UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

Teorema de Mordell

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

Matemático

P R E S E N T A :

Jacob Israel Orenday Lares

DIRECTOR DE TESIS:

Dr. Enrique Javier Elizondo Huerta

2015

Ciudad Universitaria, D. F.

Prefacio

Para un mejor entendimiento de la teoría utilizada para la demostración del teorema de Mordell es recomendable una lectura sobre geometría proyectiva, con especial énfasis en el plano proyectivo, coordenadas homogéneas, el teorema de Bezout y curvas en el plano proyectivo. Los mencionados temas se pueden encontrar en los libros Briskon -Knörrer, Fulton y Reid, cuyos títulos pueden ser consultados en la bibliografía al final de este escrito. El teorema de Mordell es un resultado sobre un cierto tipo de curvas elípticas, que permite una mejor compresión de este objeto matemático de gran importancia para las matemáticas. La importancia de las curvas elípticas puede ser observada en sus aplicaciones en la criptografía o en la demostración del último teorema de Fermat. Para profundizar en la teoría de las curvas elípticas se recomienda una lectura del libro de Joseph H. Silverman, *The Arithmetic of Elliptic Curves*.

Índice

Introducción

La teoría de ecuaciones diofantinas es una rama de la teoría de números que se dedica al estudio de las soluciones enteras y racionales de ecuaciones enteras. El nombre de esta se debe al matemático Diofantino de Alejandría, quien formuló y resolvió muchos problemas concernientes a esta teoría. Sin duda uno de los teoremas matemáticos más populares de toda la historia es el último teorema de Fermat (teorema que seguramente más de uno conoce) que establece que si n es mayor o igual que 3 es un entero, entonces la ecuación $X^n+Y^n=Z^n$. No tiene soluciones para X, Y yZ distintos de cero, equivalentemente la única solución de números racionales de la ecuación $x^n+y^n=1$ es cuando x=0 ó y=0. El teorema de fermat fue demostrado por el matemático británico Andrew Wiles en 1995 con la ayuda del matemático Richard taylor. Otro ejemplo de un problema de la teoría de ecuaciones diofantinas, es el problema de escribir un entero como la diferencia de un número cuadrático y un número cúbico. Es decir se fija un número entero "c" y encontramos las soluciones de la ecuación diofantina $y^2-x^3=c$. Supóngase que estamos interesados en obtener soluciones en números racionales x, y$\in \mathbb{Q}$. Una propiedad muy importante de esta ecuación es la existencia de una fórmula de duplicación, descubierta por Bachet en 1621. Si (x,y) es una solución de la ecuación, con x, y racionales, veamos que la siguiente fórmula

$$\left(\frac{x^4-8cx}{4y^2}, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$$

es una solución en números racionales a la misma ecuación

$$\left(\frac{-x^6-20cx^3+8c^2}{8y^3}\right)^2-\left(\frac{x^4-8cx}{4y^2}\right)^3$$

$$=\frac{x^{12}+40cx^9+384c^2x^6-320c^3x^3+64c^4-x^{12}+24cx^9-192c^2x^6+512c^3x^3}{64y^6}$$

$$=\frac{64cx^9+192c^2x^6+192c^3x^3+64c^4}{64y^6}=\frac{cx^9+3c^2x^6+3c^3x^3+c^4}{y^6}$$

como $x^3=y^2-c$, tenemos que

$$\frac{cx^9+3c^2x^6+3c^3x^3+c^4}{y^6}=\frac{c\left(\left(y^2-c\right)^3+3c\left(y^2-c\right)^2+3c^2\left(y^2-c\right)+c^3\right)}{y^6}$$

$$=\frac{c\left(y^6-3y^4c+3c^2y^2-c^3+3cy^4-6y^2c^2+3c^3+3c^2y^2-3c^3+c^3\right)}{y^6}=\frac{cy^6}{y^6}=c$$

Por lo que la fórmula anterior es una solución si (x, y) es una solución. Es posible probar que si (x, y) es una solución de la ecuación $y^2-x^3=c$ y cumple que $xy\neq 0$ y si $c\neq 1, -432$, es posible repetir el proceso anterior un número infinito de veces y por lo tanto encontrar una cantidad infinita de soluciones. Es decir, si tenemos un entero distinto de 1 y -432 que puede ser expresado como la diferencia del cuadrado de un número racional distinto de cero y el cubo de un número racional distinto de cero, entonces dicho entero puede ser expresado de infinitas maneras distintas. Por ejemplo si empezamos con la solución $(2, 4)$ a la ecuación

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

aplicando la fórmula de Bachelet, encontramos una sucesión de soluciones

$$(2,4)\,,\ \left(\frac{-112}{64}, \frac{-832}{512}\right),\ \ldots$$

Los números se hacen muy grandes de manera muy rápida. Tomemos de nueva cuenta la misma ecuación

$$y^2-x^3=c$$

ahora nos preguntamos cómo encontrar soluciones enteras para esta ecuación. En el año 1650 Fermat le propuso a la comunidad matemática inglesa demostrar que la ecuación $y^2 - x^3 = 2$ tiene solo dos soluciones enteras (por la fórmula de duplicación de Bachelet podemos encontrar un número infinito de soluciones racionales, pues $(3,5)$ es una solución por lo que $\left(\frac{129}{10^2}, \frac{-383}{10^3}\right)$ y también $\left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}\right)$ y así sucesivamente) que son $(3,5)$ y $(3,-5)$. Ningún contemporáneo de Fermat pudo resolver el problema, en 1730 Euler dio una prueba falsa, el problema pudo ser resuelto hasta el año 1880. En el año 1908, Axel Thue fue más allá y demostró que si $c \neq 0$ la ecuación $y^2 - x^3 = c$ solo puede tener un número finito de soluciones enteras, es decir, con $x, y \in \mathbb{Z}$. Lo cual resultó ser una respuesta más general al reto de Fermat, puesto que respecto al número infinito de soluciones racionales que tiene esta ecuación solo tiene un número finito de soluciones enteras. El siglo 17 atestiguó la introducción de coordenadas a la geometría, un cambio revolucionario que permitió el abordamiento de problemas geométricos desde una perspectiva algebraica y viceversa. Por ejemplo, si n es par, entonces las soluciones reales a la ecuación de Fermat $x^n + y^n = 1$ en el plano xy se ven como un círculo aplastado. Podemos ver la ecuación de Bachelet $y^2 - x^3 = c$. Recordemos que Bachelet descubrió una fórmula de duplicación que nos permite encontrar nuevas soluciones a partir de una solución racional dada. La fórmula de Bachelet es complicada, por lo que resulta natural preguntarse de dónde viene, la respuesta es, de la geometría. Supongamos que tenemos la solución de números racionales a la ecuación de Bachelet $P = (x_1, y_1)$, por lo que P es un punto en la curva definida por la ecuación de Bachelet. Si trazamos la recta tangente en el punto P, esta recta intersectará a la curva en un punto $Q = (x_2, y_2)$. La pendiente de esta recta es la derivada dy/dx en P por el teorema de la función implícita aplicado a $F(x,y) = y^2 - x^3$ tenemos que

$$\frac{dy}{dx} = -\frac{F_x}{F_y} = -\frac{-3x^2}{2y} = \frac{3x^2}{2y}$$

En consecuencia, la ecuación de la recta tangente en P es

$$y - y_1 = \frac{3x_1^2}{2y_1}(x - x_0),\ y = \frac{3x_1^2}{2y_1}(x - x_1) + y_1$$

Sustituyendo y en $F(x,y)$ obtenemos $\left(\frac{3x_1^2}{2y_1}(x - x_1) + y_1\right)^2 - x^3 = c$ que puede ser reacomodada para verse como

$$x^3 - \frac{9x_1^4}{4y_1^2}x^2 + Tx + R = 0$$

donde T y R son constantes que no necesitamos calcular de manera explícita, pues x_1 es una raíz de multiplicidad dos de la ecuación anterior. Pero la coordenada x de Q, es decir, x_2 debe también satisfacer la misma ecuación. Sabemos que la suma de las raíces de una ecuación cúbica es el negativo del coeficiente de x^2. Entonces,

$$x_2 + x_1 + x_1 = \frac{9x_1^4}{4y_1^4},\ x_2 = \frac{9x_1^4}{4y_1^2} - 2x_1 = \frac{9x_1^4 - 8x_1y_1^2}{4y_1^2}$$

Usando $y_1^2 - x_1^3 = c$, podemos reescribir x_2 como

$$x_2 = \frac{x_1^4 + 8x_1^4 - 8x_1y_1^2}{4y_1^2} = \frac{x_1^4 + 8x_1\left(x_1^3 - y_1^2\right)}{4y_1^2} = \frac{x_1^4 - 8cx_1}{4y_1^2}, \quad x_1 = \frac{x_1^4 - 8cx_1}{4y_1^2}$$

Podemos ahora computar la coordenada y de Q usando la ecuación de la recta tangente

$$y_2 = \frac{3x_1^2}{2y_1}(x_2 - x_1) + y_1 = \frac{3x_1^2}{2y_1}\left(\frac{x_1^4 - 8cx_1}{4y_1} - x_1\right) + y_1$$

$$= \frac{3x_1^6 - 24cx_1^3 - 12x_1^3y_1^2 + 8y_1^4}{8y_1^3}$$

$$= \frac{-x_1^6 - 24cx_1^3 + \left(4x_1^3y_1^2 - 4x_1^6\right) + \left(8x_1^6 - 16x_1^3y_1^2 + 8y_1^4\right)}{8y_1^3}$$

$$= \frac{-x_1^6 - 24cx_1^3 + 4x_1^3\left(y_1^2 - x_1^3\right) + 8\left(y_1^2 - x_1^3\right)^2}{8y_1^3}$$

$$= \frac{-x_1^6 - 24cx_1^3 + 4cx_1^3 + 8c^2}{8y_1^3} = \frac{-x_1^6 - 20cx_1^3 + 8c^2}{8y_1^3}$$

Por lo que $y = \frac{-x_1^6 - 20cx_1^3 + 8c^2}{8y_1^3}$. Finalmente concluimos que

$$Q = (x_2, y_2) = \left(\frac{x_1^4 - 8cx_1}{4y_1^2}, \frac{-x_1^6 - 20cx_1^3 + 8c^2}{8y_1^3}\right).$$

Por lo que la complicada fórmula algebraica de Bachet tiene una interpretación geométrica sencilla en términos de la intersección de una recta tangente con una curva. Esta es una excelente muestra de la productiva relación que existe entre la teoría de números, el álgebra y la geometría. El tipo más sencillo de una ecuación diofantina es una ecuación polinomial de una variable

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Si suponemos que $a_0, \ldots, a_n$ son enteros, nos podemos preguntar cómo encontrar todas las soluciones enteras y racionales, revisando el lema de Gauss podemos encontrar una respuesta sencilla a esta interrogante. Si p y q son primos relativos, entonces el lema de Gauss nos dice que q divide a a_n y p divide a a_0. Sabemos que esta ecuación puede tener a lo más n soluciones y por otro lado tendremos un número finito de posibles soluciones racionales, pues tendremos como candidatos a soluciones todos los números racionales que satisfagan el lema de Gauss, una vez encontrada esta lista de números racionales que no contradicen el lema de Gauss (todos los números de la forma p/q tales que p divide a a_0 y q divide a a_n) deberemos computar esta pequeña lista para determinar cuáles sí son soluciones. Por lo que encontrar las soluciones de ecuaciones diofantinas de una variable resulta una tarea fácil. Encontrar la solución de una ecuación diofantina de dos variables no resulta tan trivial como las de una variable. Supongamos que tenemos un polinomio $f(x, y)$ con coeficientes enteros y nos fijamos en la ecuación

$$f(x, y) = 0$$

Las ecuaciones de Bachet y Fermat son ecuaciones de este tipo. Aquí están algunas preguntas que nos podemos hacer (a) ¿Existen soluciones enteras? (b) ¿Existen soluciones racionales? (c) ¿Existen un número infinito de soluciones enteras? (d) ¿Existen un número infinito de soluciones racionales? En cuanto a esta generalidad, solo la pregunta (c) ha sido completamente contestada. se han hecho avances importantes sobre la pregunta (d). Al conjunto de soluciones reales de un polinomio de dos variables en el plano euclideano se le llama una curva algebraica. Por lo que al conjunto de soluciones de la ecuación $f(x, y) = 0$ forma una curva algebraica en el plano xy. En el intento por resolver las interrogantes de los incisos $(a) - (d)$ es útil fijarnos en polinomios sencillos, como por ejemplo polinomios de grado 1. Para una ecuación lineal

$$ax + by = c$$

con coeficientes enteros, resulta sencillo responder a las preguntas de los cuatro incisos. Siempre existen un número infinito de soluciones racionales que pueden ser encontradas despejando. En caso de que el $mcd(a, b)$ no divida a c no existirán soluciones enteras, de otro modo existen un número infinito de soluciones enteras. Resulta aún más sencillo resolver ecuaciones lineales que ecuaciones de una variable. Ahora nos fijamos en los polinomios de grado 2 (también llamados polinomios cuadráticos). Las gráficas de estos polinomios representan secciones cónicas. Se sabe que si un polinomio de grado dos tiene una solución racional, entonces tiene un número infinito de soluciones. El cojunto total de soluciones puede ser encontrado utilizando geometría. Esto será explicado en el capítulo I. También se explicará cómo responder a la pregunta (b) para polinomios cuadráticos. Pese a que la resolución de los polinomios cuadráticos resulta complicada sus soluciones han sido ya entendidas. El principal objetivo de esta tesis es estudiar las soluciones racionales y enteras de polinomios de grado 3. Un ejemplo de una ecuación de este

tipo es la ecuación de Bachet $y^2 - x^3 = c$, otros ejemplos que estudiaremos son las ecuaciones

$$y^2 = x^3 + ax^2 + bx + c \quad y \quad ax^3 + by^3 = c.$$

Las soluciones reales a estas ecuaciones son llamadas curvas cúbicas o curvas elípticas. En contraste con los ejemplos anteriores, las soluciones enteras y racionales de las curvas elípticas no han sido del todo entendidas; y en los casos en que las soluciones son completamente entendidas, las pruebas requieren de la teoría de números, geometría y álgebra.

El principal propósito es el estudio de las ecuaciones diofantinas estudiando a profundidad el primer caso de este tipo de ecuaciones que aún no han sido perfectamente entendidas que son las ecuaciones cúbicas de dos variables. Para que el lector comprenda los resultados que se abordarán en esta tesis, diremos los resultados que se tienen respecto a las preguntas $(a) - (d)$.

CAPÍTULO I

1.1 Puntos racionales sobre cónicas

Un número racional es el cociente de dos números enteros, hecho que es evidente para más de uno. Llamamos a un punto en el plano (x,y) un punto racional si sus dos coordenadas son números racionales. Llamamos a una recta racional, si la ecuación de la recta puede ser escrita con números racionales, eso es

$$ax + by + c = 0$$

con a, b, c racionales. Veamos que si tenemos dos puntos racionales, la recta que los une es racional. Sean (x_1, y_1) y (x_2, y_2) dos puntos racionales, entonces la ecuación que pasa por esos dos puntos es $y = \frac{y_1 - y_2}{x_1 - x_2}x + y_1 - \frac{y_1 - y_2}{x_1 - x_2}x_1$, la pendiente es racional puesto que $y_1 - y_2$ es racional y $x_1 - x_2$ es racional y la división de dos números racionales es un número racional, por lo que los coeficientes de la ecuación son racionales, por lo que esta es una ecuación racional. Ahora veamos que el punto de intersección de dos rectas racionales es un punto racional. Considérense las ecuaciones $a_1x + b_1y + c_1 = 0$ y $a_2x + b_2y + c_2 = 0$, de donde x= $\frac{-b_1y - c_1}{a_1}$, por lo que $a_2(\frac{-b_1y - c_1}{a_1}) + b_2y + c_2 = 0$, obtenemos que $\frac{-a_2b_1y - a_2c_1 + a_1b_2y}{a_1} + c_2 = 0$, se infiere que $\frac{y(-a_2b_1 + a_1b_2)}{a_1} = -\frac{a_2c_1}{a_1} - c_2$, entonces $y(-a_2b_1 + a_1b_2) = -a_2c_1 - c_2a_1$, finalmente tenemos que $y = \frac{-a_2c_1 - c_2a_1}{-a_2b_1 + a_1b_2}$ y como los coeficientes son racionales se sigue que y es racional y como $x = \frac{-b_1(\frac{-a_2c_1 - c_2a_1}{-a_2b_1 + a_1b_2}) - c_1}{a_1}$ se sigue que x es racional. Sea

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

una cónica. Decimos que una cónica es racional, si podemos escribir esta ecuación con números racionales. Si consideramos la circunferencia $x^2 + y^2 = 2$ y la recta $y = 0$, vemos que ambas son racionales y sin embargo los puntos de intersección son $\left(\sqrt{2}, 0\right)$ y $\left(-\sqrt{2}, 0\right)$, por lo que en general la intersección de una cónica racional y una recta racional no es un punto racional. Si buscamos la intersección de una recta racional y una cónica racional, lo que obtendremos es una ecuación cuadrática con coeficientes racionales, por lo que la intersección de la recta y la cónica será racional si y solamente si las raíces de esta ecuación son racionales. En general las raíces pueden ser irracionales. Sin embargo, si una de las raíces es racional también lo será la otra raíz. Esto es verdad debido a que si tenemos una ecuación cuadrática con coeficientes racionales, entonces la otra raíz es racional, porque la suma de las raíces es el coeficiente intermedio.

Supongamos que tenemos una cónica racional y que tenemos un punto O racional sobre la cónica. Entonces podemos obtener todos los puntos racionales de la cónica de manera sencilla. Primero dibujamos una recta racional y luego proyectamos la cónica desde el punto O sobre la recta racional, para proyectar el punto O sobre la recta, trazamos la recta tangente a la cónica en O. Debido a que en general una recta intersecta a una cónica en dos puntos, lo que hemos construido, es una relación biyectiva entre los puntos racionales de la cónica y los puntos racionales de la recta y de hecho entre todos los puntos de la cónica y todos los puntos de la recta (excepto para el punto O). Esto debido a que cuando tenemos una raíz racional, de la ecuación cuadrática producida por la sustitución de la ecuación de la recta en la ecuación de la cónica, la otra raíz es también racional. Lo que tenemos es dos rectas racionales (la recta que proyecta los puntos racionales sobre la recta y la recta auxiliar) cuya intersección es un punto racional. A manera de ejemplo realicemos este procedimiento al círculo

$$x^2 + y^2 = 1.$$

Proyectaremos desde el punto $(-1, 0)$ (es racional) sobre el eje y (que es una recta racional). Llamemos al punto de intersección (de la recta que une el punto (-1,0) con un punto (x, y) en la cónica y el eje y) $(0, t)$. Una vez calculado el punto (x, y), es fácil obtener el valor de t. La ecuación de la recta que une a los puntos $(-1, 0)$ y $(0, t)$

es $y = t(1+x)$. Buscamos la intersección de esta recta con la circunferencia, por lo que obtenemos la siguiente relación

$$1 - x^2 = y^2 = t^2(1+x)^2.$$

Como el punto $(-1, 0)$ está en el círculo y la recta, $x = -1$ satisface la ecuación, ahora encontremos la otra raíz

$$\begin{aligned}
(1+x)(1-x) &= t^2(1+x)(1+x),\\
t^2(1+x) &= (1-x),\\
\frac{1-x}{1+x} + 1 &= t^2 + 1,\\
\frac{2}{1+x} &= t^2 + 1,\\
\frac{2}{t^2+1} &= 1 + x,\\
\frac{2-(t^2-1)}{t^2+1} &= x,\\
\frac{1-t^2}{t^2+1} &= x.
\end{aligned}$$

Además, $y = t(1+x)$, por lo que $y = t(1 + \frac{1-t^2}{t^2+1})$, se sigue que $y = t(\frac{t^2+1+1-t^2}{t^2+1})$, por último $y = \frac{2t}{t^2+1}$. Lo que hemos obtenido es la parametrización racional del círculo. Gracias a estas fórmulas ahora es claro que si $x, y \in \mathbb{Q}$ entonces $t \in \mathbb{Q}$. Inversamente si $t \in \mathbb{Q}$ entonces $x, y \in \mathbb{Q}$. Por lo que este procedimiento funciona para encontrar puntos racionales en el círculo. Estas fórmulas son útiles para describir todos los triángulos rectángulos cuyos lados miden un número entero. Consideremos el problema de encontrar triángulos distintos al triángulo cuyos lados son 3,4,5, tales que tienen un lado que mide un número entero. Llamemos a los lados del triángulo X, Y, Z. Buscamos los enteros, tales que

$$X^2 + Y^2 = Z^2.$$

Supongamos que existe un factor común de estos tres números, entonces podemos factorizarlo y quitarlo, por lo que podemos suponer sin pérdida de generalidad que estos tres números no tienen ningún factor común. A los triángulos que tienen la característica de que todos sus lados no tienen factores comunes se les llama primitivos. Si existiera un factor común de los números X, Z, entonces dividiría a $Y^2 = Z^2 - X^2$, entonces los tres números tendrían un factor común lo cual sería contrario a nuestra suposición. Entonces si hacemos la reducción a triángulos primitivos, entonces ningún par de lados tiene un factor común. En particular, el punto (x, y) definido por

$$x = \frac{X}{Z}, \qquad y = \frac{Y}{Z},$$

es un punto racional en el círculo $x^2 + y^2 = 1$. Además como los lados no tienen factor común, x, y son fracciones irreducibles. Debido a que X y Y no tienen factor común, entonces no pueden ser par. Veamos que tampoco ambos números pueden ser impares. Notemos que el cuadrado de un número impar es congruente con 1 módulo 4. Sea $n = 2k+1$, entonces $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1(\text{mód}4)$. Si X, Y fueran ambos impares, entonces $X^2 + Y^2$ sería congruente con 2 módulo 4. Pero $X^2 + Y^2 = Z^2$ y Z es par o impar, entonces Z es congruente con 1 ó 0 módulo 4, por lo que ambos números no pueden ser impares. De ahora en adelante consideraremos X impar y Y par. Como (x, y) es un punto racional en el círculo, con las fórmulas que derivamos anteriormente podemos expresar las coordenadas x, y, en términos de la fracción irreducible $t = \frac{m}{n}$, donde $m, n \in \mathbb{Z}$. Entonces

$$\frac{X}{Z} = x = \frac{n^2 - m^2}{n^2 + m^2}, \qquad \frac{Y}{Z} = y = \frac{2mn}{n^2 + m^2}.$$

Como $\frac{X}{Z}$ y $\frac{Y}{Z}$ son fracciones irreducibles, entonces existe un entero λ tal que

$$\lambda Z = n^2 + m^2, \qquad \lambda Y = 2mn, \qquad \lambda X = n^2 - m^2.$$

Queremos demostrar que $\lambda = 1$. Como λ divide a $n^2 + m^2$ y $n^2 - m^2$, entonces existen $k_1, k_2 \in \mathbb{Z}$ tales que $\lambda k_1 = n^2+m^2$ y $\lambda k_2 = n^2-m^2$, entonces $\lambda(k_1+k_2) = n^2+m^2+n^2-m^2 = 2n^2$ y $\lambda(k_1-k_2) = n^2+m^2-n^2+m^2 = 2m^2$. Por otro lado el máximo común divisor de m y n es 1 (por hipótesis), por lo que si λ dividiera a m y n, entonces λ tendría el valor de 1 y habríamos acabado, entonces si λ divide a 2, tenemos $\lambda = 1$ ó $\lambda = 2$. Si $\lambda = 2$, obtenemos que $n^2 - m^2 = \lambda X$ es divisible por 2, pero no por 4, puesto que hemos asumido que el valor de X es impar. Como X es impar entonces existe $k \in \mathbb{Z}$ tal que $X = 2k + 1$, por lo que $2X = 4k + 2$, entonces $n^2 - m^2$ es congruente con 2 módulo 4. Pero claramente n^2 y m^2 son congruentes con 1 ó 0 modulo 4, por lo que λ no puede valer 2. Por lo tanto $\lambda = 1$. Por lo que hemos probado que para obtener todos los triángulos primitivos, tomas dos enteros primos relativos m y n y haces

$$X = n^2 - m^2, \qquad Y = 2mn, \qquad Z = n^2 + m^2,$$

los lados del triángulo. Donde X es impar y Y es par. Los otros triángulos se obtienen intercambiando la paridad de X y Y (haciendo X par y Y impar). Estas fórmulas tienen una relación muy importante ilustrada a continuación

$$x = \cos\theta, \qquad y = sen\theta; \qquad , t = tan\frac{1}{2}\theta = \frac{2t}{1+t^2}.$$

las fórmulas citadas arriba nos permiten expresar el seno y coseno racionalmente en términos de la tangente del medio ángulo

$$x = cos\theta = \frac{1-t^2}{1+t^2}, \qquad y = sen\theta = \frac{2t}{1+t^2}.$$

Otro uso útil, proviene del hecho de que estas fórmulas nos permiten expresar todas las funciones trigonométricas de un ángulo θ como expresiones racionales con $t = tan(\theta/2)$. Notemos que

$$\theta = 2arctan(t), \qquad d\theta = \frac{2dt}{1+t^2}.$$

Que resultan útiles cuando se tiene una integral de senθ, cosθ y $d\theta$, pues esta integral con una sustitución adecuada se puede transformar en una integral de t y dt. Si la integral es una función racional de senθ y cosθ, el resultado de la integral es una función racional de t. Como toda función racional puede ser integrada en términos de funciones elementales, entonces toda función racional en términos de cosθ y senθ pueden ser integradas en términos de funciones elementales. Tomemos el círculo

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

y busquemos los puntos racionales en el. Si existiera un punto racional sobre este círculo, entonces podemos escribir ese punto de la siguiente forma

$$x = \frac{X}{Z} \qquad y \qquad y = \frac{Y}{Z}$$

con $X, Y, Z \in \mathbb{Q}$; entonces

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

Utilizando el mismo argumento que se usó para encontrar los triángulos primitivos, podemos suponer que X, Y, Z no tienen factor común. Si el 3 dividiera a X, entonces 3 divide a $Y^2 = 3Z^2 - X^2$, entonces 3 divide a Y. Entonces 9 divide a $X^2 + Y^2 = 3Z^2$, entonces 3 divide a Z, en cuyo caso X, Y, Z tendrían un factor común. Por lo tanto 3 no divide a X y por las mismas razones 3 no divide a Y. Debido a que X y Y no es divisible por tres, tenemos que

$$X \equiv 3 \pm 1 \text{ (módulo 3)}, \qquad Y \equiv \pm 1 \text{ (módulo 3)}, \qquad y, \qquad X^2 \equiv Y^2 \equiv 1 \text{ (módulo 3)}.$$

pero entonces

$$0 \equiv 3Z^2 = X^2 + Y^2 \equiv 1 + 1 \equiv 2 \qquad \text{(módulo 3)}.$$

Por lo que es imposible encontrar dos números racionales cuya suma de cuadrados dé como resultado 3. Hemos visto cómo encontrar los puntos racionales en una cónica, a partir de un punto racional dado sobre la cónica, y hemos encontrado las fórmulas que permiten expresar las coordenadas en términos de un parámetro racional t. Sin embargo, este método depende del hecho de que se conozcan las coordenadas de un punto racional, entonces surge la pregunta ¿Cómo obtener el punto racional que nos permita obtener el resto de los puntos racionales? Lo que

se realizó con el círculo de radio 3 nos da una pista de cómo hacerlo, al ver que una ecuación no tenía soluciones módulo 3 pudimos ver que no había puntos racionales en dicho círculo. Existe un método que puede probar en un número finito de pasos si dada una cónica racional existe un punto racional en ella. El método consiste en buscar una congruencia que pueda ser satisfecha. El teorema que valida el método se debe a Legendre. Tomemos el caso simple en que

$$aX^2 + bY^2 = cZ^2,$$

que deseamos resolver para número enteros. El teorema de Legendre establece que existe un número entero m, que depende de cierta manera de los números a, b, c que permite que la ecuación de arriba tenga una solución en números de enteros, con alguno distinto de cero, si y sólo si la congruencia

$$aX^2 + bY^2 \equiv cZ^2 \qquad (\text{módulo m})$$

tiene solución en enteros que es primo relativo con m. Por lo que hemos encontrado un método que nos permite responder cuándo podemos encontrar un punto racional en una cónica racional y por ende encontrar el resto de los puntos racionales en la cónica. Ahora intentaremos encontrar la misma respuesta para cúbicas.

1.2. La geometría de curvas cúbicas

Iniciaremos el estudio de cúbicas. Sea

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

la ecuación general de una cúbica. Decimos que una cúbica es *racional* si los coeficientes de su ecuación son números racionales. Un ejemplo de una cúbica *racional es*

$$x^3 + y^3 = 1;$$

ó en su forma homogénea,

$$X^3 + Y^3 = Z^3.$$

Encontrar soluciones racionales de $x^3 + y^3 = 1$, equivale a encontrar soluciones enteras de $X^3 + Y^3 = Z^3$, que es el primer caso no trivial del último teorema de Fermat. Ahora que estamos trabajando con cúbicas, no podemos utilizar el mismo método geométrico que utilizamos con las cónicas para encontrar números racionales, esto debido a que, en general, una recta intersecta a una cúbica en tres puntos, por lo que de unir un punto racional que no esté en la cúbica con un punto racional sobre la cúbica, obtendríamos dos puntos adicionales, por lo que con ese método no obtenemos una correspondencia uno a uno, es decir a cada punto en la recta en la que se desea proyectar los puntos racionales de la cúbica le corresponderían 2 puntos. Este problema se soluciona si podemos encontrar dos puntos racionales en la cúbica, entonces al unir estos dos puntos obtenemos una recta racional que intersecta, en general, en un tercer punto a la cúbica. Se puede demostrar que la intersección de una recta racional y una cúbica racional, es una ecuación cúbica con coeficientes racionales. Sea $x = \frac{-c-by}{a}$ la recta racional que une a los dos puntos en la cúbica, entonces existen dos puntos $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ con $x_1, x_2, y_1, y_2 \in \mathbb{Q}$ en la cúbica y en la recta, por lo que estos puntos satisfacen las siguientes ecuaciones

$$x_1 = \tfrac{-c-by_1}{a},\ x_2 = \tfrac{-c-by_2}{a} \text{ y}$$

$$ax_{11}^3 + b_1x_1^2y_1 + c_1x_1y_1^2 + dy_1^3 + ex_1 + fx_1y_1 + gy_1^2 + hx_1 + iy_1 + j = 0 \text{ y}$$

$$a_1x_2^3 + b_1x_x^2y_2 + c_1x_2y_2^2 + dy_2^3 + ex_2 + fx_2y_2 + gy_2^2 + hx_2 + iy_2 + j = 0, \text{ por lo que}$$

$$a_1(\tfrac{-c-by_1}{a})^3 + b_1(\tfrac{-c-by_1}{a})^2y_1 + c_1(\tfrac{-c-by_1}{a})y_1^2 + dy_1^3 + e(\tfrac{-c-by_1}{a}) + f(\tfrac{-c-by_1}{a})y_1 + gy_1^2 + h(\tfrac{-c-by_1}{a}) + iy_1 + j = 0$$

$$\text{y } a_1(\tfrac{-c-by_2}{a})^3 + b_1(\tfrac{-c-by_2}{a})^2y_2 + c_1(\tfrac{-c-by_2}{a})y_2^2 + dy_2^3 + e(\tfrac{-c-by_2}{a}) + f(\tfrac{-c-by_2}{a})y_2 + gy_2^2 + h(\tfrac{-c-by_2}{a}) + iy_2 + j = 0$$

y como $a, b, c, a_1, b_1, c_1, d, e, f, g, h, i, j \in \mathbb{Q}$ entonces estas ecuaciones tienen coeficientes racionales. De aquí resulta evidente, que si se tienen dos raíces racionales la tercera debe serlo también. A continuación daremos algunos ejemplos de como funciona este método para encontrar un tercer punto racional.

Supongamos que P y Q son dos puntos racionales sobre una cúbica, tracemos la recta que une a estos dos puntos, sea P*Q el punto que denota el tercer punto de intersección con la cúbica. Si tenemos un punto racional P podemos encontrar un segundo punto racional en la cúbica, pues al trazar la recta tangente a la cúbica en el punto P, la tangente debe intersectar a la cúbica en un segundo punto. Esencialmente lo que se está haciendo es trazar una recta que va de P a P, es decir una recta racional que debe intersectar a la cúbica en un tercer punto racional, luego podemos unir estos puntos y obtener más puntos racionales en la cúbica. Si se inicia con unos cuantos puntos racionales podemos obtener muchos más. También consideraremos que si una recta va de P a Q y la recta es tangente a la curva en P, entonces diremos que $P * Q = P$, del mismo modo consideraremos $P * P = Q$. Además si tenemos el punto de inflexión P, entonces la recta tangente a la curva en P intersecta a la curva tres veces, es decir, $P * P = P$, el tercer punto de intersección de la recta que va de P a P es P.

Uno de los objetivos principales de esta tesis es demostrar teorema de Mordell que establece que si C es una curva cúbica racional no singular, entonces existe un conjunto finito de puntos racionales tal que todos los puntos racionales en C pueden ser obtenidos en la forma que describimos anteriormente. Se probará el teorema de Mordell para una clase amplia de curvas cúbicas, usando únicamente teoría de números para los enteros usuales. La versión general de este teorema emplea herramientas de la teoría algebraica de números. Por lo que reformularemos el teorema, pero antes probaremos una propiedad elemental de la geometría de las curvas cúbicas. Dos curvas cúbicas en general se intersectan en 9 puntos. Pero para que esto siempre suceda, debemos introducir el uso del plano proyectivo, aceptar multiplicidades en las intersecciones, por ejemplo considerar los puntos de tangencia como intersecciones con multiplicidad mayor a uno. También debemos introducir el uso de coordenadas complejas. El teorema de Bezout establece que una curva de grado m y una curva de grado n se intersectan en mn puntos. El teorema que queremos emplear para reformular el teorema de Mordell es si $C, C_1,$ y C son tres curvas cúbicas.

Supóngase que C intersecta a 8 puntos de los 9 puntos de la intersección de C_1 y C_2. Entonces C intersecta al noveno punto de intersección de C_1 y C_2. Para poder definir una curva cúbica, tenemos que definir 10 coeficientes. Si multiplicamos los diez coeficientes de una curva cúbica, obtenemos la misma curva, por lo que el conjunto de todas las posibles curvas cúbicas es de dimensión 9. Si por ejemplo, quisiéramos que una curva cúbica pase por un punto dado, tal que sus coordenadas x, y estén dadas, entonces estos diez coeficientes deben cumplir una condición lineal determinada, debido a que el punto con coordenadas x, y satisface la ecuación de la cúbica, por lo que el conjunto de curvas cúbicas que pasan por dicho punto debe ser de dimensión 8.

Análogamente si deseamos encontrar el conjunto de cúbicas que pasan por dos puntos dados, la dimensión de este conjunto es de dimensión 8. Entonces, la familia de cúbicas que atraviesan los 8 puntos de intersección de las curvas cúbicas C_1 y C_2 es de dimensión 1. Sean $H_1(x, y) = 0$ y $H_2(x, y) = 0$ las ecuaciones cúbicas de las curvas C_1 y C_2 respectivamente. Podemos ver a la familia de cúbicas que cruza por los ocho puntos de intersección de las curvas C_1 y C_2 como combinaciones lineales de la forma $\lambda_1 H_1 + \lambda_2 H_2$. Debido a que la familia de cúbicas que pasan por los ocho puntos de intersección de las curvas C_1 y C_2 (de los nueve), forman una familia de dimensión uno y como la familia de cúbicas de la forma $\lambda_1 H_1 + \lambda_2 H_2$ es de dimensión uno, entonces debido a que la cúbica C pasa por los ocho puntos existen λ_1, λ_2 tales que C cumple con la ecuación $\lambda_1 H_1 + \lambda_2 H_2 = 0$. Debido a que el noveno punto está en H_1 y H_2 entonces ambas ecuaciones se anulan en el noveno punto, por lo que cualquier combinación lineal de H_1 y H_2 también se anula, y dado que C es una combinación lineal de H_1 y H_2 se sigue que C se anula en el noveno punto, por lo que el noveno punto está en C. Con las cónicas vimos que es posible averiguar en un número finito de pasos si existe un punto racional sobre la cónica o no, por desgracia no se conoce un método que permita averiguar en un número finito de pasos si existe o no un punto racional en una cúbica, es decir no existe un análogo del teorema de Hasse para cúbicas. La idea empleada anteriormente para cónicas, de buscar congruencias módulo m para todo m no es suficiente. A continuación tenemos un ejemplo realizado por Selmer que ilustra la dificultad

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

Selmer demostró que no existe una solución distinta a la trivial (en enteros) y sin embargo es posible probar que para todo m la congruencia

$$3X^3 + 4Y^3 + 5Z^3 \equiv 0 \pmod{\text{módulo m}}$$

tiene soluciones enteras sin factor común. Por lo que a diferencia del caso de las cónicas, en las cúbicas la existencia de una solución módulo m para todo m no garantiza la existencia de una solución racional, es decir la existencia de un punto racional en la cúbica. Haciendo a un lado esta dificultad, podemos siempre suponer que existe un punto racional O en la cúbica. Como mencionamos anteriormente, queremos reformular el teorema de Mordell, y probar una versión particular que abarque a una amplia familia de cúbicas.

Consideremos que tenemos una cúbica racional y dos puntos P y Q en ella, entonces al dibujar la recta que une a estos dos puntos obtenemos un tercer punto al que denotamos como $P * Q$, resulta lógico preguntarse si esta "operación" define un grupo sobre los puntos de racionales de la curva cúbica, pregunta que resulta fácil de responder, consideremos que existe un elemento r tal que $r * P = P = P * r$, para todo punto P racional en la curva, por definición $r * P$ es el tercer punto de intersección de la recta que une a r y P, por lo que la única forma en que este punto sea P es que la recta que une a r y P tenga multiplicidad dos en la intersección con r, es decir que sea tangente a la cúbica en r, pero P era cualquier punto, por lo que no existe un elemento identidad.

Afortunadamente es posible darle una estructura de grupo a los puntos racionales de la cúbica, bajo la siguiente operación. Sea O el punto racional dado en la cúbica. Para sumar P y Q, tómese el punto $P * Q$ (el tercer punto de intersección de la recta que une a P y Q), únase con una recta el punto $P * Q$ con O, sea $P + Q$ el tercer punto de dicha recta. Entonces $P + Q = O * (P * Q)$. Veamos que bajo esta operación, el conjunto de puntos racionales de la curva cúbica tienen una estructura de grupo abeliano. Propiedad de conmutatividad, $P + Q = O * (P * Q)$ y $Q + P = O * (Q * P)$, por lo que basta demostrar que $(P * Q) = (Q * P)$, igualdad que resulta evidente puesto que la recta que une a P y Q es la misma que la recta que une a Q y P. Por lo tanto $P + Q = Q + P$.

Existencia del elemento identidad, proponemos O como el elemento identidad, veamos que efectivamente $P+O = P$, $P+O = O*(P*O)$ que es el punto que resulta de la intersección de la recta que va de O a $P*O$ con la cúbica. La recta que une a O y a $P * O$ intersecta a la cúbica en un tercer punto. Caso 1. Si la recta que une a estos puntos es tangente en O a la cúbica, entonces la recta intersecta dos veces a la cúbica en O, por lo que $P * O = P$. Caso 2. Si la recta que une a estos puntos no es tangente en O a la cúbica, entonces la recta que une a estos puntos intersecta en un tercer punto a la cúbica, en un punto que no es ni O ni $P * O$, y como P y O son colineales con $P * O$ entonces el tercer punto de intersección es P. Por lo tanto, $P + O = P$.

Para obtener el inverso aditivo de un elemento P, tomemos la recta tangente a la cúbica en el punto O, sea S el punto distinto de O que intersecta a la cúbica. Dado un punto Q, unimos$Q$ aS entonces el tercer punto de intersección $Q * S$ decimos que es $-Q$. Veamos que efectivamente$Q + (Q * S) = O$, $Q + (Q * S) = O * (Q * (Q * S)) = O * (S) = O$, pues la multiplicidad de la tercera intersección es 2.

La única propiedad que queda por probar es la asociatividad, es decir que dados tres puntos en la cúbica P, Q, R se cumple $(P+Q)+R = P+(Q+R)$, es decir que $O*((P+Q)*R) = O*(P*(Q+R))$ que es equivalente a probar que $O*((O*(P*Q))*R)) = O*(P*(O*(Q*R))$, por lo que es equivalente a probar que $(O*(P*Q)*R) = P*(O*(Q*R))$, es decir que $(P + Q) * R = P * (Q + R)$, es decir tenemos que probar que estos dos puntos son iguales. Recordemos que $P + Q$ se obtiene de la siguiente forma, trazamos la recta que une a P y Q y obtenemos el punto $P * Q$, luego unimos al punto O con $P * Q$ y la intersección de esa recta con la cúbica nos da $P + Q$, luego unimos el punto $P + Q$ con R y obtenemos el tercer punto de intersección con la cúbica que es el punto $(P + Q) * R$. Para obtener $P * (Q + R)$, unimos los puntos Q y R, obtenemos el tercer punto de intersección $Q * R$ lo unimos con O y obtenemos $(Q + R)$ luego unimos P con $(Q + R)$ y obtenemos la intersección de esa recta con la cúbica $P * (Q + R)$. Consideremos la recta que une a P y $Q + R$ y la recta que une a $(P + Q)$ y a R, lo que queremos responder es ¿La intersección de estas dos rectas está en la cúbica? Para responder esta pregunta, consideremos los 9 puntos, $O, P, Q, R, P * Q, P + Q, Q * R, Q + R$ y la intersección de las dos rectas (queremos ver que está en la cúbica). Consideremos las siguientes tres rectas, la recta que une a $P\, y\, Q$, la recta que une a R y a $P + Q$ y la recta que une a O y $Q + R$, llamemos a la unión de estas rectas C_1. Del mismo modo consideremos las siguientes tres rectas, la recta que va de P a $Q + R$, la recta que va de R a Q y la recta que une a O y $P + Q$, llamemos a la unión de estas tres rectas C_2. La multiplicación de tres rectas nos da como resultado una ecuación cúbica cuyo conjunto de soluciones está dado por la unión de las soluciones de cada recta. Entonces tenemos dos curvas degeneradas que contienen a 9 puntos, y la curva original contiene a 8 puntos de los 9 de la intersección de estas dos curvas, entonces por el teorema que demostramos anteriormente se sigue que la curva original contiene al punto 9. Por lo tanto $(P + Q) * R = P * (Q + R)$. Ahora probaremos que el grupo que hemos definido no depende de la elección del punto racional en la curva, es decir que si decidimos escoger como el elemento cero a un punto O' distinto a O

obtenemos un grupo con la misma estructura a la que acabamos de describir. Proponemos la siguiente función

$$\Gamma : P \to P + (O' - O)$$

como un isomorfismo que va desde el grupo G_1 con el elemento cero O al grupo G_2 con el elemento cero O'. Sea S' el tercer punto de intersección de la recta tangente a O' con la cúbica. Sean $P, Q \in G_1$, entonces $\Gamma(P) = \Gamma(P + O) = P + O + (O' - O) = P + O - O = P$ y $\Gamma(Q) = Q + (O' - O)$, por lo que $\Gamma(P) + \Gamma(Q) = P + Q + (O' - O) = P + Q - O$. Por otra parte $\Gamma(P + Q) = P + Q + (O' - O) = P + Q - O$. Por lo tanto $\Gamma(P) + \Gamma(Q) = \Gamma(P + Q)$, por lo que Γ es un morfismo. Sea $P \neq Q$, entonces $P + O' \neq Q + O'$, entonces $P + (O' - O) \neq Q + (O' - O)$, entonces $\Gamma(P) \neq \Gamma(Q)$, por lo que Γ es inyectiva. Sea $P \in G_2$, entonces $P \in G_1$, entonces $\Gamma(P + O) = P + O + (O' - O) = P$, por lo tanto Γ es suprayectiva y por lo tanto Γ es un isomorfismo.
Lo que hemos hecho hasta ahora nos permite reformular el teorema de Mordell, el teorema de Mordell nos dice que podemos obtener todos los puntos de una cúbica a partir de un conjunto finito, trazando rectas con los puntos de ese conjunto finito para obtener nuevos puntos y así sucesivamente. En términos del grupo que hemos definido, lo que nos dice es que el grupo de puntos racionales es finitamente generado. Por lo que obtenemos el siguiente enunciado del teorema de Mordell.

Teorema de Mordell. Si una cúbica plana no singular tiene un punto racional, entonces el grupo de puntos racionales es finitamente generado.
Esta reformulación del teorema nos permitirá utilizar herramientas básicas de la teoría de grupos, por lo que es de bastante utilidad.

1.3 Forma normal de Weierstrass

Probaremos el teorema de Mordell del mismo modo que Mordell lo hizo, utilizando fórmulas explícitas de la operación que describimos para una cúbica. Con el objetivo de hacer estas fórmulas lo más simples que se pueda, es importante recalcar que cualquier cúbica con un punto racional puede ser transformada en una forma especial que se denomina forma de *Weierstrass*. Para ilustrar la teoría general, trabajaremos un ejemplo específico. Restringiremos nuestra atención a las cúbicas que están dadas en la forma de *Weierstrass* que en la forma clásica están dadas en la forma de la siguiente ecuación

$$y^2 = 4x^3 - g_2 x - g_3.$$

Usaremos la ecuación un poco más general

$$y^2 = x^3 + ax^2 + bx + c,$$

y nos referiremos a cualesquiera de estas dos ecuaciones como ecuaciones en la forma de *Weierstrass*. Lo que queremos probar es que cualquier cúbica es biracionalmente equivalente a la forma de *Weierstrass*. A continuación explicaremos lo que equivalencia biracional significa.
Supongamos que tenemos una curva cúbica con un punto racional en el plano proyectivo. Lo que intentamos hacer es escoger los ejes del plano proyectivo de tal forma que la ecuación e la cúbica tenga una forma simple. Denotemos el punto racional en la cúbica como normalmente lo hacemos, consideremos el eje $Z = 0$ como la recta tangente a C en O. Como establecimos anteriormente, la multiplicidad de la intersección de $Z = 0$ y la curva C es de dos, por lo que intersecta a la curva en un punto mas, sea el eje $X = 0$ tangente a la curva en este punto de intersección. Sea $Y = 0$ cualquier recta distinta de $Z = 0$ tal que intersecte a la curva en O. Debido a que asumimos que existe un tercer punto de intersección de $Z = 0$ con la curva, hemos asumido que O no es un punto de inflexión, en caso de que O fuera un punto de inflexión el eje $X = 0$ sería cualquier recta que no contiene a O. Si escogemos los ejes de la forma en que lo hemos establecido y hacemos $x = \frac{X}{Z}$ y $y = \frac{Y}{Z}$, entonces obtenemos condiciones lineales en la ecuación que obtendremos con estas coordenadas. Esto es una transformación proyectiva. Después de la realización de varias cuentas, lo que obtenemos es la siguiente ecuación para C

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

Multiplicamos la ecuación por x,

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

Cambiando xy por y, obtenemos

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

que es $y^2 + (ax+b)y = \textit{cúbica con coeficientes en } x$. Sustituyendo y por $y - \frac{1}{2}(ax+b)$, obtenemos $(y - \frac{1}{2}(ax+b))^2 + (ax+b)(y - \frac{1}{2}(ax+b)) =$ cúbica con coeficientes en x, entonces $y^2 - y(ax+b) + \frac{1}{4}(ax+b)^2 + axy - \frac{ax}{2}(ax+b) + by - \frac{b}{2}(ax+b) =$ cúbica con coeficientes en x, entonces $y^2 - yax - by + \frac{1}{4}(ax+b)^2 + axy - \frac{ax}{2}(ax+b) + by - \frac{b}{2}(ax+b) =$ cúbica con coeficientes en x, entonces $y^2 + \frac{1}{4}(ax+b)^2 - \frac{ax}{2}(ax+b) - \frac{b}{2}(ax+b) =$ cúbica con coeficientes en x, entonces $y^2 + \frac{1}{4}(a^2x^2 + 2bax + b^2) - \frac{a^2x^2}{2} - \frac{axb}{2} - \frac{bax}{2} - \frac{b^2}{2} =$ cúbica con coeficientes en x, entonces

$$y^2 = \text{cúbica con coeficientes en x.}$$

En caso de que el coeficiente principal de la cúbica con coeficientes en x no sea 1, podemos convertirla en una que sí lo tenga, sustituyendo x y y por λx y $\lambda^2 y$, donde λ es el coeficiente principal de la cúbica. Hemos así obtenido una ecuación en la forma de Weierstrass. Y si queremos deshacernos del término x^2 en la cúbica, reemplazando x por $x - \alpha$ con una elección apropiada de α. Rastreando todas las transformaciones desde las coordenadas originales a las nuevas coordenadas, vemos que la transformación no es lineal pero es racional. Por lo tanto, puntos racionales en la curva original corresponden a puntos racionales en la nueva curva. Mostraremos un ejemplo para ilustrar lo que acabamos de asegurar sin demostrar. Supóngase que empezamos con una cúbica de la forma

$$u^3 + v^3 = \alpha,$$

donde α es un número racional dado. La forma homogénea de esta ecuación es $U^3 + V^3 = \alpha W^3$, entonces en el plano proyectivo esta curva contiene el punto racional $[1, -1, 0]$. Aplicando el procedimiento de arriba, obtenemos una nueva forma de expresar las coordenadas x y y en términos de u y v con las funciones racionales

$$x = \frac{12\alpha}{u+v} \qquad y \qquad y = 36\alpha\frac{u-v}{u+v}.$$

que satisfacen la ecuación de Weierstrass

$$y^2 = x^3 - 432\alpha^2.$$

Veamos que efectivamente satisfacen la ecuación

$$(36\alpha(\frac{u-v}{u+v}))^2 - (\frac{12\alpha}{u+v})^3 + 432\alpha^2 = \alpha^2(\frac{1296(u-v)^2}{(u+v)^2} - \alpha(\frac{12}{u+v})^3 + 432) = \alpha^2(\frac{1296(u-v)^2}{(u+v)^2} - \alpha(\frac{1728}{(u+v)^3}) + 432)$$

$$= \frac{\alpha^2}{(u+v)^2}(1296(u-v)^2 - \frac{\alpha(1728)}{(u+v)} + 432(u+v)^2) = \frac{\alpha^2}{(u+v)^2}(\frac{1296(u-v)^2(u+v) - \alpha(1728) + 432(u+v)^3}{(u+v)})$$

$$= \frac{\alpha^2}{(u+v)^2}(\frac{1296((u^2-2uv+v^2)(u+v)) - \alpha(1728) + 432(u+v)^3}{(u+v)})$$

$$= \frac{\alpha^2}{(u+v)^2}(\frac{1296(\alpha - vu^2 - uv^2) - \alpha(1728) + 432(u+v)^3}{(u+v)})$$

$$= \frac{\alpha^2}{(u+v)^2}(\frac{-432\alpha - 1296(vu^2+uv^2) + 432(\alpha + 3uv^2 + 3u^2v)}{(u+v)})$$

$$= \frac{\alpha^2}{(u+v)^2}(\frac{-1296(vu^2+uv^2) + 432(3u^2v + 3uv^2)}{(u+v)}) = 0.$$

Por lo que se satisface la ecuación. El proceso puede invertirse y es posible obtener u y v en términos de x y y.

$$u = \frac{36\alpha + y}{6x} \qquad y \qquad v = \frac{36\alpha - y}{6x}.$$

Entonces si tenemos una solución racional para $u^3 + v^3 = \alpha$, obtenemos racionales x, y que satisfacen la ecuación $y^2 = x^3 - 432\alpha^2$. Y reciprocamente, si tenemos una solución racional de $y^2 = x^3 - 432\alpha^2$, obtenemos números racionales que satisfacen $u^3 + v^3 = \alpha$. Por supuesto, si $u = -v$, el denominador es cero; pero solo existe un número finito de dichas excepciones, y son fáciles de encontrar. Entonces el problema de encontrar puntos racionales en $u^3 + v^3 = \alpha$ es el mismo que encontrar puntos racionales en $y^2 = x^3 - 432\alpha^2$. Y por lo que acabamos de exponer arriba se sigue que se cumple para cualquier cúbica. Por supuesto, la forma normal de Weierstrass tiene una forma distinta a la forma original. Existe una correspondencia biyectiva entre los puntos racionales en una curva y los puntos racionales en otra curva (excepto por una pequeña cantidad de puntos facilmente clasificables). Entonces el problema de estudiar puntos racionales en una ecuación cúbica general con un punto racional se reduce a estudiar los puntos racionales en curvas cúbicas con la forma normal de Weierstrass.
Las transformaciones que usamos para pasar una curva cúbica a su forma normal de Weierstras, no manda rectas en rectas. Lo cual resulta ser un problema debido a que definimos al grupo de los racionales con rectas, por lo que no es claro que al pasar de una curva en su forma general a su forma normal de Weierstras se preserva la estructura del grupo. Lo que veremos, es que, efectivamente el proceso de transformar una ecuación cúbica en una ecuación de Weierstrass es un homomorfismo de grupos. El problema que tenemos con la forma en que describimos la adición de puntos racionales en la curva, parece depender de la forma en que está encajada la curva en el plano. Pero de hecho la regla de adición es una operación intrínseca que puede ser descrita sobre la curva y es invariante bajo transformaciones biracionales. Esto se sigue de propiedades básicas de curvas algebraicas, pero no es tan fácil probar esto únicamente manipulando las ecuaciones de las curvas. Una ecuación en su forma normal, tiene la siguiente forma

$$y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Si suponemos que las raíces complejas de la ecuación son todas distintas, entonces llamamos a la curva una *curva elíptica*. (de manera más general, cualquier curva biracionalmente equivalente a una curva así, es llamada *curva elíptica*).
Resulta natural que el lector se pregunte ¿Por qué se llaman curvas elípticas si no son elipses? La respuesta es que esas curvas surgieron del problema de estudiar cómo calcular la longitud del arco de una elipse. Si se escribe la integral que da como resultado la medida del arco de una elipse y si se realiza una sustitución elemental, el integrando tendrá la raíz cuadrada de un polinomio cúbico o cuártico. Entonces para computar la medida del arco de una elipse, se integra una función que involucra $y = \sqrt{f(x)}$, y la respuesta es dada en términos de ciertas funciones en la curva "elíptica" $y^2 = f(x)$. Ahora consideremos $a, b, c \in \mathbb{Q}$ y coeficientes de $f(x)$, entonces en particular estos números son reales; entonces, el polinomio $f(x)$ de grado 3 tiene por lo menos una raíz real.
En números reales podemos factorizar $f(x)$ de la siguiente forma

$$f(x) = (x - \alpha)(x^2 + \beta x + \gamma) \qquad \text{con } \alpha, \beta, \gamma \text{ reales.}$$

Desde luego, es posible que la función tenga 3 raíces reales. Si solo tiene una raíz real, la curva se ve como algo parecido a la figura anterior, porque $y = 0$ cuando $x = \alpha$. En este caso las raíces reales forman dos componentes. Todo esto es válido, si las raíces de $f(x)$ son distintas. También hemos asumido que nuestra curva cúbica es no singular. Si escribimos la ecuación como $F(x, y) = y^2 - f(x) = 0$ y tomamos las derivadas parciales

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

entonces como por definición la curva es no singular, no existe un punto en la curva en el cual las derivadas parciales se anulen de manera simultánea. Lo que quiere decir que todo punto en la curva tiene una recta tangente en la curva. Esto se puede demostrar de manera sencilla. Si las derivadas parciales se anularan en un punto (x_0, y_0) de la curva entonces $-f'(x_0) = 0$ y $y_0 = 0$ y entonces $F(x_0, y_0) = 0 - f(x_0) = 0$, por lo que $f(x_0) = 0$, se sigue que f y f' tienen una raíz común x_0. Por lo tanto x_0 es una doble raíz de f. De manera inversa, si f tiene una doble raíz

x_0, entonces $(x_0, 0)$ es tal que $F(x_0, 0) = 0 - f(x_0) = 0$, entonces $f(x_0) = 0$, entonces x_0 es un punto singular de la curva, lo cual sería una contradicción a la hipótesis, por lo que f no puede tener dos raíces. Existen dos escenarios posibles para la singularidad, el primer caso se da cuando f tiene una raíz de multiplicidad dos y el segundo cuando f tiene una raíz de multiplicidad 3. Si f tiene una raíz doble, una ecuación típica es

$$y^2 = x^2(x + 1),$$

la curva tiene una singularidad con distintas direcciones tangenciales. Si $f(x)$ tiene una raíz con multiplicidad 3, entonces despues de trasladar x obtenemos la ecuación

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

que es una parábola semicúbica con un pico en el origen. Estos son ejemplos de cúbicas singulares en la forma de Weierstrass, y el caso general se ve igual después de un cambio de coordenadas. Hasta ahora hemos concentrado nuestra atención en las cúbicas no singulares, vale la pena preguntarse por qué. Esto se debe a que las curvas cúbicas singulares y las cúbicas no singulares, tienen un comportamiento totalmente distinto. De hecho, las cúbicas singulares son tan fáciles de tratar como las cónicas. Si proyectamos del punto singular sobre alguna recta, entonces como el punto es de multiplicidad dos (suponiéndolo así) la recta (desde la cual se proyecta) toca a la curva dos veces en el punto singular, por lo que sólo toca a la curva una vez más. Entonces la proyección de la curva sobre una recta es biyectiva. Entonces de manera análoga al caso de la cónica, podemos poner de esta manera en una correspondencia biunívoca los puntos racionales en la cúbica con los puntos racionales en la recta. De hecho, se pueden dar de manera sencilla las fórmulas explícitas de esta correspondencia. Si hacemos $r = \frac{y}{x}$, la ecuación $y^2 = x^2(x + 1)$ se convierte en

$$r^2 = x + 1; \qquad y,\ x = r^2 - 1 \quad y \quad y = r^3 - r.$$

Si tomamos un número racional r y definimos x y y de esta manera, entonces obtenemos un punto racional en la cúbica; y si empezamos con un punto racional (x, y) en la cúbica, entonces obtenemos un punto racional r. Estas asignaciones, son inversas la una de la otra, excepto por el punto singular $(0, 0)$ en la curva. De esta manera obtenemos todos los puntos racionales en la curva. La ecuación $y^2 = x^3$ es aun más simple. Sólo tomamos

$$x = t^2 \quad y \quad y = t^3.$$

Por lo que el análisis de las curvas cúbicas resulta trivial en lo que a puntos racionales se refiere, y el teorema de Mordell no se cumple para estas. De hecho aún no hemos explicado cómo obtener una regla de grupo para estas curvas singulares; pero si quitamos la singularidad, entonces sí se puede obtener un grupo.

1.4 Fórmulas explícitas para el grupo aditivo

Vamos a trabajar en el grupo de puntos de una curva cúbica no singular de una manera más cercana. Empecemos con la ecuación

$$y^2 = x^3 + ax^2 + bx + c$$

hagamos esta ecuación homógenea, haciendo $x = \frac{X}{Z}$ y $y = \frac{Y}{Z}$, obteniendo

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

¿Cuál es la intersección de esta cúbica con la recta con la recta al infinito $Z = 0$? Sustituyendo $Z = 0$ en la ecuación nos da como resultado $X^3 = 0$, que tiene la raíz $X = 0$ con multiplicidad 3. Esto quiere decir que intersecta a la recta al infinito en tres puntos, pero estos tres puntos son los mismos. Por lo que la cúbica sólo tiene un punto en el infinito, el punto dónde las rectas verticales ($x = constante$) se intersectan. El punto en el infinito es un punto de inflexión de la cúbica, y la tangente en ese punto es la la recta al infinito, que se "tocan" en ese punto con multiplicidad 3. Es fácil de verificar que el punto al infinito es un punto no singular, basta con evaluar las derivadas parciales en ese punto. Por lo que para una cúbica en la forma de Weierstrass existe un punto en el infinito;

llamaremos a dicho punto O. El punto O lo consideraremos como un punto racional, y lo consideraremos el elemento nulo cuando le demos la estructura de grupo al conjunto de puntos racionales. Para que lo que hemos establecido funcione, tendremos que hacer la convención de que los puntos en la cúbica consisten de puntos ordinarios en el plano afín ordinario xy junto a otro punto O que no se puede ver.
Bajo estas hipótesis, resulta verdadero que una recta cualquiera intersecta a la cúbica en tres puntos; por ejemplo, la recta al infinito intersecta a la cúbica tres veces en el punto O. Una recta vertical intersecta a la cúbica en dos puntos en el plano afín xy y una vez en el punto O. Una recta no vertical intersecta a la cúbica en tres puntos, por supuesto para que esto suceda, probablemente tengamos que permitir que x y y sean números complejos.
Ahora vamos a discutir un poco más la estructura del grupo ¿Cómo sumamos dos puntos P y Q en una ecuación cúbica con la forma de Weierstrass? Primero trazamos la recta que une a los puntos P y Q y encontramos el tercer punto de intersección $P * Q$. Luego trazamos la recta que une al punto O y el punto $P * Q$, que es la recta vertical que cruza por $P * Q$. Una curva cúbica en la forma de Weirstrass es simétrica respecto al eje x, entonces para encontrar$P + Q$, sólo tomamos $P * Q$ y lo reflejamos respecto al eje x ¿Cuál es el inverso aditivo de un punto Q en la curva? El inverso aditivo de Q se obtiene al reflejarlo; si $Q = (x, y)$, entonces $-Q = (x, -y)$. Para verificar que esto es verdad, supongamos que sumamos el punto Q al punto que denominamos como $-Q$. La recta que une a Q y $-Q$ es vertical, por lo que el tercer punto de intersección es O. Ahora unamos el punto O con el punto O y obtengamos el tercer punto de intersección.
El resultado de unir el punto O con el punto O nos da la recta al infinito, y el tercer punto de intersección es de nuevo O debido a que la recta al infinito intersecta a la curva con multiplicidad 3 en O. Esto prueba que $Q + -Q = O$. Desde luego esta fórmula no sirve para el caso en el que $Q = O$, pero es bastante claro que $O = -O$. Ahora vamos a desarrollar algunas fórmulas que nos permitirán calcular de manera eficiente $P + Q$. Hagamos

$$P_1 = (x_1, y_1),\ P_2 = (x_2, y_{2)},\ P_1 * P_2 = (x_3, y_3),\ P_1 + P_2 = (x_3, -y_3).$$

Asumimos que P_1 y P_2 son puntos dados, y queremos computar $P_1 * P_2$. Primero veamos a la recta que une a los puntos P_1 y P_2. La recta que une a estos puntos está descrita por las ecuaciones

$$y = \lambda x + v,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}\ y\ v = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Por construcción, la recta intersecta a la cúbica en dos puntos P_1 y P_2. ¿Cómo obtenemos el tercer punto de intersección? Sustituimos

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

Despejando obtenemos la siguiente ecuación

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2).$$

Y por construcción, tenemos que esta ecuación cúbica en x tiene tres raíces x_1, x_2, x_3 que son las coordenadas de las tres intersecciones de la recta con la cúbica. Por lo que,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2) = (x - x_1)(x - x_2)(x - x_3).$$

Igualando los coeficientes del término x^2 en ambos lados, encontramos que $\lambda^2 - a = x_1 + x_2 + x_3$, y entonces

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + v.$$

Estas fórmulas otorgan la manera más efectiva de computar la suma de dos puntos. Consideremos la siguiente curva cúbica.

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

que tiene los puntos racionales $P_1 = (-1, 4)$ y $P_2 = (2, 5)$. Para computar $P_1 + P_2$ primero debemos encontrar la recta que une a ambos puntos, $y = \frac{1}{3}x + \frac{13}{3}$, entonces $\lambda = \frac{1}{3}$ y $v = \frac{13}{3}$. Ahora $x_3 = \lambda^2 - x_2 - x_1 = -\frac{8}{9}$ y $y_3 = \lambda x_3 + v = \frac{109}{27}$. Finalmente, encontramos que $P_1 + P_2 = (x_3, -y_3) = (-\frac{8}{9}, -\frac{109}{27})$. Que como vemos los cálculos son bastante sencillos. Las fórmulas que dimos anteriormente involucran la pendiente λ de la recta que conecta a ambos puntos. ¿Qué pasa si ambos puntos son los mismos? Supongamos que tenemos el punto $P_0 = (x_0, y_0)$ y

queremos encontrar el punto $P_0 + P_0 = 2P_0$. Necesitamos encontrar la recta que une a P_0 con P_0. Debido a que $x_1 = x_2$ y $y_1 = y_2$ no podemos utilizar la fórmula para λ. La receta que describimos para añadir un punto consigo mismo dice que la recta que une a P_0 con P_0 es la recta tangente a la cúbica en P_0. De la relación $y^2 = f(x)$ encontramos por la derivada implícita que

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y},$$

así que eso es lo que utilizamos cuando queremos añadir un punto consigo mismo. Continuando con el ejemplo de la curva $y^2 = x^3 + 17$ y el punto $P_1 = (-1, 4)$, computamos $2P_1$ como sigue. Primero, $\lambda = {f'(x_1)}/{2y_1} = {f'(-1)}/{8} = \frac{3}{8}$. Entonces, una vez que tenemos el valor para λ, sólo sustituimos los valores en las fórmulas, como anteriormente lo hicimos, finalmente encontramos que $2P_1 = (\frac{137}{64}, -\frac{2651}{512})$. Algunas veces es conveniente tener una expresión explícita para $2P$ en términos de las coordenadas de P. Si sustituimos $\lambda = {f'(x)}/{2y}$ en las fórmulas que dimos anteriormente, poniendo todo en un denominador común, y remplazando y^2 por $f(x)$, entonces encontramos que

$$\text{coordenada } x \text{ de } 2(x, y) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

La fórmula para $x(2P)$ es usualmente llamada fórmula de duplicación.

CAPÍTULO II
Puntos de orden finito

2.1 Puntos de orden dos y tres

Un elemento P de un grupo cualquiera, se dice que tiene orden m si

$$mP = P + P... + P = O$$

pero $m'P \neq 0$ para cualquier entero m' tal que $1 \leq m' \leq m$. Si existe el m tal que cumpla con las condiciones anteriores, decimos que P tiene orden finito, y si no, decimos que m tiene orden infinito. Iniciaremos el estudio de puntos de orden finito sobre cúbicas, con puntos de orden dos y tres. Como lo hemos hecho anteriormente, consideraremos la curva cúbica no singular está dada en la forma de Weierstrass

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

y donde el punto al infinito O es el cero del grupo geométrico. Queremos encontrar, primero, los puntos de orden dos, es decir los puntos tales que $2P = O$, pero $P \neq O$, pero es más fácil ver cuando sucede que $P = -P$. Como anteriormente vimos que $-(x, y)$ es $(x, -y)$, esto pasa cuando $y = O$

$$P_1 = (\alpha_1, 0), \qquad P_2 = (\alpha_2, 0), \qquad P_3 = (\alpha_3, 0),$$

Donde $\alpha_1, \alpha_2, \alpha_3$ son las raíces del polinomio cúbico $f(x)$. Entonces si permitimos coordenadas complejas, entonces hay exactamente tres puntos de orden dos, debido a que la cúbica es no singular. Veamos como se ve una cúbica con todas las raíces reales. Si tomamos todos los puntos que satisfacen $2P = O$, incluyendo $P = O$, entonces obtenemos el conjunto $\{O, P_1, P_2, P_3\}$. Veamos que el conjunto de soluciones de la ecuación anterior forma un subgrupo de un grupo abeliano G. Sean $P_1, P_2 \in G$ un grupo abeliano, tales que $2P_1 = O$ y $2P_2 = O$. Evidentemente $2O = O$, por lo que el O satisface la ecuación. $2(P_1 - P_2) = 2P_1 - 2P_2 = O - O = O$, por lo que $P_1 - P_2$ satisfacen la ecuación. Observemos que si $2P_2 = O$, entonces $-2P_2 = O$. Por lo que el conjunto de puntos que satisfacen la ecuación $2P = O$ forman un subgrupo. Por lo que tenemos un grupo de orden 4, en el que cada elemento tiene orden 2 o 1, por lo que es evidente que lo que tenemos es el grupo de Klein, esto se sigue del hecho de que el grupo de Klein es el grupo no cíclico más pequeño. Por lo que la suma de dos puntos en el grupo te debe dar el tercero, lo cual tiene sentido pues los tres puntos son colineales. Lo anterior sucede cuando permitimos coordenadas complejas, en caso de admitir únicamente coordenadas reales, tenemos 2 casos.
El caso uno se da cuando tenemos 3 raíces reales, en el cual obtendríamos el grupo de Klein. El caso dos se da cuando tenemos 1 raíz real, caso en el cual tendríamos el grupo cíclico de orden dos. En caso de admitir únicamente coordenadas racionales, entonces obtenemos el grupo de Klein, el grupo cíclico de orden 2, o el grupo trivial, esto debido a que es posible tener 0, 1 o 3 raíces de la curva.
Ahora nos fijamos en los puntos de orden 3. Si en lugar de fijarnos en los puntos que cumplen con la ecuación $3P = O$, nos fijamos en los puntos que cumplen con la ecuación $2P = -P$, entonces un punto de orden 3 satisfacerá $x(2P) = x(-P) = x(P)$. Inversamente, si $P \neq 0$ satisface $x(2P) = x(P)$, entonces$2P = \pm P$ ó $P = O$ ó $3P = O$. Por lo que los puntos de orden 3, son los puntos que satisfacen $x(2P) = x(P)$. Para encontrar los puntos que satisfacen esta condición, usamos la fórmula de duplicación y hacemos la coordenada x de $2P$ igual a la coordenada x de P. En el capítulo I se demostró que la coordenada x de $2P$ es igual a

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Sea C la curva cúbica no singular

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

(Recordemos que C es no singular siempre que $f(x)$ y $f'(x)$ no tengan no tengan raíces complejas comunes). (a) Un punto $P = (x, y) \neq O$ en C tiene orden 2 si y sólo si $y = 0$. (b) C tiene exactamente cuatro puntos cuyo orden divide a 2. Estos cuatro puntos conforman un grupo que es el producto de dos grupos cíclicos de orden dos. (c) Un punto $P = (x, y) \neq O$ en C tiene orden 3 si y sólo si x es una raíz del polinomio

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2).$$

(d) C tiene exactamente nueve puntos cuyo orden divide a 3. Estos nueve puntos conforman un grupo que es el producto de dos grupos cíclicos de orden tres. Demostración. (d) Debido a que la coordenada x de $2P$ es igual a $\frac{f'(x)^2}{4f(x)} - a - 2x$, vemos que una expresión alternativa para ψ_3 es

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2.$$

Afirmamos que $\psi_3(x)$ tiene cuatro raíces distintas complejas. Para verificar esto, tenemos que verificar que $\psi_3(x)$ y $\psi_3'(x)$ no tienen raíces comunes. Pero

$$\psi_3' = 2f(x)f'''(x) = 12f(x);$$

entonces una raíz común de $\psi_3(x)$ y ψ_3'(x) sería una raíz común de

$$2f(x)f''(x) - f'(x)^2 \qquad y \qquad f(x),$$

y también sería una raíz común de $f(x)$ y $f'(x)$. Esto es contrario a nuestra hipótesis de que C es una curva no singular, así concluimos que $\psi_3(x)$ efectivamente tiene cuatro raíces complejas. Sean $\beta_1, \beta_2, \beta_3, \beta_4$ las cuatros raíces complejas de $\psi_3(x)$; y para cada β_i, con $i \in \{1, 2, 3, 4\}$. Sea δ_i una de las raíces cuadradas $\delta_i = \sqrt{f(\beta_i)}$. Entonces de la parte (c) del teorema, el conjunto

$$\{(\beta_1, \pm\delta_1), (\beta_2, \pm\delta_2), (\beta_3, \pm\delta_3), (\beta_4, \delta_4)\}$$

es el conjunto completo de puntos de orden 3 en C. Además, podemos observar que ningún δ_i puede ser cero, pues si así fuera $(\beta_i, \delta_i) = (\beta_i, 0)$ tendría orden dos, contradiciendo el hecho de que tiene orden tres. Por lo tanto, este conjunto contiene exactamente ocho puntos distintos, entonces C tiene ocho puntos de orden 3. El único otro punto cuyo orden divide a 3 es el punto de orden 1, es decir O, que completa la prueba de que C tiene exactamente 9 puntos cuyo orden divide a 3. Finalmente, notamos que sólo existe un grupo (abeliano) con 9 elementos tal que el orden de cada elemento divide a 3, es decir, el producto de dos grupos cíclicos de orden 3. Por lo que ahora sabemos que si permitimos números complejos, entonces los puntos cuyo orden divide a 3 forman un grupo de orden 9 que es el producto directo de dos grupos cíclicos de orden 3. Resulta que los puntos reales de orden 3 siempre forman un grupo cíclico de orden 3, mientras que los puntos racionales o bien forman un grupo cíclico de orden 3 o el grupo trivial.
Existe también una forma geométrica de describir a los puntos de orden 3; son puntos de inflexión, los puntos donde la recta tangente a la curva cúbica tiene multiplicidad tres en la intersección. Podemos ver eso de manera geométrica. Decir que $2P = -P$ quiere decir que cuando trazamos la tangente al punto P, entonces tomamos la tercera intersección y la conectamos con O, obtenemos $-P$. Ahora, ese es el caso en el que el tercer punto de intersección de la recta tangente al punto P es el mismo punto P. Entonces $2P = -P$ si y sólo si P es un punto de inflexión.

2.2 Puntos reales y complejos en curvas cúbicas

Los puntos reales en nuestra curva cúbica

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

forman una o dos componentes, dependiendo de si $f(x)$ tiene una o tres raíces reales. De hecho, la ecuación de la curva cúbica define varios conjuntos de puntos. Podríamos escribir $C(\mathbb{Q})$ para representar al conjunto de puntos con coordenadas racionales, $C(\mathbb{R})$ para los puntos de la figura de arriba tal que sus coordenadas consisten de números

reales arbitrarios, y $C(\mathbb{C})$ para el conjunto de puntos cuyas coordenadas son números complejos. Y el punto O "al infinito", que consideraremos que está en todos estos conjuntos.
Le hemos dado estructura de grupo al conjunto de puntos en la curva. Dado que la construcción es puramente algebraica funcionará para cualquiera de estos tres casos. Los puntos en la curva con coordenadas compleja conforman un grupo. Los puntos con coordenadas reales forman un subgrupo, debido a que si dos puntos tienen coordenadas reales entonces tanto la suma como la diferencia tendrán coordenadas reales. Y debido a que los coeficientes $a, b, c \in \mathbb{Q}$, es cierto incluso que los puntos con coordenadas racionales forman un subgrupo del grupo de puntos con coordenadas reales. Entonces tenemos el grupo de puntos con coordenadas complejas y sus subgrupos ilustrado a continuación

$$\{O\} \subset C(\mathbb{Q}) \subset C(\mathbb{R}) \subset C(\mathbb{C}).$$

Para estudiar el grupo de puntos reales o puntos complejos, se puede utilizar los métodos de análisis. Tomemos $P = (p_1, p_2)$ y $Q = (q_1, q_2)$ en la curva, sea $x = (x_1, x_2)$ y $y = (y_1, y_2)$ tal que x, y tienden a P, Q respectivamente, entonces la recta que une a x y y tiende a la recta que une a P y Q, por lo que $x * y$ tiende a $P * Q$, por lo que $x + y$ tiende a P+Q, debido a la continuidad de la curva, por lo tanto la función es adición es continua. Entonces el grupo de puntos reales es un grupo de Lie de dimensión uno, y este conjunto es de hecho compacto, aunque no lo parezca por tener un punto al infinito. Cualquier grupo de Lie compacto, conexo de dimensión uno es isomorfo al grupo de rotaciones del círculo; que es el grupo multiplicativo de números complejos cuya norma es 1. Entonces si el grupo de puntos reales en la curva es conexo, entonces es isomorfo al grupo del círculo (cíclico). Y de esta descripción podemos ver de manera inmediata como se ven los puntos de orden finito. Si pensamos al grupo del círculo como el grupo multiplicativo de números complejos con norma 1, los puntos cuyo orden divide a m conforman un grupo cíclico de orden m.
Explícitamente, este conjunto de números complejos es

$$\left\{1, \exp^{2\pi i/m}, \exp^{4\pi i/m}, \ldots, \exp^{2(m-1)\pi i/m}\right\}.$$

Entonces los puntos cuyo orden divide a m en $C(\mathbb{R})$ forman un grupo cíclico de orden m, al menos en el caso de que el grupo sea conexo. Si hay dos componentes conexas, entonces el grupo $C(\mathbb{R})$ es el producto directo del grupo del círculo con un grupo de orden dos. En este caso, hay dos posibilidades para los puntos cuyo orden divide a m. Si m es impar, obtenemos de nuevo un grupo cíclico de orden m, mientras si m es par, entonces tendríamos el producto directo de un grupo cíclico de orden dos y un grupo cíclico de orden m. En particular, observamos que los puntos reales cuyo orden divide a 3 siempre forma un grupo cíclico de orden tres. Dado a que hemos visto que hay ocho puntos de orden 3, nunca es posible que todos los puntos complejos de orden tres sean reales, y ciertamente no pueden ser todos números racionales.
En la sección anterior vimos que un punto tiene orden tres si y sólo si el punto es raíz del polinomio $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$. Este polinomio tiene coeficientes reales, por lo que tiene cero, dos o cuatro raíces reales. Debido a que para cada valor de x se obtienen dos posibles valores de y, esto muestra que la curva tiene cero, cuatro u ocho puntos de orden tres con coordenada x real. Antes de continuar con la discusión de puntos racionales, analicemos un poco la estructura de $C(\mathbb{C})$. Sustituyendo $x - \frac{1}{3}a$ por 'x ', podemos eliminar el término ax^2; y luego reemplazando x y y por $4x$ y $4y$ respectivamente, obtenemos la forma clásica de la ecuación de Weirstrass

$$y^2 = 4x^3 - g_2 x - g_3.$$

Como ya se ha mencionado, el polinomio cúbico a la derecha se considera que tiene raíces de multiplicidad igual a uno. En la teoría de Weirstrass de funciones elípticas, siempre que se tienen dos números complejos g_2, g_3 tal que el polinomio $4x^3 - g_2 x - g_3$ tiene raíces distintas, se pueden encontrar números complejos ω_1, ω_2 (llamados períodos) en el plano complejo u al evaluar ciertas integrales definidas. Estos períodos son $\mathbb{R}-$linealmente independientes (no se pueden expresar como combinación lineal de números reales), y se observa el grupo formado por todas las combinaciones lineales de números enteros, es decir

$$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 : \ n_1, n_2 \in \mathbb{Z}\}.$$

Aunque hay muchas opciones que generan a L; se concluye que los coeficientes g_2, g_3 determinan de manera única

el grupo L. Recíprocamente, el grupo L determina de manera única g_2, g_3 por medio de las fórmulas

$$g_2 = 60\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{\omega^4}, \qquad g_3 = 140\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{\omega^6}.$$

Utilizamos los períodos (ω_1, ω_2) para definir una función $\wp(u)$ por las series

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}}(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2}).$$

Esta función meromorfa es llamada la $\wp$ función de Weirstrass. Es claro que tiene polos en los puntos de L, y no otros polos en el plano complejo u. Menos obvio es el hecho que $\wp$ es doblemente periódica; eso quiere decir que

$$\wp(u+\omega_1) = \wp(u) \qquad y \qquad \wp(u+\omega_2) = \wp(u) \qquad \forall\, u \in \mathbb{C}$$

De esto se se obtiene que $\wp(u+\omega) = \wp(u)$ para todo $u \in \mathbb{C}$ y para todo $\omega \in L$. Nótese la similitud con funciones trigonométricas y exponenciales, que solo tienen un periodo: $f(u) = sen(u)$ tiene periodo 2π, y $f(u) = e^u$ tiene periodo $2\pi i$. La función doblemente periódica $\wp(u)$ satisface la ecuación diferencial

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3, \qquad \wp' = \frac{d\wp}{du}.$$

En consecuencia para todo número complejo u obtenemos el punto

$$P(u) = (\wp(u), \wp'(u))$$

sobre la curva dada, en general un punto con coordenadas complejas. Entonces obtenemos una función del plano complejo u a $C(\mathbb{C})$. (Mandamos, los puntos en L, que son los polos de $\wp$, a O). Notemos que esta función, es suprayectivo, no es inyectivo debido a que $\wp$ es doblemente periódica. Si u y v tienen la propiedad que su diferencia $u-v$ es igual a $m_1\omega_1+m_2\omega_2$ para algunos enteros m_1, m_2 (es decir, si la diferencia está en L), entonces $P(u) = P(v)$. Entonces, observamos los valores de u que están en el paralelogramo cuyos lados son los períodos ω_1, ω_2. Entonces es verdad que dado un punto (x, y) sobre la curva existe exactamente un punto u en el paralelogramo, cuyos lados son los períodos ω_1, ω_2, que es enviado a (x, y). En consecuencia, el paralelogramo cuyos lados son los períodos ω_1, ω_2, es enviado de manera biyectiva a los puntos complejos de la curva. La función que envía u a $P(u)$ tiene la propiedad

$$P(u_1 + u_2) = P(u_1) + P(u_2).$$

Donde $u_1 + u_2$ es sólo la adición de números complejos, mientras $P(u_1) + P(u_2)$ es la suma de puntos complejos sobre la curva. Esta ecuación, dice que $\wp$ y $\wp'$ evaluadas en $u_1 + u_2$, puede ser expresado racionalmente en términos de su evaluación en u_1 y u_2 respectivamente. Estas fórmulas son las que dimos anteriormente en el capítulo I, que expresaban $(x_3, -y_3) = P_1 + P_2$ en términos de (x_1, y_1) y (x_2, y_2). La regla de correspondencia dada por $u \to \wp(u)$ es en consecuencia un homomorfismo del grupo aditivo de números complejos sobre el grupo de puntos complejos de la cúbica; el núcleo de ese homomorfismo es L.

El grupo cociente del plano complejo u módulo L es isomorfo al grupo de puntos complejos de nuestra curva, por el primer teorema de isomorfismos y dado que la imagen de la regla de correspondencia es el grupo de puntos complejos en la curva. En consecuencia, el grupo de puntos complejos es un 2-toro, el producto directo de dos grupos circulares. Usando la descripción anterior, podemos describir cómo se ven los puntos complejos de orden finito.

Supóngase que queremos un punto de orden dos. Es decir un punto tal que $u \neq O$ pero $2u = O$, o lo que es equivalente, $u \notin L$ pero $2u \in L$. Hay tres puntos, $\frac{\omega_1}{2}, \frac{\omega_2}{2}$ y $\frac{\omega_1+\omega_2}{2}$. Similarmente, para encontrar los puntos cuyo orden divide a m, buscamos por puntos u en el paralelogramo, cuyos lados son los períodos ω_1 y ω_2, tal que $mu \in L$. Existen 25 puntos de orden 5, claramente los puntos de orden 5 son el producto de dos grupos cíclicos de orden 5. En general, los puntos complejos cuyo orden divide a m forman un grupo de orden m^2 que es el producto directo

de dos grupos cíclicos de orden m. Por lo que tenemos una manera muy clara de describir a los puntos complejos de orden finito en la curva cúbica.
Antes de regresar a los puntos racionales, comentemos qué sucede con otros campos distintos a los reales o a los complejos. Si F es un subcampo cualquiera del campo de los números complejos y si los coeficientes a, b, c de la ecuación cúbica están en F, entonces podemos fijarnos en el conjunto de soluciones (x, y) de la ecuación tal que tanto x como y están en F. Sea $C(F)$ el conjunto que denota a los puntos "F-valuados", junto al punto O. Entonces $C(F)$ forma un subgrupo de $C(\mathbb{C})$; esto es claro por las fórmulas que nos dan las reglas del grupo aditivo. De manera más general, no existe ninguna necesidad de iniciar con el campo de números complejos. Todas las operaciones, como las del grupo aditivo, son puramente algebraicas.
Si, por ejemplo, tomamos F como el campo de enteros módulo p (p primo), y tal que los coeficientes de la cúbica a, b, c están en el campo finito F. Claro que sólo hay un número finito de soluciones, debido a que sólo hay un número finito de posibilidades para x y y. Pero de nuevo estas soluciones, junto el punto al infinito, forman un grupo; con sólo usar las fórmulas del grupo aditivo. Debido a que en este caso el grupo es finito, todos los puntos tienen orden finito; y existen grupos de distintos órdenes. Resulta que los puntos de orden p o bien forman un grupo cíclico de orden p o un grupo trivial; pero si q es un número primo distinto de p, entonces los puntos de orden q forman el grupo trivial ó un grupo cíclico de orden q, o el producto directo de dos grupos cíclicos de orden q.

2.3 El discriminante

Consideremos una curva cúbica en su forma 'normal'

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

donde a, b, c son puntos racionales. Si hacemos $X = d^2x$ y $Y = d^3y$, entonces la ecuación se convierte en $Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c$. Escogiendo un entero 'grande' d, podemos quitar cualquier denominador de a, b o c. De ahora en adelante consideraremos que la ecuación de la curva cúbica tiene coeficientes enteros. El objetivo de este capítulo es probar un teorema, que fue probado primero por Nagell y Lutz, que nos dice cómo encontrar todos los puntos racionales de orden finito. Su teorema dice que todos los puntos racionales de orden finito (x, y) deben tener coordenadas enteras ($x, y \in \mathbb{Z}$), y $y = 0$ para puntos de orden dos ó $y \mid D$, donde D es el discriminante del polinomio $f(x)$. En particular, una curva cúbica sólo tiene un número finito de puntos racionales cuyo orden es finito. El *discriminante* de $f(x)$ está dado por la siguiente fórmula

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

Si factorizamos f en los números complejos,

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

entonces se puede ver que

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2;$$

y como D no se anula podemos inferir que f tiene raíces distintas. En consecuencia, el problema de encontrar los puntos racionales de orden finito puede ser resuelto en un número finito de pasos. Se toma el entero D, se consideran todos los enteros y tales que $y \mid D$. Se toman todos los y con las características anteriores y se sustituye en la ecuación $y^2 = f(x)$. El polinomio $f(x)$ tiene coeficientes enteros y coeficiente principal 1. Si tiene una raíz entera, esa raíz dividirá al término constante.
En consecuencia, sólo hay una cantidad finita de aspectos por revisar, y con este método podremos encontrar todos los puntos de orden finito, en una cantidad finita de pasos. Si $f(x)$ es un polinomio con coeficiente principal 1 en el anillo $\mathbb{Z}[x]$ de polinomios con coeficientes enteros, entonces el discriminante de $f(x)$ siempre estará en el ideal de $\mathbb{Z}[x]$ generado por $f(x)$ y $f'(x)$. Esto se sigue de la teoría general de discriminantes, pero en el caso particular del polinomio $f(x) = x^3 + ax^2 + bx + c$, la prueba más rápida (sin recurrir a la teoría general de discriminantes) es simplemente escribiendo una fórmula explícita, $D = \{(18b - 6a^2)x - (4a^3 - 15ab + 27c)\}f(x) + \{(2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2)\}f'(x)$. Debido a que D está en el ideal generado por $f(x)$ y $f'(x)$, existen polinomios $r(x)$, $s(x)$ con coeficientes enteros tales que

$$D = r(x)f(x) + s(x)f'(x).$$

Si asumimos como verdadera la primera parte del teorema de Nagell-Lutz, es decir que los puntos de orden finito tienen coordenadas enteras, entonces podemos usar la fórmula para demostrar la segunda parte, que o bien $y = 0$ ó $y \mid D$. Es decir, si P tiene orden finito, entonces claramente $2P$ tiene orden finito. Probemos lo siguiente.
Lema. Sea $P = (x, y)$ un punto en la curva cúbica, tal que P y $2P$ tengan coordenadas enteras (cualquier número entero multiplicado por un número entero es un número entero). Entonces $y = 0$ ó $y \mid D$. Prueba. sea $y \neq 0$. Debido a que $y \neq 0$, sabemos que $2P \neq 0$, entonces podemos escribir $2P = (X, Y)$. Por hipótesis, x, y, X, Y son todos enteros. Por la fórmula de duplicación, tenemos que

$$2x + X = \lambda^2 - a, \quad \lambda = \frac{f'(x)}{2y}.$$

Debido a que x, X, y a son todos enteros, entonces se sigue que λ es un entero. Ya que $2y$ y $f'(x)$ son enteros (coeficientes enteros), se obtiene que $2y \mid f'(x)$; y, en particular, $y \mid f'(x)$. Pero $y^2 = f(x)$, entonces también $y \mid f(x)$. Ahora usamos la relación

$$D = r(x)f(x) + s(x)f'(x).$$

Los coeficientes de r y s son enteros, entonces $r(x)$ y $s(x)$ toman valores enteros cuando son evaluados en x un número entero. Se sigue que y divide a D.

2.4 Los puntos de orden finito tienen coordenadas enteras

Se ha llegado a la parte más interesante del teorema de Nagell-Lutz, la prueba de que un punto racional (x, y) de orden finito debe tener coordenadas enteras. Probaremos que x y y son enteros de una manera bastante indirecta. Observemos que una manera de demostrar que un número entero es igual a 1 es demostrando que no es divisible por ningún número primo. En consecuencia podemos descomponer el problema en una infinidad de subproblemas, es decir, vemos que cuando x y y son escritos en primos relativos, no hay dos en los denominadores, no hay 3 en los denominadores, no hay 5 en los denominadores, etcétera.
Sea p un número primo, tratemos de demostrar que p no divide el denominador de x ni el denominador de y. Esto nos conduce a considerar el punto racional (x, y) donde p divide el denominador de x ó y. Va a ser útil establecer alguna notación. Todo número racional distinto de cero podemos escribirlo de manera única en la forma $\frac{m}{n}p^\nu$, donde m, n son primos relativos a p, $n \gneq 0$, y $\frac{m}{n}$ es una fracción irreducible.
Definimos el orden de ese número racional como el número entero ν, y escribimos

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

Decir que p divide a el denominador (respectivamente el numerador) de un número racional es lo mismo que decir que su orden es negativo (respectivamente, positivo). El orden de un número racional es cero si y sólo si no divide al denominador ni al numerador. Veamos al punto racional (x, y) que está en nuestra curva cúbica, dónde p divide al denominador de x, digamos

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

donde $\mu \gneq 0$ y p no divide a m, n, u, w. Evaluamos este punto en la ecuación de la curva cúbica. Poniendo los términos con un denominador común, obtenemos

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

$p \nmid (m^3 + am^2np^\mu + bmn^2p^{2\mu} + cn^3p^{3\mu})$; y por lo tanto

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

En consecuencia, $2\sigma = 3\mu$. En particular, $\sigma \gneq 0$, y entonces p divide al denominador de y. Más aún, la relación $2\sigma = 3\mu$ quiere decir que $2 \mid \mu$ y $3 \mid \sigma$, entonces tenemos $\mu = 2\nu$ y $\sigma = 3\nu$ para algún entero $\nu \gneq 0$. Similarmente, si

asumimos que p divide el denominador de y, encontramos con el mismo cálculo que exactamente el mismo resultado se cumple, es decir, $\mu = 2\nu$ y $\sigma = 3\nu$ para algún entero $\nu \gneq 0$. En consecuencia, si p aparece en el denominador de x o y, entonces está en el denominador de ambos; y en este caso la potencia exacta es $p^{2\nu}$ en x y $p^{3\nu}$ en y para algún entero positivo $\nu \gneq 0$.
Esto sugiere que hagamos la siguiente definición. Consideraremos $C(p^\nu)$ como el conjunto de puntos racionales de la curva cúbica tal que $p^{2\nu}$ divide el denominador de y. En otras palabras,

$$C(p^\nu) == \{(x,y) \in C(\mathbb{C}) \ : \ ord(x) \leq -2\nu \ y \ ord(y) \leq -3\nu\}.$$

Por ejemplo, $C(p)$ es el conjunto donde p está en el denominador de x y y, y entonces hay por lo menos un p^2 en x y un p^3 en y. Obviamente, tenemos las inclusiones

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

Por convención, incluiremos al elemento cero O en cada uno de los $C(p^\nu)$.
Recordemos que nuestro objetivo es mostrar que si (x,y) es un punto de orden finito, entonces x y y son enteros; y nuestra estrategia consiste en mostrar que para cada p primo, los denominadores de x y y no son divisibles por p. Con la notación que introducimos, esto quiere decir que queremos mostrar que un punto de orden finito no puede estar en $C\,(p)$. El primer paso para probar esto, consiste en demostrar que cada uno de los $C(p^v)$ es un subgrupo de $C(\mathbb{Q})$. Primero vamos a cambiar las coordenadas y mover el punto al infinito a un punto finito, es decir le vamos a dar coordenadas finitas. Vamos a hacer

$$t = \frac{x}{y} \quad y \quad s = \frac{1}{y}.$$

Entonces $y^2 = x^3 + ax^2 + bx + c$ se transforma en

$$s = t^3 + at^2 s + bts^2 + cs^3$$

en el plano (t,s). Siempre podemos regresar a las coordenadas originales, debido a que $y = \frac{1}{s} \quad y \quad x = \frac{t}{s}$. En el plano (t,s) tenemos todos los puntos del plano (x,y) excepto los puntos en los que $y = 0$; y el elemento cero O de la curva cúbica está ahora en el origen (0,0) del plano (t,s). Podemos visualizar la situación de la siguiente manera. Tenemos dos formas de ver la curva. Observar la curva en el plano (x,y) nos muestra todo excepto el punto O. El plano (t,s) nos muestra el punto O y todos los puntos excepto los puntos de orden dos. Excepto por O y los puntos de orden dos, existe una correspondencia biunívoca entre los puntos de la curva en el plano (x,y) y los puntos de la curva en el plano (t,s). Más aún, una recta $y = \lambda x + \nu$ en el plano (x,y) le corresponde una recta en el plano (t,s). Es decir, si dividimos $y = \lambda x + \nu$ entre νy, obtenemos

$$\frac{1}{\nu} = \frac{\lambda}{\nu}\frac{x}{y} + \frac{1}{y}, \qquad s = -\frac{\lambda}{\nu}t + \frac{1}{\nu}.$$

En consecuencia, podemos 'sumar' puntos en el plano (t,s) con el mismo procedimiento que en el plano (x,y). Necesitamos encontrar la fórmula explícita de esta suma. Es conveniente mirar a un cierto anillo que denotamos por R o R_p. Este anillo R va a ser el anillo de todos los números racionales que no tienen a un p en el denominador. Nótese que R es un anillo, puesto que si α y β no tienen un p en su denominador, entonces lo mismo es cierto para $\alpha \pm \beta$ y $\alpha\beta$ puesto que si tenemos $\frac{a}{b} + \frac{c}{d} = \frac{da+bc}{bd}$ entonces bd no tiene a p puesto que si lo tuviera $p \mid bd$ y entonces $p \mid b$ ó $p \mid d$ pero como ni el primero ni el segundo término tienen a p entonces p no está en la suma, de igual manera sucede con la resta y el producto.
Otra forma de describir a R es considerarlo como el cero unión todos los números racionales x distintos de cero tales que $ord(x) \geq 0$. El anillo R es un cierto subanillo del campo de números racionales. Es un anillo estupendo en el sentido de que tiene una factorización única; y tiene un único primo, el primo p (recordemos que estamos considerando fracciones irreducibles). Las unidades de R son sólo los números racionales de orden cero, esto es, números con numerador y denominador primos relativos de p. Observemos la divisibilidad de nuestras nuevas coordenadas s, t por potencias de p en particular por puntos en $C(p)$. Sea (x,y) un un punto racional de nuestra curva en el plano (x,y) que está en $C(p^\nu)$, entonces podemos escribir

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

para algún $i \geq 0$. Entonces

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

En consecuencia, nuestro punto (t, s) está en $C(p^\nu)$ si y solo si $t \in p^\nu R$ y $s \in p^{3\nu} R$. Esto dice que p^νdivide el numerador de t y $p^{3\nu}$ divide el numerador de s. Para probar que los $C(p^\nu)$ son subgrupos, tenemos que sumar puntos y mostrar que si una potencia grande de de p divide la coordenada t de dos puntos, entonces la misma potencia de p divide la coordenada t de su suma. Esto es sólo cuestión de escribir las fórmulas. Sean $P_1 = (t_1, s_1)$ y $P_2 = (t_2, s_2)$ dos puntos distintos. Si $t_1 = t_2$, entonces $P_1 = -P_2$, entonces $P_1 + P_2$ está en $C(p^\nu)$. Asumamos ahora que $t_1 \neq t_2$, y sea $s = \alpha t + \beta$ la recta que pasa por los puntos P_1 y P_2. La pendiente α está dada por

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

Podemos reescribir esto como sigue. Los puntos (t_1, s_1) y (t_2, s_2) satisfacen la ecuación

$$s = t^3 + at^2 s + bts^2 + cs^3.$$

Si a la ecuación asociada a P_2 le restamos la ecuación asociada a P_1 y factorizando, obtenemos

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

Algunos de los términos son divisibles por $s_2 - s_1$, y algunos de los términos son divisibles por $t_2 - t_1$. Factorizando estos términos, encontramos la siguiente expresión

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

El punto de todo esto, como podemos ver, es obtener el 1 del denominador de α, para que entonces el denominador de α sea una unidad en R. Similarmente, si $P_1 = P_2$, entonces la pendiente de la recta tangente a C en P_1 es

$$\alpha = \frac{ds}{dt}(P_1) = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2}.$$

Nótese que esta es la misma pendiente que obtenemos si sustituimos $t_1 = t_2$ y $s_1 = s_2$ en el lado derecho de (*). Por lo que usaremos (*) en todos los casos. Sea $P_3 = (t_3, s_3)$ el tercer punto de intersección de la recta $s = \alpha t + \beta$ con la curva. Para obtener la ecuación cuyas raíces son t_1, t_2, t_3, sustituimos $\alpha t + \beta$ por s en la ecuación de la curva

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

de donde obtenemos

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

Esta ecuación tiene raíces t_1, t_2, t_3, por lo que el lado derecho es igual a $constante \cdot (t - t_1)(t - t_2)(t - t_3)$. Comparando los coeficientes de t^3 y t^2, obtenemos que la suma de las raíces es

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

Estas son todas las formulas que necesitaremos excepto por la fórmula trivial

$$\beta = s_1 - \alpha t_1$$

que dice que la recta pasa por P_1. Ahora tenemos una fórmula para t_3, entonces ¿Cómo encontramos $P_1 + P_2$? Trazamos la recta que pasa por (t_3, s_3) y el elemento cero $(0, 0)$ y tomamos el tercer punto de intersección con la

curva. Es evidente de la ecuación de la curva que si (t, s) está en la curva, entonces también está $(-t, -s)$. Entonces el tercer punto de intersección es $(-t_3, -s_3)$.
Vamos a ver con más detenimiento a la expresión de α. El numerador de α está en $p^{2\nu}R$, porque cada uno de los t_1, s_1, t_2, s_2 está en $p^{\nu}R$. Por la misma razón, la cantidad $-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1s_2 + s_1^2)$ está en $p^{2\nu}R$, entonces el denominador de α es una unidad en R. Ahora es claro porqué queríamos el 1 en el denominador. Se sigue que $\alpha \in p^{2\nu}R$. Ahora, debido a que $s_1 \in p^{3\nu}R$ y $\alpha \in p^{2\nu}R$ y $t_1 \in p^{\nu}R$, se sigue de la fórmula $\beta = s_1 - \alpha t_1$ que $\beta \in p^{3\nu}R$. Además, vemos que el denominador $1 + a\alpha + b\alpha^2 + c\alpha^3$ de $t_1 + t_2 + t_3$ es una unidad en R. Viendo a la expresión para $t_1 + t_2 + t_3$ dada arriba, tenemos que

$$t_1 + t_2 + t_3 \in p^{3\nu}R.$$

Debido a que $t_1, t_2 \in p^{\nu}R$, se sigue que $t_3 \in p^{\nu}R$, y también $-t_3 \in p^{\nu}R$.
Esto prueba que si las coordenadas t de P_1y P_2 están en $p^{\nu}R$, se concluye que la coordenada t de $P_1 + P_2$ también está en en$p^{\nu}R$. Además, si la coordenada t de $P = (t, s)$ está en $p^{\nu}R$, entonces es claro que la coordenada t de $-P = (-t, -s)$ también está en $p^{\nu}R$. Esto muestra que $C(p^{\nu})$ es cerrado bajo la operación suma y cada elemento tiene a su inverso aditivo; por lo tanto es un subgrupo de $C(\mathbb{Q})$.
De hecho, hemos probado algo un poco más fuerte. Hemos probado que si $P_1, P_2 \in C(P^{\nu})$, entonces

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\nu}R.$$

Escribimos $t(P)$ para denotar la coordenada t de P; entonces si se da P en coordenadas (x, y) como $(x(P), y(P))$, entonces $t(P) = \frac{x(P)}{y(P)}$.
La última fórmula nos dice más que el hecho de que $C(p^{\nu})$ es un subgrupo. Una manera más clara de escribirlo es

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \qquad \left(mod\, p^{3\nu}R\right).$$

Nótese que $+$ en $P_1 + P_2$ denota la suma en la curva cúbica, mientras que $+$ en $t(P_1) + t(P_2)$ es la suma en R, que es simplemente la suma de números racionales. Entonces la función $P \to t(P)$ es prácticamente un homeomorfismo de $C(p^{\nu})$ al grupo aditivo de números racionales. No define precisamente un homeomorfismo, debido a que $t(P_1 + P_2)$ no es igual a $t(P_1) + t(P_2)$. Sin embargo, lo que sí obtenemos es un homeomorfismo de $C(P^{\nu})$ al grupo cociente ${}^{p^{\nu}R}/_{p^{3\nu}R}$ mandando P a $t(P)$; y el núcleo de este homeomorfismo consiste de todos los puntos P con $t(P) \in p^{3\nu}R$. En consecuencia, el núcleo es únicamente $C\left(p^{3\nu}\right)$, así que finalmente obtenemos un homeomorfismo biyectivo

$$\frac{C(p^{\nu})}{C(p^{3\nu})} \longrightarrow \frac{p^{\nu}R}{p^{3\nu}R},$$

$$P = (x, y) \longmapsto t(P) = \frac{x}{y}.$$

No es muy difícil ver que el grupo cociente $\frac{p^{\nu}R}{p^{3\nu}R}$ es un grupo cíclico de orden $p^{2\nu}$. Se sigue que el grupo cociente ${}^{C(p^{\nu})}/_{C(p^{3\nu})}$es un grupo cíclico de orden p^{σ} para algún $0 \leq \sigma \leq 2\nu$. Resumimos nuestros resultados hasta ahora, en la siguiente proposición.
Proposición. Sea p un primo, R el anillo de números racionales cuyo denominador es primo relativo de p, y sea $C(p^{\nu})$ el conjunto de puntos racionales (x, y) en nuestra curva para los cuales x tiene denominador divisible por $p^{2\nu}$, más el punto O.

(a) $C(p)$ consiste de todos los puntos racionales (x, y) para los cuales el denominador de x o y es divisible por p.

(b) Para todo $\nu \geq 1$, el conjunto $C(p^{\nu})$ es un subgrupo del grupo de puntos racionales $C(\mathbb{Q})$.

(c) la función

$$\frac{C(p^{\nu})}{C(p^{3\nu})} \longmapsto \frac{p^{\nu}R}{p^{3\nu}R}, \qquad P = (x, y) \longmapsto t(P) = \frac{x}{y}$$

es un homeomorfismo biyectivo. (Por convención, mandamos $O \longmapsto 0$).

Corolario. (a) Para todo primo p, el subgrupo $C(p)$ no contiene puntos de orden finito (distinto de O). (b) Sea $P = (x, y) \neq O$ un punto racional de orden finito. Entonces x y y son enteros. **Prueba.** Sea m el orden de P. Debido a que $P \neq O$, sabemos que $m \neq 1$. Tómese cualquier primo p. Queremos mostrar que $P \notin C(p)$. Supóngase lo contrario, que $P \in C(p)$. Llegaremos a una contradicción. El punto $P = (x, y)$ puede estar contenido en un grupo más pequeño $C(p^\nu)$, pero no puede estar contenido en todos los grupos $C(p^\nu)$, debido a que el denominador de x no puede ser divisible por potencias arbitrariamente grandes de p. Por lo que podemos encontrar un $\nu \gneq 0$ tal que $P \in C(p^\nu)$, pero $P \notin C(p^{\nu+1})$. Separamos la prueba en dos casos dependiendo de si m es o no divisible por p. Supongamos primero que $p \nmid m$. La aplicación repetida de la congruencia, nos lleva a

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \quad (mod\, p^{3\nu} R)$$

nos da la fórmula

$$t(mP) \equiv mt(P) \qquad \left(mod\, p^{3\nu} R\right).$$

Debido a que $mP = O$, tenemos que $t(mP) = t(O) = 0$. Por otro lado, debido a que m es primo relativo de p, es una unidad en R. Por lo tanto,

$$0 \equiv t(P) \pmod{p^{3\nu} R}.$$

Esto quiere decir que $P \in C\left(p^{3\nu}\right)$, contradiciendo el hecho de que $P \notin C\left(p^{\nu+1}\right)$. Ahora consideramos el caso en el que $p \mid m$. Este caso es manejado de manera similar. Primero escribimos $m = pn$, y observamos el punto $P' = nP$. Debido a que P tiene orden m, es claro que P' tiene orden p. Además, debido a que $P \in C(p)$ y $C(p)$ es un subgrupo, vemos que $P' \in C(p)$. Como lo hicimos anteriormente, podemos encontrar un $\nu \gneq 0$ tal que $P' \in C(p^\nu)$, pero $P' \notin C(p^{\nu+1})$. Entonces, justo como antes, encontramos

$$0 = t(O) = t(pP') \equiv pt(P') \pmod{p^{3\nu} R}.$$

Esto quiere decir que $t(P') \equiv 0\ (mod\, p^{3\nu-1} R$. Debido a que $3\nu - 1 \geq \nu + 1$, esto contradice el hecho de que $P' \notin C\left(p^{\nu+1}\right)$. Esto completa la parte (a) del corolario. Pero ahora la parte (b) es sencilla, porque si $P = (x, y)$ es un punto de orden finito, sabemos que $P \notin C(p)$ para cualquier primo. Lo cual quiere decir que los denominadores de x y y no son divisibles por ningún primo; por lo tanto, x y y son enteros.

Teorema de Nagell-Lutz. Sea

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

una curva cúbica no singular con coeficientes enteros a, b, c; y sea D el discriminante del polinomio cúbico $f(x)$,

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

Sea $P = (x, y)$ un punto racional de orden finito. Entonces x y y son enteros; $y = 0$, en cuyo caso P tiene orden dos, ó $y \mid D$. Prueba. En la sección 4 mostramos que un punto de orden finito tiene coordenadas enteras. Si P tiene orden dos, entonces $y = 0$, y en cuyo caso habríamos acabado. De otra manera, $2P \neq O$. Pero $2P$ es también un punto de orden finito, entonces también tiene coordenadas enteras. En la sección 3 mostramos que si tanto $P = (x, y)$ y $2P$ tienen coordenadas enteras, entonces y divide a D, lo que completa la prueba del teorema.

CAPÍTULO III
El grupo de puntos racionales

3.1 Función altura

En este capítulo probaremos el teorema de Mordell, que como ya dijimos anteriormente dice que el grupo de puntos racionales sobre una curva cúbica no singular es finitamente generado. Para realizar la demostración del teorema es necesario trabajar con una herramienta llamada *Altura.* En pocas palabras, la altura de un punto racional mide qué tan complicado es el punto desde el punto de vista de la teoría de números. Decimos que la altura de un número racional $x = \frac{m}{n}$,de tal forma que mcd(m,n)=1, es

$$H(x) = H\left(\frac{m}{n}\right) = max\left\{|m|, |n|\right\}$$

La altura de un número racional es un entero positivo. La función altura, como mencionamos tiene como objeto medir la "complejidad" de un número racional, por ejemplo si consideramos los números 1 y $\frac{99999}{100000}$. Ambos números tienen un valor absoluto muy similar, sin embargo el segundo un número es evidentemente más complicado, por lo que queda descartada la posible utilización del valor absoluto para medir la complejidad de un número. A continuación demostraremos una propiedad muy importante de la función altura que hace ver de manera más clara la importancia de esta función.

Propiedad de finitud de la función altura. El conjunto de todos los números racionales cuya altura es menor que un número fijo, es un conjunto finito. Sea C el conjunto de números racionales, tal que si $x \in C$, entonces $x = \frac{m}{n}$ implica que para algún número $z \in \mathbb{Z}$ (en los enteros), $|m| \leq z$ y $|n| \leq z$, y como m y n son números enteros, se sigue que sólo hay una cantidad finita de combinaciones de m y n, por lo que el conjunto C es finito. Si

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

es una curva cúbica no singular con coeficientes enteros a,b,c, y si $P = (x, y)$ es un punto racional sobre la curva, definiremos la función altura de P como la altura de la coordenada x,

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

Veremos que la función altura de algún modo cumple con una propiedad multiplicativa; por ejemplo, compararemos $H(P + Q)$ con el producto $H(P)H(Q)$. Por razones de notación, es a veces más útil utilizar una función que se comporte de manera aditiva, por lo que definiremos la función altura "h minúscula" así

$$h(P) = logH(P).$$

Por lo que $h(P)$ siempre es una función real no negativa. Nótese que los puntos racionales en una curva cúbica no singular C también tienen la propiedad de finitud. Si M es cualquier número positivo, entonces

$$\{P \in C\left(\mathbb{Q}\right) : H(P) \leq M\}$$

es un conjunto finito; y lo mismo sucede si cambiamos $h(P)$ con $H(P)$. Esto es cierto, pues la coordenada x, que es un número racional cumple con la propiedad de finitud y como x está en la curva la coordenada y sólo tiene dos opciones, por lo que este conjunto es efectivamente finito. Lo anterior funciona para los puntos que no están en el infinito. Existe un punto O en el infinito, del cual diremos que su altura es $H\left(O\right) = 1$, o equivalentemente, $h\left(O\right) = 0$**.** Como ya lo mencionamos el objetivo principal es probar que el grupo de puntos racionales de $C\left(\mathbb{Q}\right)$es finitamente generado. A continuación enunciaremos cuatro lemas que nos ayudarán en dicho propósito y posteriormente los demostraremos.

Lema 1. Para todo número real M, el conjunto

$$\{P \in (\mathbb{Q}) : h(P) \leq M\}$$

es finito**.**
Lema 2. Sea P_0un punto racional, fijo en C. Existe una constante k_0,que depende de P_0 y de a,b,c y tal que

$$h(P + P_0) \leq 2h(P) + k_0 \qquad \text{para todo } P \in C(\mathbb{Q}).$$

Lema 3. Existe una constante k, que depende de a,b,c, tal que

$$h(2P) \geq 4h(P) - k \qquad \text{para todo } P \in C(\mathbb{Q}).$$

Lema 4. El índice $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ es finito. Donde $2C(\mathbb{Q})$ denota el subgrupo de $C(\mathbb{Q})$que consiste de los puntos que son el doble de otros puntos. Es claro que $2C(\mathbb{Q})$ es un subgrupo puesto que, si se toma $x, y \in 2C(\mathbb{Q})$ entonces $x - y = 2x_1 - 2y_1 = 2(x_1 - y_1)$, donde $x_1, y_1 \in C(\mathbb{Q})$, por lo que $x - y \in 2C(\mathbb{Q})$ y es claro que $O = 2O$. Para cualquier grupo conmutativo Γ, la función multiplicar por m

$$\Gamma \to \Gamma, \qquad P \to P + ... + P = mP$$

es un homeomorfismo; y la imagen de ese homeomorfismo es un subgrupo $m\Gamma$ de Γ. Lo que nos dice el cuarto lema es que, para $\Gamma = C(\mathbb{Q})$,el subgrupo 2Γ tiene índice finito en Γ. Ahora probaremos como estos cuatro lemas implican que $C(\mathbb{Q})$es un grupo finitamente generado. Supóngase que Γes un grupo conmutativo, y una función altura

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

de Γa los reales positivos. Supóngase ahora que Γ y h satisfacen los cuatro lemas. Reescribiremos las hipótesis para probar el siguiente teorema
Teorema descendente. Sea Γ un grupo conmutativo. Supóngase que existe una función

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

con las siguientes tres propiedades. (a) Para todo $M \in \mathbb{R}$, el conjunto $\{P \in \Gamma : h(P) \leq M\}$es finito.
(b) Para todo $P_0 \in \Gamma$, existe una constante $k_0$tal que

$$h(P + P_0) \leq 2h(P) + k_0 \qquad \text{para todo } P \in \Gamma.$$

(c) Existe una constante k tal que

$$h(2P) \geq 4h(P) - k \qquad \text{para todo } P \in \Gamma.$$

supóngase también que (d) El subgrupo 2Γtiene índice finito en Γ. Entonces Γ es finitamente generado.
Demostración. Tomemos un representante de cada clase lateral de 2Γen Γ. Como el índice de 2Γes finito, entonces existe una cantidad finita de clases laterales, digamos que existen n clases laterales. Sean $Q_1, Q_2, ..., Q_n$ los representantes de las clases laterales. Esto quiere decir que para cualquier elemento $P \in \Gamma$existe un índice i_1, que depende de P, tal que

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

Puesto que las clases laterales de 2Γen Γ forman una partición de Γ, por lo que P está en alguna de las clases laterales de 2Γen Γ. Esto quiere decir que podemos escribir

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

para algún $P_1 \in \Gamma$. Para P_1 podemos hacer lo mismo y así sucesivamente para otros elementos de Γ, por lo que podemos escribir

$$P_1 - Q_{i_2} = 2P_2$$

$$P_2 - Q_{i_3} = 2P_3$$

$$\vdots$$

$$P_{m-1} - Q_{i_m} = 2P_m,$$

donde $Q_{i_1}, ..., Q_{i_m}$son elementos de las clases laterales $Q_1, ..., Q_n$, y $P_1, ..., P_m$ son elementos de Γ y por ende de alguna de las clases laterales. De la primera ecuación deducimos que

$$P = Q_{i_1} + 2P_1.$$

Ahora sustituyendo la segunda ecuación $P_1 = Q_{i_2} + 2P_2$ en esta para obtener

$$P = Q_{i_1} + 2Q_{i_2} + 4P_2.$$

Continuando de esta manera, obtenemos que

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

En particular, esto quiere decir que P está en el subgrupo de Γ generado por los Q_i y P_m. Aplicando la parte (b) del teorema, reemplazando $-Q_i$ en lugar de P_0, entonces obtenemos una constante k_i tal que

$$h\left(P - Q_i\right) \leq 2h(P) + k^{'} \qquad \text{para todo } P \in \Gamma.$$

Hacemos esto para cada Q_i, $1 \leq i \leq n$. i es finito debido a que el índice de 2Γ en Γ es finito, por lo que podemos escoger el más grande de los k_i. Entonces
$h\left(P - Q_i\right) \leq 2h\left(P\right) + k^{'} \qquad \forall\, P \in \Gamma \ y \forall\, 1 \leq i \leq n$. Sea k la constante de (c). Entonces podemos calcular

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

Reescribamos esto así

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

De esto vemos que si $h((P_{j-1}) \geq k^{'} + k$, entonces

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

Por lo que en la secuencia de puntos $P, P_1, P_2, P_3, ...$, mientras el punto P_j satisfaga la condición $h(P_j) \geq k^{'} + k$, entonces el número siguiente cumple que $h(P_{j+1}) \leq \frac{3}{4}h(P_j)$. De donde podemos observar que si proseguimos de esta manera, es decir si seguimos multiplicando por $\frac{3}{4}$ este número se aproxima a cero. Por lo que para un m suficientemente grande, se cumple que $h(P_m) \leq k^{'} + k$. Por lo que ahora podemos escribir cualquier elemento P de Γ de la siguiente forma

$$P = a_1Q_1 + a_2Q_2 + ... + a_nQ_n + 2^m R$$

para ciertos enteros $a_1, ..., a_n$ y algún punto $R \in \Gamma$ que satisface la desigualdad $h(R) \leq k^{'} + k$. Entonces el conjunto

$$\{Q_1, Q_2, ..., Q_n\} \cup \left\{R \in \Gamma \ : \ h(R) \leq k^{'} + k\right\}$$

genera Γ, esto quedó demostrado al expresar P en términos de los elementos del conjuntos. Que por el inciso (a) y (d) obtenemos que estos conjuntos son finitamente generados.

3.2 La altura de $P + P_0$

En esta sección probaremos el lema 2, que nos dará una relación entre las alturas de P, P_o y $P + P_o$. Antes de proceder, haremos un par de observaciones. La primera observación es que si $P = (x, y)$ es un punto racional en la curva, entonces x y y son de la forma

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

Para enteros m, n, e con $e \gneq 0$ y el $mcd(m, e) = mcd(n, e) = 1$. En otras palabras, si se escriben las coordenadas de un punto racional en su mínima expresión, entonces el denominador de x es el cuadrado de un número que elevado al cubo es el denominador de y. En esencia probamos esto en el capítulo 3, debido a que mostramos que si p^ν divide el denominador de x, entonces ν es par y $p^{3\nu/2}$ divide al denominador de y. Sin embargo, debido a que lo que queremos saber es muy fácil de probar, lo probaremos de nuevo de distinta manera. Consideremos que tenemos

$$x = \frac{m}{M} \quad y \quad y = \frac{n}{N}$$

y son fracciones irreducibles con $M \gneq 0$ y $N \gneq 0$. Sustituyendo en la ecuación de la curva, obtenemos

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

quitando los denominadores, obtenemos

$$M^3n^2 = N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3. \qquad (*)$$

Debido a que N^2 es un factor de todos los términos en la derecha, vemos que $N^2 \mid M^3n^2$. Pero $mcd(n, N) = 1$, entonces $N^2 \mid M^3$. Ahora queremos probar lo inverso, eso es, $M^3 \mid N^2$. Esto se hace en tres pasos. Primero, de (*) vemos de manera inmediata que $M \mid N^2m^3$; y debido a que el $mcd(m, M) = 1$, por el lema de Euclides $M \mid N^2$. Usando esto en (*), llegamos a que $M^2 \mid N^2m^3$, entonces $M \mid N$. Finalmente, usando (*) de nuevo, vemos que esto implica que $M^3 \mid N^2m^3$, entonces $M^3 \mid N^2$. Hemos mostrado que $N^2 \mid M^3$ y $M^3 \mid N^2$, entonces $M^3 = N^2$. Ademas, en la prueba mostramos que $M \mid N$. Entonces si hacemos $e = \frac{N}{M}$, entonces encontramos que

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

Por lo tanto $x = \frac{m}{e^2}$ y $y = \frac{n}{e^3}$ tienen la forma deseada. Nuestra segunda observación se refiere a cómo definimos la altura de los puntos racionales en nuestra curva. Si el punto P es dado en fracciones irreducibles $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, entonces la altura de P es el máximo de $\mid m \mid$ y e^2. En particular, $\mid m \mid \leq H(P)$ y $e^2 \leq H(P)$. Aseguramos que también podemos acotar el numerador de y en términos de $H(P)$. Precisamente, existe una constante $K \gneq 0$, que depende de a, b, c, tal que

$$|n| \leq KH\left(P^{3/2}\right).$$

Para probar esto sólo tenemos que utilizar el hecho de que el punto satisface la ecuación. Sustituyendo en la ecuación y multiplicando por e^6 para quitar a los denominadores obtenemos

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

Ahora tomando valores absolutos y utilizando la desigualdad del triángulo.

$$\left|n^2\right| \leq \left|m^3\right| + \left|ae^2m^2\right| + \left|be^4m\right| + \left|ce^6\right|$$

$$\leq H(P)^3 + |a| H(P)^3 + |b| H(P)^3 + |c| H(P)^3.$$

Entonces podemos tomar $K = \sqrt{1 + |a| + |b| + |c|}$. Ahora estamos preparados para probar el lema dos.

Lema 2. Sea P_0 un punto racional fijo en C. Existe una constante k_0, que depende de P_0 y de a, b, c, tal que

$$h(P + P_0) \leq 2h(P) + k_0 \qquad \forall\, P \in C(\mathbb{Q}).$$

Demostración. La prueba consiste básicamente en escribir la fórmula de la suma de dos puntos y en usar la desigualdad del triángulo. Primero observamos que el lema es trivial si $P_0 = O$; podemos considerar $P_0 \neq 0$, digamos que $P_0 = (x_0, y_0)$. Ahora observamos que para probar la existencia de la constante k_0, basta con probar que la desigualdad se cumple para todo P excepto en un conjunto fijo finito. Esto es verdad debido a que, para cualquier número finito de P, sólo observamos las diferencias $h(P + P_0) - 2h(P)$ y tomamos k_0 más grande que el número finito de valores que se producen. Dicho esto, es suficiente con probar el lema 2 para todos los puntos P tales que $P \notin \{P_0, -P_0, O\}$. Escribimos $P = (x, y)$. La razón para evitar P_0 y $-P_0$ es para tener $x \neq x_0$, porque entonces podemos evitar utilizar la fórmula de duplicación. Escribimos

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

Para obtener la altura de $P + P_0$, necesitamos calcular la altura de ξ; entonces necesitamos la fórmula de ξ en términos de (x, y) y (x_0, y_0). La fórmula que dedujimos anteriormente se ve de la siguiente manera

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

Necesitamos desarrollar esto un poco más

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

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

Si desarrollamos todo esto, entonces en el numerador aparece $y^2 - x^3$. Debido a que P está en la curva, la expresión $y^2 - x^3$ puede ser reemplazada por $ax^2 + bx + c$. Por lo que obtenemos la expresión

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

donde A, B, C, D, E, F, G son ciertos números racionales que pueden ser expresados en términos de a, bc, y (x_0, y_0). Además, multiplicando el numerador por el mínimo común denominador de A, B, C, D, E, F, G, podemos suponer que A, B, C, D, E, F, G son todos enteros. En resumen, tenemos enteros A, B, C, D, E, F, G, que dependen únicamente de a, b, c, y (x_0, y_0), de modo que para cualquier punto $P = (x, y) \notin \{P_0 - P_0, O\}$, la coordenada x de $P + P_0$ es igual a

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

El punto importante es que una vez que la curva y el punto P_0 son fijados, entonces esta expresión es correcta para todos los puntos P. Así que está bien que la constante k_0 dependa de A, B, C, D, E, F, G, siempre y cuando no dependa de (x, y). Ahora sustituyendo $x = \frac{m}{e^2}$ y $y = \frac{n}{e^3}$ y quitando los denominadores al multiplicar y el numerador por e^4. Obtenemos

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

y ahora el resultado que deseamos es casi evidente. Nótese que tenemos una expresión para ξ dada por la división de un entero entre un entero. No sabemos si esta expresión es una fracción irreducible, pero la cancelación sólo haría la altura más chica. En consecuencia,

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

Además, de lo anterior tenemos las aproximaciones

$$e \leq H(P)^{1/2}, \qquad n \leq KH(P)^{3/2}, \qquad m \leq H(P),$$

donde K depende únicamente de a, b, c. Usando esto y la desigualdad del triángulo, obtenemos

$$\left|Ane + Bm^2 + Cme^2 + De^4\right| \leq |Ane| + \left|Bm^2\right| + \left|Cme^2\right| + \left|De^4\right|$$

$$\leq (|AK| + |B| + |C| + |D|)\, H(P)^2;$$

y

$$\left|Em^2 + Fme^2 + Ge^4\right| \leq \left|Em^2\right| + \left|Fme^2\right| + \left|Ge^4\right|$$

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

Por lo tanto,

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

Tomando el logaritmo de ambos lados obtenemos

$$h\left(P + P_0\right) \leq 2h(P) + k_0,$$

donde la constante $k_0 = \text{logmax}\left\{|Ak| + |B| + |C| + |D|\,, |E| + |F| + |G|\right\}$ depende únicamente de a, b, c, y (x_0, y_0) y no depende de $P = (x, y)$. Esto completa la prueba del lema dos.

3.3 La altura de $2P$

En la sección anterior probamos que la altura de $P + P_0$ es (esencialmente) menor que el doble de la altura de P. En esta sección queremos probar el lema 3 que dice que la altura de $2P$ es (esencialmente) más grande que cuatro veces la altura de P.

Lema 3. Existe una constante k que depende de a, b, c, tal que

$$h\left(2P\right) \geq 4h\left(P\right) - k \qquad \forall\, P \in C\left(\mathbb{Q}\right).$$

Prueba. Al igual que en la prueba del lema 2, está bien ignorar cualquier conjunto finito de puntos, debido a que siempre podemos tomar k más grande que todos los puntos en el conjunto finito $4h\left(P\right)$. Descartaremos la cantidad finita de puntos que satisface $2P = O$. Sea $P = \left(x, y\right)$, y sea $2P = \left(\xi, \eta\right)$. La fórmula de duplicación que establecimos anteriormente dice que

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

Poniendo todo sobre un denominador común y usando $y^2 = f(x)$, obtenemos una fórmula explícita para ξ en términos de x

$$\xi = \frac{\left(f'(x)\right)^2 - (8x + 4a)\, f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}.$$

Nótese que $f(x) \neq 0$ debido a que $2P \neq O$. En consecuencia, ξ es el cociente de dos polinomios en x con coeficientes enteros. Debido a que la cúbica $y^2 = f(x)$ es no singular por hipótesis, sabemos que $f(x)$ y $f'(x)$ no tienen raíces complejas comunes. Se sigue que los polinomios en el numerador y denominador de ξ tampoco tienen raíces comunes. Debido a que $h\left(P\right) = h\left(x\right)$ y $h\left(2P\right) = h\left(\xi\right)$, estamos tratando de probar que

$$h\left(\xi\right) \geq 4h\left(x\right) - k.$$

En consecuencia, nos vemos obligados a probar el siguiente lema sobre alturas y cocientes de polinomios. Nótese que este lema no tiene nada que ver con curvas cúbicas.

Lema 3'. Sean $\phi\left(X\right)$ y $\psi\left(X\right)$ polinomios con coeficientes enteros y sin raíces complejas comunes. Sea d el máximo de los exponentes de ϕ y ψ. (a) Existe un entero $R \geq 1$, que depende de ϕ y ψ, tal que para cualquier número racional $\frac{m}{n}$,

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

(b) Existen constantes k_1 y k_2 que dependen de ϕ y ψ, tal que para cualquier número racional $\frac{m}{n}$ que no es raíz de ψ,

$$dh\left(\frac{m}{n}\right) - k_1 \leq h\left(\frac{\phi(m/n)}{\psi\left(m/n\right)}\right) \leq dh\left(\frac{m}{n}\right) + k_2.$$

Prueba. (a) Primero observamos que debido a que el grado máximo deϕ y ψ es a lo más d, las cantidades $n^d\phi\left(\frac{m}{n}\right)$ y $n^d\psi\left(\frac{m}{n}\right)$ son ambos números enteros, por lo que tiene sentido hablar de su máximo común divisor. El resultado que estamos tratando de probar es que no se puede cancelar mucho cuando se toma el cociente de estos dos números enteros. Ahora notamos que ϕ y ψ son intercambiables, tomaremos $grad\left(\phi\right) = d$ y el $grad\left(\psi\right) = e \leq d$. Entonces podemos escribir

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + \ldots + a_dn^d,$$

$$n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + \ldots + b_en^d.$$

Para facilitar la notación, haremos

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

Entonces necesitamos encontrar un estimado para $mcd\left(\Phi\left(m,n\right),\Psi\left(m,n\right)\right)$ que no depende de m ni de n. Debido a que $\phi\left(X\right)$ y $\psi\left(X\right)$ no tienen raíces comunes, son primos relativos en el anillo euclideano $\mathbb{Q}\left[X\right]$. En consecuencia, ellos generan el ideal unitario, entonces podemos encontrar polinomios $F\left(X\right)$ y $G\left(X\right)$ con coeficientes racionales, que satisfacen

$$F\left(X\right)\phi\left(X\right) + G\left(X\right)\psi\left(X\right) = 1. \qquad (*)$$

Sea A un entero suficientemente grande tal que $AF\left(X\right)$ y $AG\left(X\right)$ tengan coeficientes enteros. Más aun, Sea D el máximo de los grados de F y G. Nótese que A y D no dependen de m ni n. Ahora evaluemos la igualdad$(*)$ en $X = \frac{m}{n}$ y multiplíquese ambos lados por An^{D+d}. Esto nos da

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

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

$$\left\{n^DAF\left(\frac{m}{n}\right)\right\}\Phi\left(m,n\right) + \left\{n^DAG\left(\frac{m}{n}\right)\right\}\Psi\left(m,n\right) = An^{D+d}.$$

Debido a que los números dentro de las llaves son enteros, vemos que γ divide a An^{D+d}. Esto no es suficiente debido a que necesitamos probar que γ divide a un número fijo que no depende de n. Mostraremos que de hecho γ divide a Aa_0^{D+d}, donde a_0 es el coeficiente principal de $\phi\left(X\right)$. Para probar esto, observamos que como γ divide a $\Phi\left(m,n\right)$, entonces divide a

$$An^{D+d-1}\Phi\left(m,n\right) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \ldots + Aa_dn^{D+2d-1}.$$

Pero en la suma, todo término del primero tiene a An^{D+d} como factor; y como γ divide a An^{D+d}. Como también divide a la suma, se sigue que γ divide al primer término de la suma. En consecuencia, comoγ divide a ambos términos, entonces divide a $mcd\left(An^{D+d}, Aa_0m^dn^{D+d-1}\right)$; y como m y n son primos relativos, concluimos que γ divide a Aa_0n^{D+d-1}. Ahora usando el hecho de que γ divide a $Aa_0n^{D+d-2}\Phi(m,n)$ y repitiendo los pasos de arriba podemos concluir que γ divide a $Aa_0^2n^{D+d-2}$. Siguiendo estos pasos de manera recursiva podemos llegar a concluir que γ divide Aa_0^{D+d}, lo cual prueba el inciso (a). (b) Hay dos desigualdades que probar.
La cota superior es la más fácil; la prueba es similar a la prueba del lema 2. Probaremos la cota inferior. Es válido excluir a un conjunto finito de número racionales cuando se prueba una desigualdad de este tipo; simplemente tenemos que ajustar la constante k_1 para cubrir al número finito de excepciones. Por lo que podemos suponer que el número racional $\frac{m}{n}$ no es una raíz de ϕ. Si r es cualquier número racional distinto de cero, es claro de la definición que $h\left(r\right) = h\left(\frac{1}{r}\right)$. Si es necesario podemos intercambiar los papeles de ϕ y ψ, podemos suponer lo mismo que en

(a), es decir, que ϕ tiene grado d y ψ grado e con $e \leq d$. Continuando con la notación de (a), el número racional cuya altura queremos estimar es

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

Esto nos da una expresión para ξ como cociente de enteros, entonces la altura de $H\left(\xi\right)$ sería el máximo de lo enteros $\left|\Phi\left(m,n\right)\right|$ y $\left|\Psi\left(m,n\right)\right|$ excepto por los casos en los que tengan factores comunes. Probamos en (a) que hay un entero $R \geq 1$, que no depende de m y n, de tal modo que el máximo común divisor de $\Phi\left(m,n\right)$ y $\Psi\left(m,n\right)$ divide a R. Por lo que tenemos que

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

Para el último paso utilizamos el hecho de que el $max\left\{a,b\right\} \geq \frac{1}{2}\left(a+b\right)$. En notación multiplicativa, queremos comparar $H\left(\xi\right)$ con la cantidad $H\left(\frac{m}{n}\right)^d = max\left\{\left|m\right|^d, \left|n\right|^d\right\}$, por lo que consideramos el cociente

$$\frac{H\left(\xi\right)}{H\left(m/n\right)^d} \geq \frac{1}{2R} \cdot \frac{\left(\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right)}{max\left\{\left|m\right|^d, \left|n\right|^d\right\}}$$

$$= \frac{1}{2R} \cdot \frac{\left(\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)}{max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}$$

Esto nos sugiere que nos fijamos en la función p de variable real t definida por

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

Debido a que ϕ tiene grado d y ψ tiene grado a lo más d, vemos que p tiene límite distinto de cero cuando $\left|t\right|$ tiende a infinito. Este límite puede ser $\left|a_0\right|$, si ψ tiene grado menor que d, o $\left|a_0\right| + \left|b_0\right|$, si ψ tiene grado d. Así que afuera de un intervalo cerrado, la función $p\left(t\right)$ está acotada lejos del cero. Pero dentro de un intervalo cerrado, estamos viendo a una función continua que nunca se anula debido a que por suposición $\phi\left(X\right)$ y $\psi\left(X\right)$ no se hacen cero en un mismo punto. Y una función continua alcanza su mínimo y máximo en un conjunto compacto (que un intervalo cerrado cumple en este caso). En particular, debido a que nuestra función nunca es igual a cero, su valor mínimo debe ser positivo. Esto prueba que hay una constante $C_1 \gneq 0$ tal que $p\left(t\right) \gneq C_1$ para todo número real t. Usando este hecho en la desigualdad que llegamos arriba, podemos concluir que

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

Las constantes C_1 y R no dependen de n y m, así que tomando logaritmos obtenemos la desigualdad deseada

$$h\left(\xi\right) \geq dh\left(\frac{m}{n}\right) - k_1$$

con $k_1 = \log\left(2R/C_1\right)$.

3.4 Un homeomorfismo útil

Para completar la prueba del teorema de Mordell, necesitamos probar el lema 4, que dice que el subgrupo $2C(\mathbb{Q})$ tiene índice finito dentro de $C(\mathbb{Q})$. Esta es la parte fina de la prueba del teorema de Mordell. Para facilitar la notación un poco, escribiremos Γ en lugar de $C(\mathbb{Q})$

$$\Gamma = C(\mathbb{Q}).$$

Desafortunadamente, no se conoce una forma de demostrar el lema 4 para toda curva cúbica sin utilizar algo de teoría algebraica de números, y queremos mantenernos en los números racionales. Así que tomaremos la hipótesis extra de que el polinomio $f(x)$ tiene al menos una raíz racional, lo que equivale a asumir que la curva elíptica tiene al menos un punto racional de orden dos. El mismo tipo de prueba sirve en general si se toma la raíz de la ecuación $f(x) = 0$ y nos fijamos en el campo generado por esa raíz sobre los racionales. Por último necesitaremos conocer algunos hechos básicos sobre el grupo unitario y otros tópicos que son preferibles evitar. Así que probaremos el lema 4 en el caso en el que $f(x)$ tenga una raíz racional x_0.
En esta sección desarrollaremos algunas herramientas necesarias para la prueba del lema 4, y en la siguiente sección daremos la prueba, de modo que quedará demostrado el teorema de Mordell. Debido a que $f(x_0) = 0$, y f es un polinomio mónico, podemos concluir que x_0 es un entero. Haciendo un cambio de coordenadas, podemos mover el punto $(x_0, 0)$ al origen. Evidentemente esto no afecta al grupo Γ. La nueva ecuación también tiene coeficientes enteros; con las nuevas coordenadas la curva tendrá la forma

$$C: \ y^2 = f(x) = x^3 + ax^2 + bx,$$

donde a y b son enteros. Entonces

$$T = (0, 0)$$

es un punto racional sobre C que satisface $2T = O$. La fórmula para el discriminante de f dada anteriormente se convierte, en este caso en

$$D = b^2(a^2 - 4b).$$

Siempre asumimos que nuestra curva no es singular, lo que significa que $D \neq 0$, y así $a^2 - 4b$ ni b son cero. Debido a que estamos interesados en el índice $(\Gamma : 2\Gamma)$, o de manera equivalente en el orden del grupo de clases laterales $\Gamma/2\Gamma$, es extremadamente útil notar que la función $P \to 2P$ puede ser partido en dos operaciones más simples. La función de duplicación es en algún sentido de grado 4 debido a que la función racional que da la coordenada x de $2P$ es de grado cuatro en la coordenada x de P. Escribiremos la función $P \to 2P$ como la composición de dos funciones de grado dos, que serán más fácil de manejar de manera individual. Sin embargo, los dos funciones no serán de C a si misma, sino de C a otra curva $\bar{C}$ y luego de nuevo a C. Dicha curva $\bar{C}$ será la dada por la ecuación

$$\bar{C} : Y^2 = x^3 + \bar{a}x^2 + \bar{b}x,$$

donde

$$\bar{a} = -2ay \quad \bar{b} = a^2 - 4b.$$

Por razones que veremos en un momento, estas curvas están íntimamente ligadas; y es natural estudiar C si también se está estudiando $\bar{C}$. Supongamos que aplicamos el anterior procedimiento de nuevo y observamos a

$$\bar{C}' : \ y^2 = x^3 + \bar{a}'x^2 + \bar{b}'x.$$

Tenemos

$$\bar{a'} = -2\bar{a} = 4a \qquad \text{y} \qquad \bar{b}' = \bar{a}^2 - 4\bar{b} = 4a^2 - 4(a^2 - 4b) = 16b,$$

Así que la curva $\bar{C}'$ es la curva $y^2 = x^3 + +4ax^2 + 16bx$. Esto es esencialmente lo mismo que C; solo necesitamos reemplazar y por $8y$ y x por $4x$, y luego dividir la ecuación entre 64. En consecuencia, $\bar{\Gamma}'$ el grupo de puntos racionales de $\bar{C}'$ es isomorfo al grupo de puntos racionales Γ de C. Ahora vamos a definir una función $\phi : \ C \to \bar{C}$ que será homeomorfismo de grupos que mandará a los puntos racionales Γ a los puntos racionales $\bar{\Gamma}$. Y entonces, con el mismo procedimiento, definiremos la función $\psi : \ \bar{C} \to \bar{C}'$. La función $\phi : \ C \to \bar{C}$ es definido en la siguiente

manera. Si $P=(x,y)\in C$, es un punto tal que $x\neq 0$, entonces la regla de correspondencia para $\phi(x,y)=(\bar{x},\bar{y})$ es dado por las fórmulas

$$\bar{x}=x+a+\frac{b}{x}=\frac{y^2}{x^2} \qquad y \qquad \bar{y}=y\left(\frac{x^2-b}{x^2}\right)$$

Para ver que ϕ está bien definida, solo tenemos que revisar que $\bar{x}$ y $\bar{y}$ satisfacen la ecuación de $\bar{C}$

$$\begin{aligned}\bar{x}^3+a\bar{x}^2+\bar{b}\bar{x}&=\bar{x}\left(\bar{x}^2-2a\bar{x}+\left(a^2-4b\right)\right)\\&=\frac{y^2}{x^2}\left(\frac{y^4}{x^4}-2a\frac{y^2}{x^2}+\left(a^2-4b\right)\right)\\&=\frac{y^2}{x^2}\left(\frac{\left(y^2-ax^2\right)^2-4bx^4}{x^4}\right)\\&=\frac{y^2}{x^6}\left(\left(x^3+bx\right)^2-4bx^4\right)\\&=\left(\frac{y\left(x^2-b\right)}{x^2}\right)^2=y\bar{2}.\end{aligned}$$

Esto define la función en todos los puntos excepto en $T=(0,0)$ y O. Para esos puntos definimos

$$\phi(T)=\bar{O}\phi(O)=\bar{O}$$

La razón por la que se recurrió a esta definición de ϕ es para hacer énfasis en el hecho de que todas las propiedades de ϕ pueden ser inferidas con un poco de álgebra elemental y aritmética; no hay necesidad de hacer uso del análisis. Sin embargo, si se desea pensar en términos de puntos complejos y en la 'uniformización' de la curva C por la variable compleja u, entonces x y y son funciones elípticas de u y ϕ puede ser visualizada de manera clara. Lo que se quiere decir es que los puntos complejos en nuestra curva pueden ser representados en el par fundamental de períodos para los períodos adecuados ω_1,ω_2. Si cortamos el paralelogramo definido por el par fundamental de periodos a la mitad por una recta paralela a uno de los lados, obtenemos un nuevo paralelogramo con lados $\bar{\omega}_1$ y $\bar{\omega}_2$, con $\bar{\omega}_1=\frac{1}{2}\omega_1$ y $\bar{\omega}_2=\omega_2$. Este paralelogramo corresponde a la curva $\bar{C}$. Para dividir al paralelogramo tuvimos que escoger un punto de orden dos en C, llamaremos a ese punto T. Hay una función natural de la curva C sobre la curva $\bar{C}$ en el que el punto

$$u=c_1\omega_1+c_2\omega_2 \text{ le asignamos } \bar{u}=c_1\omega_1+c_2\omega_2=2c_1\bar{\omega}_1+c_2\bar{\omega}_2.$$

Si ahora cortamos el paralelogramo de la otra manera, obtenemos $\bar{C}'$ y le corresponde el paralelogramo de lados $\bar{\omega}_1'=\frac{1}{2}\omega_1,\bar{\omega}_2'=\frac{1}{2}\omega_2$. Podemos ver lo anterior desde una perspectiva distinta. Debido a que C es un grupo abeliano y $\{O,T\}$ es un subgrupo de C, podríamos decir que obtenemos a $\bar{C}$ con el grupo cociente $C/\{O,T\}$. Desafortunadamente, no resulta obvio que los elementos de este grupo cociente correspondan a alguna curva elíptica $\bar{C}$. Y aunque supiéramos que el grupo cociente es una curva elíptica, no es obvio que el homeomorfimo natural de C a $\bar{C}$ está dado por funciones racionales. Sin embargo, lo anterior se deduce de teoremas generales de grupos algebraicos. Es incluso verdad que el grupo de puntos en una curva elíptica módulo cualquier subgrupo finito es de nuevo el grupo de puntos de una curva elíptica. Aceptando esto, y sabiendo que cualquier curva elíptica puede ser escrita en la forma de Weirstrass, no es difícil adivinar las fórmulas explícitas que dimos anteriormente. Las dos perspectivas que hemos presentado nos permite ver de manera clara que la función ϕ es un homeomorfismo, pero podemos probar esto de manera directa utilizando fórmulas explícitas. A continuación presentamos la proposición que ilustra lo anteriormente dicho.

Proposición. Sean C y $\bar{C}$ curvas elípticas dadas por las ecuaciones

$$C:\ y^2=x^3+ax^2+bx \quad y \quad \bar{C}:\ y^2=x^3+\bar{a}x^2+\bar{b}x,$$

donde,

$$\bar{a}=-2a \quad y \quad \bar{b}=a^2-4b.$$

Sea $T=(0,0)\in C$. (a) Hay un homeomorfismo $\phi : C\to \bar{C}$ definido por

$$\phi(P)=\begin{cases}\left(\frac{y^2}{x^2},\frac{y\left(x^2-b\right)}{x^2}\right), & si\ P=(x,y)\neq O,T,\\ \bar{O}, & si\ P=O\ o\ P=T.\end{cases}$$

El núcleo de ϕ es $\{O,T\}$. (b) Utilizando el mismo proceso para $\bar{C}$ obtenemos la función $\bar{\phi}:\bar{C}\to\bar{C}'$. La curva $\bar{C}'$ es isomorfa a C por medio de la función $(x,y)\to(x/4,y/8)$. Hay en consecuencia un homeomorfismo $\psi:\bar{C}\to C$ definido por

$$\psi\left(\bar{P}\right)=\begin{cases}\left(\frac{\bar{y}^2}{4\bar{x}^2},\frac{\bar{y}\left(\bar{x}^2-\bar{b}\right)}{8\bar{x}^2}\right), & si\ \overline{P}=(\bar{x},\bar{y})\neq\overline{O},\overline{T},\\ O, & si\ \overline{P}=\overline{O}\ o\ \overline{P}=\overline{T}.\end{cases}$$

La composición $\psi\circ\phi: C\to C$ es multiplicar por dos $\psi\circ\phi(P)=2P$. Prueba. (a) Ya vimos que ϕ manda puntos en C a puntos en $\overline{C}$; y una vez que probemos que ϕ es un homeomorfismo, será obvio que el núcleo de ϕ consiste de O y T. Para probar que ϕ es un homeomorfismo tendríamos que probar muchos casos, solo probaremos algunos casos, casos que bastarán para ilustrar. Tenemos que probar que

$$\phi(P_1+P_2)=\phi(P_1)+\phi(P_2)\qquad \text{para todo } P_1,P_2\in C.$$

En donde la operación de la izquierda es la operación en C y la operación de la derecha la operación en $\overline{C}$. Si P_1 o P_2 es O, no hay nada que probar. Si $P_1=T$ o $P_2=T$, supongamos, $P_1=T$, entonces lo que tenemos que probar es que $\phi(T+P)=\phi(P)$. Esto no es difícil de ver. Utilizando la fórmula explícita para la operación de la suma, es fácil verificar que si $P=(x,y)$, entonces

$$P+T=\left(\frac{b}{x},-\frac{by}{x^2}\right).$$

Escribiendo $P+T=(x(P+T),y(P+T))$ y $\phi(P+T)=(\overline{x}(P+T),\overline{y}(P+T))$, obtenemos

$$\overline{x}(P+T)=\left(\frac{y(P+T)}{x(P+T)}\right)^2=\frac{\left(-by/x^2\right)^2}{\left(b/x\right)^2}=\frac{y^2}{x^2}=\overline{x}(P).$$

De la misma manera calculamos

$$\overline{y}(P+T)=\frac{y(P+T)\left(x(P+T)^2-b\right)}{x(P+T)^2}=\frac{-\frac{by}{x^2}\left(\left(\frac{b}{x}\right)^2-b\right)}{\left(\frac{b}{x}\right)^2}=\overline{y}(P).$$

Esto muestra que $\phi(P+T)=\phi(P)$, excepto en el caso en el que $P=T$. Pero en ese caso tenemos que $\phi(T+T)=\phi(T)+\phi(T)$ debido a que todo vale O. Ahora observamos que ϕ manda negativos en negativos

$$\phi(-P)=\phi(x,-y)=\left(\left(\frac{-y}{x}\right)^2,\frac{-y\left(x^2-b\right)}{x^2}\right)=-\phi(x,y)=-\phi(P).$$

Por lo que para probar que ϕ es un homeomorfismo, ahora basta con mostrar que si $P_1+P_2+P_3=O$, entonces $\phi(P_1)+\phi(P_2)+\phi(P_3)=\overline{O}$; porque una vez que sepamos esto, entonces

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

Además, de lo que ya hemos hecho, podemos asumir que ninguno de los puntos P_1,P_2,P_3 es igual a O o T. De la definición de la operación del grupo aditivo de la curva cúbica, la condición $P_1+P_2+P_3=O$ es equivalente a decir que P_1,P_2 y P_3 son colineales, sea $y=\lambda x+\nu$ la recta que pasa por esos puntos. (si dos o tres puntos coinciden la recta debe ser tangente a la curva). Debemos mostrar que $\phi(P_1)$, $\phi(P_2)$ y $\phi(P_3)$ son la intersección de una recta con $\overline{C}$. Nótese que $\nu\neq O$, porque $\nu=0$ implicaría que la recta $y=\lambda x+\nu$ pasa por T, lo cuál seria una

contradicción con nuestra suposición de que P_1, P_2, P_3 son distintos de T. La recta que intersecta a $\overline{C}$ que tomamos es

$$y = \overline{\lambda}x + \overline{\nu}, \qquad \text{donde } \overline{\lambda} = \frac{\nu\lambda - b}{\nu} \qquad y \qquad \overline{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}.$$

Para comprobar que $\phi(P_1) = \phi(x_1, y_1) = (\overline{x}_1, \overline{y}_1)$ está en la recta $y = \overline{\lambda}x + \overline{\nu}$, solo sustituimos y calculamos

$$\begin{aligned}
\overline{\lambda}\overline{x}_1 + \overline{\nu} &= \frac{\nu\lambda - b}{\nu}\left(\frac{y_1}{x_1}\right)^2 + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} \\
&= \frac{(\nu\lambda - b)\, y_1^2 + \left(\nu^2 - a\nu\lambda + b\lambda^2\right) x_1^2}{\nu x_1^2} \\
&= \frac{\nu\lambda\left(y_1^2 - a x_1^2\right) - b\,(y_1 - \lambda x_1)\,(y_1 + \lambda x_1) + \nu^2 x_1^2}{\nu x_1^2};
\end{aligned}$$

y ahora usando $y_1^2 - a x_1^2 = x_1^3 + b x_1$ y $y_1 - \lambda x_1 = \nu$, obtenemos

$$\begin{aligned}
&= \frac{\lambda\left(x_1^3 + b x_1\right) - b\,(y_1 + \lambda x_1) + \nu x_1^2}{x_1^2} \\
&= \frac{x_1^2\,(\lambda x_1 + \nu) - b y_1}{x_1^2} \\
&= \frac{\left(x_1^2 - b\right) y_1}{x_1^2} = \overline{y}_1.
\end{aligned}$$

El cálculo para $\phi(P_2)$ y $\phi(P_3)$ es exactamente el mismo. Nótese, sin embargo, que no basta con probar que los tres puntos $\phi(P_1), \phi(P_2), \phi(P_3)$ están en la recta $y = \overline{\lambda}x + \nu$. Es suficiente si $\phi(P_1), \phi(P_2), \phi(P_3)$ son distintos; pero en general tenemos que mostrar que $\overline{x}(P_1), \overline{x}(P_2), \overline{x}(P_3)$ son las tres raíces de la ecuación cúbica $\left(\overline{\lambda}x + \overline{\nu}\right)^2 = \overline{f}(x)$, independientemente de si las raíces son distintas. Se puede ver de manera clara que esto se vale si hay múltiples raíces.

Como alternativa, podríamos notar que ϕ es una función continuo de los puntos complejos de C a los puntos complejos en $\overline{C}$; así que una vez que sepamos que ϕ es un homeomorfismo para distintos puntos, obtenemos por continuidad que es un homeomorfismo en general. (b) Notamos arriba que la curva $\overline{C}'$ está dada por la ecuación

$$\overline{C}' \;:\; y^2 = x^3 + 4ax^2 + 16bx,$$

por lo que es claro que la regla de correspondencia $(x, y) \to (x/4, y/8)$ es un isomorfismo de $\overline{C}'$ en C. De (a) tenemos que hay un homeomorfismo $\overline{\phi} : \overline{C} \to \overline{C}'$ definida por las mismas ecuaciones que definen a ϕ, pero con $\overline{a}$ y $\overline{b}$ en lugar de a y b, respectivamente. Debido a que la función $\psi : \overline{C} \to C$ es la composición de $\overline{\phi} : \overline{C} \to \overline{C}'$ con el isomorfismo $\overline{C}' \to C$, obtenemos de manera inmediata que ψ es un homeomorfismo bien definido de $\overline{C}$ a C. Nos queda verificar que $\psi \circ \phi$ es la multiplicación por dos, y esa es otra multiplicación tediosa. Un poco de álgebra con las fórmula que dimos anteriormente nos da como resultado

$$2P = 2(x, y) = \left(\frac{\left(x^2 - b\right)^2}{4y^2}, \frac{\left(x^2 - b\right)\left(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2\right)}{8y^3}\right)$$

Por otro lado, tenemos

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y\left(x^2 - b\right)}{x^2}\right), \qquad \psi(\overline{x}, \overline{y}) = \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}\left(\overline{x}^2 - \overline{b}\right)}{8\overline{x}^2}\right);$$

así que podemos calcular

$$\begin{aligned}\psi\circ\phi\left(x,y\right) &= \psi\left(\frac{y^2}{x^2},\frac{y\left(x^2-b\right)}{x^2}\right)\\ &= \left(\frac{\left(\frac{y\left(x^2-b\right)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2},\frac{\frac{y\left(x^2-b\right)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2-\left(a^2-4b\right)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right)\\ &= \left(\frac{\left(x^2-b\right)^2}{4y^2},\frac{\left(x^2-b\right)\left(y^4-\left(a^2-4b\right)x^4\right)}{8y^3x^2}\right).\end{aligned}$$

Ahora sustituyendo $y^4=x^2\left(x^2+ax+b\right)^2$ y haciendo un poco de álgebra obtenemos el resultado deseado, $\psi\circ\phi\left(x,y\right)=2\left(x,y\right)$. Un cálculo similar nos da $\phi\circ\psi\left(\overline{x},\overline{y}\right)=2\left(\overline{x},\overline{y}\right)$. O podemos argumentar como sigue. Debido a que ϕ es un homeomorfismo, sabemos que

$$\phi\left(2P\right)=\phi\left(P+P\right)=\phi\left(P\right)+\phi\left(P\right)=2\phi\left(P\right).$$

Acabamos de probar que $2P=\psi\circ\phi\left(P\right)$, así que obtenemos que $\phi\circ\psi\left(\phi\left(P\right)\right)=2\left(\phi\left(P\right)\right)$. Ahora, $\phi\ :\ C\to\overline{C}$ es una función suprayectiva de puntos complejos, así que para cualquier $\overline{P}\in\overline{C}$ podemos encontrar $P\in C$ con $\phi\left(P\right)=\overline{P}$. Entonces $\phi\circ\psi\left(\overline{P}\right)=2\overline{P}$. Desde luego, solo hemos probado que $\psi\circ\phi=2$ para puntos con $x\neq0$ y $y\neq0$ porque las fórmulas que utilizamos arriba no son válidas si x o y es cero. Así que en realidad deberíamos verificar que $\psi\circ\phi\left(P\right)=O$ en los casos en que P sea un punto de orden dos. Pero de nueva cuenta podemos argumentar que por continuidad lo anterior se debe de cumplir.

3.5 Teorema de Mordell

En esta sección completaremos la demostración del teorema de Mordell. Continuaremos con la notación de la sección anterior, recordemos que tenemos dos curvas

$$C\ :\ y^2=x^3+ax^2+bx\quad y\quad \overline{C}\ :\ y^2=x^3+\overline{a}x^2+\overline{b}x,$$

donde $\overline{a}=-2a$ y $\overline{b}=a^2-4b$; y tenemos homeomorfismos

$$\phi\ :\ C\to\overline{C}\qquad y\qquad \psi\ :\ \overline{C}\to C$$

tal que las composiciones $\phi\circ\psi\ :\ \overline{C}\to\overline{C}$ y $\psi\circ\phi\ :\ C\to C$ son la multiplicación por 2. Además, el núcleo de ϕ consiste en los dos puntos O y $T=(0,0)$; y el núcleo de ψ consiste de $\overline{O}$ y $\overline{T}=(0,0)$. Sin duda resulta de gran interés estudiar las imágenes de los puntos complejos bajo ϕ yψ, pero por ahora nos concentraremos en los puntos racionales. Es claro de las fórmulas que ϕ manda inyectivamente los puntos de Γ en puntos de $\overline{\Gamma}$; pero no es claro si un punto racional en $\overline{\Gamma}$ proviene de un punto racional en Γ. Si evaluamos los puntos racionales de Γ con ϕ, obtenemos un subgrupo del conjunto de puntos racionales $\overline{\Gamma}$; denotamos este subgrupo $\phi\left(\Gamma\right)$ y lo llamamos la imagen de Γ bajo ϕ. Hacemos las siguientes tres aseveraciones, que combinadas nos dan una buena descripción de la imagen.

$$(i)\,\overline{O}\in\phi\left(\Gamma\right).$$

$$(ii)\,\overline{T}=(0,0)\in\phi\left(\Gamma\right)\text{ si y solo si }\overline{b}=a^2-4b\text{ es un cuadrado perfecto}$$

(iii) Sea $\overline{P}=(\overline{x},\overline{y})\in\overline{\Gamma}$ con $\overline{x}\neq0$. Entonces $\overline{P}\in\phi\left(\Gamma\right)$ si y solo si $\overline{x}$ es el cuadrado de un número racional. El enunciado (i) es trivial, debido a que $\overline{O}=\phi\left(O\right)$. Verifiquemos el enunciado (ii). De la fórmula de ϕ vemos que $\overline{T}\in\phi\left(\Gamma\right)$ si y solo hay un punto racional $(x,y)\in\Gamma$ tal que $\frac{y^2}{x^2}=0$. Nótese que $x\neq0$, debido a que $x=0$ quiere decir que $(x,y)=T$, y $\phi\left(T\right)$ es $\overline{O}$, no $\overline{T}$. Tenemos que $\overline{T}\in\phi\left(\Gamma\right)$ si y solo si hay un punto racional $(x,y)\in\Gamma$ con $x\neq0$ y $y=0$. Poniendo $y=0$ en la ecuación para Γ obtenemos

$$0=x^3+ax^2+bx=x\left(x^2+ax+b\right).$$

Esta ecuación tiene una raíz racional distinta de cero si y solo si la ecuación cuadrática $x^2 + ax + b$ tiene una raíz racional, lo que sucede si y solo si su discriminante $a^2 - 4b$ es un cuadrado perfecto. Esto prueba el enunciado (ii). Ahora verificamos el enunciado (iii). Si $(\overline{x}, \overline{y}) \in \phi(\Gamma)$ es un punto tal que $\overline{x} \neq 0$, la fórmula que define a ϕ muestra que $\overline{x} = {}^{y^2}/_{x^2}$ es el cuadrado de un número racional. Supongamos inversamente que $\overline{x} = w^2$ para algún número racional w. Queremos encontrar un punto racional en C que sea mapeado a $(\overline{x}, \overline{y})$. El homeomorfismo ϕ tiene dos elementos en su núcleo, O y T. En consecuencia si $(\overline{x}, \overline{y})$ está en $\phi(\Gamma)$, habrán dos puntos que van a él. Sea

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right), \qquad y_1 = x_1 w;$$

$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\overline{y}}{w}\right), \qquad y_2 = -x_2 w.$$

Aseguramos que los puntos $P_i = (x_i, y_i)$ están en C y que $\phi(P_i) = (\overline{x}, \overline{y})$ para $i = 1, 2$. Debido a que P_1 y P_2 son claramente puntos racionales, esto probará que $(\overline{x}, \overline{y}) \in \phi(\Gamma)$. La manera más eficiente para verificar que P_1 y P_2 están en C es haciéndolo de manera simultánea. Primero calculamos

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\left(\left(w^2 - a\right)^2 - \frac{\overline{y}}{w^2}\right) \\ &= \frac{1}{4}\left(\left(\overline{x} - a\right)^2 - \frac{\overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \\ &= b. \end{aligned}$$

La última recta se sigue del hecho de que $\overline{y}^2 = \overline{x}^3 - 2a\overline{x}^2 + \left(a^2 - 4b\right)\overline{x}$. Para mostrar que $P_i(x_i, y_i)$ está en C debemos mostrar que

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}.$$

Debido a que ya probamos que $b = x_1 x_2$, y debido a que de nuestra definición de y_1 y y_2 tenemos que ${}^{y_i}/_{x_i} = \pm w$, esto es lo mismo que probar que

$$w^2 = x_1 + a + x_2.$$

Esta última igualdad resulta obvia de la definición de x_1 y x_2. Nos queda verificar que $\phi(P_i) = (\overline{x}, \overline{y})$, así que tenemos que mostrar que

$$\frac{y_i^2}{x_i^2} = \overline{x} \qquad y \qquad \frac{y_i\left(x_i^2 - b\right)}{x_i^2} = \overline{y}.$$

La primera igualdad es verdadera debido a que $y_i = \pm x_i w$ y $\overline{x} = x^2$. Para probar la segunda igualdad, usamos que $b = x_1 x_2$ y la definición de y_i para calcular

$$\frac{y_1\left(x_1^2 - b\right)}{x_1^2} = \frac{x_1 w\left(x_1^2 - x_1 x_2\right)}{x_1^2} = w\left(x_1 - x_2\right) \qquad y$$

$$\frac{y_2\left(x_2^2 - b\right)}{x_2^2} = \frac{-x_2 w\left(x_2^2 - x_1 x_2\right)}{x_2^2} = w\left(x_1 - x_2\right).$$

Nos queda verificar que $w(x_1 - x_2) = \overline{y}$, lo cual se deduce trivialmente a partir de la definición de x_1 y x_2. Esto completa la prueba del enunciado (iii). Recordemos que nuestro objetivo es probar el lema 4, el cual dice que el subgrupo 2Γ tiene índice finito dentro de Γ. En breve veremos que esto se puede deducir si podemos probar que el índice $\left(\overline{\Gamma} : \phi(\Gamma)\right)$ es finito y que también el índice $\left(\Gamma : \psi\left(\overline{\Gamma}\right)\right)$ es finito. De hecho, ahora mostraremos que $\left(\overline{\Gamma} : \phi(\Gamma)\right) \leq 2^{s+1}$, donde s es el número de distintos factores primos de $\overline{b} = a^2 - 4b$, y también que $\left(\Gamma : \psi\left(\overline{\Gamma}\right)\right) \leq 2^{r+1}$, donde r es el número de distintos factores primos de b. Basta con probar solo uno de estos enunciados, así

que solo probaremos el segundo. De los enunciados (i), (ii), y (iii), sabemos que $\psi\left(\overline{\Gamma}\right)$ es el conjunto de puntos $(x,y) \in \Gamma$ tal que x es el cuadrado de un número racional distinto de cero, junto al O, y también T si b es un cuadrado perfecto. La idea de la prueba es encontrar un homeomorfismo biyectivo del grupo cociente ${}^{\Gamma}/_{\psi(\overline{\Gamma})}$ a un grupo finito. Sea $\mathbb{Q}^*$el grupo de números racionales distintos de cero bajo la operación de la multiplicación, y sea $\mathbb{Q}^{*2}$ el subgrupo de cuadrados de elementos de $\mathbb{Q}^*$

$$\mathbb{Q}^{*2} = \left\{u^2 \ : \ u \in \mathbb{Q}^*\right\}.$$

Introducimos una función α de Γ a ${}^{\mathbb{Q}^*}/_{\mathbb{Q}^{*2}}$ definido por

$$\alpha(O) = 1 \qquad \left(\text{mod } \mathbb{Q}^{*2}\right),$$

$$\alpha(T) = b \qquad \left(\text{mod } \mathbb{Q}^{*2}\right),$$

$$\alpha(x,y) = x \ \left(\text{mod } \mathbb{Q}^{*2}\right) \text{ si } x \neq 0.$$

Proposición.
(a) La función $\alpha \ : \ \Gamma \to {}^{\mathbb{Q}^*}/_{\mathbb{Q}^{*2}}$ descrito arriba es un homeomorfismo.
(b) El núcleo de α es la imagen $\psi\left(\overline{\Gamma}\right)$. Por lo tanto α induce un homeorfismo biyectivo

$$\frac{\Gamma}{\psi\left(\overline{\Gamma}\right)} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

(c) Sean $p_1, p_2, \ldots, p_t$ los distintos primos que dividen a b. Entonces la imagen de α está contenida en el subgrupo de ${}^{\mathbb{Q}^*}/_{\mathbb{Q}^{*2}}$ que consta de los elementos

$$\left\{\pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \ : \ \text{cada } \varepsilon_i \text{ es igual a } 0 \text{ o } 1\right\}.$$

(d) El índice $\left(\Gamma \ : \ \psi\left(\overline{\Gamma}\right)\right)$ es a lo más 2^{t+1}. Prueba. (a) Primero observemos que α envía inversos a inversos, porque

$$\alpha(-P) = \alpha(x,-y) = x \equiv \frac{1}{x} = \alpha(x,y)^{-1} = \alpha(P)^{-1} \left(\text{mod } \mathbb{Q}^{*2}\right).$$

Por lo tanto, con el fin de demostrar que α es un homeomorfismo, es suficiente con mostrar que siempre que $P_1 + P_2 + P_3 = O$, entonces $\alpha(P_1)\,\alpha(P_2)\,\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$. Los puntos de orden 3 consisten de la intersección de la curva con una recta. Si la recta es $y = \lambda x + \nu$ y las coordenadas de las primeras entradas de las intersecciones son x_1, x_2, x_3, vimos anteriormente que x_1, x_2, x_3 son raíces de la ecuación

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

Esto es para la ecuación cúbica $y^2 = x^3 + ax^2 + bx + c$. En consecuencia,

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

$$x_1x_2 + x_2x_3 + x_1x_3 = b - 2\lambda\nu,$$

$$x_1x_2x_3 = \nu^2 - c.$$

La última ecuación es la que queremos. Estamos viendo una curva con $c = 0$, así que obtenemos que

$$x_1x_2x_3 = \nu^2 \in \mathbb{Q}^{*2}.$$

Por lo tanto

$$\alpha(P_1)\,\alpha(P_2)\,\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \qquad \left(\text{mod } \mathbb{Q}^{*2}\right).$$

Esto completa la prueba para los casos en los que P_1, P_2, P_3 son distintos de O y T. Los otros casos se deducen fácilmente. (b) Comparando la definición de α con la descripción de $\psi\left(\overline{\Gamma}\right)$ dada en los enunciados (i), (ii), y (iii),

es claro que el núcleo de α es precisamente $\psi\left(\overline{\Gamma}\right)$. (c) Queremos saber qué números racionales x pueden haber en la coordenada x de un punto en Γ. Sabemos que tales puntos tienen coordenadas de la forma $x = {}^{m}/_{e^2}$ y $y = {}^{n}/_{e^3}$. Sustituyendo en la ecuación y quitando denominadores obtenemos

$$n^2 = m^3 + am^2e^2 + bme^4 = m\left(m^2 + ame^2 + be^4\right).$$

En esta ecuación se encuentra la clave. Expresa el cuadrado n^2 como el producto de dos número enteros. Si m y $m^2 + ame^2 + be^4$ son primos relativos, entonces cada uno de ellos serían más o menos un cuadrado, y entonces $x = {}^{m}/_{e^2}$ sería más o menos el cuadrado de un número racional. En el caso general, sea

$$d = \operatorname{mcd}\left(m, m^2 + ame^2 + be^4\right).$$

Entonces d divide a m y be^4. Pero m y e son primos relativos, debido a que asumimos que x fue escrito con el denominador y numerador primos relativos. Por lo tanto, d divide a b. Debido a que también $n^2 = m\left(m^2 + +ame^2 + be^4\right)$, deducimos que todo primo que divide a m se parece a una potencia par excepto posiblemente para los primos que dividen a b. Por lo tanto,

$$m = \pm\left(\text{entero}\right)^2 \cdot p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t},$$

donde cada ε_i es 0 o bien 1, y $p_{1,\ldots,}p_t$ son primos distintos que dividen a b. Esto prueba que

$$\alpha\left(P\right) = x = \frac{m}{e^2} \equiv \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \qquad \left(\operatorname{mod} \mathbb{Q}^{*2}\right);$$

y entonces la imagen de α está contenida en el conjunto indicado. Si $x = 0$, y por lo tanto $m = 0$, nuestro argumento sería inválido. Pero entonces la definición $\alpha\left(T\right) = b\ \left(\operatorname{mod} \mathbb{Q}^{*2}\right)$ muestra que la conclusión sigue siendo válida porque considerando cuadrados, b puede ser escrita en la forma indicada. (d) El subgrupo descrito en (c) tiene precisamente 2^{t+1} elementos. Por otro lado, (b) dice que el grupo cociente ${}^{\Gamma}/_{\psi(\overline{\Gamma})}$ es enviado de manera biyectiva en este subgrupo. Por lo tanto, el índice de $\psi\left(\Gamma\right)$ dentro de Γ es a lo más 2^{t+1}. Finalmente podemos proceder a probar el lema 4

Lema. Sean A y B grupos abelianos, y considérense dos homeomorfismos $\phi\ :\ A \to B$ y $\psi\ :\ B \to A$. Supóngase que

$$\psi \circ \phi\left(a\right) = 2a \qquad \forall\, a \in A \qquad y \qquad \phi \circ \psi\left(b\right) = 2b \qquad \forall\, b \in B.$$

Supóngase que $\phi\left(A\right)$ tiene índice finito en B, y $\psi\left(B\right)$ tiene índice finito en A. Entonces $2A$ tiene índice finito en A. Más precisamente, el índice satisface

$$\left(A\ :\ 2A\right) \leq \left(A\ :\ \psi\left(B\right)\right)\left(B\ :\ \phi\left(A\right)\right).$$

Prueba. Debido a que $\psi\left(B\right)$ tiene índice finito en A, podemos encontrar elementos $a_1, \ldots, a_n$ representativos de todas las clases laterales (tenemos una cantidad finita de clases laterales). Similarmente, debido a que $\phi\left(A\right)$ tiene índice finito en B, podemos encontrar $b_1, \ldots, b_m$ representantes de las distintas m clases laterales, para algún $m \in \mathbb{N}$. Aseguramos que el conjunto

$$\left\{a_i + \psi\left(b_j\right)\ :\ 1 \leq i \leq n,\ 1 \leq j \leq m\right\}$$

incluye un conjunto completo de representantes para las clases laterales de $2A$ dentro de A. Para ver esto, sea $a \in A$. Necesitamos mostrar que a puede ser escrito como la suma de un elemento de este conjunto con un elemento de $2A$. Debido a que $a_1, \ldots, a_n$ son representantes de las clases laterales de $\psi\left(B\right)$ dentro de A, podemos encontrar un a_i de tal modo que $a - a_i \in \psi\left(B\right)$, digamos $a - a_i = \psi\left(b\right)$. Ahora, debido a que $b_1, \ldots, b_m$ son representantes de las clases laterales de $\phi\left(A\right)$ dentro de B, podemos encontrar un b_j tal que $b - b_j \in \phi\left(A\right)$, digamos $b - b_j = \phi\left(a'\right)$. Entonces

$$\begin{aligned} a &= a_i + \psi\left(b\right) = a_i + \psi\left(b_j + \phi\left(a'\right)\right) \\ &= a_i + \psi\left(b_j\right) + \psi\left(\phi\left(a'\right)\right) = a_i + \psi\left(b_j\right) + 2a'. \end{aligned}$$

Hemos ya probado el teorema deseado.

Teorema de Mordell (para curvas con puntos racionales de orden dos) Sea C una curva cúbica no singular dada por la ecuación

$$C\ :\ y^2 = x^3 + ax^2 + bx,$$

donde a y b son enteros. Entonces el grupo de puntos racionales $C(\mathbb{Q})$ es un grupo abeliano finitamente generado.
Prueba. Vimos en la sección 1 que los lemas 1,2,3 y 4 implican que $C(\mathbb{Q})$ es finitamente generado.

Bibliografía

Fulton, W., *Algebraic Curves*, Benjamin, 1969.
Joseph H. Silverman, John Tate, *Rational Points on Eliptic Curves*, Springer Verlag.
Reid, M., *Undergraduate Algebraic Geometry*, London math. Soc. Student texts 12, Cambridge University Press, Cambridge, 1988.
Brieskorn, E., Knörrer, H., *Plane Algebraic Curves*, transl. by J. Stillwell, Birkhäuser, Basel, 1986.
Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009.