estamos en $\mathbb{P}^2$) tangente en un punto, P, a la curva.

Definición 1.5. Sea P un punto no singular de C, definimos la tangente a la curva como:

$$\frac{\partial F}{\partial x}(P) \cdot X + \frac{\partial F}{\partial y}(P) \cdot Y + \frac{\partial F}{\partial z}(P) \cdot Z = 0.$$

Definición 1.6. Definiremos la **curva afín** de C, como C' con:

$$C' = \{(x, y) \in \mathbb{A}^2 : f(x, y) = F(x, y, 1) = 0\}.$$

Observa que hay una correspondencia uno a uno entre los puntos de C' y los puntos de C de la forma $[x, y, 1] \in C$. Para los puntos $[x, y, z] = P \in C$ con $z \neq 0$ diremos que **están en la parte afín de C** y que su **coordenada afín o no homogénea** es

$$(x', y') = P' := \left(\frac{x}{z}, \frac{y}{z}\right).$$

Notemos que $P' \in C'$. A los puntos de la forma $[x, y, 0] \in C$, los llamaremos *puntos del infinito*.

Definición 1.7. Diremos que $P \in \mathbb{A}^2$, con $P \in C'$, es **singular** si

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

C' será **lisa o no singular** si no tiene puntos singulares.

Definición 1.8. Sea $P = (a, b)$ un punto no singular de C', definimos la tangente a la curva como:

$$\frac{\partial f}{\partial x}(P) \cdot (x - a) + \frac{\partial f}{\partial y}(P) \cdot (y - b) = 0.$$

Observación 1.9.

- Si C es lisa $\Rightarrow$ C' es lisa.
- $[x_0, y_0, 1] \in C$ es no singular $\Leftrightarrow$ (x_0, y_0) es no singular en C'.
- Sea $[x, y, 1] = P \in C$ y $P' \in C'$ su correspondientes coordenada no homogénea, entonces

$$\begin{array}{ccc} L := aX + bY + cZ = 0 \text{ es recta} \\ \text{tangente a } C \text{ en } P. \end{array} \Leftrightarrow \begin{array}{c} L := ax + by + c = 0 \text{ es recta} \\ \text{tangente a } C' \text{ es } P'. \end{array}$$

1.1. Intersecciones y cotas.

Dadas las curvas:

$$C_1 : \ x + y + z = 0 \quad \text{y} \quad C_2 : x^2 + y^2 + z^2 = 0,$$

podemos, de manera sencilla, calcular los puntos de intersección. Basta separar por casos, por un lado, los puntos con $z = 1$, y por otro, los puntos con $z = 0$, despejar en C_1 y sustituir en C_2. De esta forma obtenemos los puntos

$$[1, 0, 1] \quad \text{y} \quad [3, -2, 1].$$

Pero... ¿y si las potencias de C_2 fuesen sextas y las de C_1 quintas? O ¿y si fuesen dos curvas totalmente distintas, cómo podríamos calcular los puntos de intersección? Pues a esta pregunta, por lo general, no hay respuesta.

Pero que no decaigan los ánimos porque lo que sí que podemos dar es una cota, si es que la hay, del número de puntos que hay en la intersección de dos curvas proyectivas

planas y, por ende, de sus afines. Más aún, dado un conjunto de puntos contenido en la intersección, podemos decir si este es la intersección al completo o falta alguno.

Para lograr esto definiremos un función que dependerá de C_1 y C_2 y que llevará a cada punto de $\mathbb{P}^2$ a un número natural. Diremos que dicho número natural es el índice de P (con respecto a C_1 y C_2):

$$\begin{array}{rcl} I(C_1, C_2) : \mathbb{P}^2 & \longrightarrow & \mathbb{N} \\ P & \longrightarrow & I_P(C_1, C_2) \end{array}$$

Dicho número natural será 0 para todo punto $P \notin C_1 \cap C_2$ y mayor que 0 en caso contrario. De esta forma, para todo conjunto finito $S \subset \mathbb{P}^2$, daremos una cota $M_{(C_1,C_2)}$, no dependiente de S, tal que

$$\sum_{P \in S} I_P(C_1, C_2) \leq M_{(C_1,C_2)}.$$

Observemos que esta función 'cuenta', al menos una vez, cada punto de la intersección de C_1 y C_2 y 'descarta' u 'obvia' aquellos que no están. A esta función además de pedirle lo dicho, le exigiremos algunas cosas más:

(1) $I_P(C_1, C_2) = I_P(C_2, C_1)$.

(2) $I_P(C_1, C_2) = \infty$ si P pertenece a una componente en común de C_1 y C_2.

(3) $I_P(C_1, C_2) = 0$ si y solo si $P \notin C_1 \cap C_2$.

(4) Para dos rectas distintas, el único punto de intersección tiene índice 1.

(5) Si C_1 y C_2 están definidas por $F_1(x, y, x)$ y $F_2(x, y, z)$, respectivamente y C está definida por
$$F(x, y, z) = F_1(x, y, z) \cdot F_2(x, y, z)$$
entonces para D una curva
$$I_P(C, D) = I_P(C_1, D) + I_P(C_2, D).$$

(6) Si los polinomios que definen a C_1 y C_2, son F y G respectivamente, y tenemos que el polinomio $FR+G$, con R un polinomio homogéneo de grado $m-n$, define la curva E entonces:
$$I_P(C_1, C_2) = I_P(C_1, E).$$

(7) Esta función no dependerá de las coordenadas que tomemos.

La primera condición es natural, no tendría mucho sentido que el nombre u orden que demos a las curvas varíe $I_P(C_1, C_2)$. La segunda tiene una razón de ser clara, cuando dos curvas tienen componentes en común, comparten infinitos puntos, por lo que no tiene sentido tratar de encontrar una cota $M_{(C_1,C_2)}$ para los conjuntos finitos S. La tercera condición ya la hemos explicado, 'contar' solo aquellos puntos que estén en la intersección. La cuarta corresponde a la idea intuitiva, y cierta, de que solo

puede haber un punto en la intersección de dos rectas. La quinta es también natural, pues viene a decir que 'contaremos' los puntos tantas veces como aparezcan en las distintas componentes de la curva. La séptima es bastante lógica ya que no tendría mucho sentido, en principio, pensar que un simple cambio de coordenadas debiera afectar a cómo 'contamos' los puntos. La sexta es quizás la menos natural pero hace que, junto con las otras seis, el siguiente enunciado sea cierto.

Teorema 1.10. *Hay una única función $I_P(C_1, C_2)$ sobre dos curvas planas C_1 y C_2 que cumpla estas siete condiciones.*

La importancia de este enunciado radica en, además de la existencia, la unicidad - que no demostraremos-. La unicidad hace que cualquiera dos funciones que definamos y que cumplan estas siete condiciones, sean la misma. Aunque en este trabajo no daremos más que una definición de $I_P(C_1, C_2)$, cabe destacar que esto da una gran versatilidad a la hora de demostrar propiedades de $I_P(C_1, C_2)$, además de demostrar la equivalencia de funciones, que en principio, no guardan relación.

A continuación daremos ciertas definiciones con el objetivo de dar una definición explícita de $I_P(C_1, C_2)$. Nótese que de esta forma estamos demostrando su existencia.

Definición 1.11. Sea $f(x, y),\ g(x, y) \in k[x, y]$. Decimos que $\phi = \frac{f(x,y)}{g(x,y)}$, con ϕ perteneciente al cuerpo de fracciones, K, de $k[x, y]$, está definida en P si $g(P) \neq 0$.

Definición 1.12. Definimos $\mathcal{O}_P$ como

$$\mathcal{O}_P = \{\phi \in K : \phi \text{ está definido en } P\}.$$

Sean C_1 y C_2 definidas por los polinomios homogéneos $F_1(x, y, z)$ y $F_2(x, y, z)$, respectivamente. Tomaremos para las siguientes definiciones $f_1(x, y) = F_1(x, y, 1)$ y $f_2(x, y) = F_2(x, y, 1)$.

Definición 1.13. Definimos $(f_1, f_2)_P$ como el ideal generado por f_1 y f_2 en $\mathcal{O}_P$.

Definición 1.14. Definimos

$$I_P(C_1, C_2) = \dim(\mathcal{O}_P/(f_1, f_2)_P),$$

para P no perteneciente a una componente común de C_1 y C_2 y para $P = [x, y, 1]$. Si P cumple que está en una componente en común entonces:

$$I_P(C_1, C_2) = \infty.$$

Si $P = [x, y, 0]$ entonces hacemos un cambio de coordenadas homogéneas de forma que $P = [x', y', 1]$ en la nuevas coordenadas y decimos que

$$I_P(C_1, C_2) = \dim(\mathcal{O}_P/(f_1, f_2)_P),$$

con $\mathcal{O}_P,\ f_1$ y f_2 en dichas coordenadas.

Veamos que cumple los siete puntos:

1. $I_P(C_1, C_2) = \dim(\mathcal{O}_P/(f_1, f_2)_P) = \dim(\mathcal{O}_P/(f_2, f_1)) = I_P(C_2, C_1)$.

2. Por definición.

3. Resultado A.1 de la demostración del Teorema de Bezout.

4. Proposición 1.15.

5. Es decir, según nuestra definición esto equivale a que.

$$\dim(\mathcal{O}_p/(h, f_1 \cdot f_2)_P) = \dim(\mathcal{O}_p/(h, f_1)_P) + \dim(\mathcal{O}_p/(h, f_2)_P).$$

Definamos los siguiente morfismos:

$$\begin{aligned} \psi : \mathcal{O}_P/(h, f_1)_P &\longrightarrow \mathcal{O}_P/(h, f_1 f_2)_P \\ \bar{g} &\longrightarrow \psi(\bar{g}) = \overline{gf_2}. \end{aligned}$$

$$\begin{aligned} \gamma : \mathcal{O}_P/(h, f_1 f_2)_P &\longrightarrow \mathcal{O}_P/(h, f_2)_P \\ \bar{g} &\longrightarrow \gamma(\bar{g}) = \bar{g}. \end{aligned}$$

Tenemos así la siguiente sucesión exacta:

$$\mathcal{O}_P/(h, f_1)_P \xrightarrow{\psi} \mathcal{O}_P/(h, f_1 f_2)_P \xrightarrow{\gamma} \mathcal{O}_P/(h, f_2)_P,$$

es decir, ψ es inyectiva, γ es sobreyectiva y $\ker(\gamma) = \mathrm{Im}(\psi)$. Las dos últimas no son difíciles de demostrar. Veamos que ψ es inyectiva:
Si $\psi(\bar{g}) = 0$ entonces $f_2 g = uh + v f_2 f_1$ con $u,\ v \in \mathcal{O}_P$. Elegimos un $S \in k[x, y]$ con $S(P) \neq 0$ y definimos $A,\ B,\ C \in k[x, y]$ de la siguiente manera:

$$Su = A, \quad Sv = B, \quad Sg = C.$$

Tomando estas definiciones obtenemos la siguiente igualdad: $f_2(C - Bf_1) = Ah \in k[x, y]$. Como h y f_2 son coprimos, h debe dividir a $C - Bf_1$, así que $C - Bf_1 = Dh$ con $D \in k[x, y]$. Entonces:

$$g = (B/S)f_1 + (D/S)h.$$

Es decir, $\bar{g} = 0$. Como es una sucesión exacta tenemos que

$$\mathcal{O}_P/(h, f_1 f_2)_P \cong \mathcal{O}_P/(h, f_1)_P \times \mathcal{O}_P/(h, f_2)_P.$$

6. Según nuestra definición

$$\dim(\mathcal{O}_P/(f_1, f_2)_P) = \dim(\mathcal{O}_p/(f_1, f_1 r + f_2)_P).$$

Pero tenemos que $(f_1, f_2)_P = (f_1, f_1 r + f_2)_P$, por lo que 6 también se cumple.

7. Basta considerar el isomorfismo

$$\begin{aligned} \gamma : k[x, y] &\longrightarrow k[x, y] \\ f(x, y) &\longrightarrow f(x - a, y - b). \end{aligned}$$

De esta forma tenemos que $\mathcal{O}_P \cong \gamma(\mathcal{O}_P) = \mathcal{O}_{P'}$, $(f_1, f_2)_P \cong \gamma((f_1, f_2)_P) = (f_1', f_2')_{P'}$ y $\gamma((f_1, f_2)_P) \subset \gamma(\mathcal{O}_P)$.

Teorema de Bezout. *Sean C_1 y C_2 curvas proyectivas planas sobre un cuerpo cerrado, k, de grano n y m respectivamente, sin componentes en común. Entonces*

$$\sum_{P \in C_1 \cap C_2} I_P(C_1, C_2) = m \cdot n.$$

Demostración. Ver Apéndice A.1. ♮

Proposición 1.15. Sea C_1 y C_2 curvas proyectivas planas y $P \in C_1 \cap C_2$. Entonces $I_P(C_1, C_2) = 1$ si y solo si P es un punto no singular de C_1 y C_2 y las tangentes en C_1 y C_2 son distintas.

Demostración. Ver Apéndice A.2. ♮

Corolario: *Sea L la recta tangente en P a C entonces*

$$I_P(C, L) \geq 2.$$

Proposición 1.16. Sea $f(x, y) \in k[x, y]$ y $P = (0, 0)$ -en coordenadas homogéneas $P = [0, 0, 1]$- tal que $f(P) = 0$, entonces:

$$I_P(f(x, y), y) = m,$$

donde x^m es la mayor potencia de x que divide a $f(x, 0)$.

Demostración. Es decir: $\dim(\mathcal{O}_P/(f(x, y), y)_P) = m$. Observamos que $(f(x, y), y)_P = (f(x, 0), y)_P$ por lo que

$$\dim(\mathcal{O}_P/(f(x, y), y)_P) = \dim(\mathcal{O}_P/(f(x, 0), y)_P).$$

Pero tenemos que $f(x, 0) = x^m g(x)$ con $g(P) \neq 0$ por lo que $\{1, x, x^2, \ldots, x^{m-1}\}$ genera $\mathcal{O}_P/(f(x, 0), y)_P$. ♮

Proposición 1.17. Toda curva plana lisa, C, es irreducible.

Demostración. Si fuese reducible entonces si F es el polinomio homogéneo que define a C, tendríamos que $F = G(x, y, z)H(x, y, z)$ con el grado de G y H mayor que 0. Por Bezout tenemos que debe de existir un P tal que $G(P) = F(P) = 0$. Por lo que derivando F con respecto a x, y, z y utilizando la regla del producto para derivar vemos que $\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$. ♮

1.2. ¿Estamos ante un punto de inflexión?

A continuación daremos la definición para lo que llamaremos *punto de inflexión*. Ambas son equivalentes.

Definición 1.18. *Sea C una curva proyectiva plana, $P \in C$ un punto no singular y L la recta tangente a C en P. Decimos entonces que P es un* ***punto de inflexión de C*** *si*

$$I_P(C_1, C_2) \geq 3.$$

Definición 1.19. *Definimos ahora el* ***hessiano de un polinomio F en el punto P*** *de igual manera que hacemos en análisis*

$$H_F(P) = \begin{vmatrix} \frac{\partial^2 F}{\partial x^2}(P) & \frac{\partial^2 F}{\partial xy}(P) & \frac{\partial^2 F}{\partial xz}(P) \\ \frac{\partial^2 F}{\partial yx}(P) & \frac{\partial^2 F}{\partial y^2}(P) & \frac{\partial^2 F}{\partial yz}(P) \\ \frac{\partial^2 F}{\partial zx}(P) & \frac{\partial^2 F}{\partial zy}(P) & \frac{\partial^2 F}{\partial z^2}(P) \end{vmatrix},$$

con la parciales de F como la derivada formal de F con respecto de las variables correspondientes.

Proposición 1.20. Sea C una curva proyectiva plana, $P \in C$ un punto no singular y L la recta tangente a C en P. P es un **punto de inflexión en C** si y solo si

$$H_F(P) = 0.$$

Observación 1.21. Si tenemos que P es un punto de inflexión de una curva proyectiva plana C de grado 3 y L es la recta tangente en C a P entonces, por el Teorema de Bezout, tenemos que

$$C \cap L = \{P\}.$$

Para demostrar la proposición 1.20 separaremos por casos en base al grado del polinomio F que define a C.

Proposición 1.22. Sea C una curva proyectiva irreducible de grado d. Entonces

$$\text{todos los punto de C son de inflexión} \Leftrightarrow d = 1.$$

Demostración. Para la primera definición tenemos que si C tiene grado 1 entonces la recta tangente L en todo punto P de C coincide con C. Se sigue el resultado de la definición de $I_P(C_1, C_2)$.

Para la segunda definición tenemos que si $F(x, y, z)$ es de grado 1 entonces

$$\frac{\partial^2 F}{\partial x_i, x_j}(P) = 0 \quad \forall P.$$

Por lo que $H_F(P) = 0$. Para la otra implicación consultar [5] (Lema 3.32). ♮

Proposición 1.23. Si C es una curva proyectiva irreducible de grado 2, entonces no tiene puntos de inflexión.

Demostración. Ver Apéndice A.3. ♮

Proposición 1.24. Sea C un curva lisa de grado $d \geq 3$. Entonces las definiciones son equivalente

Demostración. Ver Apéndice A.4. ♮

Definición 1.25. Sea C un curva proyectiva plana, F el polinomio homogéneo que la define y K un subcuerpo del cuerpo k sobre el que está definida C. Definimos el conjunto $C(K)$ como:

$$C(K) = \{[x, y, z] \in \mathbb{P}^2(K) : F(P) = 0\}.$$

CAPÍTULO 2

Esforzarse una vez para no volver a hacerlo.

En este capítulo veremos cómo podemos extraer información sobre algunos tipos de curva de forma muy sencilla. ¿El objetivo? El de todas las matemáticas, facilitarnos la vida. Una vez visto las curvas que nos interesan, trataremos reducir el resto de ellas a estos tipos mediante un algoritmo fácil de programar. De esta forma trabajaremos solo con curvas que nos ayuden a su estudio.

2.1. Primer tipo de curva que nos interesa.

Observemos pues la siguiente curva. Sea:

$$C = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 + a_2x^2z + a_4xz^2 + a_6z^3 = 0\}.$$

¿Cuántos puntos se encuentran en la intersección de con la recta $z = 0$?

$$\mathbf{x} \in C \cap \{z = 0\} = \{[x, y, z] \in \mathbb{P}^2 : F(x, y, 0) = 0\} \Rightarrow x = 0 \Rightarrow \mathbf{x} = [0, 1, 0].$$

Es decir, hay un único punto en la curva C con $z = 0$, lo que nos permite expresar C de la siguiente manera

$$C'(K) = \{(x, y) \in \mathbb{A}^2 : f(x, y) = y^2 + a_1xy + a_3y - x^3 + a_2x^2 + a_4x + a_6z = 0\} \cup \{[0, 1, 0]\},$$

con C' su parte afín y $f(x, y) = F(x, y, 1)$. ¿Y qué tipo de punto es el $[0, 1, 0]$? ¿Singular? ¿De inflexión? Veamos cuál es su recta tangente L:

$$L : \ \frac{\partial F}{\partial x}(P) \cdot X + \frac{\partial F}{\partial y}(P) \cdot Y + \frac{\partial F}{\partial z}(P) \cdot Z = 0.$$

Pero tenemos que

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0 \qquad \text{y} \qquad \frac{\partial F}{\partial z}(P) = (1)^2 \neq 0,$$

por tanto, su recta tangente es $L : \{z = 0\}$. Del Teorema de Bezout se sigue que es un punto de inflexión, pues, como acabames de ver, es el único punto de la curva que se encuentra en L, su recta tangente.

De todo esto deducimos que las curvas con la forma de C, se pueden ver como su afín más el punto $\mathcal{O} = [0, 1, 0]$ y que dicho $\mathcal{O}$ es un punto de inflexión. Puede que ahora al lector no le parezca este hecho de suma importancia, pero veremos en la última sección de este capítulo, como estas observaciones cobran relevancia.

2.1.1. Sub-tipo de este tipo de curva que nos interesa.

Definición 2.1. *Definimos el* ***discriminante de f****, con* $f(x) = x^3 + ax^2 + bx + c$*, como*

$$d = (\alpha_1 - \alpha_2) \cdot (\alpha_2 - \alpha_3) \cdot (\alpha_3 - \alpha_1)$$

con α_1, α_2 y α_3 *raíces de f.*

Podemos observar, mediante una serie de cálculos que, si además $f(x) = x^3 + Ax + B$, entonces

$$d = -4A^2 - 27B^2.$$

Definición 2.2. Sea C una curva tal que

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2 z = x^3 + Axz^2 + Bz^3\}.$$

definimos el **discriminante de C** como

$$\Delta = -16(4A^2 + 27B^2).$$

En el siguiente teorema vemos por qué nos interesan esta definiciones y observaciones, en principio, carentes de sentido.

Teorema 2.3. *Sea* C *una curva irreducibles definida sobre un cuerpo* K*, con* $char(K) \neq 2, 3$*, y de la forma*

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

Entonces

$$C \text{ es singular} \Leftrightarrow d = 0.$$

Demostración. Sabemos que el único punto con $z = 0$ es el $[0, 1, 0]$, que no es singular. Por lo que si hay alguno que lo es debe cumplir que es de la forma $[x, y, 1] \in C$. Si es singular entonces

$$\begin{aligned}
\frac{\partial F}{\partial x}(x_0, y_0, 1) &= -3x_0^2 - A = 0, \\
\frac{\partial F}{\partial y}(x_0, y_0, 1) &= 2y_0 = 0, \\
\frac{\partial F}{\partial z}(x_0, y_0, 1) &= y_0^2 - 2Ax_0 - 3B = 0.
\end{aligned}$$

De la segunda ecuación deducimos que $y_0 = 0$. Separamos en dos casos:

$\boxed{A = 0}$ Tenemos entonces que la escuaciones se reducen a

$$3x_0 = 0 \text{ y } 3B = 0 \Leftrightarrow x_0 = 0 \text{ y } B = 0 \Leftrightarrow d = 0.$$

$\boxed{A \neq 0}$ Entonces tenemos que $x_0 = -\frac{3B}{2A}$. Si sustituímos en la primera ecuación obtenemos que $\frac{(27B^2+4A^3)}{4A^2} = 0$. Esto ocurre si y solo si $d = 0$.

♮

2.2. Algoritmo de Weierstrass.

Lo prometido es deuda. A continuación veremos como para toda curva plana irreducible, C, definida sobre K de grado 3, se puede reducir, mediante transformaciones, a una curva del tipo

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2x + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

A las curva que están expresadas de esta forma diremos que están en su forma de Weierstrass. Para llevar a cabo esto necesitamos los siguientes ingredientes: Una curva y un punto $P \in C(K)$. Separaremos que dos casos:

1. **Tenemos una curva C y punto de inflexión, $P \in C(K)$.**

2. **Tenemos una curva cúbica C y punto no singular y no de inflexión, $P \in C(K)$.**

Demostración. Ver Apéndice B. ♮

2.2.1. Forma corta de Weierstrass.

El otro tipo de curve que nos interesaba era la siguiente

$$C = \{[x, y, z] \in \mathbb{P}^2 : \ y^2z - x^3 - Axz^2 - Bz^3 = 0\}.$$

Veamos como podemos llegar a ella a partir una curva en forma de Weiersstras. Sea

$$C = \{[x, y, z] \in \mathbb{P}^2 : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

Tenemos así que $[0, 1, 0] \in C$ es un punto de inflexión. Si lo ponemos en coordenada no homogéneas:

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

Si hacemos el cambio:

$$\begin{aligned} x &\longrightarrow x, \\ y &\longrightarrow \frac{1}{2}(y - a_1x - a_3), \end{aligned}$$

obtenemos:

$$y^2 = 4x^3 + b_1x^2 + 2b_2x + b_3,$$

con $b_1,\ b_2,\ b_3$ y b_4 constantes dependientes de $a_1,\ a_2,\ a_3,\ a_4$ y a_6. Ahora hacemos el cambio

$$x \longrightarrow \frac{x - 3b_2}{36},$$
$$y \longrightarrow \frac{y}{216},$$

sacando

$$y^2 = 4x^3 - c_4x - c_6.$$

con c_4 y c_6 constantes dependientes de b_1 ,b_2 y b_3. Así que, como ya es costumbre, hacemos el cambio

$$x \longrightarrow 4x,$$
$$y \longrightarrow 4^2y,$$

obtenemos que:

$$\boxed{y^2 = x^3 + Ax + B},$$

con A y B constantes dependientes de c_1 y c_2. Observar que todos los cambios son legales para $char(K) \neq 2, 3$.

2.3. Una curva y su grupo abeliano.

Definición 2.4. *Una **curva elíptica** es una curva proyectiva plana E lisa de grado 3 junto con un punto $\mathcal{O} \in E$. Se denota como $(E, \mathcal{O})$.*
Diremos que la curva elíptica $(E, \mathcal{O})$ detá definida sobre $\boldsymbol{K}$, y escribimos E/K, si E está definida sobre K y $\mathcal{O} \in E(K) = \{[x, y, z] \in E : [x, y, z] \in \mathbb{P}^2(K)\}$

En esta sección trataremos de dar estructura de grupo a una curva elíptica definida sobre K

$$(E(K), \mathcal{O}).$$

Sea E, una curva elíptica definida sobre un cuerpo K. Sea $P, Q \in E(K)$, definimos $P*Q$ como el tercer punto de intersección de la recta, L, que une a ambos con la curva E. $P * P$ lo definimos como el tercer punto de intersección de la recta, L, tangente a C en P con E. Observar que por Bezout tenemos que este punto existe y que:

- Si $P \neq Q$ e $I_P(E, L) = I_Q(E, L) = 1$ entonces $P * Q \neq P, Q$.
- Si $P \neq Q,\ I_P(E, L) = 2$ *e* $I_Q(E, L) = 1$ entonces $P * Q = P$.
- Si $I_P(E, L) = 2$ entonces $P * P \neq P$.
- Si $I_P(E, L) = 3$ entonces $P * P = P$.

Observación 2.5. De forma sencilla podemos ver que:

(1.) $P * Q = Q * P \ \ \forall P,\ Q \in E(K)$.

(2.) $(P * Q) * Q = P \quad \forall P,\ Q \in E(K)$.

Sin embargo $E(K)$, por lo general, no es un grupo con la operación $*$, pues suele carecer de un neutro. No obstante, podemos modificar un poco la operación para hacer de $E(K)$ un grupo.

Ley de grupo: Sea $P, Q \in E(K)$, L la recta que pasa por P y Q (la recta tangente a P en caso de que $P = Q$) y L' la recta que une $P*Q$ con $\mathcal{O}$ (en caso de que $P*Q = \mathcal{O}$, la recta tangente a ambos). Diremos que $P \oplus Q$ es el tercer punto de intersección:

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

Teorema 2.6. *Sea C una cúbica plana irreducible y C' y C'' dos cúbicas. Supongamos que $C \cap C' = \{P_1, \ldots, P_8, P_9\}$, con P_i puntos no singulares de C, sin ser necesariamente dinstintos. Supongamos que $C \cap C'' = \{P_1, \ldots, P_8, Q\}$. Entonces $Q = P_9$.*

Demostración. Para la demostración consultar [3] (Proposición 3. Pág. 124). ♮

Veamos que $(E(K), \mathcal{O}, \oplus)$ cumple que es un grupo.

Teorema 2.7. *Sea E una curva elíptica. Entonces $(E(K), \mathcal{O}, \oplus)$ es un grupo, es decir:*

1. ***Existe neutro:*** $P \oplus \mathcal{O} = P \quad \forall P \in E(K)$.
2. ***Conmutativa:*** $P \oplus Q = Q \oplus P \quad \forall P, Q \in E(K)$.
3. ***Existe inverso:*** *Para $P \in E(K), \exists P' \in E(K)$ tal que $P \oplus P' = \mathcal{O}$, que demostamos por $\ominus P$. Este punto es:*

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

4. ***Asociativa:*** *Para todo $P, Q, R \in E(K)$ se tiene que*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Demostración.

1. Tenemos que por definición $P \oplus \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$, por la observación 2.5.2.
2. Tenemos que:

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

3. Veamos que $P \oplus (\ominus P) = \mathcal{O}$.

$$\begin{aligned} P \oplus (\ominus P) &= (P * (\ominus P)) * \mathcal{O} = (P * ((\mathcal{O} * \mathcal{O}) * P)) * \mathcal{O} \\ &= (P * (P * (\mathcal{O} * \mathcal{O}))) * \mathcal{O} = (\mathcal{O} * \mathcal{O}) * \mathcal{O} \\ &= \mathcal{O}. \end{aligned}$$

4. Sean $P, Q, R \in E(K)$

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R) \Leftrightarrow ((P \oplus Q) * R) * \mathcal{O} = \mathcal{O} * (P * (Q \oplus R))$$
$$\Leftrightarrow (P \oplus Q) * R = P * (Q \oplus R)$$

Por lo que basta demostrar que $(P \oplus Q) * R = P * (Q \oplus R)$. Dispongamos de los siguientes puntos

$$\mathcal{O},\ P,\ Q,\ R,\ P * Q,\ P + Q,\ Q * R,\ Q + R.$$

Ahora generamos las siguientes 2 cúbicas

$$G_1 = r \cdot s \cdot t,$$
$$G_2 = l \cdot m \cdot n,$$

con $r,\ s\ , t\ , l\ , m\ $ y n rectas tal que:

r : la recta que pasa por $R, P + Q, R * (P + Q)$,
s : la recta que pasa por $P, Q, P * Q$,
t : la recta que pasa por $Q * R, \mathcal{O}, Q + R$,
l : la recta que pasa por $R, Q, Q * R$,
m : la recta que pasa por $P, Q + R, (Q + R) * P$ y
n : la recta que pasa por $P * Q, \mathcal{O}, P + Q$.

De esta forma tenemos que E y G_1 pasan por los 9 puntos $\mathcal{O},\ P,\ Q,\ R,\ P * Q,\ P + Q,\ Q * R,\ Q + R$ y $(P \oplus Q) * R$. Por otro lado, G_2 pasa por los 8 puntos $\mathcal{O},\ P,\ Q,\ R,\ P * Q,\ P + Q,\ Q * R,\ Q + R$, es decir, que $(P \oplus Q) * R$ debe encontrarse en G_2. Pero si $(P \oplus Q) * R \neq P * (Q \oplus R)$ entonces tendríamos que $\#(E \cap G_2) \geq 10 > 9 = 3 \cdot 3$, lo que es una contradicción. Por tanto,

$$(P \oplus Q) * R = P * (Q \oplus R).$$

♮

2.3.1. Fórmulas explícitas.

En esta sección se dará de forma explícita una fórmula para calcular las coordenadas del punto $P_3 \in E(K)$ con

$$P_3 = P_2 \oplus P_1 \quad \text{con } P_1,\ P_2 \in E(K).$$

Acabamos de ver en la sección 2.2 que para toda curva proyectiva plana, E, definida por un polinomio homogéneo de grado 3, mediante el algoritmo de Weierstrass, podemos encontrar un isomorfismo tal que

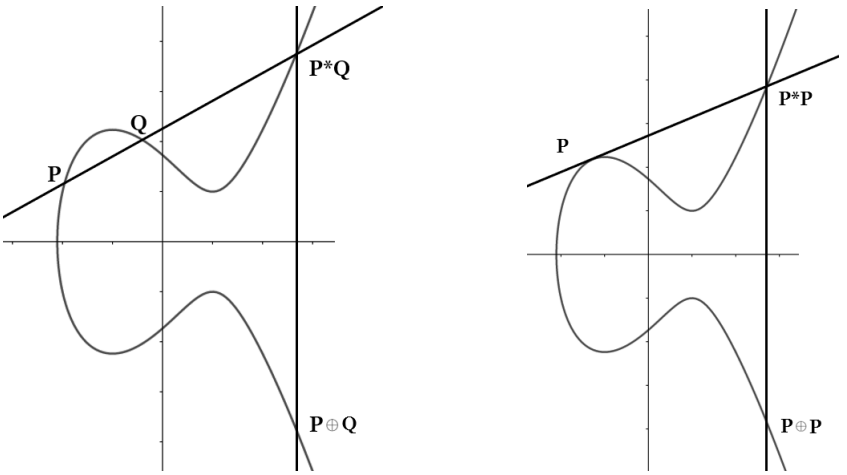
$$E(K) \cong \{[x, y, z] \in \mathbb{P}^2(K) : y^2 z = x^3 + Axz^2 + Bz^3\} := C,$$

con $A,\ B \in K$. Tomaremos así una curva de dicha forma para dar las coordenada del punto P_3. Recordemos que en este tipo de curva solo poseía un único punto en el infinito, el $[0, 1, 0]$. Por lo que podemos ver C, como

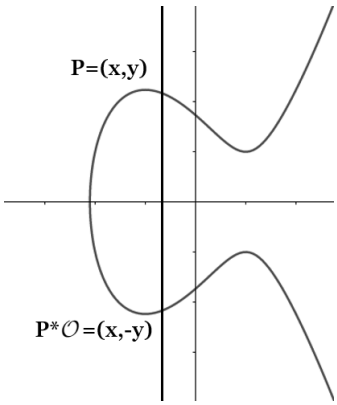
$$C' = \{(x, y) \in \mathbb{A}^2(K) : y^2 = x^3 + Ax + B\} \cup [0, 1, 0],$$

es decir, su afín junto con el único punto en el infinito de C. Este punto, el $[0,1,0]$, es el que tomaremos como $\mathcal{O}$. La toma del punto $[0,1,0]$ facilita mucho los cálculos, aunque no dejan de ser largos y tediosos. Es por ello que acontinuación solo se expondrán los resultados directamente, además de dar una explicación gráfica. Vemos esto último primero:

Sea $P_1,\ P_2$ y $P_3 = P_1 \oplus P_1$

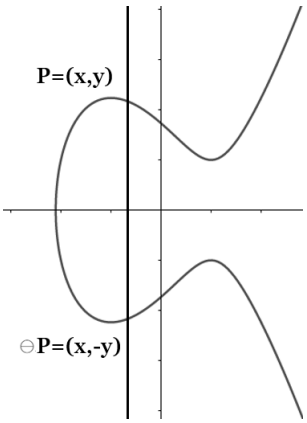


Observamos en esta representación que unir un punto $P \in E(K)$ con $\mathcal{O}$ es equivalente a trazar una recta vertical sobre $P = (x, y)$, y tomar el punto que la interseca, es decir, $P = (x, -y)$.



Por ser $\mathcal{O}$ un punto de inflexión tenemos que $\mathcal{O} * \mathcal{O} = \mathcal{O}$, por lo que si $P = (x_0, y_0) \in E(K)$ entonces

$$\ominus P = (x_0, -y_0)$$



Las fórmulas explícitas de la ley de grupo para nuestra curva

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

son: Sea $P_1 = (x_1, y_1)$ $P_2 = (x_2, y_2)$ y $P_3 = (x_3, y_3) = P_1 \oplus P_2$.

$$\begin{cases} x_3 = & \lambda - x_1 - x_2 \\ y_3 = & \lambda x_3 + \nu \end{cases} \text{ con } \begin{cases} \lambda = & \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & si \quad P_1 \neq P_2,\ P_1 \neq -P_2, \\ \dfrac{f'(x_1)}{2y_1} & si \quad P_1 = P_2. \end{cases} \\ \nu = & y_1 - \lambda x_1 = y_2 - \lambda x_2. \end{cases}$$

Cabe poner de forma explícita λ en el caso en el que $P_1 = P_2$ pues lo utilizaremos más adelante. Definimos $[m]P = \overbrace{P + \cdots + P}^{m}$.

$$\begin{cases} x([2]P_0) & = \dfrac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4x_0^3 + 4Ax_0 + 4B}, \\ y([2]P_0) & = \left(\dfrac{3x_0^2 + A}{2y_0}\right) x([2]P_0) + y_0 - \left(\dfrac{3x_0^2 + A}{2y_0}\right) x_0. \end{cases}$$

CAPÍTULO 3
Teorema de Mordell.

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

Una vez demostrado el teorema de Mordell tendremos que

$$E(\mathbb{Q}) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_m\mathbb{Z} \oplus \mathbb{Z}^r,$$

es decir,

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

donde $E(\mathbb{Q})_{tors}$ es el grupo de torsión (conjunto de puntos de orden finito en $E(\mathbb{Q})$) y r el rango de $E(\mathbb{Q})$. Para demostrar esto necesitaremos varios resultados previos. No obstante hay uno que es fundamental y le da sentido al resto: El teorema del descenso.

3.1. Teorema del descenso.

Teorema del Descenso. *Sea A un grupo abeliano y sea $h : A \longrightarrow \mathbb{R}$ una función 'altura' que satisface las siguientes propiedades:*

1. *Dado $Q \in A$, existe una constante $C_1 = C_1(Q)$ que depende de Q y A, tal que $\forall\ P \in A$,*
$$h(P \oplus Q) \leq 2h(Q) + C_1.$$

2. *Existe un entero $m \geq 2$, al que llamaremos m asociado a h, y una constante C_2 que depende sólo de A, tal que $\forall\ P \in A$*
$$h([m]P) \geq m^2 h(P) - C_2.$$

3. *Para cualquier constante C_3 el siguiente conjunto*
$$\{P \in A : h(P) \leq C_3\}$$
es finito.

Si suponemos además que para el entero m en (ii), el grupo cociente A/mA es finito, entonces A está finitamente generado.

Una vez leído el enunciado se entiende la pasada afirmación. De ser cierto -como veremos a continuación- 'solo' haría falta demostrar que, existe una altura, h, sobre $E(\mathbb{Q})$ y que su m asociado a dicha h cumple que $E(\mathbb{Q})/mE(\mathbb{Q})$ es finito, para demostrar el teorema de Mordell.

Demostración. Ver Apéndice C.1. ♮

En las próximas dos secciones demostraremos:

1. Para E, una curva elíptica definida sobre $\mathbb{Q}$, $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.
2. Existe una altura h sobre $E(\mathbb{Q})$, con su m asociada igual a 2.

De este modo habremos demostrado el **Teorema de Mordell**.

3.2. Teorema de Débil de Mordell.

Teorema débil de Mordell: *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces el grupo abeliano $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.*

Proposición 3.1. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por una ecuación de Weierstrass de la forma

$$y^2 = f(x) = x^3 + Ax + B.$$

Sea K el cuerpo de descomposición de $f(x)$, que se factoriza como:

$$f(x) = (x - \alpha)(x - \beta)(x - \gamma)$$

y el homomorfismo canónico

$$E(\mathbb{Q})/2E(\mathbb{Q}) \xrightarrow{\phi} E(K)/2E(K).$$

Entonces,

$$|ker\phi| \leq 2^{2[k:\mathbb{Q}]}.$$

Demostración. Ver Apéndice C.2. ♮

Vemos así que

$$|E(K)/2E(K)| < \infty \;\Rightarrow\; |E(\mathbb{Q})/2E(\mathbb{Q})| < \infty,$$

es decir, basta demostrar que $E(K)/2E(K)$ es finito, para ver que $|E(\mathbb{Q})/2E(\mathbb{Q})|$ lo es. Veamos algunas definiciones antes de seguir:

1. K^* el grupo multiplicativo de K.

2. $K^{*2} = \{k \in K^* : \exists k' \in K^* \text{ tal que } k = (k')^2\}$.
3. E un curva elíptica dada por $y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x)$, con K el cuerpo de descomposición de $f(x)$.

Proposición 3.2. Sea E una curva elíptica definida sobre $\mathbb{Q}$. Si definimos

$$\varphi_\alpha : E(K) \longrightarrow K^*/K^{*2}$$

mediante

$$\varphi_\alpha = \begin{cases} (x-\alpha)K^* & si\ P = (x,y) \text{ con } P \neq \mathcal{O} \text{ y } x \neq \alpha, \\ (\alpha-\beta)(\alpha-\gamma)K^{*2} & si\ P = (\alpha, 0), \\ 1 \cdot K^{*2} & si\ P = \mathcal{O}. \end{cases}$$

Entonces φ_α es un homomorfismo de grupos

Demostración. Ver Apéndice C.3. ♮

Corolario 3.3. φ_α induce un homomorfismo de grupos

$$E(K)/2E(K) \longrightarrow K^*/K^{*2}$$

que llamaremos también φ_α.

Demostración. Solo habría que demostrar que está bien definida, el que sea homomorfismo si está bien definido es una condición que se hereda de φ_α de la proposición anterior. Sea P_1 y P_2 representantes de una misma clase, entonces $P_1 - P_2 = 2P$ para algún P. Por tanto,

$$\varphi(P)^2 = \varphi(2P) = \varphi(P_1 - P_2) = \varphi(P_1) \cdot \varphi(P_2)^{-1},$$

es decir, $\varphi(\bar{P}_1) = \varphi(\bar{P}_2)$. ♮

Lema 3.4. Sea E una curva elíptica sobre K, con char(K) $\neq 2, 3$ definida por

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \text{ con } \alpha, \beta, \gamma \in K.$$

Entonces si $P_2 = (x_2, y_2) \in E(K)$, existe $P_1 = (x_1, y_1) \in E(K)$ tal que $[2]P_1 = P_2$ si y solo si:

$$\begin{cases} x_2 - \alpha = \alpha_1^2 \\ x_2 - \beta = \beta_1^2 \\ x_2 - \gamma = \gamma_1^2 \end{cases} \text{con } \alpha_1, \beta_1, \gamma_1 \in K.$$

Demostración. Para la demostración consutar [4] (Lema 3.2.3). ♮

Proposición 3.5. El homomorfimos

$$\varphi_\alpha \times \varphi_\beta : E(K)/2E(K) \longrightarrow K^*/K^{*2} \times K^*/K^{*2}$$

es inyectivo.

Demostración. Sea $P = (x, y) \in E(K)$. Si $P \in \ker\varphi_\alpha \times \varphi_\beta$ entonces

$$\varphi_\alpha(P),\ \varphi_\beta(P) \in K^{*2}.$$

Veamos que el kernel es el elemento $\mathcal{O}$. Separamos por casos:

$\boxed{P \neq (\alpha, 0), (\beta, 0)}$ Tenemos que $x - \alpha, x - \beta \in K^{*2}$. Como $P \in E(K)$,

$$(x - \alpha)(x - \beta)(x - \gamma) = y^2 \in K^{*2},$$

por tanto, $x - \gamma \in K^{*2}$, y por el lema 3.4 tenemos que $P \in 2E(K)$.

$\boxed{P = (\alpha, 0)}$ Por hipótesis tenemos que

$$\begin{aligned} &\varphi_\alpha(P) \in K^{*2},\ \text{por lo tanto}\ \ (\alpha - \beta)(\alpha - \gamma) \in K^{*2}. \\ &\varphi_\beta(P) \in K^{*2},\ \text{por lo tanto}\ \ (\beta - \alpha) \in K^{*2}. \end{aligned}$$

De donde deducimos que $(\alpha - \beta), (\alpha - \gamma) \in K^{*2}$. Por otra parte, tenemos que $\alpha - \alpha = 0 \in K^{*2}$. Aplicando nuevamente el lema 3.4 tenemos que $P = (\alpha, 0) \in 2E(K)$.

$\boxed{P = (\beta, 0)}$ Este es el último caso que nos queda. Se resuelve de forma análoga al caso $P = (\alpha, 0)$. ♮

Para demostrar, por fin, que $E(K)/2E(K)$ es finito, necesitamos enunciar un teorema y una proposición más.

Teorema 3.6. *Sea K un cuerpo de números y sea O_K su anillo de enteros. Entonces existe un anillo R con $O_K \subset R \subset K$ tal que:*

1. *R es un dominio de ideales principales y por tanto, un dominio de factorización única.*
2. *El grupo de unidades de R está finitamente generado.*

Demostración. Ver Apéndice C.4. ♮

Una vez tenemos a R, por ser un dominio de factorización única, podemos escribir

$$K^*/K^{*2} = \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\text{p primo en } R} \mathbb{Z}/2\mathbb{Z}$$

con $\mathcal{U}(R)$ las unidades de R y $\mathcal{U}^2(R)$, el conjunto de cuadrados de unidades de R. Definamos lo siguiente. Si p es un primo de R y l es un elemento de K, escribiremos $p^a || l$ si $r = p^a q$ con $q \in K$ tal que q no tenga factor de p ni en el denominador y ni en el numerador. Con esta definición en mente veamos que la imagen de

$$\varphi_\alpha \times \varphi_\beta :\ K^*/K^{*2} \times K^*/K^{*2} \longrightarrow (\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\text{p primo en } R} (\mathbb{Z}/2\mathbb{Z})^2$$

es cero en la mayoría de las coordenadas.

Por último, una pequeña observación: Sea E una curva sobre un cuerpo de fracciones K de un DFU R, definida por

$$y^2 = x^3 + Ax + B, \quad A,\ B \in K.$$

Tenemos, entonces, que podemos suponer que $A,\ B \in R$, pues si r es mínimo común denominador de A y B, podemos hacer el cambio

$$\begin{cases} r^2 x = X, \\ r^3 y = Y, \end{cases}$$

y transformar a E en una curva definida por

$$y^2 = x^3 + A'x + B', \qquad \text{con } A',\ B' \in R.$$

De esta forma, si $K = \mathbb{Q}$, una forma corta de Weierstrass para E sería:

$$y^2 = x^3 + Ax + B, \qquad A,\ B \in \mathbb{Z}.$$

Proposición 3.7. Sea E una curva elíptica definida sobre $\mathbb{Q}$:

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x) \quad \text{con } \alpha, \beta, \gamma \in \mathcal{O}_K$$

con K el cuerpo de descomposición de $f(x)$. Sea $\varphi_\alpha \times \varphi_\beta$ el homomorfismo que definimos antes y $d = (\alpha-\beta)(\alpha-\gamma)(\gamma-\beta)$ el discriminante de $f(x)$. Entonces el homomorfismo inducido por $\varphi_\alpha \times \varphi_\beta$

$$E(K)/2E(K) \longrightarrow \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{\text{p primo en } R \\ \text{tal que } p|d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$$

es inyectivo.

Demostración. Sea $P = (x, y) \in E(K)/\{\mathcal{O}\}$. Veamos que las coordenadas p-ésimas de P al aplicar $\varphi_\alpha \times \varphi_\beta$ son siempre nulas cuando p, primo de R, no divide a d, el discriminante de f.
Fijemos p un primo de R y definamos los enteros a, b, c como

$$p^a || (x-\alpha), \quad p^b || (x-\beta), \quad p^c || (x-\gamma).$$

Ya que $(x-\alpha)(x-\beta)(x-\gamma) = y^2$ tenemos que:

$$a + b + c \equiv 0 (\text{mod } 2). \tag{3.1}$$

Separemos por casos:

$\boxed{x \neq \alpha, \beta, \gamma}$

• Si tenemos que al menos uno de los a, b, c es menor que 0. Supongamos que $a < 0$. Como $\alpha \in \mathcal{O}_K$, que está contenido en R, que es un dominio de factorización, tenemos que:

$$p^a || (x-\alpha) \Rightarrow p^{|a|} || (\text{denominador de } x) \ \ \forall p.$$

De aquí deducimos que $p^a||(x-\alpha),(x-\beta),(x-\gamma)$. De modo que $a=b=c$ y por tanto utilizando (3.1)

$$a \equiv b \equiv c \equiv 0 (\text{mod } 2).$$

Luego la imagen de P en la p-ésima coordenada es cero.
• $a,b,c \geq 0$. Supongamos que al menos uno es mayor que 0, en caso contrario no habría nada que demostrar. Digamos que es $a>0$. Como $p \nmid d$, entonces $p \nmid (\alpha-\beta)$. Como

$$x-\beta = (x-\alpha)-(\alpha-\beta)$$

y $a>0$ y $b \geq 0 \Rightarrow b=0$. De manera análoga vemos que $c=0$ y utilizando (3.1) tenemos que:

$$a \equiv b \equiv c \equiv 0 (\text{mod } 2).$$

Por tanto la imagen de P en la p-ésima coordenada es cero

$\boxed{P=(\alpha,0),(\beta,0),(\gamma,0)}$.

Solo hay que observar que $\varphi_\alpha(P)$ y $\varphi_\beta(P)$ son productos de $(\alpha-\beta),(\beta-\gamma)$ y $(\gamma-\alpha)$. Como $p \nmid d$, entonces $p \nmid (\alpha-\beta), p \nmid (\beta-\gamma)$ y $p \nmid (\gamma-\alpha)$, por tanto $a=b=c=0$.
Es decir, independientemente de P, si $p \nmid d$ entonces la p-ésima coordenada es siempre 0. ♮

Como demostramos en el Teorema 3.6 las unidades R, $\mathcal{U}(R)$, son finitamente generadas, por lo que:

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\}$$

es finito, y por tanto:

$$\{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \{\mathcal{U}(R)/\mathcal{U}^2(R)\} \oplus \bigoplus_{\substack{\text{p primo en } R \\ \text{tal que } p|d}} (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$$

es finito. Y como existe una aplicación inyectiva de $E(K)/2E(K)$ a este conjunto, por la Proposición 3.7, tenemos que

$$\boxed{|E(K)/2E(K)| < \infty}.$$

3.3. Con altura.

Definición 3.8. Sea $x=\frac{m}{n} \in \mathbb{Q}$ con $\text{mcd}(m,n)=1$. Definimos las altura de x como

$$H(x) = H\left(\frac{m}{n}\right) = \text{máx}\{|m|,|n|\} \in \mathbb{Z}_{\geq 0}.$$

Veamos la siguiente proposición:

Proposición 3.9. El conjunto de los número racionales tal que su altura es menor que una cierta constante es finito.

Demostración. Sea C una constante, entonces para que $H(\frac{m}{n}) < C$ debemos tener que $|m| < C$ y $|n| < C$. ♮

Podríamos tomar como definición de altura para los $(x, y) = P \in E(\mathbb{Q})$ la siguiente función:

$$H(P) = H(x).$$

Pero queremos, como veremos más adelante, que esta función se comporte aditivamente. Teniendo en cuenta esto último y la función H, definimos lo que para nosotros será la función altura sobre $E(\mathbb{Q})$.

Definición 3.10. Sea E una curva elíptica definida sobre $\mathbb{Q}$ y sea $P = (x_1, y_1) \in E(\mathbb{Q})$ definimos como la altura en $E(\mathbb{Q})$

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

como:

$$h_x(P) = \begin{cases} \log(H(P)) & \text{si } P \neq \mathcal{O}, \\ 0 & \text{si } P = \mathcal{O}. \end{cases}$$

Teorema 3.11. *La función h_x es una altura sobre $E(\mathbb{Q})$, con E una curva elíptica definida sobre $\mathbb{Q}$.*

Veamos que esta función h_x cumple las propiedades de función de altura, con un m asociado $m = 2$, sobre el grupo abeliano $E(\mathbb{Q})$.

Demostración. Ver Apéndice C.5. ♮

CAPÍTULO 4
p-ádicos y sus aportaciones.

En este capítulo veremos dos resultado muy importantes:

1. Bajo algunas condiciones, existe un homomorfismo inyectivo entre el grupo de torsión de curva elíptica E y el grupo $E_p(\mathbb{F}_p)$ (la definición de este último grupo la veremos en este capítulo), ie, existe un σ homomorfismo inyectivo tal que
$$\sigma : E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p).$$
2. Dada la curva $E : y^2 = x^3 + Ax$, para $A \in \mathbb{Z}$ con $-A$ un cuadrado y sin potencias cuartas, tenemos que
$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

En Apéndice D encontramos una introducción a los número p-ádicos.

4.1. Reducción módulo p de una curva.

Definimos $\mathbb{Z}_{(p)}$ de la siguiente forma:
$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \in \mathbb{Q} \mid p \nmid n \right\} = \{p^n \frac{u}{v} | n \in \mathbb{N}, p \nmid uv\}.$$

Sea $[x, y, z] = P \in \mathbb{P}^2(\mathbb{Q})$ con $x, y, z \in \mathbb{Z}_{(p)}$ decimos que la coordenada $[x, y, z]$ es un *representante de p reducción* si de entre $x, y, z \in \mathbb{Z}_{(p)}$ hay al menos uno con $|\cdot|_p = 1$. Observamos que $\forall [x, y, z] \in \mathbb{P}^2(\mathbb{Q})$ podemos multiplicar por una potencia p^n de forma que $x, y, z \in \mathbb{Z}_{(p)}$ y que hay un único representante de p reducción por punto P (salvo por multiplicación de elementos con $|\cdot|_p = 1$). Esto último hace que la siguiente función esté bien definida:
$$\begin{array}{rcl} r_p : \mathbb{P}^2(\mathbb{Q}) & \longrightarrow & \mathbb{P}^2(\mathbb{F}_p) \\ [x, y, z] & \longrightarrow & r_p([x, y, z]) = [r_p(x), r_p(y), r_p(z)], \end{array}$$

donde $x, y, z \in \mathbb{Z}_{(p)}$ y al menos uno de ellos tiene $|\cdot|_p = 1$ y con
$$\begin{array}{rcl} r_p : \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{F}_p \\ q & \longrightarrow & r_p(q) = \overline{p^n \frac{u}{v}} = \bar{p^n} \cdot \bar{u} \cdot \bar{v}^{-1}, \end{array}$$

para $q = p^n \frac{u}{v}$ con $p \nmid uv$.

Fijémonos en que podemos llevar a cabo un proceso semejante con una curva E, definida por $F \in \mathbb{Q}[x, y, z]$. Nótese que para c una constante no nula, $c \cdot F$ defiene la misma curva E. De esta forma, podemos multiplicar por un $c \in \mathbb{Q}$ tal que todos los coeficientes de E se encuentren en $\mathbb{Z}_{(p)}$, con al menos uno con norma $|\cdot|_p = 1$. Esta representación de E es única salvo por multiplicación de un elemento con $|\cdot|_p = 1$. Diremos que la curva E está normalizada en p si cumple sus coeficientes están en $\mathbb{Z}_{(p)}$, con al menos uno de norma 1.

Definición 4.1. *Sea C una curva normalizada en p y*

$$F(x, y, z) = a_m x^n + a_{m-1} y^n + a_{m-2} z^n + a_{m-3} x^{n-1} y + \ldots + a_3 x + a_2 y + a_1 z + a_0,$$

con $a_i \in \mathbb{Z}_{(p)}$ y $|a_i|_p = 1$ para algún $i \in \{1, \ldots, m\}$, el polinomio que define a E. Entonces definimos C_p como:

$$C_p := \{[x, y, z] \in \mathbb{P}^2(\mathbb{Z}/p\mathbb{Z}) : \bar{F} = \bar{a}_m x^n + \ldots + \bar{a}_{m-3} x^{n-1} y + \ldots + \bar{a}_1 z + \bar{a}_0 = 0\}.$$

Nótese que el polinomio $\bar{F} \in \mathbb{Z}/p\mathbb{Z}[x, y, z]$ no es nulo por estar C normalizada módulo p.

Proposición 4.2. Sea C una curva proyectiva plana normalizada en p y definida por $F \in \mathbb{Q}[x, y, z]$. La imagen por r_p de $C(\mathbb{Q})$ está contenida en $C_p(\mathbb{F}_p)$. Es decir,

$$r_p(C(\mathbb{Q})) \subset C_p(\mathbb{F}_p).$$

Demostración. Tomamos $[x, y, z] \in C(\mathbb{Q})$ y su representante de p reducción, llamémosle $[x_0, y_0, z_0]$. Tenemos entonces, aplicando el homomorfismo r_p, que

$$0 = r_p(0) = r_p(F(x_0, y_0, z_0)) = \bar{F}(r_p(x_0), r_p(y_0), r_p(z_0)) = F_p(r_p([x_0, y_0, z_0])).$$

Es decir, $r_p([x_0, y_0, z_0]) \in C_p(\mathbb{F}_p) \Rightarrow r_p(C(\mathbb{Q})) \subset C_p(\mathbb{F}_p)$. ♮

Proposición 4.3. Sea C una curva proyectiva homogénea plana de grano n definida por un polinomio $F \in \mathbb{Q}[x, y, z]$, y L una recta definida sobre $\mathbb{Q}$ y $P = [x_0, y_0, z_0]$ un punto de L. Si $[x', y', z']$ es cualquier punto de L tal que $[x', y', z'] \neq [x_0, y_0, z_0]$, entonces $I_{P_0}(C, L)$ es igual al orden en $t = 0$ de $\gamma(t) = F(x_0 + tx', y_0 + ty', z_0 + tz')$. Es decir,

$$I_{P_0}(C, L) = ord_{t=0}(\gamma(t)).$$

Demostración. Para la demostración consultar [6] (**Proposición 2.9**). ♮

Proposición 4.4. Sea C una curva proyectiva plana de grado m definida por un polinomio $G \in \mathbb{Q}[x, y, z]$, L un recta definida sobre $\mathbb{Q}$ y $P_0 = [x_0, y_0, z_0]$ un punto de L. Si tomamos C_p y L_p, entonces

$$I_{P_0}(C, L) \leq L_{r_p(P_0)}(C_p, L_p).$$

Demostración. Durante la demostración tomaremos por C y L sus formas normalizadas y por P_0 tomaremos su representante de p reducción. Tomamos la representación de p reducción de un punto $P' = [x', y', z'] \in L$ que cumpla que $P_0 \neq P'$ y la función

$$\gamma(t) = F(P_0 + tP) = F(x_0 + tx', y_0 + ty', z_0 + tz') = t^r F_r + \ldots + t^m F_m$$

con F_i los monomios de grado i, con variables $x_0,\ x',\ y_0,\ y',\ z_0$ y z' y $F_r \neq 0$. Pero por la proposición anterior tenemos que

$$I_P(C, L) = ord_{t=0}(\gamma(t)) = r.$$

Tomando $\gamma(t)$ módulo p y aplicando nuevamente la proposición tenemos que

$$I_P(C_p, L_p) \geq r.$$

♮

Para la curva elíptica E en la forma corta de Weierstrass siguiente

$$zy^2 = x^3 + Ax + B \quad \text{con } A,\ B \in \mathbb{Z},$$

la curva E_p estaría definida de la siguiente manera

$$zy^2 = x^3 + \bar{A}x + \bar{B} \quad \text{con } \bar{A},\ \bar{B} \in \mathbb{Z}/p\mathbb{Z}.$$

Tenemos, por tanto, que

$$\Delta_p \equiv \Delta (\text{mod } p), \text{ y así, } E_p \text{ es lisa} \Leftrightarrow p \nmid \Delta.$$

Proposición 4.5. Si E_p es lisa, entonces $r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$ es un homomorfismo de grupos.

Demostración. Claramente $r_p([0, 1, 0]) = [0, 1, 0]$, por lo que el neutro va al neutro. Falta ver que se respeta la estructura de grupo. Tenemos que

$$r_p(P * Q) = r_p(P) * r_p(Q),$$

por lo que

$$\begin{aligned} r_p(P \oplus Q) &= r_p(\mathcal{O} * (P * Q)) = r_p(\mathcal{O}) * r_p(P * Q) \\ &= \mathcal{O}_P * (r_p(P) * r_p(Q)) = r_p(P) \oplus r_p(Q). \end{aligned}$$

♮

4.2. Filtración p-ádica.

Sea

$$E :\ Y^2 = X^2 + AX + B$$

con $A,\ B \in \mathbb{Z}$ y $4A^3 + 27B^2 \neq 0$.

Tomemos un primo tal que $p \nmid \Delta$. Por la proposición 4.5

$$r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p) \text{ es un homomorfismo de grupos.}$$

Teorema 4.6. *Sea E una curva elíptica definida por*

$$zy^2 = x^3 + Axz^2 + Bz^3 \qquad A, B \in \mathbb{Z}.$$

Sea $r_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$. Entonces si $p \nmid \Delta$, tenemos que

$$r_p|_{E(\mathbb{Q})_{tors}} : \ E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p)$$

es inyectiva.

Demostración. Ver Apéndice E.1. ♮

4.3. Subgrupo de torsión.

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

$$y^2 = x^3 + Ax + B, \qquad A, \ B \in \mathbb{Z}.$$

Sae $P = (x(P), y(P)) \in E(\mathbb{Q})_{tors}$. Entonces:

1. *$x(P), y(P) \in \mathbb{Z}$.*
2. *$y(P) = 0$ (entonces $[2]P = \mathcal{O}$) o bien $\quad y(P)^2 | 4A^3 + 27B^2$.*

Demostración. Ver Apéndice E.2. ♮

4.3.1. Grupo de torsión de una curva interesante.

En esta sección vamos a estudiar el grupo de torsión de la curva:

$$y^2 = x^3 + Ax, \qquad A \in \mathbb{Z}.$$

Veremos en el próximo capítulo qué la hace tan interesante para nosotros.

Teorema 4.7. *Sea E una curva elíptica dada por*

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

y supongamos que A no tiene potencias cuartas. Entonces

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \text{si } -A \text{ es un cuadrado en } \mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z} & \text{si } A = 4, \\ \mathbb{Z}/2\mathbb{Z} & \text{en otro caso.} \end{cases}$$

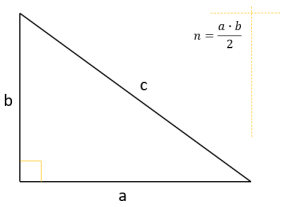
Demostración. Ver Apéndice E.3. ♮

CAPÍTULO 5

El problema del número congruente.

Recordemos el enunciado del problema del número congruente y la equivalencia dada en la introducción:

Enunciado: Dado un $n \in \mathbb{N}$ ¿Existe un triángulo rectángulo de lados racionales (a,b,c) tal que su área sea n?



Equivalencia:

n, libre de cuadrados, es congruente.	$\Leftrightarrow$	*La curva* $E_n: \ y^2 = x^3 - n^2x$ *tiene un* $P = (x, y)$ *con* $x, y \in \mathbb{Q}$ *e* $y \neq 0$

Veamos esta equivalencia:

Observación 5.1. Supongamos que existe un $n \in \mathbb{N}$ tal que hay un triángulo rectángulo (a, b, c) de lados racionales cuya área es n. Entonces, suponiendo que c es la hipotenusa, tenemos que:

$$n = \frac{ab}{2}.$$

Observamos que podemos suponer que n es libre de cuadrado pues, si no lo fuese, tenemos que existe un $s \in \mathbb{N}$ tal que $Ds^2 = n$ y D es libre se cuadrado. Dicho D es congruente pues el triángulo $(\frac{a}{s}, \frac{b}{s}, \frac{c}{s})$ es rectángulo y

$$D = \frac{n}{s^2} = \frac{ab/2}{s^2} = \frac{a/s \cdot b/s}{2}.$$

Y viceversa. Sea (a, b, c) un triángulo rectángulo de lados racionales que hace de D un número congruente, entonces tenemos que:

$$(as)^2 + (bs)^2 = (cs)^2 \quad \text{y} \quad n = Ds^2 = \frac{ab}{2}s^2 = \frac{(as)(bs)}{2}.$$

Es decir, el triángulo (as, bs, cs) hace de n un número congruente. Por tanto, n es congruente si y solo si lo es D.

Fijemos un número n libre de cuadrados y un triángulo rectángulo de lados racionales (a, b, c), que le haga congruente. Veamos que $y^2 = x^3 - n^2x$ tiene punto $P = (x, y)$ racional con $y \neq 0$. Tenemos que:

$$a^2 + b^2 = c^2 \quad \text{y} \quad n = \frac{ab}{2}.$$

Por tanto,

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

Si multiplicamos ambas igualdades vemos que

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

Llamamos $u = c^2/2$ y $v = (a^2 - b^2)/4$, y obtenemos que

$$v^2 = u^4 - s^2.$$

Multiplicando ambos lados por u^2 tenemos que

$$(uv)^2 = (u^2)^3 - n^2u^2.$$

Definimos $x = u^2$ e $y = uv$ y tenemos que

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

Por tanto, todo número congruente n, nos lleva de forma 'natural' a la curva E_n. Ahora, el triángulo (a, b, c) nos da la siguiente solución, P, para $y^2 = x^3 - n^2x$:

$$P = (x, y) = (c^4/4, (c^2(a^2 - b^2))/4).$$

Observemos, además, que $y(P) \neq 0$, pues en caso contrario: o bien $a = b = 2$ lo que es una contradicción, ya que 8 no es un cuadrado o bien $\exists p \neq 2$ tal que $p^2 | a \cdot b$, lo que es una contradicción con la suposición de que n es libre cuadrados. Tenemos así, una de las implicaciones.

Dada la curva

$$y^2 = x^3 - nx,$$

con un punto racional, $P = (x, y)$, con $y \neq 0$, definimos:

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

Veamos que $a^2 + b^2 = c^2$ y $n = \frac{ab}{2}$, es decir, que n es congruente.

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

Por último, comprobemos que $n = \frac{ab}{2}$:

$$\begin{aligned} \frac{ab}{2} &= \frac{\left(\frac{x^2-n^2}{y}\right) \cdot \left(\frac{2nx}{y}\right)}{2} = \frac{2nx(x^2 - n^2)}{2y^2} \\ &= \frac{nx(x-n)(x+n)}{y^2} \quad \text{como } P \in E_n \\ &= \frac{nx(x-n)(x+n)}{x(x-n)(x+n)} = n. \end{aligned}$$

Por tanto, siempre que exista un punto $(x, y) = P \in E(\mathbb{Q})$ tal que $y \neq 0$, tendremos que existe un triángulo rectángulo de lados racionales, a saber el triángulo (a, b, c), que haga a n congruente. Ya tenemos las implicación que nos faltaba.

Nótese que la curva

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

no es una curva elíptica cualquiera, es la que acabamos de estudiar en la sección 4.3.1, para el caso $A = -n^2$. Tenemos así que

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

con $E_n(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$. Por el teorema de Mordell

$$E_n(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}^r, \quad r \geq 0.$$

Pero $P \in E(\mathbb{Q})_{tors}$ si y solo si $y = 0$.

Reunamos estos últimos resultado, ya probados, en un solo teorema. Teorema que dará otra nueva equivalencia en el campo de curvas elípticas a nuestro problema.

Teorema 5.2. *Sean n', n y s tres números naturales tales que $s^2n = n'$ con n libre de cuadrados. Definimos la curva:*

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

Tenemos que son equivalentes:

1. *n' es un número congruente, es decir, existe un triángulo rectángulo de lados racionales A,B,C cuya área es n.*
2. *$E_n(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}^r \quad con \quad r > 0.$*
3. *Existe un $P \in E_n(\mathbb{Q})$ con $y(P) \neq 0$.*

5.1. Generalizaciones: un motor de las Matemáticas.

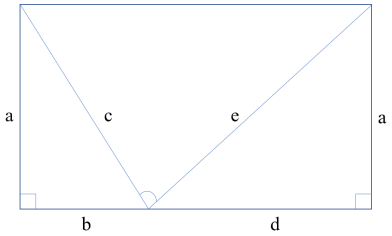
Se podría decir que la generalización es uno de los motores que mueve a las Matemáticas, y este problema no iba a ser la excepción. Veamos algunas extraídas de [9].

Definición 5.3. *Definimos ϵ como el conjunto de $n \in \mathbb{N}$ tal que existen $a,\ b,\ c,\ d,\ e \in \mathbb{Q}$, tal que:*

$$a^2 + b^2 = c^2, \qquad a^2 + d^2 = e^2, \qquad a(b+d) = n. \tag{5.1}$$

Llamaremos a la 5-upla (a,b,c,d,e) una envolvente de n.

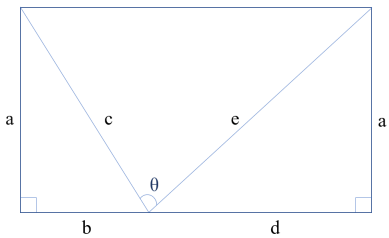
Geométricamente hablando el que n se encuentre en ϵ implica que, n es el área de un rectángulo que se forma al juntar los triángulos rectángulos (a,b,c) y (a,d,e) de la siguiente forma:



Nótese que para el caso $b = d$, tenemos el conjunto de los números congruentes.

Definición 5.4. *Sea $0 < \theta < \pi$ un ángulo. Definimos $\epsilon(\theta)$ con el subconjunto de ϵ compuesto por los $n \in \mathbb{N}$ que cumplen (5.1) y $\cos(\theta) = (a^2 - bd)/ce$. Si $n \in \epsilon(\theta)$, decimos que n es $\theta-$congruente.*
Llamaremos a la 5-upla (a,b,c,d,e) una θ-envolvente de n.

Geométricamente hablando el que n se encuentre en ϵ implica que, n es el área del rectángulo que se forma al juntar los triángulos rectángulos (a,b,c) y (a,d,e) de la misma forma que antes y, además, el ángulo que forman los picos de los dos triángulos es θ, es decir:



Veamos otra condición equivalente a que n sea congruente:

Proposición 5.5. Sea $n \in \mathbb{N}$.

$$2n \text{ es congruente si y solo si } n \in \epsilon(\pi/2).$$

Demostración. $\Leftarrow$) Tomamos una de las envolventes, (a, b, c, d, e), que hace que $n \in \epsilon(\pi/2)$. A partir de esta podemos crear una $\pi/2$-envolvente, $(2a, 2b, 2c, 2d, 2e)$, para $4n$. Tenemos así que $2n$ es un número congruente pues el triángulo rectángulo $(c, e, b+d)$ tiene área $2n$ (ver Fig. 1).
$\Rightarrow$) Tomamos el triángulo rectángulo (a, b, c) que hace de $2n$ un número congruente. Tomando la 5-upla $(ab/c, a^2/c, a, b^2/c, b)$ tenemos que $4n \in \epsilon(\pi/2)$. Tenemos, por tanto, que $n \in \epsilon(\pi/2)$ (ver Fig. 2).

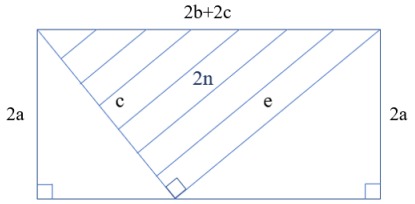


Fig. 1.

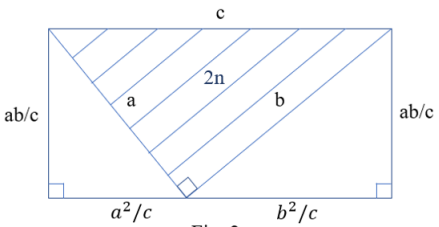


Fig. 2.

$\natural$

Al igual que el problema del número congruente estas generalizaciones tienen también sus equivalente en el campo de las curvas elípticas.

Teorema 5.6. *Sea $n \in \mathbb{N}$. Entonces $n \in \epsilon$ si y solo si las siguientes ecuaciones*

$$\begin{cases} E_k : \ y^2 = x^3 - k^2 x, \\ E_{2n-k} : \ z^2 - (2n-k)^2 z, \\ V_R : \ xw = yz, \end{cases}$$

tienen una solución racional (x, y, z, w, k) simultánea que satisface $yw \neq 0$ y $0 < k \leq n$.

En otras palabras, existe un número racional $0 < k \leq n$ tal que E_k y E_{2n-k} tienen soluciones (x, y) y (z, w) con orden infinito, es decir, que k y $2n-k$ sean congruentes, con $x/y = z/w$.

Demostración. $\Rightarrow$) Sea (a, b, c, d, e) una envolvente de n, definimos:

$$x = 2a(a+c), \quad y = 4a^2(a+c), \quad z = 2a(a+e), \quad w = 4a^2(a+e), \quad k = 2ab.$$

$\Leftarrow$) Sea $(x, y) \in E_k$ y $(z, w) \in E_{2n-k}$ con $xw = yz$ y $yw \neq 0$, definimos:

$$a = \left|\frac{y}{2x}\right| = \left|\frac{w}{2z}\right|, \quad b = \left|\frac{kx}{y}\right|, \quad c = \left|\frac{x^2+k^2}{2y}\right|,$$
$$d = \left|\frac{(2n-k)z}{w}\right|, \quad e = \left|\frac{z^2+(2n-k)^2}{2w}\right|.$$

♮

Preguntas que aún siguen abiertas:

- ¿$\epsilon = \mathbb{N}$?

Sabemos que para todo n congruente existen infinitos triángulos rectángulos que hacen de él congruente. Tenemos así, lo mismo ocurre con $4n$. Pero:

- Para $n \in \epsilon$ ¿Existen infinitas envolventes de n?

5.2. El Teorema de Tunnell y la pregunta del millón de dólares.

Veamos cuál es el Teorema de Tunnel. Ver [4] para una mayor profundización del tema.

Teorema de Tunnell. *Sea $n \in \mathbb{N}$ un número congruente, libre de cuadrados y los siguientes números:*

$$\begin{aligned} A_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 32z^2\}, \\ B_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 2x^2 + y^2 + 8z^2\}, \\ C_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 64z^2\}, \\ D_n &= \#\{(x,y,z) \in \mathbb{Z}^3 : n = 8x^2 + 2y^2 + 16z^2\}. \end{aligned}$$

Entonces

- $A_n = B_n/2$, *si n es impar.*
- $C_n = D_n/2$, *si n es par.*

Obsérvese que esta es una condición necesaria, es decir, solo nos permite descartar que n sea congruente, pero no, en cambio, saber si lo es. Esto se daría si la implicación del enunciado fuese un si y solo si. ¿Lo es? Pues es aquí donde entra la pregunta del millón de dólares, 'La conjetura BSD', uno de los problemas del milenio. Tunnell desmostró que la implicación era un si y solo si, si tomábamos por cierta 'La conjetura BSD'.

De esta forma, de ser la conjetura cierta, tendríamos que un algoritmo finito que nos permitiría saber si n es o no congruente.

5.2.1. ¿Qué es 'La conjetura BSD'?

Por desgracia, aquí se acaban los enunciado sencillos y cortos. Comencemos por una definición importante en este campo.

Como ya vismo en el capítulo 4, si E está definida por

$$zy^2 = x^3 + Ax + B \quad \text{con } A,\ B \in \mathbb{Z},$$

para la curva

$$E_p: \ zy^2 = x^3 + \bar{A}x + \bar{B} \quad \text{con } \bar{A},\ \bar{B} \in \mathbb{Z}/p\mathbb{Z}.$$

Tenemos que

$$\Delta_p \equiv \Delta (\text{mod } p),$$

es decir,

$$E_p \text{ es lisa si y solo si } p \nmid \Delta.$$

Por tanto, E_p es una curva elíptica para $p \nmid \Delta$.

Definición 5.7. Sea E una curva elíptica definida sobre $\mathbb{Q}$. Sea un primo p, entonces:

- Si $p \nmid \Delta$ definimos:

$$a_p := p + 1 - |E_p(\mathbb{F}_p)|.$$

Definimos la **función L de Hasse-Weil de E**, para $Re(s) > \frac{3}{2}$, como:

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

Faltaría definirla para un número finito de p, aquellos que dividen a Δ. Esta función se puede extender analíticamente a una función meromorfa con un solo polo $s = 1$.

Conjetura de Birch-Swinnerton-Dyer. *Sea E una curva definida sobre $\mathbb{Q}$. Entonces, para el rango, r, de $E(\mathbb{Q})$ se tiene que*

$$ord_{s=1} L_E(s) = r.$$

APÉNDICE A
Demostraciones Capítulo 1.

A.1. Demostración: Teorema de Bezout.

Demostración. Para la demostración de este teorema seguiremos el siguiente esquema:

1 Ver que el número de puntos de la intersección de C_1 y C_2, con la forma $[x, y, 1]$, es como mucho $n_1 n_2$. Para ello demostraremos que:

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \overset{(A)}{\leq} \dim(R/(f_1, f_2)) \overset{(B)}{\leq} n_1 n_2,$$

con $R = k[x, y]$.

2 Demostrar que (B) es un igualdad cuando C_1 y C_2 no se encuentran en el infinito, es decir, si la intersección no contiene ningún punto con $z = 0$.

3 'Mejoramos' la ecuación (A) para conseguir

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P) \overset{(A+)}{\leq} \dim(R/(f_1, f_2)).$$

El hecho de que se diga que (A+) 'mejora' (A) se debe a que $\forall P \in C_1 \cap C_2$ $I_P(C_1, C_2) \geq 1$, por lo que, en cierto modo, se 'afina' más el cálculo.

4 Demostramos que (A+) es de hecho una igualdad.
En este punto observamos que con 2 y 4 hemos probado Bezout para en el caso en el que C_1 y C_2 no se encuentran en el infinito.

5 Veremos que $C_1 \cap C_2$ es finito y que, por tanto, existe una recta L en $\mathbb{P}^2$ que no contiene ningún punto de la intersección. Cambiamos las coordenadas para que L sea la recta del infinito. De esta forma reducimos el caso general, en el que C_1 y C_2 pueden encontrarse en el infinito, al caso en el que no lo hacen. Completamos así la demostración del teorema de Bezout, pues dicho caso ya está demostrado.

1 Dados m puntos distintos, $P_1 = (a_1, a_2), ..., P_m = (a_m, b_m)$ del plano afín $\mathbb{A}^2$, tenemos que existen m funciones, $h_1, ..., h_m$, tales que:

$$h_i = h_i(P_n) = \begin{cases} 1 & si \quad n = i, \\ 0 & si \quad n \neq i. \end{cases}$$

Basta con observar que podemos definirlas de la siguiente manera:

$$h_i(x, y) = \prod_{n=1, n\neq i}^{m} \frac{(x \cdot b_n - y \cdot a_n)}{(a_i \cdot b_n - b_i \cdot a_n)}.$$

Ahora, supongamos que $\forall i \in \{1, ..., m\}$ $P_i \in C_1 \cap C_2$. Observamos que estas h_i funciones son linealmente independientes módulo el ideal (f_1, f_2) ya que:

$$\begin{aligned} &c_1h_1 + c_2h_2 + \cdots + c_mh_m = \ g_1f_1 + g_2f_2 = \bar{0} \Rightarrow \\ &c_1h_1(P_i) + \cdots + c_ih_i(P_i) + \cdots + c_mh_m(P_i) = \ g_1(P_i)f_1(P_i) + g_2(P_i)f_2(P_i) \Rightarrow \\ &c_1 \cdot 0 + \ldots c_i \cdot 1 + \ldots c_m \cdot 0 = \ g_1(P_i) \cdot 0 + g_2(P_i) \cdot 0 \Rightarrow \\ &c_i = \ 0. \end{aligned}$$

Y así ya tenemos demostradas la igualdad (A), es decir:

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \leq dim(R/(f_1, f_2)).$$

Para probar (B), definimos para $d \in \mathbb{N}^*$:

$$\begin{aligned} \phi(d) &= \frac{1}{2}(d+1)(d+2) = \frac{1}{2}d^2 + \frac{3}{2}d + 1. \\ R_d &= (\text{el espacio vectorial de polinomios } f(x, y) \text{ de grado } \leq \text{d}). \\ W_d &= R_{d-n_1}f_1 + R_{d-n_2}f_2. \end{aligned}$$

W_d es un espacio vectorial sobre k. Además si $d < \text{máx}\{n_1, n_2\}$, $W_d = 0$ y, en todos los caso, $W_d \subset (f_1, f_2)$. Demostrar que $\dim R_d = \phi(d)$ es pura combinatoria pues

$$\phi(d) - \phi(d-1) = d + 1 = \text{número de monomios } x^iy^i \text{ de grado } d$$

y

$$\sum_{n=1}^{d+1} 1 = \frac{(d+1)(d+2)}{2}.$$

Para $d \geq n_1 + n_2$, tenemos 2 resultados

$$R_{d-n_1}f_1 \cap R_{d-n_2}f_2 = R_{d-n_2-n_1}f_1f_2, \tag{A.1}$$

$$\dim R_d - \dim W_d = \phi(d) - \phi(d-n_1) - \phi(d-n_2) - \phi(d-n_1-n_2) = n_1n_2. \tag{A.2}$$

Para demostrar (A.1) ambos contenidos:

$\subset$) Sea $f \in R_{d-n_1} f_1 \cap R_{d-n_2} f_2$ tenemos entonces que

$$f(x,y) = \begin{cases} g_1 f_1 & \text{con} \quad g_1 \in R_{d-n_1} \\ g_2 f_2 & \text{con} \quad g_2 \in R_{d-n_2} \end{cases} \Rightarrow f_1 | g_2 f_2 \Rightarrow f_1 | g_2$$

pues f_1 y f_2 no tienen componentes en común. Tenemos así que:

$$g_1 = g_1' f_1 \quad \text{con} \quad g_1' \in R_{d-n_1-n_2} \Rightarrow f = g_1' f_1 f_2 \Rightarrow f \in R_{d-n_2-n_1} f_1 f_2.$$

$\supset$) $f \in R_{d-n_2-n_1} f_1 f_2$ entonces $f = g f_1 f_2$ con $g \in R_{d-n_1-n_2}$. Tenemos que $g f_1 \in R_{d-n_2}$ y $g f_2 \in R_{d-n_1}$, por tanto, $f \in R_{d-n_1} f_1 \cap R_{d-n_2} f_2$.

Para (A.2) solo tenemos que tener en cuenta el siguiente isomorfismo:

$$\begin{aligned} R_{d-j} &\longrightarrow R_{d-j} f \\ g &\longrightarrow fg. \end{aligned}$$

De aquí deducimos $\dim R_{d-j} f = \phi(d-j)$. Utilizando la fórmula de dimensiones de Grassman:

$$\dim(U+V) = \dim(U) + \dim(V) - \dim(U \cap V)$$

para subespacios U y V de un espacio vectorial finito, obtenemos que:

$$\begin{aligned} \dim(R_d) - \dim(W_d) &= \phi(d) - \dim(R_{d-n_1}) - \dim(R_{d-n_2} f_2) - \dim(R_{d-n_1} f_1 \cap R_{d-n_2} f_2) \\ &= \phi(d) - \phi(d-n_1) - \phi(d-n_2) - \phi(d-n_1-n_2) \\ &= n_1 n_2. \end{aligned}$$

Para demostrar (B) usaremos (A.2): sean $g_1, g_2, \ldots, g_{n_1 n_2 + 1} \in R_d$, con $d \geq n_1 + n_2$ y $d \geq \delta(g_i)\ \forall i \in \{1, \ldots, n_1 n_2 + 1\}$. Veamos que son linealmente dependientes módulo (f_1, f_2).

- Si son linealmente dependiente en R_d entonces existen $\lambda_i \in k,\ i \in \{1, \ldots, n_1 n_2 + 1\}$, tal que:
$$\lambda_1 g_1 + \ldots + \lambda_{n_1 n_2 + 1} g_{n_1 n_2 + 1} = 0 \in (f_1, f_2).$$
- Si son linealmente independientes en R_d entonces:
$$\begin{cases} \dim(R_d) - \dim(W_d) = n_1 n_2 \\ g_1, g_2, \ldots, g_{n_1 n_2 + 1} \text{ l. ind. en} R_d \end{cases}$$
entonces existe una combinación no trivial tal que
$$g = \sum c_i g_i \quad \text{con} \quad g \in W_d \text{ y } c_i \in k.$$
Pero $W_d \subset (f_1, f_2)$, por tanto, $g_1, g_2, \ldots, g_{n_1 n_2 + 1}$ son linealmente dependientes módulo (f_2, f_2). Y así tenemos la desigualdad (B), es decir:
$$\dim(R/(f_1, f_2)) \leq n_1 n_2.$$

2 Definimos f^* como los monomios de grado n de f, es decir:

$$\text{Si } f = \sum_{i,j} c_{i,j} x^i y^j \text{ polinomio de grado n, entonces } \quad f^* = \sum_{\substack{i,j=1 \\ i+j=n}}^{n} c_{ij} x^i y^j.$$

Puesto que k es un cuerpo algebráicamente cerrado, tenemos que podemos descomponer f^* en factores lineales:

$$f^* = \prod_{i=1}^{n} (a_i x + b_i y) \quad \text{con} \quad a_i, b_i \in k \quad \text{y} \quad n = \delta(f) = \delta(f^*),$$

con $\delta(f)$ el grado del polinomio f. Vemos así que los puntos en el infinito de la curva $f(x, y) = 0$ son los puntos con las coordenadas homogéneas:

$$[X, Y, Z] = [b_i, a_i, 0].$$

En consecuencia tenemos que si C_1 y C_2 no se encuentran en el infinito entonces f_1^* y f_2^* no tienen factores en común.
Ahora veamos que si f_1^* y f_2^* no tienen factores en común, lo que quiere decir que C_1 y C_2 no se encuentran en el infinito, entonces para $d \geq n_1 + n_2$:

$$(f_1, f_2) \cap R_d = W_d, \tag{A.3}$$

$$\dim(R/(f_1, f_2)) \geq n_1 n_2. \tag{A.4}$$

Para (A.3):

$\subset$) Supongamos que $f \in (f_1, f_2) \cap R_d$ se puede escribir de la forma

$$f = g_1 f_1 + g_2 f_2.$$

con g_1 con el menor grado posible. Si $\delta(g_i) \geq d - n_i$ para algún $i \in \{1, 2\}$, entonces los términos de mayor grado deben sumar 0. Con nuestra notación esto significa que:

$$g_1^* f_1^* + g_2^* f_2^* = 0.$$

Pero f_1^* y f_2^* son coprimos por lo que:

$$f_2^* | g_1^* \Rightarrow g_1^* = f_2^* \cdot g_1'.$$

Si tenemos esto en cuenta y el hecho de que:

$$\begin{aligned} f &= g_1 f_1 + g_2 f_2 \\ &= (g_1 - g_1' f_2) f_1 + (g_2 + g_1' f_1) f_2, \end{aligned}$$

obtenemos una nueva forma de poner f con respecto a f_1 y f_2 que contradice el hecho de que g_1 tenga el menor grado posible ya que:

$$\delta(g_1 - g_1' f_2) < \delta(g_1).$$

Por lo que tenemos que $f \in W_d$.

$\supset$) $W_d \subset (f_1, f_2)$ y $W_d \subset R_d \ \therefore \ W_d \subset (f_1, f_2) \cap R_d$.

Para (A.4) tenemos que por (A.2) hay $n_1 n_2$ elementos en R_d que son linealmente independientes módulo W_d. Por (A.3) si $d \geq n_1 + n_2$ tenemos que $(f_1, f_2) \cap R_d = W_d$, por lo que hay $n_1 n_2$ elementos linealmente independientes módulo (f_1, f_2) sobre R. Y así:

$$\dim(R/(f_1, f_2)) \geq n_1 n_2.$$

Unido a (B), obtenemos que si C_1 y C_2 no se encuentran en el infinito entonces

$$\dim(R/(f_1, f_2)) = n_1 n_2.$$

3 Definimos $\mathcal{M}_P$ como el kernel del homomorfismo de evaluación:

$$\begin{aligned} \mathcal{O}_P &\longrightarrow k \\ \phi &\longrightarrow \phi(P). \end{aligned}$$

Es decir, $\mathcal{M}_P = \{\phi \in \mathcal{O}_P : \phi(P) = 0\}$. Recordemos que $I_P(C_1, C_2)$ lo definíamos como

$$I_P(C_1, C_2) = \dim(\mathcal{O}_P/(f_1, f_2)_P).$$

Veamos que

$$\dim(\mathcal{O}_P/(f_1, f_2)_P) \leq \dim(R/(f_1, f_2)), \tag{A.5}$$

$$\mathcal{O}_P = R + (f_1, f_2)_P. \tag{A.6}$$

Para (A.5) notamos que todo conjunto finito de elementos de $\mathcal{O}_P$ puede ser escrito con el mismo denominador. Sean $g_1/h, g_2/h, \ldots, g_r/h$ elementos de $\mathcal{O}_P$ linealmente independientes módulo $(f_1, f_2)_P$, entonces $g_1, g_2, \ldots, g_r$ son elementos de R linealmente independientes módulo (f_1, f_2) pues si

$$\sum_{i=1}^{r} c_i g_i = h_1 f_1 + h_2 f_2 = \bar{0} \bmod (f_1, f_2) \ \Rightarrow \ \sum_{i=1}^{r} c_i \frac{g_i}{h} = \frac{h_1}{h} f_1 + \frac{h_2}{h} f_2 = \bar{0} \bmod (f_1, f_2)_P$$

por lo que si $g_1/h, g_2/h, \ldots, g_r/h$ son linealmente independientes módulo $(f_1, f_2)_P$ entonces $c_i = 0 \ \forall i \in \{1, \ldots, r\}$, es decir, $g_1/h, g_2/h, \ldots, g_r/h$ son linealmente independientes módulo (f_1, f_2). Para (A.6):

$\supset$) Tenemos que $R \subset \mathcal{O}_P$ y $(f_1, f_2)_P \subset \mathcal{O}_P \therefore R + (f_1, f_2)_P \subset \mathcal{O}_P$.

$\subset$) Por (A.5) podemos tomar una base finita, $g_1/h, g_2/h, \ldots, g_r/h$, de $\mathcal{O}_P$. $\forall T \in \mathcal{O}_P$, $\frac{T}{h} \in \mathcal{O}_P$, por lo que $\frac{T}{h}$ se puede escribir de la forma:

$$\frac{T}{h} = \sum_{i=1}^{r} c_i \frac{g_i}{h} + (\phi_1 f_1 + \phi_2 f_2)$$

con $\phi_1, \phi_2 \in \mathcal{O}_P$. Por lo que:

$$T = \sum_{i=1}^{r} c_i g_i + (h\phi_1 f_1 + h\phi_2 f_2) \in R + (f_1, f_2)_P.$$

A continuación veremos que:

$$I(C_1 \cap C_2, P) \geq 1 \Longleftrightarrow P \in C_1 \cap C_2.$$

El que $P \notin C_1 \cap C_2$ implica que $I(C_1 \cap C_2, P) = 0$ es equivalente a ver que $P \notin C_1 \cap C_2$ entonces $\mathcal{O}_P = (f_1, f_2)_P$. Supongamos que $P \notin C_1 \cap C_2$:

$\supset$) $f_1 \in R \subset \mathcal{O}_P$ y $f_2 \in R \subset \mathcal{O}_P$, por lo que, $(f_1, f_2)_P \subset \mathcal{O}_P$.

$\subset$) Sin pérdida de generalidad pongamos que $f_1(P) \neq 0$, entonces $f_1^{-1} \in \mathcal{O}_P$. Por tanto,

$$1 = f_1^{-1} \cdot f_1 \in (f_1, f_2)_P \Rightarrow (f_1, f_2)_P = \mathcal{O}_P.$$

Para la otra implicación veremos que para $P \in C_1 \cap C_2$

$$(f_1, f_2)_P \subset \mathcal{M}_P \quad \text{y} \quad I(C_1 \cap C_2, P) = 1 + dim(\mathcal{M}_P/(f_1, f_2)_P).$$

El contenido podemos verlo fácilmente. En el caso de la igualdad debemos mostrar que

$$\dim(\mathcal{O}_P/(f_1, f_2)_P) = 1 + \dim(\mathcal{M}_P/(f_1, f_2)_P). \tag{A.7}$$

El planteamiento para esta demostración será demostrar la existencia de un elemento en $\mathcal{O}_P$ que no es combinación lineal de elementos de $\mathcal{M}_P$ y dar una base $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_n$ de $\mathcal{O}_P/(f_1, f_2)_P$, tal que $g_1, g_2, \ldots, g_{n-1} \in \mathcal{M}_P$ y $g_n \in \mathcal{O}_P \backslash \mathcal{M}_P$.

■ Un elemento de $\mathcal{O}_P$ que no se puede poner como combinación lineal de elementos de $\mathcal{M}_P$ puede ser el 1. En otras palabras, si estamos en $\mathcal{O}_P/(f_1, f_2)_P$, $\bar{1}$ no se puede poner como combinación lineal de clases de elementos que se encuentran en $\mathcal{M}_P$.

■ Ahora supongamos que tenemos una base $\{\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n\}$ de $\mathcal{O}_P/\ (f_1, f_2)_P$.

Observación: La evaluación en P de dos elementos, $g_1,\ g_2$, de una clase es la misma, es decir, $g_1(P) = g_2(P)$.

$$\begin{cases} g_1(P) = \alpha_i(P) + \phi_{11}(P)f_1 + \phi_{12}f_2 = \alpha_i(P) \\ g_2(P) = \alpha_i(P) + \phi_{21}(P)f_1 + \phi_{22}f_2 = \alpha_i(P) \end{cases} \quad \therefore \forall g_1, g_2 \in \bar{\alpha}_i,\ g_1(P) = g_2(P)$$

Con $\phi_{11},\ \phi_{21} \in \mathcal{O}_P$.

Reorganizamos nuestra base de forma que

$$\alpha_i(P) \neq 0 \text{ para } i \in \{1, \ldots, m\} \text{ y } \alpha_i(P) = 0 \text{ para } i \in \{1, \ldots, n\} \backslash \{1, \ldots, m\}.$$

Cabe observar que $1 \leq m$ por lo comentado sobre $\bar{1}$. Si $m = 1$ ya lo tenemos, si $m > 1$: Sea $\bar{\alpha}_i, \bar{\alpha}_{i+1}$ con $i \in \{1, \ldots, m-1\}$,

$$\alpha_i - \frac{\alpha_i(P)}{\alpha_{i+1}(P)}\alpha_{i+1} \in \mathcal{M}_P \Rightarrow \bar{\alpha}_i - \frac{\alpha_i(P)}{\alpha_{i+1}(P)} \cdot \bar{\alpha}_{i+1} = \bar{\beta}_i \text{ con } \beta_i \in \mathcal{M}_P$$
$$\Rightarrow \bar{\alpha}_i = \frac{\alpha_i(P)}{\alpha_{i+1}(P)} \cdot \bar{\alpha}_{i+1} + \bar{\beta}_i.$$

Veamos que $\{\bar{\beta}_1, \bar{\beta}_2, \ldots, \bar{\beta}_{m-1}, \bar{\alpha}_m, \ldots, \bar{\alpha}_n\}$ en una base de $\mathcal{O}_P/(f_1, f_2)_P$. Nótese que la única clase cuyos elementos no están en $\mathcal{M}_P$ es $\bar{\alpha}_m$. Sea $v \in \mathcal{O}_P/(f_1, f_2)_P$:

$$\begin{aligned}
v &= c_1\bar{\alpha}_1 + c_2\bar{\alpha}_2 + \ldots + c_n\bar{\alpha}_n \\
&= c_1\left(\frac{\alpha_1(P)}{\alpha_2(P)}\ldots\bar{\alpha}_2 + \bar{\beta}_1\right) + c_2\bar{\alpha}_2 + \cdots + c_n\bar{\alpha}_n \\
&= c_1\bar{\beta}_1 + \left(\frac{\alpha_1(P)}{\alpha_2(P)} + c_2\right)\bar{\alpha}_2 + c_3\bar{\alpha}_3 + \ldots + c_n\bar{\alpha}_n \\
&= c_1\bar{\beta}_1 + \left(\frac{\alpha_1(P)}{\alpha_2(P)} + c_2\right)\bar{\beta}_2 + \left(\frac{\alpha_2(P)}{\alpha_3(P)}\left(\frac{\alpha_1(P)}{\alpha_2(P)} + c_2\right) + c_3\right)\bar{\alpha}_3 + \ldots + c_n\bar{\alpha}_n \\
&\qquad\qquad \vdots \\
&= \lambda_1\bar{\beta}_1 + \lambda_2\bar{\beta}_2 + \ldots + \lambda_{m-1}\bar{\alpha}_{m-1} + \lambda_m\bar{\alpha}_m + c_{m+1}\bar{\alpha}_{m+1} + \ldots + c_n\bar{\alpha}_n \\
&\quad \text{con } \lambda_1, \ldots, \lambda_m, c_{m+1}, \ldots, c_n \in k.
\end{aligned}$$

Tenemos así que $\{\bar{\beta}_1, \bar{\beta}_2, \ldots, \bar{\beta}_{m-1}, \bar{\alpha}_m, \ldots, \bar{\alpha}_n\}$ genera $\mathcal{O}_P/(f_1, f_2)_P$ y tiene n elementos, por lo que es una base. Ya tenemos, por tanto, que $P \in C_1 \cap C_2 \Rightarrow I_P(C_1, C_2) \geq 1$.

Veamos que si $P \in C_1 \cap C_2$ entonces, para $r \geq \dim(\mathcal{O}_P/(f_1, f_2)_P) = n$,

$$\mathcal{M}_P^r \subset (f_1, f_2)_P, \tag{A.8}$$

es decir, tenemos que probar que dada una colección $t_1, t_2, \ldots, t_r$ en $\mathcal{M}_P$, su producto $t_1t_2 \cdot \ldots \cdot t_r \in (f_1, f_2)_P$. Para verlo vamos a definir los siguientes ideales:

$$J_i = t_1t_2\cdots t_i\mathcal{O}_P + (f_1, f_2)_P \text{ para } 1 \leq i \leq r, \text{ y } J_{r+1} = (f_1, f_2)_P.$$

Nótese que

$$\mathcal{M}_P \supset J_1 \supset J_2 \supset \ldots \supset J_r \supset J_{r+1} = (f_1, f_2)_P.$$

Del hecho de que $r \geq \dim(\mathcal{O}_P/(f_1, f_2)_P)$ vemos que $\dim(\mathcal{M}_P/(f_1, f_2)_P) \leq r-1$, pues

$$r \geq \dim(\mathcal{O}_P/(f_1, f_2)_P) = 1 + \dim(\mathcal{M}_P/(f_1, f_2)_P) \Rightarrow \dim(\mathcal{M}_P/(f_1, f_2)_P) \leq r-1.$$

Deducimos así que $\exists$ un $i \in \{1, \ldots, r\}$ tal que $J_i = J_{i+1}$, ya que en caso contrario tendríamos que $\exists j_i \in J_i/J_{i-1}\ \forall i\ 2 \leq i \leq r+1$. Puesto que $\dim(\mathcal{M}_P/(f_1, f_2)_P) \leq r-1$, tenemos que los $\bar{j}_2, \ldots, \bar{j}_{r+1}$ son linealmente dependientes módulo $(f_1, f_2)_P$, por tanto, existe una combinación no trivial de $\lambda_i's$ tal que:

$$\bar{0} = \lambda_1\bar{j}_1 + \ldots + \lambda_r\bar{j}_r.$$

Sea l el máximo i tal que $\lambda_i \neq 0$ y m el penúltimo en cumplir lo mismo.

$$\rho = \lambda_l(t_1t_2\cdots t_l\phi_l + \rho_l) + \lambda_r(t_1t_2\cdots t_r\phi_r + \rho_r) + \ldots + \lambda_1(t_1\phi_1 + \rho_1),$$

$$t_1t_2\cdots t_l\phi_l + \rho_l = -\frac{\lambda_m}{\lambda_l}(t_1t_2\cdots t_m\phi_m + \rho_m) - \ldots - \frac{\lambda_1}{\lambda_l}(t_1\phi_1 + \rho_1) + \frac{\rho}{\lambda_l}.$$

Con $\rho, \rho_i \in (f_1, f_2)_P$ y $\phi_i \in \mathcal{O}_P$. Por tanto, $j_l \in J_m$ lo que es una contradicción. Si $i = r$ ya hemos terminado. Si $i < r$ entonces

$$t_1t_2\cdots t_i = t_1t_2\cdots t_{i+1}\phi + \rho$$

para algún $\phi \in \mathcal{O}_P$ y $\rho \in (f_1, f_2)_P$. Pero $(1+t_{i+1}\phi)(P) = 1$ por lo que $\rho(1-t_{1+i}\phi)^{-1} \in \mathcal{O}_P$. Por tanto,

$$t_1t_2\cdots t_r = \rho(1 - t_{i+1}\phi)^{-1}t_{i+1}\cdots t_r \in (f_1, f_2)_P.$$

Si el siguiente homomorfismo:

$$\begin{aligned} R &\longrightarrow \prod_{P\in C_1\cap C_2\cap\mathbb{A}^2} \mathcal{O}_P/(f_1, f_2)_P \\ f &\longrightarrow (\ldots, f \mathrm{mod}(f_1, f_2)_P, \ldots)_{P\in C_1\cap C_2\cap\mathbb{A}^2} \end{aligned}$$

fuese sobreyectivo podríamos concluir (A+) ya que, para J el kernel, $(f_1, f_2)_P \subset J$, por lo que $\dim(R/(f_1, f_2)_P) \geq \dim(R/J)$ y por la sobreyectividad tendríamos que:

$$\dim R/J = \sum_P \dim(\mathcal{O}_P/(f_1, f_2)_P) = \sum_p I(C_1 \cap C_2, P).$$

Comprobemos, y concluyamos así la sobreyectividad, que para $P \in C_1 \cap C_2 \cap \mathbb{A}^2$ y $\phi \in \mathcal{O}_P$, existe un polinomio $g \in R$ tal que:

$$\begin{aligned} &g \equiv \phi(\mathrm{mod}(f_1, f_2)_P). \\ &g \equiv 0(\mathrm{mod}(f_1, f_2)_Q) \text{para todo } Q \notin P \text{ con } Q \in C_1 \cap C_2 \cap \mathbb{A}^2. \end{aligned}$$

Como ya vimos en $\boxed{1}$, existe $h(x, y) \in R$ tal que $h(P) = 1$ y $h(Q) = 0\ \forall Q \in C_1 \cap C_2 \cap \mathbb{A}^2\backslash\{P\}$. Tenemos así que $h^{-1} \in \mathcal{O}_P$ y $h \in \mathcal{M}_Q\ \forall Q \in C_1 \cap C_2 \cap \mathbb{A}^2$. Para $r \geq 1$, $h^{-r} \in \mathcal{O}_P$ y por (A.8), para r lo suficientemente grande tenemos que $h^r \in (f_1, f_2)_Q\ \forall Q \in C_1 \cap C_2 \cap \mathbb{A}^2\backslash\{P\}$. Puesto que $\mathcal{O}_P = R + (f_1, f_2)_P$, $\exists f \in R$ tal que $f \equiv \phi h^{-r} \mathrm{mod}(f_1, f_2)_P$. Por lo que basta con tomar $g = fh^r$.

$\boxed{4}$ Para probar que $(A+)$ es una igualdad, bastaría con probar que $J \subset (f_1, f_2)$. Sea $f \in J$, definimos:

$$L = \{g \in R : gf \in (f_1, f_2)\}$$

y veamos que $1 \in L$. Supongamos lo contrario.
La primera observación es que L es un ideal. La segunda es que $\forall P \in \mathbb{A}^2$ existe un polinomio $g \in L$ tal que $g(P) \neq 0$. Esto se debe a que:

- Si $P \notin C_1 \cap C_2$: $f_i(P) \neq 0$ o $f_2(P) \neq 0$ y siempre tenemos que $f_i \in (f_1, f_2)$.
- Si $P \in C_1 \cap C_2$: Puesto que $f \in J$, tenemos que $f = \frac{h_1}{h}f_1 + \frac{h_2}{h}f_2 \in (f_1, f_2)_P$, con $\frac{h_1}{h}, \frac{h_2}{h} \in \mathcal{O}_P \therefore hf = h_1f_1 + h_2f_2 \Rightarrow h \in L$ y $h(P) \neq 0$.

Además, $\exists a \in k$ tal que $1 \notin L + R(x - a)$. Supongamos que no es así. Tenemos que no todas las potencias de x pueden ser linealmente independientes módulo L, por lo que existe una combinación no trivial para un n tal que

$$x^n + c_1x^{n-1} + \ldots + c_n \in L.$$

Puesto que k es algebráicamente cerrado tenemos que

$$x^n + c_1x^{n-1} + \ldots + c_n = (x - a_1) \cdot (x - a_2) \cdots (x - a_n) \in L \text{ y } a_i \in k.$$

Si $1 \in L + R(x - a_i)$ $\forall i = 1, \ldots, n$, entonces:

$$1 = l_i + r_i(x - a_i) \text{ con } l_i \in L,\ r_i \in R \text{ entonces } 1 = \prod_{i=1}^{n} (l_i + r_i(x - a_i)) \in L.$$

Lo que es una contradicción.

De la misma manera, pero cambiando L por $L + R(x - a)$ y x por y, demostramos que $\exists\ b \in k$ tal que $1 \notin L + R(x - a) + R(x - b)$ Por último, sea $P = (a, b)$ y $g \in L$:

$$\begin{aligned} g(x, y) &= g(a + (x - a), b + (y - b)) \\ &= g(a, b) + g_1(x, y)(x - a) + g_2(x, y)(y - b). \end{aligned}$$

lo que implica que $g(a, b) \in L + R(x - a) + R(y - b)$.

Por lo que o bien $\forall g \in L$ $g(a, b) = 0$ lo que es una contradicción o $g(a, b) \neq 0$, pero si esto último ocurre entonces dividiendo por $g(a, b)$ tenemos que, $1 \in L + R(x - a) + R(x - b)$, lo que también es una contradicción, por tanto, $1 \in L$. Y así tenemos que

$$J \subset (f_1, f_2)_P.$$

Todo lo visto hasta ahora era un medio para llegar a un fin:

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P) = \dim(R/(f_1, f_2)) \leq n_1 n_2.$$

Donde la igualdad se da si C_1 y C_2 no se encuentran en infinito. Por tanto, ya tenemos demostrado Bezout para curvas en cuya intersección no hay puntos con $z = 0$.

5 En este punto demostraremos que existe una línea L en el plano proyectivo de forma que no interseca con la intersección de C_1 y C_2. Trasladaremos L para que esta sea la línea del infinito y tengamos de esta forma que

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = \sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P) = \dim(R/(f_1, f_2)) = n_1 n_2.$$

Y así podremos dar por concluída la demostración del teorema de Bezout.

Probaremos para ello que para un conjunto finito S de puntos de $\mathbb{P}^2$, existe una línea L que no contiene a ninguno de dicho puntos y que $C_1 \cap C_2$ es finito.

Tenemos que para un conjunto de un elemento se cumple. Procedemos por inducción, supongamos que se cumple para conjuntos de n puntos y veámoslo para conjuntos de $n + 1$ puntos. Sea S un conjunto de $n + 1$ puntos, tomamos un subconjunto, S_1, de n puntos y la recta L_1 , que existe por hipótesis de inducción, tal que $L_1(P_i) \neq 0$ $\forall P \in S_1$ y otro subconjunto de n puntos S_2, con $S_1 \cap S_2 \neq S_1$, y su L_2. Definimos la siguiente recta L

$$L = L_1 + c \cdot L_2$$

y veamos qué debe cumplir este c para que $L(P) = 0\ \forall P \in S$.

- Para $P \notin S_1$ tenemos que $L(P) = L_1(P) + cL_2(P) = L_1(P)$.
- Para $P \notin S_2$ tenemos que $L(P) = L_1(P) + cL_2(P) = cL_2(P)$.
- Para $P \in S_1 \cap S_2$ tenemos que $L(P) = L_1(P) + cL_2(P)$ Por lo que cogemos una c tal que $c \neq -\dfrac{L_1(P)}{L_2(P)}\ \forall P \in S_1 \cap S_2$ esto existe porque estamos sobre un cuerpo infinito (todo cuerpo algebraico es infinito).

Hemos demostrado que existen infinitas rectas que no contienen ningún punto de S.

Veamos que $C_1 \cap C_2$ es finito. Por (1) tenemos que el número de puntos que están en $C_1 \cap C_2$ y no en la recta infinito, son finitos (siempre y cuando la recta del infinito no sea una componente de C_1 o C_2, en cuyo caso cambiamos de coordenadas). Y por (2) el número de puntos que están en el infinito y a su vez se encuentran en C_1 y C_2 es finito. Por tanto, $C_1 \cap C_2$ es finito.

En consecuencia, tenemos que podemos hacer un cambio de coordenadas tal que la recta del infinito pase a ser una que cumpla que:

- No interseca con $C_1 \cap C_2$.
- No es una componente de C_1 o C_2.

De esta forma C_1 y C_2, en estas coordenadas, no se intersecarían en el infinito y ya tendríamos demostrado el Teorema de Bezout. ♮

A.2. Demostración: Proposición 1.15.

Demostración. Puesto que $I_P(C_1, C_2)$ no depende de las coordenadas podemos suponer que $P = [0, 0, 1]$. Sea

$$\mathcal{M} = \{f = f(x, y) \in R : f(P) = f(0, 0) = 0\}.$$

Tenemos entonces que $\mathcal{M} = (x, y)$ y $\mathcal{M}_P = (x, y)_P = \mathcal{O}_P x + \mathcal{O}_P y$. De aquí deducimos que $\mathcal{M}^n$ es el ideal de R que está generado por $x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n$. Para $f \in R$ tenemos que se expresa de forma única como

$$f(x, y) = c_{00} + c_{10}x + c_{01}y + \cdots + c_{ij}x^i y^j + \cdots + c_{on}y^n + r$$

con $r \in \mathcal{M}^{n+1}$. Veamos que $R/\mathcal{M}^{n+1} \cong \mathcal{O}_P/\mathcal{M}_P^{n+1}$ para $n \geq 0$. La inclusión $R \subset \mathcal{O}_P$ induce un homomorfismo:

$$\begin{aligned} \gamma : R &\longrightarrow \mathcal{O}_P/\mathcal{M}_P^{n+1} \\ f &\longrightarrow \bar{f} \end{aligned}$$

Veamos que $\ker(\gamma) = \mathcal{M}^{n+1}$. Para ellos mostraremos que $\mathcal{O}_P = R + \mathcal{M}_P^{n+1}$ y que $\mathcal{M}_P^{n+1} \cap R = \mathcal{M}^{n+1}$. Para la primera igualdad tenemos que de forma directa la inclusión izquierda. La otra inclusión la obtenemos fijándonos en que $\forall \phi \in \mathcal{O}_P$ podemos escribir $\phi = f/(1-h)$ con $f \in R$ y $h \in \mathcal{M}$. Por tanto

$$\phi = \frac{f}{1-h} = f(1 + h + \cdots + h^n) + \frac{fh^{n+1}}{1-h} \in R + \mathcal{M}_P^{n+1}.$$

Para la segunda igualdad tenemos también la inclusión izquierda de forma directa, falta ver la derecha, pero esto se reduce a probar que si $gf \in \mathcal{M}^n$ y $g(P) \neq 0$, entonces $f \in \mathcal{M}^n$. Esto se ve simplemente observando que $g(P) \neq 0$ implica que el término independiente de g debe ser no nulo. Una vez visto esto, basta observar para $m \in \mathcal{M}_P^{n+1}$, entonces $\exists \frac{g_i}{h_i} \in \mathcal{M}$ para $i \in \{1, \ldots, n+1\}$ con $g_i,\ h_i \in R$ y $h_i(P) \neq 0$:

$$m = \frac{g_1}{h_1} \cdots \frac{g_{n+1}}{h_{n+1}} = \frac{g_1 \cdots g_{n+1}}{h_1 \cdots h_{n+1}}.$$

Si, además, $m \in R$, por lo que, $(h_1 \cdots h_{n+1} | g_1 \cdots g_{n+1})$. Así, por lo dicho antes, $m \in \mathcal{M}$.

Además $I(y - x^n, y) = n$. Vemos esta afirmación. Observamos que $(y - x^n, y) = (x^n, y)$, de donde deducimos que $\mathcal{M}^n \subset (x^n, y)$. Por el anterior isomorfismo tenemos que $\mathcal{O}_P/\mathcal{M}_P^n$ está generado por todos los monomios de la forma $x^i y^j$ con $0 \leq i, j \leq n-1$, por lo que por estar $\mathcal{M}^n \subset (x^n, y)$ tenemos que estos también generan $\mathcal{O}_P/(x^n, y)$. Sin embargo, este conjunto en $\mathcal{O}_P/(x^n, y)$ no es una base, pero sí que lo es el conjunto $1, x, x^2, \ldots, x^{n-1}$.

Supongamos ahora que J es un ideal de $\mathcal{O}_P$ contenido en el ideal $\Phi = (\phi_1, \phi_2)$ con $\phi_1,\ \phi_2 \in \mathcal{O}_P$ y que $\Phi = J + \mathcal{M}\Phi$, entonces $J = \Phi$. Comprobemos esto. Tenemos que podemos escribir:

$$\phi_1 = j_1 + \alpha\phi_1 + \beta\phi_2 \quad \text{y} \quad \phi_2 = j_1 + \gamma\phi_1 + \delta\phi_2$$

con $j_1,\ j_2 \in J$ y $\alpha,\ \beta,\ \gamma,\ \delta \in \mathcal{M}_P$. Pero entonces

$$\begin{pmatrix} 1-\alpha & \beta \\ \gamma & 1-\delta \end{pmatrix} \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix} = \begin{pmatrix} j_1 \\ j_2 \end{pmatrix}.$$

Si llamamos A a la matriz 2×2, tenemos que el determinante de A en P no es nulo pues:

$$(\det(A))(P) = (1 - \alpha(P))(1 - \delta(P)) - \gamma(P)\beta(P) = 1.$$

Por tanto, podemos ver el $\det(A)$ como una función de $\mathcal{O}_P$ que posee inverso, y así, podemos invertirla y obtener que $\phi_1,\ \phi_2 \in J$. Supongamos que

(A.9) $f_1 = ax + by + (\text{términos superiores})$ y $f_2 = cx + dy + (\text{términos superiores})$

con los términos de grados superiores en $\mathcal{M}^2$. Demostraremos que son equivalentes los siguientes enunciados y daremos así por finalizada la demostración:

1. La curvas $f_1 = 0$ y $f_2 = 0$ son lisas y con distintas direcciones de las tangente en P.

2. El determinante $ad - bc$ es no nulo, con $a,\ b,\ c$ y d las de (A.9).

3. $(f_1, f_2)_P = \mathcal{M}_P$, es decir, $I(f_1, f_2) = 1$.

Que 1 sea equivalente a 2 se demuestra directamente a partir de las definiciones.

Veamos 2 implica 3. Siguiendo la notación anterior tomaremos $J = (f_1, f_2)_P$, $\phi_1 = x$ y $\phi_2 = y$. Que $J \subset (x, y)_P$ se deduce fácilmente. Falta demostrar que

$$(x, y)_P = (f_1, f_2)_P + (x, y)_P^2.$$

La inclusión $\supset$ se sigue inmediatamente. Para $\subset$ vemos que si existieran unos $l,\ m \in k$ tal que

$$x - lf_1 - mf_2 \in (x, y)_P^2$$

entonces tendríamos que $x \in J + (x, y)_P^2$. Pero esto es cierto pues es equivalente a encontrar unos $m,\ l \in k$ tal que :

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} l \\ m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

y como $ad - bc \neq 0$ tenemos que la matriz en invertible y que, por tanto, existe solución. Para ver que $y \in J + (x, y)_P^2$ procedemos de igual manera pero con

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} l \\ m \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Veamos que 3 implica 2. Vemos que si tenemos que $ad - bc = 0$ entonces

$$\dim \left(\frac{(f_1, f_2)_P + \mathcal{M}_P^2}{\mathcal{M}_P^2} \right) \leq 1.$$

Esto se debe a que:

$$\begin{aligned} df_1 - bf_2 &= d(ax + by + m_1) - b(cx + dy + m_2) && \text{con } m_1,\ m_2 \in \mathcal{M}^2 \\ &= adx - bcx + dby - bdy + dm_1 - bm_2 && \text{como } ad = bc \\ &= dm_1 - bm_2 \in \mathcal{M}_P^2. \end{aligned}$$

Es decir, suponiendo, sin pérdida de generalidad que $b \neq 0$ (en el caso en que $b = d = 0$, la desigualdad se sigue inmediatamente), tenemos que $\bar{f}_2 = \frac{d}{b}\bar{f}_2$. Por lo que tenemos que la dimensión es menor o igual que uno. Pero como $R/\mathcal{M}^2 \cong \mathcal{O}_P/\mathcal{M}_P^2$ y $\mathcal{O}_P/\mathcal{M}_P^2 =< \bar{1},\ \bar{x},\ \bar{y} >$, tenemos que $\dim(\mathcal{M}_P/\mathcal{M}_P^2) = 2$, por lo que $(f_1, f_2)_P \neq \mathcal{M}_P$. ♮

A.3. Demostración: Proposición 1.23.

Demostración. Para la primera definición tenemos que para toda recta L por el Teorema de Bezout se cumple que $I_P(C, L) \leq 2$.

Para la segunda definición tenemos que

$$F(x,y,z) = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz.$$

Si definimos la matriz

$$M = \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix},$$

entonces F es su forma cuadrática asociada. Como F es irreducible tenemos que la matriz es no degenerada por lo que $det(M) \neq 0$, pero $\forall P \in C$

$$0 \neq det(M) = H_F(P).$$

Por lo que C no tiene puntos de inflexión. ♮

A.4. Demostración: Proposición 1.24.

Demostración. Puesto que la coordenadas no influyen en $I_P(C,L)$, podemos tomar unas en las que $P = [0,0,1]$ y su recta tangente sea el eje x. De esta forma

$$F(x,y,1) = y + f_2(x,y) + f_3(x,y) + \cdots + f_d(x,y)$$

con $f_i(x,y)$ polinomios homogéneos de grado i y

$$f_2(x,y) = \alpha x^2 + \beta xy + \gamma y^2.$$

Se sigue de la Proposición 1.16 que

$$P \text{ es un punto de inflexión} \Leftrightarrow \alpha = 0.$$

Para la segunda definición tenemos que

$$F(x,y,z) = z^{d-1}y + z^{d-2}f_2(x,y) + \ldots + f_d(x,y) = 0.$$

El hessiano en $P = [0,0,1]$ es

$$H_F(P) = \begin{vmatrix} 2\alpha & 2\beta & 0 \\ 2\beta & 2\gamma & d-1 \\ 0 & d-1 & 0 \end{vmatrix} = -2(d-1)^2\alpha.$$

Tenemos, por tanto, que P es un punto de inflexión si y solo si $\alpha = 0$. ♮

APÉNDICE B
Algoritmo de Weierstrass.

Lo prometido en el Capítulo 2 es deuda. A continuación veremos como para toda curva plana de grado 3 irreducible, C, definida sobre un cuerpo K con un punto $P \in C(K)$, se puede reducir, mediante transformaciones, a una curva del tipo

$$E = \{[x, y, z] \in \mathbb{P}^2 : y^2x + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

A las curva que están expresadas de esta forma diremos que están en forma de Weierstrass. Para llevar a cabo esto necesitamos los siguientes ingredientes: Una curva y un punto $P \in C(K)$. Separaremos dos casos:

1. P **punto de inflexión.**

Tomaremos este punto P y su recta tangente, L y haremos una transformación de forma que en la nuevas coordenada P sea el punto $[0, 1, 0]$ y su recta tangente, $L = \{z = 0\}$.
Sea C, la curva resultante de esta tranformación, dada por el polinomio

$$F(X, Y, Z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + jyz^2 + kz^3 = 0$$

con $a, b, c, d, e, f, g, h, j \in K$. Veamos qué deben cumplir los coficientes de F.

1. La recta tangente en el $[0, 1, 0]$ es $z = 0$ y

$$\frac{\partial F}{\partial x}(0, 1, 0) = c, \qquad \frac{\partial F}{\partial y}(0, 1, 0) = 3d, \qquad \frac{\partial F}{\partial z}(0, 1, 0) = g,$$

es decir,

$$L := cx + 3dy + gz = 0$$

y, $L = \{z = 0\}$ por lo que deducimos que

$$\boxed{d = 0} \quad \boxed{c = 0} \text{ y } \boxed{g \neq 0}$$

2. Como $[0,1,0]$ es un punto de inflexión tenemenos que:

$$\begin{vmatrix} 2b & 2c & f \\ 2c & 6d & 2g \\ f & 2g & j \end{vmatrix} = H_F(0,1,0) = 0.$$

Desarrollando y usando que $d = 0$ y $c = 0$, obtenemos que:

$$\boxed{b = 0}$$

Es decir que:

$$F(X,Y,Z) = ax^3 + exyz + fy^2z + gxz^2 + hyz^2 + jz^3.$$

Como sabemos que $g \neq 0$, podemos dividir F por $\frac{1}{g}$ y que el coeficiente de y^2x sea 1, de forma que tendríamos

$$F_1 = Ax^3 + Ex^2z + Gxyz + y^2z + Hxz^2 + Jyz^2 + Kz^3$$

con $A, E, G, H, J, K \in K$. Observar que esta trasformación sigue definiendo la misma curva C pues

$$D \cdot F(P) = 0 \Leftrightarrow F(P) = 0 \quad \forall P \ \ \forall D \in K \text{ y } D \neq 0.$$

Además, vemos que $A \neq 0$, pues en caso contrario tendríamos que podríamos sacar factor común z, lo que contradeciría la hipótesis de que C es irreducible.

Por último si hacemos el siguiente cambio:

$$\begin{cases} x & \longrightarrow & Ax, \\ y & \longrightarrow & A^2y, \\ z & \longrightarrow & z, \end{cases}$$

dividiendo entre A^4 y cambiando los nombre de los coeficiente, hemos transformado C en E:

$$E = \{[x,y,z] \in \mathbb{P}^2 : y^2x + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\}.$$

2. P **punto no singular y no de inflexión.**

Sea L la recta tangente a C en P. Como P no es un punto de inflección, tenemos que $I_P(L,C) = 2$. Por el Teorema de Bezout tenemos que debe existir un punto $Q \in C(K)$ con $P \neq Q$ tal que $Q \in C(K) \cap L$. Hagamos el siguiente cambio:

$$\begin{cases} Q & \longrightarrow & [0,0,1], \\ L & \longrightarrow & x = 0. \end{cases}$$

Sea C, la curva resultante de esta transpormación, dada por el siguiente polinomio

$$F(x,y,z) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxyz + gy^2z + hxz^2 + jyz^2 + kz^3.$$

Observar que con esta tranformación P está en la recta $x = 0$.

1. $[0,0,1] \in C$ por lo que

$$\boxed{\text{k=0}}$$

2. $P \neq [0,1,0]$ pues en caso contrario tendríamos $d = 0$ y podríamos sacar factor común la x, lo que contradiciría el hecho de que C es irreducible.

Es muy importante observar que el hecho de que $P \neq [0,1,0]$ nos dice que P está en la parte afín de C, ya que $P \in \{x = 0\}$ y $\{x = 0\} \cap \{z = 0\} = \{[0,1,0]\}$. Por tanto, si tomamos sus coordenadas no homogéneas, tendremos que son (x_0, y_0) con $x_0 = 0,\ y_0 \neq 0$ y su tangente será el eje y. Si tomamos la parte afín de C, tendríamos

$$C' = \{(x,y) \in K^2 : f(x,y) = 0\}$$

con

$$f(x,y) = ax^3 + bxy^2 + cx^2y + dy^3 + ex^2 + fxy + gy^2 + hx + jy = F(x,y,1) = 0.$$

Tenemos entonces para $f(x,y)$ que el eje y corta de forma tangente a la curva C' en un punto $P = (0, y_0)$ y además que su otro punto te intersección con C' es $Q = (0,0)$. Observemos que podemos expresar $f(x,y)$ como una suma de $f_i(x,y)$ polinomios homogéneos de grado i para $i = 1,2,3$

$$f(x,y) = f_1(x,y) + f_2(x,y) + f_3(x,y).$$

Entonces para $C \cap \{x = 0\}$ tenemos que

$$\begin{aligned} 0 = f(0,y) &= f_1(0,y) + f_2(0,y) + f_3(0,y) \\ &= yf_1(0,1) + y^2 f_2(0,1) + y^3 f_3(0,1) \\ &= y \cdot [f_1(0,1) + yf_2(0,1) + y^2 f_3(0,1)]. \end{aligned}$$

Teniendo en cuenta que $I_Q(C, \{x = 0\}) = 1$ y la Proposición 1.16 tenemos que y_0 debe ser una raíz doble de

$$f_1(0,1) + yf_2(0,1) + y^2 f_3(0,1).$$

como la raíz es doble tenemos que su discriminante debe ser 0, es decir que:

$$[f_2(0,1)]^2 - 4f_1(0,1)f_3(0,1) = 0.$$

Tenemos que todos los puntos, (x,y), de $\mathbb{A}^2$ se pueden expresar de la forma (x,tx), con $t \in k$, supongamos que (x,y) es solución de $f(x,y)$ y pongamos en de la forma (x,tx). Tenemos entonces para este punto:

$$\begin{aligned} f(x,tx) &= f_1(x,tx) + f_2(x,tx) + f_3(x,tx) \\ &= xf_1(x,t) + x^2 f_2(x,t) + x^3 f_3(x,t) \\ &= x[f_1(x,t) + xf_2(x,t) + x^2 f_3(x,t)]. \end{aligned}$$

Como tenemos que el punto es solución y suponiendo que $x \neq 0$ entonces:

$$x = \frac{-f_2(1,t) \pm \sqrt{(f_2(1,t))^2 - 4f_1(1,t)f_3(1,t)}}{2f_3(1,t)}.$$

Fijaremos el cambio

$$s^2 = [f_2(1,t)]^2 - 4f_1(1,t)f_3(1,t) = G(t).$$

Veamos que $G(t)$ tiene grado 4. Escribamos los polinomios $f_i(x,y)$ de la siguiente forma:

$$\begin{aligned} f_3(x,y) &= ax^3 + bxy^2 + cx^2y + dy^3, \\ f_2(x,y) &= ex^2 + fxy + gy^2, \\ f_1(x,y) &= hx + jy. \end{aligned}$$

Así que el coeficiente de t^3 en $G(t)$ es

$$g^2 - 4jd.$$

Pero observemos que:

$$f_1(0,1) = j, \qquad f_2(0,1) = g^2, \qquad f_3(0,1) = d,$$

por lo que el coeficiente de t^4 es

$$[f_2(0,1)]^2 - 4f_1(0,1)f_3(0,1)$$

que ya vimos que era 0. Ahora veamos que el coeficiente de t^3 no es nulo. El coeficiente de t^3 es:

$$2fg - 4(hd + jb).$$

Una primera observaión sería que con una cambio lineal de variable podríamos hacer que $y_0 = -1$ y, como este cambio de variable es lineal, esto no cambiaría ninguna de las conclusiones. Aplicando nuevamente que $I_Q(C, \{x = 0\}) = 1$ y la Proposición 1.16 vemos que

$$\boxed{j \neq 0}$$

pues:

$$f(0,y) = y(dy^2 + gy + j).$$

Ahora como $(0,-1) \in C$ tenemos que

$$0 = f(0,-1) = -d + g - j \Rightarrow g = j + d.$$

Pero ya habíamos visto que $g^2 - 4kd = 0$, por lo que unido a que $g = k + d$ obtenemos:

$$(j-d)^2 = 0$$

O sea que $j = d$ y $g = 2j$. Si dividemos la curva entre j, lo que no la variaría, obtenemos que:

$$\boxed{j = d = 1} \qquad \boxed{g = 2}$$

Si suponemos que el coeficiente de t^3 es 0 y utilizando esto último vemos que:

$$f = h + b.$$

Uniendo todas estas igualdades vemos que

$$\frac{\partial f}{\partial x}(0,-1) = \frac{\partial f}{\partial y}(0,-1) = 0,$$

que es una contradicción pues $(0,-1)$ no es singular. Por lo que:

$$s^2 = at^3 + bt^2 + ct + d.$$

Si hacemos el siguiente cambio:

$$s = a^2 y,$$
$$t = ax,$$

obtenemos

$$y^2 = x^3 + Ax^2 + Bx + C,$$

homogeneizando, ya tenemos que:

$$Y^2 Z = X^3 + AX^2 Z + BXZ^2 + CZ^3.$$

Observar que todos los cambios de variables y conclusiones son legales para $char(K) \neq 2$. Para $char(K) = 2$, se utiliza otro algoritmo mucho más complicado.

APÉNDICE C
Demostraciones Capítulo 3.

C.1. Demostración: Teorema del descenso.

Demostración. Puesto que en nuestra hipótesis A/mA es finito podemos elegir $Q_1, \ldots, Q_r \in A$ que sean representante de las clases. Si tomamos un $P \in A$, entonces $\exists\ i$ tal que $P - Q_i \in mA$, es decir,

$$\exists i_1 \in \{1, \ldots, r\} \text{ y } \exists P_1 \in A \text{ tal que } P - Q_{i_1} = [m]P_1.$$

Este proceso lo iteramos $n-1$ veces para $P_1, \ldots, P_{n-1}$, es decir:

$$\begin{aligned} P_1 &= [m]P_2 + Q_{i_2}, \\ P_2 &= [m]P_3 + Q_{i_2}, \\ &\vdots \\ P_{n-1} &= [m]P_n + Q_{i_n}. \end{aligned}$$

De esta forma podemos escribir:

$$\begin{aligned} P &= Q_{i_1} + [m]P_1 = Q_{i_1} + [m]Q_{i_2} + [m^2]P = \ldots = \\ &= [m^n]P_n + \sum_{j=1}^{n} [m^{j-1}]Q_{i_j}. \end{aligned}$$

Así que:

$$P \in < Q_1, \ldots, Q_r, P_n > .$$

Si demostramos que $\forall P\ \exists C$ tal que $h(P_n) \leq C$ para algún n, entonces habremos demostrado que

$$A = < \{Q_1, \ldots, Q_r\} \cup \{P \in A : h(P) \leq C\} > .$$

De aquí concluiríamos que A es finitamente generado pues por (iii) el conjunto $\{P \in A : h(P) \leq C\}$ es finito. Veamos cuál es esta constante C. Por (ii) tenemos que para cada j:

$$h([m]P_j) \geq m^2 h(P_j) - C_2.$$

Despejando:

$$h(P_j) \leq \frac{1}{m^2}[h([m]P_j) + C_2] = \frac{1}{m^2}[h(P_{j-1} \ominus Q_{i_j}) + C_2].$$

Por (1)

$$h(P_j) \leq \frac{1}{m^2}[2h(P_{j-1}) + C_1' + C_2] \tag{C.1}$$

con $C_1' = \max_{1 \leq i \leq r}\{C_1(\ominus Q_i)\}$. Nótese que ni C_1', ni C_2 dependen de los P_j. Si usamos la desigualdad (C.1) para P_n hasta llegar a P, obtenemos:

$$\begin{aligned}
h(P_n) &\leq \frac{1}{m^2}[2h(P_{n-1}) + C_1' + C_2] \\
&= \frac{2}{m^2}h(P_{n-1}) + \frac{1}{m^2}[C_1' + C_2] \\
&\leq \frac{1}{m^2}\left[\frac{2}{m^2}[2h(P_{n-2}) + C_1' + C_2]\right] + \frac{1}{m^2}[C_1' + C_2] \\
&= \left(\frac{2}{m^2}\right)^2 h(P_{n-2}) + [C_1' + C_2]\left(\frac{1}{m^2} + \frac{2}{m^4}\right) \\
&\vdots \\
&\leq \left(\frac{1}{m^2}\right)^n h(P) + \left[\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \ldots + \frac{2^{n-1}}{m^{2x}}\right]\left(C_1' + C_2\right) \\
&\leq \left(\frac{1}{m^2}\right)^n h(P) + \frac{1}{2}\left(C_1' + C_2\right)\sum_{i=1}^{n-1}\left(\frac{2}{m^2}\right)^i.
\end{aligned}$$

Como $m \geq 2$ tenemos que

$$\begin{aligned}
h(P_n) &\leq \left(\frac{1}{m^2}\right)^n h(P) + \frac{1}{2}\left(C_1' + C_2\right) \cdot \frac{\frac{2}{m^2}}{1 - \frac{2}{m^2}} \\
&\leq 2^{-n}h(P) + \frac{C_1' + C_2}{2}.
\end{aligned}$$

Si tomamos un n lo suficientemente grande tenemos que:

$$h(P_n) \leq 1 + \frac{C_1' + C_2}{2}.$$

En consecuencia, el siguiente conjunto finito

$$\{Q_1, \ldots, Q_r\} \cup \left\{Q \in A : h(Q) \leq 1 + \frac{C_1' + C_2}{2}\right\}$$

genera A. ♮

C.2. Demostración: Proposición 3.1.

Demostración. Si $P = (x, y)$ es un elemento de $E(\mathbb{Q})$ y $\sigma \in Gal(K/\mathbb{Q})$, entonces

$$P^\sigma = (\sigma(x), \sigma(y)) \in E(K).$$

Además σ actúa sobre $E(K)$ como un homomorfismo de grupos, es decir,

$$(P \oplus Q)^\sigma = P^\sigma \oplus Q^\sigma.$$

Esto se debe a que al sumar P y Q el punto de que nos queda, en su forma explícita, solo depende de los coeficientes del polinomio $f(x)$, que están en $\mathbb{Q}$, y de las coordenadas de P y Q. Definamos ahora:

$$E[2] := \{Q \in E : [2]Q = \mathcal{O}\} = \{(\alpha, 0), (\beta, 0), (\gamma, 0), \mathcal{O}\}.$$

Para un $P \in \ker(\phi)$, elegimos $Q_P \in E(K)$ de forma que $[2]Q_P = P$. Con este Q_P, dependiente de P, y P, definiremos la siguiente aplicación:

$$\begin{array}{rccl} \lambda: & \ker(\phi) & \longrightarrow & \{\textbf{Aplicaciones de } \mathrm{Gal}(K/\mathbb{Q}) \text{ a } E[2]\} \\ & P & \longrightarrow & \lambda_P: \ Gal(K/\mathbb{Q}) \longrightarrow E[2] \\ & & & \qquad \sigma \longrightarrow \lambda_P(\sigma) := Q_P^\sigma \ominus Q_P. \end{array}$$

Primero y antes que nada, hay que ver si la función está bien definida.

$$\begin{aligned} [2]\lambda_P(\sigma) &= [2](Q_P^\sigma \ominus Q_P) = ([2]Q_P)^\sigma \ominus [2]Q_P \\ &= P^\sigma \ominus P = \mathcal{O} \end{aligned}$$

pues $P \in E(\mathbb{Q})$ y $\sigma \in Gal(K/\mathbb{Q})$. Por tanto la función está bien definida. Si $\lambda_P = \lambda_{P'}$ entonces

$$Q_P^\sigma \ominus Q_P = \lambda_P(\sigma) = \lambda_{P'}(\sigma) = Q_{P'}^\sigma \ominus Q_{P'} \ \forall \sigma \in Gal(K/\mathbb{Q}),$$

por lo que

$$(Q_P \ominus Q_{P'})^\sigma = Q_P^\sigma \ominus Q_{P'}^\sigma = Q_P \ominus Q_{P'} \ \ \forall \sigma \in Gal(K/\mathbb{Q}).$$

Ahora como K es una extensión normal sobre $\mathbb{Q}$, tenemos que $K^{Gal(K/\mathbb{Q})} = \mathbb{Q}$. Por tanto,

$$Q_P \ominus Q_{P'} \in E(\mathbb{Q}),$$

es decir, que si $\lambda_P = \lambda_{P'} \ \Rightarrow \ P' - P = [2](Q_{P'} - Q_P) \in 2E(\mathbb{Q})$. Y así la función λ es inyectiva. De modo que

$$|\ker\phi| \leq \#Aplicaciones(\mathrm{Gal}(K/\mathbb{Q}), E[2]) = 4^{|Gal(K/\mathbb{Q})|} = 4^{|K:\mathbb{Q}|}.$$

$\natural$

C.3. Demostración: Proposición 3.2.

Demostración. Si tenemos $P_1 \oplus P_2 = P_3$ con $P_i \in E(K)$ para $i = \{1, 2, 3\}$, para ver que es un homomorfismo basta demostrar que:

$$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha^{-1}(P_3) \in K^{*2}.$$

Cabe mencionar dos observaciones. La primera, $\forall k \in K^*/K^{*2}$, $k = k^{-1}$. La segunda, por definición de φ_α, $\forall P \in E(K)$ tenemos que $\varphi_\alpha(P) = \varphi_\alpha(\ominus P)$. De esta forma, para ver que φ_α es un homomorfismo de grupos solo tenemos que ver que

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O} \Longrightarrow \varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

Si $P_i = \mathcal{O}$, pongamos $i = 1$, entonces $P_2 \oplus P_3 = \mathcal{O}$. De aquí deducimos que $\varphi_\alpha(P_2) = \varphi_\alpha(\ominus P_3) = \varphi_\alpha(P_3)$. Se tiene, por tanto, que

$$\varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) = [\varphi_\alpha(P_2)]^2 \in K^{*2}.$$

Asumamos ahora que ninguno de los $P_i = \mathcal{O}$. Diferenciamos en casos, igual que hicimos cuando definimos φ_α.

1. $x_i \neq \alpha$ para $i = 1, 2, 3$.
   Sea $y = mx + b$ la recta que une P_1, P_2, P_3. Cada $P_i = (x_i, y_i)$ cumple que

   $$(x_i - \alpha)(x_i - \beta)(x_i - \gamma) = y^2 = (mx_i + b)^2.$$

   Por lo que $(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = 0$ para $x = x_1, x_2, x_3$. Y así,

   $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3).$$

   Si ponemos $x = \alpha$ obtenemos

   $$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = (m\alpha + b)^2.$$

   Así que por definición de φ_α

   $$\varphi_\alpha(P_1) \cdot \varphi_\alpha(P_2) \cdot \varphi_\alpha(P_3) \in K^{*2}.$$

2. $x_1 = \alpha$.
   Entonces $(x_2, y_2), (x_3, y_3) \neq (\alpha, 0)$, ya que si no alguno de los tres puntos sería $\mathcal{O}$. Sea $y = mx + b$ la recta que une a P_1, P_2, P_3. Como $x_1 = \alpha$, tenemos

   (C.2) $$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - \alpha)(x - x_2)(x - x_3).$$

   Es decir, $(x - \alpha) | (mx + b)^2$, y de aquí deducimos que $mx + b = m(x - \alpha)$. Sustituyendo en la ecuación (C.2) tenemos

   $$(x - \alpha)(x - \beta)(x - \gamma) - m^2(x - \alpha)^2 = (x - \alpha)(x - x_2)(x - x_3).$$

Dividiendo por $(x-\alpha)$

$$(x-\beta)(x-\gamma)-m^2(x-\alpha)=(x-x_2)(x-x_3).$$

Tomando $x=\alpha$ conseguimos

$$(\alpha-\beta)(\alpha-\gamma)=(\alpha-x_2)(\alpha-x_3),$$

es decir,

$$\varphi_\alpha(P_1)=\varphi_\alpha(P_2)\cdot\varphi_\alpha(P_3).$$

Luego

$$\varphi_\alpha(P_1)\cdot\varphi_\alpha(P_2)\cdot\varphi_\alpha(P_3)=[\varphi_\alpha(P_2)\cdot\varphi_\alpha(P_3)]^2\in K^{*2}.$$

□

C.4. Demostración: Teorema 3.6.

Demostración. Sea $h=h_K$. Tomanos como representantes $I_1,\dots,I_h$ de las respectivas clases y tomamos $I_1=(1)$. Ahora escogemos un elemento $u_j\in I_j$ para cada $j\in\{1,\dots,h\}$ con $u_j\neq 0$ y definimos el elemento $u=u_1\cdots u_h$. Nótese que este $u\in I_j$ para $1\leq j\leq h$. Definimos el subconjunto $S=\{1,u,u^2,\dots\}$. Vemos S cumple:

1. $1\in S$ y $0\notin S$.
2. S es cerrado para la multiplicación.

De estas propiedades se puede deducir que $S^{-1}O_K=\{s^{-1}\alpha|s\in S,\ \alpha\in O_K\}$ es un subanillo de K. Veamos que $S^{-1}O_K$ es un dominio principal y que su grupo de unidades está finitamente generado como grupo abeliano. Con esto ya habríamos demostrado el teorema pues $O_K\subset S^{-1}O_K$ y bastaría con tomar $R=S^{-1}O_K$.
Sea I un ideal de O_K, entonces definimos $\bar{I}=S^{-1}I$. Veamos que es un ideal de $S^{-1}O_K$:

1. Sea $a=\alpha_a u^n,\ b=\alpha_b u^m\in\bar{I}$ entonces (asumiendo que $n\geq m$)

   $$a-b=(\alpha_a u^n-\alpha_b u^m)=u^n(\alpha_a-\alpha_b u^{n-m})\in\bar{I},$$

   con $u^n\in S,\ \alpha_a,\alpha_b\in I$ y $u^{n-m}\in S$, ya que $n\leq m$.
2. $\forall\eta=u^{-m}\alpha_\eta\in S^{-1}O_K$ y $\forall\theta=u^{-n}\alpha_\theta\in\bar{I}$

   $$\eta\theta=u^{-m}\alpha_\eta u^{-n}\alpha_\theta=u^{-m-n}\alpha_\eta\alpha_\theta\in\bar{I},$$

   pues $\alpha_\eta\in S^{-1}O_K$ y $\alpha_\theta\in I$.

Y así es como se generan los ideales de $S^{-1}O_K$, ya que $\forall I_S\subset S^{-1}O_K$ ideal, se tiene que $I=I_S\cap O_K$ es un ideal de O_K e $\bar{I}=S^{-1}(I_S\cap O_K)$ coincide con I_S. Veamos esto último:

$\boxed{\subset}$ Sea $i \in \bar{I}$. Entonces $i = s^{-1}\alpha$ con $\alpha \in I_S \cap O_K$. Puesto que $s^{-1} \in S^{-1} \subset S^{-1}O_K$ e I_S es un ideal de $S^{-1}O_K$ tenemos que $i = s^{-1}\alpha \in I_S$.

$\boxed{\supset}$ Si $i \in I_S$, entonces $i = s^{-1}\alpha$ con $\alpha \in O_K$. Además $\alpha = si \in I_S$ pues $s \in S^{-1}O_K$, por tanto $\alpha \in I_S \cap O_K \;\Rightarrow\; i = s^{-1}\alpha \in S^{-1}(I_S \cap O_K) = \bar{I}$.

Ahora, veamos que si I_S es in ideal de $S^{-1}O_K$ entonces es un ideal principal. Sea $I = I_S \cap S$, entonces I es equivalente a algún I_j con $1 \leq j \leq h$ $\therefore$

$$(\alpha)I = (\beta)I_j.$$

Como $u \in I_j \cap S$, tenemos que $S^{-1}I_j = S^{-1}O_K$, por lo que

$$(\alpha)_S I_S = S^{-1}(\alpha)S^{-1}I = S^{-1}(\beta) = S^{-1}O_K(\beta) = (\beta)_S, \tag{C.3}$$

donde $(\alpha)_S$ y $(\beta)_S$ son ideales principales de $S^{-1}O_K$. Veamos que

$$\beta/\alpha \in S^{-1}O_K \text{ e } I_S = (\beta/\alpha)_S.$$

(C.3) nos permite escribir $\beta = \alpha i_0$ para algún $i \in I_S$. Por tanto, $\beta/\alpha \in I_S \subset S^{-1}O_K$, y así tenemos que $(\beta/\alpha) \subset I_S$. Para la otra inclusión tenemos que: Sea $i \in I_S$, podemos escribir por (C.3) $\alpha i = \beta x$ con $x \in S^{-1}O_K$. Entonces $i = \frac{\beta}{\alpha}x$, lo que demuestra que $i \in (\beta/\alpha)_S$.

El hecho de que I_S es un ideal arbitrario de $S^{-1}O_K$, hace que ya hayamos demostrado que $S^{-1}O_K$ es un dominio de ideales principales. Nos falta demostrar que $(S^{-1}O_K)^\times$ es finitamente generado.

Sea $u^{-s}\alpha \in (S^{-1}O_K)^\times$, y escribimos $(u^{-s}\alpha)^{-1} = u^{-t}\beta$. Entonces $\alpha\beta = u^{s+t}$. Es decir, que α es un divisor de una potencia u^n con $n \in \mathbb{N}$. Buscamos un conjunto finito de generadores de los divisores de todas las potencias ≥ 0 de u.
Sea $\alpha\beta = u^r$ con $\alpha, \beta \in \mathcal{O}_K$. Sea

$$(u) = P_1^{k_1} \cdots P_N^{k_N}$$

la factorización de (u), entonces tenemos que:

$$(\alpha)(\beta) = (u^r) = (u)^r = P_1^{k_1 r} \cdots P_N^{k_N r}.$$

Por unicidad obtenemos que:

$$(\alpha) = P_1^{I_1} \cdots P_N^{I_N} \text{ con } 0 \leq l_j \leq k_j r \text{ para } 1 \leq j \leq N.$$

Por la anterior igualdad tenemos que P_j^h es un ideal principal para cada j. Escribimos $P_j^h = (\gamma_j)$. Para cada j, escribimos $l_j = q_j h + r$ con $0 \leq r_j < h$, de manera que:

$$(\alpha) = (\gamma_1)^{q_1} \cdots (\gamma_N)^{q_N} P_1^{r_1} \cdots P_N^{r_N}. \tag{C.4}$$

Así que

$$\alpha = \gamma_1^{q_1} \cdots \gamma_N^{q_N} i \quad \text{con} \quad i \in P_1^{r_1} \cdots P_N^{r_N}.$$

Dividiendo obtenemos que $\frac{\alpha}{\gamma_1^{q_1}\cdots\gamma_N^{q_N}} = i \in O_K$. Podemos, entonces, reescribir (C.4) como

$$\gamma_1^{q_1}\cdots\gamma_N^{q_N}\left(\frac{\alpha}{\gamma_1^{q_1}\cdots\gamma_N^{q_N}}\right) = (\gamma_1^{q_1}\cdots\gamma_N^{q_N})P_1^{r_1}\cdots P_N^{r_N},$$

es decir, que

$$\left(\frac{\alpha}{\gamma_1^{q_1}\cdots\gamma_N^{q_N}}\right) = P_1^{r_1}\cdots P_N^{r_N}.$$

Así que el ideal $P_1^{r_1}\cdots P_N^{r_N}$ es un ideal principal. Definamos

$$P_1^{r_1}\cdots P_N^{r_N} = (\delta_{r_1,\ldots,r_N}).$$

para cada $0 \leq r_j < h$ para $1 \leq j \leq N$. Por (C.4) tenemos que

$$\alpha = \gamma_1^{q_1}\cdots\gamma_N^{q_N}\delta_{r_1,\ldots,r_N}\epsilon \quad \text{con} \quad \epsilon \in (O_K)^\times$$

De aquí concluimos que $(S^{-1}O_K)^\times$ está generado por $\gamma_1^{q_1}\cdots\gamma_N^{q_N}$, el número finito de elementos $\delta_{r_1,\ldots,r_N}$ y $(O_K)^\times$. Puesto que, por el Teorema de las unidades de Dirichlet, $(O_K)^\times$ está finitamente generado, tenemos que ya demostrado que $(S^{-1}O_K)^\times$ es finitamente generado. ♮

C.5. Demostración: Teorema 3.11.

C.5.1. Propiedad (1):

Lema C.1. Sea E un curva elíptica de la forma

$$E : y^2 = x^3 + Ax + B$$

con $A, B \in \mathbb{Z}$. *Si* $P = (x, y)$ *un punto racional, entonces*

$$x = \frac{m}{e^2} \quad \text{e} \quad y = \frac{n}{e^3}$$

para enteros m, n y e con $e > 0$ y $\text{mcd}(e, n) = \text{mcd}(m, e) = 1$.

Demostración. Sea $x = \frac{m}{M}$ e $y = \frac{n}{N}$ con ambas fracciones irreducibles, con $M, N > 0$. Sustituyendo en la ecuación de la curva tenemos que:

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + A\frac{m}{M} + B.$$

Por tanto

$$M^3n^2 = N^2m^3 + AN^2M^2m + BN^2M^3. \tag{C.5}$$

Tenemos que por (C.5), $N^2 \mid M^3n^2$, pero como $\text{mcd}(N, n) = 1$, tenemos que $N^2 \mid M^3$. Veamos que $M^3 \mid N^2$. Por (C.5), $M^2 \mid N^2m^3$, pero como $\text{mcd}(M, m) = 1$, tenemos que $M^2 \mid N^2 \Rightarrow M \mid N$. Usando esto y nuevamente (C.5), vemos que $M^3 \mid N^2n^3$, por

lo que $M^3 = N^2$.
Sea $e = \frac{N}{M}$ entonces

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{m^2} = M \quad \text{y} \quad e^3 = \frac{N^3}{M^3} = \frac{N^3}{n^2} = N.$$

Es decir que, $x = \frac{m}{e^2}$ e $y = \frac{n}{e^3}$ con $\text{mcd}(m, e) = \text{mcd}(n, e) = 1$, esto último se debe a que m y M y n y N eran coprimos por hipótesis. ♮

Observación C.2. Antes de demostrar la propiedad (1) veamos una última observación. Sea $P = (\frac{m}{e^2}, \frac{n}{e^3})$ entonces

$$|m| \leq H(P) \quad \text{y} \quad e^2 \leq H(P).$$

Veamos que se puede acotar n en función de $H(P)$. Para ser más exactos $\exists K > 0$ constante dependiente únicamente de A, B tal que

$$|n| \leq KH(P)^{3/2} \qquad \forall P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q}).$$

Si P es un punto de la curva E entonces multiplicando por e^6 tenemos que

$$n^2 = m^3 + Ae^4m + Be^6.$$

Así que

$$\begin{aligned} |n^2| \leq |m^3| + |Ae^4m| + |Be^6| &\leq H(P)^3 + |A|H(P)^3 + |B|H(P)^3 \\ &= (1 + |A| + |B|)H(P)^3. \end{aligned}$$

Basta, por tanto, tomar $K = \sqrt{1 + |A| + |B|}$.

Propiedad (1): *Dado $Q \in E(\mathbb{Q})$, existe una constante $C_1 = C_1(Q)$ que depende de Q y A, tal que $\forall\ P \in E(\mathbb{Q})$,*

$$h(P \oplus Q) \leq 2h(Q) + C_1.$$

Demostración. Nótese que solo es necesario demostrarlo para todo $P \in E(\mathbb{Q})$ menos un conjunto finito, S, pues bastaría con coger el máximo entre la cota para los puntos $P \in E(\mathbb{Q})\backslash S$ y las diferencias $h(P \oplus Q) - 2h(Q)\ \forall P \in S$. Podemos obviar, de este modo, $P \neq Q,\ \ominus Q,\ \mathcal{O}$.
Por el Lema C.1 tenemos que podemos poner

$$P = (x, y) = \left(\frac{m}{e^2}, \frac{n}{m^3}\right) \quad \text{y} \quad Q = (x', y') = \left(\frac{m'}{e'^2}, \frac{n'}{e'^2}\right)$$

con $(m, n, e) = 1$ y $(m', n', e') = 1$. Usando las fórmulas explícita para la suma en $E(\mathbb{Q})$ que vimos en la sección 2.3.1, obtenemos:

$$\begin{aligned} x(P \oplus Q) = \left(\frac{y - y'}{x - x'}\right)^2 - (x - x') &= \frac{(xx' + A)(x + x') + 2B - 2yy'}{(x - x')^2} \\ &= \frac{(mm' + Ae^2e'^2)(me'^2 + m'e^2) + 2Be^4e'^4 - 2nen'e'}{(me'^2 - m'e^2)^2}. \end{aligned}$$

Por la definición de altura obtenemos que

$$H(x(P \oplus Q)) \leq C_1' \operatorname{máx}\{|m^2|, |e^4|, |me^2|, |ne|\} \leq C_1' \operatorname{máx}\{|m|^2, |e|^4, |ne|\}.$$

Donde C_1' depende solo de A, B, n', m', e', es decir, solo de la la curva E y del punto Q.

$$\begin{aligned} H(x(P \oplus Q)) &\leq C_1' \operatorname{máx}\{|m|^2, |e|^4, |ne|\} \\ &\leq C_1'' \operatorname{máx}\{|m|^2, |e|^4, |e|\} \ \text{ pues } |n| \text{ está acotado por C.2.} \\ &\leq C_1'' \operatorname{máx}\{|m|^2, |e|^4\} \ \text{ pues } e \in \mathbb{Z} \\ &\leq C_1'' H^2(x(P)). \end{aligned}$$

Tomando logaritmos obtenemos que

$$\log H(P \oplus Q) \leq \log(C_1'') + 2\log(H(x(P))),$$

lo que nos muestra que

$$h_x(P \oplus Q) \leq C_2 + 2h_x(P)$$

con $C_2 = \log(C_1'')$ una constante que depende únicamente de A, B, n', m', e', pues C_1'' así lo hace. Queda así demostrado la propiedad (1). ♮

C.5.2. Propiedad (2):

Lema C.3. *Sea* $d = 4A^3 + 27B^2$ *y sean*

$$\begin{aligned} F(x,z) &= x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4, \\ G(x,z) &= 4x^3x + 4Axz^3 + 4Bz^4. \end{aligned}$$

Entonces si definimos los siguientes polinomios $f_1, f_2, g_1, g_2 \in \mathbb{Q}[x,z]$:

$$\begin{aligned} f_1 &= -4(3x^2z + 4Az^3), \\ g_1 &= 27Bz^3 + 5Axz^2 - 3x^3, \\ f_2 &= -4(dx^3 - A^2bx^2z + (3A^2 + 22AB^2)xz^2 + 3(A^3B + 8B^3)z^3), \\ g_2 &= A^2Bx^3 + (5A^4 + 32AB^2)x^2z + (26A^3B + 192B^3)xz^2 - 3(A^5 - 8A^2B^2)z^3, \end{aligned}$$

tenemos que, tras ciertas manipulaciones, obtenemos:

$$\begin{aligned} f_1(x,z)F(x,z) - f_2(x,z)G(x,z) &= 4dz^7, \\ f_2(x,z)F(x,z) - g_2(x,z)G(x,z) &= 4dx^7. \end{aligned}$$

Propiedad (2)***:*** *Existe un entero* $m \geq 2$ *y una constante* C_2 *que depende sólo de* $E(\mathbb{Q})$*, tal que* $\forall\ P \in A$

$$h([2]P) \geq 2^2 h(P) - C_2.$$

Demostración. Podemos suponer que $P \neq \mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)$ y también distinto a cualquier punto de orden 2. Esto se debe a que si hallamos una C_2' $\forall P \in E(\mathbb{Q})$ menos para un conjunto finito S, entonces bastaría con tomar

$$C_2 = \text{máx}\{\{C_2'\} \cup \{-h([2]P) + 2^2 h(P)\} : P \in S\}.$$

Con nuestras suposiciones en mente, tenemos que $[2]P \neq \mathcal{O}$. Sea $P = (x, y)$, entonces por las fórmulas explícitas de la suma $\oplus$:

$$x([2]P) = \left(\frac{f'(x)}{2y}\right)^2 - 2x = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Los polinomio homogéneos del denominador y el denominador de $x([2]P)$ son

$$F(x, z) = x^4 - 2Ax^2z^2 - 8Bxz^3 + A^2z^4,$$
$$G(x, z) = 4x^3z + 4Axz^3 + 4Bz^4.$$

Por lo tando, si $x = \frac{a}{b}$ con $(a, b) = 1$ entonces

$$x([2]P) = \frac{F(a, b)}{G(a, b)}.$$

Tenemos que por ser E una curva lisa, definida por

$$y^2 = x^3 + Ax + B = f(x),$$

$f(x)$ y $f'(x)$ son siempre coprimos, es decir, que

$$F(x, 1) = x^4 - 2Ax^2 - 8Bx + A^2 = f'(x) - 8xf(x) \text{ y}$$
$$G(x, 1) = 4x^3 + 4Ax + 4B = 4f(x)$$

son coprimos entre sí. Sea $\delta = \text{mcd}\{F(a, b), G(a, b)\}$, entonces por el Lema C.3 se cumple que

$$\delta \mid 4db^7,$$
$$\delta \mid 4da^7.$$

Como $(a, b) = 1 \Rightarrow \delta \mid 4d$. Por lo que $|\delta| \leq |4d|$. Con esto tendríamos que

$$H(x([2]P)) \geq \frac{\text{máx}\{|F(a, b)|, |G(a, b)|\}}{|4d|}. \tag{C.6}$$

Por otro lado, utilizando el Lema C.3 y su notación vemos que

$$|4db^7| \leq 2\,\text{máx}\{f_1(a, b), g_1(a, b)\}\,\text{máx}\{F(a, b), G(a, b)\},$$
$$|4da^7| \leq 2\,\text{máx}\{f_2(a, b), g_2(a, b)\}\,\text{máx}\{F(a, b), G(a, b)\}.$$

Desarrollando f_1, f_2, f_2, g_2 tenemos

$$\text{máx}\{|f_1(a, b)|, |g_1(a, b)|, |f_2(a, b)|, |g_2(a, b)|\} \leq$$
$$\leq C(A, B)\,\text{máx}\{|a^2b|, |b^3|, |a^3|, |ab^2|\} = C(A, B)\,\text{máx}\{|b^3|, |a^3|\}$$

con $C(A,B)$ una constante dependiente únicamente de A y B. Si juntamos las desigualdades

$$\begin{aligned}&\text{máx}\{|4da^7|,|4db^7|\} \leq 2C(A,B)\,\text{máx}\{|a^3|,|b^3|\}\,\text{máx}\{|F(a,b)|,|G(a,b)|\},\\&\text{máx}\{|a^4|,|b^4|\} \leq 2C(A,B)\frac{\text{máx}\{|F(a,b)|,|G(a,b)|\}}{|4d|}.\end{aligned}$$

Con esto y (C.6) tenemos que

$$\text{máx}\{|a^4|,|b^4|\} \leq 2C(A,B)H(x([2]P)).$$

Por definición de altura

$$\frac{1}{2C(A,B)}H^4(x(P)) \leq H(x([2]P)).$$

Tomando logaritmos

$$4h_x(P) - C_2 \leq h_x([2]P),$$

donde $C_2 = \log(2C(A,B))$ es una constante solo dependiente de A y B. Tenemos así demostrado la propiedad (2). ♮

C.5.3. Propiedad (3):

Para toda constante C_3 el conjunto

$$\{P \in E(\mathbb{Q}) : h(P) \leq C_3\}$$

es finito.

Demostración. Esta propiedad se hereda del hecho de que H la posee sobre $\mathbb{Q}$, ya que por cada posible valor de x que haga del punto $P = (x,y)$ un punto de dicho conjunto, solo hay, como mucho, dos posibles valores para y. ♮

APÉNDICE D

Introducción a los números p-ádicos.

A continuación daremos una breve introducción a los número p-ádico para facilitar las comprención del Capítulo 4 a aquellos que no estén familiarizados con ellos.

Muchas de las propiedades del valor absoluto en los número reales se deben a esta tres propiedades:

(1) $|r| \geq 0$, y solo igual cuando $r = 0$.

(2) $|rs| = |r||s|$.

(3) $|r + s| \leq |r| + |s|$.

Se define como *valoración* a las funciones que cumplen estas tres propiedades.

Sobre $\mathbb{Q}$ podemos encontrar otras muchas *valoraciones* además del valor absoluto normal. La que ahora nos atañe y sobre la que contruiremos lo que llamaremos $\mathbb{Q}_p$ en la siguiente:
Sea p un primo, fijado definiremos para $\forall q \in \mathbb{Q}$ con $q = p^\sigma \frac{u}{v},\ u,\ v,\ \sigma \in \mathbb{Z}$ y $p \nmid uv$:

$$|q|_p = p^{-\sigma}$$

y

$$|0|_p = 0.$$

Tenemos que en efecto $|\cdot|_p$ cumple (1) y (2). Veamos que también cumple (3). Sea

$$q = p^\sigma \frac{u}{v} \text{ y } s = p^\delta \frac{m}{n} \text{ con } p \nmid uv,\ mn$$

tenemos que

$$|q|_p = p^{-\sigma} \text{ y } |s|_p = p^{-\delta}.$$

Podemos suponer sin pérdida de generalidad que $\delta \geq \sigma$, es decir, $|s|_p \leq |q|_p$. Entonces

$$q + s = p^\sigma (un + p^{\delta - \sigma} mv)/vn.$$

Donde $p \nmid vn$ y $(un + p^{\delta - \sigma m v})$ es un entero, por lo que

$$|r + s|_p \leq p^{-\sigma}$$

o sea que

$$|r + s|_p \leq \text{máx}\{|q|_p, |s|_p\} \tag{D.1}$$

lo que es más fuerte que la propiedad (3) y, por tanto. la demuestra. Y así tenemos que $|\cdot|_p$ es una *valoración*. La llamaremos *valoración p-ádica*.

Definamos ahora algunos conceptos que ya conocemos del valor absoluto para nuestra valoración. Sea una sucesión $\{a_n\}$ de $\mathbb{Q}$, diremos que es una *sucesión fundamental* si dado un $\epsilon > 0$ existe un n_0 tal que

$$|a_m - a_n|_p < \epsilon \quad \forall m, n > n_0$$

y diremos que converge a b si

$$|a_n - b|_p < \epsilon \quad \forall n \geq n_0.$$

Veamos un ejemplo. Sea $p = 5$ y consideremos la sucesión:

$$\{a_n\} : \ 3, \ 33, \ 333, \ 3333$$

Tenemos así que:

$$a_m \equiv a_n (\text{mod } 5^n) \quad m \geq n,$$

es decir

$$|a_m - a_n|_p \leq 5^{-n} \quad m \geq n.$$

Además, tenemos que

$$3a_n = 99 \ldots 99 \equiv -1 (\text{mod } 5^n)$$

por lo que

$$|3a_n + 1|_5 \leq 5^{-n}$$

y por tanto $a_n \longrightarrow -1/3$ en $\mathbb{Q}_5$.

Como vemos en el ejemplo algo es p-ádicamente pequeño cuanto mayor sea la potencia de p que le divida.

Al igual que pasa en $\mathbb{Q}$ con el valor absoluto normal, tenemos que $\mathbb{Q}$ con la valoración p-ádica no es completo, es decir, tenemos sucesiones fundamentales que no convergen a ningún $b \in \mathbb{Q}$. Veamos un ejemplo: Sea $p = 5$. Construímos un sucesión de $a_n \in \mathbb{Z}$ tal que

(1) $a_n^2 + 1 \equiv 0 (\text{mod } 5^n)$,

(2) $a_{n+1} \equiv a_n (\text{mod } 5^n)$.

Empezamos con $a_1 = 2$. Veamos que existe una sucesión $a_{n+1} = a_n + b5^n$, con $b \in \mathbb{Z}$ aún por determinar, tal que (1) y (2) se cumplen. Tenemos que (2) se cumple sin importar que b escajamos. Veamos (1)

$$(a_n + b5^n)^2 + 1 \equiv 0 (\text{mod } 5^{n+1})$$

por lo que nos queda que

$$2a_n b + c \equiv 0 (\text{mod } 5) \text{ con } c = (a_n^2 + 1)/5^n \in \mathbb{Z}.$$

Pero tenemos que $5 \nmid a_n$, por lo que, para $b \in \mathbb{Z}$ que cumpla, $b \equiv c/(2a_n) (\text{mod } 5)$, vemos que se cumple la segunda condición.
Supongamos que exite un $q \in \mathbb{Q}$ tal que $a_n \longrightarrow q$. Entonces

$$a_n^2 + 1 \longrightarrow q^2 + 1.$$

Por otra parte, por construcción tenemos que

$$a_n^2 + 1 \longrightarrow 0$$

y por tanto $q^2 + 1 = 0$, lo que es una contradicción.

De forma análoga a la contrucción de $\mathbb{R}$ a partir de $\mathbb{Q}$ con el valor absoluto, creamos $\mathbb{Q}_p$. Es decir, $\mathbb{Q}_p$ es el cuerpo resultado de completar $\mathbb{Q}$ usando la *valoración p-ádica* para un dado p.

Decimos que un cuerpo K con la *valoración* $\|\cdot\|$ es la completación del cuerpo k con la *valoración* $|\cdot|$ si existe una inyección $i : k \longrightarrow K$ tal que

- $\|i(a)\| = |a|$ $a \in k$,
- K es completo con respecto a $\|\cdot\|$,
- K es la clausura de $i(k)$ con la topología inducida por $\|\cdot\|$.

La completación siempre existe y es única, salvo isomorfismo. De ahora en adelante identificaremos k con $i(k)$ y $\|\cdot\|$ con $|\cdot|$. En nuestro caso k será $\mathbb{Q}$, K será $\mathbb{Q}_p$ y $|\cdot|$ será $|\cdot|_p$. Tenemos que

$$|a + b|_p = |a|_p \text{ si } |b|_p < |a|_p.$$

Esto se debe a que por (D.1) (no demostraremos que la extención $|\cdot|_p$ sobre $\mathbb{Q}_p$ conserva esta propiedad) tenemos $|a + b|_p \leq |a|_p$ y, como $a = (a + b) - b$, tendríamos una contradicción si $|a+b|_p < |a|_p$. De esta propiedad vemos que los valores que toma $|\cdot|_p$ en $\mathbb{Q}_p$, son los mismos que toma $|\cdot|_p$ en $\mathbb{Q}$. Esto se debe a que dado $\alpha \in \mathbb{Q}_p$ con $\alpha \neq 0$, por definición de completitud, existe un $a \in \mathbb{Q}$ tal que $|a-\alpha|_p < |\alpha|_p$, de donde deducimos que $|\alpha|_p = |a|_p$, pues en caso contrario llegaríamos a una contradicción.

Definimos $\mathbb{Z}_p$ como el conjunto de $\alpha \in \mathbb{Q}_p$ tal que $|\alpha|_p \leq 1$. Vemos que dicho conjunto es, de hecho, una anillo:

$$|\alpha|_p,\ |\beta|_p \leq 1 \Rightarrow |\alpha\beta|_p = |\alpha|_p \cdot |\beta|_p \leq 1 \text{ y } |\alpha + \beta|_p = \text{máx}\{|\alpha|_p, |\beta|_p\} \leq 1.$$

Veamos el siguiente teorema:

Teorema D.1.

1. *El grupo de unidades de* $\mathbb{Z}_p$ *es*

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Z}_p \mid |x|_p = 1\}.$$

2. *Para* $x \in \mathbb{Q}_p^\times$ *tenemos un modo único de ponerlo como* up^n *con* $u \in \mathbb{Z}_p^\times$ *y* $n \in \mathbb{Z}$.

3. $\mathbb{Q}_p$ *es el cuerpo de fracciones de* $\mathbb{Z}_p$.

4. $\mathbb{Z}_p$ *es un anillo local, es decir, tiene un único ideal maximal,* $\mathfrak{m}$, *que es*

$$\mathfrak{m} := \{x \in \mathbb{Z}_p | |x|_p < 1\} = p\mathbb{Z}_p.$$

Demostración.

- Si $x,\ x^{-1} \in \mathbb{Z}_p$, entonces $|x|_p,\ |x^{-1}|_p \leq 1$. Además $|x^{-1}|_p = |x|_p^{-1}$. Por lo que $|x|_p = 1$. Y por tanto, $|1|_p = |x \cdot x^{-1}|_p = |x|_p|x^{-1}|_p \Rightarrow |x^{-1}|_p = 1$.
- Si $x \in \mathbb{Q}_p^\times$, entonces $|x|_p = 1/p^n$ para algún n. Luego, $|xp^{-n}|_p = 1$, por lo que si definimos $u = xp^{-n} \in \mathbb{Z}_p$, tenemos que $x = up^n$. Veamos que la expresión es única. Supongamos que $up^n = vp^m$ con $m \geq n$, y tenemos que $v^{-1}u = p^{m-n} \in \mathbb{Z}_p^\times$, así que $m = n$ y por tanto $u = v$.
- Esto se deduce del anterior punto. Tenemos que todo elemento de $\mathbb{Z}_p$ se puede escribir de la forma up^n, con $u \in \mathbb{Z}_p^\times$ y $n \in \mathbb{N}$, y todo elemento de $\mathbb{Q}_p$ tiene la misma expresión pero con $n \in \mathbb{Z}$.
- Primero tenemos por un argumento igual a la demostración de que $\mathbb{Z}_p$ es un anillo que $\mathfrak{m}$ es un ideal. Después notamos $\mathbb{Z}_p/\mathfrak{m} = \mathbf{U}(\mathbb{Z}_p)$ (unidades de $\mathbb{Z}_p$), por lo que tenemos $\mathbb{Z}_p$ es un anillo local y $\mathfrak{m}$ su único ideal maximal.

$\natural$

Proposición D.2. Tenemos que $\mathbb{Z}_p/p^m\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$. En particular $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

Demostración. Definimos $\mathbb{Z}_{(p)} := \mathbb{Z}_p \cap \mathbb{Q} = \left\{\frac{m}{n} \in \mathbb{Q} \mid p \nmid n\right\} = \{p^n \frac{u}{v} \mid n \in \mathbb{N}, p \nmid uv\}$. Definimos el homomorfismo

$$\begin{array}{rccc} \sigma: & \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{Z}/p\mathbb{Z} \\ & p^n\frac{u}{v} & \longrightarrow & \overline{p^n u/v} = \bar{p}^n\bar{u}\bar{v}^{-1}. \end{array}$$

Como $\ker(\sigma) = p^n\mathbb{Z}_{(p)}$, se tiene $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$. Veamos ahora que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$. Sea el homomorfismo:

$$\begin{array}{rccc} \gamma: & \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{Z}_p/p^n\mathbb{Z}_p \\ & a & \longrightarrow & a + p^n\mathbb{Z}_p. \end{array}$$

Tenemos que $\ker(\gamma) = \{a \in \mathbb{Z}_p : p^n | a\} = p^n\mathbb{Z}_{(p)}$. Veamos que es sobreyectiva. Supongamos que $x \in \mathbb{Z}_p$. Como $\mathbb{Q}$ es denso en $\mathbb{Q}_p$ tenemos que existe un $a \in \mathbb{Q}$ tal que

$$|a - x|_p \leq 1/p^n.$$

O sea que $x \equiv a (\text{mod } p^n\mathbb{Z}_p)$. Y además $a \in \mathbb{Z}_p$ pues

$$|a|_p = |a - x + x|_p \leq \text{máx}\{|a - x|_p, |x|_p\} \leq 1.$$

Aplicando nuevamente el teorema de isomorfía tenemos que $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)}$. ♮

Lema D.3. En $\mathbb{Q}_p$ la serie $\sum_0^\infty \beta_n$ converge si y solo si $\beta_n \to 0$.

Demostración. Si $\sum \beta_n$ converge entonces, por definición, las sumas parciales $\sum_0^N \beta_n$ convergen. La convergencia implica que $\beta \to 0$. La otra implicación:

$$|\sum_0^N \beta_n - \sum_0^M \beta_n|_p = |\sum_{M+1}^N \beta_n|_p \leq \max_{M<n\leq N} |\beta_n|_p.$$

Por tanto, $\{\sum_0^N \beta_n\}$ es un sucesión fundamental. ♮

Teorema D.4. *Todo elemento de $x \in \mathbb{Z}_p$ puede representarse de forma única como*

$$x = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

donde $0 \leq a_i \leq p - 1$. Es decir, que como límite p-ádico

$$x = \lim_{n\to\infty} x_n.$$

donde

$$x_n = a_0 + a_1 p + \ldots + a_n p^n$$

Demostración. Veamos primero que el $\lim_{n\to\infty} x_n$ existe en $\mathbb{Q}_p$. Esto se debe al Lema D.3 y a que

$$|a_n p^n|_p = \frac{1}{p^n} \overset{n\to\infty}{\longrightarrow} 0.$$

Además,

$$|x|_p = \lim_{n\to\infty} |x_n|_p \leq 1$$

así que $x \in \mathbb{Z}_p$. Veamos ahora que $\forall x \in \mathbb{Z}_p$ se pueden encontrar tales a_n con $0 \leq a_n \leq p - 1$. Puesto que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$, existe un único $0 \leq a_0 \leq p - 1$ tal que $x = a_0 + y_1 p$ con $y_1 \in \mathbb{Z}_p$. Luego

$$|x - a_0|_p = |y_1|_p |p|_p \leq 1/p.$$

Sea $0 \leq a_1 \leq p-1$ el único elemento tal que $y_1 = a_1 + y_2 p$ con $y_2 \in \mathbb{Z}_p$. Tenemos así que

$$x = a_0 + a_1 p + y_2 p^2$$

y

$$|x - (a_0 + a_1 p)|_p = |y_2|_p |p|_p^2 \leq 1/p^2.$$

De esta forma, por inducción tenemos que:

$$|x - (a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1} + a_n p^n)|_p \leq 1/p^{n+1}.$$

Por tanto, la sucesión x_n tiene como límite x. Para ver que es única supongamos que

$$x = a_0' + a_1 p + a_2' p^2 + \ldots + a_{n-1}' p^{n-1} + a_n' p^n + \ldots .$$

Sea n el primer número tal que $a_n \neq a_n'$. Entonces:

$$|x_n - x_n'|_p = |(a_n - a_n')p^n|_p = 1/p^n$$

pero

$$|x_n - x_n'|_p = |(x_n - x) + (x - x_n')|_p \leq \text{máx}\{|(x_n - x)|_p, |(x - x_n')|_p\} \leq 1/p^{n+1}$$

lo que es una contradicción. ♮

APÉNDICE E
Demostraciones Capítulo 4.

E.1. Demostración: Teorema 4.6.

Para $p \nmid \Delta$, tenemos el homomorfismo

$$r_p|_{E(\mathbb{Q})_{tors}} : \ E(\mathbb{Q})_{tors} \longrightarrow E_p(\mathbb{F}_p).$$

Veamos cuál es el $\ker(r_p)$:

$$\ker(r_p) = \{[x, y, z] : r_p([x, y, z]) = [0, 1, 0]\}.$$

Tenemos que para $\mathbf{x} \in \ker(r_p)$, $r_p(y) \neq 0$. Por lo que $\mathbf{x}$ es de la forma $\mathbf{x} = [x, 1, z]$, con $\mathbf{x}$ un representante reducción módulo p. Pero vemos entonces que

$$\mathbf{x} \in \ker(r_p) \Leftrightarrow r_p(x) = r_p(z) = 0 \Leftrightarrow |x|_p, |z|_p < 1,$$

por lo que

$$E^{(1)}(\mathbb{Q}) := \{[x, 1, z] \in E(\mathbb{Q}) : |x|_p, |z|_p < 1\} = \ker(r_p).$$

Lema E.1. Sea $[x, 1, z] \in E(\mathbb{Q})$ $\forall p$ primo:

$$si \ |z|_p < 1 \Rightarrow \ |x|_p < 1 \text{ y } |z|_p = |x|_p^3.$$

Demostración. Sea $E(\mathbb{Q})$ el grupo de la curva dada por

$$y^2 z = x^3 + Axz^2 + Bz^3, \quad A, B \in \mathbb{Z}.$$

Tomando $y = 1$, la ecuación nos queda de la forma

$$z = x^3 + Axz^2 + Bz^3.$$

Vemos que si tuviésemos que $|x|_p \geq 1$ entonces, aplicando la propiedad ultramétrica, es decir, (D.1), obtenemos que $|z|_p = |x^3|_p = |x|_p^3$, pues

- $|Az^2|_p = |A|_p |z|_p^2 < 1 \leq |x|_p$.
- $|Bz^3|_p = |B|_p |z|_p^3 < 1 \leq |x|_p$.

Lo que es una contradicción, por lo que tenemos que $|x|_p < 1$.

Vemos ahora que, para $|x|_p < 1$, también se cumple que $|z|_p = |x|_p^3$. Para el caso $z = 0$, tenemos que $x = 0$, por lo que la igualdad se sigue de forma inmediata. Para $z \neq 0$:

$$x^3 = z + Axz^2 - Bz^3.$$

Si utilizamos, nuevamente, la propiedad ultramétrica:

- $|Axz^2|_p = |A|_p|x|_p|z^2|_p < |z|_p^2 < |z|_p$.
- $|Bz^3|_p = |B|_p|z^3|_p < |z|_p^3 < |z|_p$.

Por tanto, $|x|_p^3 = |x^3|_p = |z|_p$. ♮

Sea p un primo cualquiera. Definimos:

$$E^{(n)}(\mathbb{Q}) := \{[x, 1, z] \in E(\mathbb{Q}) : |z|_p < 1 \text{ y } |x|_p \leq p^{-n}\}$$

Por el Lema E.1 tenemos que:

$$E^{(n)}(\mathbb{Q}) = \{[x, 1, z] \in E(\mathbb{Q}) : |z|_p \leq p^{-3n}\}.$$

Definición E.2. Se define la **filtración p-ádica de** $E^{(1)}(\mathbb{Q})$ como

$$E^{(1)}(\mathbb{Q}) \supset E^{(2)}(\mathbb{Q}) \supset \cdots \supset E^{(n)}(\mathbb{Q}) \supset \cdots .$$

Obsérvese que se tiene que

$$\bigcap_{n=1}^{\infty} E^{(n)}(\mathbb{Q}) = \{[0, 1, 0]\}.$$

ya que, si $\mathbf{x} \in E^{(1)}(\mathbb{Q})$ entonces $\mathbf{x} = [ap^n, b, cp^{3n}]$ con $p \nmid a$ y $p \nmid c$ y, por tanto, $\mathbf{x} \notin E^{(n+1)}(\mathbb{Q})$.

Definición E.3. Decimos que $\mathbf{x} \in E^{(1)}(\mathbb{Q})$ está en el nivel n si $\mathbf{x} \in E^{(n)}(\mathbb{Q}) \backslash E^{(n+1)}(\mathbb{Q})$.

Definición E.4. Para $\mathbf{x} \in E^{(1)}(\mathbb{Q})$ con $\mathbf{x} = [x', 1, z']$ y con coordenada no homogénea, $\mathbf{x}_{noh} = (x, y)$, definimos

$$u(\mathbf{x}) = \begin{cases} x/y & \text{para } \mathbf{x} \neq \mathcal{O}, \\ 0 & \text{para } \mathbf{x} = \mathcal{O}. \end{cases}$$

Esta función está bien definida pues el único punto de $E^{(n)}(\mathbb{Q})$ con $z = 0$ es $\mathcal{O}$. Nótese que, si $|u(\mathbf{x})|_p = p^{-n}$, entonces $\mathbf{x}$ está en el nivel n.

Lema E.5. Sean $\mathbf{x}_1, \mathbf{x}_2 \in E^{(1)}(\mathbb{Q})$. Entonces

$$|u(\mathbf{x}_1 + \mathbf{x}_2) - u(\mathbf{x}_1) - u(\mathbf{x}_2)|_p \leq \text{máx}\{|u(\mathbf{x}_1)|_p^5, |u(\mathbf{x}_2)|_p^5\}.$$

Demostración. En la demostración supondremos que $E^{(1)}(\mathbb{Q})$ es un grupo $\forall p$. Si de $\mathbf{x}_1,\ \mathbf{x}_2$ y $\mathbf{x}_1+\mathbf{x}_2$ alguno es $\mathcal{O}$, la desigualdad se sigue fácilmente. Si ninguno de los tres es $\mathcal{O}$, podemos suponer sin pérdida de generalidad que

$$|u(\mathbf{x}_1)|_p \geq |u(\mathbf{x}_2)|_p.$$

Definimos N como el nivel de $\mathbf{x}_1$. Dado un $\mathbf{x}_i = [p^N x_i, y_i, p^{3N} z_i]$, definimos $\mathbf{x}_{i0} = [x_i, y_i, z_i]$. De esta forma, tenemos definidos $\mathbf{x}_{10},\ \mathbf{x}_{20}$. Como $\mathbf{x}_1$ está en el nivel $N \geq 1$, tenemos que la recta que pasa por ambos, $\mathbf{x}_{10}, \mathbf{x}_{20}$, es de la forma

$$Z = lX + mY$$

con $|l|_p, |m|_p \leq 1$, pues en caso contrario llegaríamos a una contradicción ya que nos daría que $|z_1|_p > 1$. Tenemos así que los puntos $\mathbf{x}_1,\ \mathbf{x}_2$ están en la recta

$$L:\ p^{-3N} Z = lp^{-N} X + mY,$$

de donde deducimos que

$$Z = lp^{2N} X + mp^{3N} Y.$$

Esta interseca con C en: $\mathbf{x}_1,\ \mathbf{x}_2$ y $\mathbf{x}_1+\mathbf{x}_2$. Sustituyendo obtenemos que

$$\begin{aligned} 0 &= -Y^2(lp^{2N}X + mp^{3N}Y) + X^3 + AX(lp^{2N}X + mp^{3N}Y)^2 + B(lp^{2N}X + mp^{3N}Y)^3 \\ &= c_3X^3 + c_2X^2Y + c_1XY^2 + c_0Y^3, \end{aligned}$$

con

$$\begin{aligned} c_3 &= 1 + Al^2p^{4N} + Bl^3p^{6N}, \\ c_2 &= 2Almp^{5N} + 3Bl^2mp^{7N}. \end{aligned}$$

Por lo que tenemos que

$$|c_3|_p = 1 \quad \text{y} \quad |c_2|_p \leq p^{-5n}.$$

Vemos que:

$$\begin{aligned} 0 &= c_3X^3 + c_2X^2Y + c_1XY^2 + c_0Y^3 \\ &= Y^3(c_3\left(\frac{X}{Y}\right)^3 + c_2\left(\frac{X}{Y}\right)^2 + c_1\left(\frac{X}{Y}\right) + c_0). \end{aligned}$$

Las raíces del polinomio $\frac{X}{Y}$, es decir,

$$p(t) = c_3t^3 + c_2t^2 + c_1t + c_0,$$

son $-u(\mathbf{x}_1+\mathbf{x}_2)$, $u(\mathbf{x}_1)$ y $u(\mathbf{x}_2)$ y, por tanto, su suma es igual a $\frac{-c_2}{c_3}$, de donde se deduce la desigualdad que queríamos.
Que $-u(\mathbf{x}_1+\mathbf{x}_2)$ sea raíz se debe a que

1. $u(-\mathbf{x}) = -u(\mathbf{x})$.
2. $\mathbf{x}_1 * \mathbf{x}_2 = -(\mathbf{x}_1+\mathbf{x}_2)$ y, por tanto, $-(\mathbf{x}_1+\mathbf{x}_2)$ para por la recta L.

Recordar que estamos tomando $\mathcal{O} = [0, 1, 0]$. Hemos utilizado que $E^{(1)}(\mathbb{Q})$ es un grupo al suponer que $\mathbf{u}$ está definido sobre $\mathbf{x}_1 + \mathbf{x}_2$. ♮

En la pasada demostración utilizamos que $E^{(1)}(\mathbb{Q})$ es un grupo para todo p, pues $\mathbf{u}$ solo está definida sobre $E^{(1)}(\mathbb{Q})$, por lo que $\mathbf{x}_1 + \mathbf{x}_2$ debe encontrarse en $E^{(1)}(\mathbb{Q})$ para que la demostración sea válida. Sin embargo, esto solo lo hemos demostrado para $p \nmid \Delta$, pues en dicho caso es el núcleo de r_p. Veamos que $E^{(1)}(\mathbb{Q})$ es un grupo $\forall p$. Más aún, que $E^{(n)}(\mathbb{Q})$ es un grupo para todo p.

Teorema E.6. *$E^{(n)}(\mathbb{Q})$ es un grupo $\forall n$ y $\forall p$.*

Demostración. Sea $\mathbf{x}_1,\ \mathbf{x}_2 \in E^{(n)}(\mathbb{Q})$ y $\mathbf{x}_1 * \mathbf{x}_2 = \mathbf{x}_3$, con el nivel de $\mathbf{x}_1$ mayor que el de $\mathbf{x}_2$. Procedemos del mismo modo que en la demostración anterior con,

$$L:\ Z = lp^{2N}X + mp^{3N}Y,$$

la recta que pasa por ambos puntos y $|m|_p,\ |l|_p \leq 1$. Podemos observar que el único punto con $y = 0$ en L es $[1, 0, lp^{2N}]$, pero sustituyendo en E, observamos que dicho punto no se encuentra en la curva. De esta forma, tenemos que $\mathbf{x}_3 = [x_3, 1, z_3]$ y, por tanto,

$$z_3 = lp^{2N}x_3 + mp^{3N}.$$

Tenemos que sustituyendo en E:

$$\begin{aligned} 0 &= -(lp^{2N}x_3 + mp^{3N}) + (x_3)^3 + Ax_3(lp^{2N}x_3 + mp^{3N})^2 + B(lp^{2N}x_3 + mp^{3N})^3 \\ &= c_3(x_3)^3 + c_2(x_3)^2 + c_1x_3 + c_0, \end{aligned}$$

con

$$\begin{aligned} c_3 &= 1 + Al^2p^{4N} + Bl^3p^{6N}, \\ c_2 &= 2Almp^{5N} + 3Bl^2mp^{7N}. \end{aligned}$$

Por lo que tenemos que

$$|c_3|_p = 1 \quad \text{y} \quad |c_2|_p \leq p^{-5N}.$$

Pero tenemos que las raíces del polinomio son x_1, x_2 y x_3 y, por tanto, su suma es igual a $\frac{-c_2}{c_3}$. Deducimos así que, $|x_3|_p \leq 1/p^{-N}$. Por lo que

$$|z_3|_p = |lp^{2N}x_3 + mp^{3N}|_p \leq p^{-3N},$$

y así $\mathbf{x}_3 \in E^{(n)}(\mathbb{Q})$.

Esto último es de suma importancia pues observamos que esto implica que si $\mathbf{x}_1,\ \mathbf{x}_2 \in E^{(n)}(\mathbb{Q}) \Rightarrow \mathbf{x}_3 = \mathbf{x}_1 * \mathbf{x}_2 \in E^{(n)}(\mathbb{Q})$ y como $\mathcal{O} \in E^{(n)}(\mathbb{Q})$, tenemos que $\mathbf{x}_2 + \mathbf{x}_1 = \mathbf{x}_3 * \mathcal{O} \in E^{(n)}(\mathbb{Q})$. Es decir, $E^{(n)}(\mathbb{Q})$ es un grupo para todo p primo y no solo para los p tal que $p \nmid \Delta$. ♮

Corolario E.7.

$$|u(s\mathbf{x})|_p = |s|_p|u(\mathbf{x})|_p$$

para todo $\mathbf{x} \in E^{(1)}(\mathbb{Q})$ y todo $s \in \mathbb{Z}$.

Demostración. Por inducción, para $s > 0$ tenemos

$$|u(s\mathbf{x}) - su(\mathbf{x})|_p \leq |u(\mathbf{x})|_p^5.$$

Procedamos por reducción al absurdo. Si la igualdad no fuera cierta, entonces el lado izquierdo de la desigualdad sería igual al máx$\{|u(s\mathbf{x})|_p, |su(\mathbf{x})|_p\}$. Obtendríamos así que

$$|s|_p|u(\mathbf{x})|_p \leq |u(\mathbf{x})|_p^5.$$

Pero tenemos que $|u(\mathbf{x})|_p < 1$, por lo que si $|s|_p \geq 1$ tendríamos una contradicción. Tenemos, por tanto, probado el caso en el que $p \nmid s$ y el caso $s = p$. Procedamos ahora por inducción sobre las potencias de p, ie, $s = p^n$. Para $n = 1$ ya lo tenemos, veamos que suponiendo que se cumple para n, entonces lo hace para $n + 1$.

$$\begin{aligned} |u(p^{n+1}\mathbf{x})|_p &= |u(p^n(p\mathbf{x}))|_p \\ &= |p^n|_p|u(p\mathbf{x})|_p \\ &= |p^n|_p|p|_p|u(\mathbf{x})|_p = |p^{n+1}|_p|u(\mathbf{x})|_p. \end{aligned}$$

Por último, sea $s = p^s k$ con $p \nmid k$ entonces:

$$\begin{aligned} |u(kp^s\mathbf{x})|_p &= |u(p^s(k\mathbf{x}))|_p \\ &= |p^s|_p|u(k\mathbf{x})|_p = |p^s|_p|k|_p|u(\mathbf{x})|_p = |p^s k|_p|u(\mathbf{x})|_p. \end{aligned}$$

♮

Corolario E.8. *$E^{(1)}(\mathbb{Q})$ es libre de torsión $\forall p$.*

Demostración. Si $\mathbf{x} \in E^{(1)}(\mathbb{Q})$ es de orden k, entonces

$$0 = |u(\mathcal{O})|_p = |u(k\mathbf{x})|_p = |k|_p|u(\mathbf{x})|_p.$$

Luego $u(\mathbf{x}) = 0 \Rightarrow x = 0$, pero tenemos que $\mathbf{x} \in E^{(1)}(\mathbb{Q})$, por lo que $y \neq 0 \Rightarrow z = 0$. Por tanto, $\mathbf{x} = \mathcal{O}$. ♮

Demostración del Teorema 4.6. Recordemos que teníamos que cuando $p \nmid \Delta$

$$\ker(r_p) = E^{(1)}(\mathbb{Q}).$$

Además, por el corolario E.8,

$$E(\mathbb{Q})_{tors} \cap E^{(1)}(\mathbb{Q}) = \mathcal{O},$$

por lo que la restricción $r_p|_{E(\mathbb{Q})_{tors}}$ es inyectiva. ♮

E.2. Demostración: Teorema de Nagell-Lutz.

Demostración.

1. Si $y(P) = 0$, ya lo tenemos. Supongamos que $y(P) \neq 0$. Entonces podemos poner $[x(P), y(P), 1] = [x, 1, z]$ con $x = \frac{x(P)}{y(P)}$ y $z = \frac{1}{y(P)}$. Fijado un p primo, tenemos que $E^{(1)}(\mathbb{Q})$ está libre de torsión por lo que $|z|_p \geq 1$, y así tenemos que

$$|y|_p = \frac{1}{|z|_p} \leq 1.$$

   Como esto es para todo primo, tenemos que $y \in \mathbb{Z}$.

   Si sustituimos $y(P) \in \mathbb{Z}$ en

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

   obtenemos que $x(P)$ es solución de una ecuación cúbica que tiene coeficientes enteros y es mónica, en consecuencia, $x(P)$ es entero.

2. Sea $P = (x, y) \in E(\mathbb{Q})$, tenemos que la fórmula del doble de un punto P, es:

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

   Si llamamos $\chi(x) = x^4 - 2Ax^2 - 8Bx + A^2$ y $\gamma(x) = x^3 + Ax + B = y^2$, tenemos que

$$\chi(x) = 4y^2 x(2P).$$

   Por el apartado anterior $x, x(2P)$ e $y^2 \in \mathbb{Z}$, por lo que $\chi(x) \in \mathbb{Z}$ y $y^2 | \chi(x)$. Deducimos entonces que

$$y^2 | \chi(x) \quad \text{e} \quad y^2 | \gamma(x).$$

   Haciendo ciertos cálculos llegamos a que

$$(3x^2 + 4A)\chi(x) - (3x^3 - 5Ax - 27B)\gamma(x) = 4A^3 + 27B^2,$$

   y como $y^2 | \chi(x)$ e $y^2 | \gamma(x)$, nos queda que

$$y^2 | 4A^3 + 27B^2.$$

Queda así demostrado el Teorema de Nagell-Lutz. ♮

E.3. Demostración: Teorema 4.7.

Para una introducción a la teoría algebraica de número consultar [10].

Lema E.9. Sea E_p la reducción de la curva $y^2 = x^3 + Ax$ sobre $\mathbb{F}_p$. Si $p \nmid \Delta = 4A^3$, $p \geq 7$ y $p \equiv 3 (\text{mod } 4)$. Entonces

$$|E_p(\mathbb{F}_p)|_p = p + 1.$$

Demostración. Sea p un primo $p \neq 2$, se define como **símbolo de Legendre**

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \equiv 0(\text{mod } p), \\ 1 & \text{si } \exists b \text{ tal que } a \equiv b^2(\text{mod } p), \\ -1 & \text{si } \nexists b \text{ tal que } a \equiv b^2(\text{mod } p). \end{cases}$$

Diremos que $a \in \boxed{\mathbb{F}_p}$ si $\left(\frac{a}{p}\right) = 1$. Además este símbolo cumple que

$$\left(\frac{m \cdot n}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Otra propiedad que posee es que

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1(\text{mod } 4). \\ 1 & \text{si } p \equiv 3(\text{mod } 4). \end{cases}$$

Dado $Q \in \mathbb{F}_p$, si

$$\left(\frac{Q}{p}\right) = 1 \text{ entonces } \left(\frac{-Q}{p}\right) = -1 \text{ y viceversa, pues } \left(\frac{-1}{p}\right) = -1.$$

Por lo que para un par $\{a, -a\}$ con $a \in \mathbb{F}_p$ y $Q = a^3 + Aa$, tenemos que si:

1. $Q \in \boxed{\mathbb{F}_p} \Rightarrow$ del par $\{a, -a\}$ obtenemos dos y solo dos puntos de las ecuación: $(a, \sqrt{Q})$ y $(a, -\sqrt{Q})$.
2. $Q \notin \boxed{\mathbb{F}_p} \Rightarrow -Q \in \boxed{\mathbb{F}_p} \Rightarrow$ del par $\{a, -a\}$ obtenemos dos y solo dos puntos de la ecuación: $(-a, \sqrt{-Q})$ y $(-a, -\sqrt{-Q})$.

Tenemos así que para cada par $\{a, -a\}$ le corresponde dos puntos de $E_p(\mathbb{F}_p)$. Para $x = 0$ obtenemos el punto $(0, 0)$ y también tenemos el punto $\mathcal{O}_p$. Sumando todo tenemos que:

$$|E_p(\mathbb{F}_p)| = p + 1.$$

∎

Observación: La certeza de la existencia de primos p, durante la demostración, que cumplan ciertas congruencias y que pueden ser arbitrariamente grandes (de forma que $p \nmid \Delta$), viene dada por el teorema de Dirichlet de primos en progresión aritmética. Los siguientes p primos de los que hablamos cumplen, además de otras exigencias, que $p \equiv 3 \mod 4$.

Demostración del Teorema 4.7. Veamos que 8 no divide a $|E(\mathbb{Q})_{tors}|$. Tenemos que podemos elegir p tal que $p \equiv 3(\text{mod } 8)$ y no divida a Δ. Si 8 dividise a $|E(\mathbb{Q})_{tors}|$, entonces 8|(p+1), pues $|E(\mathbb{Q})_{tors}||(p+1)$. Sin embargo, como $p \equiv 3(\text{mod } 8)$, tenemos que $p + 1 \equiv 4(\text{mod } 8)$, lo que es una contradicción.

Veamos que 3 no divide a $|E(\mathbb{Q})_{tors}|$. Podemos elegir un primo p tal que $p \equiv 7(\text{mod } 1)2$. Entonces $p \equiv 3(\text{mod } 4)$. Si 3 divide a $|E(\mathbb{Q})_{tors}|$, entonces $3|(p+1)$. Por otro lado $p+1 \equiv 8(\text{mod } 12)$ implica que $p+1 \equiv 2(\text{mod } 3)$, lo que es una contradicción.

Por último veamos que ningún primo $q > 3$ divide a $|E(\mathbb{Q})_{tors}|$. Nuevamente podemos elegir un primo p tal que $p \equiv 3(\text{mod } 4) q \Rightarrow p \equiv 3(\text{mod } 4)$. Si q divide a $|E(\mathbb{Q})_{tors}|$, entonces divide a $p+1$. Pero por la primera congruencia tenemos que $p+1 \equiv 4(\text{mod } 4)$ y, por lo tando, $q \nmid (p+1)$. Contradicción.

Es decir, tenemos que $|E(\mathbb{Q})_{tors}| = 1,\ 2$ ó 4. Pero tenemos que $\{(0,0), \mathcal{O}_p\} = \mathbb{Z}/2\mathbb{Z}$ como subgrupo de $E(\mathbb{Q})_{tors}$. Además observamos que

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \Leftrightarrow x^3 + Ax = x(x^2 + A)$$

se puede descomponer en monomios sobre $\mathbb{Q}$, es decir, si y lo si $\sqrt{-A} \in \mathbb{N}$.

Veamos si $(0,0)$ es el doble de un punto o no, para ver si estamos en el caso $\mathbb{Z}/2\mathbb{Z}$ o en el caso $\mathbb{Z}/4\mathbb{Z}$, respectivamente. Para $A = 4$ vemos que $[2](2,4) = (0,0)$, es decir, que estamos en el caso $\mathbb{Z}/4\mathbb{Z}$. Veamos si hay otros A para los que se cumpla que $(0,0) = 2(x,y)$ con $x \neq 0$. Para el punto doble tenemos que

$$0 = x^4 - 2Ax^2 + A^2 = (x^2 - A)^2.$$

O sea que $x^2 = A$, pero como A es libre de potencias cuartas entonces x está libre de cuadrados. Pero tenemos que $y^2 = x(x^2 + A) = 2x^3$, por lo que no puede haber un primo $p \neq 2$ que divida a x. Tenemos así que solo nos quedan cuatro posiblidades: $x = \pm 1$ y $x = \pm 2$. Y calculando vemos que $x = \pm 2$ y $A = 4$. ♮

Bibliografía

[1] A. Beshenov. *Introducción a los números p-ádicos*. Universidad de El Salvador, 2018. URL: http://cadadr.org/san-salvador/2018-04-numeros-p-adicos/numeros-p-adicos.pdf.

[2] J.W.S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[3] W. Fulton. *Algebraic curves: an introduction to algebraic geometry*. Addison-Wesley, 1989.

[4] E. González Jiménez. *Curvas Elípticas: Grupo de puntos racionales y curvas de rango alto*. (Tesis de Licenciatura). Universidad Autonoma de Madrid, 1998. URL: https://verso.mat.uam.es/~enrique.gonzalez.jimenez/research/papers/00_tesina.pdf.

[5] F.C. Kirwan. *Complex Algebraic Curves*. Cambridge University Press, 1992.

[6] A.W. Knapp. *Elliptic Curves*. Princeton University Press, 1992.

[7] M. N. Lalín. *Introducción a las Curvas Elípticas*. (Tesis de Licenciatura). Universidad de Buenos Aires, 1999. URL: https://dms.umontreal.ca/~mlalin/tesis.pdf.

[8] Joan-C. Lario. "Al-Karají y yo". En: *Gac. R. Soc. Mat. Esp* 19.1 (2016), págs. 133-149. URL: http://gaceta.rsme.es/english/abrir.php?id=1310.

[9] T. Ochiai. "New generalizations of congruent numbers". En: *Journal of Number Theory* 193 (2018), págs. 154-170.

[10] P. Samuel. *Teoria algebraica de numeros*. Ediciones Omega, 1972.

[11] J.H. Silverman y John T. Tate. *Rational Points on Elliptic Curves*. Springer International Publishing, 2015.

[12] Y. Tian. "Congruent numbers and Heegner points". En: *Cambridge Journal of Mathematics* 2.1 (2014), págs. 117-161.

[13] F. Zaldívar. *Del teorema de Pitágoras a la aritmética de curvas elípticas*. Universidad Autónoma Metropolitana-I, 2018. URL: http://miscelaneamatematica.org/Misc42/F_Zaldivar.pdf.