ASPECTOS DIOFÁNTICOS Y COMPUTACIONALES DE LA TORSIÓN RACIONAL EN CURVAS ELÍPTICAS

Memoria presentada por Irene García Selfa

para optar al Grado de Doctora en Matemáticas

por la Universidad de Sevilla.

V° B° del Director

Fdo. José M. Tornero
Doctor en Matemáticas

Fdo. Irene García Selfa

Sevilla, verano de 2.006

Índice

Quiero expresar mi agradecimiento, en primer lugar, al profesor José María Tornero quien desde el principio me animó a realizar este trabajo, ofreciéndome un gran apoyo, tanto a nivel profesional como personal, y contagiándome su entusiasmo con la dirección de esta tesis.

También a todos los componentes del departamento de Álgebra de esta universidad, que contribuyeron de alguna manera a que este trabajo fuera posible, en especial a los profesores Luis Narváez y Miguel Ángel Olalla, y a Adela. Así mismo, al profesor Antonio Campillo de la universidad de Valladolid, quien no dudó en ofrecerme su ayuda cuando la necesité.

Quiero mencionar también a DonDa, Magda, DonVi, Amelia y los demás, por todo lo que pude aprender con ellos.

A mis amigos, que siempre tuvieron palabras de ánimo que darme.

A mis hermanos y a Adrián, porque quizá sin saberlo, condensó en cuatro palabras lo que otros no hemos sabido resumir.

A mis padres, por su apoyo siempre incondicional en todas mis aventuras.

Y especialmente a Jose, mi esposo, por cuidarme como lo ha hecho durante todo este tiempo.

Introducción

En 1899, Poincaré conjeturaba que el grupo de puntos racionales de una curva elíptica es finitamente generado, y fue Mordell [25], en 1922, el primero en demostrar tal aserto. Más tarde, Weil [39] dio una prueba de dicho resultado mediante el conocido teorema de Mordell-Weil, cuya principal consecuencia es que, dada una curva elíptica E, el grupo de puntos racionales de la curva es

$$E(\mathbb{Q}) = \mathrm{Tor}(E(\mathbb{Q})) \oplus \mathbb{Z}^r,$$

donde $\mathrm{Tor}(E(\mathbb{Q}))$ es su subgrupo de torsión y $r \in \mathbb{N}$ su rango.

Es muchísima lo que desconocemos sobre el rango de una curva elíptica. Por ejemplo, los algoritmos que actualmente se utilizan para calcularlo admiten alguna conjetura, habitualmente la de Birch y Swinnerton-Dyer [2]. Por otra parte, tampoco se conoce si hay curvas de rango arbitrario o si, por el contrario, hay una cota superior para r.

Como se desprende del título de esta tesis, lo que aquí nos ocupa es el estudio en profundidad del grupo $\mathrm{Tor}(E(\mathbb{Q}))$, de cuyos aspectos computacionales destacamos la implementación de un algoritmo original publicado en [15]. En cuanto a los aspectos diofánticos, señalar que no se había dado hasta ahora una caracterización de las curvas elípticas cuyo grupo de torsión racional es de orden impar usando relaciones diofánticas, y esto precisamente es lo que hacemos en las cuatro últimas secciones del tercer y último capítulo de esta memoria que pasamos a describir a continuación.

En el capítulo I se recogen definiciones y resultados clásicos sobre curvas elípticas necesarios para el desarrollo de los capítulos II y III. Cabe destacar aquí uno de los resultados imprescindibles y básicos para este trabajo, el teorema de Mazur [22, 23], que nos proporciona la lista de posibilidades para el grupo de torsión de una curva elíptica definida sobre $\mathbb{Q}$, a saber

$$\mathbb{Z}/n\mathbb{Z} \quad \text{con } 1 \leq n \leq 10 \text{ ó } n = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{con } 1 \leq n \leq 4.$$

Fundamental es también el hecho de que toda curva elíptica sea birracionalmente equivalente a una dada en forma normal de Weierstrass, es decir, dada por la ecuación

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

y en particular, con un cambio lineal de variables adecuado, tenemos que toda curva elíptica se puede expresar mediante la denominada forma breve de Weierstrass,

$$Y^2 = X^3 + AX + B.$$

Con el objetivo de calcular la torsión racional, recogemos en este primer capítulo varios resultados de diferente naturaleza.

Desde el punto de vista del análisis complejo, veremos cómo las curvas elípticas están relacionadas con la función $\wp$ de Weierstrass, definida mediante la ecuación diferencial

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

donde $g_2(\Lambda)$ y $g_3(\Lambda)$ son complejos que dependen de un retículo Λ dado.

Por otra parte, el teorema de Nagell-Lutz [21, 27] afirma que los puntos de orden finito de una curva elíptica racional tienen en realidad coordenadas enteras y, además, la segunda de estas coordenadas, o bien es nula, o bien es un divisor del discriminante Δ de la curva. Este resultado se puede mejorar, en el sentido de que será el cuadrado de esta segunda coordenada quien divida a Δ, usando los cuerpos $\mathbb{Q}_p$ de números p-ádicos quienes, además, relacionaremos con los cuerpos finitos $\mathbb{F}_p$ mediante la reducción modulo p, para probar que

$$\mathrm{Tor}(E(\mathbb{Q})) \subset \overline{E}(\mathbb{F}_p),$$

siendo p un primo adecuado y $\overline{E}$ la reducida de la curva E modulo p.

En la penúltima sección de este capítulo trataremos con los polinomios de división. Veremos que, dado un punto racional P en la curva E y un entero $m \geq 1$, el punto mP admite una expresión en la que interviene el m–ésimo polinomio de división Ψ_m, lo que permitirá decidir, buscando las raíces enteras de dicho polinomio, si el punto dado es o no de orden m.

Para finalizar el capítulo I, estudiamos la forma normal de Tate de una curva elíptica, es decir, una expresión del tipo

$$Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

que será posible en determinadas condiciones y que nos resultará de mucha utilidad.

Una de las principales ventajas de expresar una curva de esta manera es que tenemos el punto $P = (0,0)$ en la curva, y podemos expresar las coordenadas de mP en función de los parámetros b y c. Esto va a permitir demostrar que las curvas elípticas en forma normal de Tate que tienen un punto de orden finito m dado, forman una familia uniparamétrica de curvas.

El capítulo II recopila y compara los algoritmos de que disponemos para el cálculo de $\mathrm{Tor}(E(\mathbb{Q}))$. En primer lugar hacemos un estudio detallado del coste computacional de la acotación del orden de este grupo, mediante la reducción mencionada en el primer capítulo. Aunque, en teoría, este coste sería del orden de $O(\log|\Delta|)$, en la práctica dicha acotación se obtiene en una cantidad muy pequeña de tiempo, como se puede comprobar con los ejemplos proporcionados en A.2. (segunda sección del apéndice), por lo que este proceso de acotación se incluirá en cada uno de los cuatro algoritmos que implementaremos para el cálculo de la torsión racional, y que exponemos con detalle en A.1.

El primero de estos algoritmos, basado en el teorema de Nagell-Lutz, es bastante sencillo. Consiste en buscar los divisores cuadrados del discriminante Δ y comprobar si corresponden a la segunda coordenada de algún punto racional de la curva, para verificar después si dicho punto es o no de orden finito.

El principal inconveniente que aquí encontramos es la necesidad de factorizar Δ, lo que eleva considerablemente la complejidad de este algoritmo que resulta de

$$O\left(e^{(C+O(1))(\log|\Delta|)^{1/3}(\log\log|\Delta|)^{2/3}}\right).$$

El segundo procedimiento que presentamos para el cálculo de $\mathrm{Tor}(E(\mathbb{Q}))$, debido a Doud [10], se basa en la parametrización analítica de una curva elíptica. Mediante el algoritmo dado en I.C., hallamos una base $\{\omega_1,\omega_2\}$ del retículo Λ asociado a la curva, y a partir de ésta buscamos los puntos de $E(\mathbb{C})$ de orden finito m a través de los complejos de $(1/m)\mathbb{C}/\Lambda$, comprobando después si dichos puntos tienen o no coordenadas racionales.

Ahora, lo más costoso computacionalmente es dar las coordenadas de los puntos de la curva que corresponden a los $u \in \mathbb{C}$ que están en el paralelogramo definido por la base del retículo tales que $mu \in \Lambda$. Con todo esto, la complejidad de este algoritmo es $O(\log^3|\Delta|)$.

En II.D. analizamos el algoritmo de los polinomios de división Ψ_m. Se

trata de averiguar si dichos polinomios tienen alguna raíz entera, para $3 \leq m \leq 9$, y comprobar que ésta corresponda a la primera coordenada de un punto racional de la curva.

Acotando las normas de los polinomios de división en función de los coeficientes de la curva, podemos estudiar la complejidad de este algoritmo usando un resultado de Loos [20], concluyendo que ésta es $O(\log^2 |\Delta|)$.

La última sección de este segundo capítulo la dedicamos al algoritmo basado en la forma normal de Tate, donde, del mismo modo que hicimos en [15], para averiguar si una curva elíptica tiene un punto de orden dado, utilizamos el teorema de la sección I.G. que caracteriza las formas normales de Tate como familias uniparamétricas de curvas.

Aunque, teóricamente, la complejidad de este algoritmo sea la misma que la del anterior, la práctica dice lo contrario, como se puede comprobar en A.3., donde se recogen unas tablas comparativas de los tiempos empleados por los cuatro algoritmos para quince ejemplos diferentes de curvas, uno por cada posible grupo de torsión racional. Estos resultados muestran que el algoritmo basado en la forma normal de Tate es más rápido que los demás a medida que aumenta el tamaño de los coeficientes de la curva, (que llegan a alcanzar en dichos ejemplos unas 6000 cifras en base decimal), y para grupos de torsión de orden mayor que 4, tanto cíclicos como no cíclicos.

El capítulo III completa la caracterización mediante ecuaciones diofánticas de las curvas elípticas con grupo de torsión racional de orden dado, que hasta ahora sólo se había hecho para el caso en que este grupo es de orden par.

En primer lugar exponemos el estudio realizado por Ono [28] sobre curvas con torsión racional no cíclica, cuyo teorema principal conduce a un algoritmo sencillo, aunque no muy práctico computacionalmente, en el que se establece una relación directa entre la existencia o no de soluciones para ciertas ecuaciones diofánticas (en las que intervienen los coeficientes de la curva), y el tipo de grupo de torsión que posee dicha curva.

A lo largo de la demostración de este teorema de Ono, se hace uso extensivo de un resultado que proporciona una condición necesaria y suficiente para que, dado un punto $P = (x_0, y_0) \in E(\mathbb{K})$, exista otro $Q = (x_1, y_1) \in E(\mathbb{K})$ verificando que $2Q = P$, y este mismo resultado es el que aprovechan Qiu y Zhang [31, 32] para caracterizar curvas elípticas con torsión racional cíclica de orden par, de manera análoga a como Ono lo hizo para el caso no cíclico.

También ahora tenemos un algoritmo sencillo que proporciona además las coordenadas de los puntos racionales de torsión, y aunque, como en el caso

anterior, no resulta práctico computacionalmente, sí tiene una gran utilidad a la hora de describir de forma explícita los grupos de torsión de curvas elípticas definidas, tanto sobre $\mathbb{Q}$, como sobre extensiones algebraicas de este cuerpo.

En la misma línea, pero mediante razonamientos necesariamente diferentes, hemos conseguido dar este tipo de caracterizaciones para curvas elípticas con torsión de orden impar, partiendo de su ecuación en forma breve de Weierstrass $Y^2 = X^3 + AX + B$, con A y B enteros tales que $x^3 + Ax + B \neq 0$ para todo $x \in \mathbb{Q}$, es decir, para curvas sin puntos racionales de orden 2.

Así, demostraremos los siguientes resultados:

Una curva tiene algún punto racional $P = (x, y)$ de orden 3 si y sólo si

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6,$$

con $m, n \in \mathbb{Z}$ tales que $n \neq -9m^3$ y $n^2 \neq 27m^6$.

Una curva tiene algún punto racional $P = (x, y)$ de orden 5 si y sólo si

$$\begin{aligned} A &= -x^2 - xv - v^2 + (x - v)s, \\ B &= -\frac{1}{4}(x + v)(-3x^2 + 2xv - 3v^2 + 2(x - v)s), \\ s^2 &= (2x + v)(x + 2v), \\ r^2 &= 3x + 2s + 3v. \end{aligned}$$

con $x, v, s, r \in \mathbb{Z}$ tales que $x \neq v$.

Una curva tiene algún punto racional $P = (x, y)$ de orden 7 si y sólo si

$$\begin{aligned} A = &\ -x^2 - v^2 - xv + s(x - v), \\ B = &\ \frac{-1}{4}\left(3x^3 + x^2w + 3xv^2 - 2xvw + 2v^3 + v^2w + 2s(x^2 - v^2)\right), \\ s^2 = &\ (v + 2x)(x + w + v), \\ 0 = &\ 3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s, \\ r^2 = &\ 3x + 2v + 2s + w, \end{aligned}$$

con $x, v, w, s, r \in \mathbb{Z}$ tales que x, v y w son distintos dos a dos.

Una curva tiene algún punto racional $P = (x, y)$ de orden 9 si y sólo si

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6,$$

con $m, n \in \mathbb{Z}$ tales que $n \neq -9m^3$, $n^2 \neq 27m^6$, y $3m^2 = x(3P)$, siendo esta última condición demasiado compleja como para que interese darla explícitamente (ver III.F.).

Proporcionamos además, en cada caso, las coordenadas de todos los puntos racionales de torsión en función de los parámetros que aparecen.

Por otra parte, usando las familias uniparamétricas de curvas en forma normal de Tate, ofrecemos también una caracterización de las curvas elípticas con torsión de orden 5, 7 y 9 mediante ecuaciones de Thue (en un sentido amplio que precisaremos).

De este modo, los coeficientes de la curva en forma breve de Weierstrass serán

$$A = A(p,q), \qquad B = B(p,q)$$

con $p, q \in \mathbb{Z}$ primos entre sí, siendo $A(p,q), B(p,q) \in \mathbb{Z}[p,q]$ homogéneos, el primero de ellos de grado 4, 8, ó 12, y el segundo de grado 6, 12 ó 18, según el orden de $\mathrm{Tor}(E(\mathbb{Q}))$ sea 5, 7 ó 9, respectivamente. Resultando, además, las coordenadas de los puntos racionales de torsión (x,y) con $x(p,q), y(p,q) \in \mathbb{Z}[p,q]$ homogéneos, siendo x de grado 2, 4, ó 6, e y de grado 3, 6 ó 9, según la torsión sea de orden 5, 7 ó 9, respectivamente.

Finalizamos esta introducción con unas líneas dedicadas a las posibles extensiones de este trabajo. El problema del cálculo de la torsión, al menos sobre $\mathbb{Q}$, creemos que puede considerarse cerrado. La magnitud de los ejemplos que se pueden calcular en tiempos muy pequeños hace que, a día de hoy, este problema esté completamente resuelto en la práctica. En el aspecto puramente formal de teoría de la complejidad, tampoco parece posible hallar cotas menores que $O(\log^2 |\Delta|)$, al ser ésta la complejidad de la mayoría de los cálculos no elementales con enteros [17].

Un caso muy distinto es el del aspecto diofántico. En cierto sentido, hemos logrado en esta memoria cubrir todos los casos posibles de órdenes para puntos racionales con ecuaciones diofánticas, y eso podría pensarse que cierra el problema.

Pero en realidad, nuestra intención es llevar esto más lejos. Es poco lo que sabemos de la torsión de las curvas elípticas sobre los cuerpos de números. El extraordinario resultado de Merel [24] afirma que todas las curvas elípticas definidas sobre una extensión algebraica K de $\mathbb{Q}$ admiten para el orden de su grupo de torsión una cota que sólo depende del grado de la extensión. Sin embargo, sólo para algunos casos conocemos acotaciones precisas y satisfactorias [7, 13, 29, 30]. En este sentido, los resultado de Ono [28] que generalizamos y completamos en III han sido de utilidad para el estudio del comportamiento de la torsión por extensión de cuerpos [19, 12]. Es nuestra intención proseguir con este estudio, con la ayuda de las caracterizaciones aquí expuestas.

Otra posible aplicación de nuestro trabajo es estudiar con más detalle el proceso de reducción, en el sentido de averiguar cuánto se aproxima la cota hallada al orden real del grupo. Sabemos que no siempre es precisa [34], pero, por ejemplo, no se sabe si este fenómeno ocurre en todos los posibles grupos, ni se conoce una caracterización de las curvas donde la reducción no predice con exactitud el número de puntos de torsión. Es de esperar que condiciones como las que hemos hallado permitan un estudio detallado de los posibles casos y, quizá, responder alguna de estas cuestiones.

I. Preliminares

En este primer capítulo sentaremos las bases para los dos siguientes en cuanto a notaciones y resultados básicos. Prácticamente cualquier referencia estándar en la materia (por ejemplo, [6, 16, 34, 35]) contiene las demostraciones que se omiten. Cuando no sea así, precisaremos dónde hallar los detalles. Los resultados sobre curvas algebraicas generales se pueden encontrar, por ejemplo, en [14]. Este capítulo no contiene, por tanto, resultados originales.

I.A. El grupo de puntos racionales de una curva elíptica

Sea $\mathbb{K}$ un cuerpo arbitrario y E una cúbica proyectiva, es decir, una curva que admite una ecuación del tipo

$$aX^3+bX^2Y+cXY^2+dY^3+eX^2Z+fXYZ+gY^2Z+hXZ^2+iYZ^2+jZ^3=0$$

donde $a,b,c,d,e,f,g,h,i,j \in \mathbb{K}$, y $Z=0$ es la recta del infinito del plano proyectivo $\mathbb{P}^2(\mathbb{K})$. El problema de determinar las soluciones de estas ecuaciones es el germen de la teoría de curvas elípticas.

Observación.– Para el caso que nos ocupará casi en todo el trabajo, $\mathbb{K}=\mathbb{Q}$, no conocemos un método general que nos determine en un número finito de pasos si una tal cúbica tiene o no algún punto con coordenadas racionales. 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). Por ejemplo, la ecuación

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

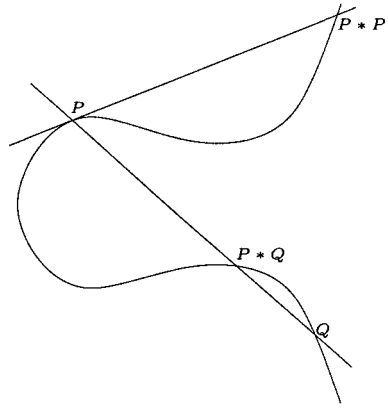
no tiene solución entera no trivial; es decir, no podemos encontrar $X,Y,Z \in \mathbb{Z}$ no todos nulos que verifiquen esta ecuación. Sin embargo, se puede demostrar

[33] que podemos encontrar solución en cualquier congruencia, a pesar de que no existe solución entera.

Vamos a suponer, en lo sucesivo, que nuestra cúbica es una curva no singular y que tiene un punto con coordenadas en $\mathbb{K}$ que llamaremos $\mathcal{O}$. Una tal curva se denomina una curva elíptica sobre $\mathbb{K}$.

Observación.– Si una recta corta a la cúbica en dos puntos con coordenadas en $\mathbb{K}$, por las relaciones de Cardano, el tercer punto de corte también tiene sus coordenadas en $\mathbb{K}$.

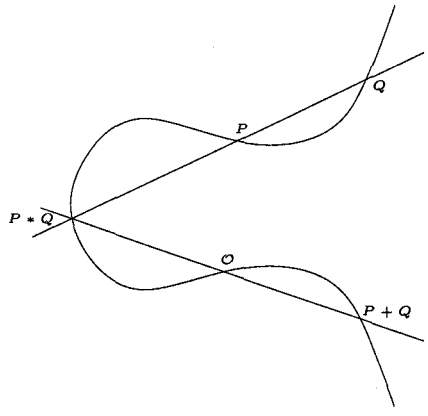
Así, si tenemos dos puntos de $\mathbb{P}^2(\mathbb{K})$ distintos, P y Q, en la cúbica, construiremos otro punto $P * Q$, que será el tercer punto de corte de la recta PQ con nuestra curva. Si P no es un punto de inflexión y $Q = P$, tomaremos la recta tangente en P, que tiene con la curva un contacto de orden 2. Esta recta corta a la curva en otro punto distinto de P, y éste 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 contacto de orden 3 con la curva) se tomará $P * P = P$.



La ley " $*$ " que acabamos de definir, es una ley interna en el conjunto de los puntos de una cúbica en $\mathbb{P}^2(\mathbb{K})$, pero no dota a este conjunto de estructura de grupo. Por ejemplo, no hay elemento neutro. Vamos a definir otra ley interna "$+$" que haga que el conjunto de puntos de una cúbica tenga estructura de grupo. Recordemos que estamos suponiendo que tenemos un punto $\mathcal{O}$ en la cúbica. Definimos ahora la siguiente ley interna: para dos puntos cualesquiera P y Q de la cúbica,

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

Veamos que ahora tenemos efectivamente un grupo, que denotaremos $(E(\mathbb{K}), +)$.



- *Elemento neutro*: $\mathcal{O} + P = P$, $\forall P \in E(\mathbb{K})$. Ya que si $P' = \mathcal{O} * P$, el tercer punto en E de la recta que pasa por $\mathcal{O}$ y P' es precisamente P.

- *Conmutativa*: Es evidente, ya que $P * Q = Q * P$.

- *Elemento opuesto*: Consideramos S el otro punto de corte con E de la tangente por $\mathcal{O}$. Entonces la recta que une un punto Q de la curva con este punto S corta a E también en un punto R. Y se tiene $Q + R = \mathcal{O}$, es decir, $R = -Q$.

- *Asociativa*: Para probar que $P + (Q + R) = (P + Q) + R$, basta ver que $P * (Q + R) = (P + Q) * R$, ya que sólo faltaría unir éstos con $\mathcal{O}$ y el tercer punto sería la suma de P, Q y R que en los dos casos es la misma 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

$$C_1 = r_1 \cup r_2 \cup r_3,$$

  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 (puede probarse directamente o usando el teorema de Riemann–Roch). Esto finaliza la prueba de que la ley " $+$ " es asociativa.

Observación.– Hay que considerar la cúbica en el plano proyectivo $\mathbb{P}^2(\mathbb{K})$, para que tenga sentido hablar del tercer punto de la intersección entre una recta y la cúbica.

Observación.– Si en vez de elegir $\mathcal{O}$ como elemento neutro elegimos otro punto $\mathcal{O}'$ de E, se puede probar que la aplicación que lleva P en $P+(\mathcal{O}'-\mathcal{O})$ es un isomorfismo entre los grupos "E, con $\mathcal{O}$ como elemento neutro" y "E, con $\mathcal{O}'$ como elemento neutro".

Observación.– Para cúbicas singulares, supuesto que $\mathcal{O}$ no es singular, se puede demostrar que, definiendo de la misma forma una operación interna, el conjunto de puntos no singulares forman un grupo abeliano.

Centrándonos más específicamente en el caso $\mathbb{K} = \mathbb{Q}$, dado que los puntos con ambas coordenadas racionales de una curva elíptica definida sobre $\mathbb{Q}$ forman un grupo abeliano, cabe preguntarse sobre la estructura de este grupo. En concreto, es lógico preguntarse si el grupo es finito o infinito y, en el segundo caso, si es o no finitamente generado. Se conoce hace muchos años la existencia de curvas elípticas con una cantidad infinita de puntos racionales, por lo que el problema queda reducido a:

Conjetura (Poincaré, 1899): Dada un curva elíptica definida sobre $\mathbb{Q}$, el grupo de sus puntos racionales es finitamente generado.

La primera demostración de este resultado la dio Mordell en 1922 [25]. Posteriormente Weil [39] generalizó este resultado en dos direcciones:

(a) Para variedades algebraicas de dimensión mayor que 1 que admitan una estructura de grupo compatible con la de variedad algebraica. Estas variedades se denominan variedades abelianas y las curvas elípticas son el caso más sencillo.

(b) Para cuerpos base que sean extensiones algebraicas de $\mathbb{Q}$ (o cuerpos de números, como comúnmente se denominan en teoría de números).

El resultado se conoce hoy generalmente como el teorema de Mordell–Weil y la demostración habitualmente ofrecida en los libros, por ejemplo [6], sigue la que dio Weil. Aunque no vamos a entrar en la demostración, porque necesitaría por sí sola un capítulo (bastante largo), sí diremos que se divide en dos partes:

Teorema débil de Mordell–Weil.– Dada una curva elíptica E, definida sobre $\mathbb{Q}$, si denotamos $2E(\mathbb{Q})$ al subgrupo

$$2E(\mathbb{Q}) = \{P \in E(\mathbb{Q}) \mid \exists Q \in E(\mathbb{Q}) \text{ con } 2Q = P\},$$

se tiene que el grupo $E(\mathbb{Q})/2E(\mathbb{Q})$ es finito.

El paso del grupo total a un cociente de la forma $E(\mathbb{K})/nE(\mathbb{K})$ se denomina n-descenso y es una de las herramientas más usadas para sondear numerosos problemas aún por resolver en la teoría de curvas elípticas.

La segunda parte de la demostración consiste en definir una función $h : E \longrightarrow \mathbb{R}_+$, denominada altura y que verifique las siguientes condiciones:

1. Dado $\rho \in \mathbb{R}_+$ sólo hay un número finito de puntos P con $h(P) < \rho$.
2. La altura de la suma de dos puntos se puede acotar en función de una constante que sólo depende de la curva y de las alturas de los sumandos.
3. La altura del doble de un punto se puede acotar en función de una constante que depende de nuevo de la curva y de la altura del punto en cuestión.

Con estas condiciones es relativamente sencillo hallar una nueva constante (de nuevo referida a la curva) de tal forma que, con los puntos de altura menor (una cantidad finita) y un conjunto cuyas clases generen $E/2E$ (también finito) se generan todos los puntos de la curva.

Las posibilidades de elección para la función h son amplias. De hecho el nombre de altura viene de que una posible elección es, precisamente

$$\begin{aligned} h : E &\longrightarrow \mathbb{R}_+ \\ P = (a, b) &\longmapsto |b| \end{aligned}$$

Como corolario inmediato del teorema de Mordell–Weil, se obtiene, por el teorema de estructura de los grupos abelianos finitamente generados, que el grupo $E(\mathbb{Q})$ es de la forma

$$E(\mathbb{Q}) = \mathrm{Tor}(E(\mathbb{Q})) \oplus \mathbb{Z}^r,$$

donde $\mathrm{Tor}(E(\mathbb{Q}))$ son los puntos de orden finito y $r \in \mathbb{N}$. En siguientes secciones de este trabajo estudiaremos a fondo el grupo $\mathrm{Tor}(E(\mathbb{Q}))$: estructuras, métodos efectivos de diversa índole para calcularlo y propiedades. El resultado esencial y de mayor calado en este contexto es el teorema de Mazur [22, 23], que expone los posibles subgrupos de torsión de un curva elíptica y que resulta fundamental en todo este trabajo.

Teorema.– Sea E una curva elíptica. Entonces el subgrupo de torsión $\mathrm{Tor}(E(\mathbb{Q}))$ del grupo $E(\mathbb{Q})$ es de una de las siguientes formas:

(a) $\mathbb{Z}/n\mathbb{Z}$ con $1 \leq n \leq 10$ ó $n = 12$.

(b) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ con $1 \leq n \leq 4$.

El número r, que aparece como exponente de $\mathbb{Z}$ en la descripción del grupo $E(\mathbb{Q})$, denominado por coherencia con la nomenclatura clásica el rango de la curva, es una cantidad mucho más intratable. Por ejemplo no se conoce si hay curvas de rango arbitrario o si, por el contrario, está acotado el grado de libertad de estos grupos. Tampoco se conocen algoritmos eficientes para calcularlos. De hecho, no se conoce ninguno que sea sustancialmente diferente al propuesto por la demostración de Weil. Los algoritmos que se usan en la actualidad admiten, bien una conjetura de Cassels, bien la conjetura de Birch y Swinnerton–Dyer [2] mencionada en la introducción y que, de ser cierta, permitiría calcular el rango de una curva como el orden de un polo de una función meromorfa fácilmente calculable a partir de la curva. La solución a esta conjetura es uno de los siete Problemas del Milenio cuya solución está premiada con un millón de dólares por el Instituto Clay.

I.B. Forma normal de Weierstrass

Toda cúbica afín no singular se puede expresar, salvo equivalencia birracional, como una de las llamadas *formas normales de Weierstrass*. Esto puede probarse usando el teorema de Riemann–Roch, o bien de forma directa.

El algoritmo presentado en [8], por ejemplo (no es fácil hallar referencias explícitas de este resultado), establece la posibilidad, cuando la característica de $\mathbb{K}$ no es 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,

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

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

Salvo mención expresa, a partir de ahora y durante toda la memoria nos ceñiremos al caso $\mathbb{K} = \mathbb{Q}$.

Proposición.– 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 sólo 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 sólo 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 sólo 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 sólo 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 sólo 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

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

Esto concluye la demostración. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Una curva elíptica es no singular por definición, por tanto f tendrá sus tres raíces distintas.

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

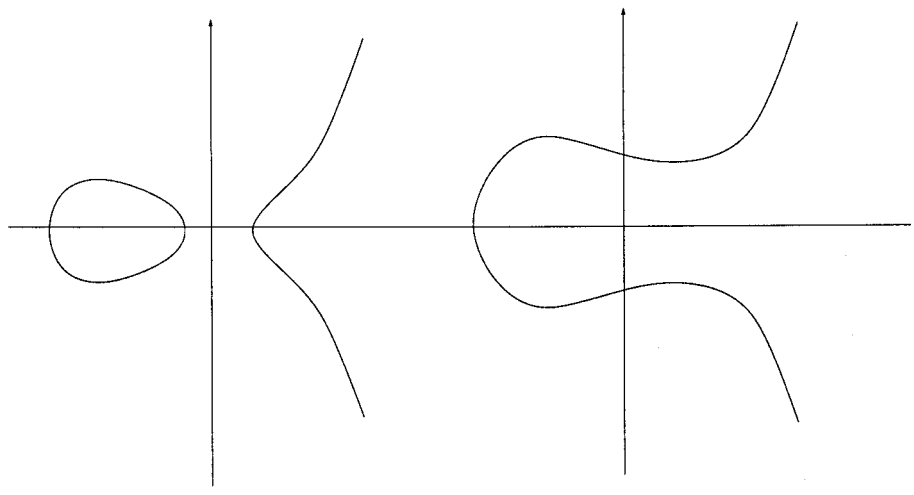
$$Y^2 = f(X) = X^3 + aX^2 + bX + c,$$

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:



Observación.– 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

$$X \longmapsto u^2X' + r, \quad Y \longmapsto u^3Y' + sX' + t,$$

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

En particular, si primero hacemos el cambio

$$Y \longmapsto Y - \frac{a_1X + a_3}{2},$$

renombrando coeficientes resulta

$$Y^2 = X^3 + a_2X^2 + a_4X + a_6,$$

y, si después hacemos el cambio

$$X \longmapsto X - \frac{a_2}{3},$$

queda una ecuación del tipo

$$Y^2 = X^3 + AX + B.$$

Ésta se conoce como forma breve o corta de Weierstrass.

Observación.– También hay otra expresión para la forma breve de Weierstrass de una curva elíptica. Haciendo el cambio

$$X \longmapsto 4X, \qquad Y \longmapsto 4Y,$$

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

$$Y^2 = 4X^3 + AX + B.$$

Observación.– Sea E una curva elíptica en forma breve de Weierstrass

$$Y^2 = X^3 + AX + B,$$

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

$$X \longmapsto u^2X, \qquad Y \longmapsto u^3Y,$$

con $u \in \mathbb{Q} \setminus \{0\}$, se obtiene una forma breve de Weierstrass equivalente a la dada. Del mismo modo, los únicos cambios de variable que conservan formas breves de Weierstrass son del tipo:

$$X \longmapsto u^2X, \qquad Y \longmapsto u^3Y,$$

con $u \in \mathbb{Q} \setminus \{0\}$.

Corolario.– Dada la curva elíptica en forma breve de Weierstrass

$$E: \ Y^2 = X^3 + AX + B,$$

se tiene que A^3/B^2 es un invariante por cambios de variables que conserven la forma breve de Weierstrass.

Definición.– Denominaremos formas de Weierstrass equivalentes a las que se diferencien en un cambio de variables lineal.

Observación.– Hemos visto que dadas dos formas breves de Weierstrass equivalentes

$$Y^2 = X^3 + AX + B, \qquad Y^2 = X^3 + A'X + B',$$

se verifica

$$\frac{A^3}{B^2} = \frac{A'^3}{B'^2}.$$

Pero el recíproco no es cierto. Sean

$$Y^2 = X^3 + AX + B, \quad Y^2 = X^3 + \frac{A}{4}X + \frac{B}{8}.$$

Se verifica

$$\frac{A^3}{B^2} = \frac{(A/4)^3}{(B/8)^2},$$

y sin embargo, en el cambio que habría que hacer para transformar una ecuación en otra habría que tomar $u = \sqrt{2}$. Por tanto, las formas normales de Weierstrass dadas no son equivalentes, a pesar de la relación que hay entre sus coeficientes.

Damos ahora un resultado que caracteriza la equivalencia entre formas breves de Weierstrass.

Proposición.– Sean

$$E: \ Y^2 = X^3 + AX + B, \quad E': \ Y^2 = X^3 + A'X + B',$$

con $A, B, A', B' \in \mathbb{Q}$, curvas elípticas dadas en forma breve de Weierstrass.

Entonces E y E' son equivalentes si y sólo si

$$\exists u \in \mathbb{Q} \text{ tal que } u^4 = \frac{A}{A'}, \ \ u^6 = \frac{B}{B'},$$

con las consideraciones obvias en caso de que algún coeficiente sea 0.

Demostración.– Si E y E' son formas normales de Weierstrass equivalentes, entonces hay un cambio del tipo

$$X \longmapsto u^2X, \qquad Y \longmapsto u^3Y,$$

con $u \in \mathbb{Q} \setminus \{0\}$, que que lleva una en otra.

Escribiendo las ecuaciones, tenemos directamente que $\exists u \in \mathbb{Q} \setminus \{0\}$ tal que

$$u^4 = \frac{A}{A'}, \ \ u^6 = \frac{B}{B'}.$$

Recíprocamente, si $u^4 = A/A', \ \ u^6 = B/B'$, con $u \in \mathbb{Q}$, podemos hacer el cambio

$$X \longmapsto u^2X, \qquad Y \longmapsto u^3Y,$$

y sustituyendo en la ecuación de E resulta una forma normal de Weierstrass equivalente:

$$(u^3Y)^2 = (u^2X)^3 + Au^2X + B.$$

Dividiendo todo por u^6 queda:

$$Y^2 = X^3 + \frac{A}{u^4}X + \frac{B}{u^6},$$

y como

$$\frac{A}{u^4} = A', \quad \frac{B}{u^6} = B',$$

se obtiene una forma normal de Weierstrass equivalente a E que es

$$Y^2 = X^3 + A'X + B'.$$

Así queda probada la equivalencia de E y E'. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– 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 $a, b, c \in \mathbb{Z}$ ya que, haciendo el cambio

$$U = u^2X, \quad V = u^3Y$$

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

$$V^2 = U^3 + u^2aU^2 + u^4bU + u^6c,$$

donde todos los coeficientes son enteros.

Definición.– El discriminante de la curva

$$Y^2 = f(X) = X^3 + aX^2 + bX + c,$$

donde los coeficientes son todos enteros, es el número:

$$\Delta = 4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2 = -(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2,$$

siendo α_1, α_2 y α_3 las raíces de $f(X)$.

Observación.– Se tienen los siguientes resultados inmediatos:

(1) En el caso de ser $a = 0$, o sea, para la forma breve de Weierstrass, se tiene $\Delta = 4b^3 + 27c^2$.

(2) Sabemos que una cúbica de ecuación $Y^2 = f(X)$ (siendo $f(X)$ un polinomio de grado 3) es no singular si y sólo si f tiene sus tres raíces distintas, luego, por la definición de discriminante se tiene que son equivalentes las siguientes afirmaciones:

(i) Las raíces de $f(X)$ son distintas dos a dos.

(ii) La cúbica $Y^2 = f(X)$ es no singular.

(iii) El discriminante de dicha curva es no nulo.

Proposición.– Sea $E:\ Y^2 = f(X)$ una curva elíptica, y denotemos Δ a su discriminante. Se verifica que $\Delta \in (f, f') \subset \mathbb{Z}[X]$, es decir,

$$\exists\, r(X), s(X) \in \mathbb{Z}[X] \ \mid\ \Delta = r(X)f(X) + s(X)f'(X).$$

Demostración.– Para comprobarlo basta tomar

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

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Definición.– Dada una curva elíptica en forma normal de Weierstrass

$$E:\ Y^2 = X^3 + AX + B,$$

con $A, B \in \mathbb{Q}$, se define su j-invariante como el número

$$j = 1728\frac{4A^3}{\Delta},$$

siendo Δ el discriminante de la curva.

Proposición.– Si dos formas normales de Weierstrass son equivalentes, entonces tienen el mismo j-invariante.

Demostración.– Sabemos que dos formas normales de Weierstrass equivalentes han de ser

$$Y^2 = X^3 + AX + B, \quad \text{e} \quad Y^2 = X^3 + \frac{A}{u^4}X + \frac{B}{u^6},$$

con $u \in \mathbb{Q} \setminus \{0\}$.

Los j-invariantes de ambas curvas son

$$j = 1728\frac{4A^3}{\Delta} = 1728\frac{4A^3}{4A^3+27B^2},$$

$$j' = 1728\frac{4A^3/u^{12}}{4A^3/u^{12}+27B^2/u^{12}} = 1728\frac{4A^3}{4A^3+27B^2} = j.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Si dos curvas elípticas en forma normal de Weierstrass tienen el mismo j-invariante, no tienen por qué ser equivalentes. Por ejemplo

$$E:\ Y^2 = X^3 + AX + B, \quad E':\ Y^2 = X^3 + \frac{A}{9}X + \frac{B}{27}$$

tienen el mismo j–invariante, pero no existe $u \in \mathbb{Q}$ tal que $u^4 = 9$ y $u^6 = 27$, es decir, E y E' no son formas normales de Weierstrass equivalentes.

Finalizaremos esta sección con algunos cálculos concretos que nos serán de utilidad posteriormente. Partimos de una curva elíptica E 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 ésta con la curva da un punto triple $\mathcal{O} = (0:1:0)$, que es el punto del infinito del eje OY y un punto de inflexión. Veámoslo: la multiplicidad de intersección de la curva con la tangente en el punto $\mathcal{O} = (0:1:0)$ es 3, es decir $i(E \cap r, \mathcal{O}) = 3$, siendo r la recta tangente a E en $\mathcal{O}$ que es $Z = 0$, o en paramétricas

$$\begin{cases} X &= t, \\ Y &= 1, \\ Z &= 0. \end{cases}$$

En efecto, sustituyendo un punto genérico $(t:1:0)$ de r en E queda:

$$-t^3 = 0,$$

de donde se deduce que $i(\mathcal{O}, E, r) = 3$, lo que prueba que $\mathcal{O}$ es un punto de inflexión de E.

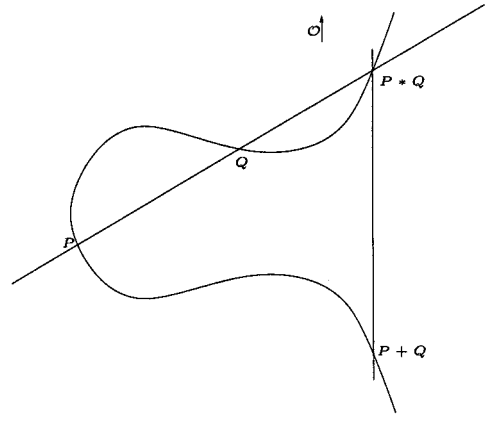
Considerando los puntos afines de la curva y su punto del infinito $\mathcal{O}$, toda recta corta a la curva en tres puntos, contando multiplicidad.

(a) Si la recta es la del infinito, corta en $\mathcal{O}$ tres veces.

(b) Si la recta es de la forma $X = X_0 \neq 0$, corta en dos puntos afines y en $\mathcal{O}$.

(c) Si la recta no es como las anteriores, corta a la curva en tres puntos afines.

Recordemos que para sumar $P + Q$ en una curva elíptica, si tomamos $\mathcal{O} = (0 : 1 : 0)$ como elemento neutro, el tercer punto de intersección de la recta PQ con la curva E es $P * Q$, y la recta que lo une con $\mathcal{O}$ es la paralela al eje OY que pasa por $P * Q$; esta recta cortará a la curva E en el punto $P + Q$ que será el simétrico de $P * Q$ respecto del eje OX.



El opuesto de un punto $Q = (x, y)$ será $-Q = (x, -y)$ (su simétrico respecto del eje OX), ya que $Q * (-Q) = \mathcal{O}$, y como la recta que une $\mathcal{O}$ con $\mathcal{O}$ es la del infinito, el tercer punto de corte con E será también $\mathcal{O}$, luego $Q + (-Q) = \mathcal{O}$.

Vamos a dar ahora una fórmula para sumar dos puntos en una curva elíptica de ecuación

$$Y^2 = f(X) = X^3 + aX^2 + bX + c.$$

Sean $P_1 = (x_1, y_1) \neq P_2 = (x_2, y_2)$; $P_1 * P_2 = (x_3, y_3)$ y $P_1 + P_2 = (x_3, -y_3)$. La recta que une P_1 y P_2 es:

$$Y = mX + n; \quad \text{con} \quad m = \frac{y_2 - y_1}{x_2 - x_1}, \quad n = y_1 - mx_1 = y_2 - mx_2,$$

y esta recta corta a la curva en tres puntos, dos de los cuales son P_1 y P_2, luego:

$$Y^2 = (mX + n)^2 = X^3 + aX^2 + bX + c \Longrightarrow$$
$$X^3 + (a - m^2)X^2 + (b - 2mn)X + (c - n^2) = 0.$$

Pero,

$$X^3 + (a - m^2)X^2 + (b - 2mn)X + (c - n^2) = (X - x_1)(X - x_2)(X - x_3),$$

y si igualamos los términos en X^2 resulta:

$$m^2 - a = x_1 + x_2 + x_3.$$

Por tanto:

$$x_3 = m^2 - a - x_1 - x_2 \ ; \quad y_3 = mx_3 + n.$$

Si lo que queremos es sumar un punto $P = (x, y)$ consigo mismo, es decir, obtener $P + P = 2P = (x', y')$, tendríamos que tomar la recta que une P con P que es la tangente a la curva E por P. Por tanto la pendiente de esta recta es

$$m = \frac{dY}{dX} \mid_P = \frac{f'(X)}{2Y} \mid_P,$$

y la primera coordenada del punto $2P$ será:

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

Esta fórmula es conocida como *fórmula de duplicación.*

I.C. Parametrización en $\mathbb{C}$

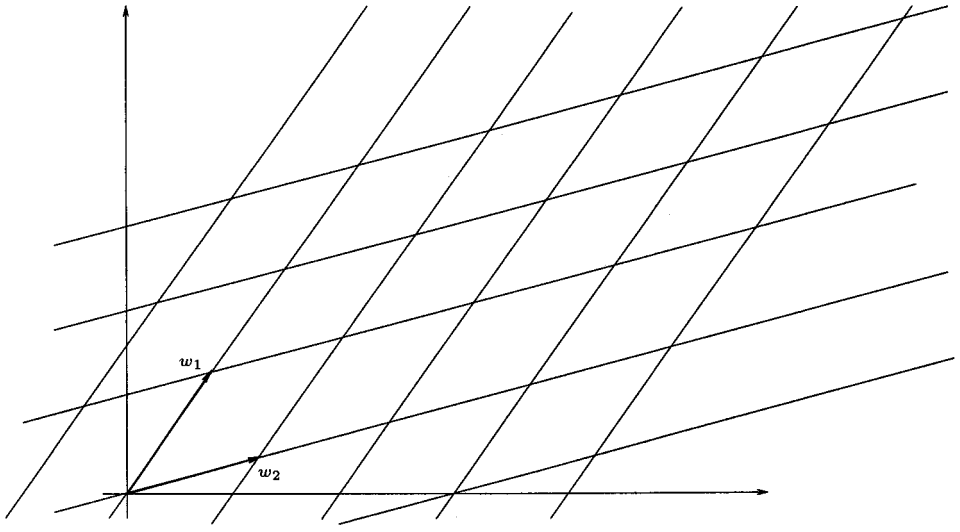
Una forma diferente de ver una curva elíptica procede del análisis complejo y, en ocasiones, permite usar herramientas analíticas para obtener información de la curva. Es lo que vamos a ver brevemente en este punto y el lector interesado puede consultar [8] para los detalles.

Definición.– Dados $\omega_1, \ \omega_2 \ \in \mathbb{C}$, $\mathbb{Z}$–linealmente independientes y un retículo

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

definimos la función $\wp$ de Weierstrass:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\alpha \in \Lambda \\ \alpha \neq 0}} \left(\frac{1}{(z - \alpha)^2} - \frac{1}{\alpha^2}\right).$$



Esta función es meromorfa y sus polos son los puntos del retículo, es decir $z \in \mathbb{C}$ es un polo de $\wp$ si y sólo si $z \in \Lambda \setminus \{0\}$.

La función $\wp(z)$ es doblemente periódica, es decir:

$$\wp(z+\omega_1) = \wp(z) \quad \text{y} \quad \wp(z+\omega_2) = \wp(z), \quad \forall z \in \mathbb{C}.$$

Además $\wp(z)$ verifica la ecuación diferencial siguiente:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

siendo $g_2(\Lambda)$ y $g_3(\Lambda)$ números complejos que dependen del retículo Λ.

Por otra parte, dada una curva elíptica en la forma $Y^2 = 4X^3 + AX + B$, siempre podemos encontrar un retículo Λ en $\mathbb{C}$ tal que

$$g_2(\Lambda) = -A \quad \text{y} \quad g_3(\Lambda) = -B.$$

Lo llamaremos retículo asociado a dicha curva y lo podremos calcular con el algoritmo que daremos al final de esta sección.

Dada una curva elíptica $E : Y^2 = 4X^3 + AX + B$, sean Λ el retículo asociado a la curva y $\omega_1, \omega_2 \in \mathbb{C}$ los generadores del retículo. Entonces, si $E(\mathbb{C})$ es el conjunto de puntos de E con coordenadas complejas, tenemos la siguiente aplicación:

$$\begin{array}{rccll} P: & \mathbb{C} & \longrightarrow & E(\mathbb{C}) & \\ & z & \longmapsto & (\wp(z), \wp'(z)), & \text{si } z \notin \Lambda \\ & z & \longmapsto & \mathcal{O}, & \text{si } z \in \Lambda, \end{array}$$

es decir, si z es un polo de $\wp$, entonces $P(z) = \mathcal{O}$; y además éstos son los únicos z que van a $\mathcal{O}$ (por las consideraciones hechas sobre $\mathcal{O}$ y por la definición de $\wp$).

Esta aplicación es sobreyectiva ya que, si (x, y) es un par de números complejos tales que

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

entonces el par (x, y) es solución de la ecuación diferencial siguiente:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda),$$

es decir, existe un $z \in \mathbb{C}$ tal que

$$x = \wp(z), \quad y = \wp'(z).$$

Por tanto, existe un $z \in \mathbb{C}$ tal que $P(z) = (x, y)$, lo que prueba la sobreyectividad.

Al ser $\wp$ doblemente periódica, la aplicación P no puede ser inyectiva en $\mathbb{C}$, ya que, si tomamos dos números complejos que se diferencien en un punto del retículo, sus imágenes por P son iguales. Es decir, dados $z \in \mathbb{C}$ y $m_1,\ m_2 \in \mathbb{Z}$, como

$$\wp(z) = \wp(z + m_1\omega_1 + m_2\omega_2),$$
$$\wp'(z) = \wp'(z + m_1\omega_1 + m_2\omega_2),$$

se tiene

$$P(z) = P(z + m_1\omega_1 + m_2\omega_2).$$

Así, para cualquier $z \in \mathbb{C}$ existe otro complejo u en el paralelogramo definido por los períodos de $\wp$ tal que

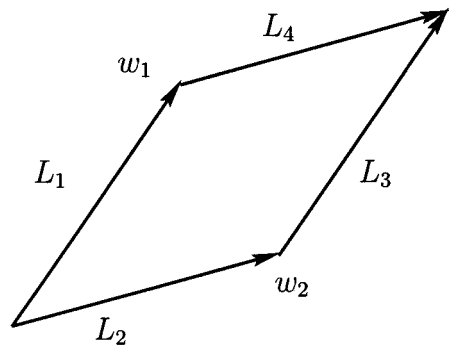
$$P(z) = P(u),$$

lo que significa que podemos restringir P al paralelogramo definido por los períodos de $\wp$, es decir, por ω_1 y ω_2, y en el interior de este recinto tendremos la inyectividad de P.

Los bordes de este paralelogramo son los cuatro segmentos siguientes:

$$\begin{aligned}
L_1 &= \{u \in \mathbb{C} :\ u = \alpha\omega_1 \text{ con } \alpha \in \mathbb{R},\ \ 0 \leq \alpha \leq 1\},\\
L_2 &= \{u \in \mathbb{C} :\ u = \alpha\omega_2 \text{ con } \alpha \in \mathbb{R},\ \ 0 \leq \alpha \leq 1\},\\
L_3 &= \{u \in \mathbb{C} :\ u = \omega_2 + \alpha\omega_1 \text{ con } \alpha \in \mathbb{R},\ \ 0 \leq \alpha \leq 1\},\\
L_4 &= \{u \in \mathbb{C} :\ u = \omega_1 + \alpha\omega_2 \text{ con } \alpha \in \mathbb{R},\ \ 0 \leq \alpha \leq 1\}.
\end{aligned}$$

Tenemos que cada punto $u = \alpha\omega_1 \in L_1$ tiene la misma imagen por la aplicación P que el punto $u = \omega_2 + \alpha\omega_1 \in L_3$, y cada punto $u = \alpha\omega_2 \in L_2$ tiene la misma imagen por P que el punto $u = \omega_1 + \alpha\omega_2 \in L_4$.



Es decir, la aplicación P nos permite identificar los bordes opuestos del paralelogramo definido por ω_1 y ω_2, de manera que se obtiene un toro.

Por otra parte, la aplicación P tiene la siguiente propiedad:

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

donde $u_1 + u_2$ representa la suma usual en $\mathbb{C}$ y $P(u_1) + P(u_2)$ representa la ley interna definida en el conjunto de puntos de la curva elíptica E.

Esta propiedad es consecuencia de las fórmulas dadas para la ley interna definida en E, y de una propiedad de la función $\wp$ que afirma que $\wp(u_1 + u_2)$ y $\wp'(u_1 + u_2)$ admiten una expresión racional en función de $\wp(u_1)$ y $\wp(u_2)$ y de $\wp'(u_1)$ y $\wp'(u_2)$, respectivamente.

Resumiendo, la aplicación

$$P : \mathbb{C} \longrightarrow E(\mathbb{C})$$

es un homomorfismo sobreyectivo cuyo núcleo es Λ (por definición de P). Por tanto, tenemos el siguiente isomorfismo:

$$\begin{array}{rccl} \varphi: & \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \\ & z + \Lambda & \longmapsto & \varphi(z + \Lambda) = (\wp(z), \wp'(z)). \end{array}$$

Y como $\mathbb{C}/\Lambda$ lo podemos representar por el paralelogramo definido por los números complejos 0, ω_1 y ω_2, que es un toro (porque la aplicación P identificaba sus bordes opuestos), se tiene que $E(\mathbb{C})$ es un toro. Es decir, el conjunto de puntos con coordenadas complejas de nuestra curva elíptica es, topológicamente, el producto directo de dos grupos isomorfos cada uno a la circunferencia unidad:

$$E(\mathbb{C}) \simeq S^1 \times S^1$$

siendo $S^1 = \{z \in \mathbb{C} : \mid z \mid = 1\}$.

Observación.– Veamos ahora el algoritmo que nos da una base del retículo asociado a una curva elíptica dada:

Sea E la curva elíptica de ecuación

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

y sea Λ el retículo asociado a dicha curva.

Calcularemos una base de Λ, $\{\omega_1, \omega_2\}$, tal que ω_1 es un número real positivo y ω_2/ω_1 tiene parte imaginaria positiva y parte real igual a 0 ó $-1/2$.

(1) Calculamos b_2, b_4, b_6 y Δ con las siguientes fórmulas:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

- Si $\Delta < 0$ vamos al paso 3.
- Si $\Delta \geq 0$ vamos al paso 2.

(2) Sean e_1, e_2 y e_3 (con $e_1 > e_2 > e_3$), las raíces reales de la ecuación $4X^3 + b_2X^2 + 2b_4X + b_6$. Tomamos entonces

$$\omega_1 = \frac{\pi}{AGM(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})},$$

$$\omega_2 = \frac{i\pi}{AGM(\sqrt{e_1 - e_3}, \sqrt{e_2 - e_3})}.$$

(3) Sea e_1 la única raíz real de $4X^3 + b_2X^2 + 2b_4X + b_6$. Llamamos

$$a = 3e_1 + \frac{b_2}{4} \; ; \quad b = \sqrt{3e_1^2 + \frac{b_2}{2}e_1 + \frac{b_4}{2}}.$$

Tomamos entonces

$$\begin{aligned} \omega_1 &= \frac{2\pi}{AGM(2\sqrt{b}, \sqrt{2b + a})}, \\ \omega_2 &= \frac{-\omega_1}{2} + \frac{i\pi}{AGM(2\sqrt{b}, \sqrt{2b - a})}. \end{aligned}$$

donde *AGM* son las siglas de *Arithmetic-Geometric Mean.* Recordemos que dados dos reales positivos a y b, se define $AGM(a,b)$ como el límite común de las dos sucesiones $(a_n)_{n\in\mathbb{N}}$ y $(b_n)_{n\in\mathbb{N}}$, siendo

$$a_0 = a,\ a_{n+1} = \frac{a_n + b_n}{2},$$

$$b_0 = b,\ b_{n+1} = \sqrt{a_n b_n}.$$

Observación.– Como vimos, el conjunto de puntos reales de una curva elíptica con coeficientes reales tiene una o dos componentes (en la topología euclídea de $\mathbb{R}^2$). La componente que no está acotada se llama "componente de la identidad", porque contiene a $\mathcal{O}$.

La base obtenida con este algoritmo verifica que los múltiplos de $\omega_1/2$ corresponden mediante P a puntos de la componente de la identidad de la curva, y los trasladados de estos múltiplos por $\omega_2/2$ corresponden a la componente acotada (si hay).

I.D. Puntos de orden finito (I)

Estudiaremos en esta sección las primeras propiedades de los puntos del subgrupo de torsión.

Proposición.– Sea E una curva elíptica racional cuya parte afín verifica la ecuación:

$$Y^2 = f(X) = X^3 + aX^2 + bX + c,$$

respecto de cierto sistema de referencia fijado. Se verifica:

1. Un punto $P = (x,y) \in E \setminus \{\mathcal{O}\}$ tiene orden 2 si y sólo si es $y = 0$. Es decir, si y sólo si $f(x) = 0$.

2. Un punto $P = (x,y) \in E \setminus \{\mathcal{O}\}$ es de orden 3 si y sólo si x verifica

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0.$$

3. Un punto es de orden 3 si y sólo si es punto de inflexión.

Demostración.– Consideramos como elemento neutro $\mathcal{O}$ el punto del infinito del eje Y. Es decir, tomamos $\mathcal{O} = (0:1:0)$.

Los puntos de orden 2 son los puntos P de la curva tales que $2P = \mathcal{O}$ y $P \neq \mathcal{O}$, es decir, los puntos P tales que $P + P = \mathcal{O}$ y $P \neq \mathcal{O}$. Pero sabemos que

$$P = -P \Longleftrightarrow (x, y) = (x, -y) \Longleftrightarrow \ y = 0,$$

y esto prueba que un punto $P = (x, y) \in E \setminus \{\mathcal{O}\}$ tiene orden 2 si y sólo si es $y = 0$.

Para ver cómo son los puntos $P \in E$ de orden 3, en vez de $3P = \mathcal{O}$, imponemos la condición

$$2P = -P.$$

Igualando en la fórmula de duplicación x con x', (primera coordenada de $-P$ y de $2P$, respectivamente), se obtiene

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

Operando obtenemos la expresión:

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0,$$

que es la condición que ha de cumplir un punto $P = (x, y) \in E$ para ser de orden 3.

Geométricamente, P es de inflexión si y sólo si

$$i(E \cap r, P) = 3,$$

siendo r la tangente a la curva E en el punto P. Esto equivale a decir que

$$P * P = P.$$

Es decir,

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

o sea, $3P = \mathcal{O}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Lema.– Sea E una curva elíptica de ecuación

$$Y^2 = f(X) = X^3 + aX^2 + bX + c, \quad \text{con } a, b, c \in \mathbb{Z}.$$

Sea $P = (x, y)$ un punto de E tal que P y $2P$ tienen coordenadas enteras. Entonces $y = 0$ o bien $y \mid \Delta$.

Demostración.– Sean $P = (x, y)$ y $2P = (x', y')$ con coordenadas enteras. Supongamos que es $y \neq 0$ y probemos que y divide a Δ. Si $y \neq 0$, entonces $2P \neq \mathcal{O}$. Usando la fórmula de duplicación se tiene,

$$2x + x' = \left(\frac{f'(x)}{2y}\right)^2 - a.$$

Como $a \in \mathbb{Z}$, y también $x, x' \in \mathbb{Z}$, se tiene

$$\left(\frac{f'(x)}{2y}\right)^2 \in \mathbb{Z},$$

pero si un número racional al cuadrado es entero, el número también lo es, es decir,

$$\frac{f'(x)}{2y} \in \mathbb{Z}.$$

Esto significa que $2y$ divide a $f'(x)$, y por tanto que y divide a $f'(x)$.

Por otra parte, como $y^2 = f(x)$ se tiene además que y divide a $f(x)$. En resumen, como el discriminante Δ estaba en el ideal de $\mathbb{Z}[X]$ generado por $f(X)$ y $f'(X)$ tenemos que y divide a Δ como queríamos probar. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Estudiaremos en lo que sigue el teorema de Nagell-Lutz. Este teorema da una condición necesaria para que un punto de una curva elíptica sea un punto de torsión. Además, de su enunciado se deduce un algoritmo que proporciona un conjunto finito de puntos racionales entre los que se encuentran los puntos de torsión de una curva dada.

Antes de dar el teorema veremos unos resultados que usaremos para su demostración. Nuestro objetivo ahora es probar que, en una curva elíptica racional, los puntos racionales de orden finito tienen coordenadas enteras.

Observación.– Sea $p \in \mathbb{Z}$ un número primo.

1. Dado $x \in \mathbb{Q} \setminus \{0\}$, podemos escribir

$$x = \frac{m}{n} p^{\nu},$$

siendo $\text{mcd}(m, n) = \text{mcd}(m, p) = \text{mcd}(n, p) = 1$ y $\nu \in \mathbb{Z}$.

Llamaremos orden de x respecto de p al entero ν, notado:

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

2. Dada una curva elíptica racional E, llamaremos $E(p^\nu)$ al subconjunto de $E(\mathbb{Q})$ definido por:

$$E(p^\nu) = \{(x,y) \in E(\mathbb{Q}) \mid \text{ord}(x) \leq -2\nu,\ \text{ord}(y) \leq -3\nu\}.$$

Proposición.– Sea E una curva elíptica racional cuya parte afín, respecto de un sistema de referencia fijado, viene dada por la ecuación $Y^2 = X^3 + aX^2 + bX + c$, con $a, b, c \in \mathbb{Q}$.

Si (x,y) es un punto de $E(\mathbb{Q})$ tal que

$$\text{ord}(x) = -\mu \quad \text{y} \quad \text{ord}(y) = -\sigma,$$

entonces se verifica:

$$2\sigma = 3\mu.$$

Además, p divide al denominador de x si y sólo si p divide al denominador de y, considerando denominadores para las formas irreducibles de x e y.

Demostración.– La segunda parte de la proposición es equivalente a probar que

$$\mu > 0 \Longleftrightarrow \sigma > 0,$$

y esto es inmediato a partir de la afirmación $2\sigma = 3\mu$ que vamos a probar.

Sabemos que

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

con $m, n, u, w \in \mathbb{Z}$ tales que $\text{mcd}(m,n) = \text{mcd}(u,w) = 1$ y p no divide a m, n, u, w.

Como (x,y) es un punto de la curva, verificará su ecuación. Sustituyendo queda:

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3}{n^3p^{3\mu}} + a\frac{m^2}{n^2p^{2\mu}} + b\frac{m}{np^\mu} + c,$$

y operando se tiene:

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

Vamos a calcular el orden respecto de p de los dos miembros de esta igualdad. Suponíamos que $p \nmid u$ y $p \nmid w$, luego $p \nmid u^2$ y $p \nmid w^2$, por tanto

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

Por otra parte, como $p \nmid m$, se tiene que

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

y por suponer también que $p \nmid n$, resulta:

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

Como hemos calculado el orden respecto de p del mismo número, se tiene:

$$-2\sigma = -3\mu.$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– En la situación de la proposición anterior, al ser $2\sigma = 3\mu$, se tiene que 3 divide a σ y 2 divide a μ. Por tanto, existirá un entero ν tal que

$$\mu = 2\nu \quad \text{y} \quad \sigma = 3\nu.$$

Además, si p divide al denominador de x (considerando x en forma irreducible), entonces será $\mu > 0$, y por la nota anterior será $\mu = 2\nu > 0$. Es decir, $p^{2\nu}$ dividirá al denominador de x, siendo ν un entero positivo. Así se tiene que si p divide al denominador de x, entonces p^2 también lo divide.

Análogamente, sabiendo que $\sigma = 3\nu$, se prueba que si p divide al denominador de y, entonces p^3 también lo divide.

Por convenio se considera

$$\mathcal{O} \in E(p^{\nu}), \quad \forall \nu \in \mathbb{Z}.$$

Por la definición dada para el conjunto $E(p^{\nu})$, se tiene la siguiente cadena de inclusiones:

$$\cdots \subset E(p^3) \subset E(p^2) \subset E(p) \subset E(\mathbb{Q}).$$

Lema.– El conjunto $E(p^{\nu})$ es un subgrupo de $E(\mathbb{Q})$, para cualquier $\nu \in \mathbb{Z}$.

Demostración.– Vamos a hacer el siguiente cambio de coordenadas:

$$T = \frac{X}{Y}, \quad S = \frac{1}{Y}.$$

El cambio inverso será:

$$X = \frac{T}{S}, \quad Y = \frac{1}{S}.$$

Así, la ecuación de la curva que teníamos,

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

si la dividimos por Y^3 queda:

$$\frac{1}{Y} = \left(\frac{X}{Y}\right)^3 + a\left(\frac{X}{Y}\right)^2 \frac{1}{Y} + b\frac{X}{Y}\left(\frac{1}{Y}\right)^2 + c\left(\frac{1}{Y}\right)^3,$$

y sustituyendo, según el cambio resulta la ecuación

$$S = T^3 + aT^2S + bTS^2 + cS^3.$$

Salvo $\mathcal{O}$ y los puntos de orden 2, (es decir los que tienen $Y = 0$), tenemos una correspondencia biyectiva entre los puntos de la curva en el plano (X, Y) y los puntos de la curva en el plano (T, S), donde el elemento neutro para la ley interna definida en la curva es el punto $(0, 0)$.

Dada una recta en el plano (X, Y), si su ecuación es

$$Y = \lambda X + \delta,$$

dividiendo por δY resulta

$$\frac{1}{\delta} = \frac{\lambda}{\delta}\frac{X}{Y} + \frac{1}{Y},$$

es decir, obtenemos una recta en el plano (T, S) cuya ecuación es

$$S = -\frac{\lambda}{\delta}T + \frac{1}{\delta}.$$

Al transformarse rectas en rectas, la ley interna definida para los puntos de la curva es compatible con el cambio de coordenadas realizado. Es decir, dados dos puntos P y Q en el plano (X, Y), y sus correspondientes P' y Q' en el plano (T, S), al cortar la curva con la recta que une P' y Q', el tercer punto de intersección es el correspondiente por el cambio al tercer punto de intersección de la curva con la recta que une los puntos P y Q en el plano (X, Y).

Consideramos ahora, para un entero primo p fijado, el anillo

$$R = \mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \setminus \{0\} \ : \ \mathrm{ord}(x) \geq 0\} \cup \{0\}.$$

En este subanillo de $\mathbb{Q}$ las unidades son los racionales tales que p no divide a su denominador ni a su numerador.

Sea $(x, y) \in E(p^\nu)$ un punto racional de nuestra curva E. Se tiene:

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

para cierto $i \geq 0$. Así

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

Para ver que $E(p^\nu)$ es un subgrupo, veremos que si $P_1(x_1, y_1)$ y $P_2(x_2, y_2)$ están en $E(p^\nu)$, entonces $P_1 + P_2$ también está. Esto es, habrá que ver que si p^ν divide a la coordenada t de cada sumando, también divide a la coordenada t de la suma.

No hace falta probar nada sobre s, porque si probamos que $t \in p^\nu R$, como $x \in p^{-2\nu}R$, al ser $s = t/x$ se tendrá lo que necesitamos, por la proposición anterior.

Sean $P_1(t_1, s_1)$ y $P_2(t_2, s_2)$ puntos distintos en la curva. Distinguimos dos casos:

En el primer caso tenemos $t_1 = t_2$. Entonces la recta que une P_1 con P_2 es $T = t_1$. Al cortar esta recta con la curva, obtenemos un punto cuya primera coordenada será también t_1. Así, el punto P_1+P_2 tiene como primera coordenada $-t_1$, por ser la curva impar en el plano (T, S). Por tanto

$$P_1 + P_2 \in E(p^\nu).$$

En el segundo caso tenemos $t_1 \neq t_2$. Entonces la recta que une P_1 con P_2 tiene por ecuación

$$P_1P_2\ :\ S = \alpha T + \beta, \qquad \text{con} \qquad \alpha = \frac{s_2 - s_1}{t_2 - t_1}.$$

Como P_1 y P_2 satisfacen la ecuación de la curva:

$$S = T^3 + aT^2S + bTS^2 + cS^3,$$

sustituyendo y restando resulta:

$$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2s_2 - t_1^2s_1) + b(t_2s_2^2 - t_1s_1^2) + c(s_2^3 - s_1^3).$$

Reagrupando los términos, de manera que cada sumando tenga como

factor a $(s_2 - s_1)$ ó $(t_2 - t_1)$, podremos despejar α a partir de esta expresión:

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

De esto obtenemos:

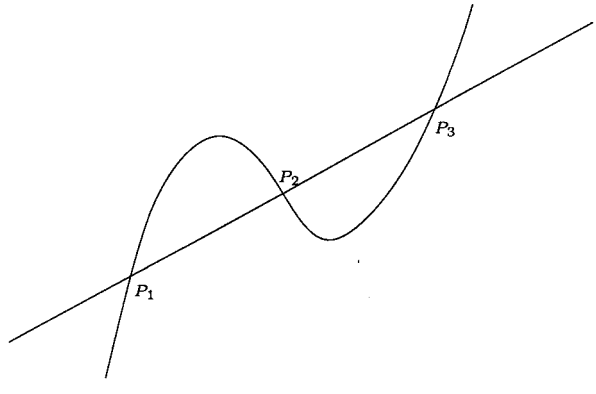
$$\begin{aligned} (s_2 - s_1)[1 - a t_1^2 - b(s_2 + s_1)t_1 - c(s_2^2 + s_2 s_1 + s_1^2)] = \\ = (t_2 - t_1)[t_2^2 + t_2 t_1 + t_1^2 + a(t_2 + t_1)s_2 + b s_2^2]. \end{aligned}$$

Por tanto, podemos escribir:

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_2 t_1 + t_1^2 + a(t_2 + t_1)s_2 + b s_2^2}{1 - a t_1^2 - b(s_2 + s_1)t_1 - c(s_2^2 + s_2 s_1 + s_1^2)} ,$$

donde α es la pendiente de la recta que une P_1 y P_2.

Llamamos $P_3(t_3, s_3)$ al tercer punto de corte de la recta P_1P_2 con la curva.



Como $S = \alpha T + \beta$ es una recta que corta a la curva en P_1, P_2 y P_3, si sustituimos S por $\alpha T + \beta$ en la ecuación de la curva, obtendremos una ecuación en T cuyas raíces son t_1, t_2 y t_3. Dicha ecuación es:

$$\alpha T + \beta = T^3 + aT^2(\alpha T + \beta) + bT(\alpha T + \beta)^2 + c(\alpha T + \beta)^3 ,$$

y agrupando términos queda:

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

Ahora, por las relaciones de Cardano, podemos afirmar que

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

Tenemos P_1, P_2 y P_3, y si consideramos la recta que une $P_3(t_3,s_3)$ con $(0,0)$, y la cortamos con la curva, obtenemos el punto

$$P_1+P_2=(-t_3,-s_3),$$

de nuevo por ser la curva impar en (T,S).

Queríamos probar que si p^ν divide a t_1 y t_2, entonces p^ν divide también a $-t_3$, primera coordenada de P_1+P_2. Sabíamos que $s_1,\ s_2 \in p^{3\nu}R$ y $t_1,\ t_2 \in p^\nu R$, por tanto,

$$t_2^2+t_2t_1+t_1^2+a(t_2+t_1)s_2+bs_2^2 \ \in p^{2\nu}R,$$

es decir, $p^{2\nu}$ divide al numerador de α.

Además,

$$at_1^2+b(s_2+s_1)t_1-c(s_2^2+s_2s_1+s_1^2) \ \in p^{2\nu}R,$$

por tanto, $1-at_1^2-b(s_2+s_1)t_1+c(s_2^2+s_2s_1+s_1^2)$ es una unidad en R, es decir, el denominador de α es una unidad en R. Así, por dividir $p^{2\nu}$ al numerador de α y ser su denominador una unidad en R, se tiene que

$$\alpha \ \in p^{2\nu}R.$$

Por otra parte, como P_1 es un punto de la recta $S=\alpha T+\beta$, se tiene que $\beta=s_1-\alpha t_1$, y como $s_1 \in p^{3\nu}R$, $\alpha \ \in p^{2\nu}R$ y $t_1 \in p^\nu R$, resulta

$$\beta \ \in p^{3\nu}R.$$

Así,

$$a\beta+2b\alpha\beta+3c\alpha^2\beta \ \in p^{3\nu}R,$$

y además

$$a\alpha+b\alpha^2+c\alpha^3 \ \in p^{2\nu}R,$$

es decir, $1+(a\alpha+b\alpha^2+c\alpha^3)$ es una unidad en R.

Por la expresión obtenida anteriormente para $t_1 + t_2 + t_3$, sabemos que su numerador está en $p^{3\nu}R$ y su denominador es una unidad en R. Con esto tenemos que

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

Por tanto, como $t_1,\ t_2\ \in p^{\nu}R$, se llega a que

$$-t_3\ \in p^{\nu}R$$

como queríamos probar. $\mathcal{Q.E.D.}$

Observación.– Dado un punto $P = (x(P), y(P))$, al hacer el cambio resulta $P = (t(P), s(P))$, siendo

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

Hemos probado además lo siguiente:

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

dicho de otra forma,

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

Tenemos definido entonces el siguiente homomorfismo

$$\begin{array}{ccc} E(p^{\nu}) & \longrightarrow & p^{\nu}R/p^{3\nu}R \\ P & \longmapsto & t(P), \end{array}$$

cuyo núcleo vamos a probar que es $E(p^{3\nu})$. Por una parte, si $P = (x, y) \in E(p^{\nu})$ entonces

$$x = \frac{m}{n}p^{-2(\nu+i)}, \quad y = \frac{u}{w}p^{-3(\nu+i)},$$

y será

$$t(P) = \frac{x}{y} = \frac{mw}{nu}p^{\nu+i},$$

con $i \in \mathbb{Z}$ positivo. Pero, si $P = (x, y)$ está en el núcleo de esta aplicación, se tendrá $t(P) \in p^{3\nu}R$, y será $i \geq 2\nu$. Así tenemos, para cierto $j \in \mathbb{Z}$,

$$x = \frac{m}{n}p^{-2(3\nu+j)}\ , \quad y = \frac{u}{w}p^{-3(3\nu+j)},$$

y esto prueba que $P = (x, y) \in E(p^{3\nu})$.

Por tanto tenemos una correspondencia inyectiva

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

Ahora, dada la clase

$$p^\nu + p^{3\nu}R \in p^\nu R/p^{3\nu}R,$$

al multiplicarla por $p^{2\nu}$ resulta

$$p^{2\nu}(p^\nu + p^{3\nu}R) = p^{3\nu} + p^{3\nu}R = 0 + p^{3\nu}R,$$

y $p^{2\nu}$ es el menor entero que cumple esto, luego

$$p^\nu R/p^{3\nu}R = \langle\, p^\nu + p^{3\nu}R \,\rangle$$

es un grupo cíclico de orden $p^{2\nu}$.

Por tanto, por la correspondencia inyectiva dada, se tendrá que

$$E(p^\nu)/E(p^{3\nu})$$

es un grupo cíclico de orden p^σ con $0 \leq \sigma \leq 2\nu$.

Vamos a demostrar ahora un resultado importante para el teorema de Nagell-Lutz.

Proposición.– Sea E una curva elíptica racional.

1. Dado un primo $p \in \mathbb{Z}$, el subgrupo $E(p)$ no contiene puntos de orden finito.
2. Sea $P=(x,y) \neq \mathcal{O}$ un punto racional de orden finito en la curva E, entonces x e y son números enteros.

Demostración.– Trataremos los dos resultados por separado. En el primer apartado, razonaremos por reducción al absurdo. Sea $P \neq \mathcal{O}$ un punto tal que $mP=\mathcal{O}$, para cierto $m \in \mathbb{N}$. Supongamos que $P \in E(p)$.

Como el denominador de $x(P)$ es un número finito, no se podrá dividir por potencias de p arbitrariamente grandes, es decir:

$$\exists \nu > 0 \mid P \in E(p^\nu) \quad \text{y} \quad P \notin E(p^{\nu+1}).$$

Distinguimos dos casos:

(a) Si $p \nmid m$. Sabíamos que

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

por tanto

$$0 = t(\mathcal{O}) = t(mP) \equiv mt(P) \pmod{p^{3\nu}R}.$$

Esto significa que $mt(P) \in p^{3\nu}R$, y como $p \nmid m$, se tiene

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

Si recordamos el núcleo del homomorfismo que definimos entre $E(p^\nu)$ y $p^\nu R/p^{3\nu}R$, veremos que $P \in E(p^{3\nu})$, lo que contradice que $P \notin E(p^{\nu+1})$, por ser $3\nu > \nu + 1$ y $E(p^{3\nu}) \subset E(p^{\nu+1})$.

(b) Si $p \mid m$. Escribimos entonces $m = pn$ para cierto natural n. Consideramos P' un punto tal que $P' = nP$, así el orden de P' es p (por ser m el orden de P).

Como $P \in E(p)$ y sabíamos que $E(p)$ era un grupo, se tiene $nP = P' \in E(p)$, es decir,

$$\exists \nu > 0 \mid P' \in E(p^\nu) \text{ y } P' \notin E(p^{\nu+1}).$$

Razonando como antes tenemos:

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

luego $t(P') \equiv 0 \pmod{p^{3\nu-1}R}$, y recordando de nuevo el homomorfismo anterior se tiene $P' \in E(p^{3\nu-1})$, lo que contradice que $P' \notin E(p^{\nu+1}) \supset E(p^{3\nu-1})$.

Para probar el segundo apartado de la proposición suponemos que $P = (x, y) \neq \mathcal{O}$ es un punto racional de la curva de orden finito, entonces, por el primer apartado, sabemos que $P \notin E(p)$, siendo p un entero primo cualquiera.

Es decir, ningún primo dividirá el denominador de x ni el de y. Esto significa que x e y son números enteros. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Enunciemos y demostremos ahora una primera versión del teorema de Nagell-Lutz [21, 27].

Teorema.– Sea E una curva elíptica de ecuación: $Y^2 = X^3 + AX + B$, con $A, B \in \mathbb{Z}$, y sea $\Delta = 4A^3 + 27B^2$ su discriminante.

Si $P = (x, y)$ es un punto de $\mathrm{Tor}(E(\mathbb{Q}))$, entonces se verifica:

(i) $x,\ y \in \mathbb{Z}$.

(ii) $y = 0$ o bien $y|\Delta$.

Demostración.– La primera parte del teorema está probada en la proposición anterior. Veamos la segunda parte. Distinguiremos dos casos:

(a) Si P es un punto de orden 2, entonces $y = 0$.

(b) Si P no es un punto de orden 2, entonces $2P \neq \mathcal{O}$. Esto significa que $2P$ es un punto afín de orden finito, y por tanto, por la proposición anterior, P y $2P$ tienen coordenadas enteras, luego (por un lema anterior) al ser $y \neq 0$, se tiene que y divide a Δ. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

I.E. Puntos de orden finito (II): Reducción

Observación.– Veremos ahora una versión más fuerte del teorema de Nagell–Lutz, que se suele usar sobre todo en aspectos computacionales, donde probaremos que, si $P = (x, y)$ es un punto racional de orden finito con $y \neq 0$, se tiene que $y^2|\Delta$. Esto nos llevará a técnicas completamente distintas. En concreto, trataremos de acercarnos a $\mathbb{Q}$ a través de los cuerpos de números p-ádicos $\mathbb{Q}_p$, siendo p un entero primo. Además, vamos a relacionar $\mathbb{Q}_p$ con los cuerpos finitos $\mathbb{F}_p$, mediante la reducción módulo p (ver [5] para una introducción detallada).

Definición.– Sea p un primo. Dado $r \in \mathbb{Q} \setminus \{0\}$, se define la norma p-ádica de r como

$$|r|_p = p^{-\mathrm{ord}(r)}.$$

Si $r = 0$, se define $|0|_p = 0$.

Recordemos que los enteros p-ádicos $\mathbb{Z}_p$ son los $\alpha \in \mathbb{Q}_p$ de la forma

$$\alpha = \sum_{n=0}^{\infty} a_n p^n,$$

con $a_n \in \{0,\ 1,\ \cdots,\ p-1\}$.

Así, la aplicación de reducción módulo p es:

$$\begin{array}{rcl} red_p : \mathbb{Z}_{(p)} & \longrightarrow & \mathbb{F}_p \\ \alpha & \longmapsto & a_0 = \overline{\alpha} \end{array}$$

Esto se puede extender a los planos proyectivos correspondientes $\mathbb{P}^2(\mathbb{Q}_p)$ y $\mathbb{P}^2(\mathbb{F}_p)$ como veremos ahora. Sea $(\alpha_1 : \alpha_2 : \alpha_3) \in \mathbb{P}^2(\mathbb{Q}_p)$, como el punto del proyectivo $(\alpha_1 : \alpha_2 : \alpha_3)$ es el mismo que el punto $(\alpha_1 p^{-n} : \alpha_2 p^{-n} : \alpha_3 p^{-n})$ para todo $n \in \mathbb{Z}$, siempre podemos suponer que, dado un punto de $\mathbb{P}^2(\mathbb{Q}_p)$, el máximo de las normas p-ádicas de sus coordenadas es 1.

Así, la reducción módulo p de $\mathbb{P}^2(\mathbb{Q}_p)$ en $\mathbb{P}^2(\mathbb{F}_p)$ es:

$$\begin{array}{rcl} \mathbb{P}^2(\mathbb{Q}_p) & \longrightarrow & \mathbb{P}^2(\mathbb{F}_p) \\ \alpha = (\alpha_1 : \alpha_2 : \alpha_3) & \longmapsto & \overline{\alpha} = (\overline{\alpha}_1 : \overline{\alpha}_2 : \overline{\alpha}_3)\ , \end{array}$$

que está bien definida, por poder suponer que algún α_i es tal que $|\alpha_i|_p = 1$.

De forma análoga, dada la recta

$$r: \quad r_1 X_1 + r_2 X_2 + r_3 X_3 = 0$$

en $\mathbb{P}^2(\mathbb{Q}_p)$, definimos su reducción módulo p:

$$\overline{r}: \quad \overline{r_1} X_1 + \overline{r_2} X_2 + \overline{r_3} X_3 = 0,$$

que será una recta en $\mathbb{P}^2(\mathbb{F}_p)$. Así, si un punto α está en la recta r, entonces $\overline{\alpha}$ estará en $\overline{r}$.

Sea $E : F(X_1, X_2, X_3) = 0$ una cúbica definida en $\mathbb{P}^2(\mathbb{Q}_p)$. Es decir,

$$F(X_1, X_2, X_3) = \sum_{i \le j \le k} f_{ijk} X_i X_j X_k \quad \in \mathbb{Q}_p[X_1, X_2, X_3],$$

donde $f_{ijk} \in \mathbb{Q}_p$ no son todos nulos.

Como antes, podemos suponer que

$$\max_{i,j,k} |f_{ijk}|_p = 1;$$

y considerar

$$\overline{F}(X_1, X_2, X_3) = \sum_{i \le j \le k} \overline{f}_{ijk} X_i X_j X_k \quad \in \mathbb{F}_p[X_1, X_2, X_3]$$

que es un polinomio no nulo que define la curva $\overline{E}$:

Observación.– Notemos los siguientes hechos:

1. La reducción $\overline{E}$ puede ser una curva reducible.

2. Si un punto α está en E, entonces $\overline{\alpha}$ estará en $\overline{E}$. Pero el recíproco necesitará una condición adicional.

Proposición.– Sea $\overline{\beta}$ un punto no singular de $\overline{E}$. Entonces, existe un punto α de E tal que $\overline{\alpha} = \overline{\beta}$.

Demostración.– Como $\overline{\beta}$ es no singular, será, por ejemplo

$$\frac{\partial \overline{F}}{\partial X_1}(\overline{\beta}) \neq 0.$$

Tomamos $\beta_1, \beta_2, \beta_3 \in \mathbb{Z}_{(p)}$ tales que $\overline{\beta} = (\overline{\beta}_1 : \overline{\beta}_2 : \overline{\beta}_3)$, y consideramos

$$G(T) = F(T, \beta_2, \beta_3) \in \mathbb{Z}_p[T] \ , \quad t_0 = \beta_1.$$

Se verifica

$$|G(t_0)|_p = |G(\beta_1)|_p = |F(\beta_1, \beta_2, \beta_3)|_p < 1,$$

por ser $F(\beta_1, \beta_2, \beta_3) \equiv \overline{F}(\overline{\beta}_1, \overline{\beta}_2, \overline{\beta}_3) \pmod{p} \equiv 0 \pmod{p}$.

Y además:

$$G'(t_0) = G'(\beta_1) \equiv \frac{\partial \overline{F}}{\partial X_1}(\overline{\beta}) \pmod{p} \not\equiv 0 \pmod{p},$$

por tanto

$$|G'(t_0)|_p = 1.$$

Es decir, tenemos que $G(T) = F(T, \beta_2, \beta_3)$ y $t_0 = \beta_1$ cumple las condiciones del lema de Hensel. Luego,

$$\exists t \in \mathbb{Z}_p \ \mid \ G(t) = 0 \quad \text{y} \quad |t - \beta_1|_p < |G(\beta_1)|_p.$$

Si tomamos $\alpha = (t : \beta_2 : \beta_3)$, resulta

$$F(\alpha) = F(t, \beta_2, \beta_3) = G(t) = 0,$$

y además

$$|t - \beta_1|_p < |G(\beta_1)|_p < 1,$$

por tanto $t - \beta_1 \equiv 0 \pmod{p}$, es decir $\overline{t} = \overline{\beta}_1$, y así $\overline{\alpha} = \overline{\beta}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Veamos ahora cómo se comporta la intersección de una recta y una cúbica al reducir módulo p. Sabemos que si una recta r corta a una curva E en un punto α, entonces $\overline{r}$ cortará a $\overline{E}$ en $\overline{\alpha}$. Pero si r corta a E en α y β tales que $\alpha \neq \beta$ y $\overline{\alpha} = \overline{\beta}$, no sabemos aún si tiene multiplicidad mayor o igual que 2 la intersección de $\overline{r}$ con $\overline{E}$ en el punto $\overline{\alpha}$. El siguiente resultado responde a nuestra pregunta.

Proposición.– Sea r una recta y E una cúbica que se cortan en α, β y γ distintos.

Entonces, se verifica una de las dos afirmaciones siguientes:

(i) La recta $\overline{r}$ está contenida en $\overline{E}$.

(ii) $\overline{r}$ corta a $\overline{E}$ en $\overline{\alpha}$, $\overline{\beta}$ y $\overline{\gamma}$.

Demostración.– Sin pérdida de generalidad, si es

$$r: \ r_1X_1 + r_2X_2 + r_3X_3 = 0,$$

podemos suponer que

$$r_3 = 1 = \max\{|r_1|_p, |r_2|_p, |r_3|_p\}.$$

Si despejamos X_3 en la ecuación de r y sustituimos en la ecuación de E, resulta

$$G(X_1, X_2) = F(X_1, X_2, -r_1X_1 - r_2X_2) \ \in \mathbb{Z}_{(p)}[X_1, X_2].$$

Su reducción módulo p es:

$$\overline{G}(X_1, X_2) = \overline{F}(X_1, X_2, -\overline{r}_1X_1 - \overline{r}_2X_2).$$

Si $\overline{G}(X_1, X_2) = 0$, entonces la recta $\overline{r}$ estará contenida en $\overline{E}$, con lo que se verificaría (i). Supongamos entonces que

$$\overline{G}(X_1, X_2) \neq 0,$$

y probemos (ii).

Podemos tomar $\alpha = (\alpha_1 : \alpha_2 : \alpha_3)$, $\beta = (\beta_1 : \beta_2 : \beta_3)$ y $\gamma = (\gamma_1 : \gamma_2 : \gamma_3)$ tales que

$$\max\{|\alpha_1|_p, |\alpha_2|_p, |\alpha_3|_p\} = \max\{|\beta_1|_p, |\beta_2|_p, |\beta_3|_p\} =$$

$$= \max\{|\gamma_1|_p, |\gamma_2|_p, |\gamma_3|_p\} = 1.$$

Como α, β y γ están en r, entonces $\overline{\alpha}$, $\overline{\beta}$ y $\overline{\gamma}$ verificarán la ecuación de $\overline{r}$. Por tanto:

$$(\overline{\alpha}_1, \overline{\alpha}_2), (\overline{\beta}_1, \overline{\beta}_2)\ , \overline{\gamma}_1, \overline{\gamma}_2) \neq (0,0),$$

si no, serían puntos del proyectivo con sus tres coordenadas nulas.

Por hipótesis podemos encontrar un $\lambda \in \mathbb{Q}_p$ tal que

$$\begin{aligned} G(X_1, X_2) &= \lambda(\alpha_2 X_1 - \alpha_1 X_2)(\beta_2 X_1 - \beta_1 X_2)(\gamma_2 X_1 - \gamma_1 X_2) \\ &= \lambda H(X_1, X_2). \end{aligned}$$

Se tiene entonces:

$$\overline{H}(X_1, X_2) = (\overline{\alpha}_2 X_1 - \overline{\alpha}_1 X_2)(\overline{\beta}_2 X_1 - \overline{\beta}_1 X_2)(\overline{\gamma}_2 X_1 - \overline{\gamma}_1 X_2) \neq 0.$$

Por tanto, $\overline{G}$ y $\overline{H}$ verifican que uno es un escalar por el otro, y así se tiene el resultado. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Si tenemos $E:\ Y^2 = X^3 + AX + B$, una curva elíptica definida sobre $\mathbb{Q}_p$, con $4A^3 + 27B^2 \neq 0$, haciendo cambios

$$X \longrightarrow u^2 X, \qquad Y \longrightarrow u^3 Y$$

podemos suponer que $A, B \in \mathbb{Z}_p$.

Tomamos $E(\mathbb{Q}_p)$, consideramos la ecuación de E en el proyectivo $\mathbb{P}^2(\mathbb{Q}_p)$:

$$E:\ Y^2 Z = X^3 + AXZ^2 + BZ^3,$$

y reducimos a $\mathbb{F}_p$

$$\overline{E}:\ Y^2 Z = X^3 + \overline{A}XZ^2 + \overline{B}Z^3,$$

que puede ser singular (si $\overline{\Delta} = 0$), pero es irreducible como se podría comprobar. Consideramos:

- En $\overline{E}$; el conjunto $\overline{E}(\mathbb{F}_p)$ de puntos de $\overline{E}$ en $\mathbb{P}_2(\mathbb{F}_p)$ (que no es un grupo), y el conjunto $\overline{E}(\mathbb{F}_p)^{(0)}$ de puntos no singulares (que sí lo es).

- En E; el conjunto $E(\mathbb{Q}_p)^{(0)}$ de puntos $P = (x : y : z)$ de $E(\mathbb{Q}_p)$, con $x, y, z \in \mathbb{Z}_{(p)}$ y $\max\{|x|_p, |y|_p, |z|_p\} = 1$, tales que $\overline{P} = (\overline{x} : \overline{y} : \overline{z}) \in \overline{E}(\mathbb{F}_p)^{(0)}$.

Por un resultado anterior, sabemos que todo punto no singular de $\overline{E}$ se levanta a un punto de E, luego la aplicación natural

$$red\,|_{E(\mathbb{Q}_p)^{(0)}}:\ E(\mathbb{Q}_p)^{(0)} \longrightarrow \overline{E}(\mathbb{F}_p)^{(0)}$$

es sobreyectiva.

Ahora hay que ver cómo afecta la reducción a la estructura de grupo. La estructura de grupo de una curva elíptica se puede definir de manera alternativa, diciendo $P+Q+R=\mathcal{O}$ si y sólo si P, Q y R están alineados, (esto es, cuando $\mathcal{O}$ es de inflexión, como es el caso). Veamos por qué:

(a) Dado un punto P, $-P$ ha de ser el tercer punto de corte de E con la recta $\mathcal{O}P$, ya que debe cumplirse $P+(-P)+\mathcal{O}=\mathcal{O}$.

(b) Dados $P,Q\in E$, para calcular $P+Q$ sólo hay que imponer $P+Q+(-P-Q)=\mathcal{O}$, luego $-P-Q$ es el tercer punto de corte de E con la recta PQ. Con el apartado (a) se puede calcular $P+Q$.

Así, imponer que $P+Q+R=\mathcal{O}$ si y sólo si P, Q y R están alineados, es equivalente a la definición de grupo por el método habitual.

Por la proposición anterior, se tiene que si $P+Q+R=\mathcal{O}$, entonces $\overline{P}+\overline{Q}+\overline{R}=\overline{\mathcal{O}}$. En particular, como en $\overline{E}$ sólo tiene sentido tomar puntos no singulares, tiene que ser $P,Q\in E(\mathbb{Q}_p)^{(0)}$, por tanto $P+Q\in E(\mathbb{Q}_p)^{(0)}$, ya que si $\overline{P+Q}$ es singular, $\overline{P}+\overline{Q}$ lo sería.

Luego tenemos que

$$red\,|_{E(\mathbb{Q}_p)^{(0)}}:\ E(\mathbb{Q}_p)^{(0)}\ \longrightarrow\ \overline{E}(\mathbb{F}_p)^{(0)}$$

es un homomorfismo de grupos.

Veamos el núcleo de la reducción. Sea $P=(x:y:z)\in E$ con $P\neq(0:1:0)$, $x,y,z\in\mathbb{Z}$ y $\max\{|x|_p,|y|_p,|z|_p\}=1$, tal que

$$(\overline{x}:\overline{y}:\overline{z})=(0:1:0)\ \in\ \overline{E}(\mathbb{F}_p)^{(0)},$$

o sea,

$$|y|_p=1,\ \ |x|_p,\ |z|_p<1.$$

Supongamos que $|z|_p=|x|_p$. Entonces, como $zy^2=x^3+Axz^2+Bz^3$, se tiene

$$|zy^2|_p=|z|_p=|x^3+Axz^2+Bz^3|_p\leq\max\{1,|A|_p,|B|_p\}|z|_p^3\ =\ |z|_p^3,$$

lo que contradice el hecho de ser $|z|_p<1$.

Supongamos que $|z|_p>|x|_p$. Análogamente se tiene

$$|zy^2|_p=|z|_p=|x^3+Axz^2+Bz^3|_p\leq\max\{|x|_p^3,|A|_p|x|_p|z|_p^2,|B|_p|z|_p^3\},$$

y cualquiera de los tres casos posibles da contradicción. Luego, ha de ser $|z|_p < |x|_p$. Entonces P, en coordenadas afines,

$$P = \left(\frac{x}{z}, \frac{y}{z}\right) = (a, b)$$

verifica

$$|a|_p = \frac{|x|_p}{|z|_p} > 1 \quad \text{y} \quad |b|_p = \frac{|y|_p}{|z|_p} > 1,$$

es decir

$$a,\ b \notin \mathbb{Z}_{(p)}.$$

Por otro lado, si un punto afín $Q = (c, d)$ de la curva verifica que $c, d \notin \mathbb{Z}_{(p)}$, tenemos

$$|d|_p^2 = |c^3 + Ac + B|_p = |c|_p^3,$$

porque es el máximo en norma de los tres sumandos, luego $|d|_p^2 = |c|_p^3$. Si homogeneizamos tendremos $Q = (c : d : 1)$ y, al pasar a la forma usual, obtendremos $Q = (\alpha c : \alpha d : \alpha)$ tal que

$$\max\{|\alpha c|_p, |\alpha d|_p, |\alpha|_p\} = 1,$$

pero este máximo ha de ser $|\alpha d|_p$, ya que $|c|_p, |d|_p > 1$ y $|d|_p^2 = |c|_p^3$.

Luego, las coordenadas del punto Q verifican

$$\begin{array}{l} \alpha c \in \mathbb{Z}_{(p)},\ |\alpha c|_p < |\alpha d|_p = 1 \\ |\alpha|_p < |\alpha d|_p = 1, \end{array}$$

de donde la reducción de Q es $(0 : 1 : 0)$. Por tanto, el núcleo de $red\,|_{E(\mathbb{Q}_p)^{(0)}}$ son los puntos afines (a, b) con $a, b \notin \mathbb{Z}_{(p)}$ y, además, el punto $(0 : 1 : 0)$.

Como hemos visto, en este caso (a, b) verifica $|b|_p^2 = |a|_p^3$, o sea

$$|a|_p = p^{2n}\ , \quad |b|_p = p^{3n}\ ,$$

para cierto $n \geq 1$, porque $a, b \notin \mathbb{Z}_{(p)}$.

Definición.– Llamamos a n el *nivel* de $P = (a, b)$, notado $\mathrm{nv}(P)$. Si un punto no se reduce a $(0 : 1 : 0)$ diremos que tiene nivel 0, y el $(0 : 1 : 0)$ tendrá nivel infinito.

Ahora fijamos un entero $N \geq 1$ y hacemos el siguiente cambio:

$$\left\{ \begin{array}{rcl} X & = & p^{-2N} X \\ Y & = & p^{-3N} Y \\ Z & = & Z, \end{array} \right.$$

entonces

$$\begin{aligned}(x:y:z) &\longmapsto (xp^{2N}:yp^{3N}:z),\\ (a,b) &\longmapsto (ap^{2N},bp^{3N}).\end{aligned}$$

Con lo que la ecuación queda

$$E_N:\ Y^2Z = X^3 + p^{4N}AXZ^2 + p^{6N}BZ^3.$$

Así, reduciendo tenemos

$$\overline{E_N}:\ Y^2Z = X^3.$$

Dado $(a,b) \in E$, tenemos su correspondiente $(ap^{2N},bp^{3N}) \in E_N$. Si (ap^{2N},bp^{3N}) se reduce al punto singular $(0,0) \in \overline{E_N}$, eso quiere decir $|ap^{2N}|_p, |bp^{3N}|_p < 1$, o sea

$$|a|_p < p^{2N}, \quad |b|_p < p^{3N},$$

o lo que es lo mismo, el nivel de (a,b) es menor que N.

Veamos cuándo el punto (ap^{2N},bp^{3N}) está en el núcleo de reducción, es decir, cuándo se reduce al $(0:1:0)$. Esto ocurre, como antes, cuando $ap^{2N}, bp^{3N} \notin \mathbb{Z}_{(p)}$, es decir, cuando

$$|ap^{2N}|_p,\ |bp^{3N}|_p\ >\ 1;$$

esto equivale a decir que $|a|_p > p^{2N}$ y $|b|_p > p^{3N}$. Dicho de otro modo, el punto (ap^{2N},bp^{3N}) está en el núcleo de reducción cuando (a,b) tiene nivel mayor que N.

En resumen tenemos:

$$E \longrightarrow E_N \longrightarrow \overline{E_N}.$$

$$\begin{aligned}\{P \mid \mathrm{nv}(P) > N\} &\longrightarrow \{(0:1:0)\}\\ \{P \mid \mathrm{nv}(P) = N\} &\longrightarrow \{P \mid P \text{ es no singular y } P \neq (0:1:0)\}\\ \{P \mid \mathrm{nv}(P) < N\} &\longrightarrow \{(0,0)\}.\end{aligned}$$

Luego, con el cambio y la reducción separamos los puntos.

Veamos ahora cómo es el grupo de puntos no singulares de $\overline{E_N}$. Al cortar $\overline{E_N}:\ Y^2Z = X^3$ con la recta $X = 0$, se obtiene el elemento neutro $(0:1:0)$ y el punto singular $(0:0:1)$. Por otra parte, en la carta afín $X \neq 0$, la ecuación queda $Y^2Z = 1$, de donde cada valor de Y determina un único valor de Z.

Luego, los puntos no singulares son $(0:1:0)$ y los puntos de la forma $(1:y:1/y^2)$ con $0 \neq y \in \mathbb{F}_p$. Así, el conjunto de puntos no singulares de

E_N es un grupo abeliano con p elementos, y como p es primo, será un grupo cíclico de orden p.

Definimos $E(\mathbb{Q}_p)^{(N)} = \{P \in E(\mathbb{Q}_p) \mid \mathrm{nv}(P) \geq N\}$. Entonces $E(\mathbb{Q}_p)^{(N)}$ es un grupo, porque es la imagen inversa del grupo de puntos no singulares de $\overline{E_N}$. Se tiene, obviamente,

$$E(\mathbb{Q}_p) \supset E(\mathbb{Q}_p)^{(0)} \supset E(\mathbb{Q}_p)^{(1)} \supset \cdots \supset E(\mathbb{Q}_p)^{(N)} \supset \cdots,$$

denominada filtración p-ádica.

Esto es coherente con el hecho de que un punto que no se reduce a $(0 : 1 : 0)$ tiene nivel 0 y con que $(0 : 1 : 0)$ tiene nivel infinito. Además:

(i) $\bigcap_{N\geq 0} E(\mathbb{Q}_p)^{(N)} = \{(0 : 1 : 0)\}$, porque claramente el nivel de un punto distinto de $(0 : 1 : 0)$ es finito.

(ii) $E(\mathbb{Q}_p)^{(0)}/E(\mathbb{Q}_p)^{(1)} \simeq \overline{E}(\mathbb{F}_p)^{(0)}$, porque $E(\mathbb{Q}_p)^{(0)} \longrightarrow \overline{E}(\mathbb{F}_p)^{(0)}$ es sobreyectiva y el núcleo es, precisamente, $E(\mathbb{Q}_p)^{(1)}$ (puntos de nivel ≥ 1, i.e. puntos que se reducen a $(0 : 1 : 0) \in \overline{E}$).

(iii) Análogamente, $E(\mathbb{Q}_p)^{(N)}/E(\mathbb{Q}_p)^{(N+1)}$ es isomorfo al grupo de puntos no singulares en $\overline{E_N}$, que es cíclico de orden p, como hemos visto.

Corolario.– Sea $P = (x, y) \in E(\mathbb{Q}_p)$ un punto de orden finito y primo con p. Entonces

$$x,\ y \in \mathbb{Z}_{(p)}.$$

Demostración.– Si $x, y \notin \mathbb{Z}_{(p)}$, el punto $P = (x, y)$ tendría nivel $n \geq 1$. Entonces,

$$P = (x, y) \in E(\mathbb{Q}_p)^{(n)}\ ,\quad (x, y) \notin E(\mathbb{Q}_p)^{(n+1)},$$

luego en el morfismo

$$E(\mathbb{Q}_p)^{(N)}/E(\mathbb{Q}_p)^{(N+1)} \longrightarrow \{P \in \overline{E_N} \mid \text{P es no singular}\},$$

el punto $P = (x, y)$ va en un elemento distinto del neutro, que tiene que tener orden p, porque la imagen de esta aplicación era un grupo cíclico de orden p. Esto está en contradicción con que el orden de P era primo con p.

Este morfismo en concreto es

$$\begin{array}{rcll} E & \longrightarrow & E_N \quad \text{(afín)} & \longrightarrow E_N \quad \text{(proyectivo)} \\ P(x,y) & \longmapsto & (xp^{2N}, yp^{3N}) & \longmapsto (xp^{2N} : yp^{3N} : 1) \end{array}$$

$$\begin{array}{rcll} E_N \text{ (proyectivo)} & \longrightarrow & \overline{E_N} & \xrightarrow{\sim} \quad \mathbb{F}_p \\ (xp^{2N} : yp^{3N} : 1) & \longmapsto & (\overline{xp^{2N}} : \overline{yp^{3N}} : 1) & \xmapsto{\sim} \quad \dfrac{\overline{xp^{2N}}}{\overline{yp^{3N}}} = p^{-N}\dfrac{\overline{x}}{\overline{y}} \mod p. \end{array}$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Para todo $P = (x,y) \in E(\mathbb{Q}_p)^{(1)}$, definimos la función u de la siguiente manera:

$$\begin{array}{rcl} u(P) & = & x/y\ , \\ u(0:1:0) & = & 0. \end{array}$$

Así se tiene que

$$|u(P)|_p = \frac{|x|_p}{|y|_p} = \frac{p^{2n}}{p^{3n}} = p^{-n},$$

siendo n el nivel del punto P.

Lema.– Sean $P_1, P_2 \in E(\mathbb{Q}_p)^{(1)}$. Entonces

$$|u(P_1+P_2) - u(P_1) - u(P_2)|_p \leq \max\{|u(P_1)|_p^5\ ,\ \ |u(P_2)|_p^5\}.$$

Corolario.– $|u(sP)|_p = |s|_p \cdot |u(P)|_p\ ,\ \ \forall P \in E(\mathbb{Q}_p)^{(1)},\ \forall s \in \mathbb{Z}.$

Demostración.– Por inducción tenemos que

$$|u(sP) - s\cdot u(P)|_p \leq |u(P)|_p^5.$$

Supongamos que $|u(sP)|_p \neq |s\cdot u(P)|_p$, y se tendrá

$$|u(sP) - s\cdot u(P)|_p = \max\{|u(sP)|_p,\ |s\cdot u(P)|_p\}.$$

Pero si $P \in E(\mathbb{Q}_p)^{(m)} \setminus E(\mathbb{Q}_p)^{(m+1)}$, entonces $sP \in E(\mathbb{Q}_p)^{(m)}$, luego, si suponemos que $p \nmid s$, resulta

$$\begin{array}{rcl} |u(sP)|_p & \leq & p^{-m}, \\ |s\cdot u(P)|_p & = & |s|_p \cdot |u(P)|_p = |u(P)|_p = p^{-m}. \end{array}$$

Así, $|u(sP)-s\cdot u(P)|_p = p^{-m} \leq p^{-5m}$, que es una contradicción, por tanto

$$|u(sP)|_p = |s\cdot u(P)|_p = |s|_p \cdot |u(P)|_p.$$

Sólo quedaría ver el caso $p \mid s$, que es análogo. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– $E(\mathbb{Q}_p)^{(1)}$ es libre de torsión.

Demostración.– Sea $P \in E(\mathbb{Q}_p)^{(1)}$ tal que $P \neq \mathcal{O}$ y $mP = \mathcal{O}$. Entonces,

$$0 = |u(mP)|_p = |m|_p \cdot |u(P)|_p \neq 0,$$

es una contradicción que indica que $E(\mathbb{Q}_p)^{(1)}$ es libre de torsión. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Corolario.– Si $p \neq 2$ y $|4A^3 + 27B^2|_p = 1$, entonces el subgrupo de torsión de $E(\mathbb{Q}_p)$ es isomorfo a un subgrupo de $\overline{E}(\mathbb{F}_p)$.

Demostración.– Como en este caso no hay puntos singulares en la curva reducida, será $E(\mathbb{Q}_p) = E(\mathbb{Q}_p)^{(0)}$. Así

$$\overline{E}(\mathbb{F}_p) \simeq E(\mathbb{Q}_p)^{(0)}/E(\mathbb{Q}_p)^{(1)} = E(\mathbb{Q}_p)/E(\mathbb{Q}_p)^{(1)}.$$

Y como $E(\mathbb{Q}_p)^{(1)}$ es libre de torsión, la torsión de $E(\mathbb{Q}_p)$ queda invariante al hacer el cociente, luego se puede considerar sumergida en $\overline{E}(\mathbb{F}_p)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Sea

$$E:\ Y^2 = X^3 + AX + B$$

una curva elíptica sobre $\mathbb{Q}$. Sin pérdida de generalidad, podemos considerar $A, B \in \mathbb{Z}$ y, al ser E no singular, será $\Delta = 4A^3 + 27B^2 \neq 0$. Entonces, si $p \neq 2$ y p no divide a Δ, se dice que p es un buen primo y que $\overline{E}(\mathbb{F}_p)$ es una buena reducción, y en este caso el corolario anterior nos dice que, salvo isomorfismo, $\mathrm{Tor}(E(\mathbb{Q})) \subset \overline{E}(\mathbb{F}_p)$. Esto es parte esencial del proceso de acotación de la torsión racional, previo al cálculo explícito de ésta (ver II.A.).

Teorema de Nagell-Lutz [27, 21].– El grupo de puntos racionales de orden finito de E, es finito. Además, si $P = (x, y) \neq \mathcal{O}$ es un punto racional de orden finito, entonces $x, y \in \mathbb{Z}$ y se tiene

$$y = 0, \quad \text{o bien} \quad y^2 \mid (4A^3 + 27B^2).$$

Demostración.– Sean $E(\mathbb{Q})$ y $E(\mathbb{Q}_p)$, donde p recorre los números primos. Sea $P = (x, y) \neq \mathcal{O}$ un punto de torsión. Como $E(\mathbb{Q}) \subset E(\mathbb{Q}_p)$, por un resultado anterior tenemos

$$x \in \mathbb{Z}_{(p)} \ , \quad y \in \mathbb{Z}_{(p)} \ , \quad \forall p \quad \text{primo} \ .$$

Por tanto, no hay ningún primo p que divida al denominador de x ni al de y, es decir

$$x \in \mathbb{Z} \ , \quad y \in \mathbb{Z}.$$

Sea ahora $p \neq 2$ un primo tal que $p \nmid (4A^3 + 27B^2)$. Por el corolario anterior, el subgrupo de torsión de $E(\mathbb{Q}_p)$ es isomorfo al subgrupo de torsión del grupo de puntos sobre $\mathbb{F}_p$. Por tanto, el grupo de torsión es finito.

Si $2(x, y) = \mathcal{O}$, entonces $y = 0$. En otro caso, $2(x, y) = (x_2, y_2)$ es también un punto de torsión, por tanto

$$x_2, \ y_2 \in \mathbb{Z}.$$

Usando la fórmula de duplicación, tenemos:

$$x_2 + 2x = \left(\frac{3x^2 + A}{2y}\right)^2 = \frac{(3x^2 + A)^2}{4(x^3 + Ax + B)},$$

y así $y^2 = x^3 + Ax + B$ divide a $(3x^2 + A)^2$.

Pero se tiene:

$$(3X^2 + 4A)(3X^2 + A)^2 \equiv 4A^3 + 27B^2 \pmod{X^3 + AX + B},$$

en $\mathbb{Z}[X, A, B]$. Por tanto,

$$y^2 \mid (4A^3 + 27B^2).$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

I.F. Puntos de orden finito (III): Polinomios de división

Vamos a definir en esta sección los polinomios de división, y veremos algunas propiedades que serán útiles para el cálculo de la torsión racional de una curva elíptica.

Observación.– De la misma manera que hicimos en la sección I.B. para la forma breve de Weierstrass, podemos dar las fórmulas explícitas para la ley

interna definida en una curva elíptica dada por su forma larga de Weierstrass, y observar que las coordenadas de la suma de dos puntos de la curva son funciones racionales de las coordenadas de dichos puntos. Por tanto, por aplicación sucesiva de estas fórmulas, si $P = (x, y)$ es un punto racional de una curva elíptica E, y m es un entero, tendremos que las coordenadas de mP son funciones racionales de x e y.

Concretamente, tenemos el siguiente resultado:

Proposición.– Sea E una curva elíptica y sea m un entero positivo. Existen polinomios ψ_m, θ_m y $\omega_m \in \mathbb{Q}[x, y]$ tales que, si $P = (x, y) \in E(\mathbb{Q})$ y $mP \neq \mathcal{O}$, entonces

$$mP = \left(\frac{\theta_m(x,y)}{\psi_m(x,y)^2}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3} \right).$$

El polinomio $\psi_m(x, y)$ se llama m-ésimo polinomio de división de la curva E.

Demostración.– Vamos a construir la sucesión ψ_m por recurrencia, a partir de los coeficientes de la curva, y veremos que las sucesiones θ_m y ω_m se pueden expresar en función de los ψ_m.

Tomamos una ecuación en forma normal de Weierstrass de E

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

con coeficientes en $\mathbb{Q}$, y consideremos las constantes definidas a partir de los coeficientes de la curva:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= a_1a_3 + 2a_4, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6.
\end{aligned}$$

El m-ésimo polinomio de división se define por la siguiente ley de recurrencia,

$$\begin{aligned}
\psi_0 &= 0, \\
\psi_1 &= 1, \\
\psi_2 &= 2y + a_1x + a_3, \\
\psi_3 &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8, \\
\psi_4 &= (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 \\
&\quad + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2)\psi_2, \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2, \\
\psi_{2m} &= \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{\psi_2}, \quad m > 2.
\end{aligned}$$

La primera observación que podemos hacer es que ψ_{2m}, con $m \geq 1$, es un polinomio divisible por ψ_2. Veámoslo, probando por inducción que el numerador de ψ_{2m} es divisible por ψ_2^2.

Los casos $m = 1$ y $m = 2$ están claros. Para $m = 3$, tenemos que el numerador de ψ_6 es el polinomio $(\psi_5\psi_2^2 - \psi_1\psi_4^2)\psi_3$, que claramente es divisible por ψ_2^2, teniendo en cuenta la definición de ψ_4.

Ahora, para $m > 3$, supongamos que el numerador de ψ_{2n} es divisible por ψ_2^2 para todo $n < m$, y probémoslo para m. El numerador de ψ_{2m} es $(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m$. Distinguiremos dos casos. Si m es par,

$$n = \frac{m}{2} < m,$$

y por ser $m > 3$, también $n + 1 < m$, luego, por hipótesis de inducción, $\psi_{m+2} = \psi_{2(n+1)}$ será mútiplo de ψ_2, al igual que $\psi_{m-2} = \psi_{2(n-1)}$ y $\psi_m = \psi_{2n}$. Por tanto, tenemos que el numerador de ψ_{2m} será divisible por ψ_2^2. Si m es impar,

$$n_1 = \frac{m-1}{2} < m \quad \text{y} \quad n_2 = \frac{m+1}{2} < m,$$

luego, por hipótesis de inducción, $\psi_{m-1} = \psi_{2n_1}$ y $\psi_{m+1} = \psi_{2n_2}$ serán mútiplos de ψ_2. Así, el numerador de ψ_{2m} será divisible por ψ_2^2 también en este caso.

Observamos también que, como los polinomios de división serán evaluados en puntos de la curva, el cálculo de ψ_m se puede hacer módulo la ecuación de la curva. En particular, podemos suponer que el grado de ψ_m en y es siempre menor o igual que 1.

Construimos ahora los polinomios θ_m de la siguiente forma,

$$\theta_m = x\psi_m^2 - \psi_{m-1}\psi_{m+1}, \quad m \geq 1,$$

y, los polinomios ω_m los definimos mediante la relación

$$2\psi_m\omega_m = \psi_{2m} - (a_1\theta_m + a_3\psi_m^2)\psi_m^2, \quad m \geq 1.$$

Ahora, con las expresiones dadas para ψ_m, θ_m y ω_m, la demostración de la proposición es simplemente una comprobación, usando las fórmulas explícitas para la ley interna definida sobre la curva elíptica E. $\mathcal{Q.E.D.}$

Definición.– Para un entero m no negativo, el conjunto de puntos de m-torsión, denotado $E[m]$, se define por

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

Observación.– Se deduce claramente de la definición que $E[m]$ es un subgrupo de $E(\mathbb{Q})$.

Por definición, $\mathcal{O} \in E[m]$ para todo m, y como se dice en el siguiente teorema, el m-ésimo polinomio de división ψ_m caracteriza los demás puntos de m-torsión de E.

Teorema.– Con la notación anterior, sea $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, y sea $m \geq 1$ un entero. Entonces, $P \in E[m]$ si y sólo si $\psi_m(P) = 0$.

Demostración.– Para ver que $mP = \mathcal{O}$, es decir, que mP es el punto del infinito de la curva, según la expresión de mP dada en la proposición anterior, basta ver que los denominadores de las coordenadas afines de mP se anulan, y esto ocurre si y sólo si se anula el polinomio de división ψ_m. $\mathcal{Q.E.D.}$

Observación.– Hemos caracterizado así los puntos de m-torsión de una curva elíptica, mediante polinomios en $\mathbb{Q}[x, y]$, pero veamos que en realidad podemos hacerlo con polinomios que sólo dependan de la variable x.

Definición.– A partir de los polinomios ψ_m, definimos

$$\Psi_m = \begin{cases} \psi_m, & m \text{ impar}, \\ \dfrac{\psi_m}{\psi_2}, & m \text{ par}. \end{cases}$$

Proposición.– Para todo entero $m \geq 1$, se tiene que $\Psi_m \in \mathbb{Q}[x]$.

Demostración.– Observemos que, en la definición por recurrencia de los ψ_m, la variable y sólo aparece a través del polinomio ψ_2. Pero además, en los Ψ_m, cuando este polinomio ψ_2 aparece, lo hace al cuadrado. Como tenemos

$$\psi_2^2 = (2y + a_1x + a_3)^2 = 4(y^2 + a_1xy + a_3y) + a_1^2x^2 + 2a_1a_3x + a_3^2$$

$$= 4(x^3 + a_2x^2 + a_4x + a_6) + a_1^2x^2 + 2a_1a_3x + a_3^2,$$

resulta que Ψ_m es un polinomio que depende sólo de x. $\mathcal{Q.E.D.}$

Observación.– Se puede ver [3] que si m es impar, el grado del polinomio Ψ_m es menor o igual que $(m^2-1)/2$, y si m es par, menor o igual que $(m^2-4)/2$. Aunque, al trabajar en $\mathbb{Q}$, (en otros cuerpos base esto puede no ser cierto) es sencillo probar que estas desigualdades son en realidad igualdades.

Corolario.– Sea $P = (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, tal que $2P \neq \mathcal{O}$, y sea $m > 2$ un entero. Entonces, $P \in E[m]$ si y sólo si $\Psi_m(x) = 0$.

Observación.– Los puntos de 2-torsión no están incluidos en este corolario, ya que éstos satisfacen que $\psi_2(P) = 0$ y, cuando m es par, ψ_m se ha dividido por ψ_2 para obtener Ψ_m.

Observación.– Sea $F(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$. Teniendo en cuenta que $F(x) = \psi_2^2$, se puede comprobar fácilmente que los polinomios Ψ_m verifican:

$$\begin{aligned}
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 1,\\
\Psi_3 &= \psi_3,\\
\Psi_4 &= \psi_4/\psi_2,\\
\Psi_{2m+1} &= \begin{cases} \Psi_{m+2}\Psi_m^3 - F^2\Psi_{m-1}\Psi_{m+1}^3, & m \text{ impar}, \quad m \geq 3,\\ F^2\Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, & m \text{ par}, \quad m \geq 2, \end{cases}\\
\Psi_{2m} &= (\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2)\Psi_m, \quad m > 2.
\end{aligned}$$

Observación.– Si expresamos la ecuación de la curva mediante la forma breve de Weierstrass,

$$E: \; Y^2 = X^3 + AX + B, \qquad \text{con } A, B \in \mathbb{Z},$$

tendremos $a_1 = a_2 = a_3 = 0$, $a_4 = A$, $a_6 = B$, $b_2 = 0$, $b_4 = 2A$, $b_6 = 4B$, y $b_8 = -A^2$. Así, las fórmulas de recursión para ψ_m resultan

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2,\\
\psi_{2m} &= \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m}{2y}, \quad m > 2.
\end{aligned}$$

Además, para $m \geq 2$, si $P = (x, y) \in E \setminus E[m]$, según una proposición anterior y las fórmulas que teníamos para θ_m y ω_m, podemos decir que

$$mP = \left(x - \frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3} \right),$$

donde los ψ_m son polinomios en x e y.

También podemos escribir esta fórmula en función de los polinomios $\Psi_m(x)$, teniendo en cuenta que

$$\Psi_m = \begin{cases} \psi_m, & m \text{ impar}, \\ \dfrac{\psi_m}{2y}, & m \text{ par}. \end{cases}$$

Las fórmulas de recursión dadas para Ψ_m no cambian, si bien, ahora resulta $F(x) = 4(x^3 + Ax + B) = 4y^2$ módulo la curva.

Observación.– También llamaremos m-ésimo polinomio de división al polinomio en una sola variable $\Psi_m(x)$.

I.G. Forma normal de Tate

Sea

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

una curva elíptica en forma normal de Weierstrass, con coeficientes en $\mathbb{Q}$.

Supongamos que E pasa por un punto afín racional. Este punto lo podemos trasladar mediante un cambio sencillo, que preserva la forma normal de Weierstrass, al punto $(0,0)$. Así, se tendrá $a_6 = 0$, y queda:

$$E_0: \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X.$$

Para hallar la pendiente de la recta tangente a la curva en $(0,0)$, derivamos la expresión anterior:

$$(2Y + a_1X + a_3)Y' = 3X^2 + 2a_2X + a_4 - a_1Y.$$

Entonces, la pendiente de la recta tangente en $(0,0)$ es a_4/a_3.

Si $a_3 = a_4 = 0$, la componente homogénea de menor grado de la ecuación de E_0 tiene grado 2, es decir, $(0,0)$ es un punto singular.

Si $a_3 = 0$ y $a_4 \neq 0$, la pendiente de la recta tangente en $(0,0)$ es infinito, es decir, la tangente es vertical. En este caso, $(0,0)$ sería un punto no singular de orden 2.

Supongamos que $(0,0)$ es un punto no singular y que no tiene orden 2, (o sea, $a_3 \neq 0$). Hacemos el siguiente cambio de variables:

$$\begin{aligned} X &\longmapsto X \\ Y &\longmapsto Y + \frac{a_4}{a_3}X. \end{aligned}$$

Sustituyendo en la ecuación de E_0 y renombrando los coeficientes resulta:

$$E_1 : \ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2.$$

Podemos comprobar ahora que la recta tangente a la curva en $(0,0)$ tiene pendiente nula. Viendo la ecuación de E_1, podemos decir que el punto $(0,0)$ tiene orden 3 si y sólo si $a_2 = 0$ y $a_3 \neq 0$.

Supongamos que $(0,0)$ no es un punto de orden 2 ni de orden 3, es decir, supongamos

$$a_2 \neq 0, \quad a_3 \neq 0.$$

Si hacemos ahora el siguiente cambio de variables:

$$\begin{array}{ccc} X & \longmapsto & u^2X \\ Y & \longmapsto & u^3Y, \end{array}$$

dividiendo por u^6 resulta:

$$E_2 : \ Y^2 + \frac{a_1}{u}XY + \frac{a_3}{u^3}Y = X^3 + \frac{a_2}{u^2}X^2.$$

Tomando

$$u = \frac{a_3}{a_2} \ \in \ \mathbb{Q} \setminus \{0\},$$

queda la ecuación

$$E_2 : \ Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

siendo

$$-b = \frac{a_3}{u^3} = \frac{a_2}{u^2}, \quad 1 - c = \frac{a_1}{u}.$$

Definición.– La forma normal de Tate de una curva elíptica E con un punto P racional de orden mayor que 3 es una ecuación del tipo:

$$E = E(b,c) : \ Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

con $P = (0,0)$.

Observación.– El discriminante de $E(b,c)$ es:

$$\begin{array}{rl} \Delta = \Delta(b,c) = & (1-c)^4b^3 - (1-c)^3b^3 - 8(1-c)^2b^4 \\ & +36(1-c)b^4 - 27b^4 + 16b^5. \end{array}$$

Proposición.– Dada la curva

$$E(b,c):\ Y^2+(1-c)XY-bY=X^3-bX^2,$$

que pasa por $P=(0,0)$, se tiene:

$$\begin{array}{ll} & -P=(0,b),\\ 2P=(b,bc), & -2P=(b,0),\\ 3P=(c,b-c), & -3P=(c,c^2),\\ 4P=(d(d-1),d^2(c-d+1)), & -4P=(d(d-1),d(d-1)^2),\\ 5P=(de(e-1),de^2(d-e)), & -5P=(de(e-1),d^2e(e-1)^2),\\ 6P=\left(\dfrac{e(d-1)(d-e)}{(e-1)^2},\dfrac{e^2(d-1)^2(de-2d+1)}{(e-1)^3}\right), & \\ -6P=\left(\dfrac{e(d-1)(d-e)}{(e-1)^2},\dfrac{e^2(d-1)(d-e)^2}{(e-1)^3}\right), & \end{array}$$

siendo

$$d=\frac{b}{c}\quad \text{y}\quad e=\frac{c}{d-1}.$$

Demostración.– Basta aplicar la ley interna definida en el conjunto de puntos de una curva elíptica.

Por ejemplo, para hallar $-P$, tomamos la recta vertical $X=0$ que pasa por P, y al cortarla con la curva se tiene:

$$Y^2-bY=0,$$

de donde obtenemos que la segunda coordenada de $-P$ es b. Así tenemos:

$$-P=(0,b).$$

Para calcular $2P$, tomamos la recta tangente a la curva en $P=(0,0)$ que era $Y=0$, al cortarla con la curva se obtiene:

$$X^3-bX^2=0,$$

de donde, además del punto doble $P=(0,0)$, tenemos el punto

$$P*P=(b,0).$$

Al tomar la recta vertical $X=b$ que pasa por $P*P$, y cortarla con la curva, se obtiene:

$$Y^2+(1-c)\cdot bY-bY=b^3-bb^2\implies Y^2-cbY=0.$$

Así probamos que $2P = (b, bc)$. Para hallar $-2P$, cortamos la recta vertical $X = b$ (que pasa por $2P$) con la curva, quedando de nuevo

$$Y^2 - cbY = 0.$$

Ahora tomamos el otro punto de corte que es $-2P = (b, 0)$.

Si queremos calcular $3P$, consideramos P y $2P$. La recta que une estos dos puntos es $Y = cX$, y al cortarla con la curva obtenemos, además de P y $2P$, el punto $P * 2P = (c, c^2)$. Al tomar ahora la recta vertical $X = c$ que pasa por $P * 2P$, y cortarla con la curva, se obtiene la ecuación:

$$Y^2 + (1-c)cY - bY = c^3 - bc^2,$$

de donde obtenemos $Y = c^2$, (que correspondía a $P * 2P$), e $Y = b - c$, que será la segunda coordenada de $3P$. Como, por construcción, $P * 2P$ es el punto $-3P$, hemos probado que

$$3P = (c, b-c), \quad \text{y} \quad -3P = (c, c^2).$$

Sumamos ahora P y $3P$ para hallar $4P$. La recta que une estos dos puntos es $Y = (b-c)/cX$, y al cortarla con la curva obtenemos la ecuación

$$\left(\frac{b-c}{c}\right)^2 X^2 + (1-c)\left(\frac{b-c}{c}\right) X^2 - b\left(\frac{b-c}{c}\right) X - X^3 + bX^2 = 0,$$

de donde, además de las primeras coordenadas de P y $3P$, tenemos

$$X = \frac{b(b-c)}{c^2}.$$

Sustituyendo en la curva, nos encontramos ahora con la ecuación

$$Y^2 - \frac{b(bc-b+c)}{c^2} Y - \frac{b^3(b-c-c^2)(b-c)^2}{c^6} = 0,$$

y de esto, obtenemos dos opciones para Y, la segunda coordenada de $-4P = P * 3P$, que era $Y = b(b-c)^2/c^3$ (obtenida, si queremos, sustituyendo en la recta que une P y $3P$) y la segunda coordenada de $4P$, que haciendo los calculos es $Y = b^2(c^2 - b + c)/c^3$. Resumiendo, tenemos

$$4P = \left(\frac{b(b-c)}{c^2}, \frac{b^2(c^2-b+c)}{c^3}\right) \quad \text{y} \quad -4P = \left(\frac{b(b-c)}{c^2}, \frac{b(b-c)^2}{c^3}\right).$$

Para simplificar notación, llamamos $d = b/c$, y así podemos escribir

$$4P = (d(d-1), d^2(c-d+1)) \quad \text{y} \quad -4P = (d(d-1), d(d-1)^2).$$

Para calcular $5P$, sumamos los puntos P y $4P$, repitiendo de nuevo el proceso. Hallamos la recta que une estos puntos,

$$Y = \frac{d(c-d+1)}{d-1}X,$$

la cortarmos con la curva, obteniendo la ecuación

$$\left(\frac{d(c-d+1)}{d-1}\right)^2 X^2 + (1-c)\left(\frac{d(c-d+1)}{d-1}\right)X^2 - b\left(\frac{d(c-d+1)}{d-1}\right)X$$

$$= X^3 - bX^2,$$

y sustituyendo la tercera solución de ésta,

$$X = \frac{bc(c^2+c-b)}{(b-c)^2},$$

en la ecuación de la curva, llamando

$$e = \frac{c}{d-1},$$

resulta ahora

$$Y^2 - de(e^2d - e^2 - ed + d)Y + d^3e^3(e-1)^2(d-e) = 0,$$

de donde conseguimos $Y = de^2(d-e)$, e $Y = d^2e(e-1)^2$. Por tanto,

$$5P = (de(e-1), de^2(d-e)), \quad \text{y} \quad -5P = (de(e-1), d^2e(e-1)^2).$$

Por último, vamos a calcular $6P = P + 5P$. Cortamos la recta

$$Y = \frac{e(d-e)}{e-1}X$$

con la curva, para obtener la ecuación

$$\left(\frac{e(d-e)}{e-1}\right)^2 X^2 + (1-c)\left(\frac{e(d-e)}{e-1}\right)X^2 - b\left(\frac{e(d-e)}{e-1}\right)X = X^3 - bX^2,$$

de donde tenemos la primera coordenada de $6P$,

$$X = \frac{e(d-1)(d-e)}{(e-1)^2}.$$

Sustituyendo en la ecuación de la curva obtenemos

$$Y^2 - \frac{e^2(d-1)(d^2-3d+1+e)}{(e-1)^2}Y + \frac{e^4(d-1)^3(ed-2d+1)(d-e)^2}{(e-1)^6} = 0,$$

cuyas soluciones son

$$Y = \frac{e^2(d-1)^2(ed-2d+ed+1)}{(e-1)^3}, \quad Y = \frac{e^2(d-1)(d-e)^2}{(e-1)^3},$$

resultando así,

$$6P = \left(\frac{e(d-1)(d-e)}{(e-1)^2}, \frac{e^2(d-1)^2(de-2d+1)}{(e-1)^3}\right) \quad \text{y}$$

$$-6P = \left(\frac{e(d-1)(d-e)}{(e-1)^2}, \frac{e^2(d-1)(d-e)^2}{(e-1)^3}\right).$$

$\mathcal{Q.E.D.}$

Observación.– Aunque la forma normal de Tate de una curva elíptica viene dada por una ecuación que depende de dos parámetros, la proposición que acabamos de demostrar, nos va a permitir afirmar que las curvas elípticas en forma normal de Tate que tienen un punto de orden dado n, forman una familia uniparamétrica de curvas [18]. Para ver esto, probaremos el siguiente teorema.

Teorema.– Toda curva elíptica que tenga un punto de orden n, con $n \in \{4, 5, 6, 7, 8, 9, 10, 12\}$, se puede escribir en forma normal de Tate

$$Y^2 + (1-c)XY - bY = X^3 - bX^2,$$

con las siguientes relaciones entre sus parámetros:

(a) Si $n = 4$, $b = \alpha$, $c = 0$.

(b) Si $n = 5$, $b = \alpha$, $c = \alpha$.

(c) Si $n = 6$, $b = \alpha(1+\alpha)$, $c = \alpha$.

(d) Si $n = 7$, $b = \alpha^2(\alpha-1)$, $c = \alpha(\alpha-1)$.

(e) Si $n = 8$, $b = (2\alpha-1)(\alpha-1)$, $c = b/\alpha$.

(f) Si $n = 9$, $c = \alpha^2(\alpha-1)$, $b = c(\alpha(\alpha-1)+1)$.

(g) Si $n = 10$, $c = \alpha(2\alpha-1)(\alpha-1)/(\alpha-(\alpha-1)^2)$, $b = c\alpha^2/(\alpha-(\alpha-1)^2)$.

(h) Si $n = 12$, $c = \alpha(1-2\alpha)(3\alpha^2-3\alpha+1)/(\alpha-1)^3$,
$b = c(2\alpha-2\alpha^2-1)/(\alpha-1)$.

Demostración.– Esencialmente, basta seguir el cálculo anterior caso a caso.

(a) $4P = \mathcal{O}$ si y sólo si $2P = -2P$.

Usando las fórmulas de la proposición anterior, resulta:

$$(b, bc) = (b, 0),$$

es decir, podemos tomar $c = 0$ y $b = \alpha$, siendo α el único parámetro que aparcerá en la ecuación de la curva.

Así, para que $P = (0,0)$ sea un punto de orden 4 en una curva elíptica en forma normal de Tate, su ecuación ha de ser:

$$Y^2 + XY - \alpha Y = X^3 - \alpha X^2.$$

Nótese que el discriminante de esta curva es $\Delta = \alpha^4(1+16\alpha) \neq 0$.

(b) $5P = \mathcal{O}$ si y sólo si $3P = -2P$.

Con las fórmulas de la proposición anterior, resulta:

$$(c, b-c) = (b, 0),$$

es decir, $b = c = \alpha$. Así, la forma normal de Tate de una curva elíptica en la que $P = (0,0)$ tiene orden 5 es

$$Y^2 + (1-\alpha)XY - \alpha Y = X^3 - \alpha X^2.$$

Su discriminante es $\Delta = \alpha^5(\alpha^2 - 11\alpha - 1) \neq 0$.

(c) $6P = \mathcal{O}$ si y sólo si $3P = -3P$.

De forma análoga a los apartados anteriores, la relación $b = c + c^2$, obtenida a partir de

$$(c, b-c) = (c, c^2),$$

da lugar a la relación $c = \alpha$, $b = \alpha(1+\alpha)$. Luego, la ecuación en forma normal de Tate, de una curva elíptica en la que $P = (0,0)$ tiene orden 6, resulta

$$Y^2 + (1-\alpha)XY - \alpha(1+\alpha)Y = X^3 - \alpha(1+\alpha)X^2.$$

En ese caso el discriminante es $\Delta = \alpha^6(\alpha+1)^3(9\alpha+1) \neq 0$.

(d) $7P = \mathcal{O}$ equivale a decir $4P = -3P$.

Por tanto, será

$$(d(d-1), d^2(c-d+1)) = (c, c^2),$$

de donde se tiene

$$c = d(d-1),$$
$$c^2 = d^2(c-d+1).$$

Sustituyendo c de la primera igualdad en la segunda, queda

$$d^2(d^2-2d+1) = d^2(c-d+1),$$

es decir,

$$c = d^2 - d = d(d-1).$$

Como $d = b/c$, se tiene

$$b = d^3 - d^2 = d^2(d-1).$$

Luego, tomando $d = \alpha$, si tenemos una curva elíptica en forma normal de Tate que tiene al punto $P = (0,0)$ de orden 7, su ecuación es

$$Y^2 + (1 - \alpha(\alpha-1))XY - \alpha^2(\alpha-1)Y = X^3 - \alpha^2(\alpha-1)X^2,$$

y su discriminante es $\Delta = \alpha^7(\alpha-1)^7(\alpha^3 - 8\alpha^2 + 5\alpha + 1) \neq 0$.

(e) $8P = \mathcal{O}$ equivale a decir $4P = -4P$.

Por tanto,

$$d^2(c-d+1) = d(d-1)^2.$$

De forma análoga a lo anterior, se tiene la siguiente relación entre los parámetros b y c:

$$c = \frac{(d-1)(2d-1)}{d}, \quad b = cd = (d-1)(2d-1).$$

Así, si de nuevo es $d = \alpha$, una curva elíptica en forma normal de Tate, que tiene al punto $P = (0,0)$ de orden 8, tiene ecuación

$$y^2 + \left(1 - \frac{(2\alpha-1)(\alpha-1)}{\alpha}\right) XY - (2\alpha-1)(\alpha-1)Y$$
$$= X^3 - ((2\alpha-1)(\alpha-1))X^2.$$

(f) $9P = \mathcal{O}$ si y sólo si $5P = -4P$.

Igualando las primeras coordenadas de $5P$ y $-4P$, se tiene la relación

$$de(e-1) = d(d-1),$$

por tanto

$$e(e-1) = d-1.$$

De esto se deduce que

$$d = e(e-1)+1 = e^2 - e + 1,$$

y podemos comprobar que al sustituir d por $e^2 - e + 1$, en las segundas coordenadas de $5P$ y $-4P$, éstas coinciden. Obtenemos entonces

$$c = e(d-1) = e^2(e-1),$$

$$b = cd = e^2(e-1)(e^2 - e + 1).$$

Luego, tomando ahora $e = \alpha$, una curva elíptica en forma normal de Tate, con $P = (0,0)$ de orden 9, es de ecuación

$$\begin{aligned} Y^2 + (1 - \alpha^2(\alpha-1))XY - \alpha^2(\alpha-1)(\alpha(\alpha-1)+1)Y \\ = X^3 - \alpha^2(\alpha-1)(\alpha(\alpha-1)+1)X^2. \end{aligned}$$

(g) $10P = \mathcal{O}$ es equivalente a $5P = -5P$, es decir

$$de^2(d-e) = d^2e(e-1)^2.$$

Luego, en este caso, tenemos la relación

$$d = \frac{e^2}{e-(e-1)^2},$$

y por tanto,

$$c = e(d-1) = \frac{e(2e-1)(e-1)}{e-(e-1)^2},$$

$$b = cd = \frac{e^3(2e-1)(e-1)}{(e-(e-1)^2)^2}.$$

Así, con $e = \alpha$, la forma normal de Tate de una curva elíptica en la que $P = (0,0)$ tiene orden 10 es

$$\begin{aligned} Y^2 + \left(1 - \frac{\alpha(2\alpha-1)(\alpha-1)}{\alpha-(\alpha-1)^2}\right)XY - \frac{\alpha^3(2\alpha-1)(\alpha-1)}{(\alpha-(\alpha-1)^2)^2}Y \\ = X^3 - \frac{\alpha^3(2\alpha-1)(\alpha-1)}{(\alpha-(\alpha-1)^2)^2}X^2. \end{aligned}$$

(h) $12P = \mathcal{O}$ si y sólo si $6P = -6P$. Por tanto, planteamos la relación

$$\frac{e^2(d-1)^2(de-2d+1)}{(e-1)^3} = \frac{e^2(d-1)(d-e)^2}{(e-1)^3},$$

y, simplificando,

$$(d-1)(de-2d+1) = (d-e)^2.$$

Ahora, como no hay una forma cómoda de despejar d en función de e, ni viceversa, expresamos las dos en función del nuevo parámetro α. Podemos comprobar fácilmente que la relación anterior se cumple tomando

$$d = \frac{2\alpha - 2\alpha^2 - 1}{\alpha - 1}, \quad e = \frac{3\alpha^2 - 3\alpha + 1}{(\alpha-1)^2}.$$

Por tanto, la forma normal de Tate de una curva elíptica con $P = (0,0)$ de orden 12 tiene ecuación

$$\begin{aligned} Y^2 + \left(1 - \frac{\alpha(1-2\alpha)(3\alpha^2-3\alpha+1)}{(\alpha-1)^3}\right)XY \\ - \frac{\alpha(1-2\alpha)(3\alpha^2-3\alpha+1)(2\alpha-2\alpha^2-1)}{(\alpha-1)^4}Y \\ = X^3 - \frac{\alpha(1-2\alpha)(3\alpha^2-3\alpha+1)(2\alpha-2\alpha^2-1)}{(\alpha-1)^4}X^2. \end{aligned}$$

$\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

II. El cálculo efectivo de la torsión racional

En este capítulo, analizaremos algunos métodos efectivos para el cálculo de la torsión de una curva elíptica racional. Métodos que van desde el clásico de Nagell-Lutz, hasta un algoritmo original basado en la forma normal de Tate, pasando por los algoritmos más usados hoy: el algoritmo de la parametrización analítica (PARI/GP) y el de los polinomios de división (APECS).

II.A. Estudio computacional de la reducción

Antes de describir los métodos anteriormente referidos, vamos a hacer un estudio detallado de la acotación del orden del grupo de torsión de una curva elíptica racional, que usaremos en posteriores secciones de este capítulo.

Sea E una curva elíptica definida sobre $\mathbb{Q}$ dada por la ecuación

$$E:\ Y^2 = X^3 + AX + B.$$

Sabemos que, sin pérdida de generalidad, podemos considerar $A, B \in \mathbb{Z}$ y, al ser una curva no singular, será $\Delta = 4A^3 + 27B^2 \neq 0$.

Entonces, como vimos en I.E., si $p \neq 2$ y p no divide a Δ, la restricción del homomorfismo de reducción entre $E(\mathbb{Q})$ y $\overline{E}(\mathbb{F}_p)$ al subgrupo $\mathrm{Tor}(E(\mathbb{Q}))$ es inyectiva, luego, no habrá más puntos en $\mathrm{Tor}(E(\mathbb{Q}))$ que en el grupo $\overline{E}(\mathbb{F}_p)$ que es fácil de examinar. Es decir, salvo isomorfismo,

$$\mathrm{Tor}(E(\mathbb{Q})) \subset \overline{E}(\mathbb{F}_p).$$

Por tanto, el proceso de acotación del orden de la torsión racional de una curva elíptica consiste en:

1. Tomar un primo p.

2. Calcular el resto de la división de $2|\Delta|$ entre p.

3. Si este resto no es cero p es un buen primo. Contamos entonceslos puntos que tiene la curva reducida en $\mathbb{P}^2(\mathbb{F}_p)$.

Después se repite el proceso hasta encontrar varios buenos primos y, así, obtener una cota del orden del grupo de torsión; cota que, en realidad, es un múltiplo de dicho orden. Ya que, considerando $p_1, \ldots, p_r$ primos impares que no dividen a Δ, y llamando E_{p_i} a la reducida de E modulo p_i, con $i = 1, \ldots, r$, si tomamos

$$C = \text{mcd}(\sharp(E_{p_1}), \ldots, \sharp(E_{p_r})),$$

se tendrá que el orden del grupo $\text{Tor}(E(\mathbb{Q}))$ es un divisor de C menor o igual que 12.

Para detallar el coste computacional que requieren estos pasos, vamos a demostrar el siguiente lema.

Lema.– Dado $N \gg 0$, para todo $\varepsilon > 0$ podemos encontrar un primo p que no divida a N y tal que $p < \log^{1+\varepsilon} N$.

Demostración.– Por reducción al absurdo, fijemos $N \gg 0$. Sea $\varepsilon > 0$ tal que no podemos encontrar un primo que sea menor que $\log^{1+\varepsilon} N$ y que no divida a N. Es decir, tenemos $\varepsilon > 0$ tal que todos los primos menores que $\log^{1+\varepsilon} N$, dividen a N. Por tanto,

$$N \geq \prod_{p \text{ primo}, p \leq \log^{1+\varepsilon} N} p,$$

y, como este producto debe tener sólo un número finito de factores, podemos escribir

$$N \geq p_1 \cdots p_s,$$

donde los p_i son los primos menores que $\log^{1+\varepsilon} N$. Luego, tomando logaritmo tenemos

$$\log N \geq \sum_{i=1}^{s} \log p_i,$$

y, como para todo $i = 1, ..., s$ es $\log p_i \geq \log 2$, será

$$\log N \geq (\log 2)s,$$

donde s es el número de primos menores que $\log^{1+\varepsilon} N$. Si llamamos $\pi(x)$ a la función que da el número de primos menores que x, resulta

$$\log N \geq (\log 2)\, \pi(\log^{1+\varepsilon} N).$$

Usando ahora la siguiente acotación para $\pi(x)$ dada por Erdös [11],

$$\pi(x) \geq \log 2 \frac{x}{\log x},$$

podemos escribir

$$\log N \geq \frac{(\log^2 2)(\log^{1+\varepsilon} N)}{\log(\log^{1+\varepsilon} N)}.$$

Dividiendo en ambos miembros por $\log N$, se obtiene

$$1 \geq \frac{(\log^2 2)(\log^{\varepsilon} N)}{\log(\log^{1+\varepsilon} N)},$$

y operando tenemos que, existe $\varepsilon > 0$ tal que

$$\log^{\varepsilon} N \leq \frac{1+\varepsilon}{(\log^2 2)} \log(\log N),$$

que es una contradicción dado que podemos tomar $N \gg 0$. $\mathcal{Q.E.D.}$

Si se trata entonces de buscar un buen primo, cuando $|\Delta|$ es pequeño, basta tomar $p > \sqrt{|\Delta|}$, y si $|\Delta|$ es suficientemente grande, con este lema hemos probado que para todo $\varepsilon > 0$ podemos encontrar un primo p que no divida a $|\Delta|$ y tal que $p < \log^{1+\varepsilon} |\Delta|$. Es decir, asintóticamente, podemos encontrar un buen primo en un número de pasos no superior a $\log |\Delta| \log^2 |(\log |\Delta|)|$ (el segundo factor proviene de la complejidad de probar que p es primo usando un test tipo Miller–Rabin, que es de $\log^2 p$).

Ahora, tras medir el tiempo de búsqueda, veamos el coste de averiguar si un primo dado es bueno o no. Tomado un primo p, para saber si el resto de la división de $2|\Delta|$ entre p es cero o no, habrá que efectuar una división euclídea cuyo coste computacional, según [17], será $O(\log |\Delta| \log^2 |(\log |\Delta|)|)$.

Por último, el tercer paso de este proceso de acotación consistía en contar los puntos de la curva reducida. Para ello, podemos encontrar un algoritmo, basado en el proceso "Baby Step/Giant Step" de Shank, que hace este recuento en un tiempo de $O(p^{1/4})$; aunque también hay un algoritmo de Schoof, con muchas variantes, que lo hace en un tiempo de $O(\log^8 p)$ [3].

Entonces, si sumamos el coste computacional de cada uno de estos tres pasos obtenemos $O(\log|\Delta|\log^2|(\log|\Delta|)|)$. Como veremos, esta acotación no es necesaria para el cálculo posterior de la torsión. Sin embargo, en la práctica, dicha acotación requiere una cantidad de tiempo insignificante y ahorra bastantes cálculos, por tanto, sería una buena opción incluirla como parte de un algoritmo para el cálculo de la torsión racional de una curva elíptica.

Observación.– El número de buenos primos que vamos a utilizar en la acotación del orden de $\mathrm{Tor}(E(\mathbb{Q}))$ no crece con $|\Delta|$. Como podemos comprobar en los ejemplos recogidos en la sección A.2. del apéndice, con cinco buenos primos se obtienen acotaciones óptimas en casi todos los casos.

Ejemplo.– Dada la curva elíptica E de ecuación

$$Y^2 + XY + Y = X^3 - X^2 + 4X + 6,$$

podemos obtener su forma normal de Weierstrass y quedaría de la siguiente manera:

$$E:\ Y^2 = X^3 + 5589X + 342630.$$

Calculamos el discriminante de la curva y obtenemos

$$\Delta = 2^8 \cdot 3^{19} \cdot 13.$$

Consideramos los primos 5, 7, 11 y 17, que no dividen a Δ, y reducimos la curva modulo estos buenos primos. Después contaremos los puntos de la curva reducida en cada caso, y al final daremos una cota C del orden del grupo de torsión de nuestra curva, que será un múltiplo de dicho orden.

- Para $p = 5$, la ecuación reducida queda

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

  Probando en la ecuación para $x, y \in \mathbb{Z}/5\mathbb{Z}$, obtenemos los siguientes puntos que la verifican:

$$E_5 = \{\mathcal{O},\ (0,0),\ (1,0),\ (2,1),\ (2,4),\ (3,2),\ (3,3),\ (4,0)\}.$$

  Así, $\sharp(E_5) = 8$.

- Para $p = 7$, la curva reducida es

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

El conjunto de puntos con coordenadas en $\mathbb{Z}/7\mathbb{Z}$ que verifican esta ecuación es

$$E_7 = \{\mathcal{O},\ (0,1),\ (0,6),\ (2,1),\ (2,6),\ (3,3),$$
$$(4,0),\ (3,4),\ (5,1),\ (5,6),\ (6,2),\ (6,5)\}.$$

Ahora tenemos $\sharp(E_7) = 12$.

- La reducida módulo $p = 11$ es

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

Probamos en la ecuación para $x, y \in \mathbb{Z}/11\mathbb{Z}$, y obtenemos:

$$E_{11} = \{\mathcal{O},\ (1,2),\ (1,9),\ (2,1),\ (2,10),\ (4,2),\ (4,9),\ (5,0),$$
$$(6,2),\ (6,9),\ (7,0),\ (8,4),\ (8,7),\ (9,5),\ (9,6),\ (10,0)\}.$$

Por tanto, $\sharp(E_{11}) = 16$.

- Por último, reduciendo módulo $p = 17$, se tiene

$$Y^2 = X^3 + 13X + 12.$$

Los puntos con coordenadas en $\mathbb{Z}/17\mathbb{Z}$ que verifican esta ecuación son

$$E_{17} = \{\mathcal{O},\ (1,3),\ (1,14),\ (4,3),\ (4,14),\ (5,7),\ (5,10),$$
$$(6,0),\ (7,2),\ (7,15),\ (8,4),\ (8,13),\ (9,5),\ (9,12),$$
$$(12,3),\ (12,14),\ (13,7),\ (13,10),\ (16,7),\ (16,10)\}.$$

Luego, $\sharp(E_{12}) = 20$.

Como $\text{mcd}(8, 12, 16, 20) = 4$, tenemos que el orden de $\text{Tor}(E(\mathbb{Q}))$ divide a $C = 4$.

II.B. El algoritmo de Nagell–Lutz

Veamos un algoritmo basado en el Teorema de Nagell-Lutz, que calcula los puntos de torsión de una curva elíptica dada.

Sea E una curva elíptica en forma normal de Weierstrass:

$$E:\ Y^2 = X^3 + AX + B.$$

Sus puntos de orden 2 son de la forma $P = (x, 0)$, y los hallamos tomando las soluciones racionales x de la ecuación $X^3 + AX + B = 0$. Vamos a hallar los demás puntos de torsión.

Para cada y tal que $y^2 \mid \Delta$, resolvemos la ecuación en X

$$y^2 = X^3 + AX + B,$$

y para cada solución racional x de esta ecuación, consideramos el punto $P = (x, y)$. Así, si $P_1, P_2, \ldots, P_s$ son los puntos obtenidos de esta manera, entonces

$$\mathrm{Tor}(E(\mathbb{Q})) \subset \{P_1, P_2, \ldots, P_s\}.$$

Ahora comprobamos si cada uno de estos puntos P_i está en $\mathrm{Tor}(E(\mathbb{Q}))$, para $i = 1, \ldots, s$. Haremos lo siguiente: sea C la cota hallada mediante la reducción. Calculamos entonces dP_i, para todo $d|C$ y se tiene que $P_i \in \mathrm{Tor}(E(\mathbb{Q}))$ si y sólo si alguno de estos múltiplos de P_i es $\mathcal{O}$.

Esto lo repetimos para cada $i = 1, \ldots, s$; a no ser que paremos antes de llegar a s por haber obtenido ya C puntos de torsión.

Ejemplo.– Vamos a utilizar ahora el ejemplo que dimos en la sección anterior para calcular, mediante el algoritmo de Nagell-Lutz, el grupo de torsión de una curva elíptica. Teníamos la curva E de ecuación

$$Y^2 + XY + Y = X^3 - X^2 + 4X + 6,$$

cuya forma normal de Weierstrass era

$$E: \; Y^2 = X^3 + 5589X + 342630.$$

Buscamos primero los puntos de orden 2. Para ello, resolvemos la ecuación $X^3 + 5589X + 342630 = 0$, y obtenemos únicamente la solución $x = -45$. Esto quiere decir que el punto $(-45, 0)$ es el único punto de orden 2 en E.

Recordemos que el discriminante de la curva era

$$\Delta = 2^8 \cdot 3^{19} \cdot 13.$$

Ahora para cada $y \in \mathbb{Q}$ tal que y^2 divida a Δ, resolvemos la ecuación

$$y^2 = X^3 + 5589X + 342630,$$

y comprobamos si los puntos obtenidos son de torsión.

Haciendo cálculos tenemos:

- Para $y^2 = 2^2 \cdot 3^{10} = (\pm 486)^2 = 236196$, la ecuación

$$236196 = X^3 + 5589X + 342630$$

tiene la solución racional $x = -18$.

- Para $y^2 = 2^4 \cdot 3^{10} = (\pm 972)^2 = 944784$, la ecuación

$$944784 = X^3 + 5589X + 342630$$

tiene la solución racional $x = 63$.

De esto obtenemos 4 posibles puntos de torsión:

$$P_1 = (-18, 486),\ P_2 = (-18, -486),\ P_3 = (63, 972),\ P_4 = (63, -972).$$

Como hemos visto en este ejemplo en la sección II.A., el grupo $\mathrm{Tor}(E(\mathbb{Q}))$ tendrá orden divisor de $C = 4$, (i.e. orden 1, 2 ó 4), luego si estos puntos P_i son de torsión, serán de orden 2 ó 4. Pero de orden 2 no son porque tienen $y \neq 0$, luego serán de orden 4.

Esto significa que para que $P_i \in \mathrm{Tor}(E(\mathbb{Q}))$, ha de ser $2P_i$ un punto de orden 2, y como el único punto de orden 2 que hay es $(-45, 0)$, tendrá que ser $2P_i = (-45, 0)$.

Ahora basta sustituir en la fórmula de duplicación y ver que

$$2P_1,\ 2P_2 \neq (-45, 0); \quad 2P_3,\ 2P_4 = (-45, 0).$$

En resumen,

$$\begin{aligned} \mathrm{Tor}(E(\mathbb{Q})) &= \{\mathcal{O},\ P = (63, 972),\ 2P = (-45, 0),\ 3P = (63, -972)\} \\ &= \langle P \rangle \simeq \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Hemos calculado así la torsión racional de E y vemos que, en este caso, forma un grupo cíclico de orden 4.

Observación.– Este algoritmo es el más útil cuando los cálculos se hacen a mano, o cuando se trabaja con curvas elípticas de discriminante pequeño. Pero, en general, no es muy eficiente, siendo su mayor inconveniente la necesidad de factorizar el discriminante Δ, para obtener los y^2 que lo dividan, ya que esto es muy costoso computacionalmente. Usando la estimación habitual [8] para el mejor algoritmo actual de factorización, la complejidad del algoritmo de Nagell-Lutz sería

$$O\left(e^{(C+O(1))(\log|\Delta|)^{1/3}(\log\log|\Delta|)^{2/3}}\right).$$

Éste es el algoritmo usado en [9], de 1992, que ha sido durante años la referencia central en aspectos computacionales de curvas elípticas. El hecho de que los algoritmos que presentaremos a continuación poseen todos ellos complejidad logarítmica, nos da una idea de cómo ha evolucionado este campo en los últimos años.

II.C. El algoritmo de la parametrización analítica

Veamos cómo la interpretación analítica de una curva elíptica puede sernos útil para calcular su torsión. El algoritmo que presentamos en esta sección es original de D. Doud [10]. Dada una curva elíptica E de ecuación

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

con $A, B \in \mathbb{Q}$, necesitamos calcular su discriminante Δ y una base del retículo asociado a la curva.

Recordemos que con el isomorfismo

$$\begin{array}{rccc} \varphi: & \mathbb{C}/\Lambda & \longrightarrow & E(\mathbb{C}) \\ & u+\Lambda & \longmapsto & \varphi(u+\Lambda) = (\wp(u), \wp'(u)), \end{array}$$

teníamos una parametrización para los puntos con coordenadas complejas de la curva elíptica E, que nos permitía identificar $E(\mathbb{C})$ con un toro.

Vamos a describir los puntos complejos de orden finito de E.

Si buscamos puntos de orden 2, necesitamos un complejo $u \notin \Lambda$ tal que $2u \in \Lambda$; ya que así tendremos

$$\varphi(u) \in E(\mathbb{C}) \setminus \{\mathcal{O}\} \text{ y } 2\varphi(u) = \varphi(u) + \varphi(u) = \varphi(u+u) = \varphi(2u) = \mathcal{O}.$$

Pero los complejos u que no están en el retículo Λ tales que $2u \in \Lambda$ son sólo tres (tomando módulo Λ):

$$\frac{\omega_1}{2}, \quad \frac{\omega_2}{2} \quad \text{y} \quad \frac{\omega_1+\omega_2}{2}.$$

De la misma forma, para dar puntos de orden divisor de m, buscamos complejos u que estén en el paralelogramo definido por la base $\langle \omega_1, \omega_2 \rangle$ del retículo, tales que $mu \in \Lambda$. Por ejemplo, si $m = 5$ encontramos 25 puntos de orden divisor de 5, que forman el producto directo de dos grupos cíclicos

de orden 5. En general, los puntos de coordenadas complejas de E de orden divisor de m forman un grupo de orden m^2 que es producto directo de dos grupos cíclicos de orden m.

Con todo esto, el problema de encontrar puntos racionales de torsión en E, se reduce a encontrar puntos complejos de orden finito en $\mathbb{C}/\Lambda$, que son los puntos de $(1/m)\mathbb{C}/\Lambda$, y comprobar si su imagen por φ en E son puntos de coordenadas racionales.

Vamos a dar un algoritmo para calcular los puntos de torsión de la curva E, usando la parametrización analítica dada para ella; recordemos que los complejos ω_1 y ω_2, que caracterizan el retículo, se calculan siguiendo el algoritmo dado en I.C.:

Primero damos una cota C para el orden de $\mathrm{Tor}(E(\mathbb{Q}))$, que como ya sabemos va a ser un múltiplo de dicho orden. Esto lo conseguimos como explicamos en la sección II.A. A continuación distinguimos tres casos:

1. Si $C = 1$, entonces es $\mathrm{Tor}(E(\mathbb{Q})) = \{\mathcal{O}\}$.

2. Si 4 no divide a C, por el teorema de Mazur, el grupo de torsión ha de ser cíclico de orden $n \leq 10$ con n divisor de C (porque los otros posibles grupos tienen orden múltiplo de 4).

   Empezando por el mayor n posible, calculamos un punto de torsión de orden n en la componente de E que contiene a $\mathcal{O}$.

   Esto lo podemos hacer hallando el punto correspondiente a ω_1/n. Se tiene entonces:

   - Si este punto es racional, genera $\mathrm{Tor}(E(\mathbb{Q}))$.
   - Si este punto no es racional y su orden es par, podría diferenciarse de un punto racional de torsión en un punto de orden 2 en la componente de E que no contiene a $\mathcal{O}$.

     Luego, calculamos dos puntos más de torsión, los correspondientes a

     $$\frac{\omega_1}{n} + \frac{\omega_2}{2} \quad \text{y} \quad \frac{\omega_1}{n} + \frac{\omega_1 + \omega_2}{2},$$

     y comprobamos si son racionales.

     Si alguno es racional, ése genera $\mathrm{Tor}(E(\mathbb{Q}))$.

   Si probando con todos los $n \leq 10$, siendo n divisor de C, no hemos encontrado un generador, entonces

   $$\mathrm{Tor}(E(\mathbb{Q})) = \{\mathcal{O}\}.$$

3. Si 4 divide a C, el grupo de torsión podría no ser cíclico. Calculamos los puntos de orden 2 en $E(\mathbb{C})$ y vemos si son racionales. Pueden darse tres casos:

   - No hay puntos de orden 2.

     En este caso el subgrupo de torsión es cíclico de orden impar, y debe estar contenido en la componente real que contiene a $\mathcal{O}$.

     Comprobamos con cada n impar tal que n sea divisor de C y $n \leq 9$, si ω_1/n corresponde a un punto racional de torsión.

     Lo comprobamos con n de mayor a menor. El primero que lo cumpla es el generador de $\mathrm{Tor}(E(\mathbb{Q}))$.

     Si ninguno lo cumple, es

     $$\mathrm{Tor}(E(\mathbb{Q})) = \{\mathcal{O}\}.$$

   - Sólo hay un punto de orden 2.

     En esta situación el grupo de torsión es cíclico de orden par. Lo calculamos como en el caso en que 4 no divide a C, pero ahora sólo necesitamos comprobar los puntos de orden par.

   - Hay más de un punto de orden 2.

     Entonces sabemos que el grupo de torsión no es cíclico.

     Podríamos tomar como uno de los generadores un punto de orden 2 en la componente de la curva que no contiene a $\mathcal{O}$.

     Como otro generador, tomaremos un punto que esté en la componente que contiene a $\mathcal{O}$ y que sea de orden 8, 6, 4 o 2. Para ello calculamos los puntos correspondientes a

     $$\frac{\omega_1}{8}, \quad \frac{\omega_1}{6} \quad \text{y} \quad \frac{\omega_1}{4},$$

     y el primero que sea racional será el segundo generador que buscábamos.

     Si ninguno de éstos es racional, el segundo generador será el punto de orden 2 de la componente que contiene a $\mathcal{O}$.

Ejemplo.– Tal y como hicimos en la sección anterior, veremos ahora cómo aplicar en la práctica este algoritmo, usando de nuevo la curva dada en el ejemplo de la sección II.A. Consideramos la curva E

$$Y^2 = X^3 + 5589X + 342630.$$

Calculamos en primer lugar una base $\langle \omega_1, \omega_2 \rangle$ del retículo Λ asociado a la curva E, y según el algoritmo dado en I.C. (cuya implementación en MAPLE se recoge en el apéndice A.1.) obtenemos

$$\begin{aligned} \omega_1 &= 0.4400541877213838, \\ \omega_2 &= -0.2200270938606919 + i\,0.1590961510406907. \end{aligned}$$

También ahora necesitamos la cota dada en II.A. para el orden del grupo de torsión racional de la curva, $C = 4$.

El siguiente paso, según el algoritmo de Doud, consiste en hallar los puntos de orden 2, pero ya sabemos (por la sección anterior) que sólo hay uno, el punto $P = (-45, 0)$.

Una vez que sabemos que el grupo de torsión es cíclico de orden par, calculamos el punto de la curva que corresponde a $\omega_1/4$, y vemos si es racional o no. Para ello, multiplicando por 4 la ecuación de partida de E, obtenemos

$$(2Y)^2 = 4X^3 - (-4 \cdot 5589)X - (-4 \cdot 342630),$$

y, tomando $Y_1 = 2Y$ y $X_1 = X$, tenemos la (también llamada) forma corta de Weierstrass

$$Y_1^2 = 4X_1^3 - (-4 \cdot 5589)X_1 - (-4 \cdot 342630),$$

donde los puntos de coordenadas (X_1, Y_1) son los puntos $(\wp(u), \wp'(u))$, para los complejos u modulo Λ. Usando las funciones de MAPLE

```
WeierstrassP(u,-4*5589,-4*342630),
WeierstrassPPrime(u,-4*5589,-4*342630);
```

para $\wp(u)$ y $\wp'(u)$, respectivamente, cuando $u = \omega_1/4$, conseguimos el punto $(X_1, Y_1) = (63, 1944)$, que corresponde al punto $P = (63, 972)$ de nuestra curva original.

Así, hemos encontrado un punto de orden 4, y podemos afirmar entonces que el grupo de torsión racional de la curva E es

$$\begin{aligned} \mathrm{Tor}(E(\mathbb{Q})) &= \{\mathcal{O},\ P = (63, 972),\ 2P = (-45, 0),\ -P = (63, -972)\} \\ &= \langle P \rangle \simeq \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Observación.– Este algoritmo es más rápido que el dado por el teorema de Nagell-Lutz. En aquel algoritmo necesitábamos la factorización del discriminante Δ; ahora lo más costoso computacionalmente es calcular los puntos de la curva que corresponden a los complejos de la forma ω_1/n, $\omega_1/n + \omega_2/2$ y

$\omega_1/n + (\omega_1 + \omega_2)/2$, dado que necesitamos operar con una precisión elevada, cuando menos del orden de $\log|\Delta| + 3$, para reconocer puntos enteros en la curva original. La complejidad de esto es muchísimo menor que la de los mejores algoritmos de factorización entera actualmente disponibles [10]. Sin tener en cuenta la acotación de la torsión usando la reducción modulo p, la complejidad de este algoritmo de Doud es de $O(\log^3|\Delta|)$.

II.D. El algoritmo de los polinomios de división

En este algoritmo aplicaremos las propiedades de los polinomios de división Ψ_m, estudiadas en la sección I.F.

El procedimiento para calcular la torsión racional de una curva elíptica sería ahora el descrito a continuación: Dada la curva elíptica E de ecuación

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

seguimos los siguientes pasos:

1. Calculamos los puntos de orden 2 de E, hallando las raíces enteras de $X^3 + AX + B$. Llamamos L al número de puntos racionales de orden 2 que tiene la curva.

2. Calculamos el discriminante, $\Delta = 4A^3 + 27B^2$, y hallamos varios buenos primos para calcular una cota C del orden del grupo de torsión, como en II.A.

   - Si $C = L + 1$, ya tenemos el grupo de torsión racional de E, que estará formado por $\mathcal{O}$ y los puntos de orden 2.
   - Si $C \neq L + 1$, vamos al paso 3. Observemos que en este caso, en realidad, C será un múltiplo de $L + 1$, ya que:
     - Si $L = 0$, está claro que $0 + 1$ divide a C.
     - Si $L = 1$, es decir, si la curva tiene sólo un punto de orden 2, el grupo de torsión es cíclico de orden par o no cíclico, por tanto, el orden del grupo de torsión es par, y tenemos que $1 + 1$ divide a C.
     - Si $L = 3$, el grupo de torsión es no cíclico, es decir, de la forma $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ con $1 \leq n \leq 4$, luego, $3 + 1$ divide a C.

3. Sean $d_1 > d_2 > \cdots > d_s$ los divisores de $C/(L + 1)$.

Para cada $d_i \leq 12$, con i desde 1 hasta s, averiguamos si hay puntos de torsión de orden d_i en E, usando los polinomios de división. Esto es, buscamos soluciones enteras de la ecuación

$$\Psi_{d_i}(x) = 0.$$

Si encontramos $i \in \{1, ..., s\}$ tal que $\Psi_{d_i}(x)$ tiene alguna raíz entera, comprobamos si x corresponde a algún punto racional de la curva, (sustituyéndolo en la ecuación de la misma), y entonces la torsión de E tendrá puntos de orden d_i. Si $\Psi_{d_i}(x)$ no tiene raíces enteras, pasamos a estudiar $\Psi_{d_{i+1}}(x)$. Una vez conocidos los órdenes de los puntos racionales del grupo de torsión, usando el teorema de Mazur, podremos averiguar de qué grupo se trata.

Si para todo $i = 1, ..., s$ resulta que $\Psi_{d_i}(x)$ no tiene raíces enteras, entonces el grupo de torsión de E está formado únicamente por $\mathcal{O}$ y los puntos de orden 2.

Observación.– Vamos a analizar el coste computacional de este algoritmo. Además de hallar y factorizar C, (cosa que, por otra parte, es innecesaria ya que, por el teorema de Mazur, sólo podemos tener puntos de orden 12 ó menor o igual que 10), todos los pasos de este algoritmo consisten en realizar operaciones aritméticas o en hallar soluciones de ecuaciones con una variable y coeficientes enteros. Esto se puede conseguir de manera bastante eficiente, como demuestra Loos [20].

Concretamente, Loos prueba que, dado un polinomio

$$f = \sum_{j=0}^{e} a_j X^j \in \mathbb{Z}[X],$$

existe un algoritmo que calcula las raíces racionales de f y que tiene una complejidad de $\mathcal{O}(\log^2 \|f\|)$, siendo

$$\|f\| = \sum_{j=0}^{e} |a_j|.$$

Veamos cómo podemos acotar las normas de nuestros polinomios de división. Sabiendo, por el teorema de Mazur, las posibilidades que tiene el orden de un punto racional de torsión de una curva elíptica, sólo nos interesan los polinomios $\Psi_3, ..., \Psi_9$, que en el caso de nuestra curva son los que aparecen de forma explícita en el programa DECDP dentro del apéndice A.1.

Si llamamos

$$N = \max\{|A|^3, |B|^2\},$$

resulta:

$$\begin{aligned}
\|\Psi_3\| &\leq 22N, \\
\|\Psi_4\| &\leq 88N, \\
\|\Psi_5\| &\leq 1332N + 5740N^2 \leq 7072N^2, \\
\|\Psi_6\| &\leq 2804N + 4162N^2 \leq 6966N^2, \\
\|\Psi_7\| &\leq 70073N + 5890763N^2 + 35170373N^3 + 10322379N^4 \\
&\leq 51453588N^4, \\
\|\Psi_8\| &\leq 74815N + 2560557N^2 + 28694293N^3 + 8825523N^4 \\
&\leq 40155188N^4, \\
\|\Psi_9\| &\leq 648462N + 306618672N^2 + 22166698686N^3 + 82306925334N^4 \\
&\quad +147171786132N^5 + 12745366702N^6 \\
&\leq 264698043988N^6.
\end{aligned}$$

Estas acotaciones se pueden resumir en una expresión general,

$$\|\Psi_i\| \leq c_i N^{2(\lceil i/2 \rceil - 1)}$$

para $i = 4, ..., 9$, siendo c_i números naturales.

Así, según Loos, la resolución de la ecuación $\Psi_i(x) = 0$, tendría una complejidad de $\mathcal{O}(\log^2 \|\Psi_i\|)$, que podemos acotar en función de N, ya que, de las acotaciones que acabamos de ver para las normas de estos polinomios se deduce que $\mathcal{O}(\log^2 \|\Psi_i\|) \leq \mathcal{O}(\log^2 N)$.

Por tanto, como $\mathcal{O}(\log^2 N) = \mathcal{O}(\log^2 |\Delta|)$, resulta que el algoritmo de los polinomios de división para calcular la torsión racional de una curva elíptica, tiene un coste en tiempo de $\mathcal{O}(\log^2 |\Delta|)$, donde Δ es el discriminante de la curva.

Observación.– El polinomio Ψ_{10} no es necesario, ya que si una curva tiene un punto de orden 10, su grupo de torsión será cíclico de orden 10, y esto sólo ocurre si tiene puntos de orden 2 y 5, cosa que se puede detectar con Ψ_5. Lo mismo ocurre con Ψ_{12}, cuyo uso será sustituido por el de Ψ_3 y Ψ_4, ya que para que el grupo de torsión sea cíclico de orden 12, es necesario y suficiente que tenga puntos de orden 3 y 4.

Ejemplo.– Completaremos esta sección con la aplicación del algoritmo de los polinomios de división al ejemplo que hemos venido usando en anteriores secciones. Dada la curva elíptica

$$E : Y^2 = X^3 + 5589X + 342630,$$

sabemos que tiene un solo punto de orden 2, el $(-45, 0)$. Tenemos entonces que $\mathrm{Tor}(E(\mathbb{Q}))$ es cíclico de orden par, pero además, por lo visto en II.A, sabemos que es de orden divisor de $c = 4$.

Para ver si $\mathrm{Tor}(E(\mathbb{Q}))$ es un grupo de orden exactamente 4, comprobamos si la ecuación $\Psi_4(x) = 0$ tiene alguna solución entera.

Esta ecuación es

$$x^6+27945x^4+6852600x^3-156184605x^2-7659836280x-1113745686669 = 0,$$

que factorizada queda

$$(x-63)(x+153)(x^4-90x^3+45684x^2+1873530x+115545771) = 0,$$

de donde se ve que tiene las soluciones enteras, $x = 63$ y $x = -153$. La segunda de éstas no corresponde a ningún punto racional de nuestra curva (ya que al sustituir X por -153 resulta $Y^2 = -4094064$), pero la primera corresponde a los puntos $P = (63, 972)$ y $-P = (63, -972)$ de orden 4. Por tanto, resulta

$$\begin{aligned} \mathrm{Tor}(E(\mathbb{Q})) &= \{\mathcal{O},\ P = (63, 972),\ 2P = (-45, 0),\ -P = (63, -972)\} \\ &= \langle P \rangle \simeq \mathbb{Z}/4\mathbb{Z}, \end{aligned}$$

grupo cíclico de orden 4.

II.E. El algoritmo de la forma normal de Tate

El algoritmo de los polinomos de división reduce el problema del cálculo de la torsión al de decidir, para una curva dada, si existe un punto de orden n. En esta sección vamos a mostrar otra forma de averiguar si una curva elíptica definida sobre $\mathbb{Q}$ tiene un punto de orden dado. Para ello, como hicimos en [15], utilizaremos el teorema demostrado en la sección I.G. que caracteriza, como familia uniparamétrica, la forma normal de Tate de una curva elíptica que posee un punto de orden dado.

Sea E una curva elíptica de ecuación

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

y supongamos que tiene un punto de orden n. Entonces, nuestra curva E debe ser isomorfa a una curva de la familia uniparamétrica que, por el teorema de I.G., corresponde a n.

El primer paso de este algoritmo consiste en tomar la forma normal de Weierstrass de una curva genérica de dicha familia,

$$Y^2 = X^3 + A(\alpha)X + B(\alpha),$$

y relacionarla con nuestra curva de partida E.

Recordemos que para que estas dos curvas $Y^2 = X^3 + AX + B$ y $Y^2 = X^3 + A(\alpha)X + B(\alpha)$, sean isomorfas es necesario y suficiente que se den las siguientes condiciones:

1. Se verifica la igualdad
$$\frac{A^3}{B^2} = \frac{A(\alpha)^3}{B(\alpha)^2}.$$

2. Existe una solcuión racional u para el sistema de ecuaciones
$$\begin{cases} u^4 = \dfrac{A}{A(\alpha)}, \\ u^6 = \dfrac{B}{B(\alpha)}, \end{cases}$$
con los ajustes obvios en caso de que alguno de los coeficientes sea nulo.

Por tanto, primero tenemos que averiguar si el polinomio

$$A^3B(\alpha)^2 - B^2A(\alpha)^3,$$

que llamaremos *el polinomio final*, tiene alguna raíz racional, y después, para cada una de estas raíces α_0, comprobar si existe algún $u \in \mathbb{Q}$ tal que

$$u^4 = \frac{A}{A(\alpha_0)} \quad \text{y} \quad u^6 = \frac{B}{B(\alpha_0)}.$$

Ejemplo.– Veamos un ejemplo concreto para ilustrar este proceso antes de continuar con su análisis. Dada la curva

$$Y^2 = X^3 + 12933X - 2285226,$$

vamos a averiguar si tiene algún punto de orden 5.

Si así fuera, la curva debería ser isomorfa a una de las curvas de la familia

$$Y^2 + (1-\alpha)XY - \alpha Y = X^3 - \alpha X^2.$$

Al calcular la forma normal de Weierstrass de una curva genérica de esta familia, se obtiene

$$Y^2 = X^3 + A_5(\alpha)X + B_5(\alpha),$$

donde

$$A_5(\alpha) = -27\alpha^4 + 324\alpha^3 - 378\alpha^2 - 324\alpha - 27,$$
$$B_5(\alpha) = 54\alpha^6 - 972\alpha^5 + 4050\alpha^4 + 4050\alpha^2 + 972\alpha + 54.$$

Entonces, el polinomio final para $n = 5$ será

$$12933^3 B_5(\alpha)^2 - (-2285226)^2 A_5(\alpha)^3,$$

que operando y factorizando resulta

$$\begin{aligned} P_5(\alpha) \;=\; & 99179645184(10\alpha + 1)(\alpha - 10)(110000\alpha^{10} - 2871000\alpha^9 \\ & +23827100\alpha^8 - 63982710\alpha^7 + 25648271\alpha^6 + 75984949\alpha^5 \\ & -25648271\alpha^4 - 63982710\alpha^3 - 23827100\alpha^2 \\ & -2871000\alpha - 110000), \end{aligned}$$

cuyas únicas raíces racionales son 10 y $-1/10$.

Para $\alpha_0 = 10$, al sustituir, queda $A_5(\alpha_0) = 12933$ y $B_5(\alpha_0) = -2285226$, por tanto, encontramos $u = 1$ solución del sistema

$$u^4 = \frac{12933}{A_5(\alpha_0)} \quad \text{y} \quad u^6 = \frac{-2285226}{B_5(\alpha_0)}.$$

Así, podemos afirmar ahora que nuestra curva de partida tiene un punto de orden 5.

Para averiguar las coordenadas de dicho punto, habrá que deshacer los cambios realizados para pasar de la forma normal de Tate, donde el punto $(0, 0)$ es de orden 5, a la forma normal de Weierstrass.

En primer lugar, en la ecuación

$$Y^2 + (1 - 10)XY - 10Y = X^3 - 10X^2,$$

el cambio

$$Y \longmapsto Y + \frac{9X + 10}{2},$$

produce la ecuación

$$Y^2 = X^3 + \frac{41}{4}X^2 + 45X + 25,$$

de donde, haciendo el cambio

$$X \longmapsto X - \frac{41}{12},$$

se obtiene

$$Y^2 = X^3 + \frac{479}{48}X - \frac{42319}{864}.$$

En esta ecuación hacemos un último cambio

$$Y \longmapsto \frac{1}{216}Y, \quad X \longmapsto \frac{1}{36}X,$$

para obtener

$$Y^2 = X^3 + 12933X - 2285226.$$

Aplicamos estos cambios al punto $(0,0)$ de la curva en forma normal de Tate, y tenemos

$$(0,0) \longmapsto (0,-5) \longmapsto \left(\frac{41}{12}, -5\right) \longmapsto (123, -1080).$$

Por tanto, nuestra curva de partida, tiene el punto $P = (123, -1080)$ que es de orden 5.

Observación.– Con el algoritmo presentado en esta sección, el único caso que queda por estudiar es $n = 3$. Es decir, necesitamos un procedimiento para decidir si una curva elíptica dada tiene o no un punto de orden 3. También podríamos dar una forma normal de Tate en este caso, pero en vez de obtener una familia uniparamétrica, obtendríamos una familia de curvas dependiente de dos parámetros. Por tanto, será mejor usar el polinomio de división correspondiente, Ψ_3, para averiguar si hay puntos de orden 3 en la curva.

Observación.– Continuando con el análisis del algoritmo, recordemos que en el primer paso, hay que averiguar si el polinomio final, $A^3B(\alpha)^2 - B^2A(\alpha)^3$, tiene alguna raíz racional. Para decidir cuál es el mejor parámetro que podemos usar, tenemos que pensar qué método vamos a emplear para la búsqueda de raíces racionales del polinomio.

Como en el caso del algoritmo de los polinomios de división, según Loos [20], la complejidad de hallar las raíces racionales del polinomio $f(X) \in \mathbb{Z}[X]$ es $\mathcal{O}(\log^2 \|f\|)$, por tanto, debemos elegir un parámetro que minimice la norma del polinomio final. A este parámetro lo llamaremos *parámetro mínimo*, y a su polinomio final, *polinomio mínimo*, que denotaremos por F_n.

Observación.– Vamos a estudiar los polinomio mínimos para cada n.

Caso $n = 4$. La ecuación general de la curva es

$$Y^2 + XY - \alpha Y = X^3 - \alpha X^2,$$

y al calcular su forma normal de Weierstrass se obtiene

$$Y^2 = X^3 + A_4(\alpha)X + B_4(\alpha),$$

donde

$$A_4(\alpha) = -432\alpha^2 - 432\alpha - 27, \text{ y}$$
$$B_4(\alpha) = -3456\alpha^3 + 6480\alpha^2 + 1296\alpha + 54.$$

Así, el polinomio final para $n = 4$ es

$$\begin{aligned} P_4(\alpha) &= A^3 \cdot B_4(\alpha)^2 - B^2 \cdot A_4(\alpha)^3 \\ &= 2^{12}3^6(4A^3 + 27B^2)\alpha^6 - 2^{12}3^7(5A^3 - 27B^2)\alpha^5 \\ &\quad +2^83^7(59A^3 + 459B^2)\alpha^4 + 2^93^611(4A^3 + 27B^2)\alpha^3 \\ &\quad +2^43^717(4A^3 + 27B^2)\alpha^2 + 2^43^7(4A^3 + 27B^2)\alpha \\ &\quad +3^6(4A^3 + 27B^2). \end{aligned}$$

Buscamos un nuevo parámetro β, con $\alpha = r\beta + s$, que sea un parámetro mínimo. Como los coeficientes del polinomio $F_4(\beta)$ deben ser enteros, en vista de los coeficientes de $P_4(\alpha)$, podemos tomar $r = 1/12$, y $s \in \mathbb{Q}$ tal que su denominador sea divisor de 12. Para que la norma de $F_4(\beta)$ sea mínima, tomamos $s = -1/12$. Luego, sustituyendo $\alpha = (\beta - 1)/12$ en $P_4(\alpha)$, se tiene el polinomio mínimo

$$\begin{aligned} F_4(\beta) &= (4A^3 + 27B^2)\beta^6 - 6(34A^3 - 135B^2)\beta^5 \\ &\quad +3(851A^3 + 2646B^2)\beta^4 + 4(313A^3 + 5940B^2)\beta^3 \\ &\quad -6(95A^3 + 2646B^2)\beta^2 - 24(7A^3 - 135B^2)\beta \\ &\quad +49A^3 - 216B^2, \end{aligned}$$

cuya norma es

$$\begin{aligned} \|F_4\| &= |4A^3 + 27B^2| + 6|34A^3 - 135B^2| + 3|851A^3 + 2646B^2| \\ &\quad +4|313A^3 + 5940B^2| + 6|95A^3 + 2646B^2| \\ &\quad +24|7A^3 - 135B^2| + |49A^3 - 216B^2|. \end{aligned}$$

Si llamamos $N = \max\{|A|^3, |B|^2\}$, tendremos

$$\|F_4\| \leq 56667N.$$

Caso $n = 5$. La ecuación en forma normal de Tate de una curva que tiene un punto de orden 5 es

$$Y^2 + (1 - \alpha)XY - \alpha Y = X^3 - \alpha X^2,$$

y su forma normal de Weierstrass es

$$Y^2 = X^3 + A_5(\alpha)X + B_5(\alpha),$$

con

$$A_5(\alpha) = -27\alpha^4 + 324\alpha^3 - 378\alpha^2 - 324\alpha - 27, \quad \text{y}$$

$$B_5(\alpha) = 54\alpha^6 - 972\alpha^5 + 4050\alpha^4 + 4050\alpha^2 + 972\alpha + 54.$$

Luego, para $n = 5$, el polinomio final es

$$\begin{aligned} P_5(\alpha) &= A^3 \cdot B_5(\alpha)^2 - B^2 \cdot A_5(\alpha)^3 \\ &= 3^6(4A^3 + 27B^2)\alpha^{12} - 2^2 3^8(4A^3 + 27B^2)\alpha^{11} \\ &\quad +2 \cdot 3^7 79(4A^3 + 27B^2)\alpha^{10} - 2^2 3^9 5^2(4A^3 + 27B^2)\alpha^9 \\ &\quad +3^7 5^2 7 \cdot 11(4A^3 + 27B^2)\alpha^8 - 2^3 3^8(148A^3 + 351B^2)\alpha^7 \\ &\quad +2^2 3^6 \cdot 11(964A^3 - 5157B^2)\alpha^6 + 2^3 3^8(148A^3 + 351B^2)\alpha^5 \\ &\quad +3^7 5^2 7 \cdot 11(4A^3 + 27B^2)\alpha^4 + 2^2 3^9 5^2(4A^3 + 27B^2)\alpha^3 \\ &\quad +2 \cdot 3^7 79(4A^3 + 27B^2)\alpha^2 + 2^2 3^8(4A^3 + 27B^2)\alpha \\ &\quad +3^6(4A^3 + 27B^2). \end{aligned}$$

Tomamos como parámetro mínimo $\beta = \alpha$, por tanto, el polinomio mínimo será $F_5(\beta) = P_5(\alpha)/3^6$, cuya norma resulta

$$\begin{aligned} \|F_5\| &= |4A^3 + 27B^2| + 2^2 3^2 |4A^3 + 27B^2| + 2 \cdot 3 \cdot 79|4A^3 + 27B^2| \\ &\quad +2^2 3^3 5^2 |4A^3 + 27B^2| + 3 \cdot 5^2 7 \cdot 11|4A^3 + 27B^2| \\ &\quad +2^3 3^2 |148A^3 + 351B^2| + 2^2 \cdot 11|964A^3 - 5157B^2| \\ &\quad +2^3 3^2 |148A^3 + 351B^2| + 3 \cdot 5^2 7 \cdot 11|4A^3 + 27B^2| \\ &\quad +2^2 3^3 5^2 |4A^3 + 27B^2| + 2 \cdot 3 \cdot 79|4A^3 + 27B^2| \\ &\quad +2^2 3^2 |4A^3 + 27B^2| + |4A^3 + 27B^2|. \end{aligned}$$

En función de N, conseguimos ahora la acotación

$$\|F_5\| \leq 898312N.$$

Caso $n = 6$. Para que una curva elíptica en forma normal de Tate tenga un punto de orden 6, su ecuación debe ser

$$Y^2 + (1 - \alpha)XY - \alpha(1 + \alpha)Y = X^3 - \alpha(1 + \alpha)X^2,$$

cuya forma normal de Weierstrass es

$$Y^2 = X^3 + A_6(\alpha)X + B_6(\alpha),$$

donde

$$A_6(\alpha) = -243\alpha^4 - 324\alpha^3 - 810\alpha^2 - 324\alpha - 27, \quad \text{y}$$

$$B_6(\alpha) = -1458\alpha^6 - 2916\alpha^5 + 7290\alpha^4 + 9720\alpha^3 + 5346\alpha^2 + 972\alpha + 54.$$

Así, el polinomio final para $n = 6$ es

$$\begin{aligned} P_6(\alpha) &= A^3 \cdot B_6(\alpha)^2 - B^2 \cdot A_6(\alpha)^3 \\ &= 3^{12}(4A^3 + 27B^2)\alpha^{12} + 2^2 3^{12}(4A^3 + 27B^2)\alpha^{11} \\ &\quad -2 \cdot 3^{13}(4A^3 - 69B^2)\alpha^{10} + 2^2 3^{11}(100A^3 - 669B^2)\alpha^9 \\ &\quad -3^{13}(12A^3 - 559B^2))\alpha^8 - 2^3 3^{11}(76A^3 + 801B^2)\alpha^7 \\ &\quad +2^2 3^9(2116A^3 + 14715B^2)\alpha^6 + 2^3 3^9 11 \cdot 17(4A^3 + 27B^2)\alpha^5 \\ &\quad +3^9 613(4A^3 + 27B^2)\alpha^4 + 2^2 3^8 109(4A^3 + 27B^2)\alpha^3 \\ &\quad +2 \cdot 3^8 29(4A^3 + 27B^2)\alpha^2 + 2^2 3^8(4A^3 + 27B^2)\alpha \\ &\quad +3^6(4A^3 + 27B^2), \end{aligned}$$

por lo que tomamos β como parámetro mínimo tal que $\alpha = (\beta - 1)/3$. Luego, el polinomio mínimo en este caso será

$$\begin{aligned} F_6(\beta) &= (4A^3 + 27B^2)\beta^{12} - 24(20A^3 - 81B^2)\beta^{10} \\ &\quad +16(20A^3 - 81B^2)\beta^9 + 1728(8A^3 + 27B^2)\beta^8 \\ &\quad -2304(8A^3 + 27B^2)\beta^7 + 768(13A^3 + 513B^2)\beta^6 \\ &\quad -13824(5A^3 + 54B^2)\beta^5 + 2304(29A^3 + 216B^2)\beta^4 \\ &\quad -4096(16A^3 + 27B^2)\beta^3 + 55296A^3\beta^2 \\ &\quad -24576A^3\beta + 4096A^3, \end{aligned}$$

cuya norma

$$\begin{aligned} \|F_6\| &= |4A^3 + 27B^2| + 24|20A^3 - 81B^2| + 16|20A^3 - 81B^2| \\ &\quad +1728|8A^3 + 27B^2| + 2304|8A^3 + 27B^2| \\ &\quad +768|13A^3 + 513B^2| + 13824|5A^3 + 54B^2| \\ &\quad +2304|29A^3 + 216B^2| + 4096|16A^3 + 27B^2| \\ &\quad +55296|A^3| + 24576|A^3| + 4096|A^3|, \end{aligned}$$

se puede acotar por

$$\|F_6\| \leq 2220071N.$$

Caso $n = 7$. Ahora la ecuación general de la curva es

$$Y^2 + (1 - \alpha(\alpha - 1))XY - \alpha^2(\alpha - 1)Y = X^3 - \alpha^2(\alpha - 1)X^2,$$

y al calcular su forma normal de Weierstrass se obtiene

$$Y^2 = X^3 + A_7(\alpha)X + B_7(\alpha),$$

donde

$$A_7(\alpha) = -27\alpha^8 + 324\alpha^7 - 1134\alpha^6 + 1512\alpha^5 - 945\alpha^4 + 378\alpha^2 - 108\alpha - 27, \text{ y}$$

$$B_7(\alpha) = 54\alpha^{12} - 972\alpha^{11} + 6318\alpha^{10} - 19116\alpha^9 + 30780\alpha^8 - 26244\alpha^7$$

$$+14742\alpha^6 - 11988\alpha^5 + 9396\alpha^4 - 2484\alpha^3 - 810\alpha^2 + 324\alpha + 54.$$

Entonces, el polinomio final para $n = 7$ es

$$\begin{aligned}
P_7(\alpha) &= A^3 \cdot B_7(\alpha)^2 - B^2 \cdot A_7(\alpha)^3 \\
&= 3^6(558(4A^3 + 27B^2)\alpha^{22} - 4920(4A^3 + 27B^2)\alpha^{21} \\
&\quad +27573(4A^3 + 27B^2)\alpha^{20} - 104328(4A^3 + 27B^2)\alpha^{19} \\
&\quad +276738(4A^3 + 27B^2)\alpha^{18} - 12(175852A^3 \\
&\quad +1183113B^2)\alpha^{17} + 30(98828A^3 + 643761B^2)\alpha^{16} \\
&\quad -4(805628A^3 + 4481541B^2)\alpha^{15} + 6(497956A^3 \\
&\quad +1518291B^2)\alpha^{14} - 2688(970A^3 - 621B^2)\alpha^{13} \\
&\quad +91(22748A^3 - 79731B^2)\alpha^{12} - 168(7876A^3 \\
&\quad -34317B^2)\alpha^{11} + 54(12436A^3 - 25785B^2)\alpha^{10} \\
&\quad -12(27220A^3 + 98199B^2)\alpha^9 + 18(8404A^3 \\
&\quad +61911B^2)\alpha^8 - 12(2348A^3 + 19737B^2)\alpha^7 \\
&\quad -5222(4A^3 + 27B^2)\alpha^6 + 3024(4A^3 + 27B^2)\alpha^5 \\
&\quad +21(4A^3 + 27B^2)\alpha^4 - 272(4A^3 + 27B^2)\alpha^3 \\
&\quad +6(4A^3 + 27B^2)\alpha^2 + 12(4A^3 + 27B^2)\alpha \\
&\quad +(4A^3 + 27B^2)).
\end{aligned}$$

Tomamos de nuevo como parámetro mínimo $\beta = \alpha$, por tanto, el polinomio mínimo será $F_7(\beta) = P_7(\alpha)/3^6$, cuya norma resulta

$$\|F_7\| \leq 110725753N.$$

Caso $n = 8$. Para que una curva elíptica en forma normal de Tate tenga un punto de orden 8, su ecuación debe ser

$$\begin{aligned}
Y^2 + \left(1 - \frac{(2\alpha - 1)(\alpha - 1)}{\alpha}\right) XY - (2\alpha - 1)(\alpha - 1)Y \\
= X^3 - (2\alpha - 1)(\alpha - 1)X^2,
\end{aligned}$$

cuya forma normal de Weierstrass es

$$Y^2 = X^3 + A_8(\alpha)X + B_8(\alpha),$$

siendo

$$\begin{aligned}
A_8(\alpha) &= -27(16\alpha^8 - 64\alpha^7 + 224\alpha^6 - 448\alpha^5 + 480\alpha^4 - 288\alpha^3 \\
&\quad +96\alpha^2 - 16\alpha + 1)/\alpha^4), \text{ y} \\
B_8(\alpha) &= -54(64\alpha^12 - 384\alpha^11 + 3520\alpha^9 - 10296\alpha^8 + 15840\alpha^7 \\
&\quad -15568\alpha^6 + 10272\alpha^5 - 4560\alpha^4 + 1328\alpha^3 - 240\alpha^2 \\
&\quad +24\alpha - 1)/\alpha^6.
\end{aligned}$$

Luego, el polinomio final para $n = 8$ es

$$\begin{aligned}
P_8(\alpha) &= (A^3 \cdot B_8(\alpha)^2 - B^2 \cdot A_8(\alpha)^3)\alpha^{12} \\
&= 3^6(4096(4A^3 + 27B^2)\alpha^{24} - 49152(4A^3 + 27B^2)\alpha^{23} \\
&\quad +73728(8A^3 + 135B^2)\alpha^{22} + 180224(10A^3 - 297B^2)\alpha^{21} \\
&\quad -12288(1309A^3 + 18198B^2)\alpha^{20} + 73728(539A^3 \\
&\quad -10233B^2)\alpha^{19} - 8192(863A^3 - 255339B^2)\alpha^{18} \\
&\quad -184320(1285A^3 + 26109B^2)\alpha^{17} + 14592(57305A^3 \\
&\quad +631449B^2)\alpha^{16} - 2048(843953A^3 + 7149033B^2)\alpha^{15} \\
&\quad +3072(836909A^3 + 6256089B^2)\alpha^{14} - 18432(159859A^3 \\
&\quad +1126413B^2)\alpha^{13} + 19968(134417A^3 + 922320B^2)\alpha^{12} \\
&\quad -15360(128470A^3 + 871911B^2)\alpha^{11} + 3072(383693A^3 \\
&\quad +2593755B^2)\alpha^{10} - 13824(41416A^3 + 279639B^2)\alpha^9 \\
&\quad +48(4694132A^3 + 31686363B^2)\alpha^8 - 17820864(4A^3 \\
&\quad +27B^2)\alpha^7 + 4476576(4A^3 + 27B^2)\alpha^6 - 876864(4A^3 \\
&\quad +27B^2)\alpha^5 + 130464(4A^3 + 27B^2)\alpha^4 - 14176(4A^3 \\
&\quad +27B^2)\alpha^3 + 1056(4A^3 + 27B^2)\alpha^2 - 48(4A^3 + 27B^2)\alpha \\
&\quad +(4A^3 + 27B^2)),
\end{aligned}$$

por lo que tomamos $\beta = \alpha$ como parámetro mínimo. Así, la norma del polinomio mínimo $F_8(\beta) = P_8(\alpha)/3^6$, la podemos acotar por

$$\|F_8\| \leq 132688626943N.$$

Caso $n = 9$. En este último caso, la ecuación de la curva es

$$\begin{aligned}
y^2 + (1 - \alpha^2(\alpha - 1))XY - \alpha^2(\alpha - 1)(\alpha(\alpha - 1) + 1)Y \\
= X^3 - \alpha^2(\alpha - 1)(\alpha(\alpha - 1) + 1)X^2,
\end{aligned}$$

cuya forma normal de Weierstrass es

$$Y^2 = X^3 + A_9(\alpha)X + B_9(\alpha),$$

con

$$\begin{aligned}
A_9(\alpha) &= -27\alpha^{12} + 324\alpha^{11} - 1458\alpha^{10} + 3456\alpha^9 - 5103\alpha^8 \\
&\quad +4860\alpha^7 - 3078\alpha^6 + 972\alpha^5 + 486\alpha^4 - 756\alpha^3 \\
&\quad +324\alpha^2 - 27, \quad \text{y} \\
B_9(\alpha) &= +54\alpha^{18} - 972\alpha^{17} + 7290\alpha^{16} - 30780\alpha^{15} + 84078\alpha^{14} \\
&\quad -160380\alpha^{13} + 222912\alpha^{12} - 228420\alpha^{11} + 174960\alpha^{10} \\
&\quad -109728\alpha^9 + 73386\alpha^8 - 58320\alpha^7 + 39690\alpha^6 \\
&\quad -16524\alpha^5 + 1458\alpha^4 + 2268\alpha^3 - 972\alpha^2 + 54.
\end{aligned}$$

Luego, para $n = 9$, el polinomio final es

$$\begin{aligned}
P_9(\alpha) &= A^3 \cdot B_9(\alpha)^2 - B^2 \cdot A_9(\alpha)^3 \\
&= 3^6((4A^3 + 27B^2)\alpha^{36} - 36(4A^3 + 27B^2)\alpha^{35} \\
&\quad +594(4A^3 + 27B^2)\alpha^{34} - 6000(4A^3 + 27B^2)\alpha^{33} \\
&\quad +41859(4A^3 + 27B^2)\alpha^{32} - 215892(4A^3 + 27B^2)\alpha^{31} \\
&\quad +860466(4A^3 + 27B^2)\alpha^{30} - 2733948(4A^3 + 27B^2)\alpha^{29} \\
&\quad +7083369(4A^3 + 27B^2)\alpha^{28} - 8(7608652A^3 \\
&\quad +51352569B^2)\alpha^{27} + 54(2033212A^3 + 13708629B^2)\alpha^{26} \\
&\quad -648(259172A^3 + 1739043B^2)\alpha^{25} + 936(234956A^3 \\
&\quad +1550961B^2)\alpha^{24} - 1188(209980A^3 + 1324053B^2)\alpha^{23} \\
&\quad +162(1540372A^3 + 8673831B^2)\alpha^{22} - 36(6282620A^3 \\
&\quad +27260037B^2)\alpha^{21} + 3348(57308A^3 + 134109B^2)\alpha^{20} \\
&\quad -324(480476A^3 + 20115B^2)\alpha^{19} + 12(9996428A^3 \\
&\quad -21648735B^2)\alpha^{18} - 216(393980A^3 - 1382211B^2)\alpha^{17} \\
&\quad +243(222308A^3 - 835677B^2)\alpha^{16} - 288(106684A^3 \\
&\quad -273267B^2)\alpha^{15} + 108(151180A^3 + 44577B^2)\alpha^{14} \\
&\quad -648(13028A^3 + 50355B^2)\alpha^{13} + 9(442444A^3 \\
&\quad +2846529B^2)\alpha^{12} - 108(12196A^3 + 93987B^2)\alpha^{11} \\
&\quad +162(4A^3 + 2619B^2)\alpha^{10} + 32(10004A^3 + 66069B^2)\alpha^9 \\
&\quad -48717(4A^3 + 27B^2)\alpha^8 + 11124(4A^3 + 27B^2)\alpha^7 \\
&\quad +2262(4A^3 + 27B^2)\alpha^6 - 2124(4A^3 + 27B^2)\alpha^5 \\
&\quad +378(4A^3 + 27B^2)\alpha^4 + 84(4A^3 + 27B^2)\alpha^3 \\
&\quad -36(4A^3 + 27B^2)\alpha^2 + (4A^3 + 27B^2)).
\end{aligned}$$

Tomando como parámetro mínimo $\beta = \alpha$, se tiene el polinomio mínimo $F_9(\beta) = P_9(\alpha)/3^6$, cuya norma resulta

$$\|F_9\| \leq 11353204955N.$$

Caso $n = 10$. Como ya mencionamos, el polinomio mínimo F_{10} no es útil en la práctica, ya que, para que una curva elíptica tenga un punto de orden 10, debe tener también puntos de orden 2 y 5. Por tanto, aunque el polinomio F_{10} es algo menos incómodo que Ψ_{10}, tampoco lo usaremos para averiguar si la torsión de la curva forma un grupo cíclico de orden 10, sino que lo haremos estudiando F_5 y los puntos de orden 2.
Caso $n = 12$. Como en el caso anterior, el uso de F_{12} será ahora sustituido por el de F_3 y F_4.

Observación.– Comparando las cotas dadas para $\|\Psi_n\|$ y $\|F_n\|$, podemos decidir si es mejor usar un polinomio u otro para comprobar la existencia de puntos de orden n en una curva elíptica. Cuando $n = 4$, las cotas son

$88N < 56667N$, luego es mejor emplear Ψ_4. En el caso $n = 5$, para $N > 128$ resulta $89831N < 7072N^2$, por tanto, mejor usar F_5 para N a partir de 128. Si $n = 6$, tenemos $2220071N < 6966N^2$ cuando $N > 318$, luego, será mejor F_6 a partir de dicho N. Para $n = 7$, resulta $110725753N < 51453588N^4$, por tanto, mejor F_7. Cuando $n = 8$, comparamos las cotas y obtenemos $132688626943N < 40155188N^4$ si $N > 14$, luego, en este caso, es preferible F_8. Por último, para $n = 9$, la cota dada para la norma de F_9 es mejor que la de Ψ_9, por tanto, también en este caso será mejor usar el algoritmo de la forma normal de Tate. En general, tal y como muestran las tablas del apéndice A.3., el hecho de que las cotas de los polinomios finales sean lineales en N, en lugar de cuadráticas (o algo peor), tiene un importante impacto en los tiempos de cálculo, tanto más notable cuanto mayores son los coeficientes.

Ejemplo.– Veamos, para terminar la sección, cómo sería el cálculo de la torsión racional de la curva de los ejemplos anteriores con este último algoritmo. Dada

$$E : Y^2 = X^3 + 5589X + 342630,$$

ya sabemos que $\mathrm{Tor}(E(\mathbb{Q}))$ es cíclico de orden par y divisor de $C = 4$. También teníamos el punto $(-45, 0)$ de orden 2.

Para comprobar si hay puntos de orden 4, buscamos soluciones racionales de la ecuación $F_4(\beta) = 0$, es decir, de

$$\begin{aligned} 0 \;=\; & 3868006162176\beta^6 + 59475243789324\beta^5 \\ & +1377594811252557\beta^4 + 3007890835183188\beta^3 \\ & -1963280447441730\beta^2 + 351030857309208\beta \\ & -16802814028419, \end{aligned}$$

que factorizada queda

$$0 = 1162261467(13\beta - 1)(\beta + 3)(256\beta^4 + 3188\beta^3 + 81915\beta^2 - 39634\beta + 4819).$$

Si tomamos la solución $\beta_0 = -3$, tendremos $\alpha_0 = (\beta_0 - 1)/12 = -1/3$, luego el sistema

$$u^4 = \frac{5589}{A_4(\alpha_0)}, \qquad u^6 = \frac{342630}{B_4(\alpha_0)},$$

resulta

$$u^4 = \frac{5589}{69}, \qquad u^6 = \frac{342630}{470},$$

que tiene la solución racional $u = 3$. Por tanto, en nuestra curva hay puntos racionales de orden 4.

Para conocer las coordenadas de dichos puntos, habrá que deshacer, como en el otro ejemplo de esta sección, los cambios realizados para pasar de la

forma normal de Tate, donde el punto $(0,0)$ es de orden 4, a la forma normal de Weierstrass.

Por una parte, en la ecuación

$$Y^2 + XY + \frac{1}{3}Y = X^3 + \frac{1}{3}X^2,$$

el cambio

$$Y \longmapsto Y - \frac{3X+1}{6},$$

produce la ecuación

$$Y^2 = X^3 + \frac{7}{12}X^2 + \frac{1}{6}X + \frac{1}{36},$$

de donde, haciendo el cambio

$$X \longmapsto X - \frac{7}{36},$$

se obtiene

$$Y^2 = X^3 + \frac{23}{432}X - \frac{235}{23328},$$

y haciendo, en esta ecuación, un último cambio

$$Y \longmapsto \frac{1}{5832}Y, \quad X \longmapsto \frac{1}{324}X,$$

se obtiene

$$Y^2 = X^3 + 5589X + 342630.$$

Por otra parte, aplicando estos cambios al punto $(0,0)$ de la curva en forma normal de Tate, tenemos

$$(0,0) \longmapsto \left(0, \frac{1}{6}\right) \longmapsto \left(\frac{7}{36}, \frac{1}{6}\right) \longmapsto (63, 972).$$

Por tanto, nuestra curva E tiene el punto $P = (63, 972)$ de orden 4, luego $\mathrm{Tor}(E(\mathbb{Q}))$ es el grupo cíclico de orden 4 generado por P, es decir,

$$\{\mathcal{O},\ P = (63, 972),\ 2P = (-45, 0),\ -P = (63, -972)\}.$$

III. Caracterización de la torsión racional mediante ecuaciones diofánticas

Este capítulo contiene tres partes claramente diferenciadas. La primera de ellas, donde recogemos los procedimentos seguidos por Ono [28] para describir las curvas elípticas cuyo grupo de torsión es no cíclico, ocupa la primera sección. Los resultados de Qiu y Zhang [31] que describen las curvas que tienen grupo de torsión cíclico de orden par, forman la segunda parte que comprende la segunda sección del capítulo. Las únicas curvas elípticas que quedaban hasta hoy por caracterizar a través de ecuaciones diofánticas, son aquéllas cuya torsión es un grupo cíclico de orden impar, (i.e. orden 3, 5, 7 ó 9), y eso es precisamente lo que haremos en la tercera parte de este capítulo, formada por sus cuatro últimas secciones, donde se recogen resultados originales aportados en esta tesis.

III.A. Torsión racional no cíclica

A partir de ahora, $\mathbb{K}^2$ denota el conjunto de elementos del cuerpo $\mathbb{K}$ que tienen raíz cuadrada en dicho cuerpo.

Sea E una curva elíptica racional cuya parte afín viene dada por la ecuación

$$Y^2 = f(X) = X^3 + a_2X^2 + a_4X + a_6, \quad \text{con } a_2, a_4, a_6 \in \mathbb{Q},$$

tal que $f(X)$ tenga tres raíces racionales. Por el teorema de Mazur, el grupo de torsión racional de E será $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}$ con $1 \leq k \leq 4$.

Antes de estudiar el grupo $\mathrm{Tor}(E(\mathbb{Q}))$, daremos un proposición que también usaremos en la próxima sección.

Proposición.– Sea E una curva elíptica definida sobre $\mathbb{K}$, cuya parte afín verifica la ecuación

$$Y^2 = f(X) = (X - \alpha)(X - \beta)(X - \gamma),$$

siendo α, β y γ elementos de $\mathbb{K}$.

Sea $P = (x_0, y_0) \in E(\mathbb{K})$ un punto de la curva con coordenadas en $\mathbb{K}$. Entonces,

$$\exists Q = (x_1, y_1) \in E(\mathbb{K}) \mid 2Q = P \iff x_0 - \alpha,\ x_0 - \beta,\ x_0 - \gamma \in \mathbb{K}^2.$$

La demostración de esta proposición se puede encontrar en [16].

Como suponemos que $f(X)$ tiene tres raíces racionales, es decir, que la curva tiene tres puntos racionales de orden dos, podemos hacer un cambio de coordenadas para que las raíces de $f(X)$ sean 0, $-M$ y $-N$; siendo $M, N \in \mathbb{Z}\setminus\{0\}$, con $M \neq N$. Los puntos de orden 2 de la curva serán entonces $(0,0)$, $(-M,0)$ y $(-N,0)$, y de este modo, la ecuación de E sería

$$Y^2 = X^3 + (M+N)X^2 + MNX.$$

En el caso que nos ocupa, el enunciado de la proposición anterior queda de la siguiente manera:

Proposición.– Sea E una curva elíptica sobre $\mathbb{Q}$, cuya parte afín verifica la ecuación

$$Y^2 = f(X) = X(X + M)(X + N),$$

siendo $M, N \in \mathbb{Z} \setminus \{0\}$, y sea $P = (x', y') \in E(\mathbb{Q})$. Entonces,

$$\exists Q = (x, y) \in E(\mathbb{Q}) \mid 2Q = P \iff x',\ x' + M \text{ y } x' + N \in \mathbb{Q}^2.$$

Observación.– En el caso de nuestra curva, para un punto $Q = (x, y)$, la fórmula de duplicación viene dada por

$$x(2Q) = \frac{x^4 - 2MNx^2 + M^2N^2}{4y^2} = \left(\frac{x^2 - MN}{2y}\right)^2.$$

El siguiente resultado da el subgrupo de torsión del grupo de puntos racionales de la curva E, y es debido a Ono [28].

Teorema.– Dada una curva elíptica E sobre $\mathbb{Q}$, cuya parte afín verifica la ecuación

$$Y^2 = f(X) = X(X+M)(X+N),$$

siendo $M, N \in \mathbb{Z} \setminus \{0\}$, el grupo $\mathrm{Tor}(E(\mathbb{Q}))$ está unívocamente determinado por las siguientes condiciones:

(i) $\mathrm{Tor}(E(\mathbb{Q})) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ si M y N son ambos cuadrados, o bien $-M$ y $N-M$ son ambos cuadrados, o bien $-N$ y $M-N$ son ambos cuadrados.

(ii) $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ si existe $d \in \mathbb{Z} \setminus \{0\}$ tal que $M = d^2u^4$ y $N = d^2v^4$, o bien $M = -d^2v^4$ y $N = d^2(u^4 - v^4)$, o bien $N = -d^2v^4$ y $M = d^2(u^4 - v^4)$; donde (u, v, w) es una terna pitagórica, es decir $u^2 + v^2 = w^2$.

(iii) $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ si existen $a, b \in \mathbb{Z}$ tales que a/b no está en $\{-2, -1, -1/2, 0, 1\}$, $M = a^4 + 2a^3b$ y $N = 2ab^3 + b^4$.

(iv) $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, en otro caso.

Demostración.– Sabemos que $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset \mathrm{Tor}(E(\mathbb{Q}))$, porque en $E(\mathbb{Q})$ hay tres puntos de orden dos: $(0,0)$, $(-M,0)$ y $(-N,0)$. Luego $\mathrm{Tor}(E(\mathbb{Q}))$ no puede ser cíclico, ya que en $\mathbb{Z}/n\mathbb{Z}$ hay sólo un punto de orden dos si n es par y ninguno si n es impar.

Probaremos el teorema buscando en la curva puntos de orden 4, 8 y 3.

Tenemos dos posibilidades: que $\mathrm{Tor}(E(\mathbb{Q}))$ contenga a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, o que no lo contenga.

El primer caso se da si tenemos algún elemento de orden 4 en $\mathrm{Tor}(E(\mathbb{Q}))$. Pero si $Q = (x, y)$ es de orden 4, entonces $2Q = (x', y')$ es de orden 2, es decir, $2Q = (x', y')$ será uno de los tres puntos siguientes: $(0,0)$, $(-M,0)$ ó $(-N,0)$. Por la proposición anterior, cada uno de estos casos se traduce en una condición sobre los coeficientes de nuestra curva. Veamos esas tres posibilidades:

- Si $2Q = (0,0)$, resulta $x' = 0$ y, por la proposición, serán 0, M y N cuadrados de números racionales. Así tendremos

$$M = m^2 \quad \text{y} \quad N = n^2 \quad \text{con} \quad m, n \in \mathbb{Z}^+,$$

entonces

$$0 = x' = x(2Q) = \left(\frac{x^2 - m^2n^2}{2y}\right)^2 \Leftrightarrow x^2 - m^2n^2 = 0 \Leftrightarrow x = \pm mn.$$

Despejamos y en la ecuación de la curva y queda:

$$\begin{aligned} y &= \pm\sqrt{(\pm mn)^3 + (m^2+n^2)(mn)^2 \pm m^2n^2mn} \\ &= \pm mn(m \pm n). \end{aligned}$$

Por tanto, tenemos dos puntos de orden 4 para cada una de la dos posibilidades de x:

$$Q = (x,y) = (mn,\ \pm mn(m+n)) \quad \text{ó} \quad (-mn,\ \pm mn(m-n)).$$

- Si $2Q = (-M, 0)$, resulta $x' = -M$. Ahora, por la proposición, serán $-M$, 0 y $-M + N$ cuadrados de números racionales. Así tendremos

$$-M = m^2 \quad \text{y} \quad N - M = k^2 \quad \text{con} \quad m, k \in \mathbb{Z}^+,$$

luego

$$\begin{aligned} m^2 &= -M = x' = x(2Q) = \left(\frac{x^2 - (-m^2)(k^2 - m^2)}{2y}\right)^2 \\ &= \left(\frac{x^2 + m^2(k^2 - m^2)}{2y}\right)^2. \end{aligned}$$

De esto se deduce que

$$y = \pm\frac{x^2 + m^2(k^2 - m^2)}{2m},$$

y si sustituimos ahora y en la ecuación de la curva, despejando x, obtenemos dos puntos de orden 4 para cada x:

$$Q = (x,y) = (m^2 - mk,\ \pm k(m^2 - mk)) \quad \text{ó} \quad (m^2 + mk,\ \pm k(m^2 + mk)).$$

- Si $2Q = (-N, 0)$, resulta $x' = -N$, luego, por la proposición se tiene que $-N$, $-N + M$ y 0 son cuadrados de números racionales. Así tendremos

$$-N = m^2 \quad \text{y} \quad M - N = k^2 \quad \text{con} \quad m, k \in \mathbb{Z}^+.$$

Se procede como en el caso anterior y se obtienen también los puntos de orden 4

$$Q = (x, y) = (m^2 - mk,\ \pm k(m^2 - mk)) \quad \text{ó} \quad (m^2 + mk,\ \pm k(m^2 + mk)).$$

Seguimos en el caso en que $\text{Tor}(E(\mathbb{Q}))$ contiene a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, pero nos planteamos ahora si hay algún elemento de orden 8, es decir, si $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Si no, tendríamos $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Si Q es un punto de orden 8, $2Q$ es uno de los puntos de orden 4 hallados anteriormente. Así tendremos tres posibilidades:

- Si $M = m^2$ y $N = n^2$ con $m, n \in \mathbb{Z}^+$.

Tenemos $x' = x(2Q) = mn$, y por la proposición sabemos que existe Q tal que $2Q$ es un punto de la curva si y sólo si

$$x' = mn,\ x' + M = mn + m^2 \quad \text{y} \quad x' + N = mn + n^2$$

son cuadrados perfectos.

Por la forma de nuestra ecuación, podemos suponer que $\text{mcd}(M, N)$ es libre de cuadrados (ya que si d^2 divide al $\text{mcd}(M, N)$, basta hacer el cambio $X \longmapsto d^2X$, $Y \longmapsto d^3Y$), por tanto, podemos suponer que $\text{mcd}(m, n) = 1$.

Así, decir que mn es un cuadrado equivale a decir que m y n son cuadrados: $m = u^2$ y $n = v^2$, con $u, v \in \mathbb{Z}$. Luego, sabemos que

$$u^2v^2,\ u^2v^2 + u^4 \quad \text{y} \quad u^2v^2 + v^4$$

son cuadrados, y esto ocurre cuando $u^2 + v^2$ es un cuadrado. Es decir, cuando $u^2 + v^2 = w^2$ para cierto $w \in \mathbb{Z}$, o lo que es lo mismo, cuando (u, v, w) sea una terna pitagórica.

En resumen, si M y N son cuadrados y $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, entonces $M = d^2u^4$ y $N = d^2v^4$ donde (u, v, w) es una terna pitagórica y d es un entero no nulo.

- Si $-M = m^2$ y $N - M = k^2$ con $m, k \in \mathbb{Z}^+$.

  Tenemos $x' = x(2Q) = m^2 + mk$, (si es preciso se elige el signo de m y k para que aquí salga $m^2 + mk$). Por la proposición, sabemos que existe $Q \in E(\mathbb{Q})$ tal que $2Q$ es un punto de la curva si y sólo si

  $$x' = m^2 + mk, \quad x' + M = mk \quad \text{y} \quad x' + N = mk + k^2$$

  son cuadrados perfectos.

  Por la forma de nuestra ecuación, ya sabemos que podemos suponer $\text{mcd}(M, N)$ libre de cuadrados, por tanto podemos suponer que $\text{mcd}(m, k) = 1$. Así, decir que mk es un cuadrado equivale a decir que m y k son cuadrados: $m = v^2$ y $k = u^2$, con $u, v \in \mathbb{Z}$. Luego, sabemos que

  $$v^4 + v^2u^2, \; u^2v^2 \quad \text{y} \quad u^2v^2 + u^4$$

  son cuadrados, y esto ocurre cuando $u^2 + v^2$ es un cuadrado, es decir, cuando $u^2 + v^2 = w^2$ para cierto $w \in \mathbb{Z}$. Por tanto, será también ahora (u, v, w) una terna pitagórica.

  En resumen, si $-M$ y $N - M$ son cuadrados y $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, entonces $M = -d^2v^4$ y $N = d^2(u^4 - v^4)$, donde (u, v, w) es una terna pitagórica y d es un entero no nulo.

- Si $-N = n^2$ y $M - N = k^2$ con $n, k \in \mathbb{Z}^+$.

  Este caso es análogo al anterior.

Finalizado el primer caso, estudiamos ahora qué ocurre cuando $\text{Tor}(E(\mathbb{Q}))$ no contiene a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Tenemos otras dos posibilidades: si en la curva hay puntos racionales de orden 3, será $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, y si no, sólo queda la opción $\text{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Como vimos en I.D., un punto $Q = (x, y) \in E(\mathbb{Q})$ es de orden 3 si y sólo si x es raíz de la ecuación

$$\Psi_3(x) = 3x^4 + 4(M + N)x^3 + 6MNx^2 - M^2N^2 = 0,$$

que es homogénea de grado 4 en M, N y x. Luego, podemos parametrizar (siguiendo a [28]):

$$\frac{M}{x} = (1 + t)^2 - 1 \; , \quad \frac{N}{x} = \left(1 + \frac{1}{t}\right)^2 - 1.$$

Si sustituimos t por a/b con $\mathrm{mcd}(a,b)=1$, resulta:

$$\frac{M}{x}=\frac{2ab+a^2}{b^2}\ ,\quad \frac{N}{x}=\frac{2ab+b^2}{a^2}.$$

Por Nagell-Lutz, como $Q=(x,y)$ es un punto de orden finito, se tiene que $x\in\mathbb{Z}$, pero de

$$x=\frac{M}{2ab+a^2}b^2=\frac{N}{2ab+b^2}a^2\ \in\mathbb{Z},$$

se deduce que

$$\frac{M}{2ab+a^2}=ka^2\ ,\quad \frac{N}{2ab+b^2}=kb^2.$$

Luego, podemos tomar $x=a^2b^2$. Por tanto:

$$M=2a^3b+a^4\ ,\quad N=2ab^3+b^4.$$

Veamos que a/b no puede estar en el conjunto $\{-2,-1,-1/2,0,1\}$:

- Si $a/b=-2$, entonces $M/x=0$. Así sería $M=0$, y esto es imposible porque las tres raíces de $f(x)$ eran distintas en nuestra curva elíptica.
- Si $a/b=-1$, entonces $M/x=-1=N/x$, luego $M=N$, lo que contradice la hipótesis de que M y N fueran distintos.
- Si $a/b=-1/2$, entonces $N=0$, y tampoco nos sirve.
- Si $a/b=0$, entonces $M=0$ y eso no era posible.
- Si $a/b=1$, $M=N=3$, pero M y N tenían que ser distintos.

Resolviendo ahora

$$y^2\ =\ x^3\ +\ (2a^3b+a^4+2ab^3+b^4)x^2\ +\ (2a^3b+a^4)(2ab^3+b^4)x$$

para $x=a^2b^2$ queda:

$$\begin{aligned} y^2 &= a^6b^6+(2a^3b+a^4+2ab^3+b^4)(a^2b^2)^2+(2a^3b+a^4)(2ab^3+b^4)a^2b^2\\ &= a^4b^4(a+b)^4. \end{aligned}$$

Luego, $y=\pm\ a^2b^2(a+b)^2$.

En resumen, hemos encontrado los puntos de orden 3:

$$Q=(a^2b^2,\ \pm a^2b^2(a+b)^2),$$

cuando $M = 2a^3b + a^4$, $N = 2ab^3 + b^4$ siendo a y b enteros tales que su cociente no está en el conjunto $\{-2, -1, -1/2, 0, 1\}$.

Por tanto, si M y N verifican en estas condiciones, es $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, y en otro caso ha de ser $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Observación.– Estas caracterizaciones (y las que daremos a continuación) de puntos de torsión mediante ecuaciones diofánticas no son muy prácticas desde el punto de vista computacional (ver [36] para un estudio actualizado de las técnicas de resolución de ecuaciones de este tipo). Sin embargo, en el estudio de la torsión sobre extensiones algebraicas de $\mathbb{Q}$ han demostrado su utilidad para describir explícitamente grupos de torsión. En esta línea se inscriben trabajos como [19, 12, 13], que se basan en este teorema de forma fundamental.

III.B. Torsión racional cíclica de orden par

Ses E una curva elíptica racional cuya parte afín viene dada por la ecuación

$$Y^2 = f(X) = X^3 + a_2X^2 + a_4X + a_6, \quad \text{con } a_2, a_4, a_6 \in \mathbb{Q},$$

tal que $f(X)$ sólo tenga una raíz racional. Es decir, estamos en el caso en que la curva tiene sólo un punto racional de orden 2.

Qiu y Zhang [31, 32], siguiendo los razonamientos de Ono, han dado una caracterización notablemente menos elegante para este caso en el que el grupo de torsión racional es cíclico de orden par. Según Mazur, sabemos que las posibilidades para $\mathrm{Tor}(E(\mathbb{Q}))$ son $\mathbb{Z}/2k\mathbb{Z}$ con $1 \leq k \leq 6$.

Podemos hacer un cambio de coordenadas, para que la única raíz racional de $f(X)$ sea $X = 0$. Entonces, la ecuación de la curva es:

$$Y^2 = f(X) = X(X - \alpha)(X - \beta),$$

con $\alpha, \beta \notin \mathbb{Q}$. Como $\alpha + \beta$ y $\alpha\beta$ son racionales (por Cardano), se tiene que:

$$\exists q_1, q_2 \in \mathbb{Q} \mid \alpha + \beta = q_1, \ \alpha\beta = q_2.$$

Así, $\alpha = q_1 - \beta$, y sustituyendo en la otra relación resulta:

$$(q_1 - \beta)\beta = q_2,$$

de donde se tiene

$$\beta^2 - q_1\beta + q_2 = 0,$$

por tanto,

$$\beta = \frac{q_1 \pm \sqrt{q_1^2 - 4q_2}}{2}, \quad \alpha = \frac{q_1 \mp \sqrt{q_1^2 - 4q_2}}{2}.$$

Es decir, encontramos tres números racionales m, n y D, tales que $n \neq 0$ y D es libre de cuadrados, sin pérdida de generalidad, verificando:

$$\alpha = m + n\sqrt{D}, \quad \beta = m - n\sqrt{D}.$$

Además, podemos suponer que m y n son enteros tales que $\mathrm{mcd}(m, n)$ es libre de cuadrados, ya que

$$\begin{aligned} f(X) &= X(X-\alpha)(X-\beta) \\ &= X(X^2 - (\alpha+\beta)X + \alpha\beta) \\ &= X(X^2 - 2mX + m^2 - n^2 D), \end{aligned}$$

y si $m = m'd^2$, $n = n'd^2$, con $\mathrm{mcd}(m', n')$ libre de cuadrados, haciendo el cambio

$$Y \longmapsto d^3 Y, \quad X \longmapsto d^2 X,$$

resulta

$$(d^3Y)^2 = d^2X(d^4X^2 - 2m'd^2d^2X + m'^2d^4 - n'^2d^4D),$$

donde simplificando queda

$$Y^2 = X(X^2 - 2m'X + m'^2 - n'^2 D),$$

con $\mathrm{mcd}(m', n')$ libre de cuadrados.

Como la ecuación de partida y ésta última representan curvas cuyos grupos de puntos racionales son isomorfos, sus subgrupos de torsión también lo serán. Así, queda probado que podemos suponer que partimos de una curva cuya ecuación es de la forma:

$$Y^2 = X(X-\alpha)(X-\beta),$$

con $\alpha = m + n\sqrt{D}$, $\beta = m - n\sqrt{D}$, siendo $m, n, D \in \mathbb{Z}$ tales que $n \neq 0$ y con D y $\mathrm{mcd}(m, n)$ libres de cuadrados.

El enunciado de la proposición dada en la sección anterior sería ahora:

Proposición.– Sea $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ y E una curva elíptica cuya parte afín verifica la ecuación

$$Y^2 = f(X) = X(X+M)(X+N),$$

donde $M = m + n\sqrt{D}$ y $N = m - n\sqrt{D}$, siendo $m, n, D \in \mathbb{Z}$, con $n \neq 0$, $D \neq 1$ y tales que $\mathrm{mcd}(m, n)$ y D son libres de cuadrados.

Sea $P = (x', y') \in E(\mathbb{K})$, entonces

$$\exists Q = (x, y) \in E(\mathbb{K}) \mid 2Q = P \iff x',\ x' + M \text{ y } x' + N \in \mathbb{K}^2.$$

El siguiente teorema da el subgrupo de torsión de una curva elíptica en el caso que nos ocupa en esta sección.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

$$Y^2 = f(X) = X(X+M)(X+N),$$

donde $M = m + n\sqrt{D}$, $N = m - n\sqrt{D}$ siendo $m, n, D \in \mathbb{Z}$, con $n \neq 0$, $D \neq 1$ y tales que $\mathrm{mcd}(m, n)$ y D son libres de cuadrados.

Entonces $\mathrm{Tor}(E(\mathbb{Q}))$ verifica:

(i)

1. $\mathrm{Tor}(E(\mathbb{Q})) \supset \mathbb{Z}/4\mathbb{Z}$ si y sólo si

$$m = a^2 + b^2 D, \quad n = 2ab,$$

con $a, b \in \mathbb{Z} \setminus \{0\}$ y primos entre sí.

2. $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/8\mathbb{Z}$ si y sólo si

$$m = u^4 + v^2 w^2 D, \quad n = 2u^2 vw, \quad 2u^2 - v^2 = w^2 D,$$

con $u, v, w \in \mathbb{Z} \setminus \{0\}$.

3. $\mathrm{Tor}(E(\mathbb{Q})) \supset \mathbb{Z}/6\mathbb{Z}$ si y sólo si

$$m = a^2 + 2ac + b^2 D, \quad n = 2b(a+c), \quad a^2 - b^2 D = c^2,$$

con $a, b, c \in \mathbb{Z} \setminus \{0\}$ y primos entre sí.

4. $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/12\mathbb{Z}$ si y sólo si

$$m = v^2 - u^2 + w^2 D, \quad n = 2vw,$$

$$3(v^2 - w^2 D)^4 - 4u^2(v^2 - w^2 D)^2(v^2 + w^2 D) - 16u^4 v^2 w^2 D = 0,$$

con $u, v, w \in \mathbb{Z} \setminus \{0\}$.

5. $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/10\mathbb{Z}$ si y sólo si

$$m = 2s(s+u) - v^2, \quad n = 2st,$$

$$(s+u)^2 - v^2 = t^2 D, \quad (u-v)^2(u+v) = 4uvs,$$

con $u, v, s, t \in \mathbb{Z} \setminus \{0\}$.

6. $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z}$ en cualquier otro caso.

(ii) Denotemos P_n a un generador del subgrupo $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/n\mathbb{Z}$ de orden n. Entonces, en cada uno de los casos del apartado (i), las primeras coordenadas de P_n y de $2P_n$, verifican:

1. $x(P_4) = a^2 - b^2 D; \quad x(2P_4) = 0.$
2. $x(P_8) = (u+v)(u-v)^3; \quad x(2P_8) = (u^2 - v^2)^2.$
3. $x(P_6) = 5c^2 + 4ac; \quad x(2P_6) = c^2.$
4. $x(P_{12}) = (u+v)^2 - w^2 D; \quad x(2P_{12}) = u^2.$
5. $x(P_{10}) = 2v^2 + 4vs - u^2; \quad x(2P_{10}) = u^2.$
6. $x(P_2) = 0.$

Demostración.– Probaremos los apartados (i) y (ii) conjuntamente, distinguiendo los seis casos del enunciado.

Por el teorema de Nagell-Lutz, sabemos que los puntos de torsión de coordenadas racionales tienen en realidad coordenadas enteras. Es decir, si $P \in \mathrm{Tor}(E(\mathbb{Q})) \subset E_{\mathbb{Q}}$ entonces $x(P),\ y(P) \in \mathbb{Z}$.

Con la ecuación de nuestra curva, la fórmula de duplicación resulta:

$$\begin{aligned} x(2P) &= \frac{x(P)^4 - 2MNx(P)^2 + (MN)^2}{4f(x(P))} \\ &= \left(\frac{x(P)^2 - MN}{2\,y(P)}\right)^2. \end{aligned}$$

1. Si $\mathrm{Tor}(E(\mathbb{Q})) \supset \mathbb{Z}/4\mathbb{Z}$, entonces la curva tiene un punto P de orden 4. Por tanto, $2P = (x_0, y_0)$ será el único punto de orden 2 que tiene la curva, es decir, $2P = (0,0)$.

   Como las raíces de $f(X)$ son ahora 0, $\alpha = -M = -(m + n\sqrt{D})$ y $\beta = -N = -(m - n\sqrt{D})$, por la proposición, se tiene que 0, M, $N \in \mathbb{K}^2$. Por tanto, M y N son cuadrados de elementos de $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, aunque en realidad, podemos decir que M y N son cuadrados de elementos de $\mathbb{Z}[\sqrt{D}]$. Es decir,

$$M = (a + b\sqrt{D})^2, \quad N = (a - b\sqrt{D})^2 \quad \text{con} \quad a, b \in \mathbb{Z}.$$

   Como eran $M = m + n\sqrt{D}$ y $N = m - n\sqrt{D}$, tenemos

$$m = \frac{M+N}{2} = \frac{(a+b\sqrt{D})^2 + (a-b\sqrt{D})^2}{2} = a^2 + b^2 D,$$

$$n = \frac{M-N}{2\sqrt{D}} = \frac{(a+b\sqrt{D})^2 - (a-b\sqrt{D})^2}{2\sqrt{D}} = 2ab,$$

   siendo $\mathrm{mcd}(a,b) = 1$, por ser $\mathrm{mcd}(m,n)$ libre de cuadrados, y además $ab \neq 0$ por ser $n \neq 0$.

   Recíprocamente, si m y n verifican las condiciones del primer apartado, entonces:

$$M = m + n\sqrt{D} = a^2 + b^2 D + 2ab\sqrt{D} = (a + b\sqrt{D})^2 \in \mathbb{K}^2,$$

$$N = m - n\sqrt{D} = a^2 + b^2 D - 2ab\sqrt{D} = (a - b\sqrt{D})^2 \in \mathbb{K}^2.$$

   Por la proposición, dado $(x_0, y_0) = (0,0) \in E(\mathbb{K})$, como 0, M, $N \in \mathbb{K}^2$, existe un punto $P \in E(\mathbb{K})$ tal que $2P = (x_0, y_0) = (0,0)$.

   Por la fórmula de duplicación, se tiene:

$$\left(\frac{x(P)^2 - MN}{2y(P)}\right)^2 = 0,$$

   es decir:

$$x(P)^2 = MN = (a + b\sqrt{D})^2(a - b\sqrt{D})^2 = (a^2 - b^2 D)^2.$$

   Así, tenemos un punto $P \in E(\mathbb{K})$ tal que

$$x(P) = \pm(a^2 - b^2 D).$$

Sustituyendo ahora en la ecuación de la curva x por $-(a^2-b^2D)$, no se obtiene solución para y, pero sustituyendo x por (a^2-b^2D), se obtiene

$$\begin{aligned} y(P) &= \pm\sqrt{(a^2-b^2D)^3+2(a^2+b^2D)(a^2-b^2D)^2+(a^2-b^2D)^3} \\ &= \pm 2a(a^2-b^2D). \end{aligned}$$

Por tanto, tenemos dos puntos de orden 4 en $E(\mathbb{K})$ con coordenadas enteras, es decir, tenemos dos puntos de orden 4 en $\mathrm{Tor}(E(\mathbb{Q}))$:

$$(a^2-b^2D, 2a(a^2-b^2D)) \quad \text{y} \quad (a^2-b^2D, -2a(a^2-b^2D)).$$

De esto se deduce que $\mathrm{Tor}(E(\mathbb{Q})) \supset \mathbb{Z}/4\mathbb{Z}$ como se decía en (i), y además

$$x(P_4) = a^2-b^2D \quad \text{y} \quad x(2P_4) = 0,$$

como se decía en (ii).

2. Supongamos que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/8\mathbb{Z}$. Sea P un punto racional de orden 8 en la curva. Así, $2P$ es de orden 4, y por el apartado anterior se tendrá:

$$m = a^2+b^2D, \quad n = 2ab \quad \text{y} \quad x(2P) = a^2-b^2D.$$

Entonces, por la proposición, sabemos que

$$\begin{aligned} x(2P) &= a^2-b^2D, \\ x(2P)+M &= 2a^2+2ab\sqrt{D}, \\ x(2P)+N &= 2a^2-2ab\sqrt{D}, \end{aligned}$$

están en $\mathbb{K}^2$. Ahora, por la fórmula de duplicación y por ser $x(P)$, $y(P)$, $x(2P)$, MN, a y b números enteros, tenemos

$$x(2P) = a^2-b^2D = c^2 \quad \text{y} \quad 2a^2+2ab\sqrt{D} = (s+t\sqrt{D})^2,$$

siendo $c, s, t \in \mathbb{Z}$. A partir de esto, se deduce que

$$2a^2+2ab\sqrt{D} = s^2+t^2D+2st\sqrt{D},$$

por tanto, será $2a^2 = s^2+t^2D$, y como $2a^2 = a(a+c)+a(a-c)$, podemos tomar

$$s^2 = a(a+c), \quad t^2D = a(a-c).$$

Como $\mathrm{mcd}(a,b) = 1$ y D es libre de cuadrados, al ser $a^2-b^2D = c^2$, se tiene $\mathrm{mcd}(a,c) = 1$ por tanto, $\mathrm{mcd}(a, a+c) = 1$, y como $s^2 = a(a+c)$,

$$\exists u, v \in \mathbb{Z} \mid a = u^2, \quad a+c = v^2, \quad \mathrm{mcd}(u,v) = 1.$$

Además, por ser D libre de cuadrados, y $t^2D = a(a-c)$, se tiene que

$$\exists w \in \mathbb{Z} \ / \ 2u^2 - v^2 = w^2D.$$

Ahora veamos que $a^2 - (vw)^2D = c^2$, y como era $a^2 - b^2D = c^2$, se tendrá que $b = vw$.

$$a^2 - (vw)^2D = a^2 - v^2w^2D = a^2 - v^2(2u^2 - v^2) = a^2 - 2u^2v^2 + v^4 =$$

$$= a^2 - 2a(a+c) + (a+c)^2 = a^2 - 2a^2 - 2ac + a^2 + 2ac + c^2 = c^2.$$

En resumen tenemos $b = vw$, por tanto,

$$m = u^4 + v^2w^2D, \quad n = 2u^2vw, \quad 2u^2 - v^2 = w^2D,$$

donde $u, v, w \in \mathbb{Z} \setminus \{0\}$.

Recíprocamente, supongamos que la curva elíptica E verifica las condiciones dadas en el segundo apartado de (i). Entonces, la curva satisface también las condiciones del primer apartado. Así, la curva tendrá un punto racional P_4 de orden 4 tal que

$$x(P_4) = a^2 - b^2D = c^2 = (u^2 - v^2)^2,$$

por ser $c + a = v^2$ y $a = u^2$.

También ahora, por darse las condiciones del primer apartado de (i), se tiene que $M = a + b\sqrt{D}$, $N = a - b\sqrt{D}$, y podemos comprobar que

$$x(P_4), \ x(P_4) + M, \ x(P_4) + N \in \mathbb{K}^2.$$

Por tanto, por la proposición, debe existir un punto P tal que $2P = P_4$. Entonces, tenemos un punto $P = (x, y)$ de orden 8 tal que

$$x(2P) = x(P_4) = (u^2 - v^2)^2.$$

Por la fórmula de duplicación

$$x(2P) = \frac{(x^2 - MN)^2}{4y^2},$$

y se tiene

$$4y^2(u^2 - v^2)^2 = (x^2 - MN)^2.$$

Como

$$M = m + n\sqrt{D} = (u^4 + v^2w^2D) + 2u^2vw\sqrt{D},$$

$$N = m - n\sqrt{D} = (u^4 + v^2w^2D) - 2u^2vw\sqrt{D},$$

resulta $MN = (u^4 + v^2w^2D)^2 - (2u^2vw\sqrt{D})^2 = (u^4 - v^2w^2D)^2$. Luego, $4y^2(u^2 - v^2)^2 = (x^2 - (u^4 - v^2w^2D)^2)^2$, y de la ecuación de la curva,

$$\begin{aligned} y^2 &= x^3 + (M+N)x^2 + MNx \\ &= x^3 + 2(u^4 + v^2w^2D)x^2 + (u^4 - v^2w^2D)^2x. \end{aligned}$$

Ahora, sustituyendo tenemos:

$$4(u^2-v^2)^2x^3+8(u^2-v^2)^2(u^4+v^2w^2D)x^2+4(u^2-v^2)^2(u^4-v^2w^2D)^2x =$$

$$x^4 - 2(u^4 - v^2w^2D)^2x^2 + (u^4 - v^2w^2D)^4,$$

y como $w^2D = 2u^2 - v^2$, resulta

$$x^4 - 4(u^2 - v^2)x^3 - 2(u^2 - v^2)^2(5u^4 + 6u^2v^2 - 3v^2)x^2$$

$$-4(u^2 - v^2)^6x + (u^2 - vr)^8 = 0.$$

Reagrupando términos queda la ecuación

$$(x - (u^2 - v^2)^2)^4 = 16u^4(u^2 - v^2)^2x^2,$$

y se puede comprobar que $x = (u+v)(v-u)^3$ es una solución entera de dicha ecuación. Además es la única. Sustituyéndola en la ecuación de la curva obtenemos también que $y \in \mathbb{Z}$.

Por tanto, hemos encontrado un punto $P_8 \in \mathrm{Tor}(E(\mathbb{Q}))$ de orden 8 tal que

$$x(P_8) = (u+v)(v-u)^3,$$

con lo que termina la demostración del segundo apartado del teorema.

3. Supongamos que $\mathrm{Tor}(E(\mathbb{Q})) \supset \mathbb{Z}/6\mathbb{Z}$. Entonces, existe un punto racional P de orden 3 en la curva. Se tiene $x(2P) = x(P) \neq 0$ y, por la fórmula de duplicación,

$$\exists u \in \mathbb{Z} \setminus \{0\} \quad | \quad x(2P) = u^2 = x(P).$$

Como ya sabemos, los puntos P de orden 3 verifican la expresión

$$3x^4 + 4(M+N)x^3 + 6MNx^2 - M^2N^2 = 0, \quad \text{con} \quad x = x(P),$$

luego, tenemos una ecuación homogénea de grado 4 en x, M y N. Según la parametrización usada en la sección anterior, se tiene

$$\frac{M}{x} = (1+t)^2 - 1, \quad \frac{N}{x} = \left(1 + \frac{1}{t}\right)^2 - 1,$$

con $t \in \mathbb{Q}(\sqrt{D}) \setminus \mathbb{Q}$. Tomamos

$$t = \frac{a + b\sqrt{D}}{c}, \quad \text{con} \quad \text{mcd}(a, b, c) = 1, \quad bc \neq 0.$$

El punto P verifica $y^2 = x(x + M)(x + N)$, por estar en la curva, pero $x \neq 0$ por ser P de orden 3 y no de orden 2. Es decir, P verifica:

$$\frac{y^2}{x^3} = \left(1 + \frac{M}{x}\right)\left(1 + \frac{N}{x}\right),$$

y por la parametrización dada, resulta

$$\frac{y^2}{x^3} = (1 + t)^2(1 + 1/t)^2 = \left(2 + t + \frac{1}{t}\right)^2.$$

Sustituimos ahora $t = (a + b\sqrt{D})/c$ y tenemos

$$\frac{y^2}{x^3} = \left(2 + \frac{a + b\sqrt{D}}{c} + \frac{c}{a + b\sqrt{D}}\right)^2,$$

y operando queda:

$$\frac{y^2}{x^3} = \left(2 + \frac{a}{c} + \frac{b\sqrt{D}}{c} + \frac{c(a - b\sqrt{D})}{a^2 - b^2D}\right)^2,$$

de donde se tiene

$$\frac{y^2}{x^3} = \left(2 + \frac{a}{c} + \frac{ac}{a^2 - b^2D} + \left(\frac{b}{c} - \frac{bc}{a^2 - b^2D}\right)\sqrt{D}\right)^2.$$

Si fuese

$$2 + \frac{a}{c} + \frac{ac}{a^2 - b^2D} = 0,$$

se tendría

$$\frac{y^2}{x^3} = \left(\frac{b}{c} - \frac{bc}{a^2 - b^2D}\right)^2 D,$$

que sería una contradicción por ser $x = u^2$ y suponer D libre de cuadrados.

Por tanto, ha de ser $2 + a/c + ac/(a^2 - b^2D) \neq 0$, y como $x, y \in \mathbb{Q}$ y se tiene

$$\begin{aligned} \frac{y^2}{x^3} &= \left(2 + \frac{a}{c} + \frac{ac}{a^2 - b^2D}\right)^2 + \left(\frac{b}{c} - \frac{bc}{a^2 - b^2D}\right)^2 D \\ &+ 2\left(2 + \frac{a}{c} + \frac{ac}{a^2 - b^2D}\right)\left(\frac{b}{c} - \frac{bc}{a^2 - b^2D}\right)\sqrt{D}, \end{aligned}$$

necesariamente será

$$\frac{b}{c} - \frac{bc}{a^2 - b^2 D} = \frac{b((a^2 - b^2 D) - c^2)}{c(a_2 - b^2 D)} = 0,$$

es decir, como $b \neq 0$, será

$$a^2 - b^2 D = c^2.$$

Por tanto,

$$\frac{1}{t} = \frac{c}{a + b\sqrt{D}} = \frac{c(a - b\sqrt{D})}{a^2 - b^2 D} = \frac{a - b\sqrt{D}}{c},$$

y se obtiene:

$$\begin{aligned} m &= \frac{M+N}{2} = \frac{x}{2}\left(\frac{M}{x} + \frac{N}{x}\right) = \frac{x}{2}\left(2t + t^2 + \frac{2}{t} + \frac{1}{t^2}\right) \\ &= x\left(\frac{a^2 + 2ac + b^2 D}{c^2}\right), \\ n &= \frac{M-N}{2\sqrt{D}} = \frac{x}{2\sqrt{D}}\left(\frac{M}{x} - \frac{N}{x}\right) = \frac{x}{2\sqrt{D}}\left(2t + t^2 - \frac{2}{t} - \frac{1}{t^2}\right) \\ &= x\left(\frac{2b(a+c)}{c^2}\right). \end{aligned}$$

Teníamos $\mathrm{mcd}(a, b, c) = 1 = \mathrm{mcd}(m, n)$, luego $\mathrm{mcd}(a^2 + 2ac + b^2 D,\ 2b(a + c),\ c^2)$ es libre de cuadrados, y ha de ser $x = c^2$. Por tanto, se tiene

$$m = a^2 + 2ac + b^2 D, \quad n = 2b(a + c), \quad a^2 - b^2 D = c^2,$$

con $\mathrm{mcd}(a, b, c) = 1$, como queríamos probar.

Supongamos ahora que la curva satisface las condiciones dadas en el tercer apartado. De ellas se obtiene un punto P_3 de orden 3 con coordenadas racionales tal que

$$x(P_3) = c^2,\ y(P_3) = \pm 2(a + c)c^2.$$

Veámoslo. Teniendo en cuenta que $c^2 = a^2 - b^2 D$, es

$$\begin{aligned} MN &= m^2 - n^2 D = (a^2 + 2ac + b^2 D)^2 - 4b^2(a + c)^2 D \\ &= 5c^2 + 4ac^3. \end{aligned}$$

Basta ahora sustituir $x = c^2$, $y = 2c^2|a+c|$ y $MN = 5c^4 + 4ac^3$ en la expresión

$$x = \left(\frac{x^2 - MN}{2y}\right)^2,$$

y comprobar que se verifica. Esto equivale a decir que $x(P_3) = x(2P_3)$, o lo que es lo mismo, que P_3 es un punto racional de orden 3.

Así, como $P_2 = (0,0)$ es un punto de orden 2, se tiene que $P_6 = P_3 + P_2$ será un punto racional de orden 6, y por las fórmulas dadas para la ley interna de la curva, se tiene:

$$\begin{aligned} x(P_6) &= \left(\frac{2c^2|a+c| - 0}{c^2 - 0}\right)^2 - (M+N) - 0 - c^2 \\ &= 5c^2 + 4ac. \end{aligned}$$

Esto finaliza la prueba del tercer apartado.

4. Supongamos que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/12\mathbb{Z}$. Entonces, la curva tiene un punto P de orden 12. Así, $2P$ tiene orden 6. Por el tercer apartado se tendrá $x(2P) = 5c^2 + 4ac$, y además serán

$$m = a^2 + 2ac + b^2D, \quad n = 2b(a+c), \quad a^2 - b^2D = c^2,$$

con $a, b, c \in \mathbb{Z} \setminus \{0\}$ y $\mathrm{mcd}(a,b,c) = 1$.

Sabemos ahora que

$$M = m + n\sqrt{D} = (a + c + b\sqrt{D})^2 - c^2,$$

$$N = m - n\sqrt{D} = (a + c - b\sqrt{D})^2 - c^2,$$

y por la proposición,

$$\begin{aligned} x(2P) &= 5c^2 + 4ac, \\ x(2P) + M &= 4c(a+c) + (a + c + b\sqrt{D})^2, \\ x(2P) + N &= 4c(a+c) + (a + c - b\sqrt{D})^2 \end{aligned}$$

están en $\mathbb{K}^2$. Pero, por la fórmula de duplicación

$$x(2P) = \left(\frac{x(P)^2 - MN}{2y(P)}\right)^2 \in \mathbb{Q},$$

por tanto,

$$x(2P) = 5c^2 + 4ac = u^2, \quad 4c(a+c) + (a + c + b\sqrt{D})^2 = (v + w\sqrt{D})^2,$$

con $u, v, w \in \mathbb{Z}$. Es decir,

$$4c(a+c) + (a+c)^2 + b^2D = v^2 + w^2D, \quad (a+c)b = vw,$$

siendo a, b, c como en el tercer apartado y $u, v, w \in \mathbb{Z} \setminus \{0\}$.

A partir de las expresiones que acabamos de obtener, se puede escribir

$$m = a^2 + 2ac + b^2D = v^2 - u^2 + w^2D,$$

$$n = 2ab(a+c) = 2vw,$$

y además, se puede comprobar que u, v y w verifican la siguiente relación:

$$3(v^2 - w^2D)^4 - 4u^2(v^2 - w^2D)^2(v^2 + w^2D) - 16u^4v^2w^2D = 0.$$

Recíprocamente, supongamos que la curva E satisface las condiciones del cuarto apartado. Entonces, también tendrá las condiciones del tercer apartado, es decir, la curva tiene un punto racional P_6 de orden 6 con $x(P_6) = 5c^2 + 4ac = u^2$.

Mediante un procedimiento similar al usado en la demostración del segundo apartado, podemos llegar ahora a que la curva tiene un punto P de orden 12. La primera coordenada de dicho punto $x = x(P)$ satisface la ecuación

$$x^4 - 4u^2x^3 - hx^2 - 4u^2ex + e^2 = 0,$$

donde

$$h = 2((v^2 - w^2D)^2 + 2u^2(v^2 + w^2D) - 3u^4),$$
$$e = (v^2 - w^2D)^2 + u^4 - 2u^2(v^2 + w^2D).$$

Usando las condiciones que tenemos sobre la curva E, y haciendo algunos cálculos, la ecuación anterior queda de la siguiente manera:

$$((x - u^2)^2 - (2u^2(v^2 + w^2D) - (v^2 - w^2D)^2))^2 = 4(v^2 - w^2D)^2x^2.$$

De esto, podemos obtener la solución entera

$$x = (u+v)^2 - w^2D,$$

y sustituyendo en la curva se obtiene $y = y(P) \in \mathbb{Z}$.

Por tanto, hemos encontrado un punto $P_{12} \in \mathrm{Tor}(E(\mathbb{Q}))$ con $x(P_{12}) = (u+v)^2 - w^2D$, lo que concluye la prueba del cuarto apartado.

5. Supongamos que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/10\mathbb{Z}$ y sea P un punto racional de orden 5. Tenemos que $x(4P) = x(P)$ y $x(2P) \neq x(P)$.

   Usando la fórmula de duplicación podemos obtener

   $$m = 2s(s+u) - v^2, \quad n = 2st,$$

   $$(s+u)^2 - v^2 = t^2 D, \quad (u+v)(u-v)^2 = 4uvs,$$

   con $u, v, s, t \in \mathbb{Z} \setminus \{0\}$.

   Recíprocamente, supongamos que la curva E satisface las condiciones del quinto apartado. Entonces, encontramos un punto racional P_5 de orden 5 tal que:

   $$x(P_5) = u^2, \quad y(P_5) = \pm u(u^2 - v^2 + 2us).$$

   Por tanto, si $P_2 = (0,0)$, se tiene que $P_2 + P_5 = P_{10}$ es un punto de orden 10, y usando las fórmulas dadas para la ley interna se obtiene:

   $$x(P_{10}) = 2v^2 + 4vs - u^2,$$

   lo que termina la prueba del quinto apartado.

6. Como tenemos una curva elíptica que sólo tiene un punto racional de orden 2, porque $f(X)$ sólo tiene una raíz racional, por el teorema de Mazur, si no se da ninguno de los cinco casos anteriores, sólo queda una opción: $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/2\mathbb{Z}$.

   Además, el único punto de orden 2 es $(0,0)$, lo que prueba que $x(P_2) = 0$, finalizando así la demostración del teorema. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Observación.– Las técnicas empleadas en las dos primeras secciones de este capítulo no son aplicables al caso de torsión cíclica de orden impar, por no poderse utilizar la proposición que hemos venido usando hasta ahora. Tendremos entonces que buscar otra manera de llegar a ecuaciones diofánticas que caractericen la torsión racional.

III.C. Torsión racional cíclica de orden 3

A partir de ahora, y hasta el final del capítulo, vamos a trabajar con curvas elípticas que no tienen puntos racionales de orden 2, es decir, con curvas

elípticas cuyos grupos de torsión son cíclicos de orden impar. Trataremos con estas curvas mediante su ecuación en forma breve de Weierstrass.

Observación.– Si una curva elíptica E dada no tiene puntos de orden 2, y tiene algún punto de orden 3, por el teorema de Mazur, sabemos que o bien $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/3\mathbb{Z}$, o bien $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/9\mathbb{Z}$. Luego, si dicha curva no cumple las condiciones que daremos en la sección III.F. para que en ella haya puntos de orden 9, la curva tendrá torsión racional cíclica de orden 3.

En el siguiente teorema vamos a caracterizar, mediante ecuaciones diofánticas, los coeficientes de las curvas elípticas en forma breve de Weierstrass que tienen algún punto racional de orden 3 y no tienen puntos racionales de orden 2.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

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

tal que $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$.

Entonces, E tiene algún punto racional de orden 3 si y sólo si

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6,$$

con $m, n \in \mathbb{Z}$ tales que $n \neq -9m^3$ y $n^2 \neq 27m^6$.

Además, si se cumplen estas condiciones, los puntos $P = (3m^2, 9m^3 + n)$ y $-P = (3m^2, -(9m^3 + n))$ son los únicos puntos racionales de orden 3 en la curva E.

Demostración.– Sabemos que un punto $(x, y) \in E(\mathbb{Q})$ es de orden 3 si y sólo si

$$\Psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

Si fuera $x = 0$, tendría que ser $A = 0$ para que x anulara a $\Psi_3(X)$, y $B = n^2$ con $n \in \mathbb{Q}$ para que el punto esté en la curva (este es el caso $m = 0$).

Visto este caso, supongamos $x \neq 0$. Dividiendo entonces $\Psi_3(x)$ por x^4 tenemos

$$3 + \frac{6A}{x^2} + \frac{12B}{x^3} - \left(\frac{A}{x^2}\right)^2 = 0,$$

que es una cónica en $X = A/x^2$ e $Y = B/x^3$,

$$3 + 6X + 12Y - X^2 = 0.$$

Esta cónica es una parábola de vértice $(3,-1)$ y eje $X=3$. Por tanto, cortando la recta $Y=0$, con las rectas que unen el punto $(3,-1)$ con puntos (X,Y) de la parábola, obtenemos puntos de la forma $(t,0)$, lo que nos permite dar la siguiente parametrización de la cónica

$$\begin{cases} X &= \dfrac{3(t+1)}{t-3} \\ \\ Y &= \dfrac{-t^2+6t+3}{(t-3)^2}, \quad t \in \mathbb{Q} \setminus \{3\}. \end{cases}$$

Así podemos parametrizar $\Psi_3(x)=0$ de la forma

$$\begin{cases} \dfrac{A}{x^2} &= \dfrac{3(t+1)}{t-3} \\ \\ \dfrac{B}{x^3} &= \dfrac{-t^2+6t+3}{(t-3)^2}, \quad t \in \mathbb{Q} \setminus \{3\}. \end{cases}$$

Llamando $t=p/q$ con $p,q \in \mathbb{Z}$ tales que $\mathrm{mcd}(p,q)=1, q \neq 0, p-3q \neq 0$, se tiene

$$\frac{A}{x^2} = \frac{3(p+q)}{p-3q}, \quad \frac{B}{x^3} = \frac{-p^2+6pq+3q^2}{(p-3q)^2}.$$

Y si llamamos $u=p-3q$, resulta $p=u+3q$, $p+q=u+4q$, y $-p^2+6pq+3q^2=12q^2-u^2$. Es decir,

$$\frac{A}{x^2} = \frac{3(u+4q)}{u}, \quad \frac{B}{x^3} = \frac{12q^2-u^2}{u^2},$$

con $u,q \in \mathbb{Z} \setminus \{0\}$ y $\mathrm{mcd}(u,q)=1$.

Tenemos entonces

$$A = \frac{3(u+4q)}{u}x^2, \quad B = \frac{12q^2-u^2}{u^2}x^3,$$

por tanto, como $(x,y) \in E(\mathbb{Q})$, aunque en realidad $x,y \in \mathbb{Z}$ por ser un punto de orden finito, será $y^2=x^3+Ax+B$, y sustituyendo A y B resulta

$$y^2 = x^3 + \frac{3(u+4q)}{u}x^2x + \frac{12q^2-u^2}{u^2}x^3,$$

de donde, operando se tiene

$$y^2 = \frac{3(u+2q)^2}{u^2}x^3,$$

es decir,

$$y^2 = \left(\frac{(u+2q)x}{u}\right)^2 3x,$$

luego, x ha de ser de la forma $x = 3m^2$ con $m \in \mathbb{Z}$.

Entonces, volviendo a la expresión de y^2 tendremos

$$y^2 = \left(\frac{(u+2q)3m^2}{u}\right)^2 3(3m^2),$$

de donde

$$y = \pm 9m^3\left(\frac{u+2q}{u}\right) = \pm\left(9m^3 + \frac{18m^3q}{u}\right) \in \mathbb{Z}.$$

Así, ha de ser $18m^3q/u \in \mathbb{Z}$, y como $\text{mcd}(u,q) = 1$ será $18m^3/u = r$ con $r \in \mathbb{Z}$. Es decir $y = \pm(9m^3 + rq)$ con $r, q, m \in \mathbb{Z}$.

Volviendo a las expresiones de A y B podemos escribir ahora

$$A = \frac{3(u+4q)}{u}(3m^2)^2 = 27m^4 + \frac{108m^4q}{u} = 27m^4 + 6rqm,$$

$$B = \frac{12q^2 - u^2}{u^2}(3m^2)^3 = \left(\frac{18m^3}{u}\right)^2 q^2 - 27m^6 = r^2q^2 - 27m^6.$$

Llamando $n = qr$, en resumen, tenemos que si (x,y) es un punto de orden 3 en la curva $Y^2 = X^3 + AX + B$, entonces existen $m, n \in \mathbb{Z}$ con

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6,$$

y el punto (x,y) tendrá coordenadas

$$x = 3m^2, \quad y = \pm(9m^3 + n).$$

Recíprocamente, el punto $(3m^2, \pm(9m^3+n))$ es de orden 3 en la curva $Y^2 = X^3 + (27m^4 + 6nm)X + (n^2 - 27m^6)$, ya que verifica la ecuación de la curva y $3m^2$ anula $\Psi_3(X)$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Ha de ser $n \neq -9m^3$ para que $y \neq 0$ y el punto no sea de orden 2. Además $n^2 \neq 27m^6$, para que $B \neq 0$, ya que en caso contrario la curva tendría el punto $(0,0)$ de orden 2.

Observación.– Estudiemos varios casos particulares:

(a) $m = 0$. En este caso son $A = 0$, $B = n^2$, $x = 0$, $y = \pm n$, y tenemos las curvas $E : Y^2 = X^3 + n^2$, donde los puntos $(0, \pm n)$ son de orden 3. Por otra parte, el discriminante de esta curva es $\Delta = -27n^4$, luego $\sqrt{\Delta} \notin \mathbb{Q}$.

(b) $2n = -9m^3$. Éste es el otro caso en el que $A = 0$. Además se tiene $B = n^2 - 27m^6$, $x = 3m^2$, e $y = \pm(-n)$, luego las curvas de ecuación $Y^2 = X^3 + n^2 - 27m^6$ tienen los puntos $(3m^2, \mp n)$ que son de orden 3. El discriminante es $\Delta = -5 \cdot 3^9 m^{12}$, por tanto $\sqrt{\Delta} \notin \mathbb{Q}$.

(c) $n = 0$. En este caso, $A = 27m^4$, $B = -27m^6$, $x = 3m^2$, $y = \pm 9m^3$, y tenemos las curvas $E : Y^2 = X^3 + 27m^4X - 27m^6$, donde los puntos $(3m^2, \pm 9m^3)$ son de orden 3. El discriminante es $\Delta = -5 \cdot 3^9 m^{12}$, luego $\sqrt{\Delta} \notin \mathbb{Q}$.

(d) $n = -6m^3$. Ahora son $A = -9m^4$, $B = 9m^6$, $x = 3m^2$, $y = \pm 3m^3$, y las curvas $E : Y^2 = X^3 - 9m^4X + 9m^6$ tienen los puntos $(3m^2, \pm 3m^3)$ de orden 3. Ahora el discriminante resulta $\Delta = 729m^{12}$, por tanto, $\sqrt{\Delta} = 27m^6 \in \mathbb{Q}$.

Ejemplo.– Dada la curva elíptica de ecuación

$$Y^2 = X^3 + 39X - 23,$$

comprobamos que no tiene puntos de orden 2, por ser $x^3 + 39x - 23 \neq 0$ $\forall x \in \mathbb{Q}$. Para ver si tiene algún punto racional de orden 3, planteamos el sistema de ecuaciones

$$\begin{aligned} 39 &= 27m^4 + 6nm, \\ -23 &= n^2 - 27m^6, \end{aligned}$$

que tiene, por ejemplo, la solución entera $\{m = 1, n = 2\}$. Por tanto, en la curva tenemos los puntos $P = (3, 11)$ y $-P = (3, -11)$ de orden 3. En principio, $\mathrm{Tor}(E(\mathbb{Q}))$ puede ser $\mathbb{Z}/3\mathbb{Z}$ ó $\mathbb{Z}/9\mathbb{Z}$.

Observación.– Haciendo $p = m$ y $q^3 = n$, podemos escribir de forma homogénea los coeficientes de una curva elíptica en forma breve de Weierstrass que tiene algún punto racional de orden 3, resultando su ecuación:

$$Y^2 = X^3 + (27p^4 + 6pq^3)X + (q^6 - 27p^6);$$

pero no siempre vamos a encontrar p y q enteros verificando

$$\begin{aligned} 27p^4 + 6pq^3 &= A, \\ q^6 - 27p^6 &= B. \end{aligned}$$

Por ejemplo, sabemos que la curva $Y^2 = X^3 + 39X - 23$, tiene el punto $P = (3, 11)$ de orden 3, sin embargo, no existen dos enteros p y q tales que $27p^4 + 6pq^3 = 39$ y $q^6 - 27p^6 = -23$.

III.D. Torsión racional cíclica de orden 5

Si una curva elíptica E dada no tiene puntos racionales de orden 2, y tiene algún punto racional de orden 5, por el teorema de Mazur, sabemos que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/5\mathbb{Z}$.

Vamos ahora a caracterizar, mediante ecuaciones diofánticas, los coeficientes de las curvas elípticas en forma breve de Weierstrass cuya torsión racional es cíclica de orden 5.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

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

tal que $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$.

Entonces, E tiene torsión racional cíclica de orden 5 si y sólo si

$$\begin{aligned} A &= -x^2 - xv - v^2 + (x-v)s, \\ B &= -\frac{1}{4}(x+v)(-3x^2 + 2xv - 3v^2 + 2(x-v)s), \\ s^2 &= (2x+v)(x+2v), \\ r^2 &= 3x + 2s + 3v. \end{aligned}$$

con $x, v, s, r \in \mathbb{Z}$ tales que $x \neq v$.

Además, si se cumplen estas condiciones, existirá un entero t tal que $t^2 = 3x - 2s + 3v$, y los puntos racionales de orden 5 de la curva E serán

$$\begin{aligned} P &= (x, (x-v)r/2), & 2P &= (v, (x-v)t/2), \\ 3P &= (v, -(x-v)t/2), & 4P &= (x, -(x-v)r/2). \end{aligned}$$

Demostración.– La prueba de que las condiciones del teorema son suficientes para que la curva tenga puntos de orden 5 es una simple comprobación. Supongamos que se verifican dichas condiciones.

Primero, si sustituimos en la ecuación de la curva X por x, y A y B por sus expresiones dadas en el enunciado, obtenemos

$$Y = \frac{1}{2}(x-v)\sqrt{3x + 2s + 3v},$$

y como suponemos que existe $r \in \mathbb{Z}$ con $r^2 = 3x + 2s + 3v$, tenemos que

$$P = (x, (x-v)r/2) \in E(\mathbb{Q}).$$

Ahora, para comprobar que este punto es de orden 5, podemos sustituir s por $\sqrt{(2x+v)(x+2v)}$ en las expresiones dadas para A y B, y éstas, ya

únicamente en función de x y v, las sustituimos primero en la fórmula de duplicación del punto P,

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)},$$

comprobando que al simplificar se obtiene v, y después, las sustituimos en la fórmula de duplicación del punto $2P$,

$$\frac{v^4 - 2Av^2 - 8Bv + A^2}{4(v^3 + Av + B)},$$

comprobando ahora que al simplificar resulta x. Esto prueba que $x(4P) = x = x(P)$, es decir, como suponíamos $x \neq v$, esto prueba que la curva tiene el punto racional P de orden 5, y como no había puntos de orden 2, se tiene que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/5\mathbb{Z}$.

Demostraremos ahora que las condiciones del teorema son necesarias.

Sea $P = (x, y) \in E(\mathbb{Q})$ un punto de orden 5, entonces se tiene que $4P = -P$. Si llamamos v a $x(2P)$, para que se cumpla esta igualdad es necesario que $x(4P) = x$ y $v \neq x$. Así, por la fórmula de duplicación tenemos

$$\begin{cases} \dfrac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = v, \\ \dfrac{v^4 - 2Av^2 - 8Bv + A^2}{4(v^3 + Av + B)} = x. \end{cases}$$

Buscamos las soluciones de este sistema de ecuaciones en el que x y v son enteros y distintos, y obtenemos la siguiente solución general:

$$\left\{ x = x,\ v = v,\ A = A,\ B = \frac{1}{4}(x + v)(x^2 - 4xv + v^2 - 2A) \right\},$$

con $x, v, A \in \mathbb{Z}$ y A raíz de $Z^2 + (2x^2 + 2xv + 2v^2)Z - x^4 + x^3v + 9x^2v^2 + xv^3 - v^4$.

Como el discriminante de este polinomio de segundo grado en Z es

$$\Delta = 4(x - v)^2(2x + v)(x + 2v),$$

para que A y B sean enteros, debe existir $s \in \mathbb{Z}$ con

$$s^2 = (2x + v)(x + 2v),$$

y así tendremos $\sqrt{\Delta} = \pm 2(x - v)s$. Para simplificar la notación, vamos a elegir la raíz positiva de s^2. Observemos que si tomáramos la raíz negativa,

los papeles de x y v se intercambiarían, como se puede comprobar a simple vista a partir de las fórmulas del enunciado; pero este intercambio no tendría ninguna repercusión en el grupo de torsión, ya que en este caso llamaríamos P a quien antes era $2P$ y viceversa.

Por tanto, con $\sqrt{\Delta} = (x-v)s$, resultan

$$A = -x^2 - xv - v^2 + (x-v)s,$$

$$B = -\frac{1}{4}(x+v)(-3x^2 + 2xv - 3v^2 + 2(x-v)s).$$

Para hallar la segunda coordenada de P, sustituimos $x = x(P)$ en la ecuación de la curva y tenemos

$$y^2 = x^3 + (-x^2 - xv - v^2 + (x-v)s)x - \frac{1}{4}(x+v)(-3x^2 + 2xv - 3v^2 + 2(x-v)s),$$

es decir, simplificando,

$$y^2 = \frac{1}{4}(x-v)^2(3x + 2s + 3v).$$

Como partimos de un punto $P = (x, y) \in E(\mathbb{Q})$ de orden 5, esto obliga a que exista $r \in \mathbb{Z}$ tal que $r^2 = 3x + 2s + 3v$, lo que finaliza la prueba de que las condiciones del teorema son necesarias.

Además, al suponer que $P = (x, y) \in E(\mathbb{Q})$, se tiene que también $2P \in E(\mathbb{Q})$, y como $v = x(2P)$, sustituyendo en la ecuación de la curva resulta que la segunda coordenada de $2P$ es $\sqrt{3x - 2s + 3v}(x-v)/2$, luego, también debe existir $t \in \mathbb{Z}$ tal que $t^2 = 3x - 2s + 3v$, como queríamos probar.

Podemos afirmar ahora que, con las condiciones necesarias para que la curva tenga algún punto racional de orden 5, su grupo de torsión resulta:

$$\{\mathcal{O}, P,\ 2P,\ 3P,\ 4P\},$$

siendo

$$\begin{aligned} P &= (x, (x-v)r/2), \\ 2P &= (v, (x-v)t/2), \\ 3P &= (v, -(x-v)t/2), \\ 4P &= (x, -(x-v)r/2). \end{aligned}$$

Q.E.D.

Ejemplo.– Aunque ya hemos demostrado la necesidad de que exista $r \in \mathbb{Z}$ tal que $r^2 = 3x + 2s + 3v$, vamos a dar un ejemplo en el que esto no se

verifica, y comprobaremos que, aunque se cumplen las demás condiciones del teorema, no hay puntos racionales de orden 5 en la curva. Dados los enteros $x = 4$ y $v = -14$, se tiene

$$\begin{aligned} (2x+v)(x+2v) = (-6)\cdot(-24) &= 12^2, \\ -x^2 - xv - v^2 + (x-v)\cdot 12 &= 60, \\ -\frac{1}{4}(x+v)(-3x^2+2xv-3v^2+2(x-v)\cdot 12) &= -790, \end{aligned}$$

pero, $3x+2\cdot 12+3v = -6$ no es el cuadrado de ningún entero. Si consideramos ahora la curva de ecuación $Y^2 = X^3 + 60X - 790$, y sustituimos X por 4, resulta $Y^2 = -486$, por tanto, no hay ningún punto racional en la curva cuya primera coordenada sea $x = 4$; es más, el grupo de torsión racional de esta curva elíptica es trivial, $\{\mathcal{O}\}$.

Observación.– Vamos a fijarnos en un aspecto práctico consecuencia de las expresiones conseguidas para los coeficientes A y B de la curva.

Si observamos la expresión de $A(x,v,s) = -x^2 - xv - v^2 + (x-v)s$, vemos que es una forma cuadrática ternaria, que además podemos expresar, completando cuadrados, como

$$A(x,v,s) = -\left(x + \frac{v}{2} - \frac{s}{2}\right)^2 + s^2 - 3\left(\frac{v}{2} + \frac{s}{2}\right)^2,$$

es decir, tras un cambio lineal,

$$A(x_1,v_1,s_1) = -x_1^2 + v_1^2 - 3s_1^2.$$

Así, dada una curva elíptica $Y^2 = X^3 + AX + B$ con A y B enteros, para ver si su torsión racional es $\mathbb{Z}/5\mathbb{Z}$, lo primero que podemos hacer es buscar soluciones enteras de la ecuación $-x_1^2+v_1^2-3s_1^2 = A$. Esto liga este problema al de la representación de un número entero por una forma cuadrática ternaria. Este problema está en constante progreso desde hace siglos, y este nuevo enfoque puede resultar interesante; pero nosotros no lo seguiremos en esta memoria.

En lugar de ello, para caracterizar las curvas elípticas cuya torsión racional es cíclica de orden 5, vamos a buscar ahora unas ecuaciones diofánticas más sencillas, llamadas ecuaciones de Thue, aunque esto suponga un aumento en el grado en las expresiones que nos dan A y B.

Definición.– Una ecuación de Thue es una ecuación diofántica del tipo $F(p,q) = m$, donde $F(p,q) \in \mathbb{Z}[p,q]$ es una forma binaria irreducible de grado $n \geq 3$ y m es un entero dado.

Observación.– En 1909, Thue [37] probó que este tipo de ecuaciones tiene sólo una cantidad finita de soluciones, y bastante más tarde, en los años sesenta, Baker [1, 26] dio un algoritmo teórico para encontrar las soluciones de dichas ecuaciones. Posteriormente, ya en 1989, Tzanakis y de Weger [38, 36] combinaron las técnicas computacionales de aproximación diofántica con la teoría de Baker, para dar un algoritmo práctico general que resuelve ecuaciones de Thue.

Por otra parte, Bombieri y Schmidt [4, 36] en 1987 dieron el siguiente resultado: Si m tiene t factores primos, el número de soluciones de la ecuación $|F(p,q)| = m$ es, a lo sumo, cn^{t+1}, donde n es el grado de F y c es una constante positiva.

Vamos entonces a caracterizar las curvas elípticas cuya torsión racional es cíclica de orden 5, mediante ecuaciones de Thue.

Observación.– Podemos suponer que los coeficientes A y B de una curva elíptica de ecuación $Y^2 = X^3 + AX + B$, son enteros verificando que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B. Ya que, en caso contrario, mediante el cambio

$$X \longmapsto k^2X, \quad Y \longmapsto k^3Y,$$

conseguimos que los coeficientes de la curva verifiquen dicha propiedad.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

$$Y^2 = X^3 + AX + B,$$

siendo $A, B \in \mathbb{Z}$ con $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$, y tales que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B.

Entonces, E tiene torsión racional cíclica de orden 5 si y sólo si

$$\begin{aligned} A &= -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4), \\ B &= 54(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4), \end{aligned}$$

con $p, q \in \mathbb{Z}$ tales que $\mathrm{mcd}(p,q) = 1$ y $pq \neq 0$.

Además los puntos racionales de orden 5 de la curva E son

$$\begin{aligned} P &= (3(p^2 - 6pq + q^2), 108p^2q), \\ 2P &= (3(p^2 + 6pq + q^2), 108pq^2), \\ 3P &= (3(p^2 + 6pq + q^2), -108pq^2), \\ 4P &= (3(p^2 - 6pq + q^2), -108p^2q). \end{aligned}$$

Demostración.– Por el teorema anterior, sabemos que si $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/5\mathbb{Z}$, los coeficientes de la curva son $A = A(x,v,s)$ y $B = B(x,v,s)$ con $s^2 = (2x+v)(x+2v)$. Por otra parte, como vimos en la sección I.G., la curva elíptica de ecuación $Y^2 = X^3 + A(x,v,s)X + B(x,v,s)$ tiene un punto de orden 5 si y sólo si esta ecuación es equivalente a la forma normal de Weierstrass de una curva en forma normal de Tate con ecuación

$$Y^2 - \alpha XY - \alpha Y = X^3 - \alpha X^2$$

donde $\alpha \in \mathbb{Q}$.

La forma normal de Weierstrass de esta curva es $Y^2 = X^3 + A(\alpha)X + B(\alpha)$, siendo

$$A(\alpha) = -27 - 324\alpha - 378\alpha^2 + 324\alpha^3 - 27\alpha^4,$$

$$B(\alpha) = 54 + 972\alpha + 4050\alpha^2 + 4050\alpha^4 - 972\alpha^5 + 54\alpha^6,$$

y será equivalente a la forma normal de Weierstrass dada si y sólo si existe $u \in \mathbb{Q}$ tal que

$$\frac{A(x,v,s)}{A(\alpha)} = u^4, \quad \frac{B(x,v,s)}{B(\alpha)} = u^6.$$

Buscando parametrizaciones sencillas, a partir de estas relaciones hemos calculado bases de Gröbner con distintos órdenes lexicográficos, como es habitual en teoría de eliminación, obteniendo los siguientes resultados:

$$\begin{aligned} x &= 3u^2(\alpha^2 - 6\alpha + 1), \\ v &= 3u^2(\alpha^2 + 6\alpha + 1), \\ s &= -9u^2(\alpha^2 - 1); \end{aligned}$$

con $u,\ \alpha \in \mathbb{Q}$. (También si x y v intercambian sus expresiones, pero esto daría las mismas A y B como se puede comprobar.)

Al ser x, v y s enteros, vamos a escribir $u = u_1/u_2$, $\alpha = p/q$, siendo $u_1,\ u_2,\ p,\ q \in \mathbb{Z}$, con $\mathrm{mcd}(p,q) = 1 = \mathrm{mcd}(u_1,u_2)$, y vamos a estudiar las posibilidades de $u_1,\ u_2,\ p$ y q.

Sabemos que $x = x(P) \in \mathbb{Z}$. Veamos que esto implica que q divide a u_1. Sustituyendo $u = u_1/u_2$ y $\alpha = p/q$ en x, y desarrollando se tiene:

$$x = 3\,\frac{u_1^2}{u_2^2}\left(\frac{p^2 - 6pq + q^2}{q^2}\right) \in \mathbb{Z}.$$

Comprobemos que $\mathrm{mcd}(p^2 - 6pq + q^2, q^2) = 1$, y así, q^2 debe dividir a $3u_1^2$. Razonemos por reducción al absurdo. Si existe m primo tal que m divide a q^2 y a $(p^2 - 6pq + q^2)$, entonces existe m primo que divide a q y a $(p^2 + q(-6p+q))$, por tanto, existirá m primo divisor de q y p^2, lo que contradice que $\mathrm{mcd}(p,q) = 1$.

Falta comprobar que si q^2 divide a $3u_1^2$, entonces q divide a u_1, como queríamos ver. Para ello distinguimos dos casos: que q sea múltiplo de 3, o que no lo sea. El segundo caso es trivial, veamos el primero. Escribimos $q = 3^r q_1$, no siendo q_1 múltiplo de 3, y tendremos que $3^{2r}q_1^2$ divide a $3u_1^2$, por tanto, $3^{2r-1}q_1^2$ divide a u_1^2. Por una parte se tiene que 3^{2r-1} es divisor de u_1^2, de donde se tiene que 3^r divide a u_1, y por otra parte, q_1^2 divide a u_1^2, y así q_1 es divisor u_1, por tanto, $3^r q_1 = q$ divide a u_1.

Llamando k a u_1/q y sustituyendo las expresiones obtenidas para x, v y s en $A(x,v,s)$ y $B(x,v,s)$, conseguimos

$$\begin{aligned} A &= -27(k/u_2)^4(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4), \\ B &= 54(k/u_2)^6(p^2+q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4). \end{aligned}$$

Demostremos ahora que $u_2 = 1$. Tenemos

$$x = \frac{3k^2(p^2 - 6pq + q^2)}{u_2^2},\ v = \frac{3k^2(p^2 + 6pq + q^2)}{u_2^2},\ s = \frac{9k^2(p^2 - q^2)}{u_2^2},$$

y, como $\mathrm{mcd}(k, u_2) = 1$, para que x, v y s sean enteros, u_2^2 debe dividir a $3(p^2 - 6pq + q^2)$, $3(p^2 + 6pq + q^2)$ y $9(p^2 - q^2)$. Sumando las dos primeras expresiones, se tiene que

$$u_2^2 \text{ divide a } 6(p^2 + q^2), \tag{1}$$

$$u_2^2 \text{ divide a } 9(p^2 - q^2). \tag{2}$$

Vamos a distinguir varios casos.

- Si 2 y 3 no dividen a u_2. Por (1) se tiene que u_2^2 divide a $p^2 + q^2$, y por (2), u_2^2 divide a $p^2 - q^2$. Sumando estas dos expresiones, resulta que u_2^2 divide a $2p^2$, y restándolas u_2^2 divide a $2q^2$. Como 2 no divide a u_2, se tiene que u_2 divide a p y q, es decir, $u_2 = 1$.

- Si 2 divide a u_2, 3 no divide a u_2 y $2 \neq u_2$. Llamando $u_2 = 2u_2'$, con $u_2' \neq 1$, por (2) tenemos que u_2^2 divide a $p^2 - q^2$, y por tanto, que $(u_2')^2$ divide a $p^2 - q^2$. Por otra parte, por (1) se tiene que $u_2^2 = 4(u_2')^2$ divide a $6(p^2+q^2)$, y como 3 no divide a u_2, resulta que $(u_2')^2$ divide a p^2+q^2. Sumando ahora las dos expresiones obtenidas, tenemos que u_2' divide a p y q, lo que contradice que $u_2' \neq 1$.

- Si 2 no divide a u_2, 3 divide a u_2 y $3 \neq u_2$. Llamando $u_2 = 3u_2'$, con $u_2' \neq 1$, por (2) tenemos que $u_2^2 = 9(u_2')^2$ divide a $9(p^2 - q^2)$, y por tanto, que $(u_2')^2$ divide a $p^2 - q^2$. Ahora por (1), $u_2^2 = 9(u_2')^2$ divide a $6(p^2 + q^2)$, y por tanto, como 2 no divide a u_2, resulta que $(u_2')^2$ divide a $p^2 + q^2$. Sumando y restando las expresiones obtenidas se tiene de nuevo contradicción con que u_2' divide a p y q, y $u_2' \neq 1$.

- Si 2 divide a u_2, 3 divide a u_2 y $6 \neq u_2$. Llamando $u_2 = 6u_2'$, con $u_2' \neq 1$, por (2) tenemos que $u_2^2 = 36(u_2')^2$ divide a $9(p^2 - q^2)$, y por tanto, que $(u_2')^2$ divide a $p^2 - q^2$. Por otra parte, por (1) se tiene que $u_2^2 = 36(u_2')^2$ divide a $6(p^2 + q^2)$, y por tanto, $(u_2')^2$ divide a $p^2 + q^2$. Ahora volvemos a repetir el razonamiento anterior para llegar a la misma contradicción.

- Si $u_2 = 2$. Como $B = 54(k/u_2)^6(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4) \in \mathbb{Z}$, sustituyendo u_2 por 2, como $\mathrm{mcd}(k, u_2) = 1$, tendría que ser $(27/2^5)(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4)$ entero, es decir, sería $(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4) \equiv 0 \pmod{32}$. Pero si comprobamos todas las posibilidades para p y q primos entre sí, vemos que en ningún caso, se obtiene solución para esta ecuación módulo 32. Por tanto, no puede ser $u_2 = 2$.

- Si $u_2 = 3$. Como $x = 3(k/u_2)^2(p^2 - 6pq + q^2) \in \mathbb{Z}$, sustituyendo u_2 por 3, como $\mathrm{mcd}(k, u_2) = 1$, tendría que ser $(1/3)(p^2 - 6pq + q^2)$ entero, es decir, sería $(p^2 - 6pq + q^2) \equiv 0 \pmod{3}$. Comprobando todas las posibilidades para p y q primos entre sí, vemos que no se obtiene solución para esta congruencia. Es decir, no puede ser $u_2 = 3$.

- Si $u_2 = 6$. Como $x = 3(k/u_2)^2(p^2 - 6pq + q^2) \in \mathbb{Z}$, sustituyendo u_2 por 6, debe ser $\frac{1}{12}(p^2 - 6pq + q^2)$ entero, es decir, $(p^2 - 6pq + q^2) \equiv 0 \pmod{12}$. Comprobando de nuevo todas las posibilidades para p y q primos entre sí, vemos que no se obtiene solución para esta congruencia. Es decir, no puede ser $u_2 = 6$.

Esto termina la prueba de que $u_2 = 1$.

Resumiendo, hemos probado que si una curva elíptica de ecuación $Y^2 = X^3 + AX + B$ con $A, B \in \mathbb{Z}$, tiene un punto racional $P = (x, y)$ de orden 5, entonces tiene coeficientes de la forma $A = -x^2 - xv - v^2 + (x - v)s$, $B = -(1/4)(x + v)(-3x^2 + 2xv - 3v^2 + 2(x - v)s)$, con

$$\begin{aligned} x &= 3k^2(p^2 - 6pq + q^2), \\ v &= 3k^2(p^2 + 6pq + q^2), \\ s &= 9k^2(p^2 - q^2); \end{aligned}$$

siendo k, p, $q \in \mathbb{Z}$ y $\mathrm{mcd}(p, q) = 1$. Sustituyendo estas expresiones en las de A y B, hemos probado que los coeficientes de una curva elíptica, en forma breve de Weierstrass, con grupo de torsión racional de orden 5 deben ser

$$\begin{aligned} A &= -27k^4(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4), \\ B &= 54k^6(p^2 + q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4), \end{aligned}$$

y como suponíamos que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B, debe ser $k = 1$. Por tanto, podemos afirmar que los coeficientes de dicha curva serán

$$\begin{aligned} A &= A(p,q) = -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4), \\ B &= B(p,q) = 54(p^2+q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4), \end{aligned}$$

y como $x = x(P)$ y $v = x(2P)$, sustituyendo en la ecuación de la curva y haciendo los cálculos para $y(P)$, $y(2P)$, $y(3P) = -y(2P)$, $y(4P) = -y(P)$, podemos dar su grupo de torsión racional:

$$\{\mathcal{O}, P,\ 2P,\ 3P,\ 4P\},$$

siendo

$$\begin{aligned} P &= (3(p^2 - 6pq + q^2), 108p^2q), \\ 2P &= (3(p^2 + 6pq + q^2), 108pq^2), \\ 3P &= (3(p^2 + 6pq + q^2), -108pq^2), \\ 4P &= (3(p^2 - 6pq + q^2), -108p^2q), \end{aligned}$$

Recíprocamente, es fácil ver que si una curva elíptica tiene coeficientes $A = A(p,q)$ y $B = B(p,q)$, entonces su torsión es cíclica de orden 5, sin más que comprobar que el punto $P = (3(p^2 - 6pq + q^2), 108p^2q)$ está en la curva y es de orden 5. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– En sentido estricto, sólo la ecuación de A es de Thue, dado que la de B está dada por una forma reducible. Formalmente, B se debe expresar como la solución a un conjunto de sistemas de Thue, correspondiendo a las factorizaciones posibles $B = B_1B_2$.

Observación.– Se puede comprobar que, con las expresiones obtenidas en este teorema, $3x + 2s + 3v$ es el cuadrado de un entero, como debía ser según el primer teorema de esta sección, ya que

$$3x + 2s + 3v = 3 \cdot 3(p^2 - 6pq + q^2) + 2 \cdot 9(p^2 - q^2) + 3 \cdot 3(p^2 + 6pq + q^2) = 36p^2.$$

Así, en la práctica, dada una curva elíptica $Y^2 = X^3 + AX + B$ con $A, B \in \mathbb{Z}$ tales que no existe $k \in \mathbb{Z}$ verificando que k^4 divida a A y k^6 divida a B, para saber si tiene torsión racional cíclica de orden 5, tendríamos que resolver el sistema formado por las ecuaciones de Thue $A(p,q) = A$, $B(p,q) = B$.

Ejemplo.– Dada la curva elíptica de ecuación $Y^2 = X^3 - 27X + 55350$, planteamos el sistema diofántico

$$\begin{cases} -27 &= -27(q^4 - 12q^3p + 14q^2p^2 + 12p^3q + p^4), \\ 55350 &= 54(p^2+q^2)(q^4 - 18q^3p + 74q^2p^2 + 18p^3q + p^4), \end{cases}$$

y hallamos sus soluciones, obteniendo $\{p = 2, q = -1\}$, $\{p = -1, q = -2\}$, $\{p = 1, q = 2\}$ y $\{p = -2, q = 1\}$. Por tanto, el hecho de que exista solución entera para este sistema de ecuaciones de Thue, implica que la curva dada tiene torsión racional $\mathbb{Z}/5\mathbb{Z}$ y, sustituyendo cualquiera de estas soluciones (por ejemplo $p = 1$, $q = 2$) en las expresiones dadas en el teorema anterior, podemos afirmar que los puntos racionales de torsión de la curva son:

$$\Big\{\mathcal{O}, P = (-21, 216),\ 2P = (51, 432),\ 3P = (51, -432),\ 4P = (-21, -216)\Big\}.$$

Observación.– Podemos comprobar que las expresiones $A(p, q)$ y $B(p, q)$ se pueden obtener directamente a partir de $A(\alpha)$ y $B(\alpha)$, sin más que sustituir α por p/q. Pero con el teorema anterior, no sólo hemos conseguido expresiones para A y B, hemos conseguido expresiones que nos llevan a ecuaciones de Thue y, además, tenemos las coordenadas de los puntos racionales de torsión en función de p y q.

III.E. Torsión racional cíclica de orden 7

Para que una curva elíptica E, que no tiene puntos racionales de orden 2, tenga $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/7\mathbb{Z}$, según Mazur, es necesario y suficiente que tenga algún punto racional de orden 7.

Vamos a caracterizar en esta sección, también mediante ecuaciones diofánticas, los coeficientes de las curvas elípticas en forma breve de Weierstrass cuya torsión racional es cíclica de orden 7.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

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

tal que $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$.

Entonces, E tiene algún punto de orden 7 si y sólo si

$$\begin{aligned}
A &= -x^2 - v^2 - xv + s(x - v),\\
B &= -\frac{1}{4}(3x^3 + x^2w + 3xv^2 - 2xvw + 2v^3 + v^2w + 2s(x - v)(x + v)),\\
s^2 &= (v + 2x)(x + w + v),\\
0 &= 3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s,\\
r^2 &= 3x + 2v + 2s + w,
\end{aligned}$$

con $x, v, w, s, r \in \mathbb{Z}$ tales que x, v y w son distintos dos a dos.

Además, si se cumplen estas condiciones, existirán dos enteros h y k tales que $h^2 = 3x + 2v + w - 2s$ y $k^2 = 4w^3 - 3wx^2 - 3v^2w - 6xvw + 4wxs - 4wvs + 3x^3 + 3xv^2 - 2sx^2 + 2v^3 + 2sv^2$, y los puntos racionales de orden 7 de la curva E serán

$$\begin{aligned} P &= (x, (x-v)r/2), \\ 2P &= (v, (x-v)h/2), \\ 3P &= (w, k/2), \\ 4P &= (w, -k/2), \\ 5P &= (v, -(x-v)h/2), \\ 6P &= (x, -(x-v)r/2). \end{aligned}$$

Demostración.– Probemos que las condiciones del teorema son suficientes para que la curva tenga puntos de orden 7. Supongamos que se verifican dichas condiciones.

Primero, si sustituimos en la ecuación de la curva X por x, y A y B por sus expresiones dadas en el enunciado, obtenemos

$$Y = \frac{1}{2}(x-v)\sqrt{3x + 2v + 2s + w},$$

y como suponemos que existe $r \in \mathbb{Z}$ con $r^2 = 3x + 2v + 2s + w$, tenemos que

$$P = (x, (x-v)r/2) \in E(\mathbb{Q}).$$

Ahora, vamos a comprobar que este punto es de orden 7. Sustituimos s por $\sqrt{(v+2x)(x+w+v)}$ en las expresiones dadas para A y B, y éstas, ya únicamente en función de x, v y w, las sustituimos en la fórmula de duplicación del punto P,

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)},$$

comprobando que al simplificar se obtiene v.

Después, sustituimos las expresiones de A y B del enunciado en la fórmula de duplicación del punto $2P$,

$$x(4P) = \frac{v^4 - 2Av^2 - 8Bv + A^2}{4(v^3 + Av + B)},$$

obteniendo

$$x(4P) = \frac{x^2 - 2xv - 2sx - 2vw + s^2}{3x + 2v + w - 2s},$$

y comprobamos que esto es w, viendo que el numerador de esta expresión coindide con su denominador multiplicado por w, ya que

$$(x^2 - 2xv - 2sx - 2vw + s^2) - w(3x + 2v + w - 2s) =$$

$$= (x^2 - 2xv - 2sx - 2vw + (v + 2x)(x + w + v)) - w(3x + 2v + w - 2s) =$$

$$= 3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s$$

y esta expresión es igual a 0 por hipótesis.

Falta comprobar que $x(3P)$ también es w. Usando las fórmulas dadas para la ley interna de la curva en el I.B., podemos calcular la primera coordenada de $3P$ en función de x,

$$x(3P) = (x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3$$

$$+48A^2Bx^2 + (96AB^2 + 9A^4)x + 8B(A^3 + 8B^2))/$$

$$/(3x^4 + 6Ax^2 + 12Bx - A^2)^2,$$

y, sustituyendo aquí las expresiones de A y B dadas en el enunciado, obtenemos una expresión en x, v, w y s con denominador $d(x, v, w, s)$ y numerador $n(x, v, w, s)$ verificando

$$wd(x, v, w, s) - n(x, v, w, s) = (3xv + vw + v^2 + 2x^2 + 2xw - s^2)\cdot$$

$$(-w^2v + 4w^2x + 8wx^2 + 4x^3 - 7v^2x - 4v^3 + 6swx + 10sx^2 - 6svw$$

$$-2svx - 8sv^2 - s^2w + 5s^2x - 4s^2v),$$

que es igual a 0, por serlo el primer factor, ya que

$$s^2 = (v + 2x)(x + w + v) = 3xv + vw + v^2 + 2x^2 + 2xw.$$

Esto prueba que $x(3P) = w = x(4P)$, es decir, como suponíamos x, v y w distintos dos a dos, esto prueba que la curva tiene el punto racional P de orden 7, y como no había puntos de orden 2, se tiene que $E(\mathrm{Tor}(\mathbb{Q})) = \mathbb{Z}/7\mathbb{Z}$.

Demostremos ahora que las condiciones del teorema son necesarias.

Un punto $P = (x, y) \in E(\mathbb{Q})$ es de orden 7 si y sólo si $4P = -3P$. Si denotamos $2P = (v, t)$ y $3P = (w, z)$, tendremos que P es de orden 7 si y sólo si $x(4P) = w$ y x, v y w son distintos dos a dos.

Por la fórmula de duplicación,

$$\frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = v,$$

luego, tenemos la relación:

$$F_1(x,v) = x^4 - 2Ax^2 - 8Bx + A^2 - 4(x^3 + Ax + B)v = 0.$$

Como ya sabemos, la primera coordenada de $3P$ en función de la primera coordenada de P resulta

$$w = x(3P) = (x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3$$

$$+48A^2Bx^2 + (96AB^2 + 9A^4)x + 8B(A^3 + 8B^2))/(3x^4 + 6Ax^2 + 12Bx - A^2)^2,$$

por tanto, tenemos también la relación

$$\begin{aligned} 0 = F_2(x,w) \;=\; & x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + \\ & +(36A^3 + 48B^2)x^3 + 48A^2Bx^2 + (96AB^2 + 9A^4)x \\ & +8B(A^3 + 8B^2) - w(3x^4 + 6Ax^2 + 12Bx - A^2)^2. \end{aligned}$$

Con las fórmulas de la suma de $P = (x,y)$ y $2P = (v,t)$, conseguimos, de otra manera, la primera coordenada de $3P$,

$$x(3P) = \frac{-x^3 + vx^2 + v^2x + y^2 - 2ty - v^3 + t^2}{x^2 - 2xv + v^2}.$$

Sustituyendo t por su expresión en función de x e y, es decir, sustituyendo t por $y(2P) = -(27x^6 + 27x^4A - 36x^3y^2 + 9x^2A^2 - 12Axy^2 + A^3 + 8y^4)/8y^3$, queda

$$x(3P) = (135x^4A^4 + 540x^6A^3 + 1215x^8A^2 + 1458x^10A + 18x^2A^5 - 2592y^2Ax^7$$

$$-1296y^2A^2x^5 - 24y^2A^4x - 288x^3y^2A^3 + 64vx^2y^6 + 1728x^4y^4A + 432x^2y^4A^2$$

$$+64v^2xy^6 + 32y^4A^3 - 384xy^6A + 2160x^6y^4 + 729x^12 - 1216x^3y^6 - 1944y^2x^9$$

$$+A^6 - 64v^3y^6 + 256y^8)/64((x^2 - 2xv + v^2)y^6),$$

y sustituyendo y^2 por $x^3 + Ax + B$, tenemos otra forma de expresar $x(3P)$, ahora en función de x y de v. Por tanto, igualando esta última expresión de $x(3P)$ a la primera expresión que teníamos de w en funciónde x, obtenemos una tercera relación,

$$F_3(x,v) = 0,$$

donde $F_3(x,v)$ es un polinomio en x y v de grado 20 que tiene 139 términos.

Para conseguir una cuarta relación, vamos a igualar dos formas de expresar $x(4P)$. La primera de ellas viene de aplicar la fórmula de duplicación al punto $2P$,

$$x(4P) = x(2(2P)) = \frac{v^4 - 2Av^2 - 8Bv + A^2}{4(v^3 + Av + B)},$$

y la segunda, de sumar P y $3P$, es decir, de

$$x(4P) = x(P + 3P) = \frac{-x^3 + wx^2 + w^2x + y^2 - 2zy - w^3 + z^2}{x^2 - 2wx + w^2}.$$

Si en esta segunda expresión sustituimos y por $\sqrt{(x^3 + Ax + B)}$ y z, es decir, $\sqrt{(w^3 + Aw + B)}$, por su expresión en función de x (conseguida al hallar la segunda coordenada de $3P$), resulta $x(4P)$ en función de x y de w.

Así, al igualar $x(2(2P))$ en función de v a esta última expresión de $x(P + 3P)$ en función de x y w, conseguimos la cuarta relación

$$F_4(x, v, w) = 0,$$

siendo $F_4(x, v, w)$ un polinomio en x, v y w de grado 18 con 321 términos.

Queremos dar A y B en función de x, v y w. Para ello, calculamos una base de Gröbner del ideal generado por F_1, F_2, F_3 y F_4, y conseguimos cinco polinomios que formarán un sistema cuya solución general es:

$$\Big\{x = x,\ v = v,\ w = w,\ A = A,$$

$$B = \frac{1}{4}(wx^2 - 2xvw + v^2w + x^3 - 4vx^2 - v^2x - 2(v + x)A)\Big\},$$

con $x, v, w, A \in \mathbb{Z}$ y A raíz del polinomio $Z^2 + (2x^2 + 2v^2 + 2vx)Z - x^4 + 3vx^3 - 2x^3w + v^3x + 3vwx^2 + 6x^2v^2 - v^3w$.

Como el discriminante de este polinomio de segundo grado en Z es

$$\Delta = 4(v + 2x)(x - v)^2(x + w + v),$$

para que A y B sean enteros, debe existir $s \in \mathbb{Z}$ con

$$s^2 = (v + 2x)(x + w + v),$$

y así tendremos $\sqrt{\Delta} = \pm 2(x - v)s$, resultando

$$A = -x^2 - v^2 - xv \pm s(x - v),$$

$$B = \frac{1}{4}(3x^3 + wx^2 + 3v^2x + v^2w - 2xvw + 2v^3 \pm 2(v^2 - x^2)s).$$

Para simplificar la notación, vamos a elegir la raíz positiva de s^2. Observemos que si tomáramos la raíz negativa, las expresiones que aparecen en el enunciado del teorema serían las mismas pero cambiando $-s$ por s, lo que

no tendría ninguna repercusión en el grupo de torsión racional de la curva, que seguiría teniendo los mismos puntos y con las mismas coordenadas.

Ahora, para imponer que el punto $P = (x, y)$ sea de orden 7, es decir, que $4P = -3P$, se igualan $x(3P)$ y $x(4P)$, y se obtiene que A debe ser raíz del polinomio

$$Z^4 + 6v(x+v)Z^3 + (-8x^4 + 15x^2v^2 + 11vx^3 + 23v^3x + 13v^4)Z^2$$

$$+(-24vx^5 + 58v^3x^3 + 42v^4x^2 - 6v^2x^4 + 4x^6 + 24v^5x + 10v^6)Z$$

$$-(x^2 + xv + v^2)(v^6 - 3v^5x - 33v^4x^2 - 20v^3x^3 + 39v^2x^4 - 12vx^5 + x^6).$$

Como ya teníamos la expresión $A = -x^2 - v^2 - xv + s(x - v)$, al sustituirla ahora en esta ecuación de grado 4 debe dar 0. De esto conseguimos la relación

$$12x^4 - 16x^3s + 24vx^3 + 2s^2x^2 + 27x^2v^2 - 24x^2sv - s^2xv - 12v^2sx$$

$$+4xs^3 + 15xv^3 - 2v^3s + 3v^4 - s^4 + 2s^3v - s^2v^2 = 0,$$

que podemos escribir de la forma

$$-s^4 + 2(2x+v)s^3 + (2x+v)(x-v)s^2 - 2(2x+v)^3s + 3(x^2+xv+v^2)(2x+v)^2 = 0,$$

y sustituyendo s^2 por $(v + 2x)(x + w + v)$, debe ser

$$(2x + v)^2(3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s) = 0.$$

Veamos que ha de ser $v \neq -2x$ y así habremos llegado a la condición necesaria:

$$3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s = 0.$$

Si $v = -2x$, entonces $s = 0$ y $x(4P) = x(5x+4w)/(w-x)$, por tanto, si P es un punto de orden 7, será $x(4P) = w$, es decir, $x(5x+4w) - w(w-x) = 0$. Pero, la ecuación $5x^2 + 5xw - w^2 = 0$ sólo tiene una solcuión racional: $\{x = 0, w = 0\}$, que no es válida porque tenía que ser $x \neq w$. Por tanto, podemos suponer $2x + v \neq 0$ como queríamos probar.

Resumiendo, por ahora tenemos

$$\begin{aligned} A &= -x^2 - v^2 - xv + s(x - v), \\ B &= -\frac{1}{4}(3x^3 + x^2w + 3xv^2 - 2xvw + 2v^3 + v^2w + 2s(x - v)(x + v)), \\ s^2 &= (v + 2x)(x + w + v), \\ 0 &= 3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x - w)s. \end{aligned}$$

Para hallar la segunda coordenada de P, sustituimos $x = x(P)$ en la ecuación de la curva y tenemos

$$\begin{aligned} y^2 &= x^3 + (-x^2 - v^2 - xv + s(x-v))x \\ &\quad + \frac{1}{4}(3x^3 + wx^2 + 3v^2x + v^2w - 2xvw + 2v^3 + 2(v^2 - x^2)s), \end{aligned}$$

es decir

$$y^2 = \frac{1}{4}(x-v)^2(3x + 2v + 2s + w),$$

lo que obliga a que exista $r \in \mathbb{Z}$ tal que

$$r^2 = 3x + 2v + 2s + w,$$

y con esto finaliza la prueba de que las condiciones del teorema son necesarias.

Además, al suponer que $P = (x, y) \in E(\mathbb{Q})$, se tiene que también $2P \in E(\mathbb{Q})$, y como $v = x(2P)$, sustituyendo en la ecuación de la curva resulta que la segunda coordenada de $2P$ es $\sqrt{3x + 2v + w - 2s}(x - v)/2$, luego, debe existir $h \in \mathbb{Z}$ tal que

$$h^2 = 3x + 2v + w - 2s.$$

Y, siguiendo el mismo razonamiento para $3P$, debe existir $k \in \mathbb{Z}$ tal que

$$k^2 = 4w^3 - 3wx^2 - 3v^2w - 6xvw + 4wxs - 4wvs + 3x^3 + 3xv^2 - 2sx^2 + 2v^3 + 2sv^2,$$

como queríamos probar.

Ahora podemos afirmar que, con las condiciones necesarias para que la curva tenga algún punto racional de orden 7, su grupo de torsión racional resulta:

$$\{\mathcal{O}, P,\ 2P,\ 3P,\ 4P,\ 5P,\ 6P\},$$

siendo

$$\begin{aligned} P &= (x, (x-v)r/2), \\ 2P &= (v, (x-v)h/2), \\ 3P &= (w, k/2), \\ 4P &= (w, -k/2), \\ 5P &= (v, -(x-v)h/2), \\ 6P &= (x, -(x-v)r/2). \end{aligned}$$

Q.E.D.

Observación.– De las relaciones obtenidas para caracterizar los coeficientes A y B de una curva elíptica con torsión racional de orden 7, vemos que

la expresión que da A es la misma que para curvas con torsión racional de orden 5, aunque evidentemente con diferentes relaciones entre los parámetros. Esto significa que tenemos de nuevo que A es una forma cuadrática ternaria equivalente a

$$A(x_1, v_1, s_1) = -x_1^2 + v_1^2 - 3s_1^2,$$

con las consecuencias prácticas ya mencionadas en la sección anterior.

Tal y como hicimos para el caso de orden 5, vamos a caracterizar ahora las curvas elípticas cuya torsión racional es cíclica de orden 7, mediante ecuaciones de Thue.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

$$Y^2 = X^3 + AX + B,$$

siendo $A, B \in \mathbb{Z}$ tales que $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$, y tales que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B.

Entonces, E tiene torsión racional cíclica de orden 7 si y sólo si

$$\begin{aligned} A &= -27k^4(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 - 15q^3p^3 + 30q^2p^4 \\ &\quad -11qp^5 + p^6), \\ B &= 54k^6(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 + 570p^8q^4 - 486p^7q^5 \\ &\quad +273p^6q^6 - 222p^5q^7 + 174p^4q^8 - 46p^3q^9 - 15p^2q^{10} + 6pq^{11} + q^{12}), \end{aligned}$$

con $p, q \in \mathbb{Z}$ tales que $\mathrm{mcd}(p, q) = 1$, $pq \neq 0$, $p \neq q$ y $k = 1$ ó $k = 1/3$.

Además, si se cumplen estas condiciones, los puntos de orden 7 de la curva E son

$$\begin{aligned} P &= (3k^2(p^4 - 6p^3q + 15p^2q^2 - 10pq^3 + q^4), 108k^3(p-q)^3pq^2), \\ 2P &= (3k^2(p^4 - 6p^3q + 3p^2q^2 + 2pq^3 + q^4), -108k^3(p-q)p^2q^3), \\ 3P &= (3k^2(p^4 + 6p^3q - 9p^2q^2 + 2pq^3 + q^4), -108k^3(p-q)^2p^3q), \\ 4P &= (3k^2(p^4 + 6p^3q - 9p^2q^2 + 2pq^3 + q^4), 108k^3(p-q)^2p^3q), \\ 5P &= (3k^2(p^4 - 6p^3q + 3p^2q^2 + 2pq^3 + q^4), 108k^3(p-q)p^2q^3), \\ 6P &= (3k^2(p^4 - 6p^3q + 15p^2q^2 - 10pq^3 + q^4), -108k^3(p-q)^3pq^2). \end{aligned}$$

Demostración.– Por el teorema probado anteriormente, sabemos que si $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/7\mathbb{Z}$, los coeficientes de la curva son

$$A = A(x, v, s) = -x^2 - v^2 - xv + s(x - v),$$

$$B = B(x, v, w, s) = -(3x^3 + x^2w + 3xv^2 - 2xvw + 2v^3 + v^2w + 2s(x-v)(x+v))/4,$$

con

$$s^2 = (v+2x)(x+w+v).$$

$$0 = 3x^2 - xw + xv - w^2 - 3vw + v^2 - 2(x-w)s.$$

Por otra parte, como también vimos en la sección I.G., la curva elíptica de ecuación

$$Y^2 = X^3 + A(x,v,s)X + B(x,v,w,s)$$

tiene un punto de orden 7 si y sólo si esta ecuación es equivalente a la forma normal de Weierstrass de una curva en forma normal de Tate con ecuación

$$Y^2 + (1-\alpha(\alpha-1))XY - \alpha^2(\alpha-1)Y = X^3 - \alpha^2(\alpha-1)X^2,$$

donde $\alpha \in \mathbb{Q}$.

La forma normal de Weierstrass de esta curva es $Y^2 = X^3 + A(\alpha)X + B(\alpha)$, siendo

$$\begin{aligned} A(\alpha) &= -27(\alpha^2-\alpha+1)(\alpha^6 - 11\alpha^5 + 30\alpha^4 - 15\alpha^3 - 10\alpha^2 + 5\alpha + 1), \\ B(\alpha) &= 54 + 324\alpha - 810\alpha^2 - 2484\alpha^3 - 26244\alpha^7 + 30780\alpha^8 + 9396\alpha^4 \\ &\quad +14742\alpha^6 - 11988\alpha^5 - 972\alpha^{11} + 54\alpha^{12} + 6318\alpha^{10} - 19116\alpha^9, \end{aligned}$$

y será equivalente a la forma normal de Weierstrass dada si y sólo si existe $u \in \mathbb{Q}$ tal que

$$\frac{A(x,v,s)}{A(\alpha)} = u^4, \quad \frac{B(x,v,w,s)}{B(\alpha)} = u^6.$$

A partir de estas relaciones, calculando de nuevo bases de Gröbner, conseguimos las siguientes expresiones:

$$\begin{aligned} x &= 3u^2(\alpha^4 - 6\alpha^3 + 15\alpha^2 - 10\alpha + 1), \\ v &= 3u^2(\alpha^4 - 6\alpha^3 + 3\alpha^2 + 2\alpha + 1), \\ w &= 3u^2(\alpha^4 + 6\alpha^3 - 9\alpha^2 + 2\alpha + 1), \\ s &= 9u^2(\alpha^2 - \alpha + 1)(\alpha^2 - 3\alpha + 1). \end{aligned}$$

Sabemos que x, v, w y s son enteros, y vamos a escribir $u = u_1/u_2$, $\alpha = p/q$, siendo u_1, u_2, p, $q \in \mathbb{Z}$, con $\mathrm{mcd}(p,q) = 1 = \mathrm{mcd}(u_1,u_2)$, para estudiar las posibilidades de u_1, u_2, p y q.

Sabemos que $x = x(P) \in \mathbb{Z}$. Veamos que esto implica que q^2 divide a u_1. Sustituyendo $u = u_1/u_2$ y $\alpha = p/q$ en x, y desarrollando se tiene:

$$x = 3\frac{u_1^2}{u_2^2}\left(\frac{p^4 - 6p^3q + 15p^2q^2 - 10pq^3 + q^4}{q^4}\right) \in \mathbb{Z}.$$

De manera análoga a como razonamos en la sección anterior, podemos comprobar que $\mathrm{mcd}(p^4 - 6p^3q + 15p^2q^2 - 10pq^3 + q^4, q^4) = 1$, y así, q^4 debe dividir a $3u_1^2$.

Falta comprobar que si q^4 divide a $3u_1^2$, entonces q^2 divide a u_1, como queríamos ver. Para ello distinguimos dos casos: que q sea múltiplo de 3, o que no lo sea. El segundo caso es trivial, veamos el primero. Escribimos $q = 3^r q_1$, con $r \geq 1$, no siendo q_1 múltiplo de 3, y tendremos que $3^{4r}q_1^4$ divide a $3u_1^2$, por tanto, $3^{4r-1}q_1^4$ divide a u_1^2. Por una parte se tiene que 3^{4r-1} es divisor de u_1^2, de donde (al ser $2r < 4r-1$) se tiene que 3^{2r} divide a u_1, y por otra parte, q_1^4 divide a u_1^2, y así q_1^2 es divisor u_1, por tanto, $3^{2r}q_1^2 = q^2$ divide a u_1.

Llamando u_3 a u_1/q^2 y sustituyendo las expresiones obtenidas para x, v, w y s en $A(x,v,s)$ y $B(x,v,w,s)$, conseguimos

$$\begin{aligned} A &= -27(u_3/u_2)^4(p^2-pq+q^2)(q^6+5q^5p-10q^4p^2-15q^3p^3+30q^2p^4 \\ &\quad -11qp^5+p^6), \\ B &= 54(u_3/u_2)^6(p^{12}-18p^{11}q+117p^{10}q^2-354p^9q^3+570p^8q^4-486p^7q^5 \\ &\quad +273p^6q^6-222p^5q^7+174p^4q^8-46p^3q^9-15p^2q^{10}+6pq^{11}+q^{12}). \end{aligned}$$

Demostremos ahora que $u_2 = 1$ ó 3. Tenemos

$$x = \frac{3u_3^2(p^4-6p^3q+15p^2q^2-10pq^3+q^4)}{u_2^2},$$

$$v = \frac{3u_3^2(p^4-6p^3q+3p^2q^2+2pq^3+q^4)}{u_2^2},$$

$$w = \frac{3u_3^2(p^4+6p^3q-9p^2q^2+2pq^3+q^4)}{u_2^2},$$

$$s = \frac{9u_3^2(p^4-4p^3q+5p^2q^2-4pq^3+q^4)}{u_2^2},$$

y, como $\mathrm{mcd}(u_3,u_2) = 1$, para que x, v, w y s sean enteros, u_2^2 debe dividir a $3(p^4-6p^3q+15p^2q^2-10pq^3+q^4)$, $3(p^4-6p^3q+3p^2q^2+2pq^3+q^4)$, $3(p^4+6p^3q-9p^2q^2+2pq^3+q^4)$, y $9(p^4-4p^3q+5p^2q^2-4pq^3+q^4)$. Restando las dos primeras expresiones se tiene que u_2^2 divide a $36(p^2q^2-pq^3)$, y restando la segunda y la tercera, que u_2^2 divide a $36(p^2q^2-p^3q)$; por tanto, u_2^2 divide al $\mathrm{mcd}(36(p^2q^2-pq^3), 36(p^2q^2-p^3q))$, es decir, a $36(p^2q-pq^2)$. Como también u_2^2 divide a $9(p^4-4p^3q+5p^2q^2-4pq^3+q^4)$, dividirá al $\mathrm{mcd}(36(p^2q-pq^2), 9(p^4-4p^3q+5p^2q^2-4pq^3+q^4))$, es decir, u_2^2 divide a 9, lo que prueba que $u_2 = 1$ ó 3.

Además, al suponer que $\mathrm{mcd}(u_3,u_2) = 1$, y que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B, será $u_3 = 1$.

En resumen, llamando k a $1/u_2$, si nuestra curva de partida, $E: Y^2 = X^3 + AX + B$, tiene torsión racional cíclica de orden 7, hemos probado que

se tiene

$$\begin{aligned} A = A(p,q,k) &= -27k^4(p^2-pq+q^2)(q^6+5q^5p-10q^4p^2-15q^3p^3 \\ &\quad +30q^2p^4-11qp^5+p^6), \\ B = B(p,q,k) &= 54k^6(p^{12}-18p^{11}q+117p^{10}q^2-354p^9q^3+570p^8q^4 \\ &\quad -486p^7q^5+273p^6q^6-222p^5q^7+174p^4q^8-46p^3q^9 \\ &\quad -15p^2q^{10}+6pq^{11}+q^{12}), \end{aligned}$$

con $p, q \in \mathbb{Z}$ tales que $\mathrm{mcd}(p,q) = 1$, y $k = 1$ ó $k = 1/3$.

Además, en estas condiciones, al sustituir en la ecuación de la curva X por x, v y w, podemos calcular los puntos racionales de orden 7, que resultan:

$$\begin{aligned} P &= (3k^2(p^4-6p^3q+15p^2q^2-10pq^3+q^4), 108k^3(p-q)^3pq^2), \\ 2P &= (3k^2(p^4-6p^3q+3p^2q^2+2pq^3+q^4), -108k^3(p-q)p^2q^3), \\ 3P &= (3k^2(p^4+6p^3q-9p^2q^2+2pq^3+q^4), -108k^3(p-q)^2p^3q), \\ 4P &= (3k^2(p^4+6p^3q-9p^2q^2+2pq^3+q^4), 108k^3(p-q)^2p^3q), \\ 5P &= (3k^2(p^4-6p^3q+3p^2q^2+2pq^3+q^4), 108k^3(p-q)p^2q^3), \\ 6P &= (3k^2(p^4-6p^3q+15p^2q^2-10pq^3+q^4), -108k^3(p-q)^3pq^2). \end{aligned}$$

Recíprocamente, se comprueba fácilmente que si una curva elíptica tiene coeficientes $A = A(p,q,k)$ y $B = B(p,q,k)$, entonces su torsión racional es cíclica de orden 7, viendo que el punto $P = (3k^2(p^4-6p^3q+15p^2q^2-10pq^3+q^4), 108k^3(p-q)^3pq^2)$ está en la curva y es de orden 7. $\mathcal{Q.E.D.}$

Observación.– Se puede comprobar que, con las expresiones obtenidas en este teorema, $3x+2s+2v+w$ es el cuadrado de un entero, como debía ser según el primer teorema de esta sección, ya que

$$\begin{aligned} 3x+2v+2s+w &= 3\cdot 3k^2(p^4-6p^3q+15p^2q^2-10pq^3+q^4) \\ &\quad +2\cdot 9k^2(p^4-4p^3q+5p^2q^2-4pq^3+q^4) \\ &\quad +2\cdot 3k^2(p^4-6p^3q+3p^2q^2+2pq^3+q^4) \\ &\quad +3k^2(p^4+6p^3q-9p^2q^2+2pq^3+q^4) \\ &= 36k^2(p-q)^4. \end{aligned}$$

Así, en la práctica, dada una curva elíptica $Y^2 = X^3+AX+B$ con $A, B \in \mathbb{Z}$, para saber si tiene torsión racional cíclica de orden 7, primero comprobamos si existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B, en cuyo caso haríamos el cambio $X \longmapsto k^2X$, $\quad Y \longmapsto k^3Y$. Después, una vez que tenemos las condiciones para aplicar el teorema anterior, tomando $k = 1$, resolvemos el sistema formado por las ecuaciones de Thue $A(p,q,1) = A$, $B(p,q,1) = B$, y si éste tuviera solución entera para p y q, entonces

$\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/7\mathbb{Z}$. Si no, tendríamos que probar con $k = 1/3$, es decir, hacemos el cambio $X \longmapsto (1/3)^2 X$, $Y \longmapsto (1/3)^3 Y$, y volvemos a plantear el mismo sistema de ecuaciones de Thue para razonar como antes. Si tampoco ahora obtenemos solución entera para p y q, entonces $\mathrm{Tor}(E(\mathbb{Q})) \neq \mathbb{Z}/7\mathbb{Z}$.

Ejemplo.– Dada la curva elíptica de ecuación $Y^2 = X^3 - 43X + 166$, planteamos el sistema de Thue

$$\begin{cases} -43 &= -27(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 \\ & \qquad -15q^3p^3 + 30q^2p^4 - 11qp^5 + p^6), \\ 166 &= 54(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 \\ & \qquad +570p^8q^4 - 486p^7q^5 + 273p^6q^6 - 222p^5q^7 \\ & \qquad +174p^4q^8 - 46p^3q^9 - 15p^2q^{10} + 6pq^{11} + q^{12}), \end{cases}$$

que no tiene solución entera en p y q. Con el cambio $X \longmapsto (1/3)^2 X$, $Y \longmapsto (1/3)^3 Y$, conseguimos una curva de ecuación $Y^2 = X^3 - 43 \cdot 3^4 X + 166 \cdot 3^6$ equivalente a la dada. Planteamos ahora el sistema de ecuaciones de Thue

$$\begin{cases} -43 \cdot 3^4 &= -27(p^2 - pq + q^2)(q^6 + 5q^5p - 10q^4p^2 \\ & \qquad -15q^3p^3 + 30q^2p^4 - 11qp^5 + p^6), \\ 166 \cdot 3^6 &= 54(p^{12} - 18p^{11}q + 117p^{10}q^2 - 354p^9q^3 \\ & \qquad +570p^8q^4 - 486p^7q^5 + 273p^6q^6 - 222p^5q^7 \\ & \qquad +174p^4q^8 - 46p^3q^9 - 15p^2q^{10} + 6pq^{11} + q^{12}), \end{cases}$$

que tiene, por ejemplo, la solución $\{p = 2, q = 1\}$, lo que implica que la curva $Y^2 = X^3 - 43 \cdot 3^4 X + 166 \cdot 3^6$ tiene torsión racional $\mathbb{Z}/7\mathbb{Z}$. Sustituyendo esta solución en las expresiones dadas en el teorema anterior para las coordenadas de los puntos racionales de torsión, podemos afirmar que éstos son:

$$\Big\{\mathcal{O}, Q = (27, 216),\ 2Q = (-45, -432),\ 3Q = (99, -864),$$
$$4Q = (99, 864),\ 5Q = (-45, 432),\ 6Q = (27, -216)\Big\}.$$

Ahora, deshaciendo el cambio, resulta que la curva $Y^2 = X^3 - 43X + 166$, tiene torsión racional $\mathbb{Z}/7\mathbb{Z}$, dada por los puntos

$$\Big\{\mathcal{O}, P = (3, 8),\ 2P = (-5, -16),\ 3P = (11, -32),$$
$$4P = (11, 32),\ 5P = (-5, 16),\ 6P = (3, -8)\Big\}.$$

Observación.– Podemos comprobar, como en la sección anterior, que las expresiones $A(p, q, 1)$ y $B(p, q, 1)$ se pueden obtener directamente a partir de

$A(\alpha)$ y $B(\alpha)$, sustituyendo α por p/q. Aunque con el teorema anterior, no sólo hemos conseguido expresiones para A y B, sino que hemos conseguido además las coordenadas de los puntos racionales de torsión en función de p y q.

III.F. Torsión racional cíclica de orden 9

Cuando una curva elíptica E no tiene puntos racionales de orden 2, y tiene algún punto racional de orden 9, por el teorema de Mazur, sabemos que $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/9\mathbb{Z}$.

En esta sección caracterizaremos, mediante ecuaciones diofánticas, los coeficientes de las curvas elípticas en forma breve de Weierstrass que tiene torsión racional cíclica de orden 9.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

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

tal que $x^3 + Ax + B \neq 0$, $\forall X \in \mathbb{Q}$.

Entonces, E tiene algún punto $P = (x, y)$ de orden 9 si y sólo si

$$A = 27m^4 + 6nm, \quad B = n^2 - 27m^6,$$

con $m, n \in \mathbb{Z}$ tales que $n \neq -9m^3$, $n^2 \neq 27m^6$, y $3m^2 = x(3P)$.

Demostración.– En una curva elíptica $Y^2 = X^3+AX+B$ con $A, B \in \mathbb{Z}$, el punto $P = (x, y)$ es de orden 9 si y sólo si $3P$ es de orden 3. Entonces, según III.C., por tener la curva un punto de orden 3, los coeficientes A y B deben ser de la forma $A = 27m^4 + 6nm$, $B = n^2 - 27m^6$, con $m, n \in \mathbb{Z}$, y el punto $3P$ tendrá coordenadas $(3m^2, \pm(9m^3 + n))$.

Como la coordenada $x(3P) = 3m^2 \in \mathbb{Z}$, se tendrá $m \in \mathbb{Z}$, y al ser $B \in \mathbb{Z}$, se tendrá también $n \in \mathbb{Z}$. $\mathcal{Q}.\mathcal{E}.\mathcal{D}$.

Observación.– Si $P = (x, y)$ es un punto racional de la curva, la primera coordenada de $3P$ es

$$x(3P) = (x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3$$

$$+48A^2Bx^2 + (96AB^2 + 9A^4)x + 8B(A^3 + 8B^2))/(3x^4 + 6Ax^2 + 12Bx - A^2)^2,$$

y como $P = (x, y)$ es de orden 9 si y sólo si $3P$ es de orden 3, tenemos que $P = (x, y)$ es de orden 9 si y sólo si

$$x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3 + 48A^2Bx^2$$

$$+(96AB^2 + 9A^4)x + 8B(A^3 + 8B^2) - 3m^2(3x^4 + 6Ax^2 + 12Bx - A^2)^2 = 0.$$

Si en esta expresión sustituimos A por $27m^4 + 6nm$ y B por $n^2 - 27m^6$, obtenemos una ecuación de grado 9 en x con coeficientes en n y m. Como una curva elíptica sólo puede tener 6 puntos de orden 9, (opuestos tres de ellos a los otros tres), este ecuación sólo puede tener 3 raíces enteras diferentes.

Así, en la práctica, para averiguar si una curva elíptica dada $Y^2 = X^3 + AX + B$ con $A, B \in \mathbb{Z}$, tiene torsión racional cíclica de orden 9, primero resolvemos el sistema diofántico

$$\begin{aligned} 27m^4 + 6nm &= A, \\ n^2 - 27m^6 &= B. \end{aligned}$$

Si no hay solución entera para m y n, entonces la curva no tiene puntos racionales de orden 9, pero si la hay, para cada solución (m, n) procedemos de la siguiente manera: sustituimos el valor obtenido para m y los valores dados de A y B en la ecuación

$$x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3 + 48A^2Bx^2$$

$$+(96AB^2 + 9A^4)x + 8B(A^3 + 8B^2) - 3m^2(3x^4 + 6Ax^2 + 12Bx - A^2)^2 = 0,$$

y buscamos sus raíces enteras. Si no hay, entonces la curva no tiene puntos racionales de orden 9, pero si hay raíces enteras, entonces habrá tres, x, v y w, que serán las primeras coordenadas de los puntos racionales de orden 9 de la curva.

Ejemplo.– Dada la curva elíptica de ecuación $Y^2 = X^3 - 219X + 1654$, planteamos el sistema

$$\begin{aligned} 27m^4 + 6nm &= -219, \\ n^2 - 27m^6 &= 1654, \end{aligned}$$

que tiene las soluciones $\{m = -1,\ n = 41\}$ y $\{m = 1,\ n = -41\}$. Al sustituir $m = 1$, $A = -219$ y $B = 1654$ en el polinomio

$$x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + (36A^3 + 48B^2)x^3 + 48A^2Bx^2$$

$$+(96AB^2 + 9A^4)x + 8B(A^3 + 8B^2) - 3m^2(3x^4 + 6Ax^2 + 12Bx - A^2)^2,$$

resulta

$$x^9 - 27x^8 + 2628x^7 - 135132x^6 + 1081566x^5 + 4376934x^4 - 90328524x^3$$

$$+2247765876x^2 - 31101795927x + 143709410845,$$

y al factorizar obtenemos

$$(x-35)(x-11)(x+13)(x^6 + 6x^5 + 3039x^4 - 38572x^3$$

$$+425967x^2 - 4992186x + 28713169).$$

Por tanto, 35, 11 y -13 son las primeras coordenadas de los puntos racionales de orden 9 de la curva, y los de orden 3 tendrán primera coordenada $3m^2 = 3$. Sustituyendo estos valores de X en la ecuación de la curva tendremos

$$\Big\{\mathcal{O}, P = (35, 192),\ 2P = (11, -24),\ 3P = (3, 32),\ 4P = (-13, 48),$$
$$5P = (-13, -48),\ 6P = (3, -32),\ 7P = (11, 24),\ 8P = (35, -192)\Big\}.$$

Como en secciones anteriores, también usaremos ecuaciones de Thue para caracterizar ahora las curvas elípticas cuya torsión racional es de orden 9.

Teorema.– Sea E una curva elíptica cuya parte afín verifica la ecuación

$$Y^2 = X^3 + AX + B,$$

siendo $A, B \in \mathbb{Z}$ tales que $x^3 + Ax + B \neq 0$, $\forall x \in \mathbb{Q}$, y tales que no existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B.

Entonces, E tiene torsión racional cíclica de orden 9 si y sólo si

$$\begin{aligned} A &= -27k^4(q^3 - 3p^2q + p^3)(q^9 - 9q^7p^2 + 27q^6p^3 - 45q^5p^4 + 54q^4p^5 \\ &\quad -48q^3p^6 + 27p^7q^2 - 9p^8q + p^9), \\ B &= 54k^6(p^{18} - 18p^{17}q + 135p^{16}q^2 - 570p^{15}q^3 + 1557p^{14}q^4 \\ &\quad -2970p^{13}q^5 + 4128p^{12}q^6 - 4230p^{11}q^7 + 3240p^{10}q^8 \\ &\quad -2032p^9q^9 + 1359p^8q^{10} - 1080p^7q^{11} + 735p^6q^{12} \\ &\quad -306p^5q^{13} + 27p^4q^{14} + 42p^3q^{15} - 18p^2q^{16} + q^{18}), \end{aligned}$$

con $p, q \in \mathbb{Z}$ tales que $\mathrm{mcd}(p, q) = 1$, $pq \neq 0$, $p \neq q$ y $k = 1$ ó $k = 1/3$.

Además, si se cumplen estas condiciones, los puntos racionales de torsión de la curva E son

$$\begin{aligned}
P &= (3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6),\\
&\quad 108k^3p^4q(p^4-3p^3q+4p^2q^2-3pq^3+q^4)),\\
2P &= (3k^2(p^6-6p^5q+21p^4q^2-34p^3q^3+30p^2q^4-12pq^5+q^6),\\
&\quad -108k^3pq^2(p^6-5p^5q+11p^4q^2-14p^3q^3+11p^2q^4-5pq^5+q^6)),\\
3P &= (3k^2(q^3-3p^2q+p^3)^2, 108k^3p^3q^3(p^3-3p^2q+3pq^2+q^3),\\
4P &= (3k^2(p^6-6p^5q+9p^4q^2-10p^3q^3+6p^2q^4+q^6),\\
&\quad 108k^3p^2q^4(p^3-2p^2q+2pq^2p-q^3)),\\
5P &= (3k^2(p^6-6p^5q+9p^4q^2-10p^3q^3+6p^2q^4+q^6),\\
&\quad -108k^3p^2q^4(p^3-2p^2q+2pq^2p-q^3)),\\
6P &= (3k^2(q^3-3p^2q+p^3)^2, -108k^3p^3q^3(p^3-3p^2q+3pq^2+q^3),\\
7P &= (3k^2(p^6-6p^5q+21p^4q^2-34p^3q^3+30p^2q^4-12pq^5+q^6),\\
&\quad -108k^3pq^2(p^6-5p^5q+11p^4q^2-14p^3q^3+11p^2q^4-5pq^5+q^6)),\\
8P &= (3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6),\\
&\quad 108k^3p^4q(p^4-3p^3q+4p^2q^2-3pq^3+q^4)).
\end{aligned}$$

Demostración.– Sabemos que, por el teorema anterior, los coeficientes de la curva deben ser

$$A = A(m,n) = 27m^4+6nm, \qquad B = B(m,n) = n^2-27m^6,$$

con $m, n \in \mathbb{Z}$.

Por otra parte, en la sección I.G. vimos que una curva elíptica $Y^2 = X^3+AX+B$ con $A, B \in \mathbb{Z}$, tiene un punto racional de orden 9 si y sólo si es equivalente a la forma normal de Weierstrass de una curva en forma normal de Tate con ecuación

$$Y^2+(1-\alpha^2(\alpha-1))XY-\alpha^2(\alpha-1)(\alpha^2-\alpha+1)Y = X^3-\alpha^2(\alpha-1)(\alpha^2-\alpha+1)X^2$$

donde $\alpha \in \mathbb{Q}$.

La forma normal de Weierstrass de esta curva es $Y^2 = X^3+A(\alpha)X+B(\alpha)$, con

$$\begin{aligned}
A(\alpha) &= -27\alpha^{12}+324\alpha^{11}-1458\alpha^{10}+3456\alpha^9-5103\alpha^8\\
&\quad +4860\alpha^7-3078\alpha^6+972\alpha^5+486\alpha^4-756\alpha^3\\
&\quad +324\alpha^2-27,\\
B(\alpha) &= +54\alpha^{18}-972\alpha^{17}+7290\alpha^{16}-30780\alpha^{15}+84078\alpha^{14}\\
&\quad -160380\alpha^{13}+222912\alpha^{12}-228420\alpha^{11}+174960\alpha^{10}\\
&\quad -109728\alpha^9+73386\alpha^8-58320\alpha^7+39690\alpha^6\\
&\quad -16524\alpha^5+1458\alpha^4+2268\alpha^3-972\alpha^2+54,
\end{aligned}$$

y será equivalente a la forma normal de Weierstrass dada si y sólo si $\exists u \in \mathbb{Q}$ tal que

$$\frac{A(m,n)}{A(\alpha)} = u^4 \quad \text{y} \quad \frac{B(m,n)}{B(\alpha)} = u^6,$$

y esto ocurre si y sólo si

$$\begin{aligned} m &= u(1-3\alpha^2+\alpha^3), \\ n &= -9m^3 + 108u^3\alpha^3(\alpha-1)^3, \end{aligned}$$

con $u,\ \alpha \in \mathbb{Q}$. (También si n y m cambian las dos su signo, pero esto daría las mismas A y B.)

Si sustituimos ahora n y m en función de u y α en el polinomio de grado 9 cuyas raíces enteras eran $x(P)$, $x(2P)$ y $x(4P)$, resulta un polinomio de grado 9 en x con coeficientes en u y α, y al factorizarlo obtenemos las 3 raíces siguientes:

$$\begin{aligned} x(P) &= 3m^2 - 4(3u)^2\alpha^2(\alpha-1), \\ x(2P) &= 3m^2 + 4(3u)^2\alpha^3(\alpha-1)^2, \\ x(4P) &= 3m^2 + 4(3u)^2\alpha(\alpha-1)^3. \end{aligned}$$

Como n y m son enteros, vamos a escribir $u = u_1/u_2$, $\alpha = p/q$, con $p,\ q,\ u_1,\ u_2 \in \mathbb{Z}$, $\mathrm{mcd}(p,q) = 1 = \mathrm{mcd}(u_1,u_2)$, y estudiamos las posibilidades de $p,\ q,\ u_1,\ \text{y}\ u_2$.

Sabemos que $x(P) \in \mathbb{Z}$. Veamos que esto implica que q^3 divide a u_1. Sustituyendo $u = u_1/u_2$ y $\alpha = p/q$ en $x(P)$, y desarrollando se tiene:

$$x(P) = 3\frac{u_1^2}{u_2^2}\Big(\frac{p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6}{q^6}\Big) \in \mathbb{Z}.$$

Comprobamos que $\mathrm{mcd}(p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6, q^6) = 1$, y así, q^6 debe dividir a u_1^2, por tanto q^3 divide a u_1, como queríamos ver.

Demostramos ahora que $u_2 = 1$ ó 3. Como $x(P), m \in \mathbb{Z}$, se tiene $x(P) - 3m^2 = -4(3u)^2\alpha^2(\alpha-1) \in \mathbb{Z}$, y por ser $u_3 := u_1/q^3 \in \mathbb{Z}$, resulta

$$-4\frac{3^2u_3^2q^6}{u_2^2}\cdot\frac{p^2}{q^2}\cdot\frac{p-q}{q} = -2^2\cdot 3^2u_3^2q^3\frac{p^2(p-q)}{u_2^2} \in \mathbb{Z}.$$

Escribimos $u_2 = 2^r3^su_4$, con $r = 1$ si 2 divide a u_2 y $r = 0$ en caso contrario, y lo mismo para s y 3. Al sustituir resulta

$$-2^2\cdot 3^2u_3^2q^3\frac{p^2(p-q)}{2^{2r}3^{2s}u_4^2} \in \mathbb{Z},$$

y como $\mathrm{mcd}(u_3, u_2) = 1 = \mathrm{mcd}(q, u_2) = 1$, será

$$\frac{-2^2 \cdot 3^2 p^2 (p-q)}{2^{2r} 3^{2s} u_4^2} \in \mathbb{Z}.$$

Vamos a distinguir varios casos.

- Si ni 2 ni 3 dividen a u_2, serán $r = s = 0$ y $u_4 = u_2$. En este caso, se tiene que u_2^2 divide a $p^2(p-q)$. Veamos que esto implica que $q^6 \equiv 0 (mod\ u_2^2)$, (i.e. que u_2 dividea q^3.)Sabemos que

  $$x(P) = 3u_3^2 \cdot \frac{p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6}{u_2^2} \in \mathbb{Z},$$

  y como 3 no divide a u_2 y $\mathrm{mcd}(u_3, u_2) = 1$,

  $$p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6 \equiv 0 \pmod{u_2^2},$$

  por tanto, $p^2(p-q)(p^3 - 5p^2q + 4pq^2 - 6q^3) \equiv -q^6 \pmod{u_2^2}$, y al dividir $p^2(p-q)$ a u_2^2, resulta $0 \equiv -q^6 \pmod{u_2^2}$, es decir, u_2 divide a q^3.

  Por tanto, si ni 2 ni 3 dividen a u_2, tenemos que u_2 divide a q^3 y q^3 divide a u_1, es decir, u_2 divide a u_1, y como u_1 y u_2 son primos entre sí, esto significa que ha de ser $u_2 = 1$.

- Si 2 divide a u_2, 3 no divide a u_2 y $2 \neq u_2$, serán $r = 1$, $s = 0$ y $u_2 = 2u_4$, con $u_4 \neq 1$. En este caso, se tiene que u_4^2 divide a $p^2(p-q)$. Razonando con u_4 de forma análoga a como lo hicimos con u_2 en el caso anterior, se llegaría a que u_4 divide a u_1, y como u_4 divide a u_2, y $\mathrm{mcd}(u_1, u_2) = 1$, esto sería una contradicción con que $u_4 \neq 1$.

- Si 2 no divide a u_2, 3 divide a u_2 y $3 \neq u_2$, serán $r = 0$, $s = 1$ y $u_2 = 3u_5$, con $u_5 \neq 1$. En este caso, se tiene que u_5^2 divide a $p^2(p-q)$. Veamos que esto implica que $q^6 \equiv 0 \pmod{u_5^2}$, es decir, que u_5 divide a q^3. Tenemos

  $$x(P) = u_3^2 \left(\frac{p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6}{3u_5^2} \right) \in \mathbb{Z},$$

  luego, al ser $\mathrm{mcd}(u_3, u_2) = 1$,

  $$p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6 \equiv 0 \pmod{u_5^2},$$

  por tanto, $p^2(p-q)(p^3 - 5p^2q + 4pq^2 - 6q^3) \equiv -q^6 \pmod{u_5^2}$, y como u_5^2 divide a $p^2(p-q)$, se tendrá $0 \equiv -q^6 (mod\ u_5^2)$. Así, tenemos que u_5 divide a q^3 y q^3 divide a u_1, es decir, u_5 divide a u_1, y como u_5 divide a u_2 y $\mathrm{mcd}(u_1, u_2) = 1$, esto contradice que $u_5 \neq 1$.

- Si 6 divide a u_2, y 6 $\neq u_2$, serán $r = 1$, $s = 1$ y $u_2 = 6u_6$, con $u_6 \neq 1$. Repitiendo el razonamiento del caso anterior, llegamos a la misma contradicción.

- Si $u_2 = 2$ resulta

$$x(P) = 3u_3^2 \left(\frac{p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6}{2^2} \right) \in \mathbb{Z},$$

luego, al ser $\text{mcd}(u_3,\ u_2 = 2) = 1$, será

$$p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6 \equiv 0 \pmod{2^2}.$$

Tomando todas las congruencias posibles módulo 4 para p y q, la expresión $p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6$ toma valores que no son múltiplos de 4, salvo en el caso en el que $p \equiv q \equiv 2 \pmod 4$, que no sirve porque $\text{mcd}(p,\ q) = 1$. Por tanto, el hecho de ser $x(P)$ entero, obliga a que $u_2 \neq 2$.

- Si $u_2 = 6$, se tiene

$$x(P) = 3u_3^2 \left(\frac{p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6}{6^2} \right) \in \mathbb{Z},$$

y como $\text{mcd}(u_3,\ u_2 = 6) = 1$, tendrá que ser

$$p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6 \equiv 0 \pmod{12}.$$

Tomando todas las posibles congruencias módulo 12 para p y q primos entre sí, vemos que en ningún caso la expresión $p^6 - 6p^5q + 9p^4q^2 - 10p^3q^3 + 6p^2q^4 + q^6$ es múltiplo de 12. Por tanto, ha de ser $u_2 \neq 6$.

Queda así demostrado que las únicas posibilidades son $u_2 = 1$ ó $u_2 = 3$.

En resumen, tenemos que una curva elíptica en forma normal de Weierstrass con grupo de torsión $\mathbb{Z}/9\mathbb{Z}$ tiene ecuación $Y^2 = X^3 + (27m^4 + 6nm)X + (n^2 - 27m^6)$, con m y n enteros verificando

$$\begin{aligned} m &= u_3(q^3 - 3p^2q + p^3)/u_2, \\ n &= -9m^3 + 108u_3^3p^3(p-q)^3q^3/u_2^3, \end{aligned}$$

siendo $u_2 = 1$ ó 3 y $u_3, p, q \in \mathbb{Z}$ tales que $\text{mcd}(p,q) = 1 = \text{mcd}(u_3, 3)$.

Sustituyendo m y n en las expresiones de $A(m,n)$ y $B(m,n)$ tenemos

$$\begin{aligned} A &= -27u_3^4(q^3-3p^2q+p^3)(q^9-9q^7p^2+27q^6p^3-45q^5p^4+54q^4p^5 \\ &\quad -48q^3p^6+27p^7q^2-9p^8q+p^9)/u_2^4, \\ B &= 54u_3^6(p^{18}-18p^{17}q+135p^{16}q^2-570p^{15}q^3+1557p^{14}q^4 \\ &\quad -2970p^{13}q^5+4128p^{12}q^6-4230p^{11}q^7+3240p^{10}q^8 \\ &\quad -2032p^9q^9+1359p^8q^{10}-1080p^7q^{11}+735p^6q^{12} \\ &\quad -306p^5q^{13}+27p^4q^{14}+42p^3q^{15}-18p^2q^{16}+q^{18})/u_2^6, \end{aligned}$$

pero como suponíamos que no existe ningún entero que elevado a la cuarta divida a A y a la sexta divida a B, tendremos que $u_3 = 1$, y llamando k a $1/u_2$, llegamos a las expresiones de A y B del enunciado del teorema.

Además, al sustituir A, B y m por sus expresiones en función de k, p y q en

$$x^9-12Ax^7-96Bx^6+30A^2x^5-24ABx^4+(36A^3+48B^2)x^3+48A^2Bx^2$$

$$+(96AB^2+9A^4)x+8B(A^3+8B^2)-3m^2(3x^4+6Ax^2+12Bx-A^2)^2,$$

que era un polinomio cuyas únicas raíces enteras eran $x(P)$, $x(2P)$ y $x(4P)$, para un punto P de orden 9, obtenemos

$$\begin{aligned} x(P) &= 3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6), \\ x(2P) &= 3k^2(p^6-6p^5q+21p^4q^2-34p^3q^3+30p^2q^4-12pq^5+q^6), \\ x(4P) &= 3k^2(p^6-6p^5q+9p^4q^2-10p^3q^3+6p^2q^4+q^6). \end{aligned}$$

Por otra parte, los puntos de orden 3 de la curva tiene como primera coordenada

$$x(3P) = 3m^2 = 3k^2(p^3-3p^2q+q^3)^2,$$

por tanto, sustituyendo en la ecuación de la curva dada, obtenemos

$$\mathrm{Tor}(E(\mathbb{Q})) = \{\mathcal{O}, P, ..., 8P\} \cong \mathbb{Z}/9\mathbb{Z},$$

siendo

$$\begin{aligned}
P &= (3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6),\\
&\quad 108k^3p^4q(p^4-3p^3q+4p^2q^2-3pq^3+q^4)),\\
2P &= (3k^2(p^6-6p^5q+21p^4q^2-34p^3q^3+30p^2q^4-12pq^5+q^6),\\
&\quad -108k^3pq^2(p^6-5p^5q+11p^4q^2-14p^3q^3+11p^2q^4-5pq^5+q^6)),\\
3P &= (3k^2(q^3-3p^2q+p^3)^2, 108k^3p^3q^3(p^3-3p^2q+3pq^2+q^3),\\
4P &= (3k^2(p^6-6p^5q+9p^4q^2-10p^3q^3+6p^2q^4+q^6),\\
&\quad 108k^3p^2q^4(p^3-2p^2q+2pq^2p-q^3)),\\
5P &= (3k^2(p^6-6p^5q+9p^4q^2-10p^3q^3+6p^2q^4+q^6),\\
&\quad -108k^3p^2q^4(p^3-2p^2q+2pq^2p-q^3)),\\
6P &= (3k^2(q^3-3p^2q+p^3)^2, -108k^3p^3q^3(p^3-3p^2q+3pq^2+q^3),\\
7P &= (3k^2(p^6-6p^5q+21p^4q^2-34p^3q^3+30p^2q^4-12pq^5+q^6),\\
&\quad -108k^3pq^2(p^6-5p^5q+11p^4q^2-14p^3q^3+11p^2q^4-5pq^5+q^6)),\\
8P &= (3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6),\\
&\quad 108k^3p^4q(p^4-3p^3q+4p^2q^2-3pq^3+q^4)).
\end{aligned}$$

Recíprocamente, se comprueba fácilmente que si una curva elíptica tiene coeficientes $A = A(p,q,k)$ y $B = B(p,q,k)$, con las expresiones dadas en el enunciado, entonces su torsión racional es cíclica de orden 9, viendo que el punto $P = (3k^2(p^6+6p^5q-15p^4q^2+14p^3q^3-6p^2q^4+q^6), 108k^3p^4q(p^4-3p^3q+4p^2q^2-3pq^3+q^4))$ está en la curva y es de orden 9. $\mathcal{Q}.\mathcal{E}.\mathcal{D}.$

Observación.– Para la aplicación de este teorema en la práctica, dada una curva elíptica $Y^2 = X^3 + AX + B$ con $A, B \in \mathbb{Z}$, procedemos como en el caso de orden 7. Primero comprobamos si existe $k \in \mathbb{Z}$ tal que k^4 divida a A y k^6 divida a B, en cuyo caso tendríamos que hacer el cambio $X \longmapsto k^2X$, $Y \longmapsto k^3Y$. Después, una vez que estamos en las condiciones de usar el teorema, tomando $k = 1$, resolvemos el sistema formado por las ecuaciones de Thue $A(p,q) = A$, $B(p,q) = B$, y si éste tuviera solución entera para p y q, entonces $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/9\mathbb{Z}$. Si no, tendríamos que probar con $k = 1/3$, es decir, hacemos el cambio $X \longmapsto (1/3)^2X$, $Y \longmapsto (1/3)^3Y$, y volvemos a plantear el mismo sistema de ecuaciones de Thue para razonar como antes. Ahora, $\mathrm{Tor}(E(\mathbb{Q})) = \mathbb{Z}/9\mathbb{Z}$ si y sólo si obtenemos solución entera para p y q en este segundo sistema de Thue.

Ejemplo.– Dada la curva elíptica de ecuación $Y^2 = X^3 - 219X + 1654$,

planteamos el sistema de Thue

$$\left\{\begin{array}{rcl} -219 & = & -27(q^3-3p^2q+p^3)(q^9-9q^7p^2+27q^6p^3-45q^5p^4+54q^4p^5 \\ & & -48q^3p^6+27p^7q^2-9p^8q+p^9), \\ 1654 & = & 54(p^{18}-18p^{17}q+135p^{16}q^2-570p^{15}q^3+1557p^{14}q^4 \\ & & -2970p^{13}q^5+4128p^{12}q^6-4230p^{11}q^7+3240p^{10}q^8 \\ & & -2032p^9q^9+1359p^8q^{10}-1080p^7q^{11}+735p^6q^{12} \\ & & -306p^5q^{13}+27p^4q^{14}+42p^3q^{15}-18p^2q^{16}+q^{18}), \end{array}\right.$$

que no tiene solución entera en p y q como se puede comprobar. Con el cambio $X \longmapsto (1/3)^2X$, $Y \longmapsto (1/3)^3Y$, conseguimos una curva de ecuación $Y^2 = X^3 - 219 \cdot 3^4X + 1654 \cdot 3^6$ equivalente a la dada. Planteamos ahora el sistema de ecuaciones de Thue

$$\left\{\begin{array}{rcl} -219\cdot 3^4 & = & -27(q^3-3p^2q+p^3)(q^9-9q^7p^2+27q^6p^3-45q^5p^4 \\ & & +54q^4p^5-48q^3p^6+27p^7q^2-9p^8q+p^9), \\ 1654\cdot 3^6 & = & 54(p^{18}-18p^{17}q+135p^{16}q^2-570p^{15}q^3+1557p^{14}q^4 \\ & & -2970p^{13}q^5+4128p^{12}q^6-4230p^{11}q^7+3240p^{10}q^8 \\ & & -2032p^9q^9+1359p^8q^{10}-1080p^7q^{11}+735p^6q^{12} \\ & & -306p^5q^{13}+27p^4q^{14}+42p^3q^{15}-18p^2q^{16}+q^{18}), \end{array}\right.$$

que tiene, entre otras, la solución $\{p = 2, q = 1\}$, por lo que la curva $Y^2 = X^3 - 219 \cdot 3^4X + 1654 \cdot 3^6$ tiene torsión racional $\mathbb{Z}/9\mathbb{Z}$. Sustituyendo esta solución en las expresiones dadas en el teorema anterior para las coordenadas de los puntos racionales de torsión, tendremos:

$$\Big\{\mathcal{O}, Q = (315, 5184), 2Q = (99, -648), 3Q = (27, 864), 4Q = (-117, 1296),$$

$$5Q = (-117, -1296), 6Q = (27, -864), 7Q = (99, 648), 8Q = (315, -5184)\Big\}.$$

Y deshaciendo el cambio, tenemos que los puntos de torsión racional de la curva $Y^2 = X^3 - 219X + 1654$ son

$$\Big\{\mathcal{O}, P = (35, 192),\ 2P = (11, -24),\ 3P = (3, 32),\ 4P = (-13, 48),$$

$$5P = (-13, -48),\ 6P = (3, -32),\ 7P = (11, 24),\ 8P = (35, -192)\Big\}.$$

Observación.– También en el caso de orden 9, podemos comprobar que las expresiones $A(p, q)$ y $B(p, q)$ se pueden obtener directamente a partir de $A(\alpha)$ y $B(\alpha)$, sustituyendo α por p/q. Aunque a diferencia de la caracterización de Tate, la de Thue proporciona además las coordenadas de los puntos racionales de torsión.

Apéndice: Complementos computacionales

A.1. Programas de MAPLE

Por motivos de compatibildad con el compilador, en esta sección no aparecen tildes.

```
#
# Este archivo contiene diversas rutinas para calcular torsion
# de curvas elipticas sobre los racionales usando la forma
# normal de Tate. Las entradas y salidas de datos son bastante
# naturales.
#

with(numtheory):

#
# El primer programa, BP, calcula los cinco primeros
# buenos primos de una curva eliptica dada en forma de
# Weierstrass. Es facilmente adaptable a una cantidad mayor o
# menor de primos.
#

BP:= proc(l::list)
   local A,B,BP,Delta,i,p:
   A:= l[1]:
   B:= l[2]:
   Delta:= 4*A^3+27*B^2:
   BP:= []:
   for i from 2 to 1000 do
```

```
      p:= ithprime (i):
      if irem(Delta,p)<>0 then
         BP:= [op(BP),p]:
         if nops(BP)= 5 then
            RETURN(BP);
         fi:
      fi:
   od:
end:

#
# El segundo programa, NDP, calcula el numero de puntos de
# una curva eliptica sobre un cuerpo finito de p elementos
# de forma elemental, ya que no esta pensado para ser utilizado
# con primos grandes. Tambien da en la salida de datos el
# numero de elementos de orden 2 del grupo de la curva sobre
# dicho cuerpo, para afinar la posterior acotacion en ciertos
# casos.
#

NDP:= proc(l::list)
   local A,B,i,j,k,m,n,p:
   A:= l[1]:
   B:= l[2]:
   p:= l[3]:
   k:= 0:
   j:= 0:
   for i from 0 to p-1 do
      if irem(i**3+A*i+B,p)=0 then
         j:= j+1:
         k:= k+1:
      else for m from 1 to p-1 do
         if irem(m**2-(i^3+A*i+B),p)=0 then
            k:= k+1:
         fi:
      od:
      fi:
   od:
   RETURN([k+1,j]);
end:
```

```
#
# El programa RS calcula el numero de puntos de orden 2 de
# una curva eliptica.
#

RS:= proc(l::list)
   local A,B,i,k,sols:
   A:= l[1]:
   B:= l[2]:
   sols:= map(simplify,[solve(X^3+A*X+B)]):
   k:= 0:
   for i from 1 to nops(sols) do
      if type(sols[i],rational) then
         k:= k+1:
      fi:
   od:
   RETURN(k):
end:

#
# La rutina SWFORM calcula la forma breve de Weierstrass de
# una curva eliptica, a partir de la ecuacion general (larga).
# La entrada de datos es la lista de coeficientes en el orden
# habitual de escritura de la forma larga; esto es: a1,a3,a2,
# a4,a6
#

SWFORM:= proc(l::list)
   local a1,a2,a3,a4,a6,A,B:
   a1:= l[1]:
   a3:= l[2]:
   a2:= l[3]:
   a4:= l[4]:
   a6:= l[5]:
   A:= -27*a1^4-216*a1^2*a2-432*a2^2+1296*a4+648*a1*a3:
   B:= 54*a1^6+648*a1^4*a2+2592*a1^2*a2^2+3456*a2^3
       -3888*a1^2*a4-1944*a1^3*a3-15552*a2*a4-7776*a2*a1*a3
       +11664*a3^2+46656*a6:
   RETURN([A,B]);
end:
```

```
#
# BOUND calcula una cota (para el orden parcial de la
# divisibilidad en Z) del orden del grupo de torsion de una
# curva eliptica, usando las rutinas anteriores.
#

BOUND:= proc(l::list)
   local A,B,BOUND,GP,k,p:
   A:= l[1]:
   B:= l[2]:
   GP:= BP([A,B]):
   BOUND:= 0:
   for k from 1 to 5 do
      if NDP([A,B,GP[k]])[2]>RS([A,B]) then
         BOUND:= igcd(BOUND,NDP([A,B,GP[k]])[1]/2);
      else
         BOUND:= igcd(BOUND,NDP([A,B,GP[k]])[1]);
      fi:
   od:
   RETURN(BOUND);
end:

#
# La rutina DEC estudia si existe un punto o no de orden p dado
# en una curva eliptica, con entrada de datos [A,B,p].
#

DEC:= proc(l::list)
   local A,B,A_aux,B_aux,i,j,k,lista_aux,lista_aux2,lista_rac,
         lista_sol,eca_aux,ecb_aux,p:
   A:= l[1]:
   B:= l[2]:
   p:= l[3]:
   A_aux:= array(1..9):
   B_aux:= array(1..9):
   A_aux[4]:= -(1/3*f+1/48+1/3*f^2):
   B_aux[4]:= -(-1/36*f-5/36*f^2+2/27*f^3-1/864):
   A_aux[5]:= -(7/24*f^2+1/48*f^4+1/4*f+1/48-1/4*f^3):
   B_aux[5]:= -(-1/48*f-25/288*f^2-1/864*f^6-1/864-25/288*f^4
               +1/48*f^5):
   A_aux[6]:= -(1/48+1/4*f+1/4*f^3+3/16*f^4+5/8*f^2):
```

```
B_aux[6]:= -(-1/48*f-11/96*f^2-5/24*f^3+1/16*f^5-1/864
            -5/32*f^4+1/32*f^6):
A_aux[7]:= -(35/48*f^4+1/48+7/8*f^6-7/6*f^5-7/24*f^2+1/12*f
            +1/48*f^8-1/4*f^7):
B_aux[7]:= -(-1/144*f-29/144*f^4-91/288*f^6-1/864+9/16*f^7
            -13/96*f^10-95/144*f^8-1/864*f^12+1/48*f^11
            +59/144*f^9+23/432*f^3+5/288*f^2+37/144*f^5):
A_aux[8]:= -(-(1/3)*(1/f^3)+10-6*1/f-28/3*f+2*1/f^2-4/3*f^3
            +1/48*1/f^4+14/3*f^2+1/3*f^4):
B_aux[8]:= -(2/27*f^6+110/27*f^3-95/18*1/f^2-5/18*1/f^4
            +107/9*1/f-4/9*f^5+83/54*1/f^3+55/3*f
            +1/36*1/f^5-143/12*f^2-973/54-1/864*1/f^6):
A_aux[9]:= -(1/4*f^11-7/12*f^3-1/4*f^2-3/8*f^4+3/4*f^5
            +15/4*f^7+19/8*f^6+63/16*f^8+1/48+9/8*f^10
            +8/3*f^9+1/48*f^12):
B_aux[9]:= -(-151/96*f^8-5/4*f^7+1/48*f^2+7/144*f^3
            -15/4*f^10-55/16*f^13-17/48*f^5-1/32*f^4
            -5/32*f^16-1/48*f^17-1/864*f^18-235/48*f^11
            -43/9*f^12-1/864-245/288*f^6-127/54*f^9
            -173/96*f^14-95/144*f^15):
for i from 4 to 9 do
   if p=i then
      lista_sol:= [solve(A_aux[i]^3*B^2-A^3*B_aux[i]^2,f)]:
      lista_rac:= []:
      for j from 1 to nops(lista_sol) do
         if type(lista_sol[j],rational) then
            lista_rac:= [op(lista_rac),lista_sol[j]]:
         fi:
      od:
      j:= 1:
      while j<nops(lista_rac)+1 do
         eca_aux:= subs(f=lista_rac[j],A_aux[i]):
         ecb_aux:= subs(f=lista_rac[j],B_aux[i]):
         lista_aux:= [solve({X^4*eca_aux-A,X^6*ecb_aux-B})]:
         for k from 1 to nops(lista_aux) do
            if type(op(2,op(1,lista_aux[k])),rational) then
               RETURN(1):
            fi:
         od:
         j:= j+1:
      od:
```

```
      fi:
   od:
   if p=3 then
      lista_aux:= [solve(3*X^4+6*A*X^2+12*B*X-A^2)]:
      for k from 1 to nops(lista_aux) do
         if type(lista_aux[k],rational) then
            lista_aux2:= [solve(Y^2-lista_aux[k]^3
              -A*lista_aux[k]-B)]:
            for j from 1 to nops(lista_aux2) do
               if type(lista_aux2[j],rational) then
                  RETURN(1):
               fi:
            od:
         fi:
      od:
   fi:
   RETURN(0):
end:

#
# El programa TORSION calcula el grupo de torsion de una curva
# eliptica, usando el algoritmo de la forma normal de Tate. La
# salida de datos es de la forma [C,n] si el
# grupo es ciclico de n elementos, o de la forma [NC,n] si el
# grupo es producto de un ciclico de 2 elementos por uno
# ciclico de orden n.
#

TORSION:= proc(l::list)
   local A,B,M,N,i,k,ords:
   A:= l[1]:
   B:= l[2]:
   k:= RS([A,B]):
   M:= BOUND([A,B]):
   ords:= divisors(M):
   if k=0 then
      ords:= ords intersect {1,3,5,7,9}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
```

```
            if DEC([A,B,ords[i]])=1 then
               RETURN([C,ords[i]]);
            fi:
         od:
         RETURN([C,1]);
      else
         RETURN([C,1]):
      fi:
   elif k=1 then
      ords:= ords intersect {2,4,6,8,10,12}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
            if ords[i]=12 then
               if DEC([A,B,3])=1 then
                  if DEC([A,B,4])=1 then
                     RETURN([C,12]);
                  fi:
               fi:
            elif ords[i]=10 then
               if DEC([A,B,5])=1 then
                  RETURN([C,10]);
               fi:
            elif DEC([A,B,ords[i]])=1 then
               RETURN([C,ords[i]]);
            fi:
         od:
         RETURN([C,2]):
      else
         RETURN([C,2]):
      fi:
   elif k=3 then
      ords:= ords intersect {4,8,12,16}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
            if DEC([A,B,ords[i]/2])=1 then
               RETURN([NC,ords[i]/2]);
            fi:
```

```
         od:
         RETURN([NC,2]):
      else
         RETURN([NC,2]):
      fi:
   fi:
end:

#
# Los dos programas siguientes calculan la torsion utilizando
# los polinomios de division. La primera rutina, DECDP, hace la
# funcion del programa anterior DEC. La creciente complejidad
# de los polinomios de division se hace obvia al dar las
# expresiones completas, pero esto ahorra un tiempo
# de calculo considerable.
#

DECDP:= proc(l::list)
   local A,B,P,XSOLS,YSOLS,i,j,p:
   A:= l[1]:
   B:= l[2]:
   p:= l[3]:
   P:= array(1..9):
   P[3]:= 3*X^4+6*A*X^2+12*B*X-A^2:
   P[4]:= X^6+5*A*X^4+20*B*X^3-5*A^2*X^2-4*A*B*X-8*B^2-A^3:
   P[5]:= 5*X^12+62*A*X^10+380*B*X^9-105*A^2*X^8+240*A*B*X^7
          -(300*A^3+240*B^2)*X^6-696*B*A^2*X^5-(125*A^4
          +1920*A*B^2)*X^4-(80*A^3*B+1600*B^3)*X^3-(50*A^5
          +240*B^2*A^2)*X^2-(100*B*A^4+640*A*B^3)*X+A^6-256*B^4
          -32*A^3*B^2:
   P[6]:= -X^12-22*A*X^10-220*B*X^9+165*A^2*X^8+528*A*B*X^7+
          (92*A^3+1776*B^2)*X^6-264*B*A^2*X^5+(960*A*B^2
          +185*A^4)*X^4+(80*A^3*B+320*B^3)*X^3+(90*A^5
          +624*B^2*A^2)*X^2+(132*B*A^4+896*A*B^3)*X+512*B^4
          +3*A^6+96*A^3*B^2:
   P[7]:= 7*X^24+308*A*X^22+3944*B*X^21-2954*A^2*X^20
          -112*A*B*X^19-42896*B^2*X^18-19852*A^3*X^18
          -92568*B*A^2*X^17-571872*A*B^2*X^16-35231*A^4*X^16
          -31808*A^3*B*X^15-829696*B^3*X^15-615360*B^2*A^2*X^14
          -82264*A^5*X^14-161840*B*A^4*X^13-2132480*A*B^3*X^13
          -928256*B^4*X^12-111916*A^6*X^12-297472*A^3*B^2*X^12
```

```
        -608160*A^5*B*X^11-2603776*B^3*A^2*X^11
        -42168*A^7*X^10-3293696*A*B^4*X^10
        -1192800*B^2*A^4*X^10-1555456*B^5*X^9
        -3727360*A^3*B^3*X^9-425712*B*A^6*X^9+15673*A^8*X^8
        -831936*A^5*B^2*X^8-7069440*B^4*A^2*X^8
        -53824*A^7*B*X^7-7127040*A*B^5*X^7
        -1314560*B^3*A^4*X^7+14756*A^9*X^6-190400*B^2*A^6*X^6
        -2809856*B^6*X^6-2293760*A^3*B^4*X^6
        -3698688*B^5*A^2*X^5+57288*B*A^8*X^5
        -168448*A^5*B^3*X^5+134400*A^7*B^2*X^4+1302*A^10*X^4
        -3039232*A*B^6*X^4+394240*B^4*A^4*X^4-802816*B^7*X^3
        +831488*A^3*B^5*X^3+1680*A^9*B*X^3+152320*B^3*A^6*X^3
        +544768*B^6*A^2*X^2+196*A^11*X^2+3696*B^2*A^8*X^2
        +96768*A^5*B^4*X^2+229376*A*B^7*X+7168*A^7*B^3*X
        +392*B*A^10*X+64512*B^5*A^4*X+3328*B^4*A^6
        +24576*B^6*A^3+160*A^9*B^2+65536*B^8-A^12:
P[8]:= X^24+68*A*X^22+1232*B*X^21-1694*A^2*X^20
        -9856*A*B*X^19-58688*B^2*X^18-3276*A^3*X^18
        +10032*B*A^2*X^17-19601*A^4*X^16-150960*A*B^2*X^16
        -49408*B^3*X^15+26368*A^3*B*X^15-278400*B^2*A^2*X^14
        -63352*A^5*X^14-140000*B*A^4*X^13-492800*A*B^3*X^13
        -86436*A^6*X^12-804160*A^3*B^2*X^12-439040*B^4*X^12
        -290304*A^5*B*X^11-2248960*B^3*A^2*X^11
        -3591680*A*B^4*X^10-63352*A^7*X^10
        -894720*B^2*A^4*X^10-2111488*B^5*X^9-293536*B*A^6*X^9
        -2213120*A^3*B^3*X^9-4753920*B^4*A^2*X^8
        -19601*A^8*X^8-848928*A^5*B^2*X^8-5320704*A*B^5*X^7
        -87808*A^7*B*X^7-1391360*B^3*A^4*X^7-3276*A^9*X^6
        -1949696*B^6*X^6-2293760*A^3*B^4*X^6
        -318080*B^2*A^6*X^6-3698688*B^5*A^2*X^5
        +4368*B*A^8*X^5-517888*A^5*B^3*X^5+20160*A^7*B^2*X^4
        -2953216*A*B^6*X^4-224000*B^4*A^4*X^4-1694*A^10*X^4
        -851968*B^7*X^3-4096*A^3*B^5*X^3-29440*B^3*A^6*X^3
        -7040*A^9*B*X^3-84480*A^5*B^4*X^2+68*A^11*X^2
        -8640*B^2*A^8*X^2-155648*B^6*A^2*X^2-163840*A*B^7*X
        -55296*B^5*A^4*X-3840*A^7*B^3*X+112*B*A^10*X
        +80*A^9*B^2-8192*B^6*A^3-32768*B^8+A^12:
P[9]:= 3*X^36+342*A*X^34+7596*B*X^33-11385*A^2*X^32
        -44352*A*B*X^31+(-463392*B^2-121392*A^3)*X^30
        -1080288*A^2*B*X^29+(-273348*A^4-11546208*A*B^2)*X^28
        +(-28417920*B^3+4580160*A^3*B)*X^27+(12988512*B^2*A^2
```

```
-4009176*A^5)*X^26+(-24372144*B*A^4
-26932608*A*B^3)*X^25+(90830592*B^4-93129696*A^3*B^2
-8458020*A^6)*X^24+(-643140864*A^2*B^3
-86937408*B*A^5)*X^23+(-1159239168*A*B^4-3546576*A^7
-222558624*B^2*A^4)*X^22+(-139265568*B*A^6
-1360164096*A^3*B^3-1423374336*B^5)*X^21
+(-3662406144*B^4*A^2-288276192*A^5*B^2
+19899882*A^8)*X^20+(-51155136*A^7*B-6795380736*A*B^5
-1006300800*A^4*B^3)*X^19+(-2339126784*B^4*A^3
-105122592*B^2*A^6-2816372736*B^6+44431044*A^9)*X^18
+(-334191744*A^5*B^3-8885458944*A^2*B^5
+180887688*B*A^8)*X^17+(850375584*B^2*A^7
-7848935424*A*B^6+39775986*A^10
+2357095680*A^4*B^4)*X^16+(204319296*B*A^9
+960602112*A^3*B^5-1911914496*B^7
+1653060096*A^6*B^3)*X^15+(22321584*A^11
+6970143744*A^5*B^4-420913152*A^2*B^6
+1175322528*B^2*A^8)*X^14+(14882918400*A^4*B^5
+2555785728*A^7*B^3+60585696*B*A^10
+1756200960*A*B^7)*X^13+(21383405568*B^6*A^3
+13729068*A^12+1482817536*B^8+498797280*A^9*B^2
+5857367040*B^4*A^6)*X^12+(1292819328*A^8*B^3
+23470276608*A^2*B^7+17081280*B*A^11
+11408560128*A^5*B^5)*X^11+(2438378496*A^7*B^4
+7820712*A^13+89271072*B^2*A^10+17155031040*A^4*B^6
+16003104768*A*B^8)*X^10+(3615510528*A^6*B^5
+252512640*A^9*B^3+21516189696*A^3*B^7
+25843536*B*A^12+4568383488*B^9)*X^9+(2304684*A^14
+3441844224*A^5*B^6+515379456*A^8*B^4
+81403488*B^2*A^11+19996803072*B^8*A^2)*X^8
+(10536615936*A*B^9+1128701952*A^7*B^5
+212232960*A^10*B^3+9253440*B*A^13
+2356051968*B^7*A^4)*X^7+(2161115136*B^10+342864*A^15
+2509111296*B^8*A^3+22549536*A^12*B^2
+378708480*A^9*B^4+1958584320*B^6*A^6)*X^6
+(1594656*B*A^14+498051072*B^5*A^8+2156101632*B^7*A^5
+45404928*A^11*B^3+2515009536*B^9*A^2)*X^5+
(3611232*A^13*B^2+584294400*B^6*A^7
+1760624640*B^8*A^4+10923*A^16+1113587712*B^10*A
+75419136*B^4*A^10)*X^4+(1358954496*B^9*A^3
+575078400*B^7*A^6+4530816*A^12*B^3+85211136*A^9*B^5
```

```
          +150994944*B^11+27072*A^15*B)*X^3+(58355712*A^8*B^6
          +42912*A^14*B^2+375128064*A^5*B^8+830472192*B^10*A^2
          +534*A^17+3377664*A^11*B^4)*X^2+(141557760*B^9*A^4
          +1640448*A^10*B^5+47232*A^13*B^3+1068*B*A^16
          +23592960*B^7*A^7+301989888*B^11*A)*X+19200*B^4*A^12
          +480*A^15*B^2+417792*B^6*A^9+25165824*B^10*A^3
          +4718592*B^8*A^6+50331648*B^12-A^18:
   XSOLS:= [solve(P[p])]:
   for i from 1 to nops(XSOLS) do
      if type(XSOLS[i],rational) then
         YSOLS:= [solve(Y^2-XSOLS[i]^3-A*XSOLS[i]-B)]:
         for j from 1 to nops(YSOLS) do
            if type(YSOLS[j],rational) then
               RETURN(1);
            fi:
         od:
      fi:
   od:
   RETURN(0):
end:

#
# El programa DP es el equivalente de TORSION para el algoritmo
# de los polinomios de division.
#

DP:= proc(l::list)
   local A,B,M,N,i,k,ords:
   A:= l[1]:
   B:= l[2]:
   k:= RS([A,B]):
   M:= BOUND([A,B]):
   ords:= divisors(M):
   if k=0 then
      ords:= ords intersect {1,3,5,7,9}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
             if DECDP([A,B,ords[i]])=1 then
                RETURN([C,ords[i]]);
```

```
            fi:
        od:
        RETURN([C,1]);
    else
        RETURN([C,1]):
    fi:
elif k=1 then
    ords:= ords intersect {2,4,6,8,10,12}:
    ords:= sort(convert(ords,list)):
    N:= nops(ords):
    if N>1 then
        for i from N by -1 to 2 do
            if ords[i]=12 then
                if DECDP([A,B,3])=1 then
                    if DECDP([A,B,4])=1 then
                        RETURN([C,12]);
                    fi:
                fi:
            elif ords[i]=10 then
                if DECDP([A,B,5])=1 then
                    RETURN([C,10]);
                fi:
            elif DECDP([A,B,ords[i]])=1 then
                RETURN([C,ords[i]]);
            fi:
        od:
        RETURN([C,2]):
    else
        RETURN([C,2]):
    fi:
elif k=3 then
    ords:= ords intersect {4,8,12,16}:
    ords:= sort(convert(ords,list)):
    N:= nops(ords):
    if N>1 then
        for i from N by -1 to 2 do
            if DECDP([A,B,ords[i]/2])=1 then
                RETURN([NC,ords[i]/2]);
            fi:
        od:
        RETURN([NC,2]):
```

```
      else
         RETURN([NC,2]):
      fi:
   fi:
end:


#
# Los siguientes tres programas calculan la torsion siguiendo
# el Teorema de Nagell-Lutz. La primera subrutina, DPL,
# aplica la formula de duplicacion para comprobar si el punto
# en cuestion tiene el orden buscado.
#

DPL:= proc(l::list)
   local A,B,x:
   A:= l[1]:
   B:= l[2]:
   x:= l[3]:
   if simplify(x**3+A*x+B)=0 then
      RETURN('0');
   else
      RETURN((x**4-2*A*x**2-8*B*x+A**2)/(4*x**3+4*A*x+4*B)):
   fi:
end:

#
# El programa DECNL hace la misma funcion que el DEC, pero
# usando el criterio de Nagell-Lutz. Notemos que el criterio
# para la decision de puntos de orden 9 y 7 es el mismo. Este
# inconveniente se resuelve en el programa principal.
#

DECNL:= proc(l::list)
   local A,B,DISC,SOLS,XLIST,YLIST_0,YLIST,i,j,p:
   A:= l[1]:
   B:= l[2]:
   p:= l[3]:
   DISC:= 4*A**3+27*B**2:
   YLIST_0:= divisors(DISC):
   YLIST:= []:
```

```
for i from 1 to nops(YLIST_0) do
   if irem(DISC,YLIST_0[i]**2)=0 then
      YLIST:= [op(YLIST),YLIST_0[i]]:
   fi:
od:
XLIST:= []:
for i from 1 to nops(YLIST) do
   SOLS:= [solve(YLIST[i]**2-X**3-A*X-B)]:
   for j from 1 to nops(SOLS) do
      if type(SOLS[j],rational) then
         XLIST:= [op(XLIST),SOLS[j]]:
      fi:
   od:
od:
if p=3 then
   for i from 1 to nops(XLIST) do
      if DPL([A,B,XLIST[i]])=XLIST[i] then
         RETURN(1):
      fi:
   od:
elif p=4 then
   for i from 1 to nops(XLIST) do
      if simplify(subs(x=DPL([A,B,XLIST[i]]),
         x**3+A*x+B))=0 then
         RETURN(1):
      fi:
   od:
elif p=5 then
   for i from 1 to nops(XLIST) do
      if DPL([A,B,DPL([A,B,XLIST[i]])])=XLIST[i] then
         RETURN(1):
      fi:
   od:
elif p=6 then
   for i from 1 to nops(XLIST) do
      if DPL([A,B,DPL([A,B,XLIST[i]])])=DPL([A,B,XLIST[i]])
         then
         RETURN(1):
      fi:
   od:
elif p=7 then
```

```
      for i from 1 to nops(XLIST) do
         if DPL([A,B,DPL([A,B,DPL([A,B,XLIST[i]])])])=XLIST[i]
            then
            RETURN(1):
         fi:
      od:
   elif p=8 then
      for i from 1 to nops(XLIST) do
         if simplify(subs(x=DPL([A,B,DPL([A,B,XLIST[i]])]),
            x**3+A*x+B))=0 then
            RETURN(1):
         fi:
      od:
   elif p=9 then
      for i from 1 to nops(XLIST) do
         if DPL([A,B,DPL([A,B,DPL([A,B,XLIST[i]])])])=XLIST[i]
            then
            RETURN(1):
         fi:
      od:
   fi:
   RETURN(0):
end:

#
# NL es el programa que calcula la torsion usando las dos
# subrutinas anteriores. Formalmente es muy similar a TORSION,
# salvo por el hecho ya mencionado de la necesidad de
# distinguir entre [C,7] y [C,9]. En realidad, no hemos
# encontrado ejemplos que, tras pasar por BOUND, necesiten esta
# distincion.
#

NL:= proc(l::list)
   local A,B,M,N,i,k,ords:
   A:= l[1]:
   B:= l[2]:
   k:= RS([A,B]):
   M:= BOUND([A,B]):
   ords:= divisors(M):
   if k=0 then
```

```
    ords:= ords intersect {1,3,5,7,9}:
    ords:= sort(convert(ords,list)):
    N:= nops(ords):
    if N>1 then
       for i from N by -1 to 2 do
           if ords[i]=9 then
              if DECNL([A,B,9])*DECNL([A,B,3])=1 then
                 RETURN([C,9]):
              fi:
           elif DECNL([A,B,ords[i]])=1 then
              RETURN([C,ords[i]]);
           fi:
       od:
       RETURN([C,1]);
    else
       RETURN([C,1]):
    fi:
elif k=1 then
    ords:= ords intersect {2,4,6,8,10,12}:
    ords:= sort(convert(ords,list)):
    N:= nops(ords):
    if N>1 then
       for i from N by -1 to 2 do
           if ords[i]=12 then
              if DECNL([A,B,3])=1 then
                 if DECNL([A,B,4])=1 then
                    RETURN([C,12]);
                 fi:
              fi:
           elif ords[i]=10 then
              if DECNL([A,B,5])=1 then
                 RETURN([C,10]);
              fi:
           elif DECNL([A,B,ords[i]])=1 then
              RETURN([C,ords[i]]);
           fi:
       od:
       RETURN([C,2]):
    else
       RETURN([C,2]):
    fi:
```

```
   elif k=3 then
      ords:= ords intersect {4,8,12,16}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
             if DECNL([A,B,ords[i]/2])=1 then
                RETURN([NC,ords[i]/2]);
             fi:
         od:
         RETURN([NC,2]):
      else
         RETURN([NC,2]):
      fi:
   fi:
end:

#
# Los siguientes programas calculan la torsion usando la
# parametrizacion analitica. En primer lugar notemos que vamos
# a usar la ecuacion de Weierstrass habitual en este contexto;
# esto es, tal que el coeficiente de X^3 sea 4. Es elemental
# ver que la curva dada por la ecuacion Y^2=X^3+AX+B es
# isomorfa a la dada por Y^2=4X^3+4AX+4B, asi que usaremos
# frecuentemente estos coeficientes en lugar de los originales.
# El primer programa calcula una base del reticulo, siguiendo
# la seccion I.C. Como indicamos en II.C. los denominadores
# que aparecen en las coordenadas de los puntos de la curva
# pueden ser 1, 2 o 4, con lo que 3 decimales de precision
# deben ser suficientes.
#

RETBASIS:= proc(l::list)
   local A,B,DISC,REALSOLS,SOLS,Z,a,b,i:
   A:= l[1]:
   B:= l[2]:
   DISC:= abs(4*A**3+27*B**2):
   Digits:= 3+ceil(evalf(log10(DISC))):
   SOLS:= [solve(X^3+A*X+B)]:
   REALSOLS:= []:
   for i from 1 to 3 do
```

```
      if type(SOLS[i],realcons) then
         REALSOLS:= [op(REALSOLS),SOLS[i]]:
      fi:
   od:
   REALSOLS:= sort(convert(REALSOLS,list)):
   Z:= [Z[1],Z[2]]:
   if nops(REALSOLS)=1 then
      a:= 3*REALSOLS[1]:
      b:= (3*REALSOLS[1]**2+A)**(1/2):
      Z[1]:= 2*Pi/GaussAGM(2*b**(1/2),(2*b+a)**(1/2)):
      Z[2]:= -Z[1]/2+I*Pi/GaussAGM(2*b**(1/2),(2*b-a)**(1/2)):
   fi:
   if nops(REALSOLS)=3 then
      Z[1]:= Pi/GaussAGM(abs(REALSOLS[3]-REALSOLS[1])**(1/2),
             abs(REALSOLS[3]-REALSOLS[2])**(1/2)):
      Z[2]:= I*Pi/GaussAGM(abs(REALSOLS[3]-REALSOLS[1])**(1/2),
             abs(REALSOLS[2]-REALSOLS[1])**(1/2)):
   fi:
   RETURN(evalf(Z)):
end:

#
# Este programa decide si un elemento del toro corresponde a un
# punto racional o, de manera mas precisa, si su imagen esta en
# Z/4 x Z/4, dado que solo nos interesa usarlo con puntos que
# pueden ser de torsion.
#

ISRAT:= proc(l::list)
   local A,B,DISC,x,y,z:
   A:= l[1]:
   B:= l[2]:
   DISC:= abs(4*A**3+27*B**2):
   Digits:= 3+ceil(evalf(log10(DISC))):
   z:= l[3]:
   x:= WeierstrassP(z,-4*A,-4*B):
   y:= WeierstrassPPrime(z,-4*A,-4*B):
   if abs(round(4*x)-(4*x))<0.1 then
      if abs(round(4*y)-(4*y))<0.1 then
         RETURN(1):
      fi:
```

```
   fi:
   RETURN([0,x,y]):
end:

#
# El ultimo programa, DOUD, calcula la torsion usando el
# algoritmo explicado en II.C. Hay que ajustar la precision
# de MAPLE en funcion de la magnitud de los coeficientes de la
# curva: para numeros grandes este es el dato que asume mayor
# cantidad de operaciones y, en consecuencia, mayor
# complejidad. La precision escogida es nuevamente
# log(|DISC|)+3, donde DISC es el discriminante de la curva,
# por las razones expuestas en II.C.
#

DOUD:= proc(l::list)
   local A,B,DISC,M,N,Z,i,k,ords:
   A:= l[1]:
   B:= l[2]:
   DISC:= abs(4*A**3+27*B**2):
   Digits:= 3+ceil(evalf(log10(DISC))):
   Z:= RETBASIS([A,B]):
   k:= RS([A,B]):
   M:= BOUND([A,B]):
   ords:= divisors(M):
   if k=0 then
      ords:= ords intersect {1,3,5,7,9}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
            if ISRAT([A,B,Z[1]/ords[i]])=1 then
               RETURN([C,ords[i]]);
            fi:
         od:
         RETURN([C,1]);
      else
         RETURN([C,1]):
      fi:
   elif k=1 then
      ords:= ords intersect {2,4,6,8,10,12}:
```

```
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
            if ISRAT([A,B,Z[1]/ords[i]])=1 then
               RETURN([C,ords[i]]):
            elif ISRAT([A,B,Z[1]/ords[i]+Z[2]/2])=1 then
               RETURN([C,ords[i]]):
            elif ISRAT([A,B,Z[1]/ords[i]+(Z[1]+Z[2])/2])=1 then
               RETURN([C,ords[i]]):
            fi:
         od:
         RETURN([C,2]):
      else
         RETURN([C,2]):
      fi:
   elif k=3 then
      ords:= ords intersect {4,8,12,16}:
      ords:= sort(convert(ords,list)):
      N:= nops(ords):
      if N>1 then
         for i from N by -1 to 2 do
             if ISRAT([A,B,Z[1]/(ords[i]/2)])=1 then
                RETURN([NC,ords[i]/2]);
             fi:
         od:
         RETURN([NC,2]):
      else
         RETURN([NC,2]):
      fi:
   fi:
end:
```

A.2. Reducción

Como ya vimos en la sección II.A., el procedimiento de acotación del orden del grupo de torsión racional de una curva elíptica, mediante la reducción modulo p, tiene en teoría un coste computacional acotado por $O(\log|\Delta|\log^2|\log(\Delta)|)$, para $|\Delta|$ suficientemente grande, pero también

señalamos en dicha sección que, en la práctica, este procedimiento requiere una cantidad de tiempo insignificante, y esta afirmación es la que vamos a justificar ahora mediante varios ejemplos ordenados en tres tablas.

La primera de ellas recoge quince ejemplos de curvas en forma breve de Weierstrass, denotadas $E_1, ..., E_{15}$, cuyos coeficientes A y B se especifican, siendo el grupo de torsión de cada una de ellas uno de los quince únicos grupos posibles según el teroema de Mazur. Estos ejemplos se han escogido de la lista exhaustiva de [34].

En las tablas 2 y 3 recogemos los tiempos necesarios para acotar el orden del grupo de torsión, según el procedimiento `BOUND` dado en A.1., para las mismas quince curvas de la primera tabla, pero esta vez se han hecho además cuatro cambios de variables del tipo

$$X \longmapsto u^2X, \quad Y \longmapsto u^3Y,$$

con $u = 4!, 16!, 64!$ y $256!$ con los que, aunque el grupo de torsión de las curvas no cambian, sí lo hacen sus coeficientes (que pasan de ser A y B a ser u^4A y u^6B) y por tanto su discriminante, que pasa de ser Δ a ser $u^{12}\Delta$. Así podemos observar que, aunque el tiempo que se tarda en realizar la acotación aumenta al hacerlo $|\Delta|$, no se obtienen tiempos tan grandes como cabía esperar en teoría, sobre todo si tenemos en cuenta que, cuando $u = 256!$, estamos trabajando con un discriminante de orden

$$\Delta = u^{12}(4A^3 + 27B^2) \simeq 2^{20000}.$$

Es decir, a pesar de trabajar con discriminantes bastante grandes en valor absoluto, y con los algoritmos de A.1., (siendo éstos menos sofisticados que los algoritmos presentados en [3] ya que, por ejemplo, nuestro `NDP` cuenta puntos directamente), se obtienen tiempos realmente pequeños, como se puede ver en las tablas 2 y 3.

La diferencia entre estas dos tablas es que en la tabla 2 se han elegido tres buenos primos para el prodeso de acotación, mientras que en la tabla 3 se han tomado cinco buenos primos. Como se puede observar por los resultados obtenidos, la diferencia en tiempo entre las tablas 2 y 3 no es muy grande, sin embargo, las acotaciones obtenidas usando cinco buenos primos son más precisas (especialmente en grupos de torsión trivial, que son los más frecuentes) ya que, en la tabla 2 hay muchos más casos que en la tabla 3 en los que la acotación no coincide con el número de puntos de torsión. Estos casos están señalados en negrita en ambas tablas.

Como observación adicional, conviene resaltar también la diferencia temporal entre grupos de torsión de orden par e impar.

Tabla 1: Curvas

Curva	A	B	$\mathrm{Tor}(E)$
E_1	0	-2	C_1
E_2	0	8	C_2
E_3	0	4	C_3
E_4	4	0	C_4
E_5	-432	8208	C_5
E_6	0	1	C_6
E_7	-43	166	C_7
E_8	-44091	3304854	C_8
E_9	-219	1654	C_9
E_{10}	-58347	3954150	C_{10}
E_{11}	-33339627	73697852646	C_{12}
E_{12}	-4	0	$C_2 \times C_2$
E_{13}	-351	1890	$C_2 \times C_4$
E_{14}	-24003	1296702	$C_2 \times C_6$
E_{15}	-1386747	368636886	$C_2 \times C_8$

Tabla 2: Tiempos de acotaciones con tres buenos primos

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	$0.02s$	$0.09s$	$\mathbf{0.31}s$	$\mathbf{1.97}s$	$\mathbf{64.48}$
E_2	$\mathbf{0.04}s$	$\mathbf{0.04}s$	$0.07s$	$0.46s$	$\mathbf{14.68}s$
E_3	$0.06s$	$0.11s$	$0.24s$	$1.48s$	$35.83s$
E_4	$0.01s$	$0.02s$	$0.04s$	$0.47s$	$15.83s$
E_5	$0.02s$	$0.19s$	$0.52s$	$4.27s$	$101.77s$
E_6	$0.04s$	$0.04s$	$0.06s$	$0.48s$	$14.58s$
E_7	$0.02s$	$0.19s$	$0.48s$	$2.64s$	$\mathbf{101.55}s$
E_8	$0.03s$	$0.03s$	$0.06s$	$0.68s$	$21.43s$
E_9	$0.02s$	$0.18s$	$0.36s$	$3.14s$	$115.02s$
E_{10}	$0.04s$	$0.04s$	$0.21s$	$0.67s$	$21.40s$
E_{11}	$0.03s$	$0.03s$	$0.09s$	$\mathbf{0.77}s$	$\mathbf{27.94}s$
E_{12}	$0.03s$	$0.02s$	$0.03s$	$0.47s$	$14.30s$
E_{13}	$0.01s$	$0.01s$	$0.03s$	$0.50s$	$15.81s$
E_{14}	$0.02s$	$0.02s$	$0.06s$	$\mathbf{0.71}s$	$24.82s$
E_{15}	$0.02s$	$0.02s$	$0.03s$	$0.71s$	$28.01s$

Tabla 3: Tiempos de acotaciones con cinco buenos primos

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	$0.06s$	$0.11s$	$0.50s$	$3.53s$	$123.71s$
E_2	$0.04s$	$0.05s$	$0.10s$	$0.87s$	$23.88s$
E_3	$0.09s$	$0.13s$	$0.49s$	$3.67s$	$121.46s$
E_4	$0.02s$	$0.03s$	$0.08s$	$0.81s$	$21.75s$
E_5	$0.08s$	$0.23s$	$0.78s$	$6.42s$	$216.67s$
E_6	$0.05s$	$0.07s$	$0.15s$	$0.86s$	$25.75s$
E_7	$0.04s$	$0.24s$	$0.77s$	$4.63s$	$197.48s$
E_8	$0.03s$	$0.04s$	$0.17s$	$1.24s$	$37.20s$
E_9	$0.06s$	$0.25s$	$0.53s$	$4.89s$	$198.55s$
E_{10}	$0.06s$	$0.06s$	$0.27s$	$1.16s$	$37.10s$
E_{11}	$0.06s$	$0.08s$	$0.12s$	$1.22s$	$38.71s$
E_{12}	$0.02s$	$0.02s$	$0.06s$	$0.81s$	$21.06s$
E_{13}	$0.03s$	$0.03s$	$0.09s$	$1.08s$	$31.44s$
E_{14}	$0.03s$	$0.03s$	$0.08s$	$\mathbf{1.12}s$	$33.55s$
E_{15}	$0.04s$	$0.07s$	$0.07s$	$1.39s$	$48.41s$

A.3. Comparación efectiva de algoritmos

El objetivo de esta sección es comparar los tiempos de los cuatro algoritmos estudiados en el capítulo II. Para que sea ésta una comparación justa, se han usado los mismos recursos en la implementación de cada algoritmo. Los cálculos se han realizado en un Pentium IV, con MAPLE 10 bajo Kubuntu 5.10.

En cada una de las cuatro tablas presentadas (una por cada algoritmo), tenemos las mismas quince curvas elípticas $E_1, ..., E_{15}$ de la sección anterior, y con los mismos cambios de variables. Destacamos, de nuevo, el tamaño que llegan a alcanzar los números con los que trabajamos, siendo éstos de unas 6000 cifras en base decimal.

Los resultados mostrados en estas tablas incluyen el tiempo dedicado a la acotación vista en la sección A.2., usando cinco buenos primos. Los tiempos marcados en negrita son los mejores para cada par (E_i, u), donde hemos tomado empatados aquéllos con diferencias menores al 5 por ciento o a 0.05 segundos.

Cuando el tiempo ha excedido el límite superior fijado para los cálculos,

1800 segundos, lo hemos reflejado en la tabla sustituyendo el dato numérico correspondiente por el símbolo $\gg$.

Por último, podemos observar que, para las curvas E_1, E_2 y E_{12} la acotación es, prácticamente, el cálculo completo de la torsión, por lo que los resultados son similares en todos los algoritmos.

Tabla 4: Tiempos para el algoritmo de Nagell–Lutz

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	**0.11**s	**0.13**s	**0.60**s	4.28s	**142.70**s
E_2	**0.06**s	**0.06**s	**0.11**s	**0.89**s	**26.35**s
E_3	0.19s	4.09s	$\gg$	$\gg$	$\gg$
E_4	**0.05**s	7.86s	$\gg$	$\gg$	$\gg$
E_5	1.12s	19.56s	$\gg$	$\gg$	$\gg$
E_6	**0.09**s	5.33s	$\gg$	$\gg$	$\gg$
E_7	0.60s	10.10	$\gg$	$\gg$	$\gg$
E_8	1.93s	41.31s	$\gg$	$\gg$	$\gg$
E_9	2.62s	33.32s	$\gg$	$\gg$	$\gg$
E_{10}	3.01s	64.61s	$\gg$	$\gg$	$\gg$
E_{11}	139.68s	1083.30s	$\gg$	$\gg$	$\gg$
E_{12}	**0.02**s	**0.02**s	**0.08**s	**0.83**s	**21.46**s
E_{13}	1.21s	22.40s	$\gg$	$\gg$	$\gg$
E_{14}	6.48s	97.26s	$\gg$	$\gg$	$\gg$
E_{15}	44.93s	705.02	$\gg$	$\gg$	$\gg$

Tabla 5: Tiempos para el algoritmo de polinomios de división

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	**0.11**s	**0.13**s	**0.61**s	4.32s	**148.08**s
E_2	**0.06**s	**0.06**s	**0.12**s	**0.90**s	**26.47**s
E_3	**0.14**s	**0.15**s	**0.61**s	**4.29**s	**146.70**s
E_4	**0.06**s	**0.06**s	**0.12**s	**0.96**s	**24.90**s
E_5	0.47s	0.74s	1.56s	9.64s	302.45s
E_6	0.17s	0.26s	0.47s	2.73s	63.54s
E_7	0.23s	2.29s	3.27s	11.96s	524.30s
E_8	1.08s	1.17s	1.74s	6.84s	204.50s
E_9	3.64s	4.06s	7.10s	24.64s	722.57s
E_{10}	**0.12**s	0.44s	0.74s	3.08s	95.08s
E_{11}	**0.16**s	**0.20**s	0.47s	3.06s	83.28s
E_{12}	**0.03**s	**0.03**s	**0.08**s	**0.85**s	**21.76**s
E_{13}	**0.05**s	**0.06**s	**0.11**s	**1.15**s	34.26s
E_{14}	**0.12**s	**0.12**s	0.46s	3.33s	92.32s
E_{15}	0.58s	0.66s	1.14s	6.15s	172.15s

Tabla 6: Tiempos para el algoritmo de la parametrización analítica

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	**0.13**s	**0.17**s	**0.65**s	4.79s	166.25s
E_2	**0.08**s	**0.08**s	**0.12**s	0.99s	27.35s
E_3	0.21s	0.29s	1.65s	20.30s	624.84s
E_4	**0.04**s	0.26s	0.61s	14.46s	215.38s
E_5	**0.11**s	**0.36**s	**1.16**s	12.26s	490.71s
E_6	**0.08**s	**0.14**s	**0.28**s	8.95s	348.63s
E_7	**0.09**s	**0.36**s	**1.28**s	11.92s	469.38s
E_8	**0.03**s	**0.11**s	**0.22**s	24.01s	924.50s
E_9	**0.12**s	**0.35**s	**1.10**s	12.00s	524.79s
E_{10}	**0.10**s	**0.14**s	**0.33**s	13.43s	306.60s
E_{11}	**0.12**s	**0.19**s	**0.27**s	3.07s	489.07s
E_{12}	**0.03**s	**0.03**s	**0.09**s	0.92s	23.01s
E_{13}	**0.06**s	**0.08**s	0.18s	2.96s	97.21s
E_{14}	**0.06**s	**0.09**s	**0.17**s	2.98s	96.05s
E_{15}	**0.06**s	**0.10**s	**0.17**s	3.09s	98.02s

Tabla 7: Tiempos para el algoritmo de la forma de Tate

E	$u = 1$	$u = 4!$	$u = 16!$	$u = 64!$	$u = 256!$
E_1	**0.11**s	**0.14**s	**0.58**s	**4.05**s	**142.86**s
E_2	**0.06**s	**0.07**s	**0.10**s	**0.85**s	**25.44**s
E_3	**0.12**s	**0.18**s	**0.66**s	4.63s	**143.71**s
E_4	**0.04**s	**0.06**s	**0.13**s	1.09s	26.81s
E_5	**0.12**s	0.66s	1.24s	**7.69**s	**246.83**s
E_6	**0.08**s	**0.14**s	**0.27**s	**1.56**s	**40.32**s
E_7	0.26s	2.17s	2.80s	**7.55**s	**235.76**s
E_8	0.17s	0.37s	0.50s	**1.84**s	**53.18**s
E_9	3.80s	4.05s	6.25s	**10.26**s	**246.69**s
E_{10}	**0.13**s	**0.13**s	0.53s	**1.73**s	**45.09**s
E_{11}	**0.17**s	**0.24**s	0.36s	**2.18**s	**62.87**s
E_{12}	**0.02**s	**0.02**s	**0.08**s	**0.83**s	**21.69**s
E_{13}	**0.05**s	**0.05**s	**0.12**s	**1.20**s	**36.61**s
E_{14}	**0.07**s	**0.10**s	**0.16**s	**1.27**s	**38.87**s
E_{15}	0.17s	0.24s	0.36s	**2.17**s	**62.91**s

Bibliografía

[1] Baker, A.: Contributions to the theory of Diophantine equations. I. On the representation of integers by binary forms. Philos. Trans. Roy. Soc. London Ser. A **263** (1967/8) 173–191.

[2] Birch, B.; Swinnerton–Dyer, H.P.F.: Notes on elliptic curves (I, II). J. Reine Angew. Math. **212** (1963) 7–25, **218** (1965) 79–108.

[3] Blake, I.F.; Seroussi, G.; Smart, N.P.: Elliptic curves in cryptography. Cambridge University Press, 1999.

[4] Bombieri, E.; Schmidt, W. M.: On Thue's equation. Invent. Math. **88** (1987) 69–81.

[5] Borevich, Z.I.; Shafarevich, I.R.: Number theory. Academic Press, 1966.

[6] Cassels, J.W.S.: Lectures on elliptic curves. Cambridge University Press, 1991.

[7] Chahal, J.S.: A remark on the torsion subgroups of elliptic curves. J. Pure Appl. Algebra **115** (1997) 321–323.

[8] Cohen, H.: A course in computational algebraic number theory. Springer–Verlag, 1984.

[9] Cremona, J.: Algorithms for modular elliptic curves. Cambridge University Press, 1992.

[10] Doud, D.: A procedure to calculate torsion of elliptic curves over $\mathbb{Q}$. Manuscripta Math. **95** (1998) 463–469.

[11] Erdös, P.: Beweis eines Satzes von Tschebycheff. Acta Sci. Math. (Szeged) **5** (1930) 194–198.

[12] Fujita, Y.: Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2–extensions of $\mathbb{Q}$. Acta Arith. **115** (2004) 29–45.

[13] Fujita, Y.: Torsion subgroups of elliptic curves in elementary abelian 2-extensions of $\mathbb{Q}$. J. Number Theory **114** (2005) 124–134.

[14] Fulton, W.: Algebraic curves. Benjamin, 1969.

[15] García–Selfa, I.; Olalla, M.A.; Tornero J.M.: Computing the rational torsion of an elliptic curve using Tate normal form. J. Number Theory **96** (2002) 76–88.

[16] Husemöller, D.: Elliptic Curves. Springer–Verlag, 1987.

[17] Knuth, D.E.: The Art of Computer Programming, v.2: Seminumerical algorithms (2nd Edition). Addison–Wesley, 1981.

[18] Kubert, D.S.: Universal bounds on the torsion of elliptic curves. Proc. London Math. Soc. **33** (3) (1976) 193–237.

[19] Kwon, S.: Torsion subgroups of elliptic curves over quadratic extensions. J. Number Theory **62** (1997) 144–162.

[20] Loos, R.: Computing rational zeros of integral polynomials by p-adic expansion. SIAM J. Comput. **12** (2) (1983) 286–293.

[21] Lutz, E.: Sur l'equation $y^2 = x^3 - ax - b$ dans les corps p-adiques. J. Reine Angew. Math. **177** (1937) 237–247.

[22] Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. **47** (1977) 33–186.

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

[24] Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124** (1996) 437–449.

[25] Mordell, L.J.: On the rational solutions of the indeterminate equations of the third and fourth degrees. Math. Proc. Cambridge Philos. Soc. **21** (1922) 179–192.

[26] Mordell, L.J.: Diophantine equations. Academic Press, 1969.

[27] Nagell, T.: Solution de quelque problemes dans la théorie arithmétique des cubiques planes du premier genre. Wid. Akad. Skrifter Oslo I, 1935.

[28] Ono, K.: Euler's concordant forms. Acta Arith. **78** (2) (1996) 101–123.

[29] Parent, P.: Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. J. Reine Angew. Math. **506** (1999) 85–116.

[30] Parent, P.: Torsion des courbes elliptiques sur les corps cubiques. Ann. Inst. Fourier (Grenoble) **50** (3) (2000) 723–749.

[31] Qiu, D.; Zhang, X.: Explicit classification for torsion cyclic subgroups of rational points with even orders of elliptic curves. Chinese Sci. Bull. **44** (1999) 1951–1953.

[32] Qiu, D.; Zhang, X.: Explicit classification for torsion subgroups of rational points of elliptic curves. Acta Math. Sin. (Engl. Ser.) **18** (2002) 539–548.

[33] Selmer, E.: The diophantine equation $ax^3 + by^3 + cz^3$. Acta Math. **85** (1951) 203–362.

[34] Silverman, J.H.: The arithmetic of elliptic curves. Springer–Verlag, 1986.

[35] Silverman, J.H.; Tate, J.T.: Rational points on elliptic curves. Springer–Verlag, 1992.

[36] Smart, N.P.: The algorithmic resolution of diophantine equations. Cambridge University Press, 1998.

[37] Thue, A.: Über Annahäherungswerte algebraischer Zahlen. J. Reine Angew. Math. **135** (1909) 284–305.

[38] Tzanakis, N.; de Weger, B. M. M.: On the practical solution of the Thue equation. J. Number Theory **31** (1989) 99–132.

[39] Weil, A.: Sur un théorème de Mordell. Bull. Sci. Math. **54** (1930) 182–191.

UNIVERSIDAD DE SEVILLA

Reunido el tribunal en el día de la fecha, integrado por los abajo firmantes, para evaluar la tesis doctoral de D.ª Irene García Sella
tiulada Aspectos diofánticos y computacionales de la torsión racional en curvas elípticas
acordó otorgarle la calificación de

Sevilla, a 13 de diciembre de 2006.

Vocal,

Vocal,

Vocal,

Presidente,

Secretario,
Miguel A. Olalla Acosta

Doctorando,