FACULTAD DE MATEMÁTICAS
DEPARTAMENTO DE ÁLGEBRA

Curvas Elípticas y el Teorema de Mordell

Jesús Navas Orozco

Memoria presentada como parte de los requisitos para la obtención del título de Grado en Matemáticas por la Universidad de Sevilla.

Prof. tutor: D. Luis Narváez Macarro

Índice

Abstract

Eliptic curves are mathematical objects that have interesting analytic, arithmetic and algebraic properties, though we'll focus on the algebraic and arithmetic aspects only. We can define a natural geometric group law on them. Mordell's theorem states that the subgroup of points with rational coordinates of and elliptic curve defined over $\mathbb{Q}$ is abelian and finitely generated and it's usually a good first objective in the study of these curves. The proof is not elementary and eventually, we'll need to use some tools of algebraic number theory.

Lista de símbolos

$\mathbb{N}$	Conjunto de los números naturales
$\mathbb{Z}$	Anillo de los números enteros
$\mathbb{Q}$	Cuerpo de los números racionales
$\mathbb{R}$	Cuerpo de los números reales
$\mathbb{C}$	Cuerpo de los números complejos
$\overline{\mathbb{Q}}$	Clausura algeraica de $\mathbb{Q}$
$\mathrm{mcd}(a, b)$	Máximo común divisor de a y b
$\mathrm{mcm}(a, b)$	Mínimo común múltiplo de a y b
$R^\times$	Grupo (multiplicativo) de las unidades del anillo R
$\mathbb{F}_q$	Cuerpo finito de q elementos
$\mathbb{Z}/n\mathbb{Z}$	Anillo de los enteros módulo n
$(E, \mathcal{O}, +)$	Grupo formado por la curva elíptica E con elemento neutro $\mathcal{O}$ y operación de grupo $+$

0 Introducción

Teorema 0.1. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces los puntos racionales, $E(\mathbb{Q})$, forman un subgrupo de E finitamente generado.*

Así reza el Teorema de Mordell, cuya prueba será el objetivo principal de este trabajo. De su enunciado podemos deducir algunas cosas. Primero la aparición de curvas elípticas. Son los objetos matemáticos que estaremos estudiando. En la sección 2 las definiremos adecuadamente, pero *grosso modo* son curvas planas (variedades algebraicas de dimensión 1) de grado 3 y género 1. Sobre un cuerpo de característica 0 como $\mathbb{Q}$, que es el caso que nos competerá, siempre tienen una ecuación de la forma:

$$E : y^2 = f(x) := x^3 + ax + b, \quad a, b \in \mathbb{Q}$$

con $f(x)$ separable para que la curva sea no singular (luego explicaremos por qué es así). Aunque la ecuación es afín, debemos ver la curva en el proyectivo (homogeneizándola). A modo de ejemplo, en la Figura 1 representamos el *locus* real de una de estas curvas.

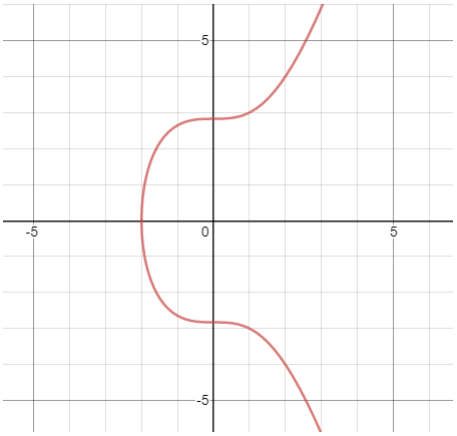

Figura 1: Curva elíptica $y^2 = x^3 + 8$

También podemos apreciar en dicho enunciado que hablamos de los puntos de la curva E como si fuesen un grupo. Como veremos en la Sección 3, podemos definir de manera sencilla una operación que dotará a los puntos de E de estructura de grupo abeliano. Este hecho es una de las propiedades más interesantes que tienen las curvas elípticas, que nos permite darles a la vez un tratamiento geométrico y algebraico. En general, las variedades algebraicas proyectivas que cumplan

- Sus puntos forman un grupo abeliano.

- Las operaciones de grupo sean compatibles con la estructura de variedad, es decir, son morfismos de variedades algebraicas.

se denominan variedades abelianas, de las cuales las curvas elípticas suponen el ejemplo más sencillo. Para variedades abelianas se da la siguiente generalización del Teorema 0.1:

Teorema 0.2. *(Teorema de Mordell-Weil) Sea A una variedad abeliana sobre un cuerpo numérico K. Entonces el grupo $A(K)$ de puntos K-racionales de A es un grupo abeliano finitamente generado.*

El caso que nos compete y objetivo de este trabajo se da cuando A es una curva elíptica y $K = \mathbb{Q}$. Fue conjeturado por Poincaré en 1901 y demostrado por Mordell en 1922, lo que le dió el nombre de Teorema de Mordell. Fue Weil el que varios años después generalizó el resultado a variedades abelianas de mayor género que proceden de variedades Jacobianas, acercándose así más al Teorema 0.2, resultado que acabó probando en 1929. A veces al Teorema de Mordell se le llama Teorema de Mordell-Weil sobre $\mathbb{Q}$, manifestando así que uno es un caso particular del otro, pero en ambos la prueba siempre pasa por el mismo camino que tomaremos nosotros para demostrar (0.1), aunque usando otras herramientas: se prueba una versión débil del teorema, que nos dice que el grupo $E(\mathbb{Q})/mE(\mathbb{Q})$ es finito (donde $mE(\mathbb{Q})$ son los puntos de $E(\mathbb{Q})$ que son la suma de m veces otros puntos de $E(\mathbb{Q})$) y después se usan funciones altura y un argumento de descenso para llegar al resultado.

Cabe remarcar que las curvas elípticas no son elipses. Estas son cónicas mientras que las curvas elípticas vienen dadas por polinomios cúbicos. Su nombre proviene de ciertas integrales (integrales elípticas) involucradas en el cálculo de la longitud de arco de las elipses. En estas integrales aparecían raíces cuadradas de polinomio de grado 3 o 4 en x.

Las curvas elípticas han suscitado interés a los matemáticos desde hace cientos de años, conociéndose su estructura de grupo desde el siglo XVII. Pero eso no ha causado que su interés haya decaído con el tiempo. Estas curvas, y en especial sus puntos racionales, han sido y siguen siendo de mucha utilidad en el estudio de ecuaciones diofánticas y teoría de números, llegando incluso a jugar un papel clave en la demostración de Andrew Wiles del *Último Teorema de Fermat*. Hoy día las curvas elípticas han encontrado un hueco en la criptografía, aunque definidas sobre cuerpos finitos, $\mathbb{F}_q$. En este caso el grupo $E(\mathbb{F}_q)$ de puntos de la curva con coordenadas en $\mathbb{F}_q$ es finito, y resolver el problema del logaritmo discreto en él se considera más difícil que sobre cuerpos finitos, permitiendo claves más cortas, mientras que mantiene un nivel de seguridad comparable al de los métodos más usados actualmente, como el RSA.

La organización del trabajo tiene la intención de ser lo más clara posible y siempre con el propósito de probar el Teorema de Mordell. En la primera sección introducimos las herramientas de Álgebra y Teoría Algebraica de Números que nos harán falta para la prueba, usando como fuente principalmente los dos libros clásicos: [6, *A Classical Introduction to Modern Number Theory*], de Kenneth Ireland y Michael Rosen, y [7, *Commutative Algebra*], de Oscar Zariski y Pierre Samuel. La mayoría de estos resultados tienen pruebas sencillas y se pueden encontrar en cualquier libro de Álgebra Conmutativa. Aún así, omitiremos sus pruebas como norma general, dando la referencia adecuada en cada caso, pues probarlos no es el objetivo de este trabajo. Solo demostraremos aquellos resultados que se puedan deducir inmediatamente de los que ya hayamos enunciado.

En las secciones 2 y 3 definimos las curvas elípticas, su ley grupo, damos fórmulas explícitas para la suma y duplicación de puntos y hablamos de los puntos de torsión y otras propiedades útiles sobre dichas curvas. Para estas dos secciones he usado principalmente los libros, [1, *Rational Points on Elliptic Curves*] y[] [2, *The Arithmetic of Elliptic Curves*], ambos de J.H. Silverman, que son la principal referencia en libros sobre curvas elípticas. El segundo es de una complejidad y generalidad considerablemente superiores al primero, pero ambos nos aportan buenas herramientas y conocimientos sobre las curvas elípticas. También se ha usado en menor medida el artículo [5], principalmente como guía debido a lo condensada que está su presentación.

La parte final, en la que probamos el Teorema de Mordell, consta de dos partes. La primera, sobre funciones alturas y el argumento de descenso, están basadas principalmente en el capítulo 2 de [1, Rational Points on Elliptic Curves], mientras que la versión débil del Teorema de Mordell, que supone la parte central de la prueba, ha sido extraída del capítulo 19 del libro [6, *A Classical Introduction to Modern Number Theory*]. Tal y como dicen los autores al comienzo de dicho capítulo, su exposición está basada en el paper de Cassel titulado [8, *The Mordell-Weil Group of Curves of Genus 2*], que expone una interesente simplificación del "Weak Mordell-Weil", presentado por Weil en su artículo de 1929 llamado "*Sur un théorème de Mordell*".

1 Preliminares de Teoría Algebraica de Números

En esta sección se enunciarán y expondrán algunos conceptos y resultados de álgebra y teoría algebraica de números que usaremos en las últimas secciones. Otros resultados más sencillos y conocidos, o que han sido estudiados a lo largo del Grado en Matemáticas, se omitirán y solo serán nombrados cuando sean usados.

A lo largo de este trabajo, como es usual en álgebra conmutativa, cuando hablamos de un anillo nos referimos a un anillo conmutativo y con elemento unidad.

Definición 1.1. *Un cuerpo numérico K es una extensión finita (y por tanto algebraica) de $\mathbb{Q}$.*

Es decir, es un cuerpo K que contenga una copia de $\mathbb{Q}$ (un subcuerpo isomorfo a $\mathbb{Q}$), y que además tenga dimensión finita como $\mathbb{Q}$-espacio vectorial.

Hablemos ahora de los ideales fraccionarios en cuerpos numéricos.

Definición 1.2. *Sea R un dominio de integridad y sea K su cuerpo de fracciones. Un ideal fraccionario de R es un R-submódulo I de K tal que existe un elemento no nulo $r \in R$ tal que $rI \subset R$.*

Un ideal principal fraccionario es un ideal fraccionario generado por un elemento no nulo de K.

Debemos pensar en el elemento r de la definición anterior como una forma de limpiar los denominadores del ideal fraccionario I, o como un común denominador de los elementos del mismo, es decir $I \subset (1/r)R$. Más concretamente $I = (1/r)\mathfrak{a}$ donde $\mathfrak{a}$ es un ideal ordinario de R. Los ideales ordinarios de R, que son un caso especial de los fraccionarios ($r = 1$), suelen llamarse ideales enteros en este contexto.

Observación 1.3. *Recordando que los R-submódulos de R son sus ideales, es inmediato que un ideal fraccionario de R está contenido en R si y solo si es un ideal de R.*

Definición 1.4. *Sea R un dominio de integridad. Un ideal fraccionario I de R de dice invertible si existe otro ideal fraccionario J tal que $IJ = R$.*

Proposición 1.5. *Sea K el cuerpo de fracciones del dominio R, y sea I un ideal fraccionario invertible. Entonces el ideal inverso J de la definición anterior está unívocamente determinado y es igual al ideal cociente:*

$$(R : I) = \{x \in K : xI \subseteq R\}$$

Demostración. [7, Ch. V, §6, Lemma 1] □

Observación 1.6. *Los ideales fraccionarios principales son de la forma* $xR = \{xy \mid y \in R\}$ *para* $x \in K, x \neq 0$. *Son invertibles y su inverso es el ideal principal fraccionario* $x^{-1}R$.

Esto nos dice los ideales fraccionarios principales forman un grupo para la multiplicación de ideales. De la Definición 1.2 es fácil ver que el producto de ideales fraccionarios es un ideal fraccionario y por tanto tenemos lo siguiente:

Observación 1.7. *Sea* R *un dominio de integridad. Sea* $\mathcal{F}$ *el conjunto de todos los ideales fraccionarios no nulos de* R. *Entonces el subconjunto de los ideales fraccionarios invertibles es un grupo para la multiplicación de ideales y los ideales fraccionarios principales forman un subgrupo.*

Observación 1.8. *Con la notación anterior, si* $(x)R = (x) \subset R$ *es un ideal principal no nulo de* R, *i.e.* $x \in R \setminus \{0\}$, *aunque su inverso es* $(x^{-1})R$, *este no es en general un ideal principal pues* x *no tiene por qué ser invertible en* R, *sino que en general se tiene* $x^{-1} \in K$, *el cuerpo de fracciones de* R *y por tanto* $(x^{-1})R$ *es un ideal fraccionario no necesariamente entero. Es decir, el inverso de un ideal (entero) principal puede ser un ideal fraccionario no entero.*

Ahora hablaremos sobre el anillo de enteros de un dominio de integridad.

Definición 1.9. *Un entero algebraico es un elemento de* $\mathbb{C}$ *que sea raíz de un polinomio mónico con coeficientes en* $\mathbb{Z}$.

Proposición 1.10. *El subconjunto de* $\mathbb{C}$ *formado por todos los enteros algebraicos es un subanillo de* $\mathbb{C}$. *Es la clausura íntegra de* $\mathbb{Z}$ *en* $\mathbb{C}$.

Demostración. Sean B un anillo y A un subanillo de B. Entonces la clausura íntegra de A en B es un subanillo de B que contiene a A. Una prueba de este hecho, que contempla el caso que queremos probar, se puede encontrar en [3, Ch. 5, §Corolario 5.3]. □

Definición 1.11. *Dado un cuerpo numérico* K, *denotamos por* $\mathcal{O}_K$ *su anillo de enteros, es decir los elementos de* K *que son enteros sobre* $\mathbb{Z}$.

Observación 1.12. $\mathcal{O}_K$ *no es más que la clausura íntegra de* $\mathbb{Z}$ *sobre* K *(elementos de* K *enteros sobre* $\mathbb{Z}$*), y obviamente es la intersección de* K *y el subconjunto de* $\mathbb{C}$ *formado por todos los enteros algebraicos.*

Observación 1.13. *Para cualquier cuerpo numérico* K, *el anillo de enteros* $\mathcal{O}_K$ *contiene a* $\mathbb{Z}$, *ya que* $\mathbb{Z}$ *es entero sobre* $\mathbb{Q}$ *y por tanto sobre* $K \supset \mathbb{Q}$. *Hay un par de casos que merece la pena destacar.*

- *Cuando $K = \mathbb{Q}$, entonces $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Para probarlo, notemos que como $\mathbb{Q}$ es el cuerpo de fracciones de $\mathbb{Z}$, nuestra afirmación es equivalente a decir que $\mathbb{Z}$ es íntegramente cerrado. Si el número racional r/s, con r y s coprimos, es entero sobre $\mathbb{Z}$, entonces debe cumplir una ecuación de la forma:*

$$(r/s)^n + a_1(r/s)^{n-1} + ... + a_n = 0, \quad a_i \in \mathbb{Z}$$

y multiplicando por s^n obtenemos:

$$r^n + a_1 r^{n-1} s + ... + a_n s^n = 0$$

luego s divide a r^n y por tanto $s = \pm 1$. Es decir, r/s es un número entero.

- *Cuando $K = \mathbb{Q}(\theta)$, siendo θ la raíz de un polinomio mónico irreducible de $\mathbb{Z}[x]$, entonces $\mathbb{Z}[\theta] \subset \mathcal{O}_K$. Esto es debido a que $\mathbb{Z} \subset \mathcal{O}_K, \theta \in \mathcal{O}_K$ y por ser $\mathbb{Z}[\theta]$ el menor anillo que contiene a $\mathbb{Z}$ y a θ se debe tener $\mathbb{Z}[\theta] \subset \mathcal{O}_K$.*

El siguiente resultado establece una relación entre el cuerpo de fracciones y el anillo de enteros de un cuerpo numérico, que es análoga a la de $\mathbb{Q}$ y $\mathbb{Z}$.

Proposición 1.14. *Sea K un cuerpo numérico y $\mathcal{O}_K$ su anillo de enteros. Entonces el cuerpo de fracciones de $\mathcal{O}_K$ es exactamente K.*

Demostración. Denotemos por $\mathcal{Q}(\mathcal{O}_K)$ el cuerpo de fracciones de $\mathcal{O}_K$. La inclusión $\mathcal{Q}(\mathcal{O}_K) \subset K$ es obvia pues $\mathcal{O}_K \subset K$ y $\mathcal{Q}(\mathcal{O}_K)$ es el menor cuerpo que contiene a $\mathcal{O}_K$.

Sea ahora $b \in K$. Como todo elemento de K es algebraico sobre $\mathbb{Q}$, b satisface un polinomio con coeficientes en $\mathbb{Q}$. Tras eliminar los denominadores obtenemos que b cumple el siguiente polinomio (no necesariamente mónico) con coeficientes en $\mathbb{Z}$:

$$a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0 = 0 \quad \text{donde } a_i \in \mathbb{Z}, a_n \neq 0$$

Multiplicando por a_n^{n-1} obtenemos:

$$(a_n b)^n + a_{n-1} (a_n b)^{n-1} + \cdots + a_1 a_n^{n-2} (a_n b) + a_n^{n-1} a_0 = 0$$

Es decir $a_n b \in K$ es raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$, luego $a_n b \in \mathcal{O}_K$. Como $0 \neq a_n \in \mathbb{Z} \subset \mathcal{O}_K$ y $b = \dfrac{a_n b}{a_n}$ se tiene $b \in \mathcal{Q}(\mathcal{O}_K)$. □

Hablamos ahora un poco de dominios de Dedekind.

Definición 1.15. *Un dominio de Dedekind es un dominio de integridad en el que todo ideal se puede expresar como producto de ideales primos.*

Proposición 1.16. *La factorización de ideales primos en un dominio de Dedekind es única.*

Demostración. [7, Ch. V, §6, Lemma 5 and Theorem 10] □

Definición 1.17. *Sea R un dominio de Dedekind e I, J dos ideales. Decimos que I divide a J si $J \subset I$.*

Corolario 1.18. *Sea R un dominio de Dedekind. Entonces todo ideal no nulo de R tiene un número finito de divisores.*

Demostración. La prueba es una consecuencia inmediata de la Proposición 1.16, con una analogía completa al caso de los números enteros y su factorización en primos (de hecho los enteros son un caso particular de dominio de Dedekind). Todo ideal I de R se puede escribir de la forma:

$$I = \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}...\mathfrak{p}_\mathfrak{n}{}^{\alpha_n}$$

para únicos $n, \alpha_1, ..., \alpha_n \in \mathbb{N}$ y donde los $\mathfrak{p}_i$ son ideales primos de R. Entonces todo divisor de I es de la forma:

$$\mathfrak{p}_{i_1}^{\beta_1}\mathfrak{p}_{i_2}^{\beta_2}...\mathfrak{p}_{\mathfrak{i}_\mathfrak{r}}{}^{\beta_r} \supset I$$

donde $r \leq n, i_j \in \{1, ..., n\}$ y $\beta_j \in \left\{0, ..., \alpha_{i_j}\right\}, j = 1, .., r$ y por tanto solo hay una cantidad finita. En concreto hay $\prod_{i=1}^{n}(\alpha_i + 1)$ divisores de I. □

A continuación damos una serie de caracterizaciones de los dominios de Dedekind.

Proposición 1.19. *Sea R un dominio de integridad. Las siguientes condiciones son equivalentes:*

1. *R es un dominio de Dedekind.*
2. *R es noetheriano, todo ideal (entero) primo no nulo de R es maximal y además R es íntegramente cerrado.*
3. *El conjunto $\mathcal{F}$ de ideales fraccionarios no nulos de R es un grupo para la multiplicación de ideales, es decir, todo ideal fraccionario no nulo es invertible.*

Demostración. [7, Ch. V, §6 Theorems 12 and 13] □

De cara a probar que $\mathcal{O}_K$ es un dominio de Dedekind, veamos el siguiente resultado.

Proposición 1.20. *Sea R un dominio de Dedekind, k su cuerpo de fracciones y L una extensión algebraica finita de k. Entonces la clausura íntegra R' de R en L es un dominio de Dedekind.*

Demostración. [7, Ch. V, §8, Theorem 19] □

Como consecuencia tenemos el siguiente resultado

Corolario 1.21. *Sea K un cuerpo numérico y $\mathcal{O}_K$ su anillo de enteros. Entonces $\mathcal{O}_K$ es un dominio de Dedekind.*

Demostración. Primero observemos que $\mathbb{Z}$ es un dominio de Dedekind. Por ser $\mathbb{Z}$ un dominio de ideales principales, dado I ideal no nulo[1] de $\mathbb{Z}$, existe un entero positivo m tal que $I = (m)$. Si $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ es una descomposición de m como producto de primos, entonces $I = (p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}) = (p_1)^{\alpha_1}(p_2)^{\alpha_2} ... (p_r)^{\alpha_r}$. Es decir, hemos visto que todo ideal no nulo se descompone como producto de ideales primos, luego $\mathbb{Z}$ es un dominio de Dedekind.

Ahora aplicamos el Teorema 1.20 a $R = \mathbb{Z}$, $k = \mathbb{Q}$ y $L = K$ (nuestro cuerpo numérico). Por definición K es una extensión algebraica finita de $\mathbb{Q}$, así que el Teorema 1.20 nos dice que la clausura íntegra de $\mathbb{Z}$ en K es un dominio de Dedekind, pero esta clausura íntegra no es más que $\mathcal{O}_K$, luego hemos terminado. □

Corolario 1.22. *Sea K un cuerpo numérico. Entonces todo ideal fraccionario de $\mathcal{O}_K$ es invertible.*

Demostración. Consecuencia de la Proposición 1.19 y el Corolario 1.21. □

Ahora introducimos la noción de *grupo de clases de ideales*.

Definición 1.23. *Sea R un dominio de integridad. Definimos la siguiente relación en el conjunto $\mathcal{F}$ de ideales fraccionarios no nulos de R:*

$$I \sim J \text{ si existen } a, b \in R \text{ no nulos tales que } (a)I = (b)J.$$

Proposición 1.24. *La relación $\sim$ de la Definición 1.23 es de equivalencia.*

Demostración. Reflexiva. para todo ideal fraccionario I se tiene $RI = RI = I$, y $R = (1)$ es principal.

Simétrica. Trivial

Transitiva Si $I_1 \sim I_2$ e $I_2 \sim I_3$, existen a, b, a', b' no nulos tales que $(a)I_1 = (b)I_2$ y $(a')I_2 = (b')I_3$. Entonces se tiene:

$$(aa')I_1 = (a')(a)I_1 = (a')(b)I_2 = (b)(b')I_3 = (bb')I_3$$

y la prueba concluye pues $aa', bb' \neq 0$ por ser R un dominio de integridad. □

[1] El caso $I = (0)$ es trivial ya que (0) es siempre un ideal primo cuando estamos en un dominio de integridad.

Observación 1.25. *1. Las clases de equivalencia por esta relación se denominan clases de ideales de R. La multiplicación de clases $[I][J] = [IJ]$ está bien definida y es conmutativa por serlo el anillo R. Los ideales principales forman la clase $[R]$ que es la identidad para la multiplicación.*

2. Cuando R es $\mathcal{O}_K$, el anillo de enteros de un cuerpo numérico K, como todos los ideales fraccionarios son invertibles, una forma equivalente de definir el grupo de clases de ideales es con el cociente de grupos: $\mathcal{F}/\mathcal{P}$ donde $\mathcal{F}$ es el grupo formado por todos los ideales fraccionarios no nulos de $\mathcal{O}_K$ y $\mathcal{P}$ el subgrupo de los ideales fraccionarios principales.

A continuación enunciaremos un resultado muy importante en la teoría algebraica de números.

Teorema 1.26. *(Finitud del número de clase). Sea K un cuerpo numérico. Entonces el orden de $\mathcal{F}/\mathcal{P}$, el grupo de clases de ideales de $\mathcal{O}_K$, es finito. Es decir hay una cantidad finita de clases de equivalencia. A este número se le llama* ***número de clase****.*

Demostración. [6, Ch. 12, §2, Theorem 1] □

Ahora vamos a ver el segundo resultado importante de esta sección, que junto con el anterior serán claves para probar el Teorema de Mordell.

Teorema 1.27. *(Teorema de las unidades de Dirichlet). Sea K un cuerpo numérico y $\mathcal{O}_K$ su anillo de enteros. Entonces el grupo de unidades de $\mathcal{O}_K$ es finitamente generado.*

Demostración. [6, Ch 19, §3, Lemma 4] □

2 Curvas elípticas

2.1 De cúbicas a curvas elípticas

En esta sección, salvo que se diga lo contrario, K denotará un cuerpo cualquiera y $\overline{K}$ su clausura algebraica. Comenzaremos pasando de una cúbica arbitraria a una expresión más particular llamada *ecuación de Weierstrass*. Después haremos aún más simplificaciones asumiendo que la característica del cuerpo no es 2 ni 3 y acabaremos dando las formas más sencillas en las que siempre podemos expresar una curva elíptica definida sobre $\mathbb{Q}$, las cuales usaremos durante el resto del trabajo. En lo que sigue supondremos que el lector tiene algunos conocimientos básicos de geometría algebraica para que el lenguaje usado no le sea en ocasiones desconocido. Aún así planteamos a continuación las definiciones y resultados que más usaremos.

Definición 2.1. *Un conjunto algebraico $V \subset \mathbb{A}^n(\overline{K})$ se dice definido sobre K si su ideal de polinomios, $\mathcal{I}(V)$, puede ser generado por polinomios de $K[x_1, ..., x_n]$.*

En el caso de una curva plana $C \subset \mathbb{A}^2(\overline{K})$, si $f(x, y)$ es un generador[2] de $\mathcal{I}(C)$, ser definida sobre K es equivalente a que f tenga sus coeficientes en K.

Definición 2.2. *Un conjunto algebraico (proyectivo) $V \subset \mathbb{P}^n(\overline{K})$ se dice definido sobre K si su ideal de polinomios, $\mathcal{I}(V)$, puede ser generado por polinomios homogéneos de $K[x_0, x_1, ..., x_n]$.*

Definición 2.3. *Sea $V \subset \mathbb{A}^n(\overline{K})$ una variedad algebraica. Definimos los puntos K-racionales de V como:*

$$V(K) := \{P = (x_1, ..., x_n) \in V \mid x_i \in K\} = V \cap \mathbb{A}^n(K).$$

Definición 2.4. *Sea V una variedad, $P \in V$, y sean $f_1, ...f_m \in \overline{K}[X_1, ..., X_n]$ polinomios generadores de $\mathcal{I}(V)$. Entonces V es no singular en P (o P es un punto no singular de V) si la matriz $m \times n$:*

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

tiene rango $n - \dim(V)$. Si V es no singular en todos sus puntos, se dice que V es una variedad no singular. Los puntos no singulares a veces son llamados simples en contraposición a los singulares, también llamados múltiples.

[2]Es decir, f es un polinomio reducido, o equivalentemente, C no tiene componentes irreducibles múltiples.

Ejemplo 2.5. *Si V está dada por una única ecuación polinómica reducida:*

$$f(X_1, ..., X_n) = 0,$$

entonces $\dim(V) = n - 1$*, luego $P \in V$ es singular si y solo si*

$$\frac{\partial f}{\partial X_1}(P) = \ldots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Como P además satisface $f(P) = 0$, esto da $n+1$ ecuaciones para las n coordenadas de cualquier punto singular. Luego, hablando de forma un poco imprecisa, para un polinomio f "aleatoriamente" escogido uno esperaría que V fuese no singular.

En concreto, para las curvas planas, dadas por un polinomio $f(x, y) = 0$, como tienen dimensión 1, un punto P es singular si y solo si

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

Definición 2.6. *Si $P = (x_0, y_0)$ es un punto no singular de la curva $C : f(x, y) = 0$ definimos la tangente a C en P como la recta:*

$$\frac{\partial f}{\partial x}(P)(x - x_0) + \frac{\partial f}{\partial y}(P)(y - y_0) = 0.$$

Observación 2.7. *Técnicamente un punto no singular $P = (x_0, y_0)$ de $C : g(x, y) = 0$ es aquel en el que podemos definir la recta tangente:*

$$\frac{\partial g}{\partial x}(P)(x - x_0) + \frac{\partial g}{\partial y}(P)(y - y_0) = 0. \tag{1}$$

de manera única. Si P es singular la expresión anterior es una trivialidad y no tenemos recta tangente en este sentido. Pero lo que ocurre en muchas ocasiones es que la curva pasa varias veces por P y hay múltiples tangentes (o la misma con multiplicidad mayor que uno). Por eso lo que se suele hacer es lo siguiente.

Supongamos que el punto singular es $P = (0, 0)$. Sea $n = \deg(g)$. Expresamos $g(x, y)$ como suma de su componentes homogéneas, es decir:

$$g(x, y) = g_m + g_{m+1} + ... + g_n \tag{2}$$

*donde cada g_i es un polinomio homogéneo de grado i en x e y. Observemos que g_m es la primera componente homogénea no nula. A este número se le llama **multiplicidad de** g **en** P o **multiplicidad de** P **en la curva** C. Además P es simple (no singular) si y solo si $m = 1$ ya que (2) no es más que el desarrolo en serie de Taylor de g en torno a P y los coeficientes del término de grado 1 son las parciales de primer orden de g en P.*

Como $P \in C$, se tiene $m > 0$ y si es singular se tiene $m > 1$. Por ser $\overline{K}$ algebraicamente cerrado todo polinomio homogéneo de grado m se puede expresar como producto de m rectas : $g_m = \prod_{i=1}^{m} L_i$. Estas rectas L_I se definen como las tangentes de C en P y su multiplicidad como tangente es su multiplicidad como factor de g_m.

Para generalizar esto a un punto $P = (a, b) \in C$ cualquiera hacemos el cambio de variables $(x, y) \mapsto (x + a, y + b)$, de manera que (a, b) es singular para $g(x, y)$ si y solo si $(0, 0)$ lo es para $g(x + a, y + b)$ y a este polinomio ya le podemos aplicar el procedimiento anterior y hallar las rectas tangentes de $g(x + a, y + b)$ en $(0, 0)$. Por último deshacemos el cambio de variables para obtener las tangentes de C en P. Una forma equivalente de hacerlo es factorizar directamente el término de menor grado en el desarrollo de Taylor de g alrededor de $P = (a, b)$.

Una exposición más detallada sobre tangentes en puntos singulares de curvas se puede encontrar en [9, Ch. 3, §1].

Observación 2.8. *Diremos a menudo que dos curvas planas proyectivas dadas por sendas ecuaciones polinómicas son isomorfas. Con ello lo que queremos decir es que son isomorfas como variedades algebraicas.*

Ahora comenzamos con nuestro estudio de cúbicas. Sea:

$$\tilde{f}(x, y) = \alpha_1 x^3 + \alpha_2 x^2 y + \alpha_3 x y^2 + \alpha_4 y^3 + \alpha_5 x^2 + \alpha_6 x y + \alpha_7 y^2 + \alpha_8 x + \alpha_9 y + \alpha_{10} = 0 \quad (3)$$

la ecuación de una cúbica general, C, es decir, f es un polinomio cualquiera de grado 3 en x e y. Como es natural en geometría, la vemos en el proyectivo para no *perdernos* ningún punto o componente, así que homogeneizamos el polinomio $\tilde{f}$, haciendo $x = X/Z, y = Y/Z$ y multiplicando por Z^3. Obtenemos el polinomio homogéneo de grado 3 que define la curva en $\mathbb{P}^2$.

$$C : \tilde{F}(X, Y, Z) = 0 \quad (4)$$

En $\mathbb{P}^2(\overline{K})$ hemos denotado a las variables por X, Y, Z donde Z es la variable que hemos usado para homogeneizar. Tras escalar los ejes adecuadamente, podemos llegar a una ecuación de la forma:

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3 \quad (5)$$

Y deshomogeneizando obtenemos:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad (6)$$

La ecuación (6) se dice que está en **forma de Weierstrass**. En el Apéndice A damos un procedimiento para llevar una cúbica cualquiera a una ecuación de

Weierstrass, válido si la característica del cuerpo es 0. Además damos un ejemplo de dicho procedimiento con una cúbica concreta.

Podemos verificar que una curva dada por una ecuación de esta forma solo tiene un punto en el infinito. Si en (5) cortamos con $Z = 0$ obtenemos $X = 0$, luego el único punto en la recta del infinito $Z = 0$ es $\mathcal{O} = [0, 1, 0]$, que es un punto K-racional de $\mathbb{P}^2(\overline{K}) = \mathbb{A}^2(\overline{K}) \cup \mathbb{P}^1(\overline{K})$. Esto nos ayudará a dotarla de estructura de grupo. Buscaremos que el elemento neutro sea el punto del infinito de la curva. Si queremos que $E(K)$ acabe siendo un subgrupo, nos es clave el hecho que podamos considerar a $\mathcal{O}$ como un punto K-racional.

Visto lo anterior, y como asumiremos de ahora en adelante, podemos ver cualquier cúbica, C, dada por $f(x, y) = 0$ en forma de Weierstrass como:

$$C = \big\{(x, y) \in \mathbb{A}^2(\overline{K}) \mid f(x, y) = 0\big\} \cup \{\mathcal{O}\} \tag{7}$$

donde $\mathcal{O}$ es el único punto del infinito de (5). Remarquemos que las coordenadas de los puntos de C están en $\overline{K}$, un cuerpo algebraicamente cerrado. Siguiendo la notación de la Definición 2.3 denotamos por $C(K)$ los puntos de C que están en $\mathbb{A}^2(K)$ además del punto $\mathcal{O}$.

Ahora pasamos a definir nuestro principal objeto de estudio.

Definición 2.9. *Se dice que la cúbica dada por la ecuación de Weierstrass:*

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

es un ***curva elíptica****, E, si $f(x, y)$ define una curva no singular.*

Si $a_i \in K$ se dice que E está definida sobre K.

Las curvas elípticas las denotaremos siempre por E y las entendemos como en (7). Hemos impuesto la condición de no singularidad sobre la ecuación afín de la curva porque, como veremos abajo, el punto $\mathcal{O}$ nunca es singular.

Originalmente las curvas elípticas se consideraban como el conjunto de soluciones de ecuaciones del tipo (6) y que no tuviesen puntos singulares. Después se probó que son curvas de grado 3 y género 1, y esta pasó a ser una definición aparentemente más general de curva elíptica. Pero resulta que toda curva elíptica (entendida como curva de grado 3 y género 1) es isomorfa a una curva dada por una ecuación del tipo (6). Una prueba de este hecho, usando el Teorema de Riemann-Roch, se puede encontrar en [2, Ch. III,§3, Proposition 3.1].

Las condiciones que impondrá sobre la ecuación de Weierstrass el hecho de que la curva sea no singular las veremos en la siguiente subsección, sobre una versión aún más reducida de la ecuación que podemos encontrar cuando trabajamos sobre un cuerpo de característica 0. Por ahora describiremos los tipos de puntos singulares que nos podemos encontrar.

Sea $E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ una cúbica en ecuación de Weierstrass. Primero veamos que el único punto del infinito, $\mathcal{O}$, **nunca es singular**. Sea $F(X,Y,Z)$ la ecuación homogeneizada de la curva, que dimos en (5). Sus derivadas parciales son:

$$\begin{aligned}\frac{\partial F}{\partial X} &= a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2\\ \frac{\partial F}{\partial Y} &= 2YZ + a_1XZ + a_3Z^2\\ \frac{\partial F}{\partial Z} &= Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^3.\end{aligned}$$

Sustituyendo en $\mathcal{O} = [0,1,0]$ vemos que

$$\left(\frac{\partial F}{\partial X}(\mathcal{O}), \frac{\partial F}{\partial Y}(\mathcal{O}), \frac{\partial F}{\partial Z}(\mathcal{O})\right) = [0,0,1] \neq [0,0,0] \tag{8}$$

luego $\mathcal{O}$ no es singular. El resto de puntos de la curva son afines así que trabajamos con la ecuación afín de la curva. Un punto $P = (x_0, y_0) \in E$ es singular si:

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

Tenemos:

$$\begin{aligned}&\frac{\partial f}{\partial x} = a_1y - 3x^2 - 2a_2x - a_4, \quad \frac{\partial f}{\partial y} = 2y + a_1x + a_3\\ &\frac{\partial^2 f}{\partial x^2} = -6x - 2a_2, \quad \frac{\partial^2 f}{\partial y^2} = 2, \quad \frac{\partial^2 f}{\partial x \partial y} = a_1 = \frac{\partial^2 f}{\partial y \partial x}.\end{aligned}$$

Y la única derivada de orden 3 no nula es $\dfrac{\partial^3 f}{\partial x^3} = -6$. Luego el desarrollo en serie de Taylor de f en torno a P tiene la forma:

$$\begin{aligned}f(x,y) &= f(x,y) - f(x_0,y_0)\\ &= \frac{1}{2!}\left(\frac{\partial^2 f}{\partial x^2}(P)(x-x_0)^2 + 2\frac{\partial^2 f}{\partial x \partial y}(P)(x-x_0)(y-y_0) + \frac{\partial^2 f}{\partial y^2}(P)(y-y_0)^2\right)\\ &\quad + \frac{1}{3!}\frac{\partial^3 f}{\partial x^3}(x-x_0)^3\\ &= (-3x_0 - a_2)(x-x_0) + a_1(x-x_0)(y-y_0) + (y-y_0)^2 - (x-x_0)^3\\ &= ((y-y_0) - \alpha(x-x_0))((y-y_0) - \beta(x-x_0)) - (x-x_0)^3\end{aligned}$$

donde $\alpha = \frac{a_1 \pm \sqrt{a_1^2 + 4(3x_0 + a_2)}}{2}$, $\beta = \frac{a_1 \mp \sqrt{a_1^2 + 4(3x_0 + a_2)}}{2}$ (nótese que cada raíz tiene signos opuestos) y $\alpha, \beta \in \overline{K}$. En realidad sobre un cuerpo algebraicamente cerrado un

polinomio homogéneo de grado n siempre se puede factorizar como producto de n factores lineales (rectas). Es lo que hemos hecho para llegar a la última igualdad con el término de segundo grado del desarrollo (tratándolo como un polinomio en $(x - x_0)$ e $(y - y_0)$).

Definición 2.10. *Sea $P = (x_0, y_0)$ un punto singular de E. Con la notación precedente decimos que:*

1. *P es un nodo si $\alpha \neq \beta$. En este caso las rectas:*

$$y - y_0 = \alpha\,(x - x_0) \qquad y \qquad y - y_0 = \beta\,(x - x_0)$$

   son las rectas tangentes en P y son distintas.

2. *P es un punto cúspide si $\alpha = \beta$. En ese caso las rectas tangentes en P coinciden y valen:*

$$y - y_0 = \alpha\,(x - x_0)\,.$$

La Figura 4 muestra un ejemplo de cada caso. Cabe remarcar que las tangentes en un nodo no tienen porqué ser reales. La Figura 2 muestra un ejemplo de como quedaría el locus real afín de la curva en este caso.

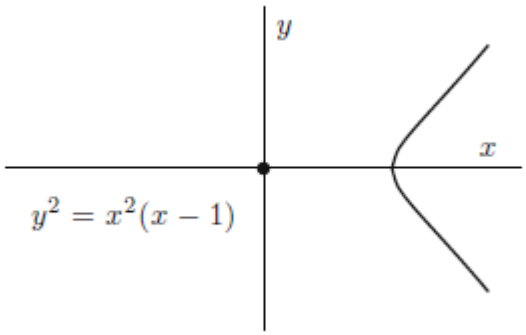

Figura 2: Nodo con tangentes complejas distintas en $(0, 0)$

2.2 Curvas elípticas sobre $\mathbb{Q}$

Hemos definido las curvas elípticas con ecuaciones de Weierstrass de la forma:

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

porque es la expresión más general a la que podemos llegar sin asumir nada sobre la característica de K (o la de $\overline{K}$, pues son iguales). A continuación presentamos sucesivas simplificaciones imponiendo restricciones a la característica y definimos cantidades que serán muy importantes en el estudio de las curvas elípticas.

Si $\mathrm{char}(\overline{K}) \neq 2$ podemos completar el cuadrado en la ecuación (6) mediante el cambio de variables:

$$y \to \frac{1}{2}\left(y - a_1x - a_3\right)$$

y tras simplificar obtenemos:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{9}$$

donde

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

También definimos las cantidades:

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta. \end{aligned} \tag{10}$$

Podemos verificar directamente las relaciones:

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2.$$

Si además $\mathrm{char}(\overline{K}) \neq 2, 3$ entonces la sustitución:

$$(x,y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right)$$

elimina el término en x^2 de (9), y la ecuación queda:

$$E : y^2 = x^3 - 27c_4x - 54c_6. \tag{11}$$

Definición 2.11. *Conservando la notación de (10), la cantidad Δ se denomina el **discriminante** de la ecuación de Weierstrass, y j es el j-**invariante** de la curva elíptica.*

Observación 2.12. *El discriminante está definido para cualquier cúbica en ecuación de Weierstrass, mientras que el j-invariante solo para curvas elípticas, pues como veremos a continuación $\Delta = 0$ si y solo si la curva es singular.*

El siguiente teorema dejará claro el porqué de sus nombres y de su importancia. Aunque su prueba es sencilla, no lo demostraremos pues en ningún momento lo usaremos de cara a probar el Teorema de Mordell. Aun así, por su belleza, lo enunciamos y damos una referencia a su prueba.

Teorema 2.13. *1. Una curva E dada por una ecuación de Weierstrass como en (6) cumple lo siguiente:*

(a) Es no singular si y solo $\Delta \neq 0$.

(b) Tiene un nodo si y solo si $\Delta = 0$ y $c_4 \neq 0$.

(c) Tiene una cúspide si y solo si $\Delta = c_4 = 0$.

2. Dos curvas elípticas son isomorfas sobre $\overline{K}$ si y solo si tienen el mismo j-invariante.

3. Para todo $j_0 \in \overline{K}$ existe una curva elíptica definida sobre $K(j_0)$ cuyo j-invariante vale j_0.

Demostración. [2, Ch. III, §1, Proposition 1.4] □

En las figuras 3 y 4 mostramos ejemplos de las tres situaciones descritas en Teorema 2.13, apartado a).

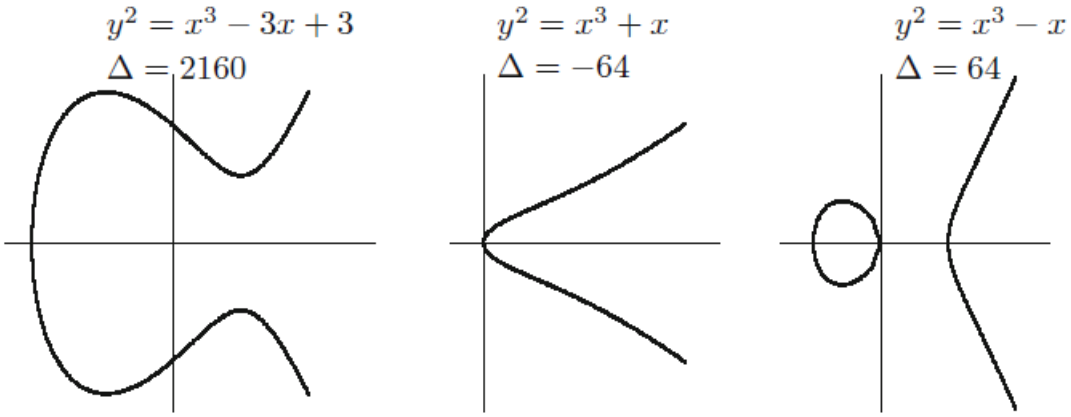

Figura 3: Tres curvas elípticas

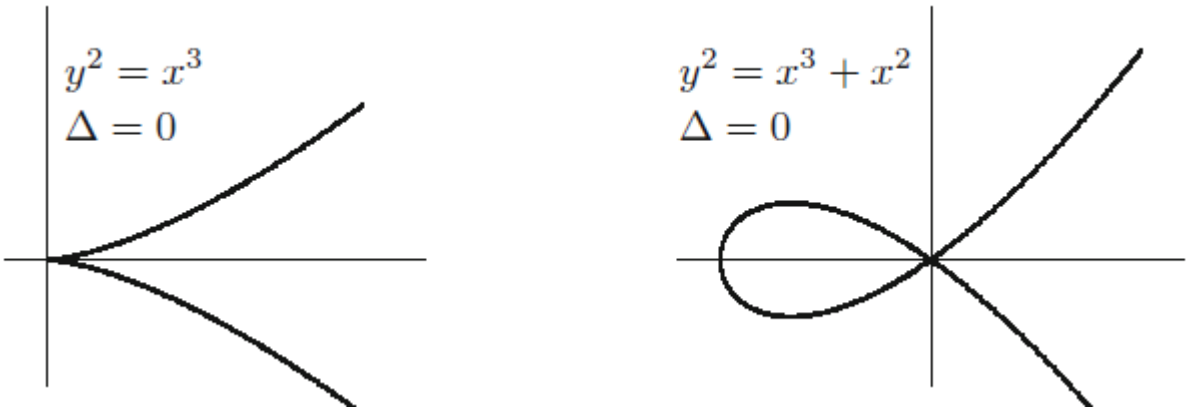

Figura 4: Dos cúbicas singulares, la izquierda con una cúspide y la derecha con un nodo.

Si E es una curva elíptica definida sobre $\mathbb{Q}$ sabemos que podemos encontrarle una ecuación de la forma (11), es decir,

$$E : y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q} \tag{12}$$

Esta última ecuación se suele llamar *forma reducida de Weierstrass*. Nosotros usaremos mayoritariamente la versión ligeramente más general:

$$E : y^2 = x^3 + ax^2 + bx + c \tag{13}$$

De esta forma nos podremos ahorrar en ocasiones tener que completar el cuadrado para llegar a (12). Ahora veremos una última simplificación que será necesaria en el futuro.

Proposición 2.14. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Entonces podemos encontrarle una ecuación de la forma:*

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}$$

Es decir, podemos suponer siempre que es definida sobre $\mathbb{Z}$.

Demostración. Si E es definida sobre $\mathbb{Q}$, sabemos que viene dada por una ecuación con coeficientes racionales:

$$y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}, \quad \tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Q}.$$

Sea D el máximo común denominador de $\tilde{a}, \tilde{b}$ y $\tilde{c}$. Multiplicamos la ecuación por D^6:

$$(D^3y)^2 = (D^2x)^3 + \tilde{a}D^2(D^2x)^2 + \tilde{b}D^4(D^2x) + \tilde{c}D^6.$$

Si hacemos el cambio de variable

$$(D^2x, D^3y) \mapsto (x, y) \tag{14}$$

y denotamos $a = \tilde{a}D^2, b = \tilde{b}D^4, c = \tilde{c}D^6$ tenemos:

$$E : y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in \mathbb{Z}.$$

□

Observación 2.15. *El cambio de variable (14) usado en la prueba anterior, es biyectivo, lineal en las variables x e y, y definido en todos los puntos. En particular esto implica que es un isomorfismo (de variedades algebraicas) entre la curva original E_1 (con coeficientes racionales) y la curva definida sobre $\mathbb{Z}$, E_2.*

Más importante aún es que conserva los puntos racionales, es decir, $E(\mathbb{Q})$ se queda fijo con el cambio (14) pues como $0 \neq D \in \mathbb{Q}$ se tiene:

$$(x, y) \in E_1(\mathbb{Q}) \iff (D^2x, D^3y) \in E_2(\mathbb{Q})$$

Veamos ahora como quedan las cantidades (10) para la ecuación (13). En este caso $a_1 = a_3 = 0, a_2 = a, a_4 = b, a_6 = c$.

$$b_2 = 4a, \quad b_4 = 2b, \quad b_6 = 4c$$
$$b_8 = 4ac - b^2, \quad c_4 = 16(a^2 - 3b)$$
$$\Delta = 16(-4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc), \quad j = 2^{12}\frac{(a^2 - 3b)^3}{\Delta}$$

Usando esto, para la ecuación en la forma (12) tenemos:

$$c_4 = -48A, \quad \Delta = -16(4A^3 + 27B^2), \quad j = -1728\frac{(4A)^3}{\Delta}$$

Estas cantidades así expresadas nos permiten un estudio rápido de la curva E y sus puntos singulares cuando viene dada por las ecuaciones (12) ó (13).

Para concluir esta sección veamos cómo se traduce la condición de no singularidad de la curva en condiciones sobre su ecuación.

Proposición 2.16. *Sea E una cúbica definida sobre $\mathbb{Q}$. Sabemos que puede venir dada por la ecuación:*

$$y^2 = f(x) \text{ donde } f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x].$$

Entonces E es una curva elíptica si y solo si $f(x)$ es separable.

Demostración. Tenemos que probar que E no tiene puntos singulares si y solo si todas las raíces de f son distintas (recordemos que esto es equivalente a que f y f' sean comprimos en $\mathbb{Q}[x]$, es decir, que f y f' no tienen raíces comunes). En primer lugar, recordemos que el punto del infinito $\mathcal{O} = [0, 1, 0]$ nunca es singular, como vimos en (8) para una versión incluso más genérica de la ecuación (en concreto aquí $a_3 = a_1 = 0$). El resto de puntos de la curva son afines, así que examinamos las derivadas de

$$g(x, y) = y^2 - f(x)$$

y obtenemos

$$\frac{\partial g}{\partial x}(x, y) = -f'(x)$$
$$\frac{\partial g}{\partial y}(x, y) = 2y.$$

Luego el punto afín $P = (x_0, y_0) \in E$ es singular si y solo si:

$$y_0^2 - f(x_0) = 0, \quad f'(x_0) = 0, \quad 2y_0 = 0.$$

La última condición nos dice que $y_0 = 0$. Es decir $E : y^2 - f(x)$ es no singular si y solo si el sistema

$$f(x_0) = 0, \qquad f'(x_0) = 0$$

es incompatible. Es decir si y solo si f y f' no tienen raíces comunes lo cual es equivalente a que f no tenga raíces múltiples. □

Observación 2.17. *Dado un polinomio cúbico mónico con coeficientes reales:*

$$f(x) = x^3 + ax^2 + bx + x = (x - e_1)(x - e_2)(x - e_3)$$

Su discriminante es la cantidad:

$$D(f) = -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc$$

O usando las raíces de f:

$$D(f) = (e_1 - e_2)^2(e_2 - e_3)^2(e_1 - e_3)^2$$

Si $D(f) > 0$, f tiene tres raíces reales distintas.
Si $D(f) = 0$, f tiene una raíz doble y todas sus raíces son reales.
Si $D(f) < 0$, f f tiene una raíz real y dos raíces complejas conjugadas distintas.
No casualmente se tiene

$$\Delta = 16D(f) \tag{15}$$

donde Δ es el discriminante de la cúbica $y^2 = f(x)$. La proposición anterior nos dice que dicha cúbica es no singular si y solo si $f(x)$ no tiene raíces dobles, y sabemos que esto ocurre si y solo si $D(f) \neq 0$. La ecuación (15) nos dice que esto es equivalente a $\Delta \neq 0$, lo cual demuestra fácilmente la afirmación 1a) de la Proposición 2.13, que nos decía que E es no singular si y solo si $\Delta \neq 0$.

3 La operación de grupo

3.1 Descripción geométrica de la ley de grupo

En esta sección expondremos la operación de grupo, primero de una forma más general considerando como elemento neutro cualquier punto racional $\mathcal{O}$. Después particularizaremos de manera que el elemento neutro será el único punto del infinito de la curva en forma de Weierstrass, que ya sabemos que es racional. Antes haremos una serie de observaciones que nos facilitarán su exposición.

Durante toda esta sección consideraremos una curva elíptica $E : y^2 = f(x) = x^3 + ax^2 + bx + x$ definida sobre $\mathbb{Q}$. Como demostramos, f debe ser separable.

Recordemos también un resultado importante. El Teorema de Bézout nos dice que la suma de las multiplicidades de intersección de los puntos de la intersección de curvas de grado n y m es exactamente nm. Esto es cierto sobre $\mathbb{P}^n(K)$ donde K es un cuerpo algebraicamente cerrado. Nosotros seguimos mirando nuestra curva en $\mathbb{P}^2(\overline{\mathbb{Q}}) \subset \mathbb{P}^2(\mathbb{C})$ como los puntos afines de $\mathbb{A}^2(\overline{\mathbb{Q}})$ que verifiquen su ecuación definida sobre $\mathbb{Q}$, unión el único punto que tiene en el infinito. Cabe remarcar que una recta no tiene por qué cortar a una cúbica en 3 puntos distintos, puede cortarla en 1,2 ó 3 pero la suma de sus multiplicidades de intersección debe ser 3.

En primer lugar, si P, Q son dos puntos de E, la recta que los une deber cortar a E en un tercer punto que denotaremos $P * Q$, no necesariamente distinto de P o Q. Si $P = Q$ la recta que los une es la tangente a E en P que corta dos veces a la curva en P, luego sigue habiendo un tercer punto de intersección. Esto se ilustra en la Figura 5.

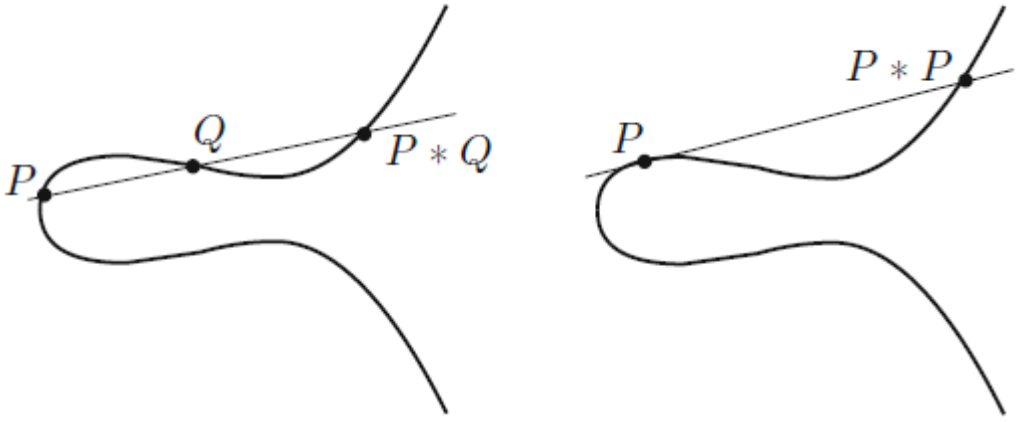

Figura 5: Ilustrando la operación $*$ de tomar una tercera intersección

Observación 3.1. *1. La operación binaria $*$ es trivialmente conmutativa, pues la recta que pasa por P y Q es la misma que pasa por Q y P*

2. Fijado un punto P_0, la operación

$$E \to E, \quad P \mapsto P * P_0$$

es una involución, es decir, es su propia inversa. Pues si $R = P * P_0$ es el tercer punto de intersección con E de la recta que une P y P_0, entonces $R * P_0$, el tercer punto de intersección de R y P_0, es claramente P.

Definición 3.2. *(**Ley de grupo**) Sean $P, Q \in E$ y L la recta pasando por P y Q. Supongamos que E tiene un punto racional $\mathcal{O}$. Sea $P * Q$ el tercer punto de intersección de L con E. Unimos $P * Q$ al punto $\mathcal{O}$ mediante la recta L'. El tercer punto de intersección de L' con E lo denotamos $P + Q$. En otras palabras:*

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

La Figura 6 ilustra la ley de grupo.

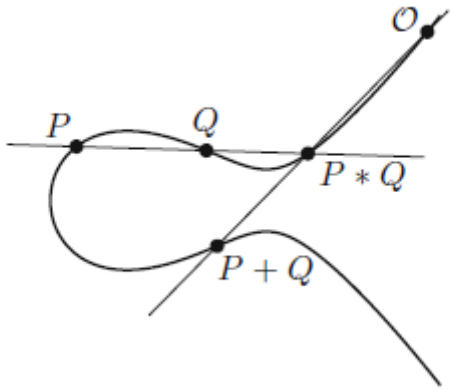

Figura 6: Ley de grupo en una curva elíptica

Antes de proceder vamos a ver un resultado general sobre cúbicas planas: el Teorema de Cayley–Bacharach. No daremos una prueba, sino una idea de la misma, ya que al fin y al cabo este resultado no nos hará estricta falta. Lo usaremos para dar una prueba geométrica para algunos casos de la asociatividad de la ley de grupo, pero podremos evadirlo cuando tengamos las fórmulas para la suma de puntos que daremos en la siguiente subsección. Una prueba completa de este

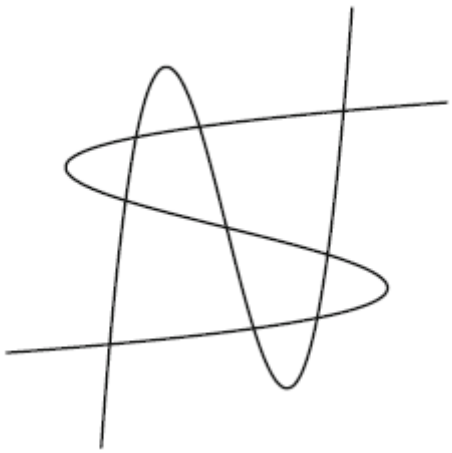

Figura 7: Intersección de dos cúbicas

teorema se puede encontrar en [10, Ch. 2, §3, Theorem 3.3] o en [9, Ch. 5, §6, Proposition 3]. Tengamos en mente que el Teorema de Bézout nos dice que dos cúbicas distintas se cortan en 9 puntos (no necesariamente distintos pues contamos la multiplicidad de cada uno de ellos). Podemos ver un ejemplo en la Figura 7. Enunciamos ahora el resultado.

Proposición 3.3. *(Teorema de Cayley–Bacharach) Sean* $C_1 : F_1(x, y) = 0$, $C_2 : F_2(x, y) = 0$ *dos cúbicas distintas que se intersectan en 9 puntos distintos:* $P_1, .., P_9$. *Entonces cualquier cúbica* C *que pase por 8 de los 9 nueve puntos de intersección pasa también por el noveno. En particular* C *tiene una ecuación de la forma* $\lambda_1 F_1(x, y) + \lambda_2 F_2(x, y) = 0, (\lambda_1, \lambda_2) \neq (0, 0)$.

Idea de la prueba Para definir un polinomio cúbico en x e y como en (3) necesitamos dar 10 coeficientes. Pero en realidad el conjunto de cúbicas posibles variando estos coeficientes es 9-dimensional[3], pues si multiplicamos los coeficientes por un elemento no nulo de K seguimos obteniendo la misma cúbica. Si imponemos que la cúbica pase por un punto dado, obtenemos una condición lineal en los coeficientes α_i de la misma. Luego el conjunto de cúbicas que pasa por un punto fijado es 8-dimensional. Cada vez que añadimos la condición de que la curva pase

[3]Cuando hablamos aquí de dimensión, lo que queremos decir es que entendemos el conjunto de cúbicas como los elementos no nulos del espacio vectorial con base $\{1, x, y, x^2, y^2, xy, x^3, y^3, xy^2, x^2y\}$ sobre K, bajo la relación de que si los coeficientes de dos curvas son proporcionales entonces ambas son iguales. Esto es equivalente a decir que dicho conjunto de cúbicas es lo mismo que $\mathbb{P}^9(K)$.

por un punto, reducimos en uno dicha dimensión[4]. En particular, la familia de cúbicas pasando por ocho puntos de $C_1 \cap C_2$, digamos $P_1, ...P_8$, es 1-dimensional.

Para todo $[\lambda_1, \lambda_2] \in \mathbb{P}^1(K), \lambda_1 F_1 + \lambda_2 F_2$ es una cúbica pasando por los puntos $P_1, ..., P_8$. Como solo hay una familia 1-dimensional de cúbicas cumpliendo esa propiedad, el haz de cúbicas $\{\lambda_1 F_1 + \lambda_2 F_2 | [\lambda_1, \lambda_2] \in \mathbb{P}^1(K)\}$ debe ser dicha familia. En particular C es de la forma $\lambda_1 F_1 + \lambda_2 F_2$ para una elección adecuada de λ_1, λ_2. Como F_1 y F_2 se anulan en el noveno punto de intersección, P_9, C también pasa por P_9.

Proposición 3.4. *La **Ley de grupo** definida en 3.2 dota a E de estructura de grupo abeliano, siendo $\mathcal{O}$ el punto neutro.*

Demostración. El grupo es trivialmente conmutativo, es decir, se tiene:

$$P + Q = Q + P$$

ya que la recta que une P y Q es la misma que une Q y P, luego $P * Q = Q * P$.

Además el punto $\mathcal{O}$ es claramente el elemento identidad. Dado $P \in E$, si unimos P y $\mathcal{O}$ con una recta y obtenemos su tercer punto de intersección con E, es decir $P * \mathcal{O}$, entonces el tercer punto de intersección de la recta que une $P * \mathcal{O}$ y $\mathcal{O}$ es P (pues $*\mathcal{O}$ es involutiva, ver Observación 3.1). Luego

$$P + \mathcal{O} = P$$

Esto se muestra en la Figura 8.

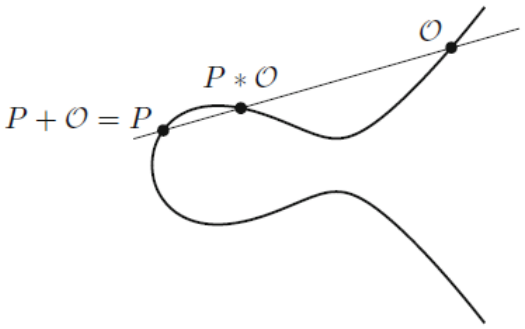

Figura 8: Verificando que $\mathcal{O}$ es el elemento identidad

[4]Para que eso ocurra necesitamos que la condición lineal que imponga cada nuevo punto sobre los coeficientes sea linealmente independiente con las anteriores. Esto ocurre si los puntos están en una posición adecuada (*posición general* con respecto a una cúbica plana).

Para conseguir inversos dibujamos la tangente a la curva en $\mathcal{O}$ (recordemos que por ahora $\mathcal{O}$ es un punto racional cualquiera, no necesariamente el del infinito). Como la tangente en un punto corta a E en ese punto con multiplicidad 2, solo corta a la curva en otro punto más, que denotamos S. Es decir, $S = \mathcal{O} * \mathcal{O}$. Además está bien definido porque E es no singular y por tanto tiene tangente en todos sus puntos. Ahora dado un punto Q definimos $-Q$ como el tercer punto de intersección con E de la recta que pasa por S y Q, es decir, $-Q = Q * S$. Comprobemos que es en efecto el inverso de Q.

$$Q + (-Q) = \mathcal{O} * (Q * (-Q)) = \mathcal{O} * S = \mathcal{O}$$

la última igualdad debiéndose a que la recta que une S y $\mathcal{O}$ es tangente a E en $\mathcal{O}$. El procedimiento para conseguir inversos se ilustra en la Figura 9.

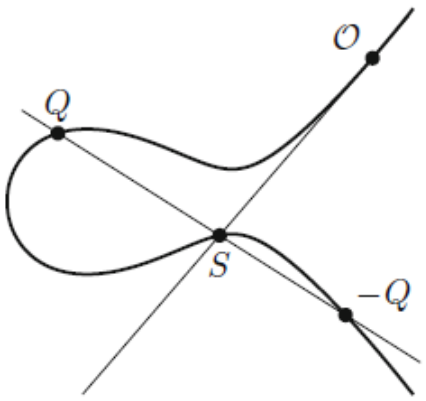

Figura 9: El inverso de un punto Q.

Nos queda probar la asociatividad de $+$ para hacer de $(E, +)$ un grupo. Esta es sin ninguna duda la tarea más difícil. Una vez que demos las fórmulas para la duplicación y suma de puntos en la siguiente subsección, el lector podrá comprobar directamente la asociatividad caso por caso. Vamos a dar aquí una prueba puramente geométrica para un caso particular basada en el Teorema de Cayley–Bacharach. Una tercera prueba, indirecta pero elegante, se puede encontrar en [2, Ch. III, §3,Proposition 3.4]. En ella se demuestra que cierta aplicación entre $\mathrm{Pic}^0(E)$ y E es un isomorfismo de grupos, donde $\mathrm{Pic}^0(E)$ es el subgrupo del grupo de Picard de E formado por los divisores de grado 0, cociente el subgrupo de divisores principales de E. Después se muestra que la ley de grupo *geométrica* que hemos definido nosotros coincide con la ley de grupo *algebraica* inducida por

dicho isomorfismo. La asociatividad en E se sigue entonce de la asociatividad en $\mathrm{Pic}^0(E)$. Procedemos ahora a dar nuestra prueba geométrica.

Sean $P, Q, R \in E$. Queremos probar:

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

Debido a la conmutatividad de la operación $*$ de tomar la tercera intersección con E, nos es suficiente mostrar:

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

El proceso para la creación de los puntos $(P + Q) * R$ y $P * (Q + R)$ está reflejado en la Figura 10 e involucra los puntos:

$$\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R, Q + R \tag{16}$$

Las rectas involucradas se muestran en la siguiente tabla:

Punteadas	Sólidas
Recta entre P, Q y $P * Q$	Recta entre R,Q y $Q * R$
Recta entre R,$P + Q$ y $(P + Q) * R$	Recta entre $\mathcal{O}$,$P * Q$ y $P + Q$
Recta entre $\mathcal{O}$, $Q * R$ y $(Q + R)$	Recta entre P,$Q + R$ y $P * (Q + R)$

Cada uno de los puntos en (16) pasa por una de las rectas descritas en la tabla anterior. Sea L_1 la recta punteada entre $P + Q$ y R y L_2 la recta sólida entre P y $Q+R$. Su tercer punto de intersección con la curva son respectivamente $(P+Q)*R$ y $P * (Q + R)$. Pero estas dos rectas deben cortarse en algún punto. ¿Está su intersección en la curva? Si es así habríamos probado que $(P+Q)*R = P*(Q+R)$ y por tanto nuestro resultado.

Tenemos nueve puntos: los ocho de (16) y la intersección de L_1 y L_2. Si multiplicamos las ecuaciones de las tres rectas punteadas, y hacemos lo mismo con las sólidas, obtenemos dos cúbicas (degeneradas), cuyas soluciones son la unión de las respectivas rectas. Ahora aplicamos el Teorema de Cayley-Bacharach siendo C_1 la unión de las líneas punteadas y C_2 la de las sólidas. Ambas pasan por los nueve puntos. Como la curva original E pasa por ocho de esos puntos, los dados en (16), debe pasar también por el noveno. Es decir, la intersección de L_1 y L_1 está en E, lo que prueba que $(P + Q) + R = P + (Q + R)$.

Hay que tener en cuenta que implícitamente hemos hecho una serie de simplificaciones. Para usar el Teorema de Cayley-Bacharach, los puntos dados en (16) deben ser distintos. Obviamente, eso no siempre se tiene. Aún así, los casos en los que esos 9 puntos no son distintos podemos verificarlos directamente con las fórmulas de duplicación y suma de puntos que daremos en la siguiente subsección. □

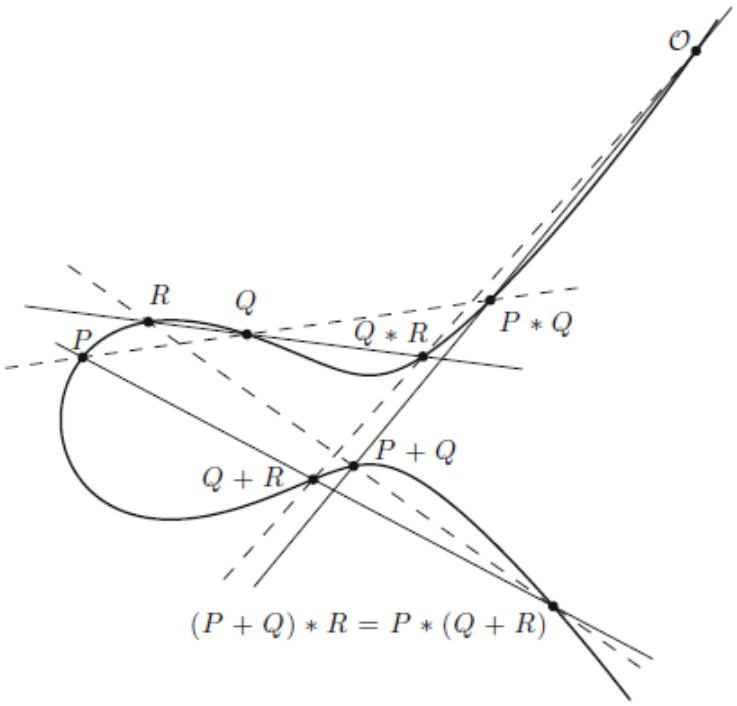

Figura 10: Verificando la asociatividad

Merece la pena mencionar que no hay nada especial en nuestra elección de $\mathcal{O}$. Si $\mathcal{O}'$ fuese otro punto de E (punto racional si queremos que $E[\mathbb{Q}]$ acabe siendo un subgrupo), entonces la aplicación:

$$P \mapsto P + \mathcal{O}'$$

es un morfismo, φ, del grupo $(E, \mathcal{O}, +)$ en el grupo $(E, \mathcal{O}', +')$, donde la nueva ley de adición sería:

$$P +' Q = P + Q - \mathcal{O}' \tag{17}$$

Verfiquemos que esto último concuerda con la ley de grupo que obtendríamos con $\mathcal{O}'$ como elemento neutro. La expresión (17) es equivalente a $P +' Q + \mathcal{O}' = P + Q$, y esto se tiene trivialmente pues:

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

Ahora comprobemos que φ es un morfismo de grupos.

$$\varphi(P+Q) = P+Q+\mathcal{O}' = (P+\mathcal{O}')+(Q+\mathcal{O}')-\mathcal{O}' = \varphi(P)+\varphi(Q)-\mathcal{O}' = \varphi(P)+'\varphi(Q)$$

El hecho de que φ es biyectiva es trivial de verificar.

Es fácil ver que para una curva elíptica, E, definida sobre $\mathbb{Q}$, los puntos con coordenadas racionales, $E(\mathbb{Q})$, son un subgrupo. Sean $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{Q})$ y sea $L : y = mx + n$ la recta que los une. Obviamente $m, n \in \mathbb{Q}$. Como $y^2 = f(x) \in \mathbb{Q}[x]$ tenemos:

$$f(x) - (mx + n)^2 = (x - x_1)(x - x_2)(x - \alpha)$$

donde α es la x-coordenada del tercer punto de intersección de L y E, $P * Q$. El polinomio $f(x) - (mx + n)^2$ es de grado 3 con coeficientes racionales. Por tanto, para que el polinomio $(x - x_1)(x - x_2)(x - \alpha)$ también lo sea debe tenerse $\alpha \in \mathbb{Q}$. La coordenada y de $P * Q$ también es racional pues vale $y = m\alpha + n$. Para hallar $P+Q$ trazamos la recta entre $\mathcal{O}$ y $P*Q$, que es racional pues ambos puntos lo son. El tercer punto de intersección de dicha recta con E es $P + Q$ y sus coordenadas son racionales por el mismo argumento con el que hemos mostrado que lo son las coordenadas de $P * Q$. Luego $P + Q \in E[\mathbb{Q}]$. Observemos que para que $E[\mathbb{Q}]$ sea un subgrupo, ha sido necesario que $\mathcal{O} \in E[\mathbb{Q}]$ pues siempre acabamos trazando rectas por ese punto. Por eso exigimos la existencia de $\mathcal{O} \in E[\mathbb{Q}]$ en la Definición de la Ley grupo.

Ahora vamos a ver cómo queda la Ley de grupo cuando tomamos como elemento neutro el punto del infinito $\mathcal{O} = [0, 1, 0]$, es decir, cuando $E : y^2 = f(x) = x^3 + ax^2 + bx + c = 0$ está en forma de Weierstrass. Primero observemos que $\mathcal{O}$ es el punto del infinito donde se unen todas las rectas verticales $x = \alpha$. Homogeneizando, las ecuaciones de las rectas verticales son:

$$X - \alpha Z = 0$$

y al cortar con la recta del infinito $Z = 0$ obtenemos $X = 0$, luego el único punto de la intersección de ambas rectas es $[0, 1, 0]$, que es precisamente $\mathcal{O}$. Además, la recta del infinito corta a E en $\mathcal{O}$ con multiplicidad 3. La forma práctica en la que aplicaremos esto es como sigue: dado un punto afín P, la recta que une P y $\mathcal{O}$ es la recta vertical que pasa por P. Además las rectas no verticales cortarán a E tres veces en el pano afín. Esto nos permite no tener que salirnos en ningún momento de la representación afín de la curva, sin olvidarnos del punto en el infinito.

Por lo dicho anteriormente, para hallar $P + Q$, primero hacemos $P * Q$ como siempre. Después, para encontrar $\mathcal{O} * (P * Q)$ solo tenemos que trazar la vertical en $P * Q$. Como la curva en forma de Weierstras es simétrica respecto al eje x, $\mathcal{O} * (P * Q)$ es la imagen especular de $P * Q$ con respecto al eje x.

Ilustramos como queda la ley de grupo ahora en la Figura 11.

¿Cómo quedan los inversos? Si $P = (x, y) \in E$ entonces $-P = (x, -y)$, la imagen especular de P respecto al eje x. Podemos comprobarlo directamente pues

la recta que une (x, y) y $(x, -y)$ es vertical, y por tanto su tercer punto de intersección con E es $\mathcal{O}$. Finalmente $\mathcal{O} * \mathcal{O} = \mathcal{O}$ luego $P + (-P) = \mathcal{O}$. ¿Concuerda esto con el procedimiento para hallar el inverso de un punto descrito en la prueba de la Proposición 3.4? La respuesta obviamente es sí. La tangente a E en $\mathcal{O}$ es la recta del infinito, que corta a E otra vez en $\mathcal{O}$. Ahora había que tomar el tercer punto de intersección de la recta $\mathcal{O}P$ con E, y como esta recta es vertical, dicho punto es $(x, -y)$. Es decir $-P = (x, -y)$. Podemos verlo representado en la Figura 12.

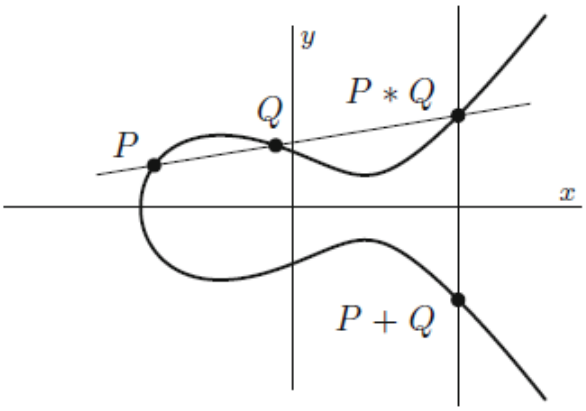

Figura 11: Ley de grupo para curvas elípticas en forma de Weierstrass

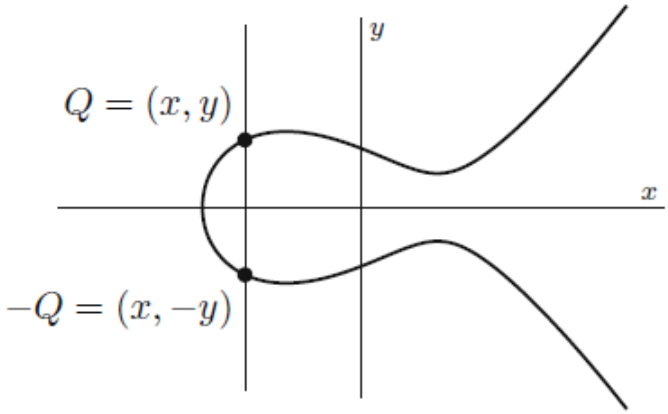

Figura 12: Tomando inversos

3.2 Fórmulas explícitas para la ley de grupo

Procedemos a dar fórmulas explícitas para la ley de grupo basándonos en la descripción geométrica de la misma. De nuevo trabajamos con una curva elíptica $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ definida sobre $\mathbb{Q}$. Dados $P_1, P_2 \in E$ queremos hallar $P_1 + P_2$. Si $P_1 = \mathcal{O}$ ó $P_2 = \mathcal{O}$ la suma es inmediata, así que podemos suponer $P_1, P_2 \neq \mathcal{O}$. En ocasiones describiremos las coordenadas de un punto P como $(x(P), y(P))$.

Escribimos:

$$P_1 = (x_1, y_1)\,, \quad P_2 = (x_2, y_2)\,, \quad P_1 * P_2 = (x_3, y_3)\,, \quad P_1 + P_2 = (x_3, -y_3)$$

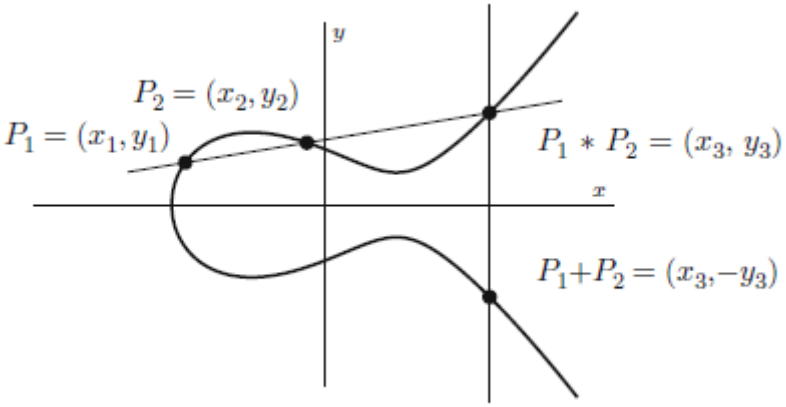

Figura 13: Hallando fórmulas para la ley de grupo

Si $x_1 \neq x_2$ (i.e., P_1 y P_2 no están en la misma vertical), creamos la recta que une P_2 y P_2. Por construcción esta recta corta a E en los puntos P_1 y P_2 y en un tercer punto que es el que queremos hallar. Su ecuación es:

$$y = \lambda x + \nu, \quad \text{donde} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{y} \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2 \tag{18}$$

Ahora la sustituimos en la ecuación de la curva y obtenemos:

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

o equivalentemente

$$0 = x^3 + \left(a - \lambda^2\right) x^2 + (b - 2\lambda\nu)x + \left(c - \nu^2\right)$$

Este es un polinomio cúbico mónico en x y sus raíces son x_1, x_2 y x_3. Por tanto tenemos:

$$x^3 + \left(a - \lambda^2\right) x^2 + (b - 2\lambda\nu)x + \left(c - \nu^2\right) = (x - x_1)(x - x_2)(x - x_3)$$

Igualando los coeficientes de x^2 en ambos lados obtenemos:

$$a - \lambda^2 = -x_1 - x_2 - x_3$$

luego

$$x_3 = \lambda^2 - a - x_1 - x_2 \quad \text{e} \quad y_3 = \lambda x_3 + \nu$$

Hemos llegado por tanto a la **Fórmula de adición de puntos**:

$$P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = \left(\lambda^2 - a - x_1 - x_2, -\lambda x_3 - \nu\right) \tag{19}$$

donde λ y ν están dados en (18).

Si $x_1 = x_2$. Tenemos dos opciones: $P_2 = -P_1$ ó $P_2 = P_1$. En el primer caso la suma es trivial, así que suponemos $P_1, = P_2 = P$ y buscamos hallar $2P$. Si P es un punto de orden 2, $2P = \mathcal{O}$ así que podemos suponer que P no es un punto de orden 2. Como veremos en la siguiente sección esto equivale a que $x(P)$ no es una raíz de $f(x)$ y por tanto $y(P) \neq 0$. Ahora la recta $y = \lambda x + \nu$ uniendo P y P es la tangente a E en P. La pendiente no la podemos calcular con la fórmula: $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. En cambio, derivamos implícitamente la expresión $y^2 = f(x)$. Es decir:

$$2y\frac{dy}{dx} = f'(x) \implies \lambda = \left.\frac{dy}{dx}\right|_P = \left.\frac{f'(x)}{2y}\right|_P$$

Si $P = (x, y)$ tenemos:

$$\lambda = \frac{f'(x)}{2y}, \quad \nu = y - \lambda x$$

Observemos que λ está bien definido pues $y \neq 0$ por hipótesis (en los puntos de orden 2 lo que ocurre es que la pendiente es infinita y la tangente es por tanto vertical). Las coordenadas de $2P$ quedan:

$$x(2P) = \lambda^2 - a - 2x, \quad y(2P) = -\lambda x(2P) - \nu \tag{20}$$

Desarrollando estas expresiones y usando que $y^2 = f(x)$ obtenemos las **Fórmulas de duplicación** para $P = (x, y)$:

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4f(x)} \tag{21}$$

$$y(2P) = -\frac{f'(x)}{2y}x(2P) - y + \frac{f'(x)}{2y}x = \frac{f'(x)}{2y}(x - x(2P)) - y \tag{22}$$

Con estas fórmulas podríamos comprobar explícitamente la asociatividad de la ley de grupo, lo cual, aunque supondría una prueba rigurosa, sería un tarea ardua y tediosa. Además nos dan otra forma de mostrar que $E[\mathbb{Q}]$ es un subgrupo de E pues si $P, Q \in E[\mathbb{Q}]$, las coordenadas de $P + Q$ proceden de evaluar funciones de $\mathbb{Q}(x)$ en números racionales.

Definimos una aplicación que usaremos de forma natural en muchas ocasiones, que no es otra que sumar m veces el mismo punto P de E para un $m \in \mathbb{Z}$.

$$\begin{aligned} m\cdot : \quad & E \to E \\ & P \mapsto \underbrace{P + ... + P}_{m \text{ términos}} = mP \end{aligned} \tag{23}$$

Como E es abeliano, esta aplicación es claramente un homomorfismo de grupos. Su núcleo son los puntos de m-torsión (o de orden que divida a m) que estudiaremos en la siguiente sección.

Observación 3.5. *Aplicando sucesivamente la fórmula de duplicación y suma de puntos podemos obtener una expresión explícita para las coordenadas de $mP, m \in \mathbb{Z}$. No la daremos explícitamente, lo importante es que si E es una curva elíptica definida sobre $\mathbb{Q}$, $x(mP)$ e $y(mP)$ son funciones racionales con coeficientes en $\mathbb{Q}$, pues la suma y composición de funciones racionales es una función racional.*

Hagamos un ejemplo. Consideremos la curva elíptica:

$$y^2 = x^3 + 17.$$

Es en efecto no singular, pues su discriminante es $\Delta = -2^4 3^3 17^2 \neq 0$. También miramos dos de sus puntos racionales: $P_1 = (-1, 4)$ y $P_2 = (2, 5)$. La recta que pasa por P_1 y P_2 es:

$$y = \frac{1}{3}x + \frac{13}{3}, \quad \text{luego} \quad \lambda = \frac{1}{3} \quad \text{and} \quad \nu = \frac{13}{3}.$$

Ahora calculamos:

$$x_3 = \lambda^2 - x_1 - x_2 = -\frac{8}{9} \quad \text{y} \quad y_3 = \lambda x_3 + \nu = \frac{109}{27}.$$

Y por tanto:

$$P_1 + P_2 = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

Vemos que hacer cálculos no es tan complicado. Ahora hallemos $2P_1$. La pendiente de la tangente en P_1 es:

$$\lambda = \frac{f'(x_1)}{2y_1} = \frac{f'(-1)}{8} = \frac{3}{8}.$$

Usando que la tangente pasa por P_1 vemos que su ecuación es $y = \frac{3}{8}x + \frac{35}{8}$, luego $\nu = \frac{35}{8}$. Usando las fórmulas de duplicación (21) y (22) para $a = b = 0, c = 17$ obtenemos las coordenadas de $2P_1$:

$$x(2P_1) = \frac{1 + 8 \cdot 17}{4 \cdot 4^2} = \frac{137}{64}$$
$$y(2P_1) = \frac{3}{8}\left(-1 - \frac{137}{64}\right) - 4 = -\frac{2651}{512}.$$

4 Puntos de torsión

Un primer paso para entender el grupo de puntos de una curva elíptica es mediante sus puntos de torsión. Sea $E : y^2 = x^3 + ax^2 + bx + c$ una curva elíptica definida sobre $\mathbb{Q}$.

Definición 4.1. *Dado $m \in \mathbb{Z}_{\geq 0}$, el conjunto de puntos de m-torsión de E es:*

$$E[m] = \left\{P \in E(\overline{\mathbb{Q}}) \mid mP = \mathcal{O}\right\}$$

Es decir, $E[m]$ está formado por los puntos de E cuyo orden divide a m. Si m es primo, $E[m]$ consiste en el del punto $\mathcal{O}$ (de orden 1) y los puntos de orden m. Además $E[m]$ es exactamente el núcleo del homomorfismo *multiplicar por m* definido en (23).

Recordemos que en virtud de la Observación 3.5, si $P = (x, y) \in E$, la primera coordenada de mP es una función racional en x con coeficientes en $\mathbb{Q}$. Una condición equivalente para que $P \in E[m]$ es $(m-1)P = -P$. Como $x(P) = x(-P)$, los puntos de $E[m]$ se encuentran entre aquellos para los que $x(P)$ es una raíz del polinomio que se obtiene al igualar $x((m-1)P) = x$ y multiplicar por el denominador de $x((m-1)P)$. Por tanto $E[m]$ es un conjunto finito (para cada raíz o valor de $x(P)$ solo hay dos valores posibles de y).

En la Definición 4.1 se recuerda que $E[m] \subset E := E(\overline{\mathbb{Q}})$, es decir, que los puntos tienen en general coordenadas sobre un cuerpo algebraicamente cerrado que contenga a $\mathbb{Q}$ (nos vale $\overline{\mathbb{Q}}$, la clausura algebraica de $\mathbb{Q}$), ya que de esta forma obtenemos todos los puntos posibles que cumplan la condición $mP = \mathcal{O}$, al ser esta una condición polinómica.

Como consecuencia inmediata de que el grupo de puntos de la curva elíptica es abeliano, tenemos que los puntos de m-torsión, $E[m]$, forman un subgrupo de E. Queremos estudiar la estructura de grupo de $E[m]$.

Consideremos puntos de orden 2, es decir, aquellos tales que $P = -P$. Con la ecuación en forma $E : y^2 = x^3 + ax^2 + bx + c = f(x)$, esto se traduce en $(x, y) = (x, -y)$. Luego $y = 0$. Si x_1, x_2, x_3 son las raíces (distintas, pues E es no singular) de $f(x)$, entonces los puntos de orden 2 tienen la forma: $(x_i, 0), i = 1, 2, 3$. Además estos 3 puntos cumplen efectivamente $2P = \mathcal{O}$, luego son exactamente los únicos puntos de orden 2 que existen. Por tanto $E[2] = \{\mathcal{O}, (x_1, 0), (x_2, 0), (x_3, 0)\}$, que es un subgrupo de E de orden 4. Luego $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ó $E[2] \cong \mathbb{Z}/4\mathbb{Z}$ (por el teorema de estructura de grupos abelianos finitamente generados). Todos los puntos no triviales tienen orden 2, luego:

$$E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \tag{24}$$

Ahora veamos qué ocurre con $E[3]$. Sus puntos no triviales cumplen que $3P = \mathcal{O}$. Luego verifican $2P = -P$ y por tanto $x(2P) = x$. Recíprocamente, si $x(2P) = x =$

$x(P)$, como y^2 es un polinomio en x, tenemos, $y(2P) = \pm y(P)$, es decir, $2P = \pm P$. Si se diese $2P = P$, implicaría que $P = \mathcal{O}$, lo cual hemos descartado por hipótesis. Luego $2P = -P$ y por tanto los puntos no triviales de orden 3 son exactamente aquellos tales que $x(2P) = x$. Usando la fórmula de duplicación (21) tenemos que $P = (x, y)$ es un punto de orden 3 si y solo si x es una raíz del polinomio:

$$g(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 \tag{25}$$

Afirmamos que $g(x)$ tiene 4 raíces distintas. Para probarlo basta ver que g y g' no tienen raíces en común. Tenemos

$$g'(x) = 12x^3 + 12ax^2 + 12bx + 12c = 12f(x) \tag{26}$$

Recordemos que $x(2P) = \dfrac{f'(x)^2}{4f(x)} - a - 2x$, expresión que vimos en (20) y que está bien definida pues P no es de 2-torsión. Como $f''(x) = 2(3x + a)$, obtenemos otra forma de expresar g:

$$g(x) = 2f(x)f''(x) - f'(x)^2 \tag{27}$$

Si g y g' tienen una raíz común, α, entonces por (26) es también raíz de f, lo que a su vez implica, por (27), que α es raíz de f', lo cual contradice el hecho de que f no tiene raíces múltiples. Luego las raíces de g son distintas.

Por tanto la coordenada x de P puede tomar 4 valores distintos para puntos de orden 3. Para cada uno de estos x hay dos valores de y asociados: $\pm\sqrt{f(x)}$, que son distintos pues $f(x) \neq 0$, ya que de lo contrario serían puntos de orden 2. Luego si denotamos x_1, x_2, x_3, x_4 a las raíces de g, $E[3]$ consta de los ocho puntos $(x_i, \pm\sqrt{f(x_i)}), i = 1, ..., 4$ además del punto $\mathcal{O}$. Es un grupo abeliano de orden 9 donde todo elemento no nulo es de orden 3, luego, de nuevo en virtud del teorema de estructura de grupos abelianos finitamente generados, tenemos:

$$E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

Nosotros solo haremos uso de la estructura de $E[2]$ para probar el Teorema de Mordell, pero en general se tiene:

Proposición 4.2. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ y $m \in \mathbb{Z}_{\geq 1}$. Se tiene:*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Demostración. Podemos encontrar una prueba en [2, Prop. 5.4.a)], que hace uso del bien conocido resultado de que $E(\overline{\mathbb{Q}}) = E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, donde Λ es un retículo. □

En el Apéndice B podemos encontrar más resultados sobre puntos de torsión. No los hemos incluido aquí por agilizar la exposición, pues no nos serán útiles de cara a probar el Teorema de Mordell.

5 E(ℚ) y el Teorema de Mordell

5.1 Alturas y Descenso

Para probar el Teorema de Mordell necesitamos una herramienta muy común en teoría de números: la altura. La altura de un punto de $E(\mathbb{Q})$ nos dirá algo de su *complejidad* aritmética. Comenzamos definiéndola para un número racional.

Definición 5.1. *Sea $x = \frac{m}{n}$ un número racional escrito como fracción irreducible (i.e., $mcd(m,n) = 1$). Definimos la altura de x como:*

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

¿Por qué es un buen medidor de la complejidad numérica de un número racional? Cojamos por ejemplo $\frac{1}{2}$ y $\frac{9999}{20000}$. Ambos tienen prácticamente el mismo valor absoluto, pero el segundo es claramente más complejo que el primero, ya que, por ejemplo, a un ordenador le costaría una mayor cantidad de bits almacenarlo. La siguiente propiedad pone aún más de manifiesto la utilidad de la altura:

Proposición 5.2. *(**Propiedad de finitud**) El conjunto de números racionales con una altura menor que un valor fijado es un conjunto finito.*

Demostración. Dada una constante C, la condición $H\left(\frac{m}{n}\right) < C$ implica $|m| < C$, $|n| < C$, luego solo hay una cantidad finita de posibilidades para m y n. □

En lo que sigue consideraremos $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ una cúbica no singular definida sobre $\mathbb{Q}$ y $P = (\alpha, \beta)$ un punto racional.

Definición 5.3. *Definimos la altura de $P = (\alpha, \beta) \in E(\mathbb{Q})$ como la altura de su primera coordenada:*

$$H(P) = H(\alpha)$$

Por convenio $H(\mathcal{O}) = 1$. Nos interesa tener una función que se comporte aditivamente, luego definimos:

$$h(P) = \log H(P) \tag{28}$$

que es siempre un número no negativo.

Observemos que $E(\mathbb{Q})$ hereda la propiedad de finitud, es decir, dado $M > 0$

$$\#\left\{P \in E(\mathbb{Q}) : H(P) \leq M\right\} < +\infty \tag{29}$$

Esto se debe a que hay solo una cantidad finita de posibilidades para las coordenadas x de los puntos, y para cada una de estas solo hay dos posibles coordenadas y. Obviamente lo mismo se da para $h(P)$.

Nuestro objetivo es demostrar que $E(\mathbb{Q})$ es finitamente generado. Para ello probaremos una serie de lemas sobre las alturas, y con estas herramientas, aplicando un algoritmo de descenso, probaremos el Teorema de Mordell. Por claridad de exposición comenzaremos por este último paso.

Para el siguiente resultado consideraremos Γ un grupo abeliano cualquiera escrito con notación aditiva y

$$h : \Gamma \to [0, +\infty)$$

una función (altura), poniendo así de manifiesto la generalidad del teorema de descenso.

Denotaremos por $m\Gamma$ el subgrupo de Γ formado por los puntos que son sumas de m veces un mismo punto de Γ. Es obviamente un subgrupo, en concreto es la imagen del homomorfismo de grupos:

$$\begin{aligned} m\cdot : \ & \Gamma \to \Gamma \\ & P \mapsto \underbrace{P + ... + P}_{m \text{ términos}} = mP \end{aligned} \tag{30}$$

que en el caso de $\Gamma = E(\mathbb{Q})$ hemos llamado *multiplicar por* m.

Teorema 5.4. *(Teorema de descenso). Sea* Γ *un grupo abeliano y supongamos que existe una función*

$$h : \Gamma \to [0, +\infty)$$

con las siguientes propiedades:

a) Para cada número real M*, el conjunto* $\{P \in \Gamma : h(P) \leq M\}$ *es finito.*

b) Para cada $P_0 \in \Gamma$ *existe una constante* κ_0 *tal que:*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \forall\ P \in \Gamma$$

c) Hay una constante κ *tal que:*

$$h(2P) \geq 4h(P) - \kappa \quad \forall\ P \in \Gamma$$

Además supongamos que:

d) El subgrupo 2Γ *tiene índice finito en* Γ*, (es decir,* $\Gamma/2\Gamma$ *es finito).*

Entonces Γ *es finitamente generado.*

Demostración. Por d) sabemos que hay una cantidad finita, digamos n, de clases de equivalencia en el cociente $\Gamma/2\Gamma$. Sean $Q_1, ..., Q_n$ representantes de estas clases.

Como todo elemento de Γ debe estar en un clase de equivalencia (ie, $\Gamma/2\Gamma = \bigsqcup_{i=1}^{n}(Q_i + 2\Gamma)$), para todo $P \in \Gamma$, existe un índice i_1 que depende de P tal que

$$P - Q_{i_1} \in 2\Gamma.$$

Luego podemos escribir

$$P - Q_{i_1} = 2P_1$$

para algún $P_1 \in \Gamma$. Ahora hacemos lo mismo con P_1 y así sucesivamente, lo que prueba que tenemos igualdades de la forma:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

donde los $Q_{i_1}, ..., Q_{i_m}$ se han escogido de entre los representantes $Q_1, ..., Q_n$ y los P_i son elementos de Γ.

De la primera de estas igualdades tenemos $P_1 = Q_{i_2} + 2P_2$, y sustituyéndolo en $P = Q_{i_1} + 2P_1$ obtenemos $P = Q_{i_1} + 2Q_{i_2} + 4P_2$. Si vamos introduciendo el resto de $P_j = Q_{i_{j+1}} + 2P_{j+1}$ para $j = 2, ..., m-1$ llegamos a:

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + ... + 2^{m-1}Q_{i_m} + 2^m P_m. \tag{31}$$

Esto en particular nos prueba que P está en el subgrupo de Γ generado por los Q_i y por P_m. Vamos a ver que cogiendo un m lo suficientemente grande podemos hacer que la altura de P_m sea menor o igual que una determinada constante que no depende de P. Entonces los Q_i juntos con el conjunto finito de puntos con altura menor que esa constante generaría Γ.

Aplicando b) con $-Q_i$ en lugar de P_0 conseguimos constantes κ_i tales que:

$$h(P - Q_i) \leq 2h(P) + \kappa_i \quad \forall\ P \in \Gamma.$$

Hacemos esto para $i = 1, .., n$ y consideramos $\kappa' = \underset{1 \leq i \leq n}{\text{máx}} \{\kappa_i\}$ de manera que:

$$h(P - Q_i) \leq 2h(P) + \kappa' \quad \forall P \in \Gamma \text{ y } \forall\ 1 \leq i \leq n.$$

Sea P_j uno cualquiera de los puntos de la secuencia $P, P_1, P_2, ...$ Aplicándole c) obtenemos:

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa + \kappa'$$

lo que podemos reescribir como:

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa + \kappa'}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\left(h(P_{j-1}) - (\kappa + \kappa')\right).$$

Luego si $h(P_{j-1}) \geq \kappa + \kappa'$, entonces

$$h(P_j) \leq \frac{3}{4}h(P_{j-1}). \tag{32}$$

Para los puntos P_j compliendo $h(P_{j-1}) \geq \kappa + \kappa'$, tras hacer uso reiterado de (32) conseguimos un $P_m, m > j$, tal que $h(P_m) \leq \kappa + \kappa'$. Hemos probado que podemos escribir cualquier $P \in \Gamma$ de la forma:

$$P = a_1 Q_1 + ... + a_n Q_n + 2^m R$$

para $a_1, ..., a_n \in \mathbb{Z}$ y algún punto $R \in \Gamma$ cumpliendo $h(R) \leq \kappa + \kappa'$. Esto se ha obtenido de (31) usando el m que hemos encontrado y agrupando los coeficientes de las $Q_{i_k}, k = 1, .., m$ en los de su respectiva Q_i. En otras palabras el conjunto:

$$\{Q_1, ..., Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa + \kappa'\}$$

genera Γ y es finito gracias a $a)$ y $d)$. □

Lo hemos llamado Teorema de Descenso porque la prueba es muy similar al método de Fermat de descenso infinito que usó para probar que $x^4 + y^4 = 1$ no tiene soluciones racionales con $xy \neq 0$. Parece ser que este es el método que tenía en mente para probar lo que se conoce como *El último teorema de Fermat*, es decir, que no hay soluciones racionales para $x^n + y^n = 1$ con $xy \neq 0$ para $n \geq 3$, pero complicaciones surgen cuando n se hace grande, y la elaborada prueba que dio Wiles en 1996 va por un camino distinto, aunque usa de manera crucial la teoría de curvas elípticas.

Nuestra intención será aplicar el teorema de descenso (**Teorema 5.4**) para el caso $\Gamma = E(\mathbb{Q})$ y h la función altura (logarítmica) que definimos al comienzo de esta sección. Necesitamos probar que se verifican las hipótesis $b), c), d)$ pues $a)$ ya ha sido probada en (29). Es a esto a lo que dedicaremos las siguientes secciones.

5.2 La altura de $P + P_0$

Comenzaremos con un resultado importante, que nos dirá la forma que tienen los puntos racionales de nuestra curva elíptica. Como ya comentamos, si la curva está definida sobre $\mathbb{Q}$ podemos encontrarle una ecuación con coeficientes en $\mathbb{Z}$.

Lema 5.5. *Sea E una curva elíptica con ecuación $E : y^2 = x^3 + ax^2 + bx + c$, $a, b, c \in \mathbb{Z}$. Si $P = (x, y)$ es un punto racional, entonces:*

$$x = \frac{m}{e^2} \quad e \quad y = \frac{n}{e^3}$$

para enteros m, n y e con $e > 0$ y $\mathrm{mcd}(m, e) = \mathrm{mcd}(n, e) = 1$.

Demostración. Escribamos $x = \frac{m}{M}$ y $y = \frac{n}{N}$ como fracciones irreducibles, con $M, N > 0$. Sustituyendo en la ecuación de la curva obtenemos:

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

que quitando denominadores queda:

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3. \tag{33}$$

Como N^2 es un factor de todos los términos de la derecha, también lo es del de la izquierda, luego $N^2|M^3n^2$, pero como $\mathrm{mcd}(n, N) = 1$ se tiene $N^2|M^3$.

Buscamos probar ahora el recíproco, es decir, $M^3|N^2$. De (33) vemos que $M|N^2m^3$, lo cual, usando que $\mathrm{mcd}(m, M) = 1$, implica $M|N^2$. Volviendo a usar esto en (33) tenemos que $M^2|N^2m^3$, es decir, $M^2|N^2$ y por tanto $M|N$. Usando de nuevo esto en (33) obtenemos $M^3|N^2m^3$, luego $M^3|N^2$.

Hemos probado que $M^3 = N^2$ además de $M|N$. Sea $e = N/M$. Entonces

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \text{ y } e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N.$$

Por tanto $x = m/e^2$ e $y = n/e^3$ y $\mathrm{mcd}(m, e) = 1 = \mathrm{mcd}(n, e)$, pues m es coprimo con M y n lo es con N. □

Antes de dar la prueba del resultado principal de esta sección, necesitamos observar lo siguiente sobre la altura de un punto racional $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, dado con fracciones irreducibles. Se tiene $H(P) = \max\{|m|, e^2\}$, es decir:

$$|m| \leq H(P) \text{ y } e^2 \leq H(P).$$

Podemos acotar también n en función de $H(P)$. En concreto existe $K > 0$ constante dependiendo de a, b y c tal que:

$$|n| \leq KH(P)^{3/2} \quad \forall\ P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q}).$$

Para probar esto sustituimos P en la ecuación de la curva y multiplicamos por e^6, lo que da:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

Y por tanto:

$$\begin{aligned}\left|n^2\right| \leq \left|m^3\right| + \left|ae^2m^2\right| + \left|be^4m\right| + \left|ce^6\right| &\leq H(P)^3 + |a|\, H(P)^3 + |b|\, H(P)^3 + |c|\, H(P^3) \\ &= (1 + |a| + |b| + |c|)H(P^3)\end{aligned}$$

Luego nos basta tomar $K = \sqrt{1 + |a| + |b| + |c|}$ para tener el resultado.

Lema 5.6. *Dado $P_0 \in E(\mathbb{Q})$ existe una constante κ_0 que depende de P_0, a, b y c tal que:*

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \forall\ P \in E(\mathbb{Q}).$$

Demostración. La prueba no es más que escribir la fórmula para la suma de dos puntos y usar la desigualdad triangular con los datos que ya tenemos. Antes observemos que si $P_0 = \mathcal{O}$ la desigualdad es trivial, así que asumiremos $P_0 \neq \mathcal{O}$, digamos, $P_0 = (x_0, y_0)$. Además para probar la existencia de κ_0 nos basta hacerlo excepto para un conjunto finito de puntos, pues para los $P = (x, y)$ de este conjunto finito, podemos mirar las diferencias $h(P + P_0) - 2h(P)$ y tomar κ_0 mayor que todas ellas. Dicho esto vamos a probar el lema para $P \notin \{P_0, -P_0, O\}$. Con esto conseguimos $x \neq x_0$, principalmente para evitar usar la fórmula de duplicación. Escribimos:

$$P + P_0 = (\xi, \eta).$$

Necesitamos calcular la altura de ξ, y para ello usamos la fórmula (19) que hallamos en la **Sección 2**

$$\xi + x + x_0 = \lambda^2 - a, \quad \text{donde} \quad \lambda = \frac{y - y_0}{x - x_0}.$$

Escribimos ξ más explícitamente:

$$\xi = \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0 = \frac{(y - y_0)^2 - (x - x_0)^2(a + x + x_0)}{(x - x_0)^2}$$

Desarrollamos el numerador y vemos que aparece $y^2 - x^3$. Usando que P cumple la ecuación de nuestra curva sustituimos $y^2 - x^3$ por $ax^2 + bx + c$. Así acabamos con una expresión de la forma:

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

donde $A, B, ..., G$ son números racionales que dependen de a, b, c, x_0 e y_0. Multiplicando numerador y denominador por el mínimo común múltiplo de los denominadores de $A, B, ..., G$, podemos suponer que estos números son enteros.

Ahora sustituimos $x = m/e^2$ e $y = n/e^3$ y eliminamos denominadores multiplicando denominador y numerador de nuestra expresión por e^4 resultando en:

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}.$$

Ya tenemos ξ como cociente de enteros, aunque no necesariamente como fracción irreducible, pero esto no importa, porque cancelar factores en numerador y denominador solo puede provocar que disminuya la altura, luego:

$$H(\xi) \leq \text{máx}\left\{\left|Ane + Bm^2 + Cme^2 + De^4\right|, \left|Em^2 + Fme^2 + Ge^4\right|\right\}.$$

Recordemos que:

$$e \leq H(P)^{1/2}, \quad |n| \leq KH(P)^{3/2}, \quad \text{y} \quad |m| \leq H(P)$$

donde K dependía solo de a, b y c. Usando ahora la desigualdad triangular obtenemos:

$$\begin{aligned}\left|Ane + Bm^2 + Cme^2 + De^4\right| &\leq |Ane| + \left|Bm^2\right| + \left|Cme^2\right| + \left|De^4\right| \\ &\leq (|AK| + |B| + |C| + |D|)\, H(P)^2\end{aligned}$$

y

$$\left|Em^2 + Fme^2 + Ge^4\right| \leq \left|Em^2\right| + \left|Fme^2\right| + \left|Ge^4\right| \leq (|E| + |F| + |G|)\, H(P)^2.$$

Luego

$$H(P + P_0) = H(\xi) \leq \text{máx}\left\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\right\} H(P)^2$$

lo que tomando logaritmos nos da:

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

donde

$$\kappa_0 = \log \text{máx}\left\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\right\}$$

depende solo de a, b, c y (x_0, y_0) pero no de $P = (x, y)$. □

5.3 La altura de $2P$

Enunciamos directamente lo que queremos probar:

Lema 5.7. *Existe una constante κ, que depende de a, b y c tal que:*

$$h(2P) \geq 4h(P) - \kappa \quad \forall\ P \in E(\mathbb{Q})$$

Demostración. Tal y como hicimos en la prueba del Lema 5.6, podemos ignorar un conjunto finito de puntos, pues siempre podemos tomar κ mayor que $4h(P)$ para todos los puntos P de dicho conjunto. En este caso vamos a ignorar los puntos de orden 2, es decir aquellos cuya coordenada x es una raíz de $f(x) = x^3+ax^2+bx+c$.

Sea $P = (x, y)$ y escribamos $2P = (\xi, \eta)$. Cuando hablamos de la duplicación de un punto en la **Sección 2** teníamos:

$$\xi + 2x = \lambda^2 - a \quad \text{donde} \quad \lambda = \frac{f'(x)}{2y}$$

y usando que $y^2 = f(x)$ llegábamos a:

$$\xi = \frac{f'(x)^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

que está bien definido pues $2P \neq \mathcal{O}$ y por tanto $f(x) \neq 0$. Como nuestra cúbica es no singular, f y f' no tienen raíces comunes sobre $\mathbb{C}$, luego el numerador y denominador de ξ son polinomios sin raíces comunes y que además podemos considerar con coeficientes enteros tras multiplicar numerador y denominador por el mínimo común denominador de a, b y c.

Como $h(\xi) = h(2P)$ y $h(x) = h(P)$, lo que queremos probar se enuncia como:

$$h(\xi) \geq 4h(x) - \kappa.$$

Por lo tanto nos basta probar el siguiente lema sobre alturas y cocientes de polinomios, que no tiene nada que ver con curvas elípticas.

Lema 5.8. *Sea $\phi(x)$ y $\psi(x)$ polinomios con coeficientes enteros y sin raíces complejas comunes. Sea d el máximo de los grados de ϕ y ψ.*

a) Existe $R \in \mathbb{Z}_{\geq 1}$, que depende de ϕ y ψ, tal que para todos número racional m/n:

$$mcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \text{ divide a } R.$$

b) Existen constantes κ_1 y κ_2, dependientes de ϕ y ψ, tales que para todo número racional m/n que no sea raíz de ψ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi\left(m/n\right)}{\psi\left(m/n\right)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Demostración. *a*) Primero observamos que como los grados de ϕ y ψ son a lo más d, $n^d\phi\left(\frac{m}{n}\right)$ y $n^d\psi\left(\frac{m}{n}\right)$ son enteros y podemos hablar de su máximo común divisor. Además en este apartado el papel de ϕ y ψ es intercambiable, luego podemos

suponer sin pérdidad de generalidad que $\deg(\phi) = d$ y $\deg(\psi) = e \leq d$. Para facilitar la notación escribiremos:

$$\Phi(m,n) = n^d \phi\left(\frac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} n + ... + a_d n^d$$
$$\Psi(m,n) = n^d \psi\left(\frac{m}{n}\right) = b_0 m^e n^{d-e} + b_1 m^{e-1} n^{d-e+1} + ... + b_e n^d.$$

Como $\phi(X)$ y $\psi(X)$ no tienen raíces comunes, son coprimos en el dominio euclídeo $\mathbb{C}[X]$ y por tanto en $\mathbb{Q}[X]$. Luego usando la identidad de Bézout en $\mathbb{Q}[X]$ (o equivalentemente teniendo en cuenta que generan el ideal total), existen polinomios $F(X)$ y $G(X)$ con coeficientes racionales satisfaciendo:

$$F(X)\phi(X) + G(X)\psi(X) = 1. \tag{34}$$

Sea A un múltiplo de los denominadores de los coeficientes de F y G, de manera que $AF(X)$ y $AG(X)$ tienen coeficientes enteros. Sea D el máximo de los grados de F y G. Notemos que A y D no dependen de m o n.

Ahora evaluamos $X = m/n$ en (34) y multiplicamos la ecuación por An^{D+d}, obteniendo así:

$$An^D F\left(\frac{m}{n}\right) n^d \phi\left(\frac{m}{n}\right) + An^D G\left(\frac{m}{n}\right) n^d \psi\left(\frac{m}{n}\right) = An^{D+d}.$$

Sea $\gamma = \gamma(m,n)$ el máximo común divisor de $\Phi(m,n)$ y $\Psi(m,n)$. Tenemos:

$$\left[An^D F\left(\frac{m}{n}\right)\right] \Phi(m,n) + \left[An^D G\left(\frac{m}{n}\right)\right] \Psi(m,n) = An^{D+d}$$

y como las cantidades entre corchetes son enteros, γ divide a An^{D+d}. Pero necesitamos que divida a un entero fijo que no dependa de n. Por eso afirmamos que γ divide Aa_0^{D+d}. Para verlo notemos que como γ divide $\Phi(m,n)$, también divide a:

$$An^{D+d-1}\Phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + ... + Aa_d n^{D+2d-1}.$$

En la suma todos los términos menos el primero tienen a An^{D+d} como factor, y como $\gamma \mid An^{D+d}$, también debe dividir al primer término $= Aa_0 m^d n^{D+d-1}$. Es decir, γ divide al $\operatorname{mcd}\left(An^{D+d}, Aa_0 m^d n^{D+d-1}\right)$. Pero teniendo en cuenta que m y n son coprimos se tiene:

$$\operatorname{mcd}\left(An^{D+d}, Aa_0 m^d n^{D+d-1}\right) = An^{D+d-1}\operatorname{mcd}\left(n, a_0 m^d\right) = An^{D+d-1}\operatorname{mcd}\left(n, a_0\right)$$

y por tanto $\gamma \mid Aa_0 n^{D+d-1}$. Observemos que hemos reducido el exponente de n a cambio de multiplicar por a_0.

Teniendo en cuenta que $\gamma \mid Aa_0 n^{D+d-2}\Phi(m,n)$, tras repetir el mismo argumento y usando que hemos probado que $\gamma \mid Aa_0 n^{D+d-1}$ obtendremos que $\gamma \mid Aa_0^2 n^{D+d-2}$.

Así, iterando el proceso ($D+d$ veces) llegamos eventualmente a la conclusión de que $\gamma \mid Aa_0^{D+d}$, como queríamos probar.

b) De nuevo podemos excluir un conjunto finito de puntos racionales para probar una desigualdad de este tipo. Así que asumimos que m/n no es una raíz de ϕ. Además si r es un racional no nulo, está claro por la definición de altura que: $h(r) = h(1/r)$, luego podemos intercambiar los papeles de ϕ y ψ y sin pérdida de generalidad asumimos $\deg(\phi) = d$ y $\deg(\psi) = e \leq d$ al igual que en a. Queremos estimar la altura de

$$\xi = \frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{n^d\phi\left(\frac{m}{n}\right)}{n^d\psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}$$

$H(\xi)$ sería el máximo de los enteros $\Phi(m,n)$ y $\Psi(m,n)$ excepto por posibles cancelaciones de factores comunes.

La cota superior es sencilla y su prueba similar a la del Lema 5.6. Recordemos que $|m|, |n| \leq H(m/n)$. Por tanto:

$$\begin{aligned}
|\Phi(m,n)| &\leq |a_0|\left|m^d\right| + |a_1|\left|m^{d-1}n\right| + ... + |a_d|\left|n^d\right| \\
&\leq (|a_0| + |a_1| + ... + |a_d|)\, H(m/n)^d, \\
|\Psi(m,n)| &\leq |b_0|\left|m^e n^{d-e}\right| + |b_1|\left|m^{e-1}n^{d-e+1}\right| + ... + |b_e|\left|n^d\right| \\
&\leq (|b_0| + |b_1| + ... + |b_e|)\, H(m/n)^d.
\end{aligned}$$

Luego tomando:

$$C_2 = \max\left(|a_0| + |a_1| + ... + |a_d|, |b_0| + |b_1| + ... + |b_e|\right) > 0$$

tenemos que:

$$H(\xi) \leq C_2 H(m/n)^d$$

y tomando logaritmos:

$$h(\xi) = h\left(\frac{\phi\,(m/n)}{\psi\,(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2, \quad \text{con} \quad \kappa_2 = \log\left(C_2\right)$$

que es lo que queríamos probar.

Procedamos ahora a probar la cota inferior. En *a*) probamos que existe un entero $R \geq 1$, independiente de m y n tal que $\gamma = \operatorname{mcd}\left(\Phi(m,n), \Psi(m,n)\right)$ divide a R. Esto nos acota las cancelaciones de manera que:

$$\begin{aligned}
H(\xi) &\geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\
&= \frac{1}{R}\max\left\{\left|n^d\phi\left(\frac{m}{n}\right)\right|, \left|n^d\psi\left(\frac{m}{n}\right)\right|\right\} \\
&\geq \frac{1}{2R}\left(\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right).
\end{aligned}$$

En la última línea hemos usado el hecho trivial de que máx$\{a, b\} \geq \frac{1}{2}(a + b)$. Queremos comparar $H(\xi)$ con:

$$H\left(\frac{m}{n}\right)^d = \text{máx}\left\{|m|^d, |n|^d\right\}$$

así que tomamos el cociente de ambos:

$$\begin{aligned}\frac{H(\xi)}{H(m/n)^d} &\geq \frac{n^d}{2R} \cdot \frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\text{máx}\left\{|m|^d, |n|^d\right\}} \\ &= \frac{1}{2R} \cdot \frac{\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\text{máx}\left\{\left|\frac{m}{n}\right|^d, 1\right\}}.\end{aligned}$$

Lo que nos sugiere que miremos la función de variable real:

$$p(t) = \frac{|\phi(t)| + |\psi(t)|}{\text{máx}\left\{|t|^d, 1\right\}}.$$

Observemos que es una función siempre positiva. Como ϕ tiene grado d y ψ tiene grado a lo más d, $p(t)$ tiene límite no nulo cuando $|t| \to \infty$. Este límite es $|a_0|$ si el grado de ψ es estrictamente menor que d, o $|a_0| + |b_0|$ si el grado de ψ es también d. En cualquier caso, fuera de un intervalo cerrado y acotado I la función $p(t)$ está acotada inferiormente por un número mayor que cero. Pero en el compacto I la función p es continua y no tiene ceros pues ϕ y ψ no tienen raíces comunes. Luego alcanza su máximo y mínimo en I, que deben ser por tanto valores estrictamente positivos. Hemos acotado inferiormente por una cantidad positiva la función $p(t)$ tanto dentro como fuera de I, es decir, $\exists\, C_1 > 0$ tal que $\forall\, t \in \mathbb{R}$ se tiene $p(t) \geq C_1$. Antes probamos que:

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R} \cdot p\left(\frac{m}{n}\right)$$

y usando $p(t) \geq C_1$ llegamos a:

$$H(\xi) \geq \frac{C_1}{2R} \cdot H\left(\frac{m}{n}\right)^d.$$

Las constantes C_1 y R depende de ϕ y ψ pero no de m y n, luego tomando logaritmos llegamos a la desigualdad deseada:

$$h(\xi) \geq dh\left(\frac{m}{n}\right) - \kappa_1 \quad \text{con} \quad \kappa_1 = \log\left(2R/C_1\right).$$

□

Recordemos que esto nos prueba como caso particular el Lema 5.7. □

5.4 Versión débil del Teorema de Mordell-Weil

Para completar la prueba del teorema de Mordell, necesitamos mostrar lo siguiente:

Teorema 5.9. *El grupo $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.*

Esto es un caso particular del resultado conocido como versión débil del Teorema de Mordell-Weil:

Teorema 5.10. *(Mordell-Weil débil). Sea K un cuerpo numérico. Entonces $E(K)/mE(K)$ es finito.*

Para probar la versión general (5.10) hay que usar herramientas de teoría algebraica de números que quedan fuera del alcance y las intenciones de este trabajo. Una prueba se puede encontrar en [2, §VIII.1, Thm 1.1]. Nosotros probaremos (5.9), es decir fijaremos $K = \mathbb{Q}$ y $m = 2$.

Vamos a mirar los números racionales *módulo cuadrados*, es decir como elementos de:

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 = \left\{ \frac{m}{n} : m \neq 0, \operatorname{mcd}(m,n) = 1, m \text{ y } n \text{ libre de cuadrados} \right\}$$

Esto equivale a mirar el numerador y denominador de cada fracción (irreducible) como su radical (parte libre de cuadrados), pues cualquier entero que sea un cuadrado vale 1 en $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Lema 5.11. *Sea $E : y^2 = x^3 + ax^2 + bx$ con $a, b, c \in \mathbb{Z}$ una curva elíptica y sea $(x, y) \in E(\mathbb{Q})$. Entonces módulo cuadrados solo hay una cantidad finita de valores posibles para x.*

Demostración. Por el Lema 5.5, $x = m/e^2, y = n/e^3$, para algunos $m, n, e \in \mathbb{Z}$ con $\operatorname{mcd}(m, e) = \operatorname{mcd}(n, e) = 1$. Nos interesa la parte libre de cuadrados de m. Introduciendo en la ecuación de E y eliminando denominadores queda:

$$n^2 = m\left(m^2 + ame^2 + be^4\right)$$

Luego el lado derecho es también un cuadrado. Sea $d = \operatorname{mcd}(m, m^2 + ame^2 + be^4)$. Como $d \mid m$ y $d \mid m^2 + ame^2 + be^4$ se tiene $d \mid be^4$. Y como $\operatorname{mcd}(m, e) = 1$ tenemos $d \mid b$. Deducimos por tanto que $\operatorname{mcd}(m, b) = d$. Luego los primos que dividen x visto como un elemento de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ están entre la cantidad finita de primos que divide a b. □

5.4.1 Versión débil del Teorema de Mordell-Weil para $m = 2$ y $K = \mathbb{Q}$

Nuestro objetivo es probar que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. Para ello vamos a definir un morfismo desde $E(\mathbb{Q})$ con núcleo $2E(\mathbb{Q})$ e imagen finita y el Primer Teorema de Isomorfía nos garantizaría el resultado. Trabajaremos exclusivamente con $\mathbb{Q}$ como cuerpo base.

Durante toda esta sección consideramos $E : y^2 = f(x) = x^3 + Ax + B$ una curva elíptica definida sobre $\mathbb{Q}$ y por tanto $f(x)$ es separable. Sin pérdida de generalidad podemos considerar que $A, B \in \mathbb{Z}$ gracias a la Proposición 2.14 y a la Observación 2.2, pues como vimos el cambio de variable que nos permite hacer esta suposición deja invariante $E(\mathbb{Q})$.

Comenzamos definiendo:

$$R = \mathbb{Q}[\xi] = \mathbb{Q}[x]/(f(x))$$

donde ξ es la clase de x en el cociente. Denotamos por $R^\times$ su grupo de unidades, que son los residuos módulo $f(x)$ de los $h(x) \in \mathbb{Q}[x]$ que sean coprimos con $f(x)$. Por el Teorema Chino del Resto tenemos:

$$R \cong \prod_{i=1}^{n} \mathbb{Q}[x]/\left(f_i(x)\right) \tag{35}$$

donde los $f = \prod_{i=1}^{n} f_i$ es la descomposición de irreducibles de f en $\mathbb{Q}[x]$ y $n = 1, 2$ ó 3 dependiendo de si f tiene $0, 1$ o todas las raíces en $\mathbb{Q}$ respectivamente.

Observación 5.12. *1) Recordemos que el producto de anillos coincide con el producto cartesiano dotado de estructura de anillo con las operaciones componente a componente.*

2) $R^\times$ es isomorfo al producto del grupo de unidades de cada factor. Escribamos esto más explícitamente y así fijamos notación para el futuro. Denotamos:

$$R_i = \mathbb{Q}[x]/\left(f_i(x)\right) = \mathbb{Q}(\theta_i)$$

que es una extensión de $\mathbb{Q}$ de grado igual al grado de f_i. De nuevo θ_i es la imagen de x en el respectivo cociente, o, con una interpretación que nos será más útil después, θ_i es una de las raíces del polinomio mónico irreducible f_i.

Sea $R_i^\times = R_i - \{0\}$ *su grupo de unidades. Se tiene entonces:*

$$R \cong \prod_{i=1}^{n} R_i \cong \prod_{i=1}^{n} \mathbb{Q}(\theta_i) \tag{36}$$

$$R^\times \cong \prod_{i=1}^{n} R_i^\times \cong \prod_{i=1}^{n} \mathbb{Q}(\theta_i)^\times \tag{37}$$

$$R^\times / \left(R^\times\right)^2 \cong \prod_{i=1}^{n} R_i^\times / \left(R_i^\times\right)^2 \tag{38}$$

Decimos algo más de cada caso y establecemos notación para cada uno a continuación.

Caso 1: El polinomio $f(x)$ no tiene ninguna raíz en $\mathbb{Q}$ y por tanto es irreducible en $\mathbb{Q}[x]$ por tener grado 3. Por ser $\mathbb{Q}[x]$ un dominio euclídeo, es un dominio de ideales principales y por tanto un dominio de factorización única. Luego todo ideal primo es maximal y todo irreducible es primo. Es decir $f(x)$ es primo en $\mathbb{Q}[x]$, $(f(x))$ es un ideal primo y por tanto maximal. Por tanto R es un cuerpo y $R^\times = R \setminus \{0\}$.

Caso 2: f tiene una única raíz $\alpha \in \mathbb{Q}$. Luego factoriza como

$$f(x) = (x - \alpha)g(x)$$

donde $g(x)$ es cuadrático, mónico e irreducible sobre $\mathbb{Q}[x]$. La expresión (35) queda en este caso:

$$R \cong \frac{\mathbb{Q}[x]}{(x-\alpha)} \times \frac{\mathbb{Q}[x]}{(g(x))}.$$

El primer factor es isomorfo a $\mathbb{Q}$ y el segundo es una extensión de $\mathbb{Q}$ de grado 2.

Caso 3: f tiene dos raíces en $\mathbb{Q}$ y por tanto tiene las tres. Luego existe $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$ distintos entre sí tales que $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$. La expresión (35)nos dice que R es de la forma:

$$R \cong \frac{\mathbb{Q}[x]}{(x-\alpha_1)} \times \frac{\mathbb{Q}[x]}{(x-\alpha_2)} \times \frac{\mathbb{Q}[x]}{(x-\alpha_3)} \cong \mathbb{Q}^3.$$

Pasamos a construir ahora el morfismo ϕ que mencionamos al principio de esta subsección.

Si $P = \mathcal{O}$ definimos $\phi(P) = 1$.

Si $P = (\alpha, \beta) \in E(\mathbb{Q})$ no es un punto de 2-torsión (i.e., α no es raíz de f), entonces $x - \alpha$ es coprimo con $f(x)$ y por tanto $\xi - \alpha$ es una unidad en $\mathbb{Q}[\xi]$. Luego tiene sentido definir $\phi(P) = \xi - \alpha \left(\mathrm{mod}\,(R^\times)^2\right)$. Es decir, entendemos la imagen en $R^\times / (R^\times)^2$.

Si $P = (\alpha, 0)$ es un punto racional de orden 2, entonces $f(x) = (x - \alpha)g(x)$ en $\mathbb{Q}[x]$ y tenemos:

$$\mathbb{Q}[\xi] \cong \mathbb{Q}[x]/(x - \alpha) \times \mathbb{Q}[x]/(g(x)) \tag{39}$$

donde $g(x) \in \mathbb{Q}[x]$ es de grado 2 no necesariamente irreducible (es decir podemos estar en el caso 2 o el caso 3 de la discusión anterior). En esta situación definimos $\phi(P) = (f'(\alpha), x - \alpha \pmod{g(x)})$. Teniendo en mente la Observación 5.12, 2), $\phi(P)$ vuelve a ser una unidad pues lo es en cada uno de los dos factores. En el primero porque $f'(\alpha) \neq 0$, por ser el polinomio separable. En el segundo porque $x - \alpha$ es coprimo con $g(x)$. Luego $(f'(\alpha), x - \alpha \pmod{g(x)}) = h(\xi)$ para algún $h(\xi) \in R^\times / (R^\times)^2$.

Observación 5.13. *Hemos tenido que cambiar la definición en el primer factor de R porque $\xi - \alpha$ ya no sería una unidad en él. En el segundo factor tomamos módulo $g(x)$ y no todo el polinomio $f(x)$. Es por eso que no escribimos ξ en lugar de x.*

Resumimos a continuación la definición.

Definición 5.14. *Definimos la aplicación:*

$$\phi : E(\mathbb{Q}) \to R^\times / \left(R^\times\right)^2$$
$$\phi(\mathcal{O}) = 1$$
$$\phi(\alpha, \beta) = \begin{cases} \xi - \alpha & , \text{ si } \beta \neq 0 \\ (f'(\alpha), x - \alpha \pmod{g(x)}) & , \text{ si } f(\alpha) = 0 \text{ y donde } g(x) := \dfrac{f(x)}{x - \alpha} \end{cases}$$

Ahora vemos dos propiedades muy importantes de esta aplicación.

Proposición 5.15. *Sea ϕ la aplicación definida en (5.14). Se tiene:*

1) ϕ es un morfismo de grupos.

2) $\ker \phi = 2E(\mathbb{Q})$.

Demostración. 1) Si $P = (\alpha, \beta)$, como la definición de ϕ es independiente de β se tiene

$$\phi(P) = \phi(-P) \tag{40}$$

identidad que se mantiene trivialmente para $P = \mathcal{O}$. Nos basta mostrar que si $A, B, C \in E(\mathbb{Q})$ son colineales, es decir si

$$A + B + C = \mathcal{O} \implies C = -(A + B) \tag{41}$$

se tiene

$$\phi(A)\phi(B)\phi(C) = 1 \tag{42}$$

ya que entonces tendríamos

$$\phi(A + B) \overset{(40)}{=} \phi(-(A + B)) \overset{(41)}{=} \phi(C) \overset{(42)}{=} (\phi(A)\phi(B))^{-1} = \phi(A)\phi(B) \tag{43}$$

En la última igualdad hemos usado que para todo $\rho \in R^{\times}/\left(R^{\times}\right)^2$ se tiene $\rho^2 = 1$, es decir todo elemento es su propio inverso.

Si uno de los puntos A, B, C es $\mathcal{O}$, digamos $C = \mathcal{O}$, entonces probar (42) es trivial, pues (41) nos dice $B = -A$ y, usando $\phi(A) = \phi(-A)$ se tiene

$$\phi(A)\phi(B)\phi(C) = \phi(A)\phi(-A) = \phi(A)^2 = 1.$$

Por tanto podemos escribir $A = (x_1, y_1), B = (x_2, y_2), C = (x_3, y_3)$.

Si $x_1 = x_2$, la condición de colinealidad (41) nos dice que, o bien A es de orden dos y por tanto $B = -A, C = \mathcal{O}$, caso que ya hemos probado, o bien A no es de orden 2 y los puntos son $A, A, -2A$. En este último caso vemos que:

$$\phi(A)\phi(A)\phi(-2A) = \phi(2A)$$

luego solo tendríamos que probar que $\phi(2A)$ es un cuadrado en R para demostrar (42), pero esto se tiene usando la fórmula de duplicación (21) que nos da explicitamente $x(2A)$ como una función racional de x_1.

Supongamos ahora $x_1 \neq x_2$. Hay 3 casos:

Primero supongamos que ninguno de los puntos A, B, C es de orden 2. Entonces la condición de colinealidad (41) y el hecho de que $x_1 \neq x_2$ nos garantiza que existe una recta $y = mx + n$ no vertical, conteniendo a A, B, C tal que:

$$f(x) - (mx + n)^2 = (x - x_1)(x - x_2)(x - x_3). \tag{44}$$

Ahora tomando (44) módulo $f(x)$ y viendo sus elementos en $R^{\times}/\left(R^{\times}\right)^2$ se llega a:

$$1 = (\xi - x_1)(\xi - x_2)(\xi - x_3) = \phi(A)\phi(B)\phi(C)$$

que es el resultado deseado.

Supongamos ahora que $A = (\alpha, 0)$ tiene orden 2, y conservamos la notación para los otros puntos, que no son de orden 2. Verificamos el resultado

para cada una de las dos componentes en (39). En el segundo factor tenemos el resultado tras tomar (44) módulo $g(x)$ y mirar la expresión módulo cuadrados:

$$1 = (x-\alpha)(x-x_2)(x-x_3) \bmod g(x) = \overline{(x-\alpha)}\,\overline{(x-x_2)}\,\overline{(x-x_3)} = \phi(A)\phi(B)\phi(C).$$

Hemos denotado con una barra superior la clase módulo $g(x)$ por simplicidad. Observemos que aunque B y C no dan problemas en la primera componente (esta sigue siendo $(x - x_i)$ módulo $(x - \alpha), i = 2, 3$) y podemos mirar por separado la segunda componente de $\phi(B)$ y $\phi(C)$ que sigue siendo $x - x_i$ módulo $g(x), i = 2, 3$.

Derivando con respecto a x la expresión (44) y sustituyendo $x = \alpha$ deducimos $f'(\alpha) = (\alpha - x_2)(\alpha - x_3)$. Además $\phi(x_i, y_i) = x - x_i \equiv \alpha - x_i \pmod{x-\alpha}, i = 2, 3$. Luego

$$\phi(A)\phi(B)\phi(C) = (\alpha - x_2)(\alpha - x_3)(\alpha - x_2)(\alpha - x_3) = \left(f'(\alpha)\right)^2 = 1.$$

Por último nos falta comprobar que (42) se verifica cuando $A = (\theta_1, 0), B = (\theta_2, 0), C = (\theta_3, 0)$ son todos puntos de orden 2 (pues si dos de ellos lo son, (41) nos dice que el tercero también). De nuevo, derivando (44) y sustituyendo $x = \theta_i$ tenemos $f'(\theta_i) = \prod_{\substack{j=1 \\ j\neq i}}^{3} (\theta_i - x_j)$ y por tanto en la componente i tenemos:

$$\phi(A)\phi(B)\phi(C) = \left(\prod_{j=1, j\neq i}^{3} (\theta_i - x_j) \right)^2 = \left(f'(\theta_i)\right)^2 = 1.$$

2) Ahora veamos que $\ker \phi = 2E(\mathbb{Q})$. Para esta prueba es clave que E venga dada por una ecuación del tipo $y^2 = x^3 + ax + b, a, b \in \mathbb{Q}$, la cual siempre podíamos conseguir mediante un cambio de variables.

Para todo $P \in E(\mathbb{Q})$ se tiene $\phi(2P) = \phi(P)^2 = 1$, luego $2E(\mathbb{Q}) \subset \ker \phi$.

Sea ahora $\mathcal{O} \neq P = (\alpha, \beta) \in \ker \phi$ y veamos que $P \in 2E(\mathbb{Q})$. Primero notemos que $\phi(P) = 1 \implies \phi(P)$ es un cuadrado en R, luego lo debe ser en todas sus componentes (recordemos que $1 \in R^\times$ es $\bigoplus_{i=1}^{n} 1$ donde cada 1 es el elemento neutro del respectivo factor en (37)). Con estas hipótesis vamos a probar que la cantidad $\xi - \alpha$ es un cuadrado en R.

Si $\beta \neq 0$ (i.e., $f(\alpha) \neq 0$), entonces $\xi - \alpha$ es exactamente $\phi(P)$ y el resultado se tiene porque $\phi(P) = 1$.

Si $\beta = 0$, es porque α es raíz de f. Entonces $\phi(P) = (f'(\alpha), x - \alpha(\mathrm{mod}\, g(x)))$ donde $f(x) = (x-\alpha)g(x)$. A su vez, $x - \alpha \pmod{g(x)}$ podría mirarse como una sola componente o como dos, dependiendo de si $g(x)$ es o no irreducible sobre $\mathbb{Q}[x]$ respectivamente. Pero eso no nos importa. Solo nos importa que $x - \alpha \pmod{g(x)}$ es un cuadrado (o, de nuevo, producto de dos cuadrados) en $\mathbb{Q}[x]/(g(x))$.

La cantidad $\xi - \alpha$, también la miramos como un elemento de

$$\mathbb{Q}[\xi] \cong \mathbb{Q}[x]/(x-\alpha) \times \mathbb{Q}[x]/(g(x))$$

y queda,

$$\xi - \alpha = (0, x - \alpha \pmod{g(x)})$$

siendo nula la primera componente porque se corresponde con
$x - \alpha \pmod{x - \alpha}$, que es 0. Es decir, la primera componente de $\xi - \alpha$ es un cuadrado, y antes mostramos que $x - \alpha \pmod{g(x)}$ también es un cuadrado en $\mathbb{Q}[x]/(g(x))$. Luego $\xi - \alpha$ es un cuadrado por serlo en todas sus componentes.

Como en $\mathbb{Q}[\xi]$ se tiene $f(\xi) = 0$, $\mathbb{Q}[\xi]$ es $\mathbb{Q}$-espacio vectorial con base $\{1, \xi, \xi^2\}$ y podemos escribir

$$\xi - \alpha = \left(\alpha_1\xi^2 + \alpha_2\xi + \alpha_3\right)^2 \tag{45}$$

con $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. En R tenemos $\xi^3 = -a\xi - b$, lo que implica:

$$\left(\alpha_1\xi^2 + \alpha_2\xi + \alpha_3\right)(-\alpha_1\xi + \alpha_2) = e_1\xi + f_1 \tag{46}$$

para algunos $e_1, f_1 \in \mathbb{Q}$, pues todos los coeficientes implicados en la izquierda de la ecuación son racionales y término de grado 2 se anula. Observemos que $\alpha_1 \neq 0$ pues de lo contrario en (45) tendríamos $\xi - \alpha = \alpha_2^2\xi^2 + 2\alpha_2\alpha_3\xi + \alpha_3^2$ y la independencia lineal de $1, \xi, \xi^2$ nos llevaría a contradicción.

Ahora elevando al cuadrado (46) y usando (45) llegamos a:

$$(\xi - \alpha)(-\alpha_1\xi + \alpha_2)^2 = (e_1\xi + f_1)^2$$

y dividiendo entre $\alpha_1^2 \neq 0$ queda:

$$(\lambda\xi + \nu)^2 = (\xi - \alpha)(\xi - h)^2 \tag{47}$$

donde $h = \alpha_2/\alpha_1 \in \mathbb{Q}$ y $\lambda, \nu \in \mathbb{Q}$. Esto implica que el polinomio
$(x - \alpha)(x - h)^2 - (\lambda x + \nu)^2$ es un múltiplo de $f(x)$, y como ambos son polinomios mónicos cúbicos se tiene:

$$f(x) = (x - \alpha)(x - h)^2 - (\lambda x + \nu)^2$$

Geométricamente hablando, esto quiere decir que la recta $y = \lambda x + \nu$ corta transversalmente a E en (α, β) (o en $(\alpha, -\beta)$ porque esta ecuación solo involucra la coordenada x) y es tangente a E en (h, t) donde $t = \lambda h + \nu \in \mathbb{Q}$. Tenemos entonces:

$$(\alpha, \pm\beta) + 2(h, t) = 0$$

y escogemos el signo adecuado para β usando la ecuación de la recta. Esto quiere decir que:

$$P = (\alpha, \beta) = 2Q$$

donde $Q = (h, \mp t) \in E(\mathbb{Q})$, escogiendo para t el signo contrario que escogimos para β. Luego hemos probado que $\ker \phi \subset 2E(\mathbb{Q})$ y por tanto $\ker \phi = 2E(\mathbb{Q})$.

□

Por el Primer Teorema de Isomorfía tenemos

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong \phi(E(K)) \subset R^\times / \left(R^\times\right)^2$$

luego solo nos hace falta probar que la imagen de ϕ es finita. Para ello es necesario que tengamos muy en mente la Observación 5.12. Recordemos que podemos expresar R como la suma directa de los cuerpos $R_i = \mathbb{Q}(\theta_i) = \mathbb{Q}[x]/(f_i(x))$ y la imagen $\phi(E(\mathbb{Q}))$, que es un subgrupo de $R^\times / \left(R^\times\right)^2$ puede ser vista como suma directa de subgrupos de cada $R_i^\times / \left(R_i^\times\right)^2$, gracias a (38). Nos basta entonces probar que la i-ésima componente de $\phi(P)$ es un subgrupo finito de $R_i^\times / \left(R_i^\times\right)^2$. Además podemos obviar la imagen de los puntos de 2-torsión pues hay una cantidad finita.

Hacemos un pequeño paréntesis para probar un caso particular del Teorema de Mordell, que aunque no usaremos en la prueba final, se expondrá por su sencillez.

Proposición 5.16. *Sea $\tilde{E} : y^2 = \tilde{f}(x) = (x - x_1)(x - x_2)(x - x_3)$ una curva elíptica de manera que las raíces de $\tilde{f}$ son racionales, i.e. $\tilde{E}[2] \subset \tilde{E}(\mathbb{Q})$. Entonces $\tilde{E}(\mathbb{Q})/2\tilde{E}(\mathbb{Q})$ es finito.*

Demostración. Sin pérdida de generalidad podemos suponer que una de las raíces de $\tilde{f}$ es 0, es decir, que $(0, 0)$ es uno de lo puntos de orden 2. Pues si $x_i \neq 0, i = 1, 2, 3$, entonces haciendo $f(x) = \tilde{f}(x + x_1)$, ahora la curva

$$E : y^2 = f(x) = x^3 + ax^2 + bx \tag{48}$$

tiene a $(0, 0)$ como punto de 2 torsión y obviamente es isomorfa a la original. Es más, $\tilde{E}(\mathbb{Q}) \cong E(\mathbb{Q})$ pues el cambio de variable $(x, y) \mapsto (x + x_1, y)$ es racional. También podemos suponer como de costumbre que $a, b, c \in \mathbb{Z}$, haciendo el cambio de variable (14), el cual mantenía isomorfo $E(\mathbb{Q})$, y no perdemos la forma de la ecuación (48).

Tenemos que mostrar que $\phi(E) \subset R^\times / (R^\times)^2$ es finito. Como $E[2] \subset E(\mathbb{Q})$, tenemos

$$R = \mathbb{Q}[x]/(f(x)) \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$$

así que pensamos en la imagen de ϕ como un subconjunto de

$$\left(\mathbb{Q}^\times / (\mathbb{Q}^\times)^2\right) \times \left(\mathbb{Q}^\times / (\mathbb{Q}^\times)^2\right) \times \left(\mathbb{Q}^\times / (\mathbb{Q}^\times)^2\right).$$

Si $P = (\alpha, \beta) \in E$, teniendo en cuenta la definición de ϕ, podemos mirar $\phi(P)$ en la componénte i-ésima como un elemento de $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ (ya valga $f'(\alpha)$ si $f(\alpha) = 0$, o $x - \alpha \mod(x - x_i)$ en caso contrario). Pero por el Lema 5.11 solo hay una cantidad finita de valores posibles para α módulo cuadrados, lo que completa la prueba de este caso particular. □

Aquí termina el paréntesis y continuamos con la prueba general.

Para simplificar la notación en lo que resta de sección escribiremos $K = \mathbb{Q}(\theta_i) = \mathbb{Q}[x]/(f_i(x))$ y trabajaremos en la componente i-ésima de (38), sin que importe en cuál, pues al no considerar los puntos de 2-torsión, ϕ se comporta igual en todas.

Sea $P \in E(\mathbb{Q})$ un punto racional que no sea de 2 torsión. El Lema 5.5 nos dice que $P = (\frac{m}{e^2}, \frac{n}{e^3})$ para enteros m, n y e, con $e > 0$ y $\text{mcd}(m, e) = \text{mcd}(n, e) = 1$. Sea $\theta = \theta_i$ una raíz fija de f_i, de manera que $K = \mathbb{Q}[\theta]$. Observemos que θ es un entero algebraico de K, ya que $f \in \mathbb{Z}[x]$. Podemos entonces escribir $f(x) = (x - \theta)g(x)$ con $g(x)$ mónico de grado 2. Veamos que $g \in (\mathbb{Z}[\theta])[x] \subset K[x]$. Para ello realizamos la división de $f(x) = x^2 + Ax + B$ entre $x - \theta$ y usando que $f(\theta) = 0$ obtenemos:

$$g(\theta) = x^2 + \theta x + (A + \theta^2) \in (\mathbb{Z}[\theta])[x]$$

como queríamos. Con esta notación se tiene que las cantidades

$$m - e^2\theta \quad \text{y} \quad h_P := g(m/e^2)e^4$$

son enteros algebraicos sobre K, pues ambas están en $\mathbb{Z}[\theta] \subset \mathcal{O}_K$. (Véase la Observación 1.13).

Definición 5.17. *Para todo $P = (m/e^2, n/e^3) \in E(\mathbb{Q})$ que no sea un punto de 2-torsión definimos el ideal:*

$$I(P) = \left(m - e^2\theta, h_P\right) \subset \mathcal{O}_K.$$

Lema 5.18. *El conjunto de ideales:*

$$\{I(P) | P \in E(\mathbb{Q}), P \notin E[2]\}$$

es finito, donde $I(P)$ son los ideales definidos en (5.17).

Demostración. Conservando la notación de la discusión previa a la Definición 5.17 tenemos

$$\begin{aligned} g(x) - g(\theta) &= x^2 + x\theta + (A + \theta^2) - 2\theta^2 - (A + \theta^2) \\ &= (x - \theta)(x + 2\theta). \end{aligned}$$

Sustituyendo $x = m/e^2$ y multiplicando por e^4 llegamos a:

$$g(\theta)e^4 = h_P - (m - e^2\theta)(m + 2\theta e^2).$$

Luego $g(\theta)e^4 \in I(P)$. De manera similar tenemos:

$$\begin{aligned} g(\theta)x^2 - g(x)\theta^2 &= g(\theta)\left(x^2 - \theta^2\right) + \theta^2(g(\theta) - g(x)) \\ &= (x - \theta)(g(\theta)(x + \theta) - \theta^2(x + 2\theta) \\ &= (x - \theta)((2\theta^2 + A)x - B) \\ &= (x - \theta)t(x) \end{aligned}$$

con $t(x) \in (\mathbb{Z}[\theta])[x]$ de grado 1. Sustituyendo de nuevo por $x = m/e^2$ y multiplicando por e^4 obtenemos:

$$g(\theta)m^2 = (m - e^2\theta)t(m/e^2)e^2 + \theta^2 g(m/e^2)e^4 \implies g(\theta)m^2 \in I(P).$$

Luego $(g(\theta)m^2, g(\theta)e^4) \subset I(P)$. Como $\text{mcd}(m^2, e^4) = 1$, existe $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha m^2 + \beta e^4 = 1$. Entonces $g(\theta) = \alpha g(\theta)m^2 + \beta g(\theta)e^4 \in (g(\theta)m^2, g(\theta)e^4)$, lo cual implica que $(g(\theta)) \subset (g(\theta)m^2, g(\theta)e^4) \subset I(P)$. Es decir, $I(P)$ divide a $(g(\theta))$ $\forall$ P. Como $\mathcal{O}_K$ es un dominio de Dedekind, por el Corolario 1.18 solo puede haber una cantidad finita de divisores de $(g(\theta))$, y por tanto de ideales $I(P)$. □

Lema 5.19. *Siguiendo con la notación precedente, $K = \mathbb{Q}(\theta)$. Para todo $P = (m/e^2, n/e^3) \in E(\mathbb{Q}) \setminus E[2]$ se tiene $(m - e^2\theta) = I(P)C^2$ para un ideal C de $\mathcal{O}_K$.*

Demostración. Teniendo en cuenta el Corolario 1.18 y su prueba, por ser $\mathcal{O}_K$ un dominio de Dedekind existen ideales: A y B coprimos (es decir, al factorizarlos como producto de ideales primos, no tienen ningún factor en común) tales que $(m - e^2\theta) = I(P)A$ y $h_P = I(P)B$. $P \in E(\mathbb{Q})$ luego tenemos:

$$n^2/e^6 = (m/e^2 - \theta)g(m/e^2) \iff n^2 = (m - e^2\theta)g(m/e^2)e^4 = (m - e^2\theta)h_P$$

y en términos de ideales

$$(n^2) = I(P)^2 AB.$$

Como A y B son coprimos, y a la izquierda tenemos un ideal al cuadrado, tanto A como B deben ser el cuadrado de algún ideal de $\mathcal{O}_K$, aunque nos basta con A. Es decir, existe C tal que $C^2 = A$, luego $(m - e^2\theta) = I(P)C^2$. □

Lema 5.20. *Hay un conjunto finito de enteros algebraicos $S \subset \mathcal{O}_K$ tal que para todo $P = (m/e^2, n/e^3) \in E(\mathbb{Q})$ podemos escribir:*

$$m - e^2\theta = u\gamma\tau^2$$

para unos adecuados $u \in \mathcal{O}_K$ unidad, $\tau \in K$, y $\gamma \in S$.

Demostración. Recordemos que el grupo de clases de ideales de $\mathcal{O}_K$ es finito. Sean $C_1, ..., C_r$ representantes de las clases de ideales, de manera que todo ideal de $\mathcal{O}_K$ es equivalente a alguno de ellos mediante la relación $\sim$ definida en (1.23). Dado $P \in E(\mathbb{Q})$ que no sea de 2-torsión, sea C un ideal de $\mathcal{O}_K$ de manera que se verifique el Lema 5.19. Como hay una cantidad finita de $I(P)$ por el Lema 5.18, también podemos coger una cantidad finita de estos C. Entonces existe $s \in \{1, ..., r\}$ tal que $C \sim C_s$ es decir, $\exists\ \tau_1, \tau_2 \in \mathcal{O}_K$ no nulos tales que $(\tau_1)C = (\tau_2)C_s$. Luego $I(P)C_s^2 \sim I(P)C^2 = (m - e^2\theta)$, es decir, $I(P)C_s^2$ es equivalente a un ideal principal, luego es principal, digamos, (γ), con $\gamma \in \mathcal{O}_K$. Para cada una de las expresiones $I(P)C$, de las cuales hay una cantidad finita, cogemos un $\gamma \in \mathcal{O}_K$ y formamos así el conjunto finito S del enunciado. Poniendo todo esto junto tenemos:

$$(\tau_1^2(m - e^2\theta)) = I(P)(\tau_2^2)C_s^2 = (\gamma\tau_2^2).$$

Como el ideal principal de la izquierda y la derecha son iguales, sus generadores son asociados. Por tanto $\exists\ u \in \mathcal{O}_K$ unidad tal que:

$$\tau_1^2(m - e^2\theta) = u\gamma\tau_2^2$$

Y el resultado sigue tras tomar $\tau = \tau_2/\tau_1$ que está en en el cuerpo de fracciones de $\mathcal{O}_K$, pero este no es más que K, gracias a la Proposición 1.14. □

Ahora podemos probar la finitud de $E(\mathbb{Q})/2E(\mathbb{Q})$.

Teorema 5.21. *El grupo $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.*

Demostración. Como ya dijimos, nos basta probar que la imagen $\phi(E(\mathbb{Q}))$ es finita en los factores $R_i^\times / \left(R_i^\times\right)^2$ de (38) y podemos excluir la imagen de los puntos de 2-torsión pues son una cantidad finita. Si $P = (m/e^2, y)$, tenemos $\phi(P) = \xi - m/e^2 \pmod{(R^\times)^2}$, donde denotábamos $\xi = x + (f(x))$, la clase de x en R. Y si miramos en la componente i-ésima: $K := R_i = \mathbb{Q}(\theta)$ de $R = \mathbb{Q}[x]/(f(x))$, la respectiva componente de ϕ vale $\theta - m/e^2$. El lema anterior nos dice que en $R_i^\times / \left(R_i^\times\right)^2$, se tiene $\theta - m/e^2 = -1(m/e^2 - \theta) = (1/e^2)u\gamma\tau^2 \equiv u\gamma \pmod{\left(R_i^\times\right)^2}$, donde γ está en un conjunto finito S de enteros algebraicos que depende de la curva E y no de P, y u es una unidad de $\mathcal{O}_K$. Por el Teorema de las Unidades de Dirichlet

(1.27), el grupo de unidades de $\mathcal{O}_K$ es finitamente generado con base, digamos, $u_1, .., u_t$. Entonces módulo $(R^\times)^2, \phi(P)$ tiene un representante de la forma:

$$u_1^{\epsilon_1} u_2^{\epsilon_2} ... u_t^{\epsilon_t} \gamma$$

donde cada ϵ_i es 0 ó 1. Como hay una cantidad finita de γ, también hay una cantidad finita de estas expresiones, lo que concluye el resultado. □

Observación 5.22. *La mayor parte de la prueba y las discusiones en esta subsección se podrían haber hecho con un cuerpo K de característica cero cualquiera en vez de $\mathbb{Q}$, e intentar conseguir la finitud de $E(K)/2E(K)$. Pero lo que ha hecho la prueba relativamente sencilla y accesible es que hayamos podido usar que los puntos racionales son de una determinada forma: Lema 5.5. Además, como ya comentamos, el resultado solo se mantiene si K es un cuerpo numérico, aunque la prueba requiere herramientas considerablemente más avanzadas de teoría algebraica de números.*

Habiendo probado que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito, ya podemos aplicar el Teorema de Descenso 5.4 a $E(\mathbb{Q})$, finalizando así la prueba del Teorema de Mordell.

A Apéndice: De cúbicas a formas de Weierstrass en característica 0.

Vamos a describir un procedimiento general para llevar una cúbica a su forma de Weierstrass en el caso de que esté definida sobre un cuerpo de característica 0. Luego daremos un ejemplo concreto para ilustrar dicho procedimiento.

Para el lector conocedor de algo de terminología de geometría algebraica, lo que vamos a mostrar es que toda cúbica es birracionalmente equivalente a una dada por una ecuación de Weiertrass, y por tanto también es isomorfa. Esto es debido a que, aunque ser isomorfas es en general una condición más fuerte que ser birracionalmente equivalentes, en el caso de curvas planas proyectivas no singulares, los dos conceptos coinciden. (Para una prueba de este hecho véase [2, Ch. II, §2, Proposition 2.1]). A continuación, damos el procedimiento que mencionamos.

1. Sea $\mathcal{O}$ un punto no singular cualquiera de C vista en $\mathbb{P}^2(\overline{K})$. Tomamos la tangente a C en $\mathcal{O}$. Este será nuestro eje $Z = 0$ en nuestro nuevo sistema coordenado.

2. Sea Q la intersección de la curva C con el eje $Z = 0$. Si $\mathcal{O}$ no es un punto de inflexión de C tomamos el eje $X = 0$ como la tangente a C en Q, pues en este caso $Q \neq \mathcal{O}$ y los ejes $Z = 0$ y $X = 0$ son distintos. Si $\mathcal{O}$ fuese un punto de inflexión de C, lo que ocurre es que $Q = \mathcal{O}$ pues la recta $Z = 0$ corta a C en $\mathcal{O}$ con orden 3, luego no la corta en ningún otro sitio (por ser C una cúbica y a consecuencia del Teorema de Bézout). En este caso tomamos $X = 0$ como cualquier recta que no pase por $\mathcal{O}$.

   Con esta elección de coordenadas el punto Q tiene coordenadas homogéneas $Q = [0, 1, 0]$.

   Estos pasos quedan ilustrados en la Figura 14.

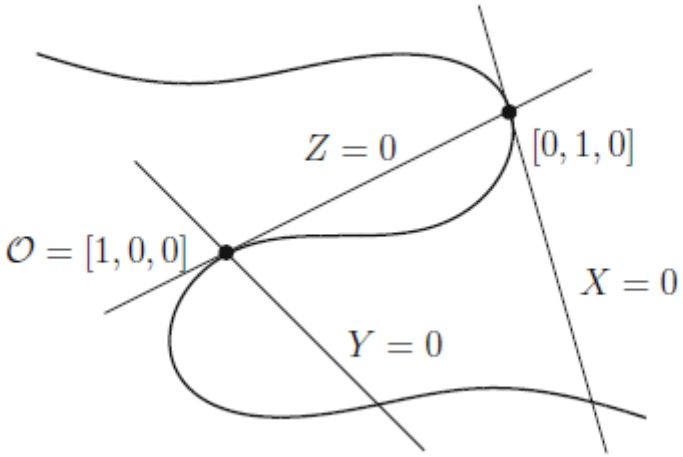

Figura 14: Escogiendo ejes para poner C en forma de Weierstrass

3. Finalmente cogemos $Y = 0$ como cualquier recta, distinta de $X = 0$ que pase por $\mathcal{O}$. Ahora $\mathcal{O}$ tiene coordenadas $[1, 0, 0]$.

4. Tras esta transformación, que es un ejemplo de transformación proyectiva, nuestra curva tiene ecuación $C : F(X, Y, Z) = 0$ y contiene a los puntos $\mathcal{O} = [1, 0, 0]$ y $Q = [0, 1, 0]$. Vamos a seguir denotando C a la curva obtenida con cada transformación que hagamos, para no complicar la notación.

   Como F es un polinomio cúbico homogéneo tiene la forma:

   $$F(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eZ \cdot G(X, Y, Z)$$

   con a, b, c, d no todos nulos y G es un polinomio homogéneo de grado 2. Vamos a mostrar que $a = b = d = 0$.

   a) Como $\mathcal{O} = [1, 0, 0] \in C$ se tiene $F(1, 0, 0) = a = 0$
   b) Como $Q = [0, 1, 0] \in C$ se tiene $F(0, 1, 0) = d = 0$
   c) La recta $Z = 0$ corta a la curva C dos veces en $\mathcal{O}$ y una vez en Q. Esta intersección está dada por la ecuación $F(X, Y, 0) = 0$, y teniendo en cuenta que ya sabemos que $a = d = 0$, esto se traduce en:

      $$bX^2Y + cXY^2 = XY(bX + cY) = 0.$$

      Cada factor lineal se corresponde con un punto de intersección. Por tanto Q satisface $X = 0$ y $\mathcal{O}$ satisface $Y = 0$ y $bX + cY = 0$, luego $b = 0$.

Por tanto el polinomio F en nuestro nuevo sistema de coordenadas tiene la forma:

$$F(X,Y,Z) = cXY^2 + eZ \cdot G(X,Y,Z), \quad c \neq 0$$

y tras deshomogeneizar (haciendo $Z = 1$) y dividir entre $c \neq 0$ obtenemos:

$$f(x,y) = xy^2 + ax^2 + bxy + cy^2 + dx + ey + g = 0 \tag{49}$$

cuyo único término de grado 3 es xy^2.

5. Escribimos la ecuación como:

$$f(x,y) = (x+c)y^2 + ax^2 + bxy + dx + ey + g = 0.$$

Nótese que estamos rehusando los nombres de los coeficientes por simplicidad. Cada vez que hacemos un cambio, los nuevos coeficientes son polinomios en los anteriores. Luego si los anteriores estuviesen en K, los nuevos lo seguirían estando.

Ahora hacemos el cambio de variable $x + c \to x$ y renombramos los coeficientes, resultando en:

$$xy^2 + (ax+b)y = cx^2 + dx + e.$$

A continuación multiplicamos por x:

$$(xy)^2 + (ax+b)xy = cx^3 + dx^2 + ex.$$

Ahora le damos un nuevo nombre a xy, por simplicidad lo llamaremos de nuevo y, y obtenemos:

$$y^2 + (ax+b)y = cx^3 + dx^2 + ex.$$

6. Haciendo la sustitución $y \mapsto y - \dfrac{1}{2}(ax-b)$, válida pues $\mathrm{char}(K) \neq 2$ obtenemos:

$$y^2 = \text{cúbica en } x.$$

La cúbica en x puede no tener coeficiente líder 1. Sea λ su coeficiente líder. La sustitución $(x,y) \mapsto (\lambda x, \lambda^2 y)$ convierte el polinomio cúbico en mónico resultando en una ecuación de la forma:

$$y^2 = x^3 + ax^2 + bx + c, \quad a,b,c,d \in K$$

que es la forma de Weierstrass deseada.

Podemos eliminar el término ax^2 en la anterior ecuación con la sustitución $x \mapsto x - a/3$ ($\text{char}(K) \neq 3$) para obtener su forma de Weierstrass reducida $y^2 = x^3 + Ax + B, \quad A, B \in K$.

Ahora ilustramos este procedimiento con el ejemplo:

$$C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0 \text{ y el punto } \mathcal{O} = [1, 1, 1].$$

Antes de empezar, recordemos que El Teorema de Euler nos dice que si $F(X, Y, Z)$ es un polinomio homogéneo de grado n entonces:

$$\underline{X} \cdot \nabla F(\underline{X}) = nF(\underline{X})$$

donde $\underline{X} = (X, Y, Z)$. Es decir

$$\frac{\partial F}{\partial x} \cdot X + \frac{\partial F}{\partial y} \cdot Y + \frac{\partial F}{\partial z} \cdot Z = nF(X, Y, Z). \tag{50}$$

Recordando la Definición 2.6, la tangente a la curva : $F(X, Y, Z) = 0$, en un punto $P_0 = [X_0, Y_0, Z_0] \in \mathbb{P}^2$ de la misma, viene dada en principio por el polinomio lineal homogéneo:

$$\frac{\partial F}{\partial X}(P_0)(X - X_0) + \frac{\partial F}{\partial Y}(P_0)(Y - Y_0) + \frac{\partial F}{\partial Z}(P_0)(Z - Z_0) = 0.$$

Evaluando la expresión (50) en P_0 vemos que:

$$\frac{\partial F}{\partial x}(P_0) \cdot X_0 + \frac{\partial F}{\partial y}(P_0) \cdot Y_0 + \frac{\partial F}{\partial z}(P_0) \cdot Z_0 = nF(X_0, Y_0, Z_0) = 0.$$

Y por tanto la recta tangente en P_0 viene dada por el polinomio lineal homogéneo:

$$\frac{\partial F}{\partial X}(P_0) X + \frac{\partial F}{\partial Y}(P_0) Y + \frac{\partial F}{\partial Z}(P_0) Z = 0 \tag{51}$$

Ahora procedemos con nuestra curva C. Un buen primer paso sería mover el punto $\mathcal{O}$ a al punto $[1, 0, 0]$. Para ello hacemos las sustituciones

$$X_1 = X, \quad Y_1 = Y - X, \quad Z_1 = Z - X$$

que transforma la ecuación de C en:

$$C : X_1^2 Y_1 + 6X_1 Y_1^2 + 2Y_1^3 + 5X_1^2 Z_1 - 7X_1 Y_1 Z_1 + 12X_1 Z_1^2 + 4Z_1^3 = 0.$$

Usando (51) vemos que la tangente a C en $\mathcal{O} = [1, 0, 0]$ es $Y_1 - 5Z_1 = 0$. De acuerdo a la Figura 14, queremos que esta tangente sea el nuevo eje $Z = 0$. Así que hacemos la sustitución:

$$X_2 = X_1, \quad Y_2 = Y_1, \quad Z_2 = Y_1 - 5Z_1$$

que nos da la ecuación

$$C : 635X_2Y_2^2 + 254Y_2^3 - 125X_2^2Z_2 + 55X_2Y_2Z_2 - 12Y_2^2Z_2 \\ + 60X_2Z_2^2 + 12Y_2Z_2^2 - 4Z_2^3 = 0.$$

Ahora la tangente en $\mathcal{O} = [1, 0, 0]$ es $Z_2 = 0$. Para hallar la tercera intersección de esta recta con C, sustituimos $Z_2 = 0$ en su ecuación y obtenemos $127Y_2^2\,(5X_2 + 2Y_2) = 0$. Luego el tercer punto de intersección es

$$\mathcal{O} * \mathcal{O} = [2, -5, 0].$$

Siguiendo nuestro procedimiento general, queremos mover este punto a $[0, 1, 0]$. Para ello hacemos el cambio de variable

$$X_3 = 5X_2 + 2Y_2, \quad Y_3 = Y_2, \quad Z_3 = Z_2$$

y obtenemos

$$C : 127X_3Y_3^2 - 5X_3^2Z_3 + 31X_3Y_3Z_3 - 54Y_3^2Z_3 + 12X_3Z_3^2 - 12Y_3Z_3^2 - 4Z_3^3 = 0.$$

La tangente a C en $[0, 1, 0]$ se calcula ahora fácilmente y es $127X_3 - 54Z_3 = 0$. Queremos que este sea el nuevo eje $X = 0$ sin mover el punto $\mathcal{O} = [1, 0, 0]$ y el eje $Z = 0$. Por ello hacemos las sustituciones

$$X_4 = 127X_3 - 54Z_3, \quad Y_4 = Y_3, \quad Z_4 = Z_3$$

que transforman la ecuación de C en:

$$C : 16129X_4Y_4^2 - 5X_4^2Z_4 + 3937X_4Y_4Z_4 + 984X_4Z_4^2 \\ + 19050Y_4Z_4^2 + 32000Z_4^3 = 0.$$

Ya casi hemos terminado. Ahora deshomogeneizamos la anterior ecuación haciendo $x_5 = X_4/Z_4, y_5 = Y_4/Z_4$ y obtenemos

$$C : 3200 + 984x_5 - 5x_5^2 + 19050y_5 + 3937x_5y_5 + 16129x_5y_5^2 = 0.$$

Ahora multiplicamos por x_5 y hacemos el cambio $x_6 = x_5, y_6 = x_5y_5$, lo que nos da

$$C : 3200x_6 + 984x_6^2 - 5x_6^3 + 19050y6 + 3937x_6y_6 + 16129y_6^2 = 0.$$

Para conseguir que el coeficiente de x_6 sea 1 y el de y_6 sea 4 hacemos la sustitución $x_7 = 20x_6, y_7 = 2540y_6 = 4 \cdot 5 \cdot 127y_6$. Obtenemos

$$C : 256000x_7 + 3936x_7^2 - x_7^3 + 12000y_7 + 124x_7y_7 + 4y_7^2 = 0.$$

Finalmente completamos el cuadrado en y_7 haciendo

$$x = x_7 \quad \text{and} \quad y = 2y_7 + 31x_7 + 3000$$

lo que nos deja la ecuación de C en forma de Weierstrass[5]

$$C : y^2 = x^3 - 2975x^2 - 70000x + 9000000.$$

Componiendo todas las sustituciones que hemos ido haciendo, vemos que la transformación que nos lleva la ecuación original

$$C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0$$

a la forma de Weierstrass que hemos hallado está dada por las fórmulas

$$\begin{aligned} x &= \frac{100(33X + 40Y + 54Z)}{4X + Y - 5Z} \\ y &= \frac{-63500\,(6X^2 - 7XY - 18Y^2 + 21XZ - 14YZ + 12Z^2)}{(4X + Y - 5Z)^2}. \end{aligned}$$

Además podemos apreciar que dichas fórmulas son funciones racionales en X, Y, Z. Es decir, como dijimos en el procedimiento general, la curva original no es solo birracionalmente equivalente a la curva en forma de Weierstrass, sino también isomorfa.

[5]Si además hacemos el cambio de variables $(x, y) = (25x_0, 125y_0)$ la ecuación de Weierstrass queda con coeficientes considerablemente más pequeños: $y_0^2 = x_0^3 - 119x_0^2 - 112x_0 + 576$.

B Apéndice: Más resultados sobre los puntos de torsión.

Consideramos como siempre una curva elíptica $y^2 = f(x) = x^3 + ax^2 + bx + c$ definida sobre $\mathbb{Q}$ y recordemos que podemos considerar que sus coeficientes son enteros haciendo un cambio de variable.

Definición B.1. *Denotamos por E_{tors} el conjunto formado por todos los puntos de orden finito de E, también llamado conjunto puntos de torsión. Análogamente definimos $E(\mathbb{Q})_{tors}$ como los puntos de orden finito de $E(\mathbb{Q})$.*

Observación B.2. *Sin más que tener en cuenta que E es un grupo abeliano, vemos que E_{tors} es subgrupo de E y $E(\mathbb{Q})_{tors}$ es subgrupo de $E(\mathbb{Q})$.*

Si queremos definirlos formalmente escribimos:

$$E_{\text{tors}} = \bigcup_{m=1}^{\infty} [m]$$
$$E(\mathbb{Q})_{\text{tors}} = \bigcup_{m=1}^{\infty} E(\mathbb{Q})[m]$$

donde entendemos que $E[1] = \{\mathcal{O}\}$.

Tenemos el siguiente sorprendente resultado:

Proposición B.3. *Sea $E : y^2 = x^3+ax^2+bx+c$ con $a, b, c \in \mathbb{Z}$ una curva elíptica. Si $(x, y) \in E(\mathbb{Q})_{tors}$, entonces $x, y \in \mathbb{Z}$. Es decir, los puntos racionales de torsión tienen coordenadas enteras.*

Demostración. Una prueba muy elemental puede encontrarse claramente expuesta en [1, Ch. 2,§4]. □

Este resultado compone la parte más importante del conocido como Teorema de Nagell-Lutz.

Proposición B.4. *(Teorema de Nagell-Lutz) Sea $E : y^2 = f(x) = x^3+ax^2+bx+c$ una cúbica no singular con $a, b, c \in \mathbb{Z}$. Sea D el discriminante del polinomio cúbico $f(x)$,*

$$D = \frac{\Delta}{16} = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Sea $P = (x, y) \in E(\mathbb{Q})_{tors}$ un punto racional de orden finito. Entonces $x, y \in \mathbb{Z}$ y, o bien $y = 0$ y entonces P es de orden 2, o bien $y \mid D$.

Demostración. [1, Ch.2,§5, Theorem 2.5] □

Como consecuencia del Nagell-Lutz vemos que $E(\mathbb{Q})_{\text{tors}}$ es finito, pues solo hay una cantidad finita de divisores del entero D que sirvan como coordenadas y de los puntos de $E(\mathbb{Q})_{\text{tors}}$, y para cada una de estos valores de y hay a lo más tres valores de x.

Pero a nosotros no nos hace falta el Teorema de Nagell-Lutz para probar que $E(\mathbb{Q})_{\text{tors}}$ es finito. Podemos usar el Teorema de Mordell, que ya hemos probado. Es decir, sabemos que $E(\mathbb{Q})$ es finitamente generado. El Teorema de Estructura de Grupos Abelianos Finitamente Generados nos dice entonces que:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}} \tag{52}$$

donde los p_i son primos distintos y esta descomposición es única (salvo orden de los factores) y unívocamente determinada por $E(\mathbb{Q})$, ergo por E.

El subgrupo $\mathbb{Z}_{p_1^{\nu_1}} \oplus \mathbb{Z}_{p_2^{\nu_2}} \oplus \cdots \oplus \mathbb{Z}_{p_s^{\nu_s}}$ se corresponde con el subgrupo de puntos de orden finito de $E(\mathbb{Q})$, es decir, $E(\mathbb{Q})_{\text{tors}}$, y es claramente finito. Más concretamente su orden es $p_1^{\nu_1}...p_s^{\nu_s}$. Podemos por tanto escribir

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}. \tag{53}$$

El entero r en (52) y (53) es el **rango** del grupo $E(\mathbb{Q})$. Es el número de copias de $\mathbb{Z}$ que contiene. Una observación sencilla al respecto es que

$$E(\mathbb{Q}) \text{ es infinito} \iff r \geq 1.$$

Es un problema abierto si el rango de una curva elíptica puede ser arbitrariamente grande. La curva elíptica con el rango más grande conocido fue dada por Noam Elkies en 2006 y su ecuación es:

$$E : y^2 + xy + y = x^3 - x^2 + b + c$$

para

$$\begin{aligned} b &= -20067762415575526585033208209338542750930230312178956502, \\ c &= 3448161179503055646703298569039056974855944359319180361 \\ &\quad 266008296291939448732243429 \end{aligned}$$

y solo se conoce que $\text{rank}(E(\mathbb{Q})) \geq 28$, pero no su rango exacto.

En luz del la Proposición B.3, tiene sentido reducir las coordenadas de los puntos de torsión racionales módulo p. Usaremos $(\tilde{x}, \tilde{y})$ para denotar (x, y) con las coordenadas vistas módulo p. En general, cuando reduzcamos un entero k módulo p lo denotaremos por $\tilde{k}$.

Seguimos considerando $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ una curva elíptica con coeficientes enteros. Para computar el subgrupo de torsión de $E(\mathbb{Q})$ nos convendrá

a veces considerar la curva sobre $\mathbb{F}_p$ para $p \geq 3$ primo, es decir $\tilde{E} : y^2 = \tilde{f}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$. Las fórmulas de duplicación y adición siguen teniendo sentido, pero no siempre obtenemos otra curva elíptica al reducir los coeficientes de una curva elíptica módulo p. Necesitamos que $x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}$ tenga raíces distintas para que $\tilde{E}$ sea no singular. Decimos E tiene *buena reducción* para p si este es el caso y que tiene *mala reducción* si no lo es.

Sea $D = \dfrac{\Delta}{16} = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ el discriminante del polinomio cúbico f. Es un polinomio en los coeficientes de f, y por tanto tomar discriminante y reducir módulo p conmutan. Es decir, $\tilde{D}$ es el discriminante de $\tilde{f}$. Por tanto tenemos las siguientes condiciones equivalentes para que $\tilde{E}$ sea no singular:

$$\tilde{f} \text{ tiene raíces distintas} \iff p \nmid D \iff \tilde{D} \neq 0.$$

Tenemos el siguiente resultado, que además supone una tercera forma de demostrar que $E(\mathbb{Q})_{\text{tors}}$ es finito.

Teorema B.5. *Sea p un primo tal que que E tiene buena reducción en p. Entonces la aplicación*

$$\phi : E(\mathbb{Q})_{tors} \to \tilde{E}(\mathbb{F}_p), \quad \mathcal{O} \mapsto \tilde{\mathcal{O}}, \quad (x, y) \mapsto (\tilde{x}, \tilde{y})$$

es un morfismo de grupos inyectivo, y por tanto $E(\mathbb{Q})_{tors}$ es isomorfo a un subgrupo de $\tilde{E}(\mathbb{F}_p)$.

Demostración. Comenzamos viendo que ϕ es un morfismo. Observemos que

$$\phi(-P) = \phi(x, -y) = (\tilde{x}, -\tilde{y}) = -\phi(P)$$

Por tanto, para probar $\phi(P + Q) = \phi(P) + \phi(Q)$, nos basta ver que si $P = (x_1, y_1), Q = (x_2, y_2), R = (x_3, y_3) \in E(\mathbb{Q})_{\text{tors}}$ estan alineados (suman $\mathcal{O}$) entonces

$$\phi(P) + \phi(Q) + \phi(R) = \tilde{P} + \tilde{Q} + \tilde{R} = \tilde{\mathcal{O}}.$$

La identidad anterior es trivial si P, Q ó R son $\mathcal{O}$. Luego podemos suponer $P, Q, R \neq \mathcal{O}$, y como son puntos afines colineales tenemos:

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) \tag{54}$$

donde $\lambda x + \nu, \lambda, \nu \in \mathbb{Q}$ es la recta que une los tres puntos. Como a, b, c, x_1, x_2, x_3 son enteros, λ y ν también deben serlo, luego tiene sentido reducir (54) módulo p. Esto implica que $\tilde{P}, \tilde{Q}$ y $\tilde{R}$ son colineales y por tanto suman $\tilde{\mathcal{O}}$. Es decir, ϕ es un homomorfismo.

Por como está definida ϕ tenemos $\ker(\phi) = \mathcal{O}$, luego ϕ es inyectiva. □

Corolario B.6. *El orden de $E(\mathbb{Q})_{tors}$ divide al orden de $\tilde{E}(\mathbb{F}_p)$ para todo primo p en el que E tenga buena reducción.*

Demostración. □

Este resultado es muy útil para computar $E(\mathbb{Q})_{\text{tors}}$, como ilustramos en el siguiente ejemplo:

Considermos $E : y^2 = x^3 - x = x(x+1)(x-1)$. Entonces $E(\mathbb{Q})_{\text{ tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Demostración. Tenemos $E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}$ luego $|E(\mathbb{Q})_{\text{ tors}}| \geq 4$. Para conseguir una cota superior usamos el corolario anterior. Como $D = \dfrac{\Delta}{16} = -4$, E tiene buena reducción para $p = 3$. Reduciendo módulo 3 obtenemos la curva $\tilde{E} : y^2 = x^3 - x$ sobre $\mathbb{F}_3$. Para todo $x \in \mathbb{F}_3$ se tiene $x^3 - x = 0$ luego $\tilde{E}(\mathbb{F}_p) = \{\tilde{\mathcal{O}}, (0,0), (1,0), (2,0)\}$ (ya vemos que esto no es más que $E[2]$ reducido módulo 3), y por tanto $\left|\tilde{E}(\mathbb{F}_p)\right| = 4$. Es decir $|E(\mathbb{Q})_{\text{ tors}}|$ divide a 4. Por tanto $E(\mathbb{Q})_{\text{ tors}}$ tiene orden 4, lo cual junto a $E[2] \subset E(\mathbb{Q})_{\text{ tors}}$ implica

$$E(\mathbb{Q})_{\text{ tors}} = E[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

□

Referencias

[1] Joseph H. Silverman, John T. Tate, *Rational Points on Elliptic Curves*, second edition, Springer.

[2] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, second edition, Springer.

[3] M.F.Atiyah, I.G. Macdonald, *Introducción al Álgebra Conmutativa* , versión española, editorial Reverté.

[4] Robin Hartshorne, *Algebraic Geometry*, Springer.

[5] Karen Butt, *Elliptic Curves and Mordell-Weil Theorem.* **Ubicación**: `http://math.uchicago.edu/~may/REU2016/REUPapers/Butt.pdf`

[6] Kenneth Ireland, Michael Rosen. *A Classical Introduction to Modern Number Theory.* Springer. 1990. Second edition

[7] Oscar Zariski, Pierre Samuel, *Commutative Algebra, Volume I*, Springer.

[8] *Arithmetic and Geometry*, Papers Dedicated to I.R.Shafarevich on the Occasion of His Sixtieth Birthday, Volume I: Arithmetic. Birkhäuser.

[9] William Fulton *Curvas algebraicas*, Editorial Reverté, versión española por Dr. Josep Plá i Carrera.

[10] Dale Husemöller, *Elliptic curves.* Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics, 111. Springer-Verlag, New York.