El teorema de Nagell-Lutz

Pablo Cano Wall

El teorema de Nagell-Lutz

Pablo Cano Wall

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

Tutorizada por

Prof. José María Tornero Sánchez

Agradecimientos

A José María, mi tutor, por el tiempo que ha dedicado a mejorar y enriquecer este trabajo y por la empatía y paciencia que ha mostrado en todo momento.

A Marta, por no soltar nunca mi mano y estar siempre conmigo.

A mi hermano y a mi madre, que siempre han creído en mí, me han apoyado en cualquier proyecto que tuviera entre manos y gracias a ellos soy la persona que soy. Sin ellos nada hubiera sido posible.

Y especialmente a ti, papá. No te imaginas cuánto te echo de menos. Te quiero.

Índice general

English Abstract

The goal of this memory is to prove the Nagell-Lutz theorem, an important theorem about the rational torsion of elliptic curves, which gives us a necessary condition for a point to have finite order. To do this, we will start by studying the geometry of elliptic curves, how to endow them with an abelian group structure, the group formulas and some birational transformations that put the elliptic curve into the so-called Weierstrass normal form.

Given an elliptic curve in Weierstrass normal form, we will show that if a point has finite order, then its coordinates must be integers, and we will summarize all the work in the proof of the theorem.

Introducción

Las curvas cúbicas son un tipo de curvas algebraicas muy interesantes. Siendo precisos, son particularmente interesantes cuando la curva cúbica es no singular, ya que actualmente no entendemos este tipo de curvas tan bien como nos gustaría y hay importantes problemas abiertos, entre ellos uno de los Problemas del Milenio (la Conjetura de Birch y Swinnerton–Dyer). Estas curvas se denominan curvas elípticas y son el objeto principal de este trabajo.

Definiremos este tipo de curvas en el espacio proyectivo, pero nuestro interés estará en la carta afín, donde nuestra curva se define por una ecuación del tipo $y^2 = f(x)$ siendo $f(x)$ un polinomio de grado 3. Ahora, es muy natural preguntarse de dónde proviene este nombre, ya que estas curvas ciertamente no son elipses. La respuesta es que estas curvas surgieron al estudiar el problema de cómo calcular la longitud del arco de una elipse. Si se escribe la integral que da la longitud del arco de una elipse y se hace una sustitución elemental, el integrando involucrará la raíz cuadrada de un polinomio cúbico o cuártico. Entonces, para calcular la longitud del arco de una elipse, se integra una función que involucra $y = \sqrt{f(x)}$, y la respuesta se da en términos de ciertas funciones en la curva elíptica $y^2 = f(x)$.

Las curvas elípticas relacionan ramas de las matemáticas distantes a menudo, como son la geometría algebraica, la teoría de grupos, la teoría de números, el análisis complejo y la topología. En este trabajo solo nos centraremos en su relación con la teoría de grupos, ya que, sorprendentemente, se puede definir una operación interna de modo que el conjunto de los puntos de la curva con coordenadas sobre un cuerpo tenga estructura de grupo abeliano. Más concretamente, estamos interesados en los puntos con coordenadas racionales y, en particular, estudiaremos la torsión de este grupo.

Los usos de las curvas elípticas son diversos. Por ejemplo, uno muy destacable es que Andrew Wiles se sirvió de ellas para demostrar el último teorema de Fermat, que

llevaba más de 300 años sin ser resuelto, en 1995. Juegan también un papel importante en la criptografía, un tema de actualidad y otro motivo más que sirve de aliciente para estudiar estas curvas, aunque en este caso se definan sobre cuerpos finitos y no sobre $\mathbb{Q}$, como haremos en esta memoria. De hecho, resolver el problema del logaritmo discreto en curvas elípticas es tan difícil como factorizar números enteros arbitrariamente grandes, que es justo en lo que se basa el protocolo RSA, pero la criptografía de curvas elípticas cuenta con la ventaja de ser más rápida y usar claves más cortas proporcionando un nivel de seguridad equivalente.

El objetivo de este trabajo es demostrar el Teorema de Nagell-Lutz.

Teorema (Nagell-Lutz)**.** *Sea*

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

una curva elíptica con coeficientes enteros a, b, c, y sea $\boldsymbol{D}$ el discriminante del polinomio cúbico $f(x)$,

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

Sea $\boldsymbol{P} = (x, y)$ un punto racional de la curva de orden finito. Entonces x e y son números enteros. Además, o bien $y = 0$, en cuyo caso $\boldsymbol{P}$ tiene orden dos, o bien y^2 divide a $\boldsymbol{D}$.

En el Capítulo 1 comenzaremos estudiando la geometría de las curvas cúbicas y viendo cómo dotar a la curva de estructura de grupo abeliano, además de dar unas fórmulas explícitas para la operación de grupo, las cuales son muy útiles en algunos casos en los que no es suficiente con la construcción algebraica. Un hecho destacable del que hablaremos también es que el grupo de puntos racionales es finitamente generado, resultado que demostró Mordell. Asimismo, mencionaremos en este capítulo que toda curva elíptica es birracionalmente equivalente a una cúbica como la del enunciado del teorema, llamada forma normal de Weierstrass, un hecho que facilita mucho el estudio de estas curvas. Finalizaremos este capítulo estudiando ciertas propiedades del discriminante del polinomio cúbico $f(x)$, propiedades que son cruciales en la demostración del teorema.

En el Capítulo 2, enunciaremos un teorema sobre los puntos racionales de orden dos y tres, en el cual los caracterizamos y vemos cómo son los subgrupos de puntos con coeficientes en $\mathbb{C}$ tales que su orden divide a dos y tres, respectivamente. En la Sección 2 de este capítulo demostraremos que si un punto es de orden finito, necesariamente tiene que tener coordenadas enteras y, en la última sección, resumimos todos los resultados del trabajo en la prueba del Teorema de Nagell-Lutz. Siguiendo

con la torsión de las curvas, enunciaremos el Teorema de Mazur, que nos dice qué posibles estructuras puede tomar ser el grupo formado por todos los puntos racionales de orden finito.

La mayor parte del trabajo y las imágenes están basadas en [5]. Además, las secciones 1.1 y 1.2 se han visto muy influenciadas por [1] y especialmente por [4]. Para aspectos computacionales, se ha usado [6] en el Apéndice.

1 Geometría y Aritmética

1.1 La geometría de las curvas cúbicas

En todo el trabajo k denotará un cuerpo, aunque nuestro mayor interés será $k = \mathbb{Q}$.

Definición 1.1.1. *Diremos que una curva de $\mathbb{P}^2(k)$ es una cúbica si admite una ecuación del tipo*

$$F(X, Y, Z) = 0 \tag{1.1}$$

con $F(X, Y, Z) \in k[X, Y, Z]$ homogéneo de grado 3.

Ejemplo 1.1.1. Un ejemplo famoso es

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

el primer caso no trivial del último teorema de Fermat.

Definición 1.1.2. *Se dice que una curva cúbica (1.1) es una curva elíptica si es no singular.*

Para el estudio de estas curvas, existe un principio geométrico que podemos usar:

Proposición 1.1.1. Sea K un cuerpo tal que $k \subseteq K$. Dados dos puntos P y Q con coordenadas en un cuerpo K de una curva cúbica, genéricamente es posible encontrar un tercer punto de la curva con coordenadas en K, alineado con P y Q.

Demostración. Basta tomar la recta que une P y Q. Si una recta corta a la cúbica en dos puntos con coordenadas en K, por las relaciones de Cardano se tiene que el tercer punto de corte también tiene coordenadas en K. ∎

Observación 1.1.1. Aplicando esto para $k = K = \mathbb{Q}$, podemos ver que si tenemos dos puntos racionales podemos encontrar un tercer punto racional.

Observación 1.1.2. Si tenemos dos puntos proyectivos distintos de la cúbica, P y Q, construiremos otro punto $P * Q$, que será el tercer punto de corte de la recta PQ con nuestra curva. Si P no es un punto de inflexión y $Q = P$, tomaremos la recta tangente en P, que tiene con la curva un contacto de orden 2. Esta recta corta a la curva en otro punto distinto de P, y este será $P * P$. Por último, en el caso en que P sea un punto de inflexión (es decir, que la tangente por P tenga un índice de intersección 3 con la curva, ver más adelante) se tomará $P * P = P$.

Así que esto da una especie de ley de composición: comenzando con dos puntos P y Q, trazamos la recta que pasa por P y Q y denotamos por $P * Q$ al tercer punto de intersección de la recta con la cúbica, ver la Figura 1.1.

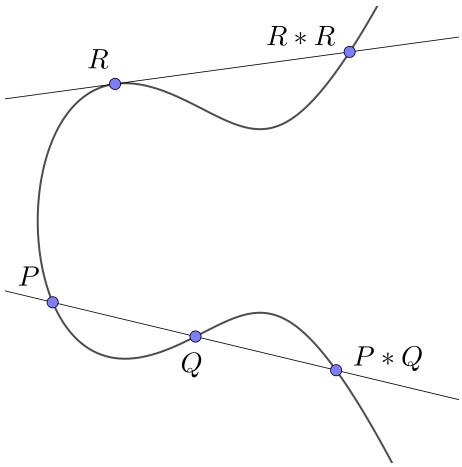

Figura 1.1: La composición de puntos en una cúbica.

Hemos definido estas curvas en el espacio proyectivo, pero nuestro interés es la carta afín, donde nuestra curva estará definida por una ecuación del tipo $y^2 = f(x)$ siendo $f(x)$ un polinomio de grado 3.

Un resultado importante es el teorema de Mordell (1922), que establece que si C es una curva elíptica racional, entonces hay un conjunto *finito* de puntos racionales tal que todos los demás puntos racionales se puede obtener dibujando rectas repetidamente y tomando intersecciones. El teorema de Mordell puede reformularse para que sea más esclarecedor. Para hacer esto, primero enunciaremos el teorema de Bézout y lo aplicaremos para nuestro caso particular.

Dadas dos curvas proyectivas E_1 y E_2 sin componentes comunes, para cada punto $P \in \mathbb{P}^2$ se define el índice (o número) de intersección $i_P(E_1, E_2)$. Este es un número

entero no negativo que refleja hasta qué punto E_1 y E_2 son tangentes entre sí en P. Su definición formal [2] escapa al objetivo de este trabajo, pero se puede tener una buena idea de este índice con las siguientes propiedades:

(i) Si $P \notin E_1 \cap E_2$, entonces $i_p(E_1, E_2) = 0$.
(ii) Si $P \in E_1 \cap E_2$, si P es un punto no singular de ambas curvas y E_1 y E_2 tienen direcciones tangentes distintas en P, entonces $i_P(E_1, E_2) = 1$. En este caso, decimos que E_1 y E_2 se cortan en P transversalmente.
(iii) Si $P \in E_1 \cap E_2$ y E_1 y E_2 no se cortan transversalmente en P, entonces $i_P(E_1, E_2) \geq 2$.

Teorema 1.1.2 (Bézout). *Sea k un cuerpo algebraicamente cerrado y sean $E_1, E_2 \in \mathbb{P}^2(k)$ dos curvas sin componentes comunes definidas por los polinomios F y G, respectivamente. Entonces*

$$\sum_{P \in E_1 \cap E_2} i_P(E_1, E_2) = \operatorname{gr}(F) \cdot \operatorname{gr}(G).$$

En particular, si E_1 y E_2 son curvas no singulares con solo intersecciones transversales, entonces $\#(E_1 \cap E_2) = \operatorname{gr}(F) \cdot \operatorname{gr}(G)$, y en todos los casos tenemos la desigualdad

$$\#(E_1 \cap E_2) \leq \operatorname{gr}(F) \cdot \operatorname{gr}(G).$$

Corolario 1.1.3. En general, sobre un cuerpo algebraicamente cerrado, dos curvas cúbicas sin componentes comunes se encuentran en nueve puntos (contados de acuerdo a su índice).

Demostración. Inmediato aplicando el Teorema de Bézout. ∎

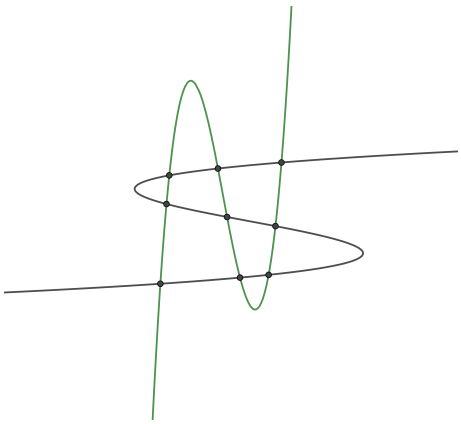

Figura 1.2: La intersección de dos curvas cúbicas.

El teorema que queremos utilizar es el siguiente:

Teorema 1.1.4. *Sean E, E_1 y E_2 curvas cúbicas tales que $i_P(E_1, E_2) = 1$ para todo $P \in E_1 \cap E_2$. Supongamos que E pasa por ocho de los nueve puntos de intersección de E_1 y E_2. Entonces E pasa por el noveno punto de intersección.*

Indicaciones. Consideremos el problema de construir una curva cúbica que pase por un cierto número de puntos. Para definir una curva cúbica 1.1, tenemos que dar diez coeficientes. Si multiplicamos todos los coeficientes por una constante distinta de cero, obtenemos la misma curva. Así que realmente el conjunto de todas las cúbicas posibles es, por así decirlo, de nueve dimensiones. Y si queremos que la cúbica pase por un punto cuyas coordenadas están dadas, eso impone una condición lineal a los coeficientes del polinomio cúbico. El conjunto de cúbicas que pasan por un punto dado es, por así decirlo, de ocho dimensiones. Cada vez que imponemos la condición de que la cúbica debe contener otro punto especificado, imponemos otra condición lineal sobre los coeficientes, lo que reduce en uno la dimensión del conjunto de todas esas cúbicas[1]. En particular, la familia de todas las cúbicas que pasan por de ocho puntos de intersección dados $P_1, \dots, P_8$ de E_1 y E_2 es una familia unidimensional.

Sean $F_1(X, Y, Z) = 0$ y $F_2(X, Y, Z) = 0$ las ecuaciones cúbicas que dan E_1 y E_2. Entonces, para cada elección de números λ_1 y λ_2, la combinación lineal $\lambda_1 F_1 + \lambda_2 F_2$ es una cúbica que pasa por $P_1, \dots, P_8$. Dado que solo existe una familia unidimensional de tales cúbicas, el conjunto de cúbicas $\lambda_1 F_1 + \lambda_2 F_2$ debe ser esa familia. En particular, la cúbica E viene dada por una ecuación $\lambda_1 F_1 + \lambda_2 F_2 = 0$ para una elección adecuada de λ_1 y λ_2.

Como P_9 está tanto en E_1 como en E_2, sabemos que $F_1(x, y)$ y $F_2(x, y)$ se anulan en P_9. De ello se deduce que $\lambda_1 F_1 + \lambda_2 F_2$ también se anula en P_9, por lo que E para por P_9.

Observación 1.1.3. En el teorema anterior hemos exigido que todos los cortes de E_1 y E_2 sean transversales, pero el resultado sigue siendo cierto sin esta condición (teniendo en cuenta de la forma correcta el número de interesección).

De paso, mencionamos que no existe un método conocido que esté garantizado para determinar, en un número finito de pasos, si una cúbica racional dada tiene un punto racional. De hecho, es el caso más simple de curvas donde las congruencias no aportan toda la información necesaria sobre este particular (el denominado principio de Hasse-Minkowsky). Dejamos de lado este difícil problema y asumimos de ahora en adelante que nuestra cúbica tiene un punto racional, que denotamos por $\mathcal{O}$.

[1] Hay que tener en cuenta que en realidad esto es solo un argumento de plausibilidad; para hacerlo riguroso, necesitaríamos demostrar que cada nueva condición lineal es independiente de las anteriores.

Queremos reformular el teorema de Mordell de una manera que tenga ventajas estéticas y técnicas. Hemos visto que si tenemos dos puntos racionales cualesquiera en una cúbica racional, digamos P y Q, entonces podemos trazar la recta que une P con Q y obtener un tercer punto que denotamos $P * Q$. Se intuye cierta estructura de grupo, ya que si consideramos el conjunto de todos los puntos racionales en la cúbica, podemos decir que hay una operación que envía el par (P, Q) al punto $P * Q$. Lamentablemente no obtenemos un grupo ya que, para empezar, está bastante claro que no hay ningún elemento neutro.

Sin embargo, manipulando un poco, podemos convertir el conjunto de puntos racionales en un grupo de tal manera que el punto racional $\mathcal{O}$ dado se convierte en el elemento neutro. Denotaremos la operación del grupo con + porque va a ser un grupo conmutativo, pero hacemos hincapié en que esta nueva "suma en una curva cúbica" no tiene nada que ver con la suma ordinaria. La regla es la siguiente:

Definición 1.1.3. *Sea E una curva elíptica y sea $\mathcal{O}$ un punto de la curva. Dados dos puntos de la curva P y Q, se define la operación + como sigue:*
Para sumar P y Q, se toma el tercer punto de intersección $P * Q$, se traza la recta que pasa por $P * Q$ y $\mathcal{O}$ y, finalmente, se toma el tercer punto de intersección de esta recta con E como $P + Q$. En otras palabras, $P + Q = \mathcal{O} * (P * Q)$.

Esta operación de adición se ilustra en la Figura 1.3.

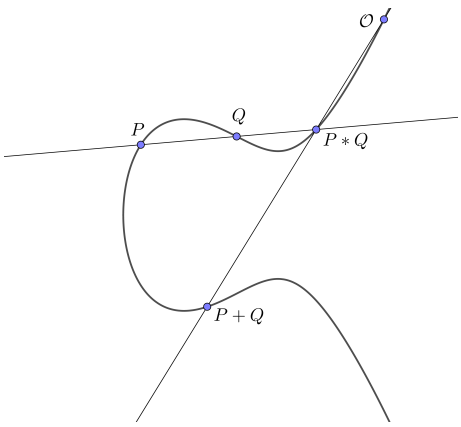

Figura 1.3: La operación de grupo en una cúbica.

Definición 1.1.4. *Dada una cúbica E en el plano $\mathbb{P}^2(k)$, definida por un polinomio $F(X, Y, Z) \in k[X, Y, Z]$, y dado un cuerpo K con $k \subset K$, se denota por $E(K)$ al*

conjunto de puntos en la curva cuyas coordenadas se pueden definir en K,

$$E(K) = \left\{ (\alpha : \beta : \gamma) \in \mathbb{P}^2(K) \;\middle|\; F(\alpha, \beta, \gamma) = 0 \right\}.$$

Teorema 1.1.5. *Sea* E *una curva elíptica, un cuerpo* K *y* $\mathcal{O} \in E(K)$ *un punto, entonces* $(E(K), +)$ *es un grupo conmutativo con elemento neutro* $\mathcal{O}$.

Demostración. Es claro que la operación $+$ es interna y que esta operación es conmutativa, es decir,

$$P + Q = Q + P,$$

dado que la recta que pasa por P y Q es la misma que la recta que pasa por Q y P, entonces $P * Q = Q * P$ e inmediatamente se obtiene la conmutatividad de $+$.

El elemento neutro es $\mathcal{O}$, pues $P + \mathcal{O} = P$ para todo $P \in E(K)$. Veamos esto último. Si unimos P con $\mathcal{O}$, obtenemos el punto $P * \mathcal{O}$ como tercer punto de intersección. Luego unimos $P * \mathcal{O}$ con $\mathcal{O}$ y tomamos el tercer punto de intersección. Ese tercer punto de intersección es claramente P. Entonces

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

El hecho de que $\mathcal{O}$ actúa como elemento neutro se muestra en la Figura 1.4.

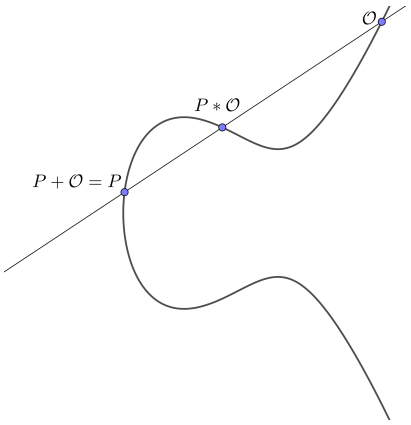

Figura 1.4: Verificando que $\mathcal{O}$ es el elemento neutro.

Para obtener opuestos, se dibuja la recta tangente a la cúbica en $\mathcal{O}$, que sabemos que existe pues E es no singular, y se halla el otro punto de intersección con la cúbica que será el punto adicional S, es decir, $S = \mathcal{O} * \mathcal{O}$. Entonces, dado un punto Q, unimos Q con S, y el tercer punto de intersección $Q * S$ será $-Q$; véase la Figura

1.5. Para comprobar que esto es así, sumamos Q a $-Q$. Para hacer esto, tomamos la tercera intersección de la recta que pasa por Q y $-Q$, que es S. Luego unimos S con $\mathcal{O}$ y tomamos el tercer punto de intersección $S * \mathcal{O}$. Pero la recta que pasa por S y $\mathcal{O}$ se encuentra con la cúbica una vez en S y dos veces en $\mathcal{O}$, porque es tangente a la cúbica en $\mathcal{O}$. Entonces, la tercera intersección es la segunda vez que se encuentra con la cúbica en $\mathcal{O}$. Por lo tanto $Q + (-Q) = \mathcal{O}$.

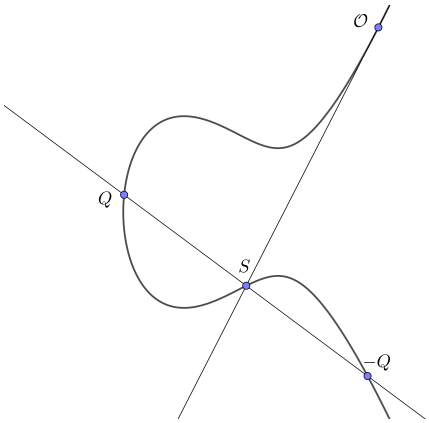

Figura 1.5: El opuesto de un punto.

Por último, nos falta comprobar que + es asociativa. Sean P, Q y R tres puntos en la curva. Para probar que $P + (Q + R) = (P + Q) + R$, basta ver que $P * (Q + R) = (P + Q) * R$, ya que solo faltará unir estos con $\mathcal{O}$ y el tercer punto será la suma de P, Q y R que en los dos casos es el mismo por estar uniendo el mismo punto con $\mathcal{O}$. Se trata de ver si la recta que une P y $Q + R$ y la recta que une $P + Q$ y R se cortan sobre la curva. Entonces el punto de corte de estas rectas será el punto de corte de cada una con la curva, es decir:

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

Consideramos dos nuevas cúbicas, cada una de ellas formada por tres rectas. La primera de ellas es

$$E_1 = r_1 \cup r_2 \cup r_3,$$

siendo r_i rectas tales que

$$\begin{aligned} r_1 &\supset \{Q, R, Q * R\}, \\ r_2 &\supset \{\mathcal{O}, P * Q, P + Q\}, \\ r_3 &\supset \{P, Q + R, P * (Q + R)\}. \end{aligned}$$

Y la otra cúbica es

$$C_2 = s_1 \cup s_2 \cup s_3,$$

siendo s_i rectas tales que

$$\begin{aligned} s_1 &\supset \{P, Q, P * Q\}, \\ s_2 &\supset \{\mathcal{O}, Q * R, Q + R\}, \\ s_3 &\supset \{P + Q, R, (P + Q) * R\}. \end{aligned}$$

Las dos cúbicas coinciden en los 9 puntos siguientes: $\mathcal{O}$, P, Q, R, $P * Q$, $P+Q$, $Q * R$, $Q + R$ y el punto intersección de las dos rectas que queríamos ver que se cortan sobre E. Como los primeros 8 puntos están en E, el noveno punto también estará en E aplicando el Teorema 1.1.4. Esto finaliza la prueba de que la ley "+" es asociativa.

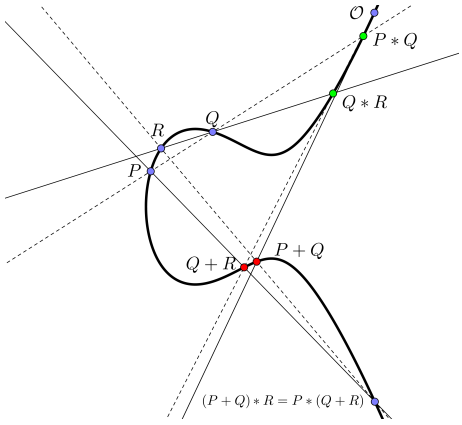

Figura 1.6: Verificando la propiedad asociativa.

No haremos más para probar que la operación + convierte los puntos de $E(K)$ en un grupo. Posteriormente, cuando tengamos una forma normal, tendremos fórmulas explícitas para sumar puntos.

También queremos mencionar que no hay nada especial en nuestra elección de $\mathcal{O}$. Si elegimos un punto $\mathcal{O}'$ diferente para que sea el elemento neutro de nuestro grupo, entonces obtenemos un grupo con exactamente la misma estructura. De hecho, se puede demostrar que la aplicación

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

es un isomorfismo del grupo $(E(K), +)$, con elemento neutro $\mathcal{O}$, al grupo $(E(K), +')$, con elemento neutro $\mathcal{O}'$, donde la nueva operación está definida por

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

¿Cómo nos permite lo que hemos hecho reformular el teorema de Mordell? Este resultado nos dice que obtenemos todo punto racional comenzando con un conjunto finito de puntos, dibujando rectas a través de esos puntos para obtener nuevos puntos, luego dibujando rectas a través de los nuevos puntos para obtener aún más puntos, y así sucesivamente. En términos de la operación de grupo, esto dice que el grupo de puntos racionales se genera de forma finita. Entonces podemos dar el siguiente enunciado alternativo:

Teorema 1.1.6 (Mordell). *Si una curva elíptica plano proyectivo racional tiene un punto en $\mathbb{P}^2(\mathbb{Q})$, entonces el grupo de puntos racionales es finitamente generado.*

1.2 Forma normal de Weierstrass

Toda curva elíptica afín se puede expresar, salvo equivalencia birracional[2], como una de las llamadas *formas normales de Weierstrass*. Esto puede probarse usando el Teorema de Riemann-Roch [2], o bien de forma directa.

El algoritmo presentado en [1], por ejemplo (no es fácil hallar referencias explícitas de este resultado), establece la posibilidad, cuando la característica de k es distinta de 2, de hallar una ecuación de la forma

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

que es un caso particular de la denominada forma larga de Weierstrass, algo más general y válida en cualquier característica,

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

Notemos que los subíndices de los coeficientes se escogen por homogeneidad: dando a y un peso 3, a x un peso 2 y a cada coeficiente a_i el peso indicado en el subíndice obtenemos una ecuación homogénea de grado 6.

[2]El concepto de equivalencia birracional se trabaja ampliamente en la asignatura del grado Álgebra Conmutativa y Geometría Algebraica.

Ejemplo 1.2.1. Consideremos las curvas elípticas

$$Y : u^3 + v^3 = \alpha \qquad \text{y} \qquad Z : y^2 = x^3 - 432\alpha^2,$$

con $\alpha \neq 0$, y las aplicaciones racionales

$$\begin{array}{rcl} f : Y & \to & Z \\ (u,v) & \mapsto & \left(\dfrac{12\alpha}{u+v}, 36\alpha\dfrac{u-v}{u+v}\right) \end{array} \qquad \begin{array}{rcl} g : Z & \to & Y \\ (x,y) & \mapsto & \left(\dfrac{36\alpha+y}{6x}, \dfrac{36\alpha-y}{6x}\right) \end{array}$$

Para ver que las aplicaciones están bien definidas, basta hacer los cálculos y comprobar que dado $(u,v) \in Y$ su imagen $f(u,v)$ verifica la ecuación de Z y, dado $(x,y) \in Z$, su imagen $g(x,y)$ verifica la ecuación de Y.

Ahora podemos comprobar que las curvas Y y Z son birracionalmente equivalentes. Tenemos que ver que $f \circ g$ y $g \circ f$ son la identidad. Compongamos:

$$\begin{aligned} (f\circ g)(x,y) &= f\left(\frac{36\alpha+y}{6x}, \frac{36\alpha-y}{6x}\right) \\ &= \left(\frac{12\alpha}{\frac{36\alpha+y}{6x} + \frac{36\alpha-y}{6x}}, 36\alpha\frac{\frac{36\alpha+y}{6x} - \frac{36\alpha-y}{6x}}{\frac{36\alpha+y}{6x} + \frac{36\alpha-y}{6x}}\right) \\ &= \left(\frac{12\alpha}{12\alpha/x}, 36\alpha\frac{y/3x}{12\alpha/x}\right) = \left(x, 36\alpha\frac{xy}{36\alpha x}\right) = (x,y) \end{aligned}$$

Veamos ahora la otra composición, que se resuelve de forma similar:

$$\begin{aligned} (g\circ f)(u,v) = g(f(u,v)) &= g\left(\frac{12\alpha}{u+v}, 36\alpha\frac{u-v}{u+v}\right) = \\ &= \left(\frac{36\alpha + 36\alpha\frac{u-v}{u+v}}{6\frac{12\alpha}{u+v}}, \frac{36\alpha - 36\alpha\frac{u-v}{u+v}}{6\frac{12\alpha}{u+v}}\right) = \left(\frac{72\alpha u}{72\alpha}, \frac{72\alpha v}{72\alpha}\right) = (u,v) \end{aligned}$$

Por tanto, las curvas son birracionalmente equivalentes.

Salvo mención expresa, a partir de ahora y durante todo el trabajo nos ceñiremos al caso $k = \mathbb{Q}$.

Proposición 1.2.1. Sea

$$E : Y^2Z = F(X,Z) = X^3 + aX^2Z + bXZ^2 + cZ^3$$

una cúbica en forma normal de Weierstrass, y sea

$$f(X) = F(X,1) = X^3 + aX^2 + bX + c.$$

Entonces f tiene 3 raíces distintas si y solo si la curva es no singular.

Demostración. Supongamos primero que estamos en la carta afín $Z \neq 0$. Una curva $G(X,Y,Z) = 0$ es singular en un punto $(X_0 : Y_0 : Z_0)$ si las derivadas parciales de G respecto de X, Y y Z se anulan a la vez en dicho punto.

La ecuación de nuestra curva es de la forma $G(X,Y,Z) = Y^2Z - F(X,Z) = 0$, por tanto, esta curva es singular en un punto $(X_0 : Y_0 : Z_0)$ con $Z_0 \neq 0$ si y solo si

$$\begin{cases} \dfrac{\partial G}{\partial X} = -3X_0^2 - 2aX_0Z_0 - bZ_0^2 = 0, \\ \dfrac{\partial G}{\partial Y} = 2Y_0Z_0 = 0, \end{cases}$$

es decir, tomando $Z_0 = 1$, el punto es no singular si y solo si

$$\begin{cases} -f(X_0) = 0, \\ 2Y_0 = 0, \end{cases}$$

Por tanto, la curva es singular en un punto $(X_0 : Y_0 : 1)$ si y solo si X_0 anula a la vez a f y a f', (ya que $f(X_0) = Y_0^2 = 0$). Esto es equivalente a decir que f tiene una raíz múltiple.

Veamos ahora qué pasa con los puntos de la curva que tienen $Z_0 = 0$. En realidad solo hay un punto con esta condición, el de coordenadas $(0 : 1 : 0)$. Este punto no es singular porque no anula la parcial de G respecto de Z, ya que

$$\frac{\partial G}{\partial Z}|_{(0:1:0)} = (Y_0^2 - aX_0^2 - 2bX_0Z_0 - 3Z_0^2)|_{(0:1:0)} = 1^2 - a \cdot 0 - 2b \cdot 0 - 3 \cdot 0^2 = 1.$$

∎

Observación 1.2.1. Por definición, una curva cúbica dada en la forma anterior es una curva elíptica si es no singular, o lo que es lo mismo, si el polinomio f que la define tiene tres raíces distintas.

Dada una curva elíptica, con su parte afín en forma normal de Weierstrass,

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

si a, b y c son racionales, también serán reales, luego $f(x)$ tiene una o tres raíces reales:

$$f(x) = (x - \alpha)(x^2 + \beta x + \gamma)$$

con α, β y γ números reales.

La gráfica de la curva será de uno de los dos tipos siguientes, según tenga una o tres raíces reales:

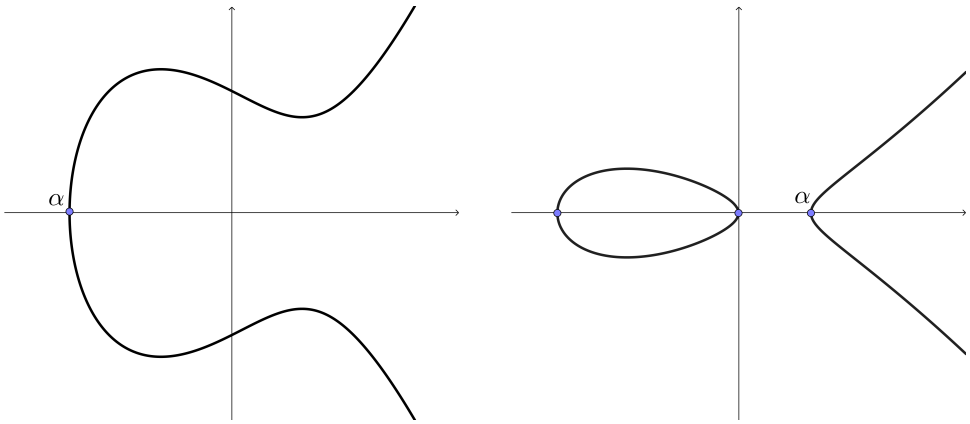

Figura 1.7: Cúbicas con una y tres raíces reales.

Proposición 1.2.2. Si una curva elíptica viene dada en forma larga de Weierstrass

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

entonces todo cambio de variables del tipo

$$x \mapsto u^2x' + r, \qquad y \mapsto u^3y' + sx' + t,$$

con $r, s, t, u \in \mathbb{Q}$, $u \neq 0$, lleva la ecuación a otra, también de Weierstrass.

En particular, podemos conseguir una ecuación del tipo

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

Esta se conoce como forma breve o corta de Weierstrass.

Demostración. Solo demostraremos el caso particular. Si primero hacemos el cambio $y \mapsto y - (a_1x + a_3)/2$, y renombramos coeficientes obtenemos

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

Ahora si hacemos el cambio $x \mapsto x - (a_2/3)$, queda una ecuación del tipo

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

Observación 1.2.2. También hay otra expresión para la forma breve de Weierstrass de una curva elíptica, llamada *forma clásica de Weierstrass*. Haciendo el cambio

$$x \mapsto 4x, \quad y \mapsto 4y,$$

en la forma corta anterior y llamando A a $A/4$ y B a $B/16$, obtenemos

$$y^2 = 4x^3 + Ax + B.$$

Proposición 1.2.3. Sea C una curva elíptica en forma breve de Weierstrass

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

con $A, B \in \mathbb{Q}$. Si hacemos el cambio

$$x \mapsto u^2x, \quad y \mapsto u^3y,$$

con $u \in \mathbb{Q}\backslash\{0\}$, se obtiene una forma breve de Weierstrass equivalente a la dada. Estos son los únicos cambios de variable que conservan formas breves de Weierstrass.

Observación 1.2.3. Dada la curva elíptica en forma normal de Weierstrass,

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

con $a, b, c \in \mathbb{Q}$, podemos suponer en realidad que tenemos $a, b, c \in \mathbb{Z}$. Haciendo el cambio

$$X = u^2x, \quad Y = u^3y$$

con $u \in \mathbb{Z}$ bien escogido según los denominadores de a, b y c, se consigue que la ecuación de la curva sea

$$Y^2 = X^3 + u^2aX^2 + u^4bX + u^6c,$$

donde todos los coeficientes son enteros.

Las transformaciones que necesitamos usar para poner la curva en forma normal no llevan líneas rectas a líneas rectas. Dado que definimos la operación de grupo en nuestra curva usando rectas que unen puntos, no está del todo claro que nuestra transformación conserve la estructura del grupo. En otras palabras, ¿nuestra transformación es un homomorfismo de grupo? Lo es, pero eso no es nada obvio. La cuestión es que nuestra descripción de la suma de puntos en la curva no es buena, porque parece depender de la forma en que la curva está inmersa en el plano. Pero, de hecho, la operación de adición es una operación intrínseca que puede describirse en la curva y es invariante bajo transformaciones birracionales. Esto se deriva de hechos generales sobre curvas algebraicas, usando resultados como el Teorema de Riemann–Roch, pero no es fácil de probar simplemente manipulando las ecuaciones explícitas y no entraremos aquí [4].

Ejemplo 1.2.2. En el ejemplo 1.2.1 vimos una transformación birracional entre las curvas $Y : u^3+v^3 = \alpha$ y $Z : y^2 = x^3-432\alpha^2$. Además, dicha transformación también es un isomorfismo entre los grupos $(Z,+)$ con elemento neutro $\mathcal{O} = (0 : 1 : 0)$ e $(Y,+')$ con elemento neutro $\mathcal{O}' = (1 : -1 : 0)$. Dejamos al lector interesado que compruebe esta afirmación ayudándose de las fórmulas explícitas que se dan en la sección 1.3 para la suma de puntos en Z y de las siguientes expresiones para la suma de puntos en Y:

- Si $P_1 = (u_1, v_1) \neq (u_2, v_2) = P_2$, entonces

$$P_1 + P_2 = \left(-\lambda\left(-u_1 - u_2 - \frac{3\lambda^2\delta}{1+\lambda^3}\right) + \delta, -u_1 - u_2 - \frac{3\lambda^2\delta}{1+\lambda^3}\right)$$

  con $\lambda = (v_2 - v_1)/(u_2 - u_1)$ y $\delta = v_1 - \lambda u_1 = v_2 - \lambda u_2$.
- La fórmula para duplicar un punto $P_0 = (u_0, v_0)$ es

$$2P_0 = \left(-\lambda\left(-2u_0 - \frac{3\lambda^2\delta}{1+\lambda^3}\right) + \delta, -2u_0 - \frac{3\lambda^2\delta}{1+\lambda^3}\right)$$

  con $\lambda = u_0^2/v_0^2$ y $\delta = v_0 - \lambda u_0$.

Hemos concentrado la atención solo en cúbicas no singulares porque las cúbicas singulares y las cúbicas no singulares tienen comportamientos completamente diferentes. Por ejemplo, las cúbicas singulares son tan fáciles de tratar como las cónicas. Si proyectamos desde el punto singular sobre alguna recta, vemos que la recta que pasa por ese punto singular se encuentra con la cúbica dos veces en el punto singular, por lo que se encuentra con la cúbica solo una vez más. La proyección de una curva

cúbica singular sobre una recta es, por tanto, uno a uno. Así que, al igual que para una cónica, los puntos racionales no singulares de una cúbica singular se pueden poner en correspondencia uno a uno con los puntos racionales de una recta. De hecho, es muy fácil hacerlo explícitamente con fórmulas.

Ejemplo 1.2.3. Lo ilustramos con la cúbica singular $y^2 = x^2(x+1)$. Si tomamos $r = y/x$, entonces la ecuación se convierte en

$$r^2 = x + 1,$$

y por lo tanto

$$x = r^2 - 1, \qquad y = rx = r^3 - r.$$

Así, si tomamos cualquier número racional r y usamos estas ecuaciones para definir x e y, entonces obtenemos un punto racional en la cúbica; y si comenzamos con un punto racional $(x, y) \neq (0, 0)$ en la cúbica, obtenemos un número racional correspondiente $r = x/y$. Estas operaciones son inversas entre sí y se definen en todos los puntos racionales excepto en el punto singular $(0, 0)$. De esta manera obtenemos todos los puntos racionales en la curva.

La curva $y^2 = x^3$ es aún más simple. Solo tomamos

$$x = t^2, \qquad y = t^3.$$

De modo que los puntos racionales en cúbicas singulares son triviales de analizar. En realidad no hemos explicado cómo obtener una operación de grupo para estas curvas singulares, pero si se evita la singularidad y se usa el procedimiento que describimos anteriormente, se obtiene un grupo.

1.3 Fórmulas explicitas para la operación de grupo

Ya hemos visto la estructura algebraica de nuestras curvas, pero a veces es conveniente tener fórmulas explícitas para que trabajar con estas se haga de manera eficiente. Partimos de una curva elíptica C en forma normal de Weierstrass:

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

siendo su homogeneizada la curva proyectiva de ecuación:

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

Al tomar como recta del infinito $Z = 0$, la intersección de esta con la curva da un punto $\mathcal{O} = (0 : 1 : 0)$, que es el punto del infinito del eje OY, es decir, el punto en el infinito donde se encuentran las rectas verticales, y además es un punto de inflexión ya que la recta tangente en ese punto es la recta en el infinito y esa recta tangente tiene índice de intersección 3 con la curva. Ya hemos visto también que el punto en el infinito es un punto no singular.

El punto $\mathcal{O}$ se cuenta como un punto racional y lo tomamos como el elemento neutro cuando formamos el conjunto de puntos en un grupo. Entonces, para que todo funcione en el plano afín, tenemos que hacer la convención de que los puntos de nuestra cúbica consisten en los puntos ordinarios del plano afín junto con otro punto $\mathcal{O}$ que no se puede ver. De este modo, tenemos que cada recta se encuentra con la cúbica en tres puntos:

a) Si la recta es la del infinito, corta a la cúbica en $\mathcal{O}$ tres veces.
b) Si la recta es vertical, corta a la cúbica en dos puntos en el plano afín y también en el punto $\mathcal{O}$.
c) Si la recta no es como las anteriores, corta a la curva en tres puntos afines (por supuesto, es posible que sean complejos).

Ahora vamos a discutir la estructura del grupo un poco más de cerca. Para sumar dos puntos P y Q en una curva elíptica en forma de Weierstrass, primero trazamos la recta que pasa por P y Q y encontramos el tercer punto de intersección $P * Q$. Luego trazamos la recta que pasa por $P * Q$ y $\mathcal{O}$, que es solo la recta vertical que pasa por $P * Q$. Una curva cúbica en forma de Weierstrass es simétrica con respecto al eje x, por lo que para encontrar $P + Q$, simplemente tomamos $P * Q$ y lo reflejamos sobre el eje x. Este procedimiento se ilustra en la Figura 1.8.

El opuesto de Q es el punto reflejado, es decir, si $Q = (x, y)$, entonces $-Q = (x, -y)$; vea la Figura 1.9. Para comprobar esto, supongamos que sumamos Q al punto que afirmamos que es $-Q$. La recta que pasa por Q y $-Q$ es vertical, por lo que el tercer punto de intersección es $\mathcal{O}$. Ahora unimos $\mathcal{O}$ con $\mathcal{O}$ y buscamos la tercera intersección. Unir $\mathcal{O}$ con $\mathcal{O}$ da la recta en el infinito, y la tercera intersección es nuevamente $\mathcal{O}$. Esto muestra que $Q + (-Q) = \mathcal{O}$, entonces $-Q$ es el opuesto de Q. Por supuesto, este razonamiento no se aplica al caso $Q = \mathcal{O}$, pero es fácil ver que $-\mathcal{O} = \mathcal{O}$. También mencionamos que si P, Q, R son puntos distintos, entonces $P + Q + R = \mathcal{O}$ si y solo si P, Q, R son colineales.

Ahora desarrollamos algunas fórmulas para calcular $P + Q$ de manera eficaz:

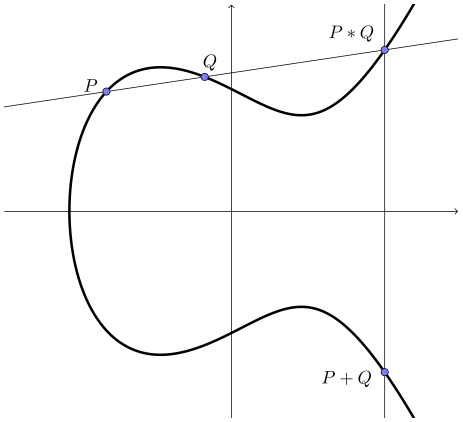

Figura 1.8: Suma en una cúbica en forma normal de Weierstrass.

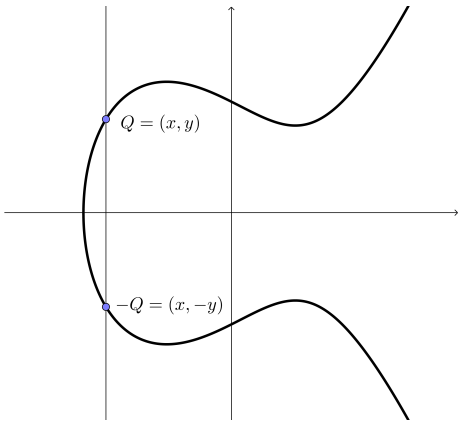

Figura 1.9: Elemento opuesto en una cúbica en forma normal de Weierstrass.

Proposición 1.3.1. Dados dos puntos distintos $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ de la curva $y^2 = x^3 + ax^2 + bx + c$, entonces $P_1 + P_2 = (x_3, y_3)$, donde

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = -(\lambda x_3 + \nu)$$

con $\lambda = (y_2 - y_1)/(x_2 - x_1)$ y $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Demostración. Tenemos $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 * P_2 = (x_3, y_3)$ y $P_1 + P_2 = (x_3, -y_3)$, ver la Figura 1.10. Queremos calcular (x_3, y_3).

Primero miramos la ecuación de la recta que une (x_1, y_1) con (x_2, y_2). Esta recta tiene la ecuación

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

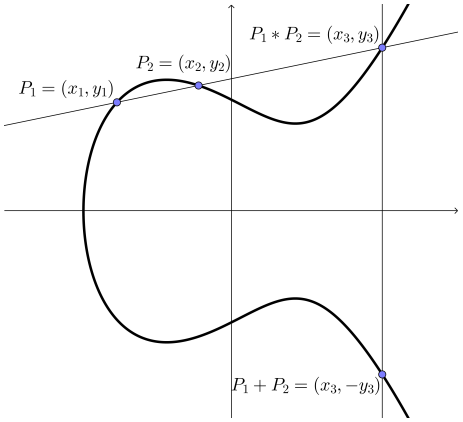

Figura 1.10: Construyendo una fórmula para la operación de adición.

Por construcción, esta recta corta a la cúbica en los dos puntos (x_1, y_1) y (x_2, y_2). Sustituimos $y = \lambda x + \nu$ en la ecuación de la curva para obtener

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

Pasando todo a un lado,

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

Esta es una ecuación cúbica en x, y sus tres raíces x_1, x_2, x_3 nos dan las coordenadas x de los tres puntos de intersección. Por lo tanto

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

Al igualar los coeficientes del término x^2 en cada lado, llegamos a que

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

y entonces

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

Estas fórmulas son la forma más eficiente de calcular la suma de dos puntos distintos. Hagamos un ejemplo:

Ejemplo 1.3.1. Sea la curva cúbica

$$y^2 = x^3 - x + 1,$$

que tiene los dos puntos racionales $P_1 = (0, 1)$ y $P_2 = (3, 5)$. Para calcular $P_1 + P_2$, tomamos la recta que pasa por P_1 y P_2. Esta es la recta

$$y = \frac{4}{3}x + 1, \qquad \text{entonces } \lambda = \frac{4}{3},\ \nu = 1.$$

Se sigue que

$$x_3 = \lambda^2 - x_1 - x_2 = -\frac{11}{9} \qquad \text{e} \qquad y_3 = \lambda x_3 + \nu = -\frac{17}{27}.$$

Finalmente, llegamos a

$$P_1 + P_2 = (x_3, -y_3) = \left(-\frac{11}{9}, \frac{17}{27}\right).$$

Las fórmulas que hemos dado para $P_1 + P_2$ involucran la pendiente de la recta que conecta P_1 con P_2. ¿Y si los dos puntos son iguales? Entonces no podemos usar la fórmula anterior, pero hay otra que sí podemos usar si tenemos en cuenta la recta tangente.

Proposición 1.3.2. Dado un punto $P_0 = (x_0, y_0)$ de la curva $y^2 = f(x) = x^3 + ax^2 + bx + c$, entonces $2P_0 = \left(x_1, y_1\right)$, donde

$$x_1 = \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c}, \qquad y_1 = \frac{3x_0^2 + 2ax_0 + b}{2y_0}\left(x_0 - x_1\right) - y_0.$$

Demostración. Para duplicar el punto P_0, tenemos que usar la recta tangente a la curva en P_0. De la relación $y^2 = f(x)$, encontramos por diferenciación implícita que la pendiente de la recta viene dada por

$$\lambda = \left.\frac{dy}{dx}\right|_{P_0} = \frac{f'(x_0)}{2y_0} = \frac{3x_0^2 + 2ax_0 + b}{2y_0}.$$

Así, tenemos que dicha recta es $r : y = \lambda x + \nu$ con $\nu = y_0 - \lambda x_0$. Por construcción, esta recta corta a la curva dos veces en P_0. Busquemos el tercer punto de intersección de la recta con la curva:

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

Pasándolo todo a un lado, obtenemos

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

Tenemos un polinomio cúbico, del cual sabemos que x_0 es una raíz doble. Busquemos la tercera raíz que denotaremos por x_1:

$$\begin{aligned} x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + c - \nu^2 &= (x - x_0)^2(x - x_1) \\ &= x^3 - (2x_0 + x_1)x^2 + (x_0^2 + 2x_0x_1)x - x_0^2x_1. \end{aligned}$$

Igualando los coeficientes de x^2, obtenemos $a - \lambda^2 = -(2x_0 + x_1)$. Despejando:

$$\begin{aligned} x_1 = \lambda^2 - a - 2x_0 &= \left(\frac{3x_0^2 + 2ax_0 + b}{2y_0}\right)^2 - a - 2x_0 \\ &= \frac{9x_0^4 + 12ax_0^3 + (4a^2 + 6b)x_0^2 + 4abx_0 + b^2}{4y_0^2} - a - 2x_0 \\ &= \frac{9x_0^4 + 12ax_0^3 + (4a^2 + 6b)x_0^2 + 4abx_0 + b^2}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} - a - 2x_0 \\ &= \frac{9x_0^4 + 12ax_0^3 + (4a^2 + 6b)x_0^2 + 4abx_0 + b^2 - 4ax_0^3 - 4a^2x_0^2 - 4abx_0}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} - \\ &\qquad - \frac{4ac + 8x_0^4 + 8ax_0^3 + 8bx_0^2 + 8cx_0}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \\ &= \frac{9x_0^4 + 8ax_0^3 + 6bx_0^2 + b^2 - 4ac - 8x_0^4 - 8ax_0^3 - 8bx_0^2 - 8cx_0}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \\ &= \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \end{aligned}$$

Para la coordenada y, basta sustituir x_1 en la ecuación de la recta y quedarnos con su opuesta, para que sea la suma de puntos y no la composición.

$$y_1 = \lambda x_1 + \nu = \lambda x_1 + y_0 - \lambda x_0 = y_0 + \lambda\left(x_1 - x_0\right) = y_0 + \frac{3x_0^2 + 2ax_0 + b}{2y_0}\left(x_1 - x_0\right).$$

Esta fórmula para x_1 se llama *fórmula de duplicación.*

En lo que sigue usaremos habitualmente la notación $P = (x(P), y(P))$, de uso frecuente en curvas elípticas. La fórmula de la duplicación, por ejemplo, quedaría entonces

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

Ejemplo 1.3.2. Continuando con nuestra curva de ejemplo $y^2 = x^3 - x + 1$ y el punto $P = (x_0, y_0) = (0, 1)$, usaremos las fórmulas vistas para calcular $2P$.

$$\begin{aligned} x(2P) &= \frac{x_0^4 - 2bx_0^2 - 8cx_0 + b^2 - 4ac}{4x_0^3 + 4ax_0^2 + 4bx_0 + 4c} \\ &= \frac{0^4 - 2\cdot(-1)\cdot 0^2 - 8\cdot 1\cdot 0 + (-1)^2 - 4\cdot 0\cdot 1}{4\cdot 0^3 + 4\cdot 0\cdot 0^2 + 4\cdot(-1)\cdot 0 + 4\cdot 1} = \frac{1}{4} \\ y(2P) &= \frac{3x_0^2 + 2ax_0 + b}{2y_0}\left(x_0 - x_1\right) - y_0 = \frac{3\cdot 0^2 + 2\cdot 0\cdot 0 - 1}{2\cdot 1}\left(0 - \frac{1}{4}\right) - 1 = -\frac{7}{8}. \end{aligned}$$

Por tanto, $2P = (1/4, -7/8)$.

Proposición 1.3.3. Sea $C : y^2 = f(x) = x^3 + ax^2 + bx + c$ una curva elíptica en forma Weierstrass y $P_0 = (x_0, y_0) \in C$. Una forma alternativa para la fórmula de duplicación es

$$x(2P_0) = \frac{f'(x_0)^2 - 4(a + 2x_0)f(x_0)}{4f(x_0)}.$$

Demostración. En la demostración de la Proposición 1.3.2 se vio que $x(2P_0) = \lambda^2 - a - 2x_0$, siendo $\lambda = f'(x_0)/(2y_0)$. Entonces, tenemos que:

$$\begin{aligned} x(2P_0) = \lambda^2 - a - 2x_0 &= \left(\frac{f'(x_0)}{2y_0}\right)^2 - a - 2x_0 = \frac{f'(x_0)^2}{4y_0^2} - a - 2x_0 \\ &= \frac{f'(x_0)^2}{4f(x_0)} - a - 2x_0 = \frac{f'(x_0)^2 - 4(a + 2x_0)f(x_0)}{4f(x_0)}. \end{aligned}$$

∎

Corolario 1.3.4. Sea $y^2 = f(x) = x^3 + ax^2 + bx + c$ una curva elíptica en forma Weierstrass. Entonces el numerador y el denominador de la fórmula

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

no tienen raíces comunes.

Demostración. Por definición de curva elíptica tenemos que las tres raíces de $f(x)$ son distintas. Ya se ha visto que

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

Si existiese algún valor que anule tanto el numerador como el denominador, necesariamente sería una de las tres raíces de $f(x)$. Si nos fijamos ahora en el numerador, el

segundo sumando, es decir, $4(a+2x)f(x)$, también se anularía en dicho valor. Pero como este valor hacía cero al numerador, obligatoriamente también debe ser raíz de $f'(x)$, cosa que no es posible pues si las tres raíces de $f(x)$ son distintas entonces $f(x)$ y $f'(x)$ no tienen raíces comunes.

Estas son las fórmulas básicas para la suma de puntos en una cúbica cuando está en forma de Weierstrass. Por supuesto, hay muchos casos especiales a considerar, como cuando uno de los puntos es el opuesto de otro, pero dejaremos aquí esta descripción.

1.4 El discriminante

Como siempre, tomamos nuestra curva en su forma normal,

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

donde a, b, c son números racionales. Es más, supondremos que $a, b, c \in \mathbb{Z}$ gracias a la Observación 1.2.3.

Definición 1.4.1. *Se define el discriminante de* $f(x) = x^3 + ax^2 + bx + c$ *como*

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

La fórmula más habitual se tiene cuando $a = 0$, en cuyo caso $D = -4b^3 - 27c^2$. Si factorizamos f sobre los números complejos,

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

entonces se puede comprobar que

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

De ello se deduce que $D \neq 0$ si y solo si las raíces de $f(x)$ son distintas.

Nuestro objetivo es demostrar un teorema, probado por primera vez (independientemente) por Nagell y Lutz en la década de 1930, que nos dirá cómo encontrar todos los puntos racionales de orden finito. El resultado tiene dos partes. La primera parte dice que si (x, y) es un punto racional de orden finito, entonces sus coordenadas son números enteros. La segunda parte dice que $y = 0$, en cuyo caso es un punto de orden dos, o bien $y^2 | D$, donde D es el discriminante del polinomio $f(x)$ (en un primer paso

probaremos que $y = 0$ o $y|D$). En particular, una curva cúbica tiene solo un número finito de puntos racionales de orden finito.

Por tanto, utilizando el Teorema de Nagell-Lutz, la cuestión de encontrar los puntos racionales de orden finito puede resolverse en un número finito de pasos. Se toma el número entero D y se considera cada uno de los números finitos y tales que y^2 divide a D. Se toman estos valores y se sustituyen en la ecuación $y^2 = f(x)$. El polinomio $f(x)$ tiene coeficientes enteros y coeficiente líder 1, por lo que si tiene una raíz entera, esa raíz dividirá el término constante. Por lo tanto, solo hay un número finito de posibles puntos para verificar, y de esta manera estaremos seguros de encontrar todos los puntos de orden finito en un número finito de pasos.

Observación 1.4.1. No estamos afirmando que todo punto (x, y) con coordenadas enteras y tal que $y^2|D$ deba tener un orden finito. El Teorema de Nagell-Lutz **no** es una caracterización de los puntos de orden finito (veremos un contraejemplo más adelante).

Proposición 1.4.1. Sea $f(x) \in \mathbb{Z}[x]$ mónico. Entonces el discriminante de $f(x)$ siempre estará en el ideal de $\mathbb{Z}[x]$ generado por $f(x)$ y $f'(x)$, es decir,

$$\exists r(x), s(x) \in \mathbb{Z}[x] \text{ con } D = r(x)f(x) + s(x)f'(x).$$

Demostración. Basta comprobarlo para

$$\begin{aligned} r(x) &= (18b - 6a^2)x - (4a^3 - 15ab + 27c), \\ s(x) &= (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2). \end{aligned}$$

∎

Lo importante a recordar es que hay polinomios $r(x)$ y $s(x)$ con coeficientes enteros, de modo que D se puede escribir como

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

¿Por qué queremos esta fórmula para D? Si asumimos 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, es decir, que $y = 0$ o $y|D$. Más precisamente, si P tiene orden finito, entonces claramente $2P$ también tiene orden finito, por lo que la primera parte del Teorema de Nagell-Lutz implica que tanto P como $2P$ tienen coordenadas enteras. Por tanto, la segunda parte del Teorema de Nagell-Lutz se deriva del siguiente resultado:

Lema 1.4.2. Sea $P = (x, y)$ un punto en nuestra curva cúbica tal que tanto P como $2P$ tienen coordenadas enteras. Entonces $y = 0$ o $y|D$.

Demostración. Suponemos que $y \neq 0$ y demostraremos que $y|D$. Como $y \neq 0$, sabemos[3] que $2P \neq \mathcal{O}$, por lo que podemos escribir $2P = (X, Y)$. Por hipótesis, x, y, X, Y son todos números enteros. La fórmula de duplicación dice que

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

Dado que x, X y a son todos números enteros y λ es un número racional, se deduce que λ también es un número entero. Ya que tanto $2y$ como $f'(x)$ son números enteros, vemos que $2y|f'(x)$, y en particular $y|f'(x)$. Pero $y^2 = f(x)$, entonces también $y|f(x)$. Ahora, gracias a la Proposición 1.4.1, sabemos que

$$D = r \cdot f + s \cdot f'.$$

Los coeficientes de r y s son enteros, por lo que ambos polinomios toman valores enteros cuando se evalúan en $x \in \mathbb{Z}$. De ello se deduce que y divide a D. ∎

[3] Esta afirmación se demuestra en el Teorema 2.1.1.

2 Puntos de Orden Finito

2.1 Puntos de orden dos y tres

Definición 2.1.1. *Se dice que un elemento P de un grupo aditivo con elemento neutro $\mathcal{O}$ tiene orden m si*

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

pero $m'P \neq \mathcal{O}$ para todos los enteros $1 \leq m' < m$. Si tal m existe, entonces P tiene orden finito, de lo contrario tiene orden infinito.

Comenzamos nuestro estudio de puntos de orden finito en curvas cúbicas observando puntos de orden dos y tres. Durante todo el capítulo tomaremos el punto en el infinito $\mathcal{O}$ como el elemento neutro de la operación de grupo.

Teorema 2.1.1 (Puntos de orden dos y tres). *Sea C una curva elíptica en forma normal de Weierstrass*

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

(a) Un punto $P = (x, y) \neq \mathcal{O}$ en C tiene orden dos si y solo si $y = 0$.

(b) La curva C tiene exactamente cuatro puntos con coordenadas en $\mathbb{C}$ de orden que divide a dos. Estos cuatro puntos forman un grupo que es producto de dos grupos cíclicos de orden dos.

(c) Un punto $P = (x, y) \neq \mathcal{O}$ en C tiene orden tres si y solo si x es una raíz del polinomio

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

(d) La curva C tiene exactamente nueve puntos con coordenadas en $\mathbb{C}$ de orden que divide a tres. Estos nueve puntos forman un grupo que es producto de dos grupos cíclicos de orden tres.

Demostración.

(a) Buscamos los puntos de nuestro grupo que satisfacen $2P = \mathcal{O}$, pero $P \neq \mathcal{O}$. En lugar de $2P = \mathcal{O}$, es más fácil observar la condición equivalente $P = -P$. Dado que $-(x, y) = (x, -y)$, esto se da si y solo si $y = 0$.

(b) Es claro que los puntos de orden 2 son

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

donde $\alpha_1, \alpha_2, \alpha_3$ son las raíces (complejas) del polinomio cúbico $f(x)$. Entonces, si permitimos coordenadas complejas, hay exactamente tres puntos de orden dos, porque la no singularidad de la curva asegura que $f(x)$ tenga raíces distintas. Si las tres raíces de $f(x)$ son reales, entonces la imagen se parece a la Figura 2.1.

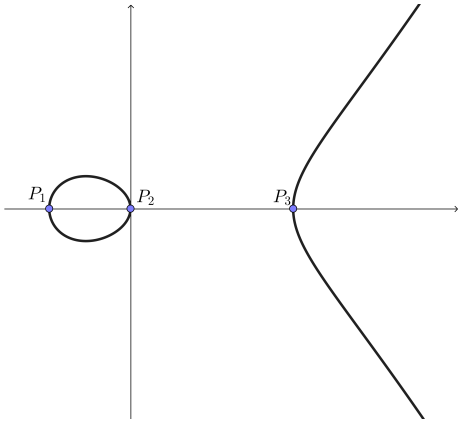

Figura 2.1: Puntos de orden dos.

Si tomamos todos los puntos que satisfacen $2P = \mathcal{O}$, incluido $P = \mathcal{O}$, obtenemos el conjunto $\{\mathcal{O}, P_1, P_2, P_3\}$. Se ve fácilmente que en cualquier grupo abeliano, el conjunto de soluciones de la ecuación $2P = \mathcal{O}$ forma un subgrupo (de manera más general, para cualquier m, el conjunto de soluciones de $mP = \mathcal{O}$ forma un subgrupo). Así que tenemos un grupo abeliano de orden cuatro, y dado que cada elemento tiene orden uno o dos, está claro que este grupo es el *grupo de Klein*, es decir, un producto directo de dos grupos de orden dos. Esto significa que la suma de dos puntos cualesquiera P_1, P_2, P_3 debe ser igual al tercero, lo cual es obvio por el hecho de que los tres puntos son colineales.

(c) En lugar de $3P = \mathcal{O}$, escribimos $2P = -P$, por lo que un punto de orden tres satisfará $x(2P) = x(-P) = x(P)$. Recíprocamente, si $P \neq \mathcal{O}$ satisface $x(2P) = x(P)$, entonces $2P = \pm P$, por lo que $P = \mathcal{O}$ (excluido por suposición)

o $3P = \mathcal{O}$. En otras palabras, los puntos de orden tres son exactamente los puntos que satisfacen $x(2P) = x(P)$.
Para encontrar los puntos que satisfacen esta condición, usamos la fórmula de duplicación e imponemos que la coordenada x de $2P$ sea igual a la coordenada x de P. Si escribimos $P = (x, y)$ y usamos la fórmula de la duplicación, obtenemos

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

$$4x^4 + 4ax^3 + 4bx^2 + 4cx = x^4 - 2bx^2 - 8cx + b^2 - 4ac$$

$$3x^4 + 4ax^3 + 6bx^2 + 12cx - b^2 + 4ac = 0$$

Por tanto, x es raíz del polinomio $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$.

(d) Dado que

$$x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x,$$

vemos que una expresión alternativa para $\psi_3(x)$ es

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

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

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

entonces una raíz común de $\psi_3(x)$ y $\psi_3'(x)$ sería una raíz común de $2f(x)f''(x) - f'(x)^2$ y de $12f(x)$, y así sería una raíz común de $f(x)$ y $f'(x)$. Esto contradice nuestra suposición de que C no es singular. Concluimos que $\psi_3(x)$ de hecho tiene cuatro raíces complejas distintas.
Sean $\beta_1, \beta_2, \beta_3, \beta_4$ las cuatro raíces complejas de $\psi_3(x)$, y para cada β_i, sea δ_i una de las raíces cuadradas $\delta_i = \sqrt{f(\beta_i)}$. Por (c), el conjunto

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

es el conjunto completo de puntos de orden tres en C. Además, observamos que ningún δ_i puede ser igual a cero, porque de lo contrario el punto $(\beta_i, \delta_i) = (\beta_i, 0)$ tendría orden dos, contradiciendo el hecho de que tiene orden tres. Por lo tanto, el conjunto contiene ocho puntos distintos, por lo que C contiene ocho puntos de orden tres. El único otro punto en C con orden que divide a tres es el punto de orden uno, a saber, $\mathcal{O}$, que completa la prueba de que C tiene exactamente nueve puntos de orden que dividen a tres.

Finalmente, observamos que solo hay un grupo (abeliano) con nueve elementos, de modo que cada elemento tiene un orden que divide a tres y no es otro que el producto de dos grupos cíclicos de orden tres.

Ejemplo 2.1.1. Para la curva particular $y^2 = x^3 + 1$, vamos a encontrar todos los puntos que satisfagan $3P = \mathcal{O}$. En este caso, el polinomio es $g(x) = 3x^4 + 12x = 3x(x^3 + 4)$. Del segundo factor obtenemos:

$$x^3 + 4 = 0 \Rightarrow x = \sqrt[3]{-4} = \sqrt[3]{4}\sqrt[3]{-1}.$$

Por tanto, concluimos que las raíces de g son

$$x_1 = 0, \quad x_2 = -\sqrt[3]{4}, \quad x_3 = \frac{\sqrt[3]{4}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}i, \quad x_4 = \frac{\sqrt[3]{4}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}i.$$

Para cada una de estas coordenadas de x obtenemos dos valores posibles para la coordenada y. Como $y^2 = x^3 + 1$, tenemos que $y = \pm\sqrt{x^3 + 1}$.

$$y_{11} = -\sqrt{x_1^3 + 1} = -\sqrt{0^3 + 1} = -1.$$
$$y_{12} = \sqrt{x_1^3 + 1} = \sqrt{0^3 + 1} = 1.$$
$$y_{21} = -\sqrt{x_2^3 + 1} = -\sqrt{\left(-\sqrt[3]{4}\right)^3 + 1} = -\sqrt{-4 + 1} = -\sqrt{-3} = -\sqrt{3}i.$$
$$y_{22} = \sqrt{x_2^3 + 1} = \sqrt{\left(-\sqrt[3]{4}\right)^3 + 1} = \sqrt{-4 + 1} = \sqrt{-3} = \sqrt{3}i.$$
$$y_{31} = -\sqrt{x_3^3 + 1} = -\sqrt{\left(\frac{\sqrt[3]{4}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}i\right)^3 + 1} = -\sqrt{-4 + 1} = -\sqrt{3}i.$$
$$y_{32} = \sqrt{x_3^3 + 1} = \sqrt{\left(\frac{\sqrt[3]{4}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}i\right)^3 + 1} = \sqrt{-4 + 1} = \sqrt{-3} = \sqrt{3}i.$$
$$y_{41} = -\sqrt{x_4^3 + 1} = -\sqrt{\left(\frac{\sqrt[3]{4}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}i\right)^3 + 1} = -\sqrt{-4 + 1} = -\sqrt{3}i.$$

$$y_{42} = \sqrt{x_4^3 + 1} = \sqrt{\left(\frac{\sqrt[3]{4}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}i\right)^3 + 1} = \sqrt{-4+1} = \sqrt{-3} = \sqrt{3}i.$$

Por tanto, los puntos que satisfacen $3P = \mathcal{O}$ son

$$\left\{\mathcal{O},\ (0,-1),\ (0,1),\ \left(-\sqrt[3]{4}, -\sqrt{3}i\right),\ \left(-\sqrt[3]{4}, \sqrt{3}i\right),\ \left(\frac{\sqrt[3]{4}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}i, -\sqrt{3}i\right),\right.$$

$$\left.\left(\frac{\sqrt[3]{4}}{2} + \frac{\sqrt{3}\sqrt[3]{4}}{2}i, \sqrt{3}i\right),\left(\frac{\sqrt[3]{4}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}i, -\sqrt{3}i\right),\left(\frac{\sqrt[3]{4}}{2} - \frac{\sqrt{3}\sqrt[3]{4}}{2}i, \sqrt{3}i\right)\right\}.$$

Ahora sabemos exactamente cómo es el grupo de puntos P tal que $2P = \mathcal{O}$. Si permitimos coordenadas complejas, es el grupo de Klein. Si permitimos solo coordenadas reales, es el grupo de Klein o un grupo cíclico de orden dos, dependiendo de si $f(x)$ tiene tres raíces reales o una raíz real. Y si restringimos la atención a puntos con coordenadas racionales, hay tres posibilidades, es el grupo de Klein, es cíclico de orden dos, o es trivial, dependiendo de si $f(x)$ tiene tres, una o cero raíces racionales.

Además, sabemos que si permitimos números complejos, los puntos de orden que dividen a tres forman un grupo de orden nueve que es el producto directo de dos grupos cíclicos de orden tres. Los puntos reales de orden tres siempre forman un grupo cíclico de orden tres o el grupo trivial, aunque no veremos este resultado con detalle [5].

También hay una forma geométrica curiosa de describir los puntos de orden tres. Son los puntos de inflexión en C, es decir, los puntos donde la recta tangente a la cúbica tiene un contacto de triple orden. Podemos ver esto geométricamente. La condición $2P = -P$ significa que cuando dibujamos la tangente en el punto P, luego tomamos el tercer punto de intersección y lo conectamos con $\mathcal{O}$, obtenemos $-P$. Ahora, ese es el caso solo si la tercera intersección de la tangente en P es el mismo punto P. Entonces $2P = -P$ si y solo si P es un punto de inflexión. Por supuesto, esto también se puede mostrar analíticamente.

2.2 Los puntos de orden finito tienen coordenadas enteras

Ahora llegamos 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. Demostraremos que x e y son números enteros de una manera bastante indirecta. Observamos que una forma de demostrar que un entero positivo es igual a 1 es demostrar que no es divisible por ningún número primo. Por lo tanto, podemos dividir el problema en un número infinito de subproblemas, es decir, mostramos que cuando los números racionales x e y se escriben en términos mínimos, sus denominadores no son divisibles por 2, y no son divisibles por 3, y no son divisible por 5, y así sucesivamente.

Así que se considera un primo p y tratamos de demostrar que p no divide ni al denominador de x ni al de y. Eso nos lleva de forma natural a considerar el conjunto de puntos racionales (x, y) donde p divide el denominador de x o y.

Será útil establecer alguna notación. Para cada primo p, todo número racional distinto de cero puede escribirse de forma única en la forma $(m/n)p^v$, donde m y n son números enteros que son primos con p, $n \geq 1$, la fracción m/n está en forma irreducible y $v \in \mathbb{Z}$.

Definición 2.2.1. *Para cada primo p, se define el orden respecto a p de cualquier número racional $(m/n)p^v$ como el exponente v, lo cual se denota como*

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

A menos que haya riesgo de confusión, omitiremos respecto a qué primo p nos referimos en el orden.

Decir que p divide al denominador de un número racional es lo mismo que decir que su orden es negativo, y de manera similar decir que p divide al numerador de un número racional es lo mismo que decir que su orden es positivo. El orden de un número racional es cero si y solo si p no divide ni a su numerador ni a su denominador.

Proposición 2.2.1. Dado un punto racional $(x, y) \in C : y^2 = x^3 + ax^2 + bx + c$ y un primo p, si p divide al denominador de x o al denominador de y entonces divide al denominador de ambos.

Más concretamente, la potencia exacta que divide al denominador es p^{2v} para x y p^{3v} para y, para algún entero positivo v.

Demostración. Vamos a asumir que p divide el denominador de x. Por lo tanto,

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

donde $\mu > 0$ y p no divide a m, n, u ni w. Si ponemos este punto en la ecuación de nuestra cúbica, al poner todo sobre un denominador común, tenemos que

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

Sabemos que $p \nmid u^2$ y $p \nmid w^2$, por lo que

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

Además, dado que $\mu > 0$ y $p \nmid m$, se sigue que

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

y por lo tanto

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

Entonces $2\sigma = 3\mu$. En particular, $\sigma > 0$, por lo que p divide al denominador de y. Además, la relación $2\sigma = 3\mu$ significa que $2|\mu$ y $3|\sigma$, por lo que se tiene que $\mu = 2\nu$ y $\sigma = 3\nu$ para algún número entero $\nu > 0$.

De manera similar, si asumimos que p divide al denominador de y, obtenemos mediante el mismo cálculo que se cumple exactamente el mismo resultado, es decir, que $\mu = 2\nu$ y $\sigma = 3\nu$ para algún número entero $\nu > 0$. ∎

Esto sugiere que hagamos la siguiente definición:

Definición 2.2.2. *Se define $C(p^{\nu})$ como el conjunto de puntos racionales (x, y) de la curva cúbica de manera que $p^{2\nu}$ divide al denominador de x y $p^{3\nu}$ divide al denominador de y, junto con el punto $\mathcal{O}$. En otras palabras,*

$$C(p^{\nu}) = \left\{(x, y) \in C(\mathbb{Q}) \;\middle|\; \operatorname{ord}(x) \leq -2\nu,\ \operatorname{ord}(y) \leq -3\nu\right\} \cup \{\mathcal{O}\}.$$

Ejemplo 2.2.1. $C(p)$ es el conjunto donde p aparece en el denominador de x e y, luego hay al menos un p^2 en el denominador de x y un p^3 en el de y. Obviamente, tenemos las inclusiones

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

Recordemos que nuestro objetivo es mostrar que si (x, y) es un punto de orden finito, entonces x e y son números enteros, y nuestra estrategia es mostrar que para cada primo p, los denominadores de x e y no son divisibles por p. Con nuestra nueva notación, esto significa que queremos mostrar que un punto de orden finito no puede estar en $C(p)$. El primer paso para mostrar esto es demostrar que cada uno de los conjuntos $C(p^\nu)$ es un subgrupo de $C(\mathbb{Q})$.

Si el lector conoce los números p-ádicos verá que tiene sentido considerar esta cadena descendente de subgrupos. Una potencia alta de p en el denominador significa, en el sentido p-ádico, que el número es muy grande (en norma). A medida que bajamos por la cadena de subgrupos $C(p^\nu)$, encontramos puntos (x, y) con coordenadas cada vez mayores en el sentido p-ádico. Estos son puntos que se están acercando cada vez más al infinito y, por lo tanto, cada vez más cerca del elemento neutro de nuestro grupo. Los $C(p^\nu)$ son entornos de $\mathcal{O}$ en la topología p-ádica. Todo este comentario es solo a modo de motivación, en realidad no necesitaremos saber nada sobre los números p-ádicos para la prueba.

Primero vamos a cambiar las coordenadas y mover el punto en el infinito a un lugar finito. Sean

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

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

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

en el plano (t, s). Siempre podemos recuperar las coordenadas antiguas, por supuesto, porque $y = 1/s$ y $x = t/s$. En el plano (t, s), tenemos todos los puntos del antiguo plano (x, y) excepto los puntos donde $y = 0$, y el elemento neutro $\mathcal{O}$ de nuestra curva está ahora en el origen $(0, 0)$ del plano (t, s).

Puede visualizar la situación de esta manera. Tenemos dos vistas de la curva. La vista en el plano (x, y) nos muestra todo excepto $\mathcal{O}$. La vista en el plano (t, s) nos muestra $\mathcal{O}$ y todos los demás puntos, excepto los de orden dos. Aparte de $\mathcal{O}$ 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); ver la Figura 2.2.

Además, una recta $y = \lambda x + \nu$ en el plano (x, y) corresponde a una recta en el plano (t, s). Es decir, si dividimos $y = \lambda x + \nu$ por νy, obtenemos

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

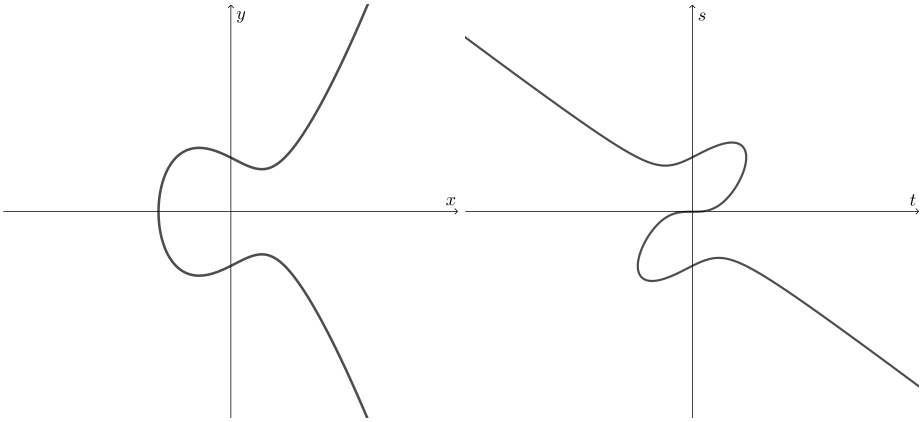

Figura 2.2: Dos vistas de una curva cúbica.

Por tanto, podemos sumar puntos en el plano (t, s) mediante el mismo procedimiento que en el plano (x, y). Necesitamos encontrar fórmulas explícitas.

Es conveniente trabajar en un cierto anillo:

Definición 2.2.3. *Se define el anillo R, o R_p si queremos enfatizar que depende de p, como el conjunto de todos los números racionales tales que p no divide al denominador, es decir,*

$$R = \left\{ \frac{m}{n} \in \mathbb{Q} \;\middle|\; m \text{ y } n \text{ coprimos}, p \nmid n \right\}.$$

Observación 2.2.1. R es un anillo ya que si α y β son números racionales tales que p no divide a sus denominadores, entonces lo mismo ocurre con $\alpha \pm \beta$ y $\alpha\beta$.

Observación 2.2.2. Otra forma de describir R es decir que consta de cero junto con todos los números racionales distintos de cero tales que $\mathrm{ord}_p(x) \geq 0$, o si hacemos la convención de que $\mathrm{ord}_p(0) = \infty$, entonces

$$R = \left\{ \alpha \in \mathbb{Q} \;\middle|\; \mathrm{ord}(\alpha) \geq 0 \right\}.$$

Proposición 2.2.2. El anillo R es un subanillo del cuerpo de los números racionales. Además, es un DFU y un anillo local[1], cuyo ideal maximal es el ideal generado por p. Las unidades en R son solo números racionales de orden cero, es decir, números racionales con numerador y denominador primos con p.

Veamos la divisibilidad de nuestras nuevas coordenadas s y t por potencias de p.

[1]Esto significa que tiene un solo ideal maximal.

Proposición 2.2.3. Sea $(x, y) \in C(p^\nu)$. Si nos fijamos en el punto correspondiente en el plano (t, s), entonces p^ν divide al numerador de t y $p^{3\nu}$ divide al numerador de s.

Demostración. Si (x, y) se encuentra en $C(p^\nu)$, lo podemos escribir como

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

para algún $\iota \geq 0$. Entonces

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

Por lo tanto, 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 es, p^ν divide al numerador de t y $p^{3\nu}$ divide al numerador de s. ∎

Para probar que los $C(p^\nu)$ son subgrupos, tenemos que sumar puntos y demostrar que si una determinada potencia de p divide la coordenada t de dos puntos, entonces esa potencia de p divide la coordenada t de su suma. Esto es solo una cuestión de escribir las fórmulas:

Proposición 2.2.4. Sean $C : s = t^3 + at^2s + bts^2 + cs^3$ una curva elíptica y $P_1, P_2 \in C(p^\nu)$. Entonces las coordenadas t de $P_1 + P_2$ y de $-P_1$ también se encuentran en $p^\nu R$.

Demostración. Sean $P_1 = (t_1, s_1)$ y $P_2 = (t_2, s_2)$ puntos distintos en $C(p^\nu)$. Si $t_1 = t_2$, entonces la recta vertical $t = t_1$ corta a C en P_1, P_2 y un tercer punto $P_3 = (t_1, s_3)$, donde P_3 puede ser igual a P_1 o P_2. Entonces $P_1 + P_2 = (-t_1, -s_3)$, por lo que la coordenada t de $P_1 + P_2$ está en $p^\nu R$, lo que muestra que $P_1 + P_2 \in C(p^\nu)$.

Entonces nos reducimos a estudiar el caso de que $t_1 \neq t_2$. Sea $s = \alpha t + \beta$ la recta que pasa por P_1 y P_2. La pendiente α de esta recta está dada por

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

Podemos reescribir esto de la siguiente manera. Los puntos (t_1, s_1) y (t_2, s_2) satisfacen la ecuación

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

Restamos la ecuación de P_1 de la ecuación de P_2 y factorizaramos:

$$s_2 - s_1 = (t_2^3 - t_1^3) + a(t_2^2 s_2 - t_1^2 s_1) + b(t_2 s_2^2 - t_1 s_1^2) + c(s_2^3 - s_1^3) =$$

$$= (t_2^3 - t_1^3) + a\left((t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)\right) + b\left((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)\right) + c(s_2^3 - s_1^3).$$

Algunos de los términos son divisibles por $s_2 - s_1$, y algunos de los términos son divisibles por $t_2 - t_1$. Factorizando estas cantidades, podemos expresar su razón en términos de lo que queda, llegando (después de algunos cálculos) a

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 + t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}. \tag{2.1}$$

El objetivo de todo esto, como veremos, era obtener el 1 en el denominador de α, por lo que el denominador de α será una unidad en R.

De manera similar, si $P_1 = P_2$, entonces la pendiente de la recta tangente a C en P_1 es

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

Observe que esta es la misma pendiente que obtenemos si sustituimos $t_2 = t_1$ y $s_2 = s_1$ en el lado derecho de 2.1. Entonces podemos usar 2.1 en todos los casos.

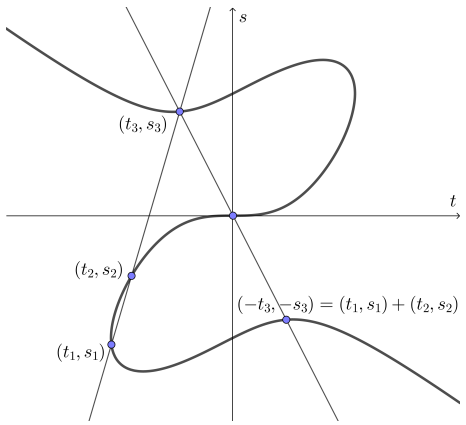

Figura 2.3: Sumando puntos en el plano (t, s).

Sea $P_3 = (t_3, s_3)$ el tercer punto de intersección de la recta $s = \alpha t + \beta$ con la curva; vea la Figura 2.3. 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,

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

Multiplicando esto y agrupando potencias de t obtenemos

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

Esta ecuación tiene raíces t_1, t_2, t_3, por lo que el lado derecho es igual a

$$(\text{constante}) \cdot (t - t_1)(t - t_2)(t - t_3).$$

Comparando los coeficientes de t^3 y t^2, obtenemos que la suma de las raíces es

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

Estas son todas las fórmulas que necesitaremos excepto la trivial

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

diciendo que la recta pasa por P_1.

Ahora que tenemos una fórmula para t_3, ¿cómo encontramos $P_1 + P_2$? Dibujamos la recta que pasa por (t_3, s_3) y el elemento neutro $(0, 0)$ y tomamos el tercer punto de intersección con la curva. De la ecuación de la curva se desprende de inmediato que si (t, s) está en la curva, entonces también lo está $(-t, -s)$. Entonces, el tercer punto de intersección es $(-t_3, -s_3)$.

Veamos más de cerca la expresión de α. El numerador de α se encuentra en $p^{2\nu}R$, porque cada uno de t_1, s_1, t_2, s_2 está en $p^\nu R$. Por la misma razón, la cantidad

$$-at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)$$

está en $p^{2\nu}R$, y en consecuencia el denominador de α es una unidad en R (para esto necesitamos el 1 en el denominador). De ello se deduce que $\alpha \in p^{2\nu}R$.

A continuación, dado 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. Mirando la expresión para $t_1 + t_2 + t_3$ dada arriba, tenemos

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

Dado que $t_1, t_2 \in p^\nu R$, se sigue que $t_3 \in p^\nu R$, y por lo tanto también que $-t_3 \in p^\nu R$.

Por último, si la coordenada t de $P = (t, s)$ se encuentra en $p^\nu R$, entonces está claro que la coordenada t de $-P = (-t, -s)$ también se encuentra en $p^\nu R$. ∎

Corolario 2.2.5. $C(p^\nu)$ es un subgrupo de $C(\mathbb{Q})$.

Demostración. En la proposición anterior se ha demostrado que $C(p^\nu)$ es cerrado para la suma y para el cálculo de opuestos, por lo que es un subgrupo de $C(\mathbb{Q})$.

Observación 2.2.3. De hecho, hemos probado algo un poco más fuerte. Hemos demostrado que si $P_1, P_2 \in C(p^\nu)$, entonces

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

Aquí estamos escribiendo $t(P)$ para denotar la coordenada t de P, esto es, $t(P) = x(P)/y(P)$.

Esta última fórmula nos dice más que el mero hecho de que $C(p^\nu)$ es un subgrupo de $C(\mathbb{Q})$. Una forma más sugerente de escribirlo es

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

Téngase en cuenta que la suma en $P_1 + P_2$ es la suma en nuestra curva cúbica, que viene dada por fórmulas bastante complicadas, mientras que la suma en $t(P_1)+t(P_2)$ es la suma en R, que es solo la suma de números racionales. Así que la aplicación $P \mapsto t(P)$ es prácticamente un homomorfismo de $C(p^\nu)$ en el grupo aditivo de números racionales. No define del todo un homomorfismo, porque $t(P_1 + P_2)$ no es realmente igual a $t(P_1) + t(P_2)$. Sin embargo, lo que sí obtenemos es un homomorfismo de $C(p^\nu)$ al grupo cociente $p^\nu R/p^{3\nu} R$ enviando P a la clase de congruencia de $t(P)$, y el núcleo de este homomorfismo consta de todos los puntos P con $t(P) \in p^{3\nu} R$. Por lo tanto, el núcleo es $C(p^{3\nu})$, por lo que finalmente obtenemos un homomorfismo inyectivo

$$\begin{aligned} C(p^\nu)/C(p^{3\nu}) &\longrightarrow p^\nu R/p^{3\nu} R \\ P = (x, y) &\longmapsto t(P) = x/y \end{aligned}$$

No es difícil ver que el grupo cociente $p^\nu R/p^{3\nu} R$ es un grupo cíclico de orden $p^{2\nu}$. De ello se deduce que el grupo cociente $C(p^\nu)/C(p^{3\nu})$ es un grupo cíclico de orden p^σ para algún $0 \le \sigma \le 2\nu$.

Resumimos nuestros resultados hasta ahora en la siguiente proposición:

Proposición 2.2.6. Sea p un primo, sea R el anillo de números racionales con denominador primo con p, y sea $C(p^\nu)$ el conjunto de puntos racionales (x, y) en nuestra curva para los cuales x tiene denominador divisible por $p^{2\nu}$, junto con el punto $\mathcal{O}$.

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

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

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

es un homomorfismo inyectivo (por convenio, enviamos $\mathcal{O} \mapsto 0$).

Usando esta proposición, no es difícil probar nuestra afirmación de que los puntos de orden finito tienen coordenadas enteras:

Corolario 2.2.7. (a) Para todo primo p, el único punto de orden finito en el grupo $C(p)$ es el punto identidad $\mathcal{O}$.
(b) Sea $P = (x, y) \in C(\mathbb{Q})$ un punto racional de orden finito. Entonces x e y son números enteros.

Demostración. Sea $P \in C(\mathbb{Q})$ un punto de orden m con $m \geq 2$. Necesitamos demostrar que $P \notin C(p)$ para todo primo p.

Por reducción al absurdo, supongamos que $P \in C(p)$ para algún p. El punto $P = (x, y)$ puede estar contenido en un grupo $C(p^\nu)$ más pequeño, pero no puede estar contenido en todos los grupos $C(p^\nu)$, porque el denominador de x no puede ser divisible por potencias arbitrariamente altas de p. Entonces podemos encontrar algún $\nu > 0$ de modo que $P \in C(p^\nu)$ y $P \notin C(p^{\nu+1})$, específicamente $\nu = -\operatorname{ord}(x)/2$. Se pueden dar dos casos, dependiendo de si m es divisible por p.

Supongamos primero que $p \nmid m$. Repitiendo la aplicación de la congruencia

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

se obtiene la fórmula

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

Como $mP = \mathcal{O}$, tenemos $t(mP) = t(\mathcal{O}) = 0$. Por otro lado, dado que m es primo con p, es una unidad en R. Por lo tanto

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

Esto significa que $P \in C(p^{3\nu})$, lo que contradice el hecho de que $P \notin C(p^{\nu+1})$.

A continuación, suponemos que $p|m$. La prueba en este caso es similar. Primero, escribimos $m = pn$ y miramos el punto $P' = nP$. Dado que P tiene orden m, está

claro que P' tiene orden p. Además, dado que $P \in C(p)$ y $C(p)$ es un subgrupo de $C(\mathbb{Q})$, vemos que $P' \in C(p)$. Escribiendo $P' = (x', y')$, consideramos $\nu = -\operatorname{ord}(x')/2$. Entonces $P' \in C(p^\nu)$ y $P' \notin C(p^{\nu+1})$ y, al igual que antes, encontramos que

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

Esto significa que

$$t(P') \equiv 0 \pmod{p^{3\nu-1}R}.$$

Dado que $3\nu - 1 \geq \nu + 1$, esto contradice el hecho de que $P' \notin C(p^{\nu+1})$, lo que completa la demostración del apartado (a) del corolario.

Pero ahora la parte (b) es fácil, porque si $P = (x, y)$ es un punto de orden finito, entonces sabemos por (a) que $P \notin C(p)$ para todos los primos p. Esto significa que los denominadores de x e y no son divisibles por números primos y, por lo tanto, x e y son números enteros.

2.3 El Teorema de Nagell-Lutz y más resultados

Realmente hemos terminado la demostración del Teorema de Nagell-Lutz, pero para resumir todo lo expresaremos formalmente y recordaremos las dos partes de la demostración.

Teorema 2.3.1 (Nagell-Lutz). *Sea*

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

una curva cúbica elíptica con coeficientes enteros a, b, c, y sea D el discriminante del polinomio cúbico,

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

Sea $P = (x, y)$ un punto racional de orden finito. Entonces x e y son números enteros. Además, o bien $y = 0$, en cuyo caso P tiene orden dos, o bien y divide a D.

Demostración. En el Corolario 2.2.7 mostramos que un punto de orden finito tiene coordenadas enteras. Si P tiene orden dos, entonces sabemos por el Teorema 2.1.1 que $y = 0$, así que hemos terminado. De lo contrario, $2P \neq \mathcal{O}$. Pero $2P$ también es un punto de orden finito, por lo que también tiene coordenadas enteras. En el Lema 1.4.2 mostramos que si tanto $P = (x, y)$ como $2P$ tienen coordenadas enteras, entonces y divide a D, lo que completa la demostración del teorema de Nagell-Lutz.

Para propósitos computacionales, existe una forma más fuerte del Teorema de Nagell-Lutz que a menudo es útil:

Corolario 2.3.2 (Forma fuerte del Teorema de Nagell-Lutz). En las condiciones anteriores, si $P = (x, y)$ es un punto racional de orden finito distinto de dos, entonces $y^2 | D$.

Demostración. Demostramos en la Proposición 1.3.2 que si $P = (x, y)$ es un punto en la cúbica, entonces la coordenada x de $2P$ viene dada por la fórmula de duplicación

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4f(x)}.$$

Denotemos $\phi(x) = x^4 - 2bx^2 - 8cx + b^2 - 4ac$. Considerando $F(x) = 3x^3 - ax^2 - 5bx + 2ab - 27c$ y $\Phi(x) = -3x^2 - 2ax - 4b - a^2$, se puede comprobar que

$$F(X)f(X) + \Phi(X)\phi(X) = D.$$

Despejando de la fórmula de duplicación, obtenemos que $\phi(x) = 4f(x)x(2P)$, y como $y^2 = f(x)$, tenemos que $\phi(x) = 4x(2P)y$. Usando la relación de F y Φ, la expresión anterior de $\phi(x)$ y usando de nuevo que $y^2 = f(x)$, llegamos a

$$F(X)y^2 + 4\Phi(X)x(2P)y^2 = (F(X) + 4\Phi(X)x(2P))y^2 = D,$$

y por tanto $y^2 | D$. ∎

Observación 2.3.1. Queremos reiterar que el Teorema de Nagell-Lutz no es un enunciado "si y sólo si". Es muy posible tener puntos (x, y) con coordenadas enteras y tales que $y | D$ pero que no sean puntos de orden finito. El Teorema de Nagell-Lutz se puede usar para compilar una lista de puntos que incluya todos los puntos de orden finito, pero nunca se puede usar para demostrar que un punto en particular realmente tiene un orden finito. Para verificar que un punto P tiene orden finito, se debe encontrar un número entero $n \geq 1$ tal que $nP = \mathcal{O}$.

En particular, en el apéndice demostraremos que el punto $(1, 3)$, perteneciente a la curva $C : y^2 = x^3 + 8$, que tiene como discriminante $D = 1728$, es de orden infinito.

Por otro lado, el Teorema de Nagell-Lutz a menudo se puede utilizar para demostrar que un punto dado tiene un orden *infinito*. La idea es calcular $P, 2P, 3P, \ldots$ hasta que se llega a un múltiplo nP cuyas coordenadas no son números enteros. Entonces se sabe que nP, y a fortiori también P, no pueden tener un orden finito. Este cálculo se puede acelerar calculando en cambio solo las coordenadas x de $2P, 4P, 8P, \ldots$ aplicando repetidamente la fórmula de duplicación hasta que alguna coordenada x no sea un número entero.

Naturalmente, surge la pregunta de qué ordenes (finitos) pueden ocurrir en una curva elíptica. Ya hemos visto que es fácil obtener puntos de orden dos tomando el polinomio cúbico para tener una raíz racional. De manera similar, usando nuestra descripción de los puntos de orden tres, no es difícil encontrar curvas cúbicas tales que $C(\mathbb{Q})$ tenga un punto de orden tres.

Es posible, de hecho, encontrar puntos individuales de orden superior, como se ilustra en el siguiente ejemplo:

Ejemplo 2.3.1. El punto $P = (1, 1)$ en la curva

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

tiene orden cuatro, ya que uno verifica fácilmente que $2P = (0, 0)$, y sabemos que $(0, 0)$ tiene orden dos. Entonces $3P = -P = (1, -1)$ también es un punto de orden cuatro. También notamos que las otras dos raíces de $x^3 - x^2 + x$ son complejas, por lo que el único punto de orden dos es $(0, 0)$.

Podemos usar el teorema de Nagell-Lutz para comprobar que no hay otros puntos de orden finito en esta curva. El discriminante es $D = -3$, por lo que los únicos valores posibles para y son ± 1 y ± 3. Ya sabemos que $y = \pm 1$ da puntos de orden cuatro, por lo que verificamos $y = \pm 3$. Esto conduce a la ecuación $x^3 - x^2 + x - 9 = 0$. Las únicas raíces racionales posibles son los números enteros que dividen a 9, y se comprueba rápidamente que ± 1, ± 3 y ± 9 no son raíces. Entonces, los únicos puntos de orden finito son los que conocemos, y el subgrupo de puntos de orden finito es un grupo cíclico de orden cuatro.

De hecho, hay infinitas curvas con un punto racional de orden cuatro. Para todo número racional t excepto $t = 0$ y $t = 1/4$, el punto (t, t) en la curva cúbica no singular

$$y^2 = x^3 - (2t - 1)x^2 + t^2 x$$

es un punto de orden cuatro.

De manera similar, se pueden escribir infinitos ejemplos de curvas con puntos racionales de orden 5, 6, 7, 8, 9, 10 y 12. En esencia, estos ejemplos se escribieron durante la segunda mitad del siglo XIX. Pero nadie pudo encontrar ni un solo ejemplo de una curva cúbica con un punto racional de orden 11. Hay una buena razón para esto, porque Billing y Mahler demostraron en 1940 que no existe tal curva.

Mucha gente trabajó en el problema de determinar qué órdenes son posibles, culminando en la década de 1970 con un teorema muy hermoso y muy difícil, el teorema

de Mazur. Ni siquiera podremos indicar la estrategia de la prueba, pero el enunciado, que es fácil de entender, es el siguiente [3]:

Teorema 2.3.3 (Mazur). *Sea C una curva cúbica racional no singular y supongamos que $C(\mathbb{Q})$ contiene un punto de orden finito m. Entonces*

$$1 \leq m \leq 10 \quad o \quad m = 12.$$

Más precisamente, el conjunto de puntos de orden finito en $C(\mathbb{Q})$ forma un subgrupo que tiene una de las siguientes formas:

(i) Un grupo cíclico de orden N con $1 \leq N \leq 10$ o $N = 12$.
(ii) El producto de un grupo cíclico de orden dos y un grupo cíclico de orden $2N$ con $1 \leq N \leq 4$.

Apéndice: Algunos Cálculos Explícitos

Como aplicación de los teoremas de Nagell-Lutz y Mazur, resolveremos el ejercicio 2.12 de [5]. Para ello, tendremos en cuenta algunos aspectos de las curvas elípticas y de su grupo de puntos racionales:

- Para poder usar el Teorema de Nagell-Lutz, necesitamos que la curva venga dada en forma normal de Weierstrass. Si esto no ocurriese, necesitamos transformarla, estudiar su transformada, y luego deshacer la transformación.
- Dado un punto $P = (x, y)$ del grupo de puntos racionales de una curva elíptica, por ser un grupo, tiene opuesto. Si la curva viene dada en forma normal de Weierstrass, sabemos que esta es simétrica respecto al eje x, y el opuesto de P no es más que $-P = (x, -y)$. Sabemos que el orden de $-P$ es el mismo que el de P, es decir, $\text{ord}(P) = \text{ord}(-P)$, por lo que para saber el orden de $-P$ bastará conocer el orden de P.

El enunciado del problema es el siguiente:

2.12. Para cada una de las siguientes curvas, determine los puntos de orden finito. También determina la estructura del grupo formado por los puntos de orden finito.

(a) $\boxed{y^2 = x^3 - 2}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 2$ son

$$x_1 = \sqrt[3]{2}, \quad x_2 = -2^{-2/3}\left(1 - \sqrt{3}i\right), \quad x_3 = -2^{-2/3}\left(1 + \sqrt{3}i\right),$$

de las cuales ninguna es racional, lo cual implica que no hay puntos racionales de orden dos.
Busquemos el resto de puntos racionales de orden finito. Tenemos que $D = -108 = -2^2 \cdot 3^3$, por lo que

$$\text{Div}(108) = \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}.$$

Como $y^2 | (-108)$, solo nos fijamos en $\{1, 2, 3\}$. Ninguno de estos valores para y proporcionan puntos racionales.
Por tanto, el único punto racional de orden finito es $\mathcal{O}$, por lo que el grupo de los puntos racionales de orden finito es el trivial.

(b) $\boxed{y^2 = x^3 + 8}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 + 8$ son

$$x_1 = -2, \quad x_2 = 1 - \sqrt{3}i, \quad x_3 = 1 + \sqrt{3}i,$$

de las cuales solo $x_1 = -2$ es racional. Esta nos da el punto racional de orden dos $P_2 = (-2, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es un grupo cíclico de orden dos.
Busquemos el resto de puntos racionales de orden finito. Tenemos que $D = 1728 = 2^6 \cdot 3^3$, y del conjunto Div(1728), nos quedamos solo con

$$\{1, 2, 3, 4, 6, 8, 12, 24\},$$

ya que $y^2 | 1728$. De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(b.1) Si $y = \pm 3$, entonces $x^3 = 1$, que nos da los dos puntos racionales $P_{y=\pm 3} = (1, \pm 3)$. Veamos si son de orden finito.
- Si evaluamos $\psi_3(x) = 3x^4 + 96x$ en $x = 1$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Veamos si tienen orden cuatro. Como $x\left(2P_{y=\pm 3}\right) = -7/4$ no tiene coordenadas enteras, sabemos que $2P_{y=\pm 3}$ no pueden tener orden finito. Por tanto, tampoco pueden tener orden finito $P_{y=\pm 3}$.

(b.2) Si $y = \pm 4$, entonces $x^3 = 8$, que nos da los dos puntos racionales $P_{y=\pm 4} = (2, \pm 4)$.
- Si evaluamos $\psi_3(x) = 3x^4 + 96x$ en $x = 2$ no obtenemos cero, por lo que no pueden ser de orden tres.

- Veamos si tiene orden cuatro. Como $x\left(2P_{y=\pm 4}\right) = -7/4$ no tiene coordenadas enteras, sabemos que $2P_{y=\pm 4}$ no pueden tener orden finito. Por tanto, tampoco pueden tener orden finito $P_{y=\pm 4}$.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\{\mathcal{O}, P_2\},$$

que es un grupo cíclico de orden dos.

(c) $\boxed{y^2 = x^3 + 4}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 + 4$ son

$$x_1 = 2^{-1/3}, \quad x_2 = 2^{-1/3}\left(1 - \sqrt{3}i\right), \quad x_3 = 2^{-1/3}\left(1 + \sqrt{3}i\right),$$

de las cuales ninguna es racional, lo cual implica que no hay puntos racionales de orden dos.
Busquemos el resto de puntos racionales de orden finito. Tenemos que $D = -432 = -2^4 \cdot 3^3$, y por tanto del conjunto Div(432), nos quedamos solo con $\{1, 2, 3, 4, 6, 12\}$. De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales, es decir, $y = \pm 2$.
Si $y = \pm 2$, entonces $x^3 = 0$, que nos da los dos puntos racionales $P_{y=\pm 2} = (0, \pm 2)$. Veamos si son de orden finito. Si evaluamos $\psi_3(x) = 3x^4 + 48x$ en $x = 0$ obtenemos cero, por lo que $P_{y=\pm 2}$ son puntos de orden tres.
Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_{y=-2}, P_{y=2}\right\},$$

que es un grupo cíclico de orden tres.

(d) $\boxed{y^2 = x^3 + 4x}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 + 4x = x(x^2 + 4)$ son

$$x_1 = 0, \quad x_2 = -2i, \quad x_3 = 2i,$$

de las cuales solo $x_1 = 0$ es racional. Esta nos da el punto racional de orden dos $P_2 = (0, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es un grupo cíclico de orden dos.
Busquemos el resto de puntos racionales de orden finito. Tenemos que $D = -256 = -2^8$, y del conjunto Div(256), nos quedamos con $\{1, 2, 4, 8, 16\}$. De

estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales, que son $y = \pm 4$.
Si $y = \pm 4$, entonces $x^3 + 4x - 16 = (x-2)(x^2+2x+8) = 0$, que nos da los dos puntos racionales $P_{y=\pm 4} = (2, \pm 4)$. Veamos si son de orden finito:

- Si evaluamos $\psi_3(x) = 3x^4 + 24x^2 - 16$ en $x = 2$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Veamos si tienen orden cuatro. Como $2P_{y=\pm 4} = (0,0)$ y este tiene orden dos, tenemos que $P_{y=\pm 4}$ tienen orden cuatro.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_2, P_{y=-4}, P_{y=4}\right\},$$

que es un grupo cíclico de orden cuatro.

(e) $\boxed{y^2 - y = x^3 - x^2}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo el cambio $y \mapsto y + 1/2$, llegamos a $y^2 = x^3 - x^2 + 1/4$. Ahora queremos que los coeficientes sean enteros, así que hacemos el cambio $(x, y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 - 4x^2 + 16$, y esta será la ecuación que usaremos.
En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 4x^2 + 16$ no son racionales, lo cual implica que no hay puntos racionales de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = -2816 = -2^8 \cdot 11$, y del conjunto Div(2816), nos quedamos solo con $\{1, 2, 4, 8, 16\}$. De estos posibles valores para y, estudiaremos solo $y = \pm 4$, que es el único que proporciona puntos racionales.
Si $y = \pm 4$, entonces $x^3 - 4x^2 = x^2(x-4) = 0$, que nos da los cuatro puntos racionales $P_{0,y=\pm 4} = (0, \pm 4)$ y $P_{4,y=\pm 4} = (4, \pm 4)$. Veamos si son de orden finito:

- Si evaluamos $\psi_3(x) = 3x^4 - 16x^3 - 192x - 256$ en $x = 0$ o $x = 4$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que

$$\begin{aligned} 2P_{0,y=4} &= (4,-4), & 3P_{0,y=4} &= (4,4), \\ 4P_{0,y=4} &= (0,-4) = P_{0,y=-4}, & 5P_{0,y=4} &= \mathcal{O}; \end{aligned}$$

por lo que $P_{0,y=\pm 4}$ son de orden cinco. Análogamente,

$$\begin{aligned} 2P_{4,y=4} &= (0,4), & 3P_{4,y=4} &= (0,-4), \\ 4P_{4,y=4} &= (4,-4) = P_{4,y=-4}, & 5P_{4,y=4} &= \mathcal{O}; \end{aligned}$$

por lo que $P_{4,y=\pm 4}$ son de orden cinco.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\{\mathcal{O}, (0,-4), (0,4), (4,-4), (4,4)\},$$

que es un grupo cíclico de orden cinco y el generador sería cualquier punto menos $\mathcal{O}$.
Deshaciendo los cambios, el grupo en la curva original es:

$$\big\{\mathcal{O}, (0,0), (0,1), (1,0), (1,1)\big\}.$$

(f) $\boxed{y^2 = x^3 + 1}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 + 1 = (x+1)(x^2 - x + 1)$ son

$$x_1 = -1, \quad x_2 = \frac{1}{2}\left(1 - \sqrt{3}i\right) \quad \text{y} \quad x_3 = \frac{1}{2}\left(1 + \sqrt{3}i\right),$$

de las cuales solo $x_1 = -1$ es racional. Esta nos da el punto racional de orden dos $P_2 = (-1, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es un grupo cíclico de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = -27 = -3^3$, y del conjunto Div(27), nos podemos quedar solo con $\{1, 3\}$. Ambos puntos proporcionan puntos racionales, veamos qué ocurre con ellos:

(f.1) Si $y = \pm 1$, entonces $x^3 = 0$, que nos da los dos puntos racionales $P_{y=\pm 1} = (0, \pm 1)$. Si evaluamos $\psi_3(x) = 3x^4 + 12x$ en $x = 0$ obtenemos cero, por lo que $P_{y=\pm 1}$ son puntos de orden tres.

(f.2) Si $y = \pm 3$, entonces $x^3 = 8$, que nos da los dos puntos racionales $P_{y=\pm 3} = (2, \pm 3)$. Veamos si son de orden finito:

- Sabemos que de orden tres no pueden ser ya que los dos anteriores tienen este orden.
- Como $2P_{y=3} = (0, 1)$ y este punto es de orden tres, sabemos que $P_{y=\pm 3}$ tienen orden que divide a 6. Puesto que $2P_{y=3} \neq P_{y=-3}$, necesariamente $P_{y=\pm 3}$ tienen orden seis.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_2, P_{y=-1}, P_{y=1}, P_{y=-3}, P_{y=3}\right\},$$

que es un grupo cíclico de orden seis y el generador sería $P_{y=-3}$ o $P_{y=3}$.

(g) $\boxed{y^2 = x^3 - 43x + 166}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 43x + 166$ no son racionales, lo cual implica que no hay puntos racionales de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = -425984 = -2^{15} \cdot 13$, y del conjunto Div$(-425984)$, nos quedamos solo con $\{1, 2, 4, 8, 16, 32, 64, 128\}$. De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(g.1) Si $y = \pm 8$, entonces $x^3 - 43x + 102 = 0$, que nos da los dos puntos racionales $P_{y=\pm 8} = (3, \pm 8)$.
- Si evaluamos $\psi_3(x) = 3x^4 - 258x^2 + 1992x - 1849$ en $x = 3$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que

$$2P_{y=8} = (-5, -16), \quad 3P_{y=8} = (11, -32), \quad 4P_{y=8} = (11, 32)$$

de donde $3P_{y=8} = -4P_{y=8}$ y por tanto $P_{y=8}$ tiene orden 7. Análogamente se tiene para $P_{y=-8} = -P_{y=-8}$.

(g.2) Si $y = \pm 16$, entonces $x^3 - 43x - 90 = 0$, que nos da los dos puntos racionales $P_{y=\pm 16} = (-5, \pm 16)$.
Sabemos que de orden tres no pueden ser, pues al haber encontrado un punto de orden siete, sabemos que el orden del grupo de puntos racionales de orden finito es múltiplo de 7, por tanto ha de ser un grupo cíclico de orden 7 (por el Teorema de Mazur), y $7P_{y=\pm 16} = \mathcal{O}$.

(g.3) Si $y = \pm 32$, entonces $x^3 - 43x - 858 = 0$, que nos da los dos puntos racionales $P_{y=\pm 32} = (11, \pm 32)$. Por el mismo razonamiento que para los últimos dos puntos, llegamos a que $P_{y=\pm 32}$ tienen orden siete.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_{y=-8}, P_{y=8}, P_{y=-16}, P_{y=16}, P_{y=-32}, P_{y=32}\right\},$$

que es un grupo cíclico de orden siete y el generador sería cualquiera elemento excepto $\mathcal{O}$.

(h) $\boxed{y^2 + 7xy = x^3 + 16x}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo el $y \mapsto y - 7x/2$, llegamos a $y^2 = x^3 + 49x^2/4 + 16x$. Ahora queremos que los coeficientes sean enteros, así que hacemos el cambio $(x, y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 + 49x^2 + 256x$.

En primer lugar veamos los puntos de orden dos. De las raíces de $f(x) = x^3 + 49x^2 + 256x = x(x^2 + 49x + 256)$, solo $x_1 = 0$ es racional. Esta nos da el punto racional de orden dos $P_2 = (0, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es un grupo cíclico de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 90243072 = 2^{16} \cdot 3^4 \cdot 17$, y del conjunto Div(90243072), nos quedamos *solo* con

$$\{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 64, 72, 96, \\ 128, 144, 192, 256, 288, 384, 576, 768, 1152, 2304\}.$$

De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(h.1) Si $y = \pm 24$, entonces $x^3 + 49x^2 + 256x - 576 = 0$, que nos da los dos puntos racionales $P_{y=\pm 24} = (-8, \pm 24)$.
- Si evaluamos $\psi_3(x) = 3x^4 + 196x^3 + 1536x^2 - 65536$ en $x = -8$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que $2P_{y=24} = (16, 144)$ y $4P_{y=24} = (0, 0) = P_2$, por lo que $4P_{y=24}$ tiene orden dos, y en consecuencia $P_{y=\pm 24}$ tiene orden ocho.

(h.2) Si $y = \pm 96$, entonces $x^3 + 49x^2 + 256x - 9216 = 0$, que nos da los dos puntos racionales $P_{y=\pm 96} = (-32, \pm 96)$.
- Si evaluamos $\psi_3(x) = 3x^4 + 196x^3 + 1536x^2 - 65536$ en $x = -32$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que $2P_{y=96} = (16, -144)$ y $4P_{y=96} = (0, 0) = P_2$, por lo que $4P_{y=96}$ tiene orden dos, y en consecuencia $P_{y=\pm 96}$ tiene orden ocho.

(h.3) Si $y = \pm 144$, entonces $x^3 + 49x^2 + 256x - 20736 = 0$, que nos da los dos puntos racionales $P_{y=\pm 144} = (16, \pm 144)$.
- Si evaluamos $\psi_3(x) = 3x^4 + 196x^3 + 1536x^2 - 65536$ en $x = 16$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que $2P_{y=144} = (0, 0) = P_2$, por lo que $2P_{y=144}$ tiene orden dos, y en consecuencia $P_{y=\pm 144}$ tiene orden cuatro.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_2, P_{y=-24}, P_{y=24}, P_{y=-96}, P_{y=96}, P_{y=-144}, P_{y=144}\right\},$$

que es un grupo cíclico de orden ocho y los generadores son cualquier punto de los cuatro que tienen orden 8, como por ejemplo $P_{y=24}$.
Deshaciendo los cambios, el grupo en la curva original es:

$$\{\mathcal{O}, (0, 0), (-2, 4), (-2, 10), (-8, 16), (-8, 40), (4, -32), (4, 4)\}.$$

(i) $\boxed{y^2 + xy + y = x^3 - x^2 - 14x + 29}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo $y \mapsto y - (x+1)/2$, llegamos a

$$y^2 = x^3 - \frac{3}{4}x^2 - \frac{27}{2}x + \frac{117}{4}.$$

Ahora queremos que los coeficientes sean enteros, así que hacemos el cambio $(x, y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 - 3x^2 - 216x + 1872$.
En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 3x^2 - 216x + 1872$ no son racionales, lo cual implica que no hay puntos racionales de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = -31850496 = -2^{17} \cdot 3^5$, y del conjunto Div(31850496), nos quedaremos solo con

$$\{1, 2, 3, 4, 6, 8, 9, 12, 16, 18, 24, 32, 36, 48, 64, 72, 96, \\ 128, 144, 192, 256, 288, 384, 576, 768, 1152, 2304\}.$$

De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(i.1) Si $y = \pm 24$, entonces $x^3 - 3x^2 - 216x + 1296 = 0$, que nos da los dos puntos racionales $P_{y=\pm 24} = (12, \pm 24)$.
- Si evaluamos $\psi_3(x) = 3x^4 - 12x^3 - 1296x^2 + 22464x - 69120$ en $x = 12$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Calculando sus múltiplos, hallamos que

$$4P_{y=24} = (36, -192), \quad 5P_{y=24} = (36, 192) = -4P_{y=24}$$

por lo que $P_{y=\pm 24}$ tienen orden nueve.

(i.2) Si $y = \pm 32$, entonces $x^3 - 3x^2 - 216x + 848 = 0$, que nos da los dos puntos racionales $P_{y=\pm 32} = (4, \pm 32)$. Si evaluamos $\psi_3(x) = 3x^4 - 12x^3 - 1296x^2 + 22464x - 69120$ en $x = 4$ obtenemos cero, por lo que $P_{y=\pm 32}$ son puntos de orden tres.

(i.3) Si $y = \pm 48$, entonces $x^3 - 3x^2 - 216x - 432 = 0$, que nos da los dos puntos racionales $P_{y=\pm 48} = (-12, \pm 48)$. Puesto que $3P_{y=48} = (4, 32)$ y este tiene orden tres, $P_{y=\pm 48}$ tienen orden nueve.

(i.4) Si $y = \pm 192$, entonces $x^3 - 3x^2 - 216x - 34992 = 0$, que nos da los dos puntos racionales $P_{y=\pm 192} = (36, \pm 192)$. Puesto que $3P_{y=192} = (4, 32)$ y este tiene orden tres, $P_{y=\pm 48}$ tienen orden nueve.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O},\ P_{y=-24},\ P_{y=24},\ P_{y=-32},\ P_{y=32},\ P_{y=-48},\ P_{y=48},\ P_{y=-192},\ P_{y=192}\right\},$$

que es un grupo cíclico de orden nueve y los generadores son cualquier punto de los seis que tienen orden 9. Deshaciendo los cambios, el grupo en la curva original es:

$$\big\{\mathcal{O},\ (3,-5),\ (3,1),\ (1,-5),\ (1,3),\ (-3,-5),\ (-3,7),\ (9,-29),\ (9,19)\big\}.$$

(j) $\boxed{y^2+xy=x^3-45x+81}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo $y \mapsto y-x/2$, llegamos a $y^2 = x^3+x^2/4-45x+81$. Ahora queremos que los coeficientes sean enteros, así que hacemos el cambio $(x,y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 + x^2 - 720x + 5184$, y esta será la ecuación que usaremos.
En primer lugar veamos los puntos de orden dos. De las raíces de $f(x) = x^3 + x^2 - 720x + 5184 = (x-8)(x^2+9x-648)$, solo $x_1 = 8$ es racional. Esta nos da el punto racional de orden dos $P_2 = (8,0)$. Así, el grupo de puntos racionales con orden que divide a dos es un grupo cíclico de orden dos.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 700710912 = 2^{18}\cdot 3^5 \cdot 11$, y del conjunto Div(700710912), nos quedamos solo con

$$\{1,2,3,4,6,8,9,12,16,18,24,32,36,48,64,72,96,128,144,\\ 192,256,288,384,512,576,768,1152,1536,2304,4608\}.$$

De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(j.1) Si $y = \pm 48$, entonces $x^3+x^2-720x+2880 = 0$, que nos da los dos puntos racionales $P_{y=\pm 48} = (24, \pm 48)$.

- Si evaluamos $\psi_3(x) = 3x^4 + 4x^3 - 4320x^2 + 62208x - 497664$ en $x = 24$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que

$$2P_{y=48} = (72,-576), \quad 3P_{y=48} = (72,576),$$

por lo que $P_{y=\pm 48}$ tienen orden cinco.

(j.2) Si $y = \pm 72$, entonces $x^3 + x^2 - 720x = 0$, que nos da los dos puntos racionales $P_{y=\pm 72} = (0, \pm 72)$. Tenemos que

$$\begin{aligned} 2P_{y=72} &= (24, 48), & 3P_{y=72} &= (-24, -96), \\ 4P_{y=72} &= (72, -576), & 5P_{y=72} &= (8, 0) = P_2, \end{aligned}$$

por lo que $P_{y=\pm 72}$ tienen orden diez.

(j.3) Si $y = \pm 96$, entonces $x^3 + x^2 - 720x - 4032 = 0$, que nos da los dos puntos racionales $P_{y=\pm 96} = (-24, \pm 96)$. Análogamente al caso (j.2), $P_{y=\pm 96}$ tienen orden diez.

(j.4) Si $y = \pm 576$, entonces $x^3 + x^2 - 720x - 326592 = 0$, que nos da los dos puntos racionales $P_{y=\pm 576} = (72, \pm 576)$. Análogamente al caso (j.1), $P_{y=\pm 576}$ tienen orden cinco.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_2, P_{y=-48}, P_{y=48}, P_{y=-72}, P_{y=72}, P_{y=-96}, P_{y=96}, P_{y=-576}, P_{y=576}\right\},$$

que es un grupo cíclico de orden diez y los generadores son cualquier punto de los cuatro que tienen orden 10.

Deshaciendo los cambios, el grupo en la curva original es:

$$\left\{\mathcal{O}, (2, -1), (6, -9), (6, 3), (0, -9), (0, 9), (-6, -9), (-6, 15), (18, -81), (18, 63)\right\}.$$

(k) $\boxed{y^2 + 43xy - 210y = x^3 - 210x^2}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Hacemos $y \mapsto y - (43x - 210)/2$, seguido de $(x, y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 + 1009x^2 - 72240x + 705600$, que será la ecuación que usemos.

En primer lugar veamos los puntos de orden dos. De las raíces de

$$f(x) = x^3 + 1009x^2 - 72240x + 705600 = (x - 56)(x^2 + 1065x - 12600),$$

solo $x_1 = 56$ es racional. Esta nos da el punto racional de orden dos $P_2 = (56, 0)$. Así, el grupo de puntos racionales contiene un grupo cíclico de orden dos.

Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 2^{20} \cdot 3^6 \cdot 5^3 \cdot 7^4 \cdot 13$, y del conjunto $\mathrm{Div}(D)$, nos quedamos con los 264 divisores y que verifican que $y^2 | D$.

Comprobando con SageMath, [6], los puntos para todos estos posibles valores de y, concluimos que el grupo de puntos racionales de orden finito es (la tercera coordenada de los punto, en negrita, es el orden)

$$\begin{aligned} \Big\{\mathcal{O},\ &(56, 0, \mathbf{2}),\ (0, \pm 840, \mathbf{12}),\ (120, \pm 2880, \mathbf{3}),\ (-168, \pm 6048, \mathbf{4}), \\ &(-840, \pm 13440, \mathbf{12}),\ (840, \pm 35280, \mathbf{6})\Big\}, \end{aligned}$$

que es un grupo cíclico de orden 12. Deshaciendo los cambios, el grupo en la curva original es:

$$\{\mathcal{O},\ (14,-196),\ (0,0),\ (0,210),\ (30,-900),\ (30,-180),\ (-42,252),\ (-42,1764),\ (-210,2940),\ (-210,6300),\ (210,-8820),\ (210,0)\}.$$

(l) $\boxed{y^2 = x^3 - 4x}$

Solución. En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 4x = x(x^2 - 4)$ son

$$x_1 = 0, \quad x_2 = -2, \quad x_3 = 2.$$

Esto nos da los puntos racionales de orden dos $P_{21} = (0,0)$, $P_{22} = (-2,0)$ y $P_{23} = (2,0)$. Así, el grupo de puntos racionales con orden que divide a dos es el grupo de Klein.

Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 256 = 2^8$, y del conjunto Div(256), nos quedamos con $\{1,2,4,8,16\}$. Ninguno de estos valores para y proporcionan puntos racionales y por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\{\mathcal{O}, P_{21}, P_{22}, P_{23}\},$$

que es el grupo de Klein.

(m) $\boxed{y^2 + xy - 5y = x^3 - 5x^2}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo $y \mapsto y - (x-5)/2$, llegamos a $y^2 = x^3 - 19x^2/4 - 5x/2 + 25/4$. Ahora queremos que los coeficientes sean enteros, así que hacemos el cambio $(x,y) \mapsto (x/4, y/8)$, quedando entonces $y^2 = x^3 - 19x^2 - 40x + 400$.

En primer lugar veamos los puntos de orden dos. Las raíces de $f(x) = x^3 - 19x^2 - 40x + 400$ son

$$x_1 = -5, \quad x_2 = 4, \quad x_3 = 20.$$

Esto nos da los puntos racionales de orden dos $P_{21} = (-5,0)$, $P_{22} = (4,0)$ y $P_{23} = (20,0)$. Así, el grupo de puntos racionales con orden que divide a dos es el grupo de Klein.

Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 12960000 = 2^8 \cdot 3^4 \cdot 5^4$, y del conjunto Div($D$), nos quedamos **solo** con

$$\{1,2,3,4,5,6,8,9,10,12,15,16,18,20,24,25,30,36,40,45,48,50,60,72,75,80,90,100,120,144,150,180,200,225,240,300,360,400,450,600,720,900,1200,1800,3600\}.$$

De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(m.1) Si $y = \pm 20$, entonces $x^3 - 19x^2 - 40x = 0$, que nos da los dos puntos racionales $P_{y=\pm 20} = (0, \pm 20)$.
- Si evaluamos $\psi_3(x) = 3x^4 - 76x^3 - 240x^2 + 4800x - 32000$ en $x = 0$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que $2P_{y=\pm 20} = (20, 0) = P_{23}$, y, como este tiene orden dos, $P_{y=\pm 20}$ tienen orden cuatro.

(m.2) Si $y = \pm 180$, entonces $x^3 - 19x^2 - 40x - 3200 = 0$, que nos da los dos puntos racionales $P_{y=\pm 180} = (40, \pm 180)$.
- Si evaluamos $\psi_3(x) = 3x^4 - 76x^3 - 240x^2 + 4800x - 32000$ en $x = 40$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que $2P_{y=\pm 180} = (20, 0) = P_{23}$, y, como este tiene orden dos, $P_{y=\pm 20}$ tienen orden cuatro.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_{21}, P_{22}, P_{23}, P_{y=-20}, P_{y=20}, P_{y=-180}, P_{y=180}\right\},$$

que es el producto de un grupo cíclico de orden dos y uno de orden cuatro. Deshaciendo los cambios, el grupo en la curva original es:

$$\left\{\mathcal{O}, \left(\frac{-5}{4}, \frac{25}{8}\right), (1,2), (5,0), (0,0), (0,5), (10,-25), (10,20)\right\}.$$

(n) $\boxed{y^2 + 5xy - 6y = x^3 - 3x^2}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo los cambios usuales llegamos a la ecuación que usaremos, que es $y^2 = x^3 + 13x^2 - 240x + 576$.
Tenemos que

$$f(x) = x^3 + 13x^2 - 240x + 576 = (x + 24)(x - 3)(x - 8),$$

lo que nos da los puntos racionales de orden dos $P_{21} = (-24, 0)$, $P_{22} = (3, 0)$ y $P_{23} = (8, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es de nuevo el grupo de Klein.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 18662400 = 2^{10} \cdot 3^6 \cdot 5^2$, y del conjunto $\mathrm{Div}(D)$, nos quedamos con

$$\{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 27, 30, 32, 36, 40, 45,$$
$$48, 54, 60, 72, 80, 90, 96, 108, 120, 135, 144, 160, 180, 216, 240,$$
$$270, 288, 360, 432, 480, 540, 720, 864, 1080, 1440, 2160, 4320\}.$$

De estos posibles valores para y, estudiaremos solo los que proporcionan puntos racionales:

(n.1) Si $y = \pm 24$, entonces $x^3 + 13x^2 - 240x = 0$, que nos da los dos puntos racionales $P_{y=\pm 24} = (0, \pm 24)$.
- Si evaluamos $\psi_3(x) = 3x^4 + 52x^3 - 1440x^2 + 6912x - 27648$ en $x = 0$ no obtenemos cero, por lo que no pueden ser de orden tres.
- Tenemos que

$$2P_{y=24} = (12, 36), \quad 3P_{y=24} = (-24, 0) = P_{21},$$

y, como este tiene orden dos, $P_{y=\pm 24}$ tienen orden seis.

(n.2) Si $y = \pm 36$, entonces $x^3 + 13x^2 - 240x - 720 = 0$, que nos da los dos puntos racionales $P_{y=\pm 36} = (12, \pm 36)$. Si evaluamos ahora $\psi_3(x)$ en $x = 12$ obtenemos cero, por lo que $P_{y=\pm 36} = (12, \pm 36)$ son de orden tres.

(n.3) Si $y = \pm 60$, entonces $x^3 + 13x^2 - 240x - 3024 = 0$, que nos da los dos puntos racionales $P_{y=\pm 60} = (-12, \pm 60)$. Tenemos que

$$2P_{y=60} = (12, -36), \quad 3P_{y=60} = (3, 0) = P_{22},$$

y, como este tiene orden dos, $P_{y=\pm 60}$ tienen orden seis.

(n.4) Si $y = \pm 360$, entonces $x^3 + 13x^2 - 240x - 129024 = 0$, que nos da dos puntos racionales $P_{y=\pm 360} = (48, \pm 360)$. Tenemos que

$$2P_{y=360} = (12, 36), \quad 3P_{y=360} = (8, 0) = P_{23},$$

y de nuevo, como este tiene orden dos, $P_{y=\pm 360}$ tienen orden seis.

Por tanto, concluimos que el grupo de puntos racionales de orden finito es

$$\left\{\mathcal{O}, P_{21}, P_{22}, P_{23}, P_{y=-24}, P_{y=24}, P_{y=-36}, P_{y=36}, P_{y=-60}, P_{y=60}, P_{y=-360}, P_{y=360}\right\},$$

que es el producto de un grupo cíclico de orden dos y uno de orden seis. Deshaciendo los cambios, el grupo en la curva original es:

$$\left\{\mathcal{O}, (-6, 18), \left(\frac{3}{4}, \frac{9}{8}\right), (2, -2), (0, 0), (0, 6), (3, -9), (3, 0), (-3, 3), (-3, 18), (12, -72), (12, 18)\right\}.$$

(o) $\boxed{y^2 + 17xy - 120y = x^3 - 60x^2.}$

Solución. Lo primero es poner la curva en forma normal de Weierstrass. Haciendo los cambios habituales resulta la ecuación $y^2 = x^3 + 49x^2 - 16320x + 230400$.
En primer lugar veamos que

$$f(x) = x^3 + 49x^2 - 16320x + 230400 = (x + 160)(x - 15)(x - 96),$$

por lo cual los puntos racionales de orden dos son $P_{21} = (-160, 0)$, $P_{22} = (15, 0)$ y $P_{23} = (96, 0)$. Así, el grupo de puntos racionales con orden que divide a dos es el grupo de Klein.
Busquemos el resto de puntos racionales de orden finito. El discriminante es $D = 2^{16} \cdot 3^8 \cdot 5^4 \cdot 7^2$, y del conjunto $\mathrm{Div}(D)$, nos quedamos con los 270 divisores y tales que $y^2 | D$.
Comprobando con SageMath, [6], los puntos para todos estos posibles valores de y, concluimos que el grupo de puntos racionales de orden finito es (la tercera coordenada, en negrita, es el orden)

$$\Big\{\mathcal{O},\ (96, 0, \mathbf{2}),\ (15, 0, \mathbf{2}),\ (-160, 0, \mathbf{2}),\ (0, \pm 480, \mathbf{8}),\ (120, \pm 840, \mathbf{8}),\\ (-48, \pm 1008, \mathbf{4}),\ (-120, \pm 1080, \mathbf{8}),\ (240, \pm 3600, \mathbf{4}),\ (960, \pm 30240, \mathbf{8})\Big\},$$

que es el producto de un grupo cíclico de orden 2 y un grupo cíclico de orden 8. Deshaciendo los cambios, el grupo en la curva original es:

$$\Big\{\mathcal{O},\ (24, -144),\ \Big(\frac{15}{4}, \frac{225}{8}\Big),\ (-40, 400),\ (0, 0),\ (0, 120),\\ (30, -300),\ (30, -90),\ (-12, 36),\ (-12, 288),\ (-30, 180),\\ (-30, 450),\ (60, -900),\ (60, 0),\ (240, -5760),\ (240, 1800)\Big\}.$$

Bibliografía

[1] Cohen, H.: *A course in computational algebraic number theory*. Springer-Verlag (1984).

[2] Fulton, W.: *Algebraic curves*. Edición original en Benjamin, versión actualizada accesible libremente en https://dept.math.lsa.umich.edu/ wfulton/

[3] Mazur, B.: *Rational isogenies of prime degree*. Invent. Math. **44** (1978) 129–162.

[4] García Selfa, I.: *Aspectos diofánticos y computacionales de la torsión racional en curvas elípticas*. Tesis doctoral, Universidad de Sevilla (2006).

[5] Silverman, J.H. y Tate, J.T.: *Rational points on elliptic curves*, 2nd ed. Springer International Publishing (2015).

[6] Cano Wall, P., García Barranco, M. y Lorite Budiño, P.: Script creado con el programa SageMath (2022).