UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE CIENCIAS
ESCUELA PROFESIONAL DE MATEMÁTICA

TESIS

"EL TEOREMA DE MORDELL SOBRE EL CUERPO GAUSSIANO"

PARA OPTAR EL TÍTULO PROFESIONAL DE :

LICENCIADO EN MATEMÁTICA

ELABORADO POR:

VÍCTOR EDUARDO RODRÍGUEZ SOTO

ASESOR:

MG. RONALD JESÚS MÁS HUAMÁN

LIMA- PERU
2019

Agradecimientos

Agradezco en primer lugar a Dios, por otorgarme salud, disposición y condiciones espirituales y materiales para que consiga culminar una etapa más de mi vida. A mi familia, en especial a mi pequeño Joaquín, a mi esposa Vanessa, y a mis padres, por darme fuerza en los momentos más difíciles para que no desistiese y me motivaran a culminar este trabajo.
Al Magister Ronald Jesús Mas Huamán, mi asesor y un gran amigo, quien con sus consejos, dedicación y profesionalismo, me brindó apoyo y alentó a finalizar la tesis.

Víctor Eduardo Rodríguez Soto

UNI, 01 de octubre de 2019.

Resumen

En el presente trabajo se desarrolla el Teorema de Mordell - Weil para curvas elípticas sobre el cuerpo gaussiano, para ello se define la curva sobre una extensión finita $\mathbb{Q}(i)$. Previo a esto, se desarrolla la teoría de las curvas elípticas se tratará también lo relacionado al espacio proyectivo bidimensional $\mathbb{P}^2_{\mathbb{K}}$, pues permite identificar los puntos del plano afín con los del plano proyectivo. Una curva elíptica es aquella de la forma

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

Siendo $a_1, a_2, a_3, a_4, a_6 \in K$ (cuerpo) y se caracteriza por no poseer puntos singulares. Lo anterior es conocido también como ecuación de Weierstrass, la cual se puede simplificar a

$$Y^2 = X^3 + AX + B, \quad \text{con } A, B \in K$$

cuando la característica es diferente de 2 y 3. En ella se define la operación adición de puntos de una curva elíptica, y en la que se estudiaran los casos que se suelen presentar para efectuar dicha operación (secante, tangente).

Posteriormente se estudiará lo concerniente al Teorema de Mordell-Weil sobre una extensión finita Q, el cual establece que todos los puntos racionales de una curva elíptica pueden generarse a partir de un número finito de ellos. Para ello se estudiará el Teorema del Descenso en la que definida una función altura $h\colon A \to \mathbb{R}$ y siendo $(A; \oplus)$ un grupo abeliano y el grupo A/Ma es finito, entonces A es finitamente generado, siendo m un entero.

Demostraremos, luego, el Teorema débil de Mordell - Weil, el cual nos asegura que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. A continuación se demuestra el Teorema de Mordell - Weil, el cual dice que siendo E una curva definida sobre $\mathbb{Q}$, entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado. Ya estudiado el Teorema de Mordell - Weil para $\mathbb{Q}$, se procede a tratar el teorema para $\mathbb{Q}(i)$, el cual nos dice que el

grupo cociente $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es finito.

Así, la presente tesis consta de cuatro capítulos los cuales son desarrollados como sigue:

En el capítulo 1 se aborda lo concerniente a las Curvas en el espacio proyectivo, en el que se abarca el estudio del espacio proyectivo, las curvas y tangentes, concluyendo con el estudio de los enteros gaussianos.

El capítulo 2 trata sobre la Teoría básica de una curva elíptica, en donde introduciremos la Ecuación de Wierstrass, el estudio de los puntos de la curva elíptica en el plano proyectivo, la ley de grupo, finalizando con el Teorema de Lutz Nagell.

En el capitulo 3 se trata lo referente a Curvas elípticas en $\mathbb{Q}$, en donde se define el método del descenso y se tratan los teoremas de Mordell - Weil.

Finalmente, en el capítulo 4, se estudia el Teorema débil de Mordell - Weil en $\mathbb{Q}(i)$, apoyandonos para esto con la definición de Altura para el caso gaussiano, para luego proceder a demostrar el Teorema de Mordell-Weil para $\mathbb{Q}(i)$.

Índice general

Introducción

Una curva elíptica sobre un cuerpo K es una curva plana completa no singular con un punto distinguido. Cuando la característica de K no es 2 o 3, la curva puede abordarse como una curva proyectiva plana

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \quad 4a^3 + 27b^2 \neq 0$$

En donde cada ecuación define una curva elíptica sobre K. El punto distinguido es $(0 : 1 : 0)$.

Aunque el problema de calcular los puntos en una curva elíptica E, con números racionales como coordenadas, ha fascinado a los matemáticos desde la época de los antiguos griegos, no fue hasta 1922 que se demostró que es posible construir todos los puntos a partir de un número finito, dibujando cuerdas y tangentes. El teorema de Mordell muestra con mayor precisión que los puntos racionales forman un grupo finito generado $E(\mathbb{Q})$. Hay un simple algoritmo para calcular el subgrupo de torsión de $E(\mathbb{Q})$ pero todavía no hay algoritmo probado para calcular el rango.

Las curvas elípticas se han utilizado para arrojar luz sobre algunos problemas importantes que, a primera vista, parecen no tener nada que ver con las curvas elípticas.

Motivación para estudiar curvas sobre $\mathbb{Q}$

Con la teoría que vamos a desarrollar en la presente tesis, podremos tratar problemas como el siguiente (resuelto por Mordell en 1962):

Demostrar que los únicos números naturales no nulos que pueden expresarse simultáneamente como producto de dos y tres números consecutivos son

$$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 \quad y \quad 210 = 14 \cdot 15 = 5 \cdot 6 \cdot 7$$

El problema puede ser abordado mediante técnicas de la teoría algebraica de números, es decir utilizando la factorización real o ideal de los anillos de enteros algebraicos de los cuerpos numéricos. Sin embargo en éste se puede tratar desde el punto de vista de la geometría algebraica pues la ecuación anterior determina una curva proyectiva regular en el cuál se debe encontrar los puntos con coordenadas enteras de una curva algebraica dada.

Motivación para estudiar curvas sobre $\mathbb{Q}(i)$

Esta teoría nos permite notar que las soluciones enteras a la ecuación diofántica se convierten en puntos racionales gaussianos en la curva elíptica. El siguiente ejemplo fue presentado por Peter Brown (2016).

Consideremos la ecuación diofántica

$$v^2 = 2u^4 - 1$$

La ecuación anterior posee como soluciones enteras a $(1, 1)$ y $(13, 329)$. Por un cambio de variables

$$x = \frac{2iv - 2}{u^2}, \text{ y } \quad y = \frac{-4(v + i)}{u^3}$$

esta ecuación se transforma en una curva elíptica

$$y^2 = x^3 + 8$$

donde sus soluciones iniciales $(1, 1)$ y $(13, 329)$ corresponden a los números racionales gaussianos

$$(-2 + 2i, -4 - 4i), \ (\frac{2(-1 + 239i)}{13^2}, \frac{-4(239 + i)}{13^3})$$

Capítulo 1

Curvas en el espacio proyectivo

El estudio de las curvas en el espacio proyectivo es de gran utilidad al trabajar con puntos en el infinito, lo cual visto en el plano afín suele a veces ser no tan sencillo. En este espacio se encuentran curvas que inicialmente se encontraban el el espacio afín, cuyo comportamiento se trabajará en este capítulo, así como también obtendremos una completa respuesta al estudio de las unidades, de los elementos primos y de la factorización única.

1.1. Espacio proyectivo

Definición 1.1. *Dado un cuerpo k, definamos la relación $\sim$ sobre $k^3 - \{(0,0,0)\}$ como*

$$(x,y,w) \sim (x',y',w') \Leftrightarrow \exists \lambda \in k\backslash\{0\} \quad tal\ que \quad (x',y',w') = \lambda(x,y,w).$$

Definición 1.2. *Definamos el espacio proyectivo bidimensional, denotado por $\mathbb{P}_k^2$, como*

$$\mathbb{P}_k^2 = \{[(x,y,w)] : (x,y,w) \in k^3 - (0,0,0)\}$$

donde

$$[(x,y,w)] = \{(x',y',w') : (x,y,w) \sim (x',y',w')\}$$

Denotaremos la clase de equivalencia $[(x,y,z)]$ como $(x:y:z)$. Si $(x:y:z)$ es un punto con $z \neq 0$ entonces $(x:y:z) = (x/z : y/z : 1)$ son los **puntos finitos** en

$\mathbb{P}^2_K$. Sin embargo, si $z = 0$ entonces dividir por z puede ser tomado como un punto al infinito y por lo tanto los puntos $(x : y : 0)$ son llamados **puntos al infinito** en $\mathbb{P}^2_K$.

Definición 1.3. *Sea k un cuerpo. Se define la recta sobre k como el polinomio no nulo $L = ax + by + cw$ en $k[x, y, w]$*

Consideramos que L y una recta $L' = a'x + b'y + c'w$ se encuentran sobre una misma recta si (a', b', c') es un múltiplo de (a, b, c). El lugar

$$L(k) = \{(x, y, w) \mid ax + by + cw = 0\}$$

definido en $\mathbb{P}^2_k$, es llamado el conjunto de k puntos o los k puntos racionales de L.

Definición 1.4. *Definamos el plano afín bidimensional sobre k, denotado por $\mathbb{A}^2_k$ como*

$$\mathbb{A}^2_k = \big\{(x, y) \in k \times k\big\}$$

Sean $U = \{(x : y : w) | \, w \neq 0\}$ y $L_\infty(w) = \{(x : y : w) | \, w = 0\}$ tenemos que

$$\begin{array}{ccccccccc} \psi_1 : & \mathbb{A}^2_k & \to & U & y & \psi_2 : & \mathbb{P}^1_k & \to & L_\infty(k) \\ & (x, y) & \to & (x : y : 1) & & & (x : y) & \to & (x : y : 0) \end{array}$$

siendo ψ_1 y ψ_2 biyecciones.
De esta manera el plano afín esta identificado con los puntos finitos de $\mathbb{P}^2_k$, además $\mathbb{P}^2_k = U \cup L_\infty(k)$, siendo esta unión disjunta. Es más, el plano afín $\mathbb{A}^2_k = \{(x, y)\}$ se relaciona uno a uno con el proyectivo $\mathbb{P}^2_k$. Podemos relacionar a un punto (x, y) con $[(x, y, 1)]$ de ambos planos respectívamente.
De cierta forma, la geometría de $\mathbb{P}^2_k$ es más simple que la geometría de k^2, y esto se nota ya que:

1. Dos rectas distintas en $\mathbb{P}^2_k$ se intersectan en un único punto. En efecto, escogemos el siguiente sistema de ecuaciones

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} x \\ y \\ w \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Puesto que las líneas son diferentes, la matríz de coeficientes tiene rango igual a 2, por lo que el núcleo tiene dimensión igual a 1, y así hay un solo punto de intersección.

2. Dos puntos distintos en $\mathbb{P}^2_k$ descansan en una única recta. En efecto, escogemos el sistema de ecuaciones

$$\begin{pmatrix} x & y & w \\ x' & y' & w' \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

y argumentamos de manera similar.

Sea $\phi \in GL(3,k)$. Luego ϕ lleva elementos del conjunto k^3, hacia k^3 y los pasa a una aplicación $\mathbb{P}^2_k$ a $\mathbb{P}^2_k$ llamada la transformación proyectiva correspondiente a ϕ.

Si L es la recta, cuyos coeficientes estan dados por el vector fila $\begin{pmatrix} a & b & c \end{pmatrix}$ y si ϕ es una transformación proyectiva, entonces el vector fila $\begin{pmatrix} a & b & c \end{pmatrix} \phi^{-1}$ define una nueva recta L^ϕ y los k puntos racionales de L^ϕ se encuentran dados por

$$L^\phi(k) = \phi(L(k)).$$

En efecto, sea $\begin{pmatrix} x \\ y \\ w \end{pmatrix}$ en $L(k)$. Entonces $\begin{pmatrix} x' \\ y' \\ w' \end{pmatrix} = \phi \begin{pmatrix} x \\ y \\ w \end{pmatrix}$ esta en $\phi(L(k))$ y satisface

$$\begin{pmatrix} a & b & c \end{pmatrix} \phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix} = 0;$$

por tanto se encuentra en $L^{\phi}(k)$. Análogamente si $\begin{pmatrix} x' \\ y' \\ w' \end{pmatrix}$ se encuentra en $L^{\phi}(k)$,

entonces $\begin{pmatrix} x \\ y \\ w \end{pmatrix} = \phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix}$ satisface

$$\begin{pmatrix} a & b & c \end{pmatrix} \begin{pmatrix} x \\ y \\ w \end{pmatrix} = \begin{pmatrix} a & b & c \end{pmatrix} \phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix} = 0;$$

y así $\begin{pmatrix} x' \\ y' \\ w' \end{pmatrix}$ es imágen de ϕ de algún elemento en $L(k)$.

Para cualquier punto en $\mathbb{P}^2_k$, podemos introducir varios sistemas de coordenadas locales afines.

Fijemos $[(x_0, y_0, w_0)]$ en $\mathbb{P}^2_k$. Escojamos algún ϕ en $GL(3,k)$ con $\phi(x_0, y_0, w_0) = (0,0,1)$. Luego podemos definir coordenadas locales sobre $\phi^{-1}(k \times k \times \{1\})$ a k^2 vía la aplicación uno a uno con

$$\begin{array}{rccc} \varphi: & \phi^{-1}(k \times k \times \{1\}) & \to & k^2 \\ & (x, y, w) & \to & (\frac{x}{w} : \frac{y}{w}) \end{array}$$

tal que

$$\varphi(\phi^{-1}(x, y, 1)) = (x, y)$$

Ejemplo 1.5. Supongamos que $(x_0, y_0, w_0) = (x_0, y_0, 1)$. Podemos escoger

$\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$. Entonces

$$\phi \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x - x_0 \\ y - y_0 \\ 1 \end{pmatrix}.$$

En este caso, las coordenadas locales se encuentran definidas sobre

$$\phi^{-1}(k \times k \times \{1\}) = k \times k \times \{1\}$$

y son dadas por

$$\varphi(x, y, 1) = \varphi(\phi^{-1}(\phi(x, y, 1))) = \varphi(\phi^{-1}(x - x_0, y - y_0, 1)) = (x - x_0, y - y_0).$$

.

Este ϕ es útil para llevar de $(x_0, y_0, 1)$ en $\mathbb{P}^2_k$ a $(0, 0)$ en k^2.

Ejemplo 1.6. Supongamos que $(x_0, y_0, w_0) = (0, 1, 0)$. Podemos escoger $\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

Entonces

$$\phi \begin{pmatrix} x \\ 1 \\ w \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ 1 \\ w \end{pmatrix} = \begin{pmatrix} w \\ x \\ 1 \end{pmatrix}.$$

y

$$\varphi(x, 1, w) = \varphi(\phi^{-1}(\phi(x, 1, w))) = \varphi(\phi^{-1}(w, x, 1)) = (w, x).$$

.

Este ϕ será útil para para estudiar el comportamiento del punto al infinito en la forma cúbica de Weierstrass.

Las coordenadas afínes locales son usadas en el estudio de polinomios homogéneos de tres variables. Decimos que un polinomio no nulo $F \in k[x, y, w]$ es homogéneo de grado d si cada monomio en F posee grado total igual a d. Podemos escribir $k[x, y, w]_d$ para denotar el conjunto de tales polinomios. Para cada F se satisface

$$F(\lambda x, \lambda y, \lambda w) = \lambda^d F(x, y, w) \quad \text{para} \quad x, y, w, \lambda \in k \tag{1.1}$$

.

Lema 1.7. *Si k es un cuerpo infinito, entonces un polinomio no nulo $f \in k[x_1, \ldots, x_n]$ es no nulo en algún punto.*

Demostración. Usemos la inducción sobre n. El caso $n = 1$ es trivial. Asumamos el resultado para $n-1$, y supongamos que $f(c_1, \ldots, c_n) = 0$ para todo $(c_1, \ldots, c_n)$. Por inducción

$$f(x_1, \ldots, x_{n-1}, c) \tag{1.2}$$

es el polinomio nulo de $n-1$ variables para cada c escogido. Fijemos un monomio $x_1^{\alpha_1} \ldots x_{n-1}^{\alpha_{n-1}}$ de $n-1$ variables. Los monomios de n variables que que contienen a este monomio de $n-1$ variables

$$\sum_{j \geq 0} b_j x_1^{\alpha_1} ... x_{n-1}^{\alpha_{n-1}} x_n^j$$

originan a f y (1.2) nos dice que $\sum_{j \geq 0} b_j c^j = 0$ para todo c. Por lo tanto, todos los b_j son cero. Repitiendo el proceso para todos los monomio de $n-1$ variables, vemos que f es el polinomio nulo. □

Proposición 1.8. *Si k es un cuerpo infinito, entonces un polinomio no nulo $F \in k[x, y, w]$ que satisface (1.1) es homogéneo de grado d.*

Demostración. Escribamos F como la suma de los términos homogéneos de diferentes grados: $F = \sum_{j=1}^{n} F_j$ con F_j de grado d_j y con $d_1 = d$. Luego (1.1) nos da

$$\lambda^d F(x_0, y_0, w_0) = \lambda^d F_1(x_0, y_0, w_0) + \lambda^{d_2} F_2(x_0, y_0, w_0) + ... + \lambda^{d_n} F_n(x_0, y_0, w_0)$$

.

para todo λ. Puesto que k es infinito, esta igualdad para todo λ implica que $F(x_0, y_0, w_0) = F_1(x_0, y_0, w_0)$ y también que $F_j(x_0, y_0, w_0) = 0$ para todo $j \geq 2$. Haciendo que (x_0, y_0, w_0) varíe y aplicando el lema (1.7) a $F - F_1$ y a F_j para $j \geq 2$, queda probada la proposición. □

Un polinomio homogéneo $F \neq 0$ de grado mayor que 0 no es una función en $\mathbb{P}_k^2$. Sin embargo, podemos examinar el comportamiento de F cerca al punto (x_0, y_0, w_0) en $k^3 - \{(0,0,0)\}$ al escoger ϕ en $GL(3,k)$ con $\phi(x_0, y_0, w_0) = (0,0,1)$ y definiendo

$$f(x,y) = F(\phi^{-1}(x,y,1)).$$

Ejemplo 1.9. Supongamos que $(x_0, y_0, w_0) = (x_0, y_0, 1)$ y

$$\phi = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & 1 \end{pmatrix}$$

luego

$$\phi^{-1} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} x + x_0 \\ y + y_0 \\ 1 \end{pmatrix}$$

$$f(x,y) = F(x + x_0, y + y_0, 1).$$

Para

$$F(x,y,w) = x^2y + xyw + w^3,$$

el correspondiente $f(x,y)$ se divide en términos homogéneos como

$$f(x,y) = (x_0^2y_0 + x_0y_0 + 1) + (x_0^2y + 2x_0y_0x + x_0y + y_0x) + (y_0x^2 + 2x_0xy + xy) + (x^2y).$$

Ejemplo 1.10. Supongamos que $(x_0, y_0, w_0) = (0,1,0)$ y

$$\phi = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

luego

$$\phi^{-1} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} y \\ 1 \\ x \end{pmatrix}$$

$$f(x, y) = F(y, 1, x).$$

Para el mismo F del ejemplo 1.9, al hacer

$$F(x, y, w) = x^2y + xyw + w^3,$$

obtenemos

$$f(x, y) = (y^2 + xy) + (x^3)$$

sin términos de orden total 0 o 1.

Recíprocamente si d y ϕ se encuentran dados y si f en $k[x, y]$ tiene grado d, podemos reconstruir F. En el ejemplo 1.10 con $d = 3$ y con f como como ya se vió, definimos $G(x, y, w)$ al insertar potencias de w para hacer todos los términos de grado 3:

$$G(x, y, w) = y^2w + xyw + (x^3)$$

A continuación escribir $F = G \circ \phi$ y hacer $F(x, y, w) = x^2y + xyw + w^3$.

1.2. Curvas y tangentes

Una curva plana o curva proyectiva plana definida sobre k es un polinomio homogéneo no nulo $F \in k[x, y, w]_d$ para algún $d > 0$, excepto que consideremos dos de tales polinomios como la misma curva si ellos son múltiplos de cada una. Como ya se mencionó, F no se encuentra definida sobre $\mathbb{P}^2_K$. Sin embargo, el lugar cero de F da lugar a un conjunto en el espacio proyectivo. Esto es, si K es una extensión del cuerpo k, entonces el lugar

$$F(K) = \{(x, y, w) \mid F(x, y, w) = 0\}$$

se encuentra bien definido en $\mathbb{P}^2_k$, puesto que F es homogéneo. Este lugar es llamado el conjunto de los K puntos o los K puntos racionales de la curva. En el caso especial que $d = 1, 2$ o 3, la curva es llamada recta, curva o cúbica respectivamente. Si F es una curva plana y si tenemos un sistema de coordenadas afín dado por ϕ con $\phi(x_0, y_0, w_0) = (0, 0, 1)$, entonces la curva afín correspondiente es

$$f(x,y) = F(\phi^{-1}(x,y,1)) \quad en \quad k[x,y]$$

Entre los k puntos racionales de una curva, podemos distinguir entre puntos singulares y no singulares. Así, sea $F \neq 0$ en $k[x,y,w]_d$, fijemos $(x_0,y_0,w_0) \in F(k)$ y escojamos coordenadas locales afínes sobre (x_0,y_0,w_0) dados por algún ϕ con $\phi(x_0,y_0,w_0) = (0,0,1)$. Sea

$$f(x,y) = F(\phi^{-1}(x,y,1)) \in k[x,y].$$

Por ejemplo, como se vio en el ejemplo 1.9., se tuvo que $w_0 = 1$ y

$$F(x,y,w) = x^2y + xyw + w^3,$$

como consecuencia

$$f(x,y) = (x_0^2y_0 + x_0y_0 + 1) + (x_0^2y + 2x_0y_0x + x_0y + y_0x) + (y_0x^2 + 2x_0xy + xy) + (x^2y)$$

$$= f_0(x,y) + f_1(x,y) + f_2(x,y) + f_3(x,y).$$

El término constante f_0 es 0, puesto que $(x_0,y_0,1)$ está en $F(k)$. En este ejemplo y en general, f es la suma de términos homogéneos de grado 1 hasta d, es decir $f = f_1 + ... + f_d$ depende de (x_0,y_0,w_0) y de ϕ
Decimos que (x_0,y_0,w_0) es un punto no singular si f_1 no es el polinomio nulo en $k[x,y]$, de otra forma (x_0,y_0,w_0) es un punto singular. En nuestro ejemplo, con $w_0 = 1$, consideremos

$$f_1(x,y) = (2x_0y_0 + y_0)x + (x_0^2 + x_0)y.$$

Los puntos singulares en $F(k)$ son aquellos en donde los coeficientes de x y de y son cero. Los coeficientes son cero cuando $(x_0,y_0) = (0,0)$ y $(x_0,y_0) = (-1,0)$. En $\mathbb{P}_k^2$, estos puntos son (0,0,1) y (-1,0,1)). Pero ninguno de estos se encuentra en $F(k)$.

Por lo tanto, F es no singular en cada punto de $F(k)$ para el cual $w_0 = 1$.
Necesitamos comprobar que la no singularidad no depende de la elección de ϕ. Así, debemos suponer también que $\psi(x_0, y_0, w_0) = (0, 0, 1)$. Luego $\psi \circ \phi^{-1} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ r & s & 1 \end{pmatrix}$ con $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertible. Escribamos $f(x, y) = F(\phi^{-1}(x, y, 1))$ y también

$$\begin{aligned} f(x,y) &= (F \circ \psi^{-1})(\psi \circ \phi^{-1})(x, y, 1) \\ &= (F \circ \psi^{-1})(ax + by, cx + dy, rx + sy + 1) \\ &= (F \circ \psi^{-1}) \left((rx + sy + 1) \left(\tfrac{ax+by}{rx+sy+1}, \tfrac{cx+dy}{rx+sy+1}, 1 \right) \right) \\ &= (rx + sy + 1)^d g \left(\tfrac{ax+by}{rx+sy+1}, \tfrac{cx+dy}{rx+sy+1} \right) \\ &= (rx + sy + 1)^d (g_1 + ...g_d) \left(\tfrac{ax+by}{rx+sy+1}, \tfrac{cx+dy}{rx+sy+1} \right) \\ &= (rx + sy + 1)^{d-1} g_1 (ax + by, cx + dy) + ... + g_d (ax + by, cx + dy.) \end{aligned} \tag{1.3}$$

Al expandir las diferentes potencias de $(rx+sy+1)$ y reagrupando por homogeneidad, tenemos

$$f_1(x, y) = g_1(ax + by, cx + dy). \tag{1.4}$$

Similarmente
$g_1(x, y) = f_1(\alpha x + \beta y, \gamma x + \delta y)$ con con $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$.

Así f_1 y g_1 son nulos o no son nulos.

Proposición 1.11. *Supongamos que $F \in k[x, y, w]_m$ y $G \in k[x, y, w]_n$ son curvas planas. Si (x_0, y_0, w_0) se encuentran en $F(k) \cup G(k)$, entonces (x_0, y_0, w_0) es un punto singular de FG.*

Demostración. Escogemos coordenadas locales afines con $\phi(x_0, y_0, w_0) = (0, 0, 1)$, y definimos $f(x, y) = F(\phi^{-1}(x, y, 1))$ y $g(x, y) = G(\phi^{-1}(x, y, 1))$.

Entonces podemos escribir $f = f_1 + ... + f_m$ y $g = g_1 + ... + g_n$. Puesto que

$$f(x, y)g(x, y) = (FG)(\psi^{-1}(xy, 1)),$$

y puesto que f no tiene términos de primer grado, se sigue que FG tiene un punto singular en (x_0, y_0, w_0).

□

Decimos que la curva plana F sobre k es no singular (o suave) si F es no singular en cada punto de $F(\overline{k})$, donde $\overline{k}$ es la clausura algebraica de k. De otro modo decimos que F es singular. La no singularidad en todos los puntos de $F(k)$ no implica que F sea no singular. Por ejemplo, la curva

$$F(x, y, w) = x^3 - 6xw^2 + 6yw^2 - y^3$$

se encuentra definida sobre $k = \mathbb{Q}$. es no singular en cada punto de $F(\mathbb{Q})$,y tiene un punto singular en $(x, y, w) = (\sqrt{2}, \sqrt{2}, 1)$. Así la curva es singular.

Teorema 1.12. *(Teorema de Bezout). Supongamos que $F \in k[x, y, w]_m$ y $G \in k[x, y, w]_n$ son curvas planas. Entonces $F(\overline{k}) \cap G(\overline{k})$ es no vacío. Si tuviese mas de mn puntos, entonces F y G tienen como un factor común a algún polinomio homogéneo de grado mayor que cero.*

Demostración. Consultar [5,p.50] □

Lema 1.13. *Supongamos que F es una curva plana e irreductible sobre $\overline{k}$. Entonces los factores son polinomios homogéneos, y F es singular.*

Demostración. Escribamos $F = F_1F_2$. Sea d_1 y e_1 los grados mas alto y mas bajo, respectivamente, de los términos en F_2. El producto de los términos de grado d_1 en F_1 y los términos de grado d_2 en F_2 es no nulo y es el grado e_1e_2 de F. Puesto que F es homogéneo, $d_1d_2 = e_1e_2$. Se sigue que $d_1 = e_1$ y $d_2 = e_2$, así $F1$ y $F2$ son homogéneos. El teorema de Bezout nos dice que $F_1(\overline{k}) \cap F_2(\overline{k})$ es no vacío, además la proposición 1.1 nos dice que cualquier punto en esta intersección es un punto singular para F. Por lo tanto, F es singular. □

Supongamos que $(x_0, y_0, w_0) = (0, 0, 1)$ es un punto no singular de $F(k)$ y que $\phi(x_0, y_0, w_0) = (0, 0, 1) = (0, 0, 1)$. Hemos escrito $f(x, y) = F(\phi^{-1}(x, y, 1))$ con $f = f_1 + ... + f_d$. Luego $f_1(x, y) = px + qy$ con p y q en k, distintos de cero. Consideremos f_1 como un polinomio en tres variables $\tilde{f}_1(x, y, w)$ independiente de w. Reincorporemos

un miembro distinto de cero $L = \tilde{f} \circ \phi$ de $k[x, y, w]_1$, y el resultado es llamado la recta tangente a F en (x_0, y_0, w_0).

Veamos que la recta tangente es independiente de la elección de las coordenadas locales afines. Así, supongamos también que $\psi(x_0, y_0, w_0) = (0, 0, 1)$. Formemos $g(x, y) = F(\psi^{-1}(x, y, 1))$ y $\psi \circ \phi^{-1} = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ r & s & 1 \end{pmatrix}$, y sean las respectivas rectas tangentes L_ϕ y L_ψ. Tenemos entonces

$$L_\phi(x, y, w) = \tilde{f}_1(\phi(x, y, w)), \tag{1.5}$$

$$\begin{aligned} \tilde{f}_1(x, y, w) &= f_1(x, y) = g_1(ax + by, cx + dy) \\ &= \tilde{g}_1(ax + by, cx + dy, rx + sy + w) = \tilde{g}_1(\psi \circ \phi^{-1}(x, y, w)), \end{aligned}$$

$$\begin{aligned} L_\psi(x, y, w) &= \tilde{g}_1(\psi(x, y, w)) \\ &= \tilde{g}_1(\psi \circ \phi^{-1}(\phi(x, y, w))) = \tilde{f}_1(\phi(x, y, w)). \end{aligned} \tag{1.6}$$

Comparando (1.5) y (1.6) vemos que $L_\phi(x, y, w) = L_\psi(x, y, w)$.

Si F es una curva plana y ϕ es una transformación proyectiva, entonces $F^\phi = F \circ \phi^{-1}$ es otra curva plana, y los k puntos racionales de F^ϕ son dados por

$$F^\phi(k) = \phi(F(k)),$$

Notemos que si (x_0, y_0, w_0) es un punto no singular para F, entonces $\phi(x_0, y_0, w_0)$ es un punto no singular para F^ϕ.

Proposición 1.14. *Sea F una curva plana sobre k. Si (x_0, y_0, w_0) se encuentra sobre la curva, entonces (x_0, y_0, w_0) es un punto no singular si y solo sí al menos una de las derivadas $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}, \frac{\partial F}{\partial w}$ es no nula en (x_0, y_0, w_0). En este caso, la recta tangente L a F en (x_0, y_0, w_0) se encuentra dada por*

$$L = \left[\frac{\partial F}{\partial x}\right]_{(x_0,y_0,w_0)} x + \left[\frac{\partial F}{\partial x}\right]_{(x_0,y_0,w_0)} y + \left[\frac{\partial F}{\partial x}\right]_{(x_0,y_0,w_0)} w.$$

Demostración. Escogemos coordenadas locales afines con $\phi(x_0, y_0, w_0) = (0, 0, 1)$. Puesto que (x_0, y_0, w_0) se encuentra sobre la curva, $F \circ \phi^{-1}$ contiene un factor de x o y, lo cual conlleva a que

$$\frac{\partial^n}{\partial w^2}(F \circ \phi^{-1})(0, 0, 1) = 0 \quad \text{para cada} \quad n \tag{1.7}$$

Escribamos $f(x, y) = F(\phi^{-1}(x, y, 1))$ con $f_1 + ... + f_d$. Los coeficientes del término lineal f_1 son $\frac{\partial f}{\partial x}(0, 0)$ y $\frac{\partial f}{\partial y}(0, 0)$. Puesto que

$$f = F \circ \phi^{-1} \circ ((x, y) \to (x, y, 1)),$$

la regla de la cadena nos da

$$\begin{pmatrix} \dfrac{\partial f}{\partial x} & \dfrac{\partial f}{\partial y} \end{pmatrix}_{(0,0)} = \begin{pmatrix} \dfrac{\partial F}{\partial x} & \dfrac{\partial F}{\partial y} & \dfrac{\partial F}{\partial w} \end{pmatrix}_{(x_0,y_0,w_0)} \phi^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}. \tag{1.8}$$

Sean (x', y', w') dados. Multiplicando a la derecha por $\begin{pmatrix} x' \\ y' \end{pmatrix}$, obtenemos

$$\begin{aligned} \tilde{f}_1(x', y', w') &= \left(\tfrac{\partial f}{\partial x} \quad \tfrac{\partial f}{\partial y}\right)_{(0,0)} \begin{pmatrix} x' \\ y' \end{pmatrix} \\ &= \left(\tfrac{\partial F}{\partial x} \quad \tfrac{\partial F}{\partial y} \quad \tfrac{\partial F}{\partial w}\right)_{(x_0,y_0,w_0)} \phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix} \end{aligned} \tag{1.9}$$

Por (1.7) para $n = 1$, la tercera entrada de

$$\begin{pmatrix} \dfrac{\partial F}{\partial x} & \dfrac{\partial F}{\partial y} & \dfrac{\partial F}{\partial w} \end{pmatrix}_{(x_0,y_0,w_0)} \phi^{-1}$$

es cero. Así, el lado derecho de (1.9) es

$$\begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} & \frac{\partial F}{\partial w} \end{pmatrix}_{(x_0,y_0,w_0)} \phi^{-1} \begin{pmatrix} x' \\ y' \\ w' \end{pmatrix}.$$

Tomando $(x', y', z') = \phi(x, y, w)$, obtenemos

$$\begin{aligned} L(x', y', w') &= \tilde{f}_1 \circ \phi(x, y, w) \\ &= \begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} & \frac{\partial F}{\partial w} \end{pmatrix}_{(x_0,y_0,w_0)} \begin{pmatrix} x \\ y \\ w \end{pmatrix} \end{aligned} \tag{1.10}$$

por (1.8), tenemos un punto singular si todas las primeras derivadas parciales de F son cero. De otra manera (1.10) nos muestra que $\tilde{f}_1$ no es cero; por tanto f_1 no es cero y el punto es no singular. En este caso, (1.10) nos da la recta tangente. □

El término cuadrático $\tilde{f} \circ \phi(x, y, w)$ puede ser identificado similarmente, siempre que la característica de k no sea 2. Pero la expresión es mas complicada y depende de la elección de ϕ. Esto implica también la matriz hessiana de F, definida como

$$H = H(x_0, y_0, w_0) = \begin{pmatrix} \frac{\partial^2 F}{\partial x^2} & \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial x \partial w} \\ \frac{\partial^2 F}{\partial x \partial y} & \frac{\partial^2 F}{\partial y^2} & \frac{\partial^2 F}{\partial y \partial w} \\ \frac{\partial^2 F}{\partial x \partial w} & \frac{\partial^2 F}{\partial y \partial w} & \frac{\partial^2 F}{\partial w^2} \end{pmatrix}_{(x_0,y_0,w_0)} \tag{1.11}$$

1.3. Los enteros gaussianos

Las igualdades

$$2 = 1 + 1, \quad 5 = 1 + 4, \quad 13 = 4 + 9, \quad 17 = 1 + 16, \quad 29 = 4 + 25, \quad 37 = 1 + 36$$

muestra que los primeros números primos pueden ser representados como la suma de dos cuadrados. Exceptuando a 2, ellos son congruentes a 1 módulo 4. En general cualquier número primo impar de la forma $p = a^2 + b^2$ satisface $p \equiv 1 \mod 4$, esto debido a que todo cuadrado al dividirse por cuatro posee residuo cero o uno, lo cual se evidencia. Lo que no es evidente, es el hecho que lo recíproco se cumpla también.

Teorema 1.15. *Dado $p \in \mathbb{Z}^+$, un número primo mayor que 2, se tiene que*

$$p = a^2 + b^2 \quad (a, b \in \mathbb{Z}) \quad \Longleftrightarrow \quad p \equiv 1 \mod 4.$$

Para la resolución de este teorema, recurrimos al conjunto de los enteros gaussianos

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \quad i^2 = -1.$$

En este anillo, la ecuación $p = x^2 + y^2$, se convierte en el producto

$$p = (x + iy)(x - iy),$$

Es decir, el problema se convierte en uno de factorización en $\mathbb{Z}[i]$.

Proposición 1.16. *El anillo $\mathbb{Z}[i]$ es euclídeo, por tanto, en particular, dominio de factorización única.*

Demostración. Mostremos que $\mathbb{Z}[i]$ es euclídeo respecto a la función $\mathbb{Z}[i] \to \mathbb{N} \cup \{0\}, \alpha \mapsto |\alpha|^2$. Así que, para $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$, uno tiene que verificar la existencia de enteros gaussianos γ, ρ tales que

$$\alpha = \gamma\beta + \rho \qquad \text{y} \qquad |\rho|^2 < |\beta|^2$$

Basta encontrar $\gamma \in \mathbb{Z}[i]$ tal que $\left|\frac{\alpha}{\beta} - \gamma\right| < 1$. Los enteros gaussianos forman un enmallado en el plano complejo $\mathbb{C}$ (los puntos con coordenadas enteras respecto a las bases $1, i$). El número complejo $\frac{\alpha}{\beta}$ cae en una malla del enmallado y la distancia desde el punto enmallado mas cercano no es mayor que la mitad del tamaño de la diagonal de la malla, es decir, $\frac{1}{\sqrt{2}}$. Por tanto, existe un elemento $\gamma \in \mathbb{Z}[i]$ con $\left|\frac{\alpha}{\beta} - \gamma\right| \leq \frac{1}{\sqrt{2}} < 1$. □

Basado en este resultado para el anillo $\mathbb{Z}[i]$, el teorema 1.15 se puede enunciar como que es suficiente mostrar que un número primo $p \equiv 1 \mod 4$ de $\mathbb{Z}$ no sigue siendo un elemento primo en el anillo $\mathbb{Z}[i]$. En efecto, si esto se prueba, entonces existe una descomposición

$$p = \alpha.\beta$$

en dos elementos α, β de $\mathbb{Z}[i]$. La norma de $z = x + iy$ se encuentra definida por

$$N(x + iy) = (x + iy)(x - iy) = x^2 + y^2$$

es decir por $N(z) = |z|^2$. Al ser multiplicativo, tenemos que

$$p^2 = N(\alpha).N(\beta)$$

Puesto que α y β no son unidades, se sigue que $N(\alpha)$ y $N(\beta)$ son diferentes a 1. Por tanto, $p = N(\alpha) = a^2 + b^2$, donde escogemos $\alpha = a + bi$.
Finalmente, para probar que un primo racional de la forma $p = 1 + 4n$ no puede ser un elemento primo en $\mathbb{Z}[i]$, notemos que la congruencia

$$-1 \equiv x^2 \mod p$$

admite una solución a la cual llamamos $x = (2n)!$.
En efecto, puesto que $-1 \equiv (p-1)! \mod p$, por el teorema de Wilson tenemos que

$$-1 \equiv (p-1)! = [1 \cdot 2 \ldots (2n)] [(p-1)(p-2) \ldots (p-2n)] \equiv [(2n)!] \left[(-1)^{2n}(2n)!\right] = [(2n)!] \equiv p.$$

Así tenemos que $p \mid x^2 + 1 = (x + i)(x - i)$. Pero en vista que $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$ no divide a ninguno de los factores $x + i, x - i$, por tanto no es un elemento primo en el anillo $\mathbb{Z}[i]$.
Cuando se desarrolla la teoría de divisibilidad para un anillo, se presentan dos problemas básicos: determinar las unidades del anillo en cuestión y determinar sus elementos primos. La respuesta a lo primero es relativamente fácil. Un número $\alpha = a + bi \in \mathbb{Z}[i]$ es una unidad si y solo sí su norma es 1:

$$N(\alpha) := (a + ib)(a - ib) = a^2 + b^2 = 1$$

es decir, ya sea $a^2 = 1, b^2 = 0$ o $a^2 = 0, b^2 = 1$. Así obtenemos la siguiente proposición

Proposición 1.17. *El grupo de unidades del anillo $\mathbb{Z}[i]$ consta de las cuatro raíces de la unidad,*

$$\mathbb{Z}^*[i] = \{1, -1, i, -i\ \}.$$

Para responder la pregunta para los primos, es decir, elementos irreductibles del anillo $\mathbb{Z}[i]$, recordemos que dos elementos α, β en un anillo son llamados asociados, simbólicamente $\alpha \sim \beta$, si ellos difieren solo en un factor unitario y cada elemento asociado a un elemento irreductible π es también irreductible.

Teorema 1.18. *Los π elementos primos de $\mathbb{Z}[i]$, hasta los elementos asociados, son dados como sigue*

1. $\pi = 1 + i$
2. $\pi = a + bi$ *con* $a^2 + b^2 = p, p \equiv 1 \mod 4, a > |b| > 0$,
3. $\pi = p, \quad p \equiv 3 \mod 4$.

Aquí p denota un número primo en $\mathbb{Z}$.

Demostración. Los números como en (1) o en (2) son primos debido a que una descomposición $\pi = \alpha.\beta$ en $\mathbb{Z}[i]$ implica una ecuación

$$p = N(\pi) = N(\alpha).N(\beta),$$

con algún número primo p. Por tanto, ni $N(\alpha) = 1$ ni $N(\beta) = 1$, así tenemos que ni α ni β es una unidad.
Los números $\pi = p$, donde $p \equiv 3 \mod 4$, son primos en $\mathbb{Z}[i]$, debido a que una descomposición $p = \alpha.\beta$ en α, β, los cuales no son unidades, implicaría que $p^2 = N(\alpha).N(\beta)$, así que $p = N(\alpha) = N(a + bi) = a^2 + b^2$, lo cual, deacuerdo con el teorema 1.15., nos lleva a que $p \equiv 1 \mod 4$.
Dicho esto, tenemos que comprobar que un elemento primo arbitrario π de $\mathbb{Z}[i]$ se encuentra asociado a uno de la lista. Antetodo, la descomposición

$$N(\pi) = \pi.\bar{\pi} = p_1 ... p_r,$$

con primos racionales p_i, muestra que $\pi \mid p$, para algún $p = p_i$. Esto nos da que $N(\pi) \mid N(p) = p^2$, así que, de cualquier manera, $N(\pi) = p$ o $N(p) = p^2$. En el caso que $N(\pi) = p$, tenemos que $\pi = a + bi$ con $a^2 + b^2 = p$, así que π es del tipo (2), o si $p = 2$, es asociado a $1 + i$. Por otra parte, si $N(\pi) = p^2$, entonces π se encuentra asociado a p puesto que p/π es un entero con norma uno y por tanto una unidad. Además $p \equiv 3 \mod 4$ se debe mantener, pues de lo contrario, tendremos que $p = 2$ o que $p \equiv 1 \mod 4$ y debido al teorema 1.15., $p = a^2 + b^2 = (a + bi)(a - bi)$ no puede ser primo. □

La proposición también resuelve la interrogante de como los números primos $p \in \mathbb{Z}$ se descomponen en $\mathbb{Z}[i]$. El número primo $2 = (1 + i)(1 - i)$ es asociado al cuadrado del elemento primo $1 + i$. En efecto, la identidad $1 - i = -i(1 + i)$ muestra que $2 \sim (1 + i)^2$. Los números primos $p \equiv 1 \mod 4$ se descomponen en dos factores primos conjugados

$$p = (a + bi)(a - bi)$$

y los números primos $p \equiv 3 \mod 4$ permanecen primos en en $\mathbb{Z}[i]$.
Los enteros gaussianos, juegan el mismo papel en el cuerpo

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

tal como los enteros racionales lo hacen en el cuerpo $\mathbb{Q}$. Así que deberían ser vistos como enteros en $\mathbb{Q}(i)$.

Proposición 1.19. *El cuerpo $\mathbb{Z}[i]$ consta de elementos del cuerpo de extensión $\mathbb{Q}(i)$ de $\mathbb{Q}$ los cuales satisfacen la ecuación polinomial mónica*

$$x^2 + ax + b = 0$$

con coeficientes $a, b \in \mathbb{Z}$.

Demostración. Un elemento $\alpha = c + di \in \mathbb{Q}(i)$ es un cero del polinomio

$$x^2 + ax + b \in \mathbb{Q}[x] \quad \text{con} \quad a = -2c, \quad b = c^2 + d^2.$$

Si c y d son enteros racionales, entonces lo son también a y b. Recíprocamente, si a y b son enteros, entonces $2c$ y $2d$ lo son también. De $(2c)^2 + (2d)^2 = 4b \equiv 0$ mód 4, de donde $(2c)^2 \equiv (2d)^2 \equiv 0 \mod 4$, puesto que los cuadrados son siempre $\equiv 0$ o $\equiv 1$. Por tanto c y d son enteros.

□

Capítulo 2

Teoría básica de una curva elíptica

Las aplicaciones de las curvas elípticas poseen diversos usos en las matemáticas, como es en el caso de factorización de enteros, o en forma más general en criptografía. La idea principal en esas aplicaciones es que al tener un algoritmo el cual emplea ciertos grupos finitos, se pueda reescribir, usando para ello, los grupos de puntos racionales de curvas elípticas. En este capítulo, vamos a ver que una curva elíptica posee la estructura de un grupo abeliano, la cual se da mediante la operación de adición, finalizando con el teorema de Lutz-Nagell para curvas elípticas de la forma $y^2 = x^3 + ax + b$.

2.1. Ecuación de Weierstrass

Definición 2.1. *Una curva elíptica E sobre un cuerpo K se encuentra definida por la ecuación:*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.1}$$

Con $a_1, a_2, a_3, a_4, a_6 \in K$ y $\Delta \neq 0$, siendo Δ la discriminante de E, la cual se encuentra definida por

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \tag{2.2}$$

donde:

$$\begin{aligned} d_2 &= a_1^2 + a_2 \\ d_4 &= 2a_4 + a_1 a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1 a_6^2 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \end{aligned}$$

Denotemos $E(K)$ como el conjunto de puntos que cumplen dicha ecuación.

Observaciones

1. La ecuación (2.1) se conoce como la ecuación de Weierstrass.

2. La curva elíptica se encuentra definida sobre K, pues $a_1, a_2, a_3, a_4, a_6 \in K$. Al encontrarse E definida sobre K, entonces E también esta definida entre cualquier extensión de K.

3. La condición $\Delta \neq 0$ asegura que la curva elíptica no tenga puntos singulares, esto es, puntos que anulen las derivadas parciales de la función polínomica

   $$f(X, Y) = Y^2 + a_1 XY + a_3 Y - X^3 - a_2 X^2 - a_4 X - a_6$$

   asociada a la curva elíptica. Esto asegura que no haya puntos en los que la curva tenga dos o más rectas tangentes.

4. El punto $\mathcal{O}$ lo llamaremos *punto al infinito*. Es el único punto en la recta del infinito que satisface la forma proyectiva de la ecuación de Weierstrass.

2.1.1. La ecuación simplificada de Weierstrass

Definición 2.2. *Dos curvas elípticas E_1 y E_2 definidas sobre K y dadas por las ecuaciones de Weierstrass:*

$$\begin{aligned} E_1: \ y^2 + a_1 xy + a_3 y &= x^3 + a_2 x^2 + a_4 x + a_6 \\ E_2: \ y^2 + \bar{a}_1 xy + \bar{a}_3 y &= x^3 + \bar{a}_2 x^2 + \bar{a}_4 x + \bar{a}_6 \end{aligned}$$

se dicen isomorfos sobre K si existe u, r, s, $t \in K$, $u \neq 0$, tal que el cambio de variables:

$$(x, y) \to (u^2 x + r, u^3 y + u^2 s x + t) \tag{2.3}$$

transforma la ecuación E_1 a E_2. Esta transformación es llamada un cambio admisible de variable.

Dado $(x, y) \in E(K)$, entonces la ecuación de Weierstrass

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

puede ser simplificado considerando el cambio admisible de variable.
Analicemos tres casos:

1. Si la característica de K no es 2 ni 3, el cambio admisible de variable:

$$(x, y) \to \left(\frac{x - 3a_1^2 - 12a_2}{36}, \frac{y - 3a_1x}{216} - \frac{a_1^3 + 4a_1a_2 - 12a_3}{24}\right)$$

Transforma a E en la curva:

$$y^2 = x^3 + ax + b \tag{2.4}$$

donde a, $b \in K$, siendo $\Delta = -16(4a^3 + 27b^2)$

2. Si la característica de K es 2, debemos considerar dos casos.
Si $a_1 \neq 0$, entonces, el cambio admisible de variable:

$$(a, b) \to \left(a_1^2x + \frac{a_3}{a_1}, a_1^3y + \frac{a_1^2a_4 + a_3^2}{a_1^3}\right)$$

transforma a E en la curva:

$$y^2 + xy = x^3 + ax^2 + b \tag{2.5}$$

donde a, $b \in K$, siendo $\Delta = b$. Esta curva es no singular si y solo si $b \neq 0$.
Si $a_1 = 0$, entonces, el cambio admisible de variable:

$$(x, y) \to (x + a_2, y)$$

transforma a E en la curva:

$$y^2 + cy = x^3 + ax + b \tag{2.6}$$

donde a, b, $c \in K$, siendo $\Delta = c^4$. Esta curva es no singular si y solo si $c \neq 0$.

3. Si la característica de K es 3, debemos considerar dos casos.

Si $a_1^2 \neq -a_2$, entonces el cambio admisible de variables

$$(x, y) \to \left(x + \frac{d_4}{d_2} \text{ , y } + a_1 x + a_1 \frac{d_4}{d_2} + a_3 \right)$$

Siendo $d_2 = a_1^2 + a_2$ y $d_4 = a_4 - a_1 a_3$

Transforma a E en la curva:

$$y^2 = x^3 + ax^2 + b \tag{2.7}$$

donde a, b, $\in K$, siendo $\Delta = -a^3 b$.

Si $a_1^2 = -a_2$, entonces el cambio admisible de variable

$$(x, y) \to (x, y + a_1 x + a_3)$$

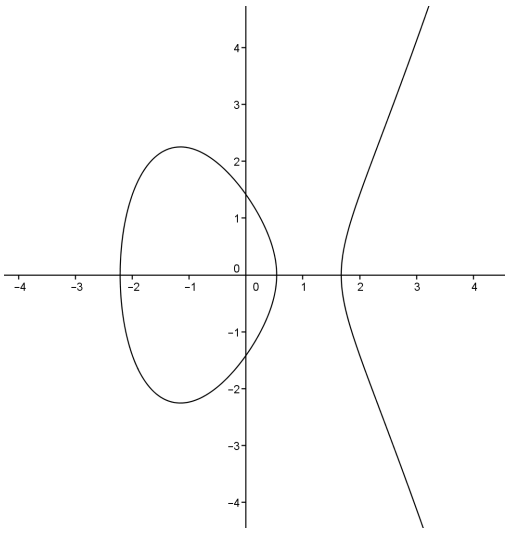
transforma a E en la curva:

$$y^2 = x^3 + ax + b \tag{2.8}$$

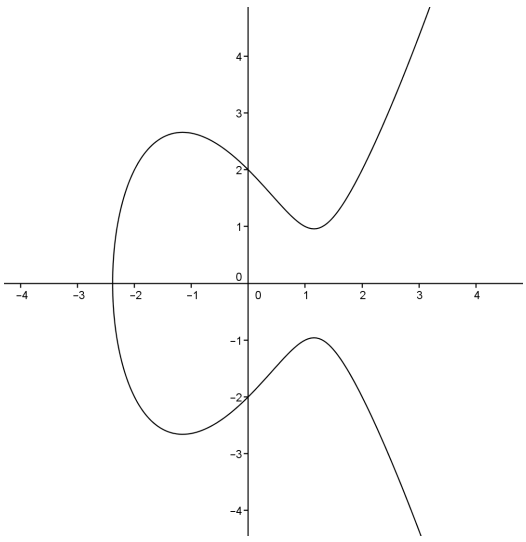
donde a, b, $\in K$, siendo $\Delta = -a^3$.

Como no es posible visualizar las gráficas de curvas elípticas sobre todos los cuerpos arbitrarios, los ejemplos se abordarán en $\mathbb{R}$.

Ejemplos



$y^2 = x^3 - 4x + 2$



$y^2 = x^3 - 4x + 4$

2.2. Puntos de la curva elíptica en el plano proyectivo

Definición 2.3. *Un polinomio $F \in K[X, Y, Z]$ se dice que es homogéneo de grado positivo n si todos sus términos poseen el mismo grado n.*

Es decir un polinomio $F \in K[X, Y, Z]$ es homogéneo de grado n si

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^n F(X, Y, Z)$$

para todo $\lambda \in K$.

Definición 2.4. *Dado un polinomio $F \in K[X, Y, Z]$ homogéneo no constante, definamos el conjunto de los K-puntos racionales de la curva proyectiva sobre el cuerpo K como*

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

Observaciones:

1. Si $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ con (x_1, y_1, z_1) y (x_2, y_2, z_2) pertenecientes a $(x : y : z) \in C(K)$ entonces

   $$F(x_1, y_1, z_1) = 0 \text{ si y sólo si } F(x_2, y_2, z_2) = 0,$$

   esto quiere decir que no depende de quién sea el representante.

2. Si $F(X, Y, Z)$ fuese un polinomio no homogéneo no podríamos hablar de un cero en $\mathbb{P}^2_K$, esto debido a que si el polinomio por ejemplo fuese $F(X, Y, Z) = X^3 + 2XY - 3Z$ tenemos que $F(1, 1, 1) = 0$ sin embargo $F(3, 3, 3) = 36$, aquí si dependería de su representante, este es uno de los motivos por lo que trabajaremos con polinomios homogéneos.

3. El polinomio $f(X, Y) = Y^2 - X^3 - AX - B$ puede ser transformado a un polinomio homogéneo agregandole potencias de Z, de la siguiente manera $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$.

Veamos el significado de que dos rectas paralelas se cortan en el infinito. Sean

$$y = mx + b_1, \;\; y = mx + b_2$$

dos rectas paralelas con $b_1 \neq b_2$, su forma homogénea sería

$$y = mx + b_1 z, \;\; y = mx + b_2 z.$$

Al resolver ambas ecuaciones se tiene que $z = 0$ y $y = mx$ con $x \neq 0$ por lo tanto estas rectas se intersectan en el punto

$$(x : mx : 0) = (1 : m : 0).$$

De igual manera, si $x = c_1$ y $x = c_2$, con $c_1 \neq c_2$ su forma homogénea sería

$$x = c_1 z, \;\; x = c_2 z.$$

Resolviendo tendríamos que $z = 0$ y $x = 0$, entonces $y \neq 0$ por lo tanto el punto de intersección de ambas rectas sería

$$(0 : y : 0) = (0 : 1 : 0).$$

Para el caso de una curva elíptica, veamos que puntos se encuentran en el infinito. Sea la curva elíptica $y^2 - x^3 - Ax - B = 0$ definida sobre K , su forma homogénea sería $y^2 z - x^3 - Axz^2 - Bz^3 = 0$, los puntos en la curva elíptica original de la forma (x, y) corresponden a los puntos $(x : y : 1)$ en su forma homogénea, pero si $z = 0$ entonces $x = 0$ y como $(x, y, z) \neq (0, 0, 0)$, tenemos que el único punto de $\mathbb{P}^2_K$ que pertenece a la curva elíptica es

$$(0 : y : 0) = (0 : 1 : 0) = (0 : -1 : 0).$$

Es más, debido a que $(0 : 1 : 0)$ pertenece a una recta vertical podemos afirmar que toda recta vertical intersecta a la curva elíptica E en dicho punto, esto ocurre en $\mathbb{P}_K$.

2.3. Ley de grupo

Definición 2.5. *Sea E una curva elíptica definida por la ecuación $y^2 = x^3 + Ax + B$ sobre un cuerpo K de característica distinta de 2 y 3. Definimos la operación binaria*

$$+ : E(K) \times E(K) \to E(K)$$

como sigue:
Dado un par de puntos $P = (x_1; y_1)$ y $Q = (x_2; y_2)$ que pertenecen a la curva elíptica $E(K)$, tracemos una recta L que pase a través de P y Q. Vemos que L intersecta a la curva E en un tercer punto R'.Reflejamos R' sobre el eje X (cambia el signo de la segunda coordenada del punto R'). Definimos $P + Q = -R' = R$

Teorema 2.6. *El conjunto $E(K)$ con la operación definida anteriormente posee la estructura de un grupo abeliano. Es decir:*

1. *Dados P_1 y P_2 puntos en $E(K)$ se tiene que $P_1 + P_2 \in E(K)$ (Clausura)*
2. *$P+\mathcal{O}=P$, para todo $P \in E(K)$ (Existencia del neutro)*
3. *Dado $P \in E(K)$ existe un $P' \in E(K)$ con $P + P' = \mathcal{O}$. Este punto P' se denota por $-P$. (Existencia del inverso)*
4. *$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ para todo $P_1, P_2, P_3 \in E(K)$. (Asociatividad)*
5. *$P_1 + P_2 = P_2 + P_1$, para todo $P_1, P_2 \in E(K)$ (Conmutatividad)*

Demostración. Consultar [8,p.28] □

2.3.1. La fórmula de adición

Supongamos primero que $P_1 \neq P_2$ y que ningún punto es $\mathcal{O}$. Tracemos la recta L que pasa a través de P_1 y P_2, su pendiente será:

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Se presentan dos casos:

1. Si $x_1 \neq x_2$, la recta L esta dada por

$$y = m(x - x_1) + y_1$$

Para ver donde intersecta la recta L a la curva elíptica E, reemplazamos y en la ecuación de la curva

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Ordenando obtenemos

$$0 = x^3 - m^2x^2 + \ldots$$

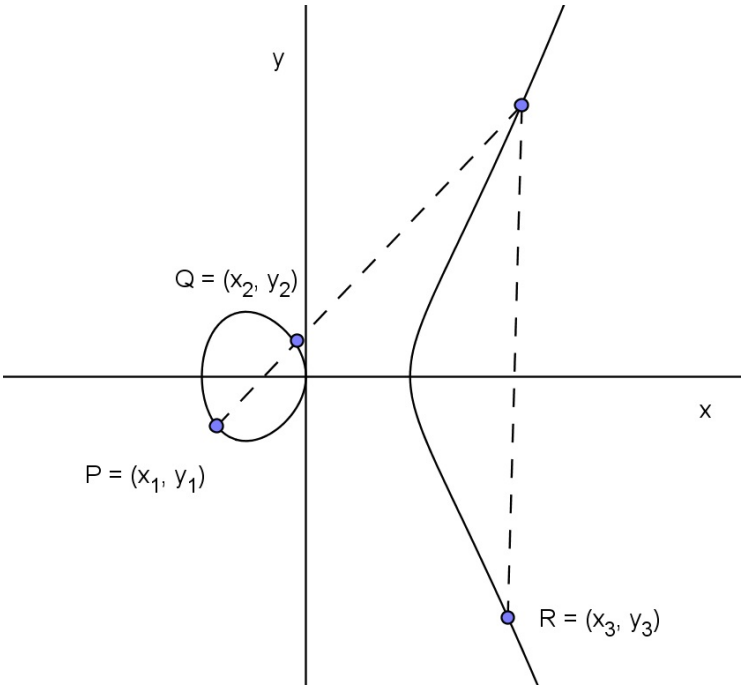
Las tres raíces de esta ecuación cúbica corresponden a los tres puntos de intersección de L con E. Como P_1, P_2 son puntos de L y E entonces se conoce dos raíces de esta ecuación que serían las primeras coordenadas de estos puntos se puede conocer la tercera raíz x, ya que $x_1+x_2+x = m^2$, ordenando obtenemos:

$$\begin{aligned} x &= m^2 - x_1 - x_2 \\ y &= m(x - x_1) + y_1 \end{aligned}$$

Ahora reflejando sobre el $eje\, x$ obtenemos el punto $P_3 = (x_3, y_3)$ con

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

2. Si $x_1 = x_2$ pero $y_1 \neq y_2$, la recta que pasa por P_1 y P_2 es una recta vertical por lo tanto intersecta a E en $\mathcal{O}$. Reflejando $\mathcal{O}$ respecto al $eje\, x$ genera el mismo punto $\mathcal{O}$. Por lo tanto, en este caso $P_1 + P_2 = \mathcal{O}$.



2.3.2. La fórmula de duplicación

Ahora consideremos el caso donde $P_1 = P_2 = P = (x_1, y_1)$. La recta que pasa por esos puntos es una recta tangente. Por lo tanto, cuando dos puntos coinciden tomamos una recta L que pase por ellos, esta será la recta tangente. Calculemos la pendiente m de esta recta L:

$$2y\frac{dy}{dx} = 3x^2 + A \text{ , } entonces \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

1. Si $y_1 = 0$ entonces la recta es vertical y $P_1 + P_2 = \mathcal{O}$, además el numerador $3x_1^2 + A \neq 0$.

2. Si $y_1 \neq 0$, la recta L es:

$$y = m(x - x_1) + y_1$$

De igual manera como en el caso anterior obtenemos la ecuación cúbica

$$0 = x^3 - m^2x^2 + ...$$

En este caso sólo conocemos una raíz, digamos que sea x_1, pero es una raíz doble, ya que L es tangente a E en P y sea $2P = (x_3, y_3)$. Por lo tanto

$$\begin{aligned} x_3 &= m^2 - 2x_1 \\ y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

Reemplazando $m = \frac{3x_1^2+A}{2y_1}$ obtenemos que

$$x_3 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2} \tag{2.9}$$

y

$$y_3 = \frac{x_1^6 + 5Ax_1^4 + 20Bx_1^3 - 5A^2x_1^2 - 4ABx_1 - A^3 - 8B^2}{(2y_1)^3} \tag{2.10}$$

Esta fórmula de duplicación también puede estar dada en función de una de las raíces del polinomio $p(x) = x^3 + Ax + B$ con $A, B \in K$, supongamos que $r \in K$ es una raíz de dicho polinomio entonces

$$B = -r^3 - Ar$$

reemplazando en la ecuación (2.9) tenemos que

$$\begin{aligned} x_3 &= \frac{x_1^4 - 2Ax_1^2 - 8(-r^3 - Ar)x_1 + A^2}{4y_1^2} \\ &= \frac{x_1^4 - 2Ax_1^2 - 8(-r^3 - Ar)x_1 + A^2}{4y_1^2} + 4r(r^3 + Ar + B) \\ &= \frac{(2rx_1 - x_1^2)^2 + 2(2rx_1 - x_1^2)(A + 2r^2) + (A + 2r^2)^2}{4y_1^2} + r \end{aligned}$$

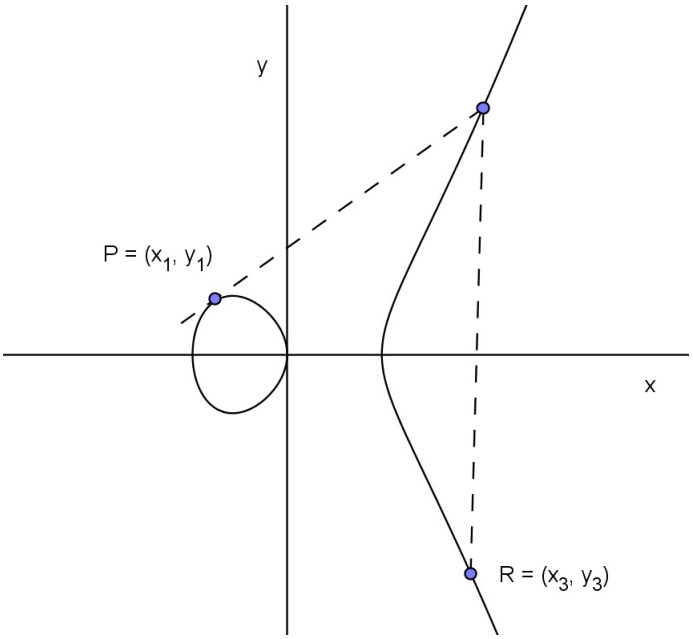
Por lo tanto

$$x_3 = \big[\frac{-x_1^2 + 2rx_1 + A + 2r^2}{2y_1}\big]^2 + r \tag{2.11}$$

Finalmente supongamos $P_2 = \mathcal{O}$. La recta que pasa por P_1 y $\mathcal{O}$ es una recta vertical que intersecta E en el punto P_1' el cuál es reflejada por P_1 respecto al $eje\, X$ para conseguir $P_3 = P_1 + P_2$. Por lo tanto

$$P_1 + \mathcal{O} = P_1$$

para todo P_1 en E. Podemos decir además que $\mathcal{O} + \mathcal{O} = \mathcal{O}$. Notemos que, si P_1 y P_2 tienen coordenadas en un cuerpo K con $A, B \in K$ entonces $P_1 + P_2$ también tiene coordenadas en K. Por lo tanto $E(K)$ es cerrado con la suma de puntos.



Ejemplo 2.7. Para la curva elíptica definida sobre $\mathbb{R}$, dada por:

$$Y^2 = X^3 + 2X + 3$$

Sean $P_1 = (-1, 0)$ y $P_2 = (0, \sqrt{3})$, puntos de dicha curva.
Luego tenemos que:

$$P_1 + P_2 = (4; -8, 66)$$

Ejemplo 2.8. Para la curva elíptica definida sobre $\mathbb{R}$, dada por:

$$Y^2 = X^3 + X + 1$$

Sean $P_1 = P_2 = (2, \sqrt{11})$, puntos de dicha curva. Luego tenemos:

$$P_1 + P_2 = (-0, 16; 0, 915)$$

Es bien sabido que el grupo de torsión de una curva elíptica está conformado por toda los puntos de la curva elíptica que tienen orden finito. Veremos un teorema que nos permita hallar el grupo de torsión de una curva elíptica el cual fue demostrado por Lutz-Nagell:

2.3.3. El teorema de Lutz-Nagell

Teorema 2.9. *(Teorema de Lutz-Nagell)*
Sea E una curva elíptica dada por $Y^2 = X^3 + AX + B$ con $A, B \in \mathbb{Z}$. Sea $P = (x, y) \in E(\mathbb{Q})$ se cumple:

1. *Si P tiene orden finito entonces $x, y \in \mathbb{Z}$.*
2. *Si P tiene orden finito con $y \neq 0$ entonces $y^2 \mid 4A^3 + 27B^2$.*

Demostración. Consultar [14,p.205] □

Ejemplo 2.10. Sea la curva elíptica dada por

$$Y^2 = X^3 - 2$$

Si $y = 0$ entonces $x^3 - 2 = 0$, pero esta ecuación no posee soluciones racionales, por lo tanto $y \neq 0$. Sea $P = (x, y) \in E(\mathbb{Q})$ con orden finito entonces $y^2 \mid 4A^3 + 27B^2 = 108$. Los posibles valores para y son:

$$y = \pm 1, \pm 2 \pm 3 \pm 6.$$

Notamos que ningún valor de y produce un valor entero para x, así el único elemento del subgrupo de torsión es el neutro. Luego

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$$

Ejemplo 2.11. Sea la curva elíptica dada por

$$Y^2 = X^3 + 4X$$

Si $y = 0$, entonces $x = 0; -4$, El punto $(0, 0)$ tiene orden 2. Sea $P = (x, y) \in E(\mathbb{Q})$ con orden finito entonces si $y \neq 0$, tenemos $y^2 \mid 4A^3 + 27B^2 = 16$. Los posibles valores para y son:

$$y = \pm 1, \pm 2 \pm 4.$$

Trabajando todas las posibilidades obtenemos los puntos $(2, -4)$ y $(2, 4)$. Rápidamente se muestra que $2(2, \pm 4) = \mathcal{O}$ Por lo tanto, el subgrupo de torsión es cíclico de orden 2.

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (-2, -4), (-2, 4)\}$$

Capítulo 3

Curvas elípticas sobre $\mathbb{Q}$

En este capítulo veamos que el conjunto de puntos racionales de una curva elíptica denotada por $E(\mathbb{Q})$ es un grupo finitamente generado. La demostración se basará en la aplicación del teorema de Mordell, para ello, en la sección 1 demostraremos el teorema del descenso, en donde dado un grupo abeliano A en el cual se define una función altura que cumple con ciertas hipótesis, y un entorno $m \leq 2$ tal que A/mA es finito , lleva a que A es finito.
En la sección 2 demostraremos el teorema débil de Mordell, el cual nos asegura que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.
Por último, en la sección 3 definiremos una función altura en el grupo abeliano $E(\mathbb{Q})$, de modo que, aplicando los teoremas de las secciones anteriores, llegaremos a demostrar el teorema de Mordell.

3.1. El teorema del descenso

Definición 3.1. *Sea $(A, \oplus)$ un grupo abeliano y sea $h : A \to \mathbb{R}$ una función. Decimos que h es una función altura si cumple:*

(i) Dado $Q \in A$, existe una constante $C_1 = C_1(Q)$ que depende de Q y A, tal que para todo $P \in A$,

$$h(P \oplus Q) \leq 2h(P) + C_1$$

(ii) Existe un entero $m \geq 2$ y una constante C_2 que depende sólo de A, tal que

para todo $P \in A$,

$$h(mP) \geq m^2 h(P) - C_2$$

(iii) Para cualquier constante C_3,

$$\{P \in A : h(P) \leq C_3\} \text{ es un conjunto finito.}$$

Teorema 3.2. *(Teorema del descenso)*
Sea $(A; \oplus)$ *un grupo abeliano y* $h : A \to \mathbb{R}$ *una función altura. Si para el entero* m *de (ii) el grupo* A/mA *es finito, entonces* A *es finitamente generado.*

Demostración. Supongamos que el grupo m/mA tenga r elementos. Elegimos $Q_1, ..., Q_r \in A$, representantes de las clases de A/mA. Sea $P \in A$, luego

$$\exists i_1 \in \{1, ...r\} \text{ y } \exists P_1 \in A \text{ tal que } P = mP_1 \oplus Q_{i_1}$$

Procediendo inductivamente se tiene

$$\begin{aligned} P_1 &= mP_2 \oplus Q_{i_2}, \\ &\vdots \\ P_{n-1} &= mP_n \oplus Q_{i_n}, \end{aligned}$$

es decir:

$$\begin{aligned} P &= Q_{i_1} \oplus mP_1 = Q_{i_1} \oplus mQ_{i_2} \oplus m^2 P_2 \ldots = \\ &= m^n P_n \oplus \textstyle\sum_{j=1}^{n} m^{j-1} Q_{i_j}. \end{aligned}$$

Por tanto

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

Ahora para cada j, por (ii) se tiene:

$$h(mP_j) \geq m^2 h(P_j) - C_2,$$

de donde

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

Al usar (i) se tiene

$$h(P_j) \leq \frac{1}{m^2}[2h(P_{j-1}) + C_1' + C_2] \tag{3.1}$$

donde $C_1' = \underset{1\leq i\leq r}{\max}\{C_1(-Q_i)\}$ (C_1' y C_2 no dependen de P_j). Al repetir la desigualdad (3.1) se tiene

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

Como $m \geq 2$ entonces

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

Así, para n suficientemente grande, se cumplirá que

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

Por lo tanto todo elemento de A es una combinación lineal de puntos del conjunto

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

el cual es un conjunto finito y por la propiedad (iii) se tiene que A es finitamente generado. □

En resumen para encontrar generadores de A se debe seguir los siguientes pasos

1. Calcular las constantes $C_1 = C_1(Q_i)$, para cada elemento $Q_1, \ldots Q_i \in A$, representantes de las distintas clases de A/mA.

2. Calcular la constante C_2.

3. Para cualquier constante C_2, deberemos ser capaces de encontrar los elementos en el conjunto finito $\{P \in A : h(P) \leq C_3\}$.

Se pueden obtener estas constantes para las funciones altura, que se define en curvas elípticas, para encontrar elementos en $E(K)$ que generen el grupo finito $E(K)/mE(K)$. Desafortunadamente no se conoce ningún método que nos proporcione generadores para $E(K)/mE(K)$.

3.2. El teorema débil de Mordell-Weil

Teorema 3.3. *(Teorema débil de Mordell Weil. Caso especial). Sea E una curva elíptica definida sobre $\mathbb{R}$, por*

$$y^2 = x^3 + Ax + B, \text{ donde } A, B \in \mathbb{Q}.$$

Y supongamos que las raíces de $p(x) = x^3 + Ax + B$, e_1, e_2, e_3 están en $\mathbb{Q}$. Entonces

$$E(\mathbb{Q})/2E(\mathbb{Q})$$

es un grupo finito.

Antes de la prueba de este teorema, mencionamos algunos resultados que nos seran necesarios:

Sea E un curva elíptica de la forma

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

con $e_1, e_2, e_3 \in \mathbb{Z}$ y $e_i \neq e_j$ para $i \neq j$. Sea $(x, y) \in E(\mathbb{Q})$ con $y \neq 0$.
Sean:

$$\begin{aligned} x - e_1 &= au^2 \\ x - e_2 &= bv^2 \\ x - e_3 &= cw^2 \end{aligned}$$

con $a, b, c, u, v, w \in \mathbb{Q}$. Entonces $y^2 = abc(uvw)^2$ con $a, b, c \in \mathbb{Z}$, es mas, podemos suponer que $a, b, c \in \mathbb{Z}$ son libres de cuadrados.

Teorema 3.4. *Sea*

$$S = \{p \in \mathbb{Z} : p \text{ es primo y } p|(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

Si p es primo y $p|abc$, entonces $p \in S$

Demostración. Sea $p|abc$, entonces $p|a$, $p|b$ o $p|c$. Supongamos que $p|a$. Como $x-e_1 = au^2$, entonces p^k, con $k \in \mathbb{Z}$ impar, es la potencia exacta de p dividiendo $x - e_1$.
$k > 0$, en efecto, si $k < 0$, entonces p^{-k} es la potencia exacta de p en el denominador de x, ya que $e_1 \in \mathbb{Z}$. Así mismo p^{-k} es la potencia exacta de p en el denominador de $x - e_2$ y en el de $x - e_3$, ya que $e_2, e_3 \in \mathbb{Z}$. Entonces p^{-3k} es la potencia exacta de p en el denominador

$$(x - e_1)(x - e_2)(x - e_3) = y^2$$

lo cual es un contradicción, puesto que $3k$ es impar. Así, $k > 0$ ($k = 0$ no puede ocurrir ya que hemos supuesto que $p|a$, y por tanto, p es un factor de $x - e_1 = au^2$), esto es, $x \equiv e_1$ mód p. x no tiene p en el denominador puesto que $x \equiv e_1$ mód p y $e_1 \in \mathbb{Z}$.
Como $x - e_2 = cv^2$, tenemos que

$$bv^2 \equiv e_1 - e_2 \text{ mód } p,$$

y puesto que $x - e_3 = cw^2$,

$$cw^2 \equiv e_1 - e_3 \text{ mód } p,$$

Supongamos que $p \notin S$, luego $p \nmid (e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Así, tenemos que

$$p \nmid (x - e_2) \text{ y } p \nmid (x - e_3),$$

Entonces p^k es la potencia exacta de p en el numerador de $(x - e_1)(x - e_2)(x - e_3)$. Luego p^k, con k impar, es la potencia de p en el numeral de y^2, lo cual es una contradicción.
Por tanto $p \in S$ □

Teorema 3.5. *Sea E una curva elíptica dada por*

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

definida sobre $\mathbb{Q}$, con $e_1, e_2, e_3 \in \mathbb{Z}$. La función definida por

$$\phi\colon E(\mathbb{Q}) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \bigoplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \bigoplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2)$$

$$\phi(x,y) = \begin{cases} (\overline{x-e_1}, \overline{x-e_2}, \overline{x-e_3}) & si \quad y \neq 0 \\ (\overline{1}, \overline{1}, \overline{1}) & si \quad (x,y) = \mathcal{O} \\ (\overline{(e_1-e_2)(e_1-e_3)}, \overline{e_1-e_2}, \overline{e_1-e_3}) & si \quad (x,y) = (e_1,0) \\ (\overline{e_2-e_1}, \overline{(e_2-e_1)(e_2-e_3)}, \overline{e_2-e_3}) & si \quad (x,y) = (e_2,0) \\ (\overline{e_3-e_1}, \overline{e_3-e_2}, \overline{(e_3-e_1)(e_3-e_2)}) & si \quad (x,y) = (e_3,0) \end{cases}$$

es un homomorfismo y su nucleo es $2E(\mathbb{Q})$.

Demostración.

ϕ es un homomorfismo

En efecto, analicemos por casos:

1. Si $P_i = (x_i, y_i) \in E(\mathbb{Q})$, $i = 1,2,3$ tales que $y_i \neq 0$ y $P_3 = -(P_1 + P_2)$, como P_1, P_2, P_3 son colineales, entonces sea la recta $y = ax + b$ que contiene a dichos puntos. Sea el polinomio

$$P(X) = (X-e_1)(X-e_2)(X-e_3) - (aX+b)^2$$

De raíces x_1, x_2, x_3. Notemos que $P(X)$ posee coeficiente principal 1, luego podemos escribir

$$P(X) = (X-e_1)(X-e_2)(X-e_3) - (aX+b)^2 = (X-x_1)(X-x_2)(X-x_3)$$

Notemos que:

$$\begin{aligned} \phi(x_1,y_1) &= (\overline{x_1-e_1}, \overline{x_1-e_2}, \overline{x_1-e_3}) = \phi(P_1) \\ \phi(x_2,y_2) &= (\overline{x_2-e_1}, \overline{x_2-e_2}, \overline{x_2-e_3}) = \phi(P_2) \\ \phi(x_3,y_3) &= (\overline{x_3-e_1}, \overline{x_3-e_2}, \overline{x_3-e_3}) = \phi(P_3) \end{aligned}$$

Entonces

$$\begin{aligned} \phi(P_1)\phi(P_2)\phi(P_3) = &(\overline{(x_1-e_1)(x_2-e_1)(x_3-e_1)}, \overline{(x_1-e_2)(x_2-e_2)(x_3-e_2)}, \\ &\overline{(x_1-e_3)(x_2-e_3)(x_3-e_3)}) = (\overline{1}, \overline{1}, \overline{1}), \end{aligned}$$

pues evaluando cada e_i con $i = 1,2,3$, tenemos:

$$(x_1-e_i)(x_2-e_i) = (ae_i+b)^2 \in (\mathbb{Q}^*)^2$$

Ahora: $\phi(P_1+P_2+P_3)=\phi((-P_3)+P_3)=\phi(\mathcal{O})=(\overline{1},\overline{1},\overline{1})$
Por lo anterior

$$\phi(P_1)\phi(P_2)\phi(P_3)=\phi(P_1+P_2+P_3)$$

2. Si $P_1=(x_1,0)$ y $P_2=(x_2,y_2)$ con $y_2\neq 0$, luego $P_3=-(P_1+P_2)=(x_3,y_3)$, con $y_3\neq 0$, por lo anterior tenemos que $\phi(P_2+P_3)=\phi(P_2)\phi(P_3)$, reemplazando $P_3=-(P_1+P_2)$ tenemos que

$$\begin{aligned}\phi(-P_1) &= \phi(P_2+-(P_1+P_2))\\ &= \phi(P_2)\phi(-(P_1+P_2))\end{aligned}$$

En consecuencia

$$\phi(P_1+P_2)=\phi(P_1)\phi(P_2)$$

3. Si $P_1=\mathcal{O}$ y $P_2\neq\mathcal{O}$, tenemos que

$$\phi(P_1+P_2)=\phi(P_2)=(\overline{1},\overline{1},\overline{1})\phi(P_2)=\phi(P_1)\phi(P_2)$$

El caso en que $P_2=\mathcal{O}$ y $P_1\neq\mathcal{O}$ es similar.

4. Si $P_1=(x_1,0)$ y $P_2=(x_2,0)$, puesto que $x_i\in\{e_1,e_2,e_3\}$, podemos considerar $P_1=(e_1,0)$ y $P_2=(e_2,0)$, obteniendo:

$$\begin{aligned}\phi(P_1) &= (\overline{(e_1-e_2)(e_1-e_3)},\overline{e_1-e_2},\overline{e_1-e_3})\\ \phi(P_2) &= (\overline{e_2-e_1},\overline{(e_2-e_1)(e_2-e_3)},\overline{e_2-e_3})\end{aligned}$$

En consecuencia

$$\begin{aligned}\phi(P_1)\phi(P_2) = {} & (\overline{(e_1-e_2)(e_1-e_3)(e_2-e_1)},\overline{(e_1-e_2)(e_2-e_1)(e_2-e_3)},\\ & \overline{(e_1-e_3)(e_2-e_3)})\end{aligned}$$

Puesto $P_1+P_2=P_3$, tenemos que

$$\phi(P_1+P_2)=(\overline{(e_3-e_1)},\overline{(e_3-e_2)},\overline{(e_3-e_1)(e_3-e_2)})$$

Por lo tanto ϕ es un homomorfismo.
Así queda probado que ϕ es un homomorfismo

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

1. $2E(\mathbb{Q}) \subset ker(\phi)$: Sea $P \in 2E(\mathbb{Q})$ entonces existe $Q \in E(\mathbb{Q})$ tal que $P = 2Q$, entonces

$$\phi(P) = \phi(Q+Q) = \phi(Q)\phi(Q) = \overline{1}$$

De ahí que $P \in ker(\phi)$. Por lo tanto

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

2. $ker(\phi) \subset 2E(\mathbb{Q})$: Sea $P = (x, y) \in ker(\phi)$, entonces

$$x - e_i = v_i^2,\ i = 1, 2, 3.$$

Por simplicidad, asumamos que $e_1+e_2+e_3 = 0$, lo que significa que la ecuación para nuestra curva elíptica tiene la forma $y^2 = x^3 + Ax + B$. Cuando $e_1 + e_2 + e_3 \neq 0$, el coeficiente de x^2 es diferente de cero, podemos hacer un cambio de variable. Sea $f : \mathbb{R} \to \mathbb{R}$ una función tal que

$$f(T) = u_0 + u_1T + u_2T^2$$

tal que $f(e_i) = v_i$, $i = 1, 2, 3$. Para probar la existencia de f es suficiente tomar:

$$f(T) = v_1\frac{1}{(e_1 - e_2)(e_1 - e_3)}(T-e_2)(T-e_3)+v_2\frac{1}{(e_2 - e_1)(e_2 - e_3)}(T-e_1)(T-e_3)$$
$$+ v_3\ \tfrac{1}{(e_3-e_1)(e_3-e_2)}\ (T - e_1)(T - e_2)$$

Definamos $g(T) = x - T - f(T)^2$ tal que cumple $g(e_i) = 0, i = 1, 2, 3$, y

$$T^3 + AT + B = (T - e_1)(T - e_2)(T - e_3)\, divide\, a\, g(T)$$

Por lo tanto $g(T) \equiv 0\, mod\, (T^3 + AT + B)$, así

$$x - T \equiv (u_0 + u_1T + u_2T^2)^2\, mod(\, T^3 + AT + B).$$

Sabemos

$$T^3 \equiv -AT - B\, mod\, (T^3 + AT + B)$$

$$T^4 \equiv T \cdot T^3 \equiv -AT^2 - BT \, mod \, (T^3 + AT + B).$$

Por lo tanto

$$\begin{aligned} x - T &\equiv (u_0 + u_1 T + u_2 T^2)^2 \\ &\equiv u_0^2 + 2u_0 u_1 T + (u_1^2 + 2u_0 u_2)T^2 + 2u_1 u_2 T^3 + u_2^2 T^4 \\ &\equiv (u_0^2 - 2Bu_1 u_2) + (2u_0 u_1 - 2Au_1 u_2 - Bu_2^2)T \\ &\quad +(u_1^2 + 2u_0 u_2 - Au_2^2)T^2. \end{aligned}$$

Por otro lado si dos polinomios P_1 y P_2 de grado a los más 2 son congruentes módulo un polinomio de grado 3, entonces la diferencia $P_1 - P_2$ es un polinomio de grado a lo más 2 que es divisible por un polinomio de grado 3. Esto significa que $P_1 = P_2$. Por lo tanto

$$x = u_0^2 - 2Bu_1 u_2 \tag{3.2}$$

$$-1 = 2u_0 u_1 - 2Au_1 u_2 - Bu_2^2 \tag{3.3}$$

$$0 = u_1^2 + 2u_0 u_2 - Au_2^2. \tag{3.4}$$

Si $u_2 = 0$, reemplazando en (3.4) tenemos que también $u_1 = 0$. Entonces $f(T)$ es constante, así $v_1 = v_2 = v_3$. Esto significa que $e_1 = e_2 = e_3$, lo cual es una contradicción. Por lo tanto $u_2 \neq 0$, multiplicando (3.4) por u_1/u_2^3 y multiplicando otra vez a la misma ecuación (3.4) por $1/u_2^2$, restando las nuevas ecuaciones obtenemos

$$(\frac{1}{u_2})^2 = (\frac{u_1}{u_2})^3 + A(\frac{u_1}{u_2}) + B.$$

Sea

$$x_1 = \frac{u_1}{u_2}, \; y_1 = \frac{1}{u_2}$$

así $(x_1, y_1) \in E(\mathbb{Q})$. Afirmamos que $2(x_1, y_1) = \pm(x, y)$.
De la ecuación (3.4) tenemos que

$$u_0 = \frac{Au_2^2 - u_1^2}{2u_2} = \frac{A - x_1^2}{2y_1}.$$

Reemplazando esto en (3.2) tenemos

$$x = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2}.$$

Esta es la primera coordenada de $2(x_1, y_1)$ por (2.9). La segunda coordenada esta determinada por la primera coordenada, así $2(x_1, y_1) = (x, \pm y) = \pm(x, y)$. Por lo tanto $(x, y) = 2(x_1, y_1)$ ó $2(x_1, -y_1)$. En ambos casos tenemos que $(x, y) \in 2E(\mathbb{Q})$.

□

Ahora procedamos a demostrar el teorema 3.3

Demostración. Puesto que $e_1, e_2, e_3 \in \mathbb{Q}$, supongamos que $e_1, e_2, e_3 \in \mathbb{Z}$. Del homomorfismo ϕ definido en el teorema 3.5 tenemos el homomorfismo inyectivo inducido,

$$\begin{array}{rcl} \hat{\phi} : E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \oplus (\mathbb{Q}^*/(\mathbb{Q}^*)^2) \\ \overline{(x, y)} & \longmapsto & \hat{\phi}(\overline{(x, y)}) = \phi(x, y). \end{array} \tag{3.5}$$

Del teorema 3.4, si $(\bar{a}, \bar{b}, \bar{c}) \in Im(\hat{\phi})$,, entonces, existe $P = (x, y) \in E(\mathbb{Q})$ tal que

$$\hat{\phi}(\overline{(x, y)}) = \phi((x, y)) = (\bar{a}, \bar{b}, \bar{c}),$$

donde a, b y c son representantes de clase de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, los que pueden ser elegidos enteros libres de cuadrados. Luego a, b y c son productos de primos en el conjunto

$$S = \{p \in \mathbb{Z} : p \text{ es primo y } p|(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)\}.$$

del teorema 3.4. En vista que si $p \in \mathbb{Z}$ es primo tal que $p|a$, entonces $p|abc$ y del teorema 3.4 tenemos que $p \in S$. Puesto que el conjunto S es finito, existén sólo una cantidad finita de factores primos de a. De igual forma, la cantidad de factores primos de b y c es finito. Así, tenemos que existe a lo más una cantidad finita de elementos de

$$\hat{\phi}(E(\mathbb{Q})/2E(\mathbb{Q})) \cong E(\mathbb{Q})/2E(\mathbb{Q}).$$

Lo cual prueba el teorema. □

Definición 3.6. *Sea $\mathbb{Q}^*$ un grupo multiplicativo y su subgrupo $(\mathbb{Q}^*)^2$. Definamos el grupo cociente*

$$\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2} = \{\overline{x} : x \in \mathbb{Q}^*\} \text{ con } \overline{x} = \{xu^2 \in \mathbb{Q}^* : u \in \mathbb{Q}^*\}$$

Esto significa que si consideramos dos números racionales $\overline{x_1}, \overline{x_2}$ como equivalentes entonces la razón x_1/x_2 es el cuadrado de un número racional. Todo elemento de $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ puede ser representado por ± 1 veces un producto de primos distintos, ya que $\overline{x}$ es congruente a $\overline{x^{-1}}$ módulo cuadrados. Así podemos decir que

$$\frac{\mathbb{Q}^*}{(\mathbb{Q}^*)^2} = \{\pm\overline{2^m}\,\overline{3^n}\,\overline{5^p}\ldots \mid m, n, p, \ldots \in \{0, 1\}\} \tag{3.6}$$

Notemos que si $x - e_1 = au^2$, entonces $\overline{x - e_1} = \overline{a}$ en $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Teorema 3.7. *(Caso general del teorema débil de Mordell-Weil) Sea E una curva elíptica definida sobre $\mathbb{Q}$ por*

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

y sea K el cuerpo de descomposición del polinomio cúbico $p(x) = x^3 + Ax + B$ con raíces $e_1, e_2, e_3 \in K$. Entonces

$$E(\mathbb{Q})/2E(\mathbb{Q})$$

es un grupo finito.

Demostración. Para probar el caso general, debemos imitar el caso particular reemplazando $\mathbb{Q}$ por K, con lo que se nos presentan tres problemas:

1. Obtendremos información de $E(K)/2E(K)$ y no de $E(\mathbb{Q})/2E(\mathbb{Q})$. Para tal fin, debemos hallar una relación entre ellos.

2. Para conseguir que $E(\mathbb{Q})/2E(\mathbb{Q})$ sea finito en el teorema anterior usamos el hecho de que el conjunto S definido en el teorema 3.4 sea finito, usando para ello la factorización única en $\mathbb{Z}$. Pero esto podría fallar en el anillo de enteros algebraicos A_K que reemplazará a $\mathbb{Z}$.

3. Como todo elemento de $\mathbb{Q}^*/\mathbb{Q}^{*^2}$, se puede representar como ± 1 veces un producto de primos distintos y ± 1 representa las unidades en $\mathbb{Z}$, estas unidades necesitan ser controladas en el anillo que reemplaza a $\mathbb{Z}$ en el caso general.

El siguiente teorema nos ayudará a cubrir la parte 1).

Teorema 3.8. *Sea E una curva elíptica definida sobre $\mathbb{Q}$ por*

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

Sea K el cuerpo de descomposición de $p(x) = (x - e_1)(x - e_2)(x - e_3) \in \mathbb{Q}[x]$ sobre $\mathbb{Q}$. Entonces el homomorfismo canónico

$$\begin{array}{rccc} \varphi: & E(\mathbb{Q})/2E(\mathbb{Q}) & \to & E(K)/2E(K) \\ & P + 2E(\mathbb{Q}) & \to & P + 2E(K) \end{array}$$

tiene a lo más $2^{2[K:\mathbb{Q}]}$ elementos en su núcleo. En consecuencia, si $E(K)/2E(K)$ es finito, entonces $E(\mathbb{Q})/2E(\mathbb{Q})$ también lo es.

Demostración. Dado $Q \in E(K)$ y $\sigma \in Gal(K/\mathbb{Q})$, entonces $\sigma(Q) = (\sigma(x), \sigma(y)) \in E(K)$, ya que E se encuentra definida sobre Q. Denotemos en adelante $Q^\sigma = \sigma(Q)$. Sea $P \in ker(\varphi)$, entonces $P \in E(\mathbb{Q}) \cap 2E(K)$. Como $P \in 2E(K)$, existe $Q_P \in E(K)$ tal que $P = 2Q_P$.
Para cada $P \in ker(\varphi)$, definamos la función

$$\begin{array}{rccc} \lambda_P: & Gal(K/\mathbb{Q}) & \to & E[2] \\ & \sigma & \to & Q_P^\sigma - Q_P \end{array}$$

siendo

$$E[2] = \{P \in E(K) : 2P = \mathcal{O}\}.$$

La función esta bien definida, pues la imagen de λ_P se encuentra en $E[2]$.
En efecto

$$2(Q_P^\sigma - Q_P) = 2Q_P^\sigma - 2Q_P = P^\sigma - P = \mathcal{O}$$

Afirmamos que si $\lambda_P = \lambda_{P'}$ entonces $P' \in P + 2E(\mathbb{Q})$.
En efecto:
Como $\lambda_P = \lambda_{P'}$, luego

$$Q_P^\sigma - Q_P = \lambda_P(\sigma) = \lambda_{P'}(\sigma) = Q_{P'}^\sigma - Q_{P'} \text{ para todo } \sigma \in Gal(K/\mathbb{Q})$$

Luego:

$$(Q_{P'} - Q_P)^\sigma = Q_{P'} - Q_P.$$

Ahora, puesto que K es una extensión, entonces $K^{Gal(K/\mathbb{Q})} = \mathbb{Q}$.
Por lo tanto $Q_{P'} - Q_P \in E(\mathbb{Q})$. De ahí que

$$P' - P = 2(Q_{P'} - Q_P) \in 2E(\mathbb{Q})$$

Puesto que cada elemento $P \in ker(\varphi)$, podemos asociarlo a λ_P y para cada elemento diferente del núcleo tenemos una función diferente λ_P de $Gal(K/\mathbb{Q})$ a $E[2]$.
Así, el orden del núcleo es menor ó igual al número de funciones de $Gal(K, \mathbb{Q})$ a $E[2]$, el cual está por

$$4^{|Gal(K,\mathbb{Q})|} = 2^{2[K:\mathbb{Q}]}.$$

Al mostrar que $E(K)/2E(K)$ es finito, entonces $E(\mathbb{Q}/2\mathbb{Q})$ también es finito. □

Ahora veamos como resolver los problemas 2) y 3), empecemos viendo unos ejemplos.

Ejemplo 3.9. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

$$Y^2 = X^3 + X$$

El cuerpo de descomposición es $K = \mathbb{Q}(i)$. El anillo de enteros $A_K = \mathbb{Z}[i]$ es un dominio de factorización única y su grupo de unidades es $\{(i)^k\}_{k=0}^{3} \cong \mathbb{Z}_4$

Ejemplo 3.10. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

$$Y^2 = X^3 - 2X$$

El cuerpo de descomposición es $K = \mathbb{Q}(\sqrt{2})$. El anillo de enteros $A_K = \mathbb{Z}[\sqrt{2}]$ es un dominio de factorización única, y su grupo de unidades es el grupo infinito $\{\pm(1 \pm \sqrt{2})^k\}_{k=-\infty}^{\infty}$.

Ejemplo 3.11. Sea E una curva elíptica definida sobre $\mathbb{Q}$ por

$$Y^2 = X^3 + 5X$$

El cuerpo de descomposición es $K = \mathbb{Q}(\sqrt{-5})$. El anillo de enteros algebraicos $A_K = \mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única, ya que $2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$, es mas, estos números son todos primos. El grupo de unidades es $\{\pm 1\} \cong \mathbb{Z}_2$.

Teorema 3.12. *Sea $K|\mathbb{Q}$ una extensión finita. Sea A_K el anillo de enteros algebraicos de K sobre $\mathbb{Q}$. Luego, existe un anillo R con $A_K \subseteq R \subseteq K$, tal que:*

1. *R es un dominio de ideales principales, por tanto un dominio de factorización única.*

2. *El grupo de unidades de R es finitamente generado.*

Demostración. Consultar [6,p.122] □

Teorema 3.13. *Sea E una curva elíptica dada por $y^2 = (x-e_1)(x-e_2)(x-e_3)$, definida sobre $\mathbb{Q}$, con $e_1, e_2, e_3 \in R$. La función definida por*

$$\phi\colon E(K) \to (K^*/(K^*)^2) \bigoplus (K^*/(K^*)^2) \bigoplus (K^*/(K^*)^2)$$

$$\phi(x,y) = \begin{cases} (\overline{x-e_1}, \overline{x-e_2}, \overline{x-e_3}) & si \quad y \neq 0 \\ (\overline{1}, \overline{1}, \overline{1}) & si \quad (x,y) = \mathcal{O} \\ (\overline{(e_1-e_2)(e_1-e_3)}, \overline{e_1-e_2}, \overline{e_1-e_3}) & si \quad (x,y) = (e_1,0) \\ (\overline{e_2-e_1}, \overline{(e_2-e_1)(e_2-e_3)}, \overline{e_2-e_3}) & si \quad (x,y) = (e_2,0) \\ (\overline{e_3-e_1}, \overline{e_3-e_2}, \overline{(e_3-e_1)(e_3-e_2)}) & si \quad (x,y) = (e_3,0) \end{cases}$$

es un homomorfismo y $ker\ (\phi) = 2E(K)$.

Demostración. Reemplazando $\mathbb{Q}$ por K en la prueba del teorema 3.3 tenemos, $e_1, e_2, e_3 \in K = frac(R)$, haciendo un cambio de variables podemos asumir que $e_1, e_2, e_3 \in R$. Del homomorfimo dado en el teorema anterior, tenemos el homomorfismo inyectivo inducido

$$\begin{array}{rccc} \hat{\phi}: & E(K)/2E(K) & \to & (K^*/K^{*^2}) \bigoplus (K^*/K^{*^2}) \bigoplus (K^*/K^{*^2}) \\ & \overline{(x,y)} & \to & \hat{\phi}(\overline{(x,y)}) = \phi((x,y)) \end{array}$$

Por el teorema de homomorfismo de grupos tenemos que

$$E(K)/2E(K) \cong \hat{\phi}(E(K)/2E(K))$$

Afirmamos que $E(K)/2E(K)$ es finito. En efecto basta probar que $\hat{\phi}(E(K)/2E(K))$ es finito. Sea $(\overline{a}, \overline{b}, \overline{c}) \in \hat{\phi}(E(K)/2E(K))$ (considerando a, b, c; enteros libre de cuadrados), entonces existe $P = (x, y) \in E(K)$ tal que

$$\hat{\phi}((\overline{x, y})) = \phi((x, y)) = (\overline{a}, \overline{b}, \overline{c})$$

Por el teorema 3.4, tenemos que los primos de R que dividen a a, b, c; también dividen a $(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)$. Luego, la imagen de ϕ esta contenida en el grupo generado por S y las unidades de R y así las componentes de la imagen de ϕ forman grupos finitamente generados. Como $\hat{\phi}(E(K)/2E(K))$ es finitamente generado y de torsión, entonces $\hat{\phi}(E(K)/2E(K))$ es finito. Por el teorema 3.4 tenemos que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. □

3.3. El teorema de Mordell-Weil

Definición 3.14. *Sea $x = a/b \in \mathbb{Q}$, con $mcd(a, b) = 1$. Definamos*

$$\begin{aligned} \widetilde{H}(x) &= \text{máx}(|a|, |b|) \quad (\textbf{\textit{altura}}\ de\, a/b) \\ \widetilde{h}(x) &= log\widetilde{H}(a/b) \quad (\textbf{\textit{altura logarítmica}}\ de\, a/b). \end{aligned}$$

Definición 3.15. *Sea $P = (x, y) \in E(\mathbb{Q})$, con $P \neq \mathcal{O}$. Definamos*

$$\begin{aligned} H(x, y) &= \widetilde{H}(x) \quad (\textbf{\textit{altura}}\ de\, (x, y)) \\ h(x, y) &= \widetilde{h}(x) \quad (\textbf{\textit{altura logarítmica}}\ de\, (x, y)). \end{aligned}$$

Si $P = \mathcal{O}$, entonces $H(P) = 1$

Teorema 3.16. *Existe una constante c_1 tal que*

$$|h(P + Q) + h(P - Q) - 2h(P) - 2h(Q)| \leq c_1$$

para todo $P, Q \in E(\mathbb{Q})$

Demostración. Afirmamos que existen constantes c' y c'' tales que:

$$2h(P) + 2h(Q) - c' \leq h(P + Q) + h(P - Q) \tag{3.7}$$

$$h(P + Q) + h(P - Q) \leq 2h(P) + 2h(Q) + c'' \tag{3.8}$$

En efecto, comenzaremos probando la segunda desigualdad.
Sea una curva elíptica E dada por $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Sean

$$P = (\frac{a_1}{b_1}, y_1),\ Q = (\frac{a_2}{b_2}, y_2)$$

$$P + Q = (\frac{a_3}{b_3}, y_3),\ P - Q = (\frac{a_4}{b_4}, y_4)$$

con $P, Q \in E(\mathbb{Q})$ y $a_i, b_i \in \mathbb{Z}$ tal que $mcd(a_i, b_i) = 1$, para $i = 1, 2, 3, 4$. Para la adición de dos puntos se tiene:

$$\frac{a_3}{b_3} = m_1^2 - \frac{a_1}{b_1} - \frac{a_2}{b_2} = \ con\ m_1 = \frac{y_2 - y_1}{\frac{a_2}{b_2} - \frac{a_1}{b_1}}$$

$$\frac{a_4}{b_4} = m_2^2 - \frac{a_1}{b_1} - \frac{a_2}{b_2} = \ con\ m_2 = \frac{-y_2 - y_1}{\frac{a_2}{b_2} - \frac{a_1}{b_1}}$$

Efectuando operaciones, obtenemos:

$$\frac{a_3}{b_3} + \frac{a_4}{b_4} = \frac{g_1}{g_3},\ \ \frac{a_3 a_4}{b_3 b_4} = \frac{g_2}{g_3}$$

con

$$\begin{aligned} g_1 &= 2(a_1 b_2 + a_2 b_1)(A b_1 b_2 + a_1 a_2) + 4B b_1^2 b_2^2 \\ g_2 &= (a_1 a_2 - A b_1 b_2)^2 - 4B(a_1 b_2 + a_2 b_1) b_1 b_2 \\ g_3 &= (a_1 b_2 - a_2 b_1) \end{aligned}$$

Los siguientes lemas permitirán continuar la prueba.

Lema 3.17. *Sean $c_1, c_2, d_1, d_2 \in \mathbb{Z}$. Se cumple:*

$$\text{máx}(|c_1|, |d_1|) \leq 2\,\text{máx}(|c_1 c_2|, |c_1 d_2 + c_2 d_1|, |d_1 d_2|).$$

Demostración. Supongamos que $|c_1| \leq |d_1|$, si no fuese así intercambiamos los lugares. Sea L la parte izquierda de la desigualdad del lema y R la parte derecha. Esto indica tres casos:

1. Si $|c_2| \leq |d_2|$, entonces $L = |d_1 d_2|$ y $2|d_1 d_2| \leq R$, así $L \leq R$.

2. Si $|c_2| \geq |d_2| \geq (1/2)|c_2|$, entonces $L = |d_1 c_2|$ y $R \geq 2|d_1 d_2| \geq |d_1 c_2| \geq L$.

3. Si $|d_2| \leq (1/2)|c_2|$, entonces $L = |d_1 c_2|$ y

$$\begin{aligned} R &\geq 2|c_1 d_2 + c_2 d_1| \\ &\geq 2(|c_2 d_1| - |c_1 d_2|) \\ &\geq 2(|c_2 d_1| - |d_1|(1/2)|c_2|) \\ &= |c_2 d_1| = L \end{aligned}$$

Esto completaría la prueba. □

Lema 3.18. *Sean $c_1, c_2, d_1, d_2 \in \mathbb{Z}$, con $mcd(c_i, d_i) = 1$ para $i = 1, 2$. Se cumple*

$$mcd(c_1 c_2, c_1 d_2 + c_2 d_1, d_1 d_2) = 1$$

Demostración. Sea $d = mcd(c_1 d_2 + c_2 d_1, d_1 d_2)$. Sea $p \in \mathbb{Z}$ un número primo tal que $p \mid c_1$ y $p \mid d$. Como $mcd(c_1, d_1) = 1$, entonces $p \nmid d_1$, pero como $p \mid d_1 d_2$, entonces $p \mid d_2$. Así $p \nmid c_2$ ya que $mcd(c_2, d_2) = 1$. Luego $p \mid c_1 d_2$ y $p \nmid c_2 d_1$ entonces $p \nmid c_1 d_2 + c_2 d_1$. Por lo tanto $p \nmid d$, lo cuál es una contradicción. De la misma manera no existe un primo p que divida a c_2 y d. Por tanto no existe un primo p que divida a $c_1 c_2$ y d, con lo cuál queda probado el lema. □

Continuando con la prueba del teorema, como $mcd(a_3, b_3) = 1$ y $mcd(a_4, b_4) = 1$, debido al lema anterior tenemos que

$$mcd(a_3 a_4, a_3 b_4 + a_4 b_3, b_3 b_4) = 1.$$

Luego existen $x, y, z \in \mathbb{Z}$ tales que

$$a_3 a_4 x + (a_3 b_4 + a_4 b_3) y + b_3 b_4 z = 1.$$

Puesto que

$$g_3(a_3 b_4 + a_4 b_3) = g_1(b_3 b_4) \text{ y } g_3(a_3 a_4) = g_2(b_2 b_4), \tag{3.9}$$

tenemos que

$$\begin{aligned} g_3 &= g_3(a_3 a_4)x + g_3(a_3 b_4 + a_4 b_3)y + g_3(b_3 b_4)z \\ &= g_2(b_3 b_4)x + g_1(b_3 b_4)y + g_3(b_3 b_4)z. \end{aligned}$$

Por lo tanto $b_3 b_4 \mid g_3$, así

$$|b_3 b_4| \leq |g_3|.$$

De manera análoga tenemos que

$$|a_3a_4| \leq |g_2|.$$

De la ecuación (3.6) y de $|b_3b_4| \leq |g_3|$ tenemos que

$$|a_3b_4 + a_4b_3| \leq |g_1|.$$

En función de la altura H tenemos que

$$\begin{aligned} H(P+Q)H(P-Q) &= \text{máx}(|a_3|,|b_3|)\,\text{máx}(|a_4|,|b_4|) \\ &\leq 2\,\text{máx}(|a_3a_4|,|a_3b_4+a_4b_3|,|b_3b_4|) \\ &\leq 2\,\text{máx}(|g_2|,|g_1|,|g_3|). \end{aligned}$$

Sean $H_1 = \text{máx}(|a_1|,|b_1|)$ y $H_2 = \text{máx}(|a_2|,|b_2|)$. Entonces

$$\begin{aligned} |g_1| &= |2(a_1b_2+a_2b_1)(Ab_1b_2+a_1a_2+4Bb_1^2b_2^2)| \\ &\leq 2(H_1H_2+H_2H_1)(|A|H_1H_2+H_1H_2)+4|B|H_1^2H_2^2 \\ &\leq 4(|A|+1+8|B|)H_1^2H_2^2. \end{aligned}$$

De manera análoga

$$\begin{aligned} |g_2| &= |(a_1a_2-Ab_1b_2)^2-4B(a_1b_2+a_2b_1)b_1b_2| \\ &\leq (H_1H_2+|A|H_1H_2)^2+4|B|(H_1H_2+H_1H_2)H_1H_2 \\ &\leq ((1+|A|)^2+8|B|)H_1^2H_2^2. \end{aligned}$$

y $|g_3| \leq 4H_1^2H_2^2$

Por lo tanto $H(P+Q)H(P-Q) \leq CH_1^2H_2^2 = CH(P)^2H(Q)^2$, donde $C = 2m|A|x\{4((1+|A|^2)+8|B|), 4(|A|+1+|B|), 4\}$. Tomando logaritmo a cada miembro de la desigualdad

$$log(H(P+Q)H(P-Q)) \leq log(CH_1^2H_2^2) = log(CH(P)^2H(Q)^2),$$

tenemos

$$h(P+Q)+h(P-Q) \leq 2h(P)+2h(Q)+c''. \tag{3.10}$$

donde $c'' = logC$.

Lo cuál probaría la ecuación (3.5). Probaremos a continuación la ecuación (3.4), para tal efecto veamos un lema que nos será de utilidad en nuestra prueba. □

Lema 3.19. *Sea* $\Delta = 4A^3 + 27B^2$ *y sean los polinomios*

$$\begin{aligned} F(X,Z) &= X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4 \\ G(X,Z) &= 4Z(X^3 + AXZ^2 + BZ^3). \end{aligned}$$

Entonces existen $f_1, f_2, g_1, g_2 \in \mathbb{Z}[X,Z]$*, polinomios homogéneos de grado 3, tales que*

$$Ff_1 - Gg_1 = 4\Delta Z^7 \text{ y } Ff_2 + Gg_2 = 4\Delta X^7.$$

Demostración. Reemplazando $Z = 1$ en $F(X,Z)$ y $G(X,Z)$, tenemos

$$\begin{aligned} F(X,1) &= X^4 - 2AX^2 - 8BX + A^2 \\ G(X,1) &= 4(X^3 + AX + B). \end{aligned}$$

Dividiendo $F(X,1)$ entre $G(X,1)$, tenemos que

$$F(X,1) = G(X,1)(\frac{1}{4}X) + (-3AX^2 - 9BX + A^2)$$

Por consiguiente:

$$G(X,1) = \frac{4}{x}(F(x,1) + 3Ax^2 + 9Bx - A^2), \text{ con } A \neq 0$$

$$XG(X,1) = (-3AX^2 - 9BX + A^2)(-\frac{4}{3A}X + \frac{4B}{A^2}) + (\frac{4\Delta}{3A^2}X), \text{ con } A \neq 0.$$

De ahí que

$$(-3AX^2 - 9BX + A^2) = (\frac{4\Delta}{3A^2}X)(-\frac{9A^3}{4\Delta}X) + (-9BX + A^2)$$

$$(\frac{4\Delta}{3A^2}X) = (-9BX + A^2)(-\frac{4\Delta}{27BA^2}) + \frac{4\Delta}{27B}, \text{ con } A, B \neq 0$$

Por lo tanto

$$4\Delta = (12X^2 + 16A)F(X,1) + (-3X^3 + 5AX + 27B)G(X,1). \tag{3.11}$$

Reemplazando X por $\frac{X}{Z}$ en (3.8) tenemos

$$4\Delta = (12\frac{X^2}{Z^2} + 16A)F(\frac{X}{Z},1) + (-3\frac{X^3}{Z^3} + 5A\frac{X}{Z} + 27B)G(\frac{X}{Z},1). \tag{3.12}$$

Como $F(X,Z)$ y $G(X,Z)$ son polinomios homogéneos de grado 4, multiplicando a (3.9) por Z^7 tenemos

$$4\Delta Z^7 = (12X^2Z + 16AZ^3)F(X,Z) + (-3X^3 + 5AXZ^2 + 27BZ^3)G(X,Z).$$

Haciendo $f_1(X,Z) = 12X^2Z + 16AZ^3$ y $g_1(X,Z) = -3X^3 + 5AXZ^2 + 27BZ^3$ tenemos el resultado requerido. De igual manera se puede obtener

$$\begin{aligned} f_2 &= 4\Delta X^3 - 4A^2BX^2Z + 4A(3A^2 + 22B^2)XZ^2 + 12B(A^3 + 8B^2)Z^3 \\ g_2 &= A^2BX^3 + A(5A^3 + 32B^2)X^2Z + 2B(13A^3 + 96B^2)XZ^2 - 3A^2(A^2 + 8B^2)Z^3, \end{aligned}$$

tales que

$$Ff_2 + Gg_2 = 4\Delta X^7.$$

□

Lema 3.20. *Sea $R \in E(\mathbb{Q})$. Existe una constante C_2, independiente de R que cumple*

$$4h(R) \leq h(2R) + C_2.$$

Demostración. Sea

$$R = (\frac{a}{b}, y)$$

con $y \in \mathbb{Q}$ y $a, b \in \mathbb{Z}$, con $mcd(a,b) = 1$.
Definamos

$$\begin{aligned} h_1 &= a^4 - 2Aa^2b^2 - 8Bab^3 + A^2b^4 \\ h_2 &= (4b)(a^3 + Aab^2 + Bb^3) \\ \Delta &= 4A^3 + 27B^2. \end{aligned}$$

Por el lema anterior, van a existir polinomios homogéneos $r_1, r_2, s_1, s_2 \in \mathbb{Z}[a,b]$ de grado 3 tales que

$$4\Delta b^7 = r_1h_1 + r_2h_2 \tag{3.13}$$

$$4\Delta a^7 = s_1h_1 + s_2h_2 \tag{3.14}$$

Para un polinomio homogéneo de grado 3 de la forma

$$p(X,Y) = c_0X^3 + c_1X^2Y + c_2XY^2 + c_3Y^3$$

tenemos

$$|p(a,b)| \leq (|c_0| + |c_1| + |c_2| + |c_3|)\,\text{máx}(|a|,|b|)^3.$$

Supongamos que $|b| \geq |a|$, de ahí que

$$\begin{aligned} |4\Delta||b|^7 &\leq |r_1(a,b)||h_1| + |r_2(a,b)||h_2| \\ &\leq C_1|b|^3\,\text{máx}(|h_1|,|h_2|), \end{aligned}$$

para alguna constante C_1. Por lo tanto

$$|4\Delta||b|^4 \leq C_1\,\text{máx}(|h_1|,|h_2|).$$

Sea $d = mcd(h_1,h_2)$. Entonces por (3.12) y (3.13) tenemos que

$$d|4\Delta b^7 \ y \ d|4\Delta a^7.$$

Como $mcd(a,b) = 1$, tenemos que $d|4\Delta$, así $d \leq |4\Delta|$, por otro lado, como

$$H(2R) = H(x_1,y_1) = \tilde{H}(x_1) = \text{máx}(\frac{|h_1|}{d}, \frac{|h_2|}{d}),$$

tenemos que

$$\begin{aligned} |4\Delta|H(R)^4 &= |4\Delta||b|^4 \\ &\leq c_1\,\text{máx}(|h_1|,|h_2|) \\ &\leq c_1|4\Delta|\,\text{máx}(|h_1|/d,|h_2|/d) \\ &\leq c_1|4\Delta|H(2R). \end{aligned}$$

Dividiendo entre 4Δ y tomando logaritmo tenemos

$$4h(R) \leq h(2R) + C_2$$

donde $C_2 = log(C_1)$. □

Reemplazando P por $P+Q$ en (3.7) tenemos

$$h(2P) + h(2Q) \leq 2h(P+Q) + 2h(P-Q) + c''.$$

Por el lema anterior

$$4h(P) + 4h(Q) - 2c_2 \leq h(2P) + h(2Q).$$

Luego

$$2h(P) + 2h(Q) - c' \leq h(P+Q) + h(P-Q)$$

para alguna constante c'. Esto completaría la prueba del teorema 3.11. □

Teorema 3.21. *Sea E una curva elíptica definida sobre $\mathbb{Q}$. Existe una función*

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$$

con las siguientes propiedades:

1. $\hat{h}(P) \geq 0$ para todo $P \in E(\mathbb{Q})$
2. Existe una constante c_1 tal que $|\frac{1}{2}h(P) - \hat{h}(P)| \leq c_1$ para todo P.
3. Dada una constante c, existe solamente una cantidad finita de puntos $P \in E(\mathbb{Q})$, tales que $\hat{h}(P) \leq c$.
4. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$, para todo P, Q.
5. $\hat{h}(mP) = m^2\hat{h}(P)$, para todo $m \in \mathbb{Z}$ y todo $P \in E(\mathbb{Q})$.
6. $\hat{h}(P) = 0$ si y sólo sí P es un punto de torsión.

Demostración. (1) Haciendo $Q = P$ en el teorema anterior, obtenemos

$$|h(2P) - 4h(P)| \leq c_1, \textit{ para todo } P \in E(\mathbb{Q}). \tag{3.15}$$

Para cada $P \in E(\mathbb{Q})$, definamos

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P).$$

Veamos si esta bien definida, para ello probemos la existencia del límite. Tenemos

$$\lim_{n\to\infty} \frac{1}{4^n} h(2^n P) = h(P) + \sum_{j=1}^{\infty} \frac{1}{4^j}(h(2^j P) - 4h(2^{j-1}P)). \tag{3.16}$$

Por (3.15) tenemos

$$|\frac{1}{4^j}(h(2^j P) - 4h(2^{j-1}P))| \leq \frac{c_1}{4^j}$$

así la suma infinita converge. Por lo tanto $\hat{h}(P)$ esta bien definida, de ahí que

$$\hat{h}(P) \geq 0 \textit{ para todo } P \in E(\mathbb{Q}).$$

(2) De la parte (1) tenemos que

$$\sum_{j=1}^{\infty} \frac{c_1}{4^j} = \frac{c_1}{3}$$

De ahíÂ que $|\hat{h}(P) - \frac{1}{2}h(P)| \leq c_1/6$.

(3) Si $\hat{h}(P) \leq c$, entonces $h(P) \leq 2c + \frac{c_1}{3}$. Por lo tanto existe una cantidad finita de puntos P que satisfacen esta desigualdad.

(4) Esta propiedad es conocida como la **ley del paralelogramo** debido a que es originada por 0 y los vectores $P, Q, P+Q$ (adición ordinaria de dos vectores), estos puntos son los vértices de un paralelogramo. Sabemos que

$$\frac{1}{4^n}|h(2^nP + 2^nQ) - 2h(2^nP) - 2h(2^nQ)| \leq \frac{c_1}{4^n}.$$

haciendo que $n \to \infty$ tenemos el resultado esperado.

(5) Como la altura depende solamente de la primera coordenada, $\hat{h}(-P) = \hat{h}(P)$. Por lo tanto, asumamos que $m \geq 0$. Para $m = 0, 1$ la prueba es trivial. Si $Q = P$ por la parte (4) tenemos el caso en que $m = 2$. Supongamos que conocemos el resultado para $m-1$ y m. Entonces

$$\hat{h}((m+1)P) = -\hat{h}((m-1)P) + 2\hat{h}(mP) + 2\hat{h}(P) \text{ (por la parte (4))}$$

$$= (-(m+1)^2 + 2m^2 + 2)\hat{h}(P) = (m+1)^2\hat{h}(P).$$

Por inducción el resultado es verdadero para todo m.

(6) Si $mP = \mathcal{O}$, entonces $m^2\hat{h}(P) = \hat{h}(mP) = \hat{h}(\mathcal{O}) = 0$, así $\hat{h}(P) = 0$. Recíprocamente, si $\hat{h}(P) = 0$, entonces $\hat{h}(mP) = m^2\hat{h}(P) = 0$, para todo m. Sabemos que existe una cantidad finita grande de puntos de altura 0, el conjunto de múltiplos de P es finita. Por lo tanto P es un punto de torsión. Esto completa la prueba del teorema.

□

Teorema 3.22. *(Teorema de Mordell-Weil) Sea E una curva definida sobre $\mathbb{Q}$. Entonces $E(\mathbb{Q})$ es un grupo abeliano finitamente generado.*

Demostración. Sean los puntos $R_1, ..., R_n \in E(\mathbb{Q})$ representantes de las clases del grupo cociente finito $E(\mathbb{Q})/2E(\mathbb{Q})$. Definamos

$$c = \text{máx}\{\hat{h}(R_i)\} \quad \text{con } i = 1, ...n$$

y sean $\{Q_1, ..., Q_m\}$ el conjunto de puntos en $E(\mathbb{Q})$ tal que $\hat{h}(Q_i) \leq c$, el cual es finito por el teorema anterior. Definamos

$$G = \langle R_1, ..., R_n, Q_1, ...Q_m \rangle$$

el subgrupo de $E(\mathbb{Q})$ generado por $R_1, ..., R_n, Q_1, ...Q_m$.
Afirmamos que $G = E(\mathbb{Q})$. En efecto, supongamos que existe $P \in E(\mathbb{Q}) \setminus G$, entonces existe una cantidad finita de puntos de altura menor que la de P, podríamos cambiar P por uno de estos, si fuese necesario, y asumamos que P tiene la altura más pequeña entre todos los puntos que pertenecen a $E(\mathbb{Q})$, pero que no están en G. Por otro lado, como $\overline{P} \in E(\mathbb{Q})/2E(\mathbb{Q})$, entonces $\overline{P} = \overline{R_i}$, para algún $i = 1, 2, \ldots, n$. De ahí que

$$P - R_i = 2P_1$$

para algún $i = 1, 2, \ldots, n$ y algún $P_1 \in E(\mathbb{Q})$. Por el Teorema anterior:

$$\begin{aligned} 4\hat{h}(P_1) &= \hat{h}(2P_1) \\ &= \hat{h}(P - R_i) \\ &= 2\hat{h}(P) + 2\hat{h}(R_i) - \hat{h}(P + R_i) \\ &\leq 2\hat{h}(P) + 2c \end{aligned}$$

Como $c < \hat{h}(P)$, ya que $P \neq Q_j$ tenemos que

$$\begin{aligned} 4\hat{h}(P_1) &\leq 2\hat{h}(P) + 2c \\ &< 2\hat{h}(P) + 2\hat{h}(P) \\ &= 4\hat{h}(P). \end{aligned}$$

Por lo tanto

$$\hat{h}(P_1) < \hat{h}(P).$$

Como P tiene la altura más pequeña de puntos en $E(\mathbb{Q})$, pero que no están en G, tenemos que $P_1 \in G$. Por lo tanto

$$P = R_i + 2P_1 \in G.$$

Lo cual sería una contradicción, por lo tanto $E(\mathbb{Q}) = G$. Esto completaría la prueba del teorema de Mordell. $\square$

Capítulo 4

Curvas elípticas sobre $\mathbb{Q}(i)$

En el capítulo anterior hemos probado que $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito. Aunque esto parece ser una propiedad local según el cuerpo en el que trabajamos, resulta que esto sigue siendo cierto para cualquier extensión de $\mathbb{Q}$, incluyendo $\mathbb{Q}(i)$.
En esta sección mencionamos otra forma de demostrar el teorema de Mordell-Weil para que luego con esa idea pasemos a probar que $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es también finito. En vez de tratar con la teoría de grupo avanzada, se construye el resultado vía una extensión elemental de la prueba original. En este capítulo, solo se prueba este resultado para todas las curvas elípticas de la forma

$$y^2 = f(x) = x^3 + Ax + B, \quad A, B \in \mathbb{Z}(i)$$

asumiendo que $f(x) = (x-r_1)(x-r_2)(x-r_3)$, donde $r_j \in \mathbb{Z}(i)$ para todo $j = 1, 2, 3$.

Definición 4.1. *Los enteros gaussianos son de la forma*

$$\mathbb{Z}(i) = \{a + bi : \ a, b \in \mathbb{Z}\}$$

Definición 4.2. *Sean $z, w \in \mathbb{Z}(i)$ con $w \neq 0$. Decimos que z es divisible por w si existe $u \in \mathbb{Z}(i)$ tal que $z = wu$.*

Observaciones

1. Para cada $z = a + bi \in \mathbb{Z}(i)$ la norma se define como $N(z) = ||z||^2 = a^2 + b^2$.

2. Las unidades de $Z(i)$ son ± 1 y $\pm i$.

3. Un número $p \in \mathbb{Z}(i)$, decimos que es un primo gaussiano si y solo si p es divisible por $\pm 1, \pm i, \pm p$ y $\pm ip$.

4. Un número primo $p \in \mathbb{Z}$ es también un primo gaussiano si y solo si $p \equiv 3(mod\, 4)$.

5. Un número $p \in \mathbb{Z}(i)$ es un primo gaussiano si y solo si $N(p)$ es un primo en los enteros.

6. Si $x \in \mathbb{Q}(i)$ entonces $x = \frac{g}{h}$ con $g, h \in \mathbb{Z}(i)$ y además g y h son coprimos (no poseen factores comunes a excepción de $\pm 1, \pm i$).

Ejemplo: No todo número primo en los enteros resulta ser un primo en los enteros gaussianos, por ejemplo 5 es primo en los enteros pero no es un entero gaussiano ya que $5 = (1 + 2i)(1 - 2i)$

4.1. El teorema de Mordell-Weil

Teorema 4.3. *(Teorema de Mordell-Weil)*
Sea E una curva elíptica sobre $\mathbb{Q}$. El grupo $E(\mathbb{Q})$ es finitamente generado.

La prueba usa dos resultados:

1. $E(\mathbb{Q})/2E(\mathbb{Q}) = \{R_i + 2E(\mathbb{Q}) : R_i \in E(\mathbb{Q})\}$, es finitamente generado, donde R_i es el representante de cada clase de $E(\mathbb{Q})$ relativo a $2E(\mathbb{Q})$.

2. El descenso infinito.

Recordando la prueba vista en el capítulo 3, $E(\mathbb{Q})$ es la unión finita disjunta de estas clases. Así cualquier punto $P \in E(\mathbb{Q})$ debe estar en alguna clase, es decir $P = R_{n_1} + 2P_1$ para algún $n_1 \in \mathbb{Z}$, y $P_1 \in E(\mathbb{Q})$. Entonces, $P_1 \in E(\mathbb{Q})$ implica que $P = R_{n_2} + 2P_2$ para algún $n_2 \in \mathbb{Z}$, y $P_2 \in E(\mathbb{Q})$. Repitiendo el proceso, tenemos

$$\begin{aligned} P &= R_{n_1} + 2P_1 \\ &= R_{n_1} + 2R_{n_2} + 4P_2 \\ &= R_{n_1} + 2R_{n_3} + 8P_3 \\ &\vdots \\ &= \sum_{j=1}^{\ell} 2^{j-1} R_{n_j} + 2^{\ell} P_{\ell} \end{aligned}$$

después de ℓ iteraciones. Si podemos mostrar que el proceso termina, es decir, si existe un conjunto finito S tal que para cada $P \in E(\mathbb{Q}), P_\ell \in S$, para algún ℓ, luego el conjunto $\{R_{n_j} : 1 \leq j \leq \ell\} \bigcup S$ genera P. Esto se conoce como el *método del descenso*. El primer problema es la construcción de tal S, el cual se logra recurriendo a los siguientes conceptos:

4.1.1. La función altura

Definición 4.4. *(Función Altura)*
Dada una función $H : \mathbb{Q} \to \mathbb{Z}^+$, definimos

$$H(x) = \begin{cases} \text{máx}\{|a|, |b|\} & \textit{si } x \neq 0, x = a/b, \ \textit{mcd } (a, b) = 1 \\ 1 & \textit{si } x = 0 \end{cases}$$

Con la definición anterior, podemos extender H para medir la complejidad de un punto racional $P = (x, y) \in E(\mathbb{Q})$, por

$$H(P) = H(x, y) = \begin{cases} H(x) & \text{si } P \neq \mathcal{O} \\ 1 & \text{para cualquier otro caso.} \end{cases}$$

Lema 4.5. *Para cualquier constante $K > 0$, el conjunto $\{P \in E(\mathbb{Q}) : H(P) < K\}$ es finito.*

Lema 4.6. *Sea $R \in E(\mathbb{Q})$, un punto fijo. Entonces, existe una constante $c \geq 1$ que depende solo de R y E, tal que $H(P+R) \leq c(H(P))^2$ para todo $P \in E(\mathbb{Q})$, siempre que $P \neq \mathcal{O}; \pm R$.*

Lema 4.7. *Existe una constante $d \geq 1$ que depende solo de E , tal que $H(P)^4 \leq d(H(2P))$ para todo $P \in E(\mathbb{Q})$.*

Prueba del descenso infinito:
Mostremos como obtener el teorema de Mordell-Weil usando el método del descenso. El lema 4.5 siempre es verdad. Los lemas 4.6 y 4.7 se prueban mas adelante. Sean $R_1, R_2, \cdots, R_n$ los representantes de cada clase en $E(\mathbb{Q})/2E(\mathbb{Q})$. Sea c_j la constante en el lema 4.6, que depende solamente de $-R_j$ y E. Sea d la constante dada en el lema 4.7 (que depende solamente de E). Ahora sea

$$\rho = d \cdot \max_{1 \leq j \leq n}(c_j),$$

y definamos

$$S = \{P \in E(\mathbb{Q}) : \, H(P) \leq \rho^2\}.$$

Luego S es finito por el lema 4.5. Mostremos que S es el conjunto deseado, es decir $P_\ell \in S$, con P_ℓ ya definido anteriormente. Supongamos lo contrario, es decir, existe $P \in E(\mathbb{Q})$ tal que $P_j \notin S$ para todo $j \geq 1$. Notemos que $P_{j-1} = R_j + 2P_j$ para $j \geq 1$ y $P = P_0$.
Luego tenemos

$$\begin{aligned}(H(P_j))^4 &\leq dH(2P_j)) \\ &= dH(P_{j-1} - R_{n_j}) \\ &\leq dc_{n_j} H(P_{j-1})^2 \\ &\leq \rho((H(P_{j-1}))^2,\end{aligned}$$

y así $H(P_j) \leq \rho^{1/4}\sqrt{H(P_{j-1})} \leq \rho\sqrt{H(P_{j-1})}$. Pero $P_{j-1} \notin S$, es decir $H(P_{j-1}) > \rho^2$. Por tanto tenemos

$$H(P_j) \leq \rho\sqrt{H(P_{j-1})} < H(P_{j-1}),$$

en otras palabras, $H(P_j) \leq H(P_{j-1}) - 1$ puesto que H es un entero positivo. Se sigue que

$$H(P_\ell) \leq H(P_{\ell-1}) - 1 \leq H(P_{\ell-2}) - 2 \leq \cdots \leq H(P_1) - (\ell - 1) \leq H(P) - \ell.$$

Escogemos $\ell > H(P)$ que hará $H(P_\ell)$ negativo, lo que contradice la positividad de H. Así queda completa la prueba del descenso infinito.

Definición 4.8. *(Modificación de la función altura)*
Sea E una curva elíptica sobre $\mathbb{Q}(i)$. Asumamos que E posee la forma $y^2 = x^3 + Ax + B$, donde $A, B \in \mathbb{Z}(i)$, Definimos la función altura extendida $H' : \mathbb{Q}(i) \to \mathbb{Z}^+$ por

$$H'(z) = \begin{cases} \max\{|z_1|^2, |z_2|^2\} & si\ z \neq 0, z = z_1/z_2 \\ 1 & si\ z = 0 \end{cases}$$

Siendo $z = z_1/z_2$ un cociente de enteros gaussianos primos entre sí.

Con lo anterior podemos definir la función altura extendida para un punto $P = (x, y) \in E(\mathbb{Q}(i))$ de manera similar por

$$H'(P) = \begin{cases} H(z) & \text{si } P \neq \mathcal{O} \\ 1 & \text{para cualquier otro caso.} \end{cases}$$

Mostremos que la definición de H' satisface los lemas anteriores al reemplazar H por H'.

Lema 4.9. *Para cualquier constante $K > 0$, el conjunto $\{P \in E(\mathbb{Q}(i)) : H'(P) < K\}$ es finito.*

Demostración. Sea $P = (x, y) \in E(\mathbb{Q}(i))$. Por definición de H', tenemos $H'(P) = H'(x)$. Puesto que cada $x \in \mathbb{Q}(i)$ da a lo mas dos valores de y, queda probar que el número de tales $x \in \mathbb{Q}(i)$, con $H'(x) < K$, es finito. Recordando la definición de H', el problema es equivalente a contar el número de puntos enteros en un hipercubo 4-dimensional de lado $\sqrt{K}$, el cual es finito. Esto completa la prueba. □

Lema 4.10. *Para $P = (x, y) \in E(\mathbb{Q}(i))$, existen $x_1, y_1, z \in \mathbb{Z}(i)$, donde x_1, y_1 son primos relativos a $\mathbb{Z}$ como enteros gaussianos, tal que*

$$x = \frac{x_1}{z^2}, \quad y = \frac{y_1}{z^3}$$

Demostración. Escribimos $x = x_1/z_1$ y $y = y_1/z_2$ como cociente de enteros gaussianos, es decir, $\text{mcd}(x_1, z_1)$ y $\text{mcd}(y_1, z_2)$ es la unidad. Sustituyendo x, y en la ecuación de la curva E, tenemos:

$$\left(\frac{y_1}{z_2}\right)^2 = \left(\frac{x_1}{z_1}\right)^3 + \frac{Ax_1}{z_1} + B,$$

es decir

$$y_1^2 z_1^3 = x_1^3 z_2^2 + Ax_1 z_1^2 z_2^2 + Bz_1^3 z_2^2$$

Así tenemos $z_2^2 \mid z_1^3$ y $z_1^2 \mid z_2^2$. El último resultado implica que $z_1^3 \mid x_1^3 z_2^2$ y $z_1^3 \mid z_2^2$, y con ello tenemos que $z_1^3 = z_2^2$. Sea $z = z_2/z_1 \in \mathbb{Z}(i)$, entonces

$$z^2 = \frac{z_2^2}{z_1^2} = z_1, \quad z^3 = \frac{z_2^3}{z_1^3} = z_2,$$

y esto prueba el lema. □

Lema 4.11. *Existe una constante $K \geq 1$, que depende solo de E, tal que*

$$|y| \leq K(H'(P))^{3/4}$$

para cada punto $P = (x, y) \in E(\mathbb{Q}(i))$.

Demostración. Escribamos $P = (x_1/z^2, y_1/z^3)$ como en el lema 4.10. Sustituyendo en la ecuación de E, y multiplicando ambos lados por z^6, tenemos

$$y_1^2 = x_1^3 + Ax_1 z^4 + Bz^6.$$

Notar que $H'(P) = H'(x) = \text{máx}\{|x_1|^2, |z^2|^2\}$. Por la desigualdad triangular, tenemos

$$\begin{aligned} |y_1|^2 &\leq |x_1|^{2.3/2} + |A||x_1|^{2.1/2}|z^2|^2 + |B||z|^{2.3/2} \\ &\leq (H'(P))^{3/2}(1 + |A| + |B|) \end{aligned}$$

es decir

$$|y| \leq \frac{(H'(P))^{3/4}\sqrt{1 + |A| + |B|}}{z^3} \leq (H'(P))^{3/4}\sqrt{1 + |A| + |B|} = K(H'(P))^{3/4}$$

puesto que $z \neq 0 \in \mathbb{Z}(i)$ y así $|z| \geq 1$ □

Supongamos que tenemos dos puntos $P = (x_1, y_1), R = (x_2, y_2) \in E(\mathbb{Q}(i))$, tal que ninguno es $\mathcal{O}$, y $P \neq \pm R$. Denotemos por $x(P + R)$ a la primera componente de $P + R$. De la fórmula de adición, tenemos:

$$x(P + R) = (\frac{y_2 - y_1}{x_2 - x_1})^2 - (x_1 + x_2).$$

Usando el hecho que ${y_1}^2 = {x_1}^3 + Ax_1 + B$ y ${y_2}^2 = {x_2}^3 + Ax_2 + B$, podemos reescribir esto como

$$x(P + R) = \frac{(A + x_1x_2)(x_1 + x_2) + 2B - 2y_1y_2}{(x_2 - x_1)^2} \tag{4.1}$$

Lema 4.12. *Sea $R = (x_0, y_0) \in E(\mathbb{Q}(i))$ un punto fijo. Existe una constante $c \geq 1$, que depende solo de R y E, tal que*

$$H'(P + R) \leq c(H'(P))^2$$

para cada $P \in E(\mathbb{Q}(i))$, donde $P \neq \mathcal{O}, \pm R$

Demostración. El resultado es trivial si $R = \mathcal{O}$. Sea $P = (x, y) = (x_1/z^2, y_1/z^3)$, con $x_1, y_1, z_1 \in \mathbb{Z}(i)$ como ya se vió antes. Luego de (4.1), tenemos

$$\begin{aligned} x(P + R) &= \frac{\left(A + \frac{x_0x_1}{z^2}\right)\left(x_0 + \frac{x_1}{z^2}\right) + 2B - \frac{2y_0y_1}{z^3}}{\left(x_0 - \frac{x_1}{z^2}\right)^2} \\ &= \frac{\alpha_1 z^4 + \alpha_2 x_1 z^2 + \alpha_3 {x_1}^2 + \alpha_4 y_1 z}{\alpha_5 z^4 + \alpha_6 x_1 z^2 + {x_1}^2} \end{aligned}$$

después de multiplicar el numerador y denominador por z^4. Aquí $\alpha_1, \alpha_2, \cdots, \alpha_6$ son algunas de las constantes que dependen de R (en términos de x_0, y_0) y E (en términos de A, B). Notemos que

$$|x_1| \leq \sqrt{H'(P)}, \quad |z^2|^2 \leq H'(P), \quad |y_1| \leq K(H'(P))^{3/4}$$

por la definición de $H'(P)$ y el lema 4.11. Luego tenemos que

$$|\alpha_1 z^4 + \alpha_2 x_1 z^2 + \alpha_3 {x_1}^2 + \alpha_4 y_1 z| \leq (|\alpha_1| + |\alpha_2| + |\alpha_3| + K|\alpha_4|)\, H'(P),$$

y

$$|\alpha_5 z^4 + \alpha_6 x_1 z^2 + x_1^2| \leq (|\alpha_5| + |\alpha_6| + 1)\, H'(P).$$

Por lo tanto, podemos concluír que

$$H'(P+R) = H'(x(P+R)) \leq c(H'(P))^2$$

donde $c = \text{máx}\{(|\alpha_1| + |\alpha_2| + |\alpha_3| + K|\alpha_4|)^2, (|\alpha_5| + |\alpha_6| + 1)^2\}$. Claramente $c \geq 1$ y depende solo de R y E. □

4.1.2. Fórmula de duplicación gaussiana

Sea $y^2 = f(x) = x^3 + Ax + B \quad con \quad A, B \in \mathbb{Z}(i)$ una curva elíptica sobre $\mathbb{Q}(i)$. Sean r_1, r_2, r_3 raíces de $f(x)$, asumiendo que $r_j \in \mathbb{Z}(i)$, para todo $j = 1, 2, 3$. Escribiremos r para cada una de estas raíces.
Sea $P = (x_1, y_1) \in E(\mathbb{Q}(i))$, tal que $P \neq (\mathcal{O}), (r, 0)$. Puesto que la línea tangente a la curva en P intercepta a la curva en el punto $-2P$, entonces estos puntos satisfacen

$$[m(x - x_1) + y_1]^2 = x^3 + Ax + B, \quad \text{donde} \quad m = \frac{3x_1^2 + A}{2y_1} \tag{4.2}$$

son P y $\pm 2P$. Para una raíz fija $r = r_j$, escribimos

$$X_1 = x_1 - r \quad y \quad X = x - r$$

Por (4.2) tenemos

$$[m(X - X_1) + y_1]^2 = [m(x - x_1) + y_1]^2 = x^3 + Ax + B = f(X + r)$$

Pero podemos reescribir esto como

$$\begin{aligned} f(X+r) &= x^3 + Ax + B \\ &= (x-r)^3 + 3x^2 r + x(A - 3r^2) + r^3 + B \\ &= (x-r)^3 + 3r(x-r)^2 + x(A + 3r^2) - 2r^3 + B \\ &= (x-r)^3 + 3r(x-r)^2 + (A + 3r^2)(x-r) + (r^3 + Ar + B) \\ &= X^3 + 3rX^2 + (A + 3r^2)X \quad (\text{pues} \quad f(r) = 0). \end{aligned}$$

Esto implica que $X = 0$ es una raíz de $f(X + r)$.
Puesto que x_1 y $x(2P)$ satisfacen (4.2), $x_1 - r$ y $x(2P) - r$ son raíces de $f(X + r)$. El producto (con multiplicidad 2, debido a $x_1 - r$) de estas raíces debe ser el término constante de la ecuación anterior, es decir

$$\begin{aligned}(x(2P) - r)(x_1 - r)^2 &= (y_1 - mX_1)^2 \\ &= \left[y_1 - \tfrac{(3x_1^2+A)(x_1-r)}{2y_1}\right]^2 \\ &= \left[\tfrac{2y_1^2-(x_1-r)(3x_1^2+A)}{2y_1}\right]^2\end{aligned} \tag{4.3}$$

Así el numerador de (4.3) se convierte

$$2y_1^2 - (x_1 - r)(3x_1^2 + A) = (x_1 - r)(-x_1^2 + 2rx_1 + A + 2r^2)$$

Después de simplificar la expresión, tenemos

$$x(2P) - r = \left[\frac{-x_1^2 + 2rx_1 + A + 2r^2}{2y_1}\right]^2 \tag{4.4}$$

para cada $r = r_1, r_2, r_3$.

Lema 4.13. *Existe una constante $d \geq 1$, que depende solo de E, tal que*

$$(H'(P))^4 \leq dH'(2P)$$

para todo $P \in E(\mathbb{Q}(i))$.

Demostración. La prueba es trivial cuando $P = \mathcal{O}$. Si $P = (r_j, 0)$ donde r_j es la j-ésima raíz de $x^3 + Ax + B$, entonces $P = \mathcal{O}$ y así $H'(2P) = 1$. En este caso, podemos incrementar d si fuese necesario para hacer que la desigualdad se mantenga. Por tanto, asumamos que P no es ninguno de estos puntos. Escribamos P como $(x_1/z_1^2, y_1/z_1^3)$, y $2P$ como $(x_2/z_2^2, y_2/z_2^3)$ en (4.4). Luego de simplificar obtenemos

$$x_2 - r_j z_2^2 = \left[\frac{-x_1^2 + 2r_j x_1 z_1^2 + (A + 2r_j^2)z_1^4}{2y_1 z_1}\right]^2$$

y hacemos

$$\alpha_j = \left(\frac{z_2}{2y_1z_1}\right)\left[-x_1^2 + 2r_jx_1z_1^2 + (A+2r_j^2)z_1^4\right]. \tag{4.5}$$

Claramente $\alpha_j \in \mathbb{Q}(i)$. También $\alpha_j^2 = x_2 - r_jz_2^2 \in \mathbb{Z}(i)$, puesto que $r_j \in \mathbb{Z}(i)$ por lo que se asumió. Así $\alpha_j \in \mathbb{Z}(i)$. Ahora tenemos

$$\begin{aligned}
|\alpha_j|^2 = |x_2 - r_jz_2^2| &\leq |x_2| + |r_j||z_2^2| \\
&\leq |r_j|\left(|x_2| + |z_2^2|\right) \quad (\text{como } r_j \in \mathbb{Z}(i), \text{ entonces } |r_j| \geq 1) \\
&\leq 2|r_j|\left(\text{máx}\{|x_2|^2, |z_2|^2\}\right)^{1/2} \\
&= 2|r_j|\sqrt{H'(2P)}
\end{aligned}$$

Por tanto $|\alpha_j| \leq c\left(H'(2P)\right)^{1/4}$, donde $c = \sqrt{\text{máx}\{2|r_1|, 2|r_2|, 2|r_3|\}} \geq 1$ depende solamente de E.

Ahora deseamos estimar $H'(P)$. De (4.5), podemos reordenar términos para obtener:

$$\alpha_j = \mu_1 + \mu_2r_j + \mu_3r_j^2$$

siendo

$$\mu_1 = \frac{z_2(-x_1^2 + Az_1^4)}{2y_1z_1}, \quad \mu_2 = \frac{x_1z_1z_2}{y_1}, \quad \mu_3 = \frac{z_2z_1^4}{y_1z_1}.$$

Podemos escribir el sistema de ecuaciones($j = 1, 2, 3$) en forma matricial como

$$\begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_1 & r_1^2 \\ 1 & r_1 & r_1^2 \end{pmatrix}\begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \Longrightarrow \mathcal{R}\mu = \alpha$$

donde $\mathcal{R}$ es la matriz de Vandermonde, siendo su determinante

$$\det\mathcal{R} = \prod_{i>j}(r_i - r_j).$$

Claramente $\det\mathcal{R} \in \mathbb{Z}(i)$ y nunca es cero, pues todas las raíces son diferentes. Luego μ se encuentra únicamente determinada por la regla de Cramer. Para ser precisos para $j = 1, 2, 3$.

$$\mu_j = \frac{D_j}{D} = \frac{\det\mathcal{R}_j}{\det\mathcal{R}},$$

donde $\mathcal{R}_j$ es obtenido al reemplazar la j-ésima columna de $\mathcal{R}$ con α. En otras palabras, $D\mu_j$ es una combinación lineal de $\alpha_1, \alpha_2, \alpha_3$ con coeficientes enteros gaussianos. Así $D\mu_j \in \mathbb{Z}(i)$ para todo $j = 1, 2, 3$. Un cálculo directo nos lleva a

$$D(A\mu_3 - 2\mu_1) = D\left[\frac{Az_2z_1^4 - z_2(-x_1^2 + Az_1^4)}{y_1z_1}\right] = \left(\frac{Dz_2}{y_1z_1}\right)x_1^2$$

y también

$$D(\mu_3) = \left(\frac{Dz_2}{y_1z_1}\right)z_1^4$$

Puesto que x_1 y z_1 no tienen factor común no unitario, esto implica que $z_1|z_2$. Similarmente, puesto que y_1 y z_1 no tienen factor común no unitario, entonces $y_1|Dz_2$ también.
Por tanto, concluímos que $y_1z_1|Dz_2$, es decir

$$\frac{Dz_2}{y_1z_1} \in \mathbb{Q}(i)$$

lo cual implica que

$$x_1^2|D(A\mu_3 - 2\mu_1) \quad \text{y} \quad z_1^4|DA\mu_3,$$

entonces

$$|x_1|^2 \leq |D(A\mu_3 - 2\mu_1)| \quad \text{y} \quad |z_2^2|^2 \geq |DA\mu_3|.$$

Así mostramos que $D\mu_j$ es una combinación lineal de α_j con coeficientes enteros gaussianos, y también

$$|\alpha_j| \leq c(H'(2P))^{1/4}$$

para $j = 1, 2, 3$. Por lo tanto.

$$|x_1|^2 \leq c_1(H'(2P))^{1/4}, \quad |z_2^2|^2 \leq c_2(H'(2P))^{1/4}$$

para algunas constantes apropiadas $c_1, c_2 \geq 1$ (las cuales aún dependen solo de E). Por tanto

$$H'(P) = \text{máx}\{|x_1|^2, |z_2^2|^2\} \leq d(H'(2P))^{1/4}, \quad \text{donde} \quad d = \text{máx}\{c_1, c_2\}$$

Elevando ambos lados a la cuarta potencia, se obtiene lo requerido. □

Se vé inmediatamente que el método del descenso infinito es aún válido si reemplazamos la función altura con la función altura extendida. Probemos que el análogo del teorema débil de Mordel-Weil es válido.

4.2. El teorema débil de Mordell-Weil

Definición 4.14. *Sea $\mathbb{Q}^*(i)$ un grupo multiplicativo y su subgrupo $(\mathbb{Q}^*(i))^2$. Definamos el grupo cociente*

$$\frac{\mathbb{Q}^*(i)}{(\mathbb{Q}^*(i))^2} = \{\overline{z} : z \in \mathbb{Q}^*(i)\} \text{ con } \overline{z} = \{zu^2 \in \mathbb{Q}^*(i) : u \in \mathbb{Q}^*(i)\}$$

Teorema 4.15. *(Teorema débil de Mordell-Weil)*
El grupo cociente $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es finito.

Para la prueba, imitemos el caso Q, es decir:

1. Construir un homomorfismo

$$\begin{array}{rcl} \phi : E(\mathbb{Q}(i)) & \to & \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \\ P & \longmapsto & (\phi_1(P), \phi_2(P), \phi_3(P)) \end{array}$$

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

3. Probar que la imagen de ϕ es finita

Empecemos definiendo ϕ.
Para cada j, definamos la aplicación $\phi_j : E(\mathbb{Q}(i)) \to \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2$ por

$$\phi_j(P) = \phi_j((x, y)) = [\rho_j(x)](\mathbb{Q}^*(i))^2$$

donde

$$\rho_j(x) = \begin{cases} 1 & \text{si } P = \mathcal{O} \\ (x - r_i)(x - r_k), \quad (i \neq j \neq k) & \text{si } P = (r_j, 0) \\ x - r_j & \text{para cualquier otro caso.} \end{cases}$$

y

$$\phi(P) = (\phi_1(P), \phi_2(P), \phi_3(P)).$$

Lema 4.16. *ϕ es un homomorfismo.*

Demostración. Es suficiente mostrar que para cada j,

$$\phi_j(P + Q) = \phi_j(P)\phi_j(Q) \tag{4.6}$$

para cualquier P, $Q \in E(\mathbb{Q}(i))$. La prueba es trivial si uno de estos punto es $\mathcal{O}$. Asumamos que ningún punto es $\mathcal{O}$.
Es fácil ver que $\phi(P) = \phi(-P)$ para cualquier $P \in E(\mathbb{Q}(i))$ (ya que ϕ es independiente de la coordenada y). También

$$(\phi_j(P))^2 = (x(P) - r_j)^2(\mathbb{Q}^*(i))^2 \in (\mathbb{Q}^*(i))^2$$

Por lo tanto probar (4.6) es equivalente a probar que

$$\phi_j(P + Q)\phi_j(P)\phi_j(Q) = (\mathbb{Q}^*(i))^2. \tag{4.7}$$

Sea $y = mx + b$ la linea que intersecta P, Q, y $-(P + Q)$. Entonces $x(P)$, $x(Q)$, y $x(P + Q)$ deben satisfacer

$$y^2 = (mx + b)^2 = (x - r_1)(x - r_2)(x - r_3).$$

Por lo tanto $(x - r_1)(x - r_2)(x - r_3) - (mx + b)^2 = 0$ cuando $x = x(P)$, $x(Q)$, $x(P + Q)$ y así

$$\prod_{j=1}^{3}(x - r_j) - (mx + b)^2 = (x - x(P))(x - x(Q))(x - x(P + Q)). \tag{4.8}$$

Consideremos los siguientes casos:

- Ningún punto es $(r_j, 0)$ donde $j = 1, 2$ o 3. Si hacemos $x = r_j$ (para $j = 1, 2, 3$) en (4.8), obtenemos

$$(mr_j + b)^2 = (x(P) - r_j)(x(Q) - r_j)(x(P + Q) - r_j)$$

lo cual implica (4.7).

- Exactamente un punto es de la forma $(r_j, 0)$, es decir, $P = (r_1, 0)$. De (4.8) tenemos

$$(x-r_1)(x-r_2)(x-r_3)-(mx+b)^2 = (x-r_1)(x-x(Q))(x-x(P+Q)). \quad (4.9)$$

Si hacemos $x = r_2, r_3$, esto implica (4.7) para cuando $j = 2, 3$. Para $j = 1$, notemos que la línea $y = mx + b$ intercepta al punto $P = (r_1, 0)$, así tenemos $0 = mr_1 + b$, es decir, $b = -mr_1$, de modo que

$$y = mx + b = m(x - r_1) \quad (4.10)$$

Tomemos el límite cuando $x \to r_1$ en (4.9). Al sustituir (4.10) en (4.9), obtenemos

$$(x - r_1)(x - r_2)(x - r_3) - m^2(x - r_1)^2 = (x - r_1)(x - x(Q))(x - x(P + Q)).$$

Cancelando $(x - r_1)$ de ambos lados tenemos

$$(x - r_2)(x - r_3) - m^2(x - r_1) = (x - x(Q))(x - x(P + Q)).$$

Sea $x = r_1$, obtenemos

$$(r_1 - r_2)(r_1 - r_3) = (x(Q) - r_1)(x(P + Q) - r_1),$$

lo cual implica que $\phi_1(P) = \phi_1(x(Q))\phi_1(x(P + Q))$, luego (4.7) es cierto para $j = 1$.

- Si ambos puntos son de la forma $(r_j, 0)$, podemos decir que $P = (r_1, 0)$ y $Q = (r_2, 0)$. Es facil ver (de la construcción geométrica de la adición) que $P + Q = (r_3, 0)$. Por lo tanto para cualquier $j = 1, 2, 3$, tenemos

$$\phi_j(P + Q)\phi_j(P)\phi_j(Q) = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2(\mathbb{Q}^*(i))^2 = (\mathbb{Q}^*(i))^2.$$

Esto completa la prueba. □

Lema 4.17. *Sea $P \in E(\mathbb{Q}(i))$, con $P \notin \{\mathcal{O}, (r_1, 0), (r_2, 0), (r_3, 0)\}$. Si $P \in \ker \phi$, entonces $P = 2Q$ para algún $Q \in E(\mathbb{Q}(i))$.*

Demostración. Supongamos que $P = (x, y) \in \ker \phi$. Si existe tal punto $Q = (x_1, y_1)$, entonces x_1 debe satisfacer la fórmula de duplicación:

$$x - r_j = x(P) - r_j = x(2Q) - r_j = \left[\frac{-x_1^2 + 2r_j x_1 + A + 2r_j^2}{2y_1}\right]^2 \tag{4.11}$$

□

para todo $j = 1, 2, 3$. Puesto que $P \in \ker \phi$, la definición de ϕ implica que $\phi_j(P) = (x - r_j)(\mathbb{Q}^*(i))^2 = (\mathbb{Q}^*(i)^2)$, es decir $x - r_j$ es el cuadrado de un número en $\mathbb{Q}(i)$, y escojamos $\lambda_j = \sqrt{x - r_j} \in \mathbb{Q}(i)$.
Luego de ordenar los términos con respecto a las potencias de r_j en (4.11) obtenemos

$$\lambda_j = \mu_1 + \mu_2 r_j + \mu_3 r_j^2, \tag{4.12}$$

donde

$$\mu_1 = \frac{-x_1^2 + A}{2y_1}, \quad \mu_2 = \frac{x_1}{y_1}, \quad \mu_3 = \frac{1}{y_1} \tag{4.13}$$

Se puede ver que el sistema de ecuaciones correspondiente es

$$\begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_1 & r_1^2 \\ 1 & r_1 & r_1^2 \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} \Longrightarrow \mathcal{R}\mu = \lambda$$

donde $\mathcal{R}$ es la matriz de Vandermonde. Puesto que $\det \mathcal{R} \neq 0$, $\mu \in (\mathbb{Q}(i))^3$ y es único por la regla de Cramer. Por (4.13), $Q = (x_1, y_1) \in (\mathbb{Q}(i))^2$. Ahora queda por ver que $Q \in E(\mathbb{Q}(i))$.
Notemos que $\lambda_j^2 = x - r_j$. Entonces de (4.12), obtenemos

$$(\mu_1^2 - 2B\mu_2\mu_3 - x)v_0 + (1 + 2\mu_1\mu_2 - 2A\mu_2\mu_3 - B\mu_3^2)v_1 + (\mu_2^2 + 2\mu_1\mu_3 - A\mu_3^2)v_2 = 0$$

(usando el hecho que $r_j^3 = -Ar_j - B$ para los términos r_j^3, r_j^4), donde v_j es la $j-$ésima columna de $\mathcal{R}$. Puesto que $\det \mathcal{R} \neq 0$, todas las columnas de $\mathcal{R}$ son linealmente independientes y por lo tanto cada escalar es cero. En particular,

$$2\mu_1\mu_2 - 2A\mu_2\mu_3 - B\mu_3^2 = -1 \tag{4.14}$$

$$\mu_2^2 + 2\mu_1\mu_3 - A\mu_3^2 = 0 \tag{4.15}$$

Puesto que $\mu_3 = 1/y_1 \neq 0$, podemos resolver para μ_1 en (4.15). Sustituyendo μ_1 en (4.14) tenemos

$$\mu_2^3 + A\mu_2\mu_3^2 + B\mu_3^2 = \mu_3$$

Dividiendo ambos lados por μ_3^3 tenemos

$$\left(\frac{\mu_2}{\mu_3}\right)^3 + A\left(\frac{\mu_2}{\mu_3}\right) + B = \left(\frac{1}{\mu_3}\right)^2,$$

es decir $x_1^3 + Ax_1 + B = y_1^2$ por (4.13). Por lo tanto $Q \in E(\mathbb{Q}(i))$, con lo cual concluye la prueba.

Lema 4.18. *Sea $E : y^2 = f(x) = x^3 + Ax + B$ una curva elíptica sobre $\mathbb{Q}(i)$, con $A, B \in \mathbb{Z}(i)$ y $r_1, r_2, r_3 \in \mathbb{Z}(i)$ los ceros de $f(x)$. Entonces*

$$(r_j - r_l)(r_j - r_k) = 3r_j^2 + A$$

donde $j, k, l \in \{1, 2, 3\}$ y $k \neq j \neq l$.

Demostración. Usando la suma y productos de las raíces, vemos que

$$r_1 + r_2 + r_3 = 0 \quad \text{y} \quad r_1r_2 + r_2r_3 + r_1r_3 = A.$$

Así,

$$\begin{aligned}(r_j - r_l)(r_j - r_k) &= r_j^2 - r_jr_k - r_jr_l + r_lr_k \\ &= r_j^2 + (r_jr_k + r_jr_l + r_lr_k) - 2r_j(r_k + r_l) \\ &= 3r_j^2 + A - 2r_j(r_j + r_k + r_l) \\ &= 3r_j^2 + A - 2r_j(0) = 3r_j^2 + A.\end{aligned}$$

□

Lema 4.19. *Sea $P \in E(\mathbb{Q}(i))$ con $P \in \{\mathcal{O}\} \cup \{(r_j, 0) : j = 1, 2, 3\}$. Si $P \in \ker \phi$, entonces $P = 2Q$ para algún $Q \in E(\mathbb{Q}(i))$.*

Demostración. El caso cuando $P = \mathcal{O}$ es trivial, ya que claramente $P \in ker\ \phi$ y $P = 2Q$, cuando $Q = \mathcal{O}$, $(r_j, 0) \in E(\mathbb{Q}(i))$ para $j = 1, 2, 3$ por suposición. Así podemos asumir que $Q \neq \mathcal{O}$ y $(Q) \neq 0$.
Supongamos que $P = (r_j, 0)$ y $P \in \ker \phi$. Por simplicidad, tomemos $P = (r_1, 0)$ (los casos cuando $j = 2, 3$ son tratados similarmente). Por la definición de ϕ,

$$\begin{aligned} \phi_1(P) &= (r_1 - r_2)(r_2 - r_3)(\mathbb{Q}^*(i))^2, \\ \phi_2(P) &= (r_1 - r_2)(\mathbb{Q}^*(i))^2, \\ \phi_3(P) &= (r_1 - r_3)(\mathbb{Q}^*(i))^2. \end{aligned}$$

Ya que $P \in \ker \phi$, entonces cada componente es el cuadrado de un número en $\mathbb{Q}(i)$. Es decir,

$$r_1 - r_2 = s^2, \text{ y }, r_1 - r_3 = t^2, \tag{4.16}$$

para algún $s, t \in \mathbb{Q}(i)$. Si hay tal punto $Q = (x_1, y_1)$ tal que $P = 2Q$, la línea tangente a la curva en el punto Q es

$$y - y_1 = m(x - x_1), \quad \text{donde } m = \frac{3x_1^2 + A}{2y_1}$$

que puede ser reordenado

$$2y_1 y = 3(x_1^2 + A)x + (2B - x_1^3 + Ax_1). \tag{4.17}$$

Si $P = 2Q$, entonces $-P = P$ esta sobre esta línea. Sustituyendo $P = (r_1, 0)$ en (4.17) resulta

$$x_1^3 - 2r_1x_1^2 - Ax_1 - (Ar_1 + 2B) = 0$$

Claramente $x_1 - r_1$ es un factor de este polinomio. Dividiendo por $x_1 - r_1$ tenemos

$$x_1^2 - 2r_1x_1 - (A + r_1^2) = 0$$

y por lo tanto

$$\begin{aligned} x_1 = \tfrac{2r_1 \pm \sqrt{4r_1^2 + 4(A + 2r_1^2)}}{2} &= r_1 \pm \sqrt{3r_1^2 + A} \\ &= r_1 \pm \sqrt{(r_1 - r_2)(r_1 - r_3)} \\ &= r_1 \pm st \in \mathbb{Q}(i), \end{aligned}$$

por el lema 4.18 y (4.16). Después de sustituir $(x, y) = Q = (x_1, y_1)$ en (4.17), tenemos que

$$y_1^2 = x_1^2 + Ax_1 + B,$$

es decir $Q = (x_1, y_1)$ está en E, y por lo tanto $y_1^2 = (x_1 - r_1)(x_1 - r_2)(x_1 - r_3)$. Un calculo directo muestra que

$$y_1^2 = \begin{cases} s^2t^2(s+t)^2, & \text{si } x_1 = r_1 + st \\ s^2t^2(s-t)^2, & \text{si } x_1 = r_1 - st \end{cases}$$

Ya que $s, t \in \mathbb{Q}(i)$, entonces tenemos $y_1 \in \mathbb{Q}(i)$. Por lo tanto $P = 2Q$ para algún $Q \in E(\mathbb{Q}(i))$. Esto completa la prueba. □

Proposición 4.20. ker $\phi = 2E(\mathbb{Q}(i))$.

Demostración. Afirmamos que $2E(\mathbb{Q}(i)) \subseteq \ker \phi$. En efecto, sea $P \in E(\mathbb{Q}(i))$. Entonces $P = 2Q$ para algún $Q \in E(Q(i))$

$$\phi_j(2Q) = \phi_j(Q)\phi_j(Q) = (\phi_j(Q))^2 \in (\mathbb{Q}^*(i))^2$$

para todo $j = 1, 2, 3, ...$ □

El último paso es asegurar que la imagen de ϕ es finita. Antes de probar esto, notemos que se puede escribir

$$x - r_1 = au^2, \quad x - r_2 = bv^2, \quad x - r_3 = cw^2$$

para algún $u, v, w \in \mathbb{Q}(i)$ con a, b, c enteros gaussianos libres de cuadrados, esto es, enteros gausianos que no tiene factor cuadrático.

Definición 4.21. *Se define la valuación p-ádica de un número racional como:*

a) $v_p(x) = \text{máx}\{n \in \mathbb{Z} : p^n | x, \text{ si } x \in \mathbb{Z} \setminus \{0\}\}$

b) $v_p(q) = v_p(a) - v_p(b), \text{si } q = a/b \in \mathbb{Q}$

Por convención se toma $v_p(0) = \infty$.

Ejemplo 4.22. $v_2(1) = 0$, $v_3(162) = 4$, *y* $v_7(7/50) = -2$.

Definición 4.23. *Dado un número $p \in \mathbb{Z}(i)$ primo gaussiano. Se define la valuación p-ádica gaussiana de un número $q \in \mathbb{Q}(i)$:*

$$g_p(q) = g_p(\frac{a}{b}) = r, \text{ tal que } \frac{a}{b} = p^r \frac{a_1}{b_1}$$

donde $a, b, a_1, b_1 \in \mathbb{Z}(i)$ y $p \nmid a_1 b_1$. Por convención se toma $g_p(0) = \infty$.

Ejemplo 4.24. $g_{2i}(5i/48) = -4$, $g_{7i}(49/(3i+1)) = 2$.

Proposición 4.25. *Sea*

$$S = \{p : p \text{ es un primo gaussiano, y } p|(r_1 - r_2)(r_1 - r_3)(r_2 - r_3)\}.$$

Si p es un primo gaussiano tal que $p|abc$, entonces $p \in S$.

Demostración. Supongamos que p es un primo gaussiano que divide a abc. Sea

$$k = g_p(x - r_1), \quad l = g_p(x - r_2), \quad m = g_p(x - r_3),$$

donde w_p es el valor p-adico extendido.
Ya que $p|abc$, p divide al menos uno de los a, b, c, es decir, $p|a$. Así p^k es la potencia más grande de p que divide a $x - r_1$. Ya que $x - r_1 = au^2$ y $a \in \mathbb{Z}(i)$ es cuadrado libre, se deduce que k es impar.
Supongamos que $k < 0$. Entonces $p^{|k|}$ es la potencia más grande de p que divide al denominador de $x - r_1$. Pero $r_1 \in \mathbb{Z}(i)$, $p^{|k|}$ debe dividir al denominador de x. Ya que $r_2, r_3 \in \mathbb{Z}(i)$, luego $p^{|k|}$ es la potencia más grande de p dividido por los denominadores $x - r_2$ y $x - r_3$, es decir

$$k = l = m$$

Por lo tanto $p^{|3k|}$ es la potencia más grande de p que divide a $y^2 = (x - r_1)(x - r_2)(x - r_3)$, lo cual es imposible (ya que $k + l + m$ debe ser par). Por lo tanto $k > 0$.
Usamos la notación $a|b$, donde $a \in \mathbb{Z}(i)$ y $b \in \mathbb{Q}(i)$ escritos como un cociente de enteros gaussianos, para denotar que a divide al numerador de b. Puesto que $k > 0$, debemos tener

$$p^k | x - r_1 \quad \Longrightarrow \quad x \equiv r_1 (\text{mod } p)$$

y por lo tanto

$$x - r_2 \equiv r_1 - r_2 (\text{mod } p), \quad \text{y}, \quad x - r_3 \equiv r_1 - r_3 (\text{mod } p).$$

Si $p \notin S$, es decir $p \nmid (r_1 - r_2)(r_1 - r_2)(r_2 - r_3)$, entonces tenemos

$$\begin{aligned} p \nmid r_1 - r_2 &\implies p \nmid x - r_2, \quad \text{y} \\ p \nmid r_1 - r_3 &\implies p \nmid x - r_3, \end{aligned}$$

es decir $l = m = 0$. Por lo tanto, la potencia más grande de p que divide a

$$y^2 = (x - r_1)(x - r_2)(x - r_3)$$

es $p^{k+l+m} = p^k$. Pero k es impar, lo cual es imposible. Por lo tanto $p \in S$. □

Lema 4.26. *La imagen de ϕ es finita.*

Demostración. Supongamos que (α, β, γ) es la terna representante de $\phi(P)$, para algún $P \in E(\mathbb{Q}(i))$. Sin pérdida de generalidad, podemos asumir que $\alpha, \beta, \gamma \in \mathbb{Z}(i)$ son libres de cuadrados.
La proposición 4.25 dice que cada α, β, γ es un producto de algunos primos gaussianos en S, como se definió en la proposición. Ya que S es finito, solo hay un número finito de posibilidades de α, β, γ. Así la imagen de ϕ es finito. □

Al tener el homomorfismo

$$\phi : E(\mathbb{Q}(i))/2E(\mathbb{Q}(i)) \longrightarrow \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2 \times \mathbb{Q}^*(i)/(\mathbb{Q}^*(i))^2$$

por el teorema fundamental de grupos, tenemos

$$E(\mathbb{Q}(i))/2E(\mathbb{Q}(i)) \cong Im(\phi)$$

Puesto que $Im(\phi)$ es finito, concluímos que $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es finito y esto completa la prueba del teorema 4.15.
A continuación demostremos el teorema de Mordell - Weil para $Q(i)$

Prueba del teorema de Mordell - Weil para $\mathbb{Q}(i)$

Del teorema 4.15 tenemos que $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es finito. Por el teorema 3.2, entonces concluímos que $E(\mathbb{Q}(i))$ es finitamente generado. Esto completa la prueba del teorema.

Conclusiones

- Se consiguió una caracterización de todos los elementos primos $\pi \in \mathbb{Z}[i]$, llamados primos gaussianos y estos son:

  1. $\pi = 1 + i$
  2. $\pi = a + bi$ con $a^2 + b^2 = p, p \equiv 1 \mod 4, a > |b| > 0$,
  3. $\pi = p, \quad p \equiv 3 \mod 4$.

- Se construyó un grupo abeliano adicionando un punto $\mathcal{O}$ a la curva elíptica por medio de una identificación entre los puntos del plano afín $\mathbb{A}_k^2$ y los puntos finitos del espacio proyectivo $\mathbb{P}_k^2$, junto con las identificacion de $\mathcal{O}$ con los puntos infinitos de $\mathbb{P}_k^2$.

- Se demostró que el grupo cociente $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito para dos casos. El primero teniendo en cuenta que el polinomio $p(x) = x^2 + Ax + B$, con $A, B \in \mathbb{Q}$ se descompone sobre $\mathbb{Q}$. El segundo, que la descomposición de dicho polinomio se da en una extensión finita de $\mathbb{Q}$.

- Para el caso general del teorema débil de Mordell - Weil, debido a que el anillo donde el polinomio $p(x) = x^2 + Ax + B$ se descompone, no siempre es un dominio de factorización única. Se realizó la localización del anillo el cual permitió recuperar propiedades como el dominio de factorización única. (Teorema 3.12).

- Se probó del teorema de Mordell - Weil para el caso gaussiano, es decir, se demostró que el grupo cociente $E(\mathbb{Q}(i))/2E(\mathbb{Q}(i))$ es finito, usando técnicas similares al caso racional para luego definir una función altura que permita probar que $E(\mathbb{Q}(i))$ es finitamente genrado (Teorema de Mordell - Weil).

Bibliografía

[1] Artin,E. (1998). *Galois theory*. Notre Dame, Francia: Notre Dame Press.

[2] Cassels, J.(1991). *Lectures on elliptic curves*. Cambridge, Reino Unido: Cambridge University Press.

[3] Cornell, G. y Silverman, J. (1986). *Arithmetic Geometry*. Connecticut, Estados Unidos: Springer-Verlag.

[4] Hankerson, D.; Menezes, A. y Vanstone, S. (2004). *Guide to Elliptic curve cryptography*. New York. Estados Unidos: Springer-Verlag.

[5] Husemöller, D. (2004). *Elliptic curves*. New York, Estados Unidos: Springer-Verlag.

[6] Knapp, A.(1992). *Elliptic curves*. New Yersey, Estados Unidos: Princeton University Press.

[7] Lang, S.(1978). *Elliptic curves: Diophantine Analysis*. Berlin, Alemania: Springer-Verlag.

[8] Mas, R. (2011). *Los grupos de torsión de una curva elíptica sobre los racionales (Tesis de pregrado)* . Universidad Nacional de Ingeniería, Lima, 2011.

[9] Milne, J. (2003). *Fields and Galois Theory*. Recuperado de: https://www.jmilne.org/math/CourseNotes/FTe6.pdf

[10] Milne, J. (2006), *Elliptic curves*. Estados Unidos:BookSurge Publishing.

[11] Neukirch, J.(2006) *Galois Theory*. Berlin, Alemania: Springer-Verlag.

[12] Robert, A. (1973). *Elliptic curves*. Berlin, Alemania: Springer-Verlag.

[13] Silverman, J. (1992). *Rational points of elliptic curves*. New York, Estados Unidos: Springer-Verlag.

[14] Washington, L. (2008). *Elliptic curves: Number theory and criptography*. Florida, Estados Unidos: Chapnan & Hall CRC.