El diablo de los números

Sección a cargo de

Javier Cilleruelo Mateo

Buscando puntos racionales en curvas elípticas: Métodos explícitos

por

Álvaro Lozano Robledo

¿Qué números naturales son área de un triángulo recto con lados racionales? A estos números se les llama *números congruentes*. Por ejemplo, el triángulo asociado a la terna pitagórica $(3, 4, 5)$ tiene área 6. Sorprendentemente, un número natural n es congruente si y sólo si la ecuación $y^2 = x^3 - n^2x$ tiene infinitas soluciones racionales. Esta ecuación es un ejemplo de *curva elíptica*. Del mismo modo, muchos otros problemas aritméticos y geométricos están relacionados con curvas de este tipo. Por desgracia, hasta la fecha no se ha encontrado un algoritmo capaz de encontrar todas los puntos racionales en curvas elípticas. En este artículo presentamos algunos de los métodos parciales y resultados más eficientes en este campo.

1 Introducción

Desde la antigüedad, las ecuaciones diofánticas han sido objeto de estudio por numerosos matemáticos y admiradas por su engañosa y cautivadora simplicidad. La solución de muchos problemas está enterrada bajo la sutil aritmética de determinadas ecuaciones, del mismo modo que el problema de los números congruentes está asociado[1] a la ecuación $y^2 = x^3 - n^2x$. Por tanto,

[1]Sea (a, b, c) una terna pitagórica, esto es $a^2 + b^2 = c^2$, con $n = \frac{a \cdot b}{2}$. Si definimos un cambio de coordenadas $x = (c/2)^2$, $y = c \cdot (b^2 - a^2)/8$, es fácil ver que las nuevas variables satisfacen la ecuación mencionada en el texto. Nótese que x es un cuadrado perfecto.

dada una ecuación polinómica

$$f(x_1, x_2, \dots, x_r) = 0 \tag{1}$$

con coeficientes enteros nos hacemos tres preguntas básicas. Primero, ¿podemos determinar si *existen* soluciones con coordenadas enteras ($\mathbb{Z}$) o racionales[2] ($\mathbb{Q}$)? En caso afirmativo ¿somos capaces de encontrar *alguna* de las soluciones? y finalmente, ¿podemos garantizar que hemos encontrado *todas* las soluciones? La primera de estas tres preguntas era el problema número 10 de los que Hilbert presentó a la comunidad matemática a comienzos del siglo XX. En 1970, Matiyasevich descubrió que no existe un algoritmo general que decida si la ecuación (1) tiene soluciones enteras (véase [Mat93]). Sin embargo, restringiendo la pregunta a casos particulares, sí que se han podido responder las preguntas aquí planteadas. Los avances más significativos se han obtenido en ecuaciones con una o dos variables:

- *Polinomios en una variable*:

  $$a_0X^n + a_1X^{n-1} + \ldots + a_n = 0.$$

  Este caso es sencillo. El siguiente criterio determina cómo buscar las raices enteras o racionales de un polinomio: si $\frac{p}{q} \in \mathbb{Q}$ es una solución entonces a_n es divisible por p y a_0 es divisible por q.

- *Ecuaciones lineales en dos variables*:

  $$aX + bY = d.$$

  Es claro que una ecuación de este tipo siempre tiene infinitas soluciones racionales. El *algoritmo de Euclides* determina si existen soluciones en números enteros y, en caso positivo, produce todas las soluciones. En particular, la ecuación tiene soluciones si y sólo si d es divisible por el máximo común divisor de a y b.

- *Ecuaciones cuadráticas (cónicas)*:

  $$aX^2 + bXY + cY^2 + dX + eY = f.$$

  Este es otro problema clásico. El *criterio de Legendre*[3] determina si existen soluciones racionales. En caso positivo, los puntos racionales de una cónica se pueden encontrar usando una parametrización de la curva, que

[2] En general, podemos hacer las mismas preguntas sobre cuerpos de números y sus correspondientes anillos de enteros.

[3] Una cónica C tiene soluciones racionales si y sólo si C tiene puntos p-adicos para todo número primo p, lo cual puede ser comprobado resolviendo un número finito de congruencias.

puede ser obtenida mediante *proyección estereográfica* de la curva sobre una recta. Las soluciones enteras son mucho más difíciles de encontrar. El problema es equivalente a encontrar una solución a la *ecuación de Pell*, $x^2 - Dy^2 = 1$, o en otras palabras, encontrar una unidad fundamental en los enteros algebraicos de extensiones cuadráticas de $\mathbb{Q}$. Este último problema se puede resolver, por ejemplo, con la ayuda de las *fracciones continuas*[4].

- *Ecuaciones cúbicas*:

$$aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + jY + k = 0$$

Tal ecuación puede no tener soluciones racionales, un número finito de ellas, o una infinitud. Por desgracia, hasta la fecha, no se conoce ningún procedimiento general para calcular las soluciones racionales de una ecuación de este tipo. En este artículo analizamos algunos de los avances en este terreno e introducimos al lector en la teoría de *curvas elípticas*.

- *Ecuaciones de grado arbitrario.* Sorprendentemente, dada una curva C: $f(x, y) = 0$, el género[5], el cual es un invariante topológico, condiciona de manera profunda la aritmética de los puntos racionales de C. De hecho, Mordell conjeturó, y fue demostrado por Faltings en 1983, que si C es una curva de género mayor o igual que 2 entonces sólo hay un número finito de soluciones con coordenadas racionales, aunque carecemos de un algoritmo para encontrarlas. Si la curva es de género 0, el problema puede reducirse a resolver una cónica. En el caso que C sea de género 1 (una curva elíptica), existe un cambio de coordenadas que reduce el problema a la resolución de una ecuación de tercer grado (Proposición 2).

2 Curvas Elípticas

Definición 1. *Una* curva elíptica *definida sobre un cuerpo K es un esquema proyectivo no singular de dimensión 1 (una curva) y género 1, junto con un punto definido sobre K, el origen $\mathcal{O}$ (o = zero).*

[4]Existe una *convergente* $\omega = x/y$ de la fracción continua de $\sqrt{D}$ tal que (x, y) satisface la ecuación de Pell.

[5]El género de una curva algebraica C, proyectiva y no singular, se define como el número entero g tal que para toda 1-forma diferencial $\omega \in \Omega_C$ se cumple que el grado del divisor de ω es $\deg(\mathrm{div}(\omega)) = 2g - 2$, ver [Har77]. El género clasifica las curvas desde el punto de vista topológico. $\mathbb{P}^1(\mathbb{C})$ y las cónicas son curvas de género 0, homeomórficas a una esfera (sobre $\mathbb{C}$). Las curvas elípticas son homeomórficas a un toro.

Una vez establecida esta definición formal, nos olvidamos de ella inmediatamente. De aquí en adelante asumiremos una definición mucho más sencilla (y equivalente): una curva elíptica E definida sobre K es una curva cúbica no singular[6]:

$$\begin{aligned} f(X,Y,Z) &= aX^3 + bX^2Y + cXY^2 + dY^3 \\ &\quad + eX^2Z + fXYZ + gY^2Z + hXZ^2 + jYZ^2 + kZ^3 = 0, \end{aligned} \tag{2}$$

con coeficientes en K y con al menos un punto $\mathcal{O} \in E$ al cual llamamos "origen".

La ecuación (2) está dada en coordenadas proyectivas, es decir, la curva está definida por un polinomio homogéneo en sus variables. En general deshomogeneizamos la ecuación con un cambio de variables

$$X/Z \mapsto x, \quad Y/Z \mapsto y$$

y obtenemos una curva plana

$$\begin{aligned} E\colon f(x,y) &= ax^3 + bx^2y + cxy^2 + dy^3 \\ &\quad + ex^2 + fxy + gy^2 + hx + jy + k = 0. \end{aligned} \tag{3}$$

Debemos tener precaución y no olvidar que puede haber algunos puntos de E en el "infinito", es decir, aquellos puntos que en la ecuación (2) tenían coordenada $Z = 0$.

La siguiente proposición es una considerable simplificación:

Proposición 2. *Sea E una curva elíptica definida sobre K, un cuerpo de característica distinta de 2 ó 3. Entonces existe un cambio de coordenadas racional tal que E tiene una* **ecuación de Weierstrass** *de la forma*

$$y^2 = x^3 + Ax + B, \quad A, B \in K, \ \textit{con } 4A^3 + 27B^2 \neq 0.$$

El origen $\mathcal{O}$ tiene coordenadas (proyectivas) $[0,1,0]$ y es el único punto en el "infinito".

La existencia de tal cambio de coordenadas (para curvas de género 1 en general, con un punto racional dado) es una consecuencia del teorema de Riemann-Roch (véase [Sil86], Capítulo III.3). En [SiT92], I. 3, se describe un método explícito para encontrar las nuevas coordenadas.

[6]Una curva $C\colon f(x,y,z) = 0$ es singular en un punto $P \in C$ si y sólo si $\partial f/\partial x(P) = \partial f/\partial y(P) = \partial f/\partial z(P) = 0$. Una curva $E : y^2 = x^3 + Ax + B$ es no singular si y sólo si $4A^3 + 27B^2 \neq 0$. La cantidad $\Delta = -16 \cdot (4A^3 + 27B^2)$ es llamada el *discriminante* de E.

3 La Estructura de Grupo

Sea E una curva elíptica definida sobre $\mathbb{Q}$ con ecuación de Weierstrass

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

Con un cambio de coordenadas $(x, y) \mapsto (u^{-2}x,\ u^{-3}y)$ podemos encontrar una curva equivalente tal que $A, B \in \mathbb{Z}$. En 1929 Siegel demostró el siguiente resultado acerca de las soluciones enteras:

Teorema 3. *Sea $E/\mathbb{Q}$ una curva elíptica de ecuación $y^2 = x^3 + Ax + B$ con $A, B \in \mathbb{Z}$. Entonces E tiene sólo un número finito de soluciones con coordenadas enteras.*

El teorema de Siegel es una consecuencia de un conocido teorema de Roth en la teoría de aproximación diofántica. Desgraciadamente, la demostración del teorema de Siegel no ofrece un método efectivo para encontrar las soluciones de E. Sin embargo, en [Bak90], Alan Baker ofreció una demostración alternativa que produce una cota superior explícita, aunque poco útil. En particular, si $(x, y) \in \mathbb{Z}^2$ satisface $y^2 = x^3 + Ax + B$ entonces

$$\text{máx}(|x|, |y|) < \exp((10^6 \cdot \text{máx}(|A|, |B|))^{10^6}).$$

De ahora en adelante nos concentramos en encontrar los puntos de la curva E con coordenadas racionales. Introducimos la siguiente notación para dicho conjunto:

$$E(\mathbb{Q}) = \{(x, y) \in E \mid x, y \in \mathbb{Q}\}.$$

Uno de los aspectos más notables de la teoría de curvas elípticas es que el conjunto $E(\mathbb{Q})$ puede ser dotado de una estructura de grupo de naturaleza geométrica. La operación de adición se define del siguiente modo (ver figura 1): dados dos puntos $P, Q \in E(\mathbb{Q})$, sea $\mathfrak{L} = \overline{PQ}$ la línea que pasa por P y Q (si $P = Q$, entonces definimos $\mathfrak{L}$ como la recta tangente a E que pasa por P). Como la curva E está dada por una ecuación de tercer grado, existe un único tercer punto de intersección R en $\mathfrak{L} \cap E$, que también está definido sobre $\mathbb{Q}$,

$$\mathfrak{L} \cap E(\mathbb{Q}) = \{P, Q, R\}.$$

La suma de P y Q, $P + Q$, es por definición el segundo punto de intersección con E de la recta vertical que pasa por R.

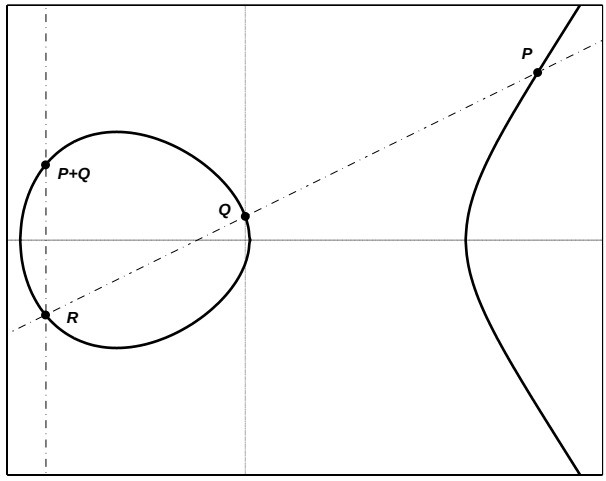

Figura 1: Adición de puntos en curvas elípticas.

Es fácil comprobar que la operación de suma así definida es conmutativa. El *origen* $\mathcal{O}$ es el elemento zero, y para todo punto $P \in E(\mathbb{Q})$ existe un punto $-P$ tal que $P+(-P) = \mathcal{O}$, *i.e.* un inverso aditivo[7]. La adición también satisface la propiedad asociativa (un poco más tedioso de comprobar), y por tanto $(E, +)$ es un grupo abeliano.

La estructura de grupo nos proporciona un método para encontrar soluciones racionales a partir de dos puntos racionales P y Q (cabe la posibilidad de usar $Q = P$). En efecto, dados $P, Q \in E(\mathbb{Q})$ la adición en la curva produce un punto racional $S = P + Q$, y podemos, en general, producir nuevos puntos racionales a partir de P, Q y S.

Ejemplo 4. *Sea E la curva definida por la ecuación de Weierstrass $y^2 = x^3 - 25x$. Hemos visto antes, que si E tiene una solución cuya coordenada x es un cuadrado perfecto e $y \neq 0$, entonces podemos afirmar que $n = 5$ es un número congruente. Fácilmente podemos encontrar un par de puntos racionales de la curva, $P = (-5, 0)$ y $Q = (-4, 6)$. La suma de estos dos puntos produce una nueva solución $P + Q = (45, -300)$. Del mismo modo, los múltiplos de Q son soluciones no triviales, por ejemplo $2Q = (1681/144, -62279/1728)$. Nótese que $x(2Q) = (41/12)^2$ es un cuadrado perfecto*[8]*, y en efecto, esta solución nos permite encontrar el triángulo recto de lados $(3/2,\ 20/3,\ 41/6)$ y área 5.*

Como hemos mencionado antes, $E(\mathbb{Q})$ es un grupo *abeliano* (o conmutativo). El siguiente paso en la clasificación de estos grupos fue dado por Mordell en 1922, que demostró el siguiente teorema:

[7]El inverso aditivo de $P = (x, y)$ es la reflexión de dicho punto con respecto a la recta $y = 0$, esto es $-P = (x, -y)$.

[8]Esto no es casualidad, si E tiene ecuación $y^2 = x^3 - n^2x$ y P es un punto de orden mayor que 2, entonces $x(2P) = (x(P)^2 + n^2)^2/4y(P)^2$.

Teorema 5 **(Mordell-Weil)**. *$E(\mathbb{Q})$ es un grupo abeliano generado por un número finito de puntos racionales.*

André Weil generalizó el teorema a todos los cuerpos de números en su tesis[9] en 1928. Dada la importancia de este teorema, el grupo $E(\mathbb{Q})$ suele ser llamado el grupo de Mordell-Weil. La demostración tiene tres ingredientes fundamentales: el *teorema débil de Mordell-Weil* (ver más adelante); el concepto de *función de altura*[10] para grupos abelianos y el teorema de "*descenso*", el cual establece que un grupo abeliano A con una función de altura h, tal que A/mA es finito (donde m es como en (ii) de la función de altura), es finitamente generado.

Teorema 6 **(Mordell-Weil débil)**. *$E(\mathbb{Q})/mE(\mathbb{Q})$ es un grupo finito para todo $m \geq 2$.*

Louis Mordell (1888-1972) y André Weil (1906-1998).

El teorema de Mordell-Weil, junto al teorema fundamental de clasificación de grupos abelianos finitamente generados, implica que para toda curva elíptica $E/\mathbb{Q}$ el grupo de puntos racionales tiene la siguiente forma:

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{torsión}} \bigoplus \mathbb{Z}^{R_E}$$

[9]El teorema de Mordell-Weil es cierto para curvas elípticas definidas sobre: $\mathbb{Q}$, cualquier cuerpo de números K, cuerpos finitos $\mathbb{F}_q$, cuerpos de funciones $F(T)$ (siendo F cualquiera de los cuerpos mencionados antes). Véase [Sil86], Capítulo VIII, pg. 189 para una prueba detallada.

[10]Una función de altura de un grupo abeliano G es una función $h\colon G \to \mathbb{R}$ tal que (i) para cada $Q \in G$ existe una constante $C_1 = C_1(G, Q)$ tal que para todo $P \in G$ $h(P+Q) \leq 2h(P)+C_1$; (ii) existe un entero $m \geq 2$ y una constante $C_2 = C_2(G)$ tal que para todo $P \in G$, $h(mP) \geq m^2 h(P) - C_2$; (iii) para todo $C_3 \in \mathbb{R}$ el conjunto $\{P \in G : h(P) \leq C_3\}$ es finito. Por ejemplo, si $G = (\mathbb{Q}, +)$ podemos definir una función de altura $h(p/q) = \log(\max\{|p|, |q|\})$. Si E es una curva elíptica, definimos $H(P) = h(x(P))$ donde $P \neq \mathcal{O}$.

donde $E(\mathbb{Q})_{\text{torsión}}$ denota el conjunto de los puntos de *torsión* (o de orden finito), y R_E, que depende de la curva E a estudiar, es un entero no negativo que es llamado el *rango* de la curva elíptica.

El rango de $E/\mathbb{Q}$ es, en cierto sentido, un medidor de la complejidad aritmética de dicha curva. Se desconoce si hay alguna cota superior para los valores posibles de R_E. De hecho, es una conjetura que para todo $n \in \mathbb{N}$ existe una curva elíptica E definida sobre $\mathbb{Q}$ tal que $R_E \geq n$. Sin embargo, hasta ahora sólo se ha demostrado la conjetura hasta $n = 24$ (en [Duj04] se puede examinar una lista con los actuales records y ejemplos de curvas). Este problema, encontrar curvas de alto rango, es ciertamente interesante por su dificultad aritmética y computacional. Una de las piezas clave que nos hace pensar que la conjetura del rango es cierta fue ofrecida por Shafarevich y Tate, al demostrar que existen curvas elípticas definidas sobre cuerpos de funciones $\mathbb{F}_p(T)$ (con coeficientes en un cuerpo finito) con rango arbitrario (véase [ShT67]).

Ejemplo 7. *1. La curva elíptica* $E_1/\mathbb{Q}\colon y^2 = x^3 + 6$ *tiene rango* 0 *y no tiene ninguna solución racional, esto es* $E_1(\mathbb{Q}) \simeq 0$.

2. Sea $E_2/\mathbb{Q}\colon y^2 = x^3 + 1$*, entonces* $E_2(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$*. El grupo de torsión está generado por el punto* $(2, 3)$.

3. $E_3/\mathbb{Q}\colon y^2 = x^3 + 109858299531561$ *satisface* $E_3(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z} \bigoplus \mathbb{Z}^5$ *(véase la web*[11] *del autor para una descripción de los generadores del grupo).*

4. Si definimos $E_4/\mathbb{Q}\colon$ $y^2 + 1951/164xy - 3222367/40344y = x^3 + 3537/164x^2 - 40302641/121032x$, *entonces* $E_4(\mathbb{Q}) \simeq \mathbb{Z}^{10}$.

4 Puntos de Torsión

En esta sección nos concentramos en los puntos de torsión de E. Podemos describir dichos puntos como el conjunto:

$$E(\mathbb{Q})_{\text{torsión}} = \{P \in E(\mathbb{Q}) \mid \exists m \in \mathbb{N} \text{ tal que } m \cdot P = \mathcal{O}\}$$

Ejemplo 8. *La ecuación* $E_n\colon y^2 = x^3 - n^2x$ *tiene tres soluciones triviales,* $P = (0, 0), Q = (-n, 0), R = (n, 0)$*, y es fácil ver (geométricamente) que estos son puntos de orden* 2 *(*$2P = 2Q = 2R = \mathcal{O}$*). De hecho:*

$$E_n(\mathbb{Q})_{\text{torsión}} = \{\mathcal{O}, P, Q, R\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Nótese que el teorema de Mordell-Weil implica que $E(\mathbb{Q})_{\text{torsión}}$ es un grupo abeliano finito. La pregunta es inmediata: *¿qué grupos finitos surgen en este contexto?* Barry Mazur encontró la respuesta:

[11] `http://www.colby.edu/personal/alozano`

Teorema 9 **(Mazur, [Maz77], [Maz78])**. *Sea $E/\mathbb{Q}$ una curva elíptica. Entonces, el subgrupo de torsión $E(\mathbb{Q})_{\text{torsión}}$ es isomorfo exactamente a uno de los siguientes grupos*

$$\mathbb{Z}/N\mathbb{Z} \quad con \quad 1 \leq N \leq 10 \quad ó \quad N = 12$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} \quad 1 \leq N \leq 4$$

Además, existen familias infinitas de curvas elípticas con grupo de torsión isomorfo a cada uno de los grupos de la lista[12].

El teorema de Mazur es, por supuesto, de gran interés dentro de la teoría de curvas elípticas. Una consecuencia útil es que si el orden de un punto racional $P \in E(\mathbb{Q})$ es mayor que 12, entonces P es en verdad de orden infinito y por tanto la curva tiene infinitas soluciones racionales. Excepto este criterio, desde el punto de vista computacional el teorema no ofrece ningún método sistemático para determinar puntos de torsión. El siguiente resultado fue demostrado independientemente por E. Lutz y T. Nagell, y ofrece un algoritmo muy simple.

Teorema 10 **(Nagell-Lutz, [Nag35], [Lut37])**. *Supongamos que $E/\mathbb{Q}$ es una curva elíptica con ecuación de Weierstrass:*

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

Entonces todos los puntos de torsión $P \neq \mathcal{O}$ satisfacen:

1. *Las coordenadas de P son números enteros, es decir $x(P), y(P) \in \mathbb{Z}$.*
2. *Si el orden de P es mayor que 2, entonces $4A^3 + 27B^2$ es divisible por $y(P)^2$.*
3. *Si P es de orden 2, entonces $y(P) = 0$ y $x(P)^3 + Ax(P) + B = 0$.*

Todas las curvas elípticas sobre $\mathbb{Q}$ se pueden transformar en una curva elíptica como la del teorema, por lo que el resultado es totalmente general.

Ejemplo 11. *Sea p un número primo y definamos una curva $E_{3,p}\colon y^2 = x^3 + p^2$. Como $x^3 + p^2 = 0$ no tiene soluciones racionales, $E_{3,p}$ no tiene puntos de orden 2. Además, la lista de todos los cuadrados que dividen $4A^3 + 27B^2 = 27p^4$ es corta, y nos proporcionan los posibles valores de $y(P)$:*

$$y = \pm 1,\ \pm p,\ \pm p^2,\ \pm 3p,\ \pm 3p^2$$

Es claro que $(0, \pm p) \in E_{3,p}$, y con un mínimo de esfuerzo uno puede demostrar que estos son los únicos puntos de torsión en la curva. En concreto, el grupo de torsión de $E_{3,p}$ es isomorfo a $\mathbb{Z}/3\mathbb{Z}$.

[12] Véase [Duj04], y [Kub76] pg. 217, Tabla 3. El lector también puede encontrar ejemplos de todos los grupos de torsión en la *web* del autor.

Definición 12. *Sea E una curva elíptica definida sobre $\mathbb{Q}$, $E\colon y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Q}$. Definimos Δ, el* discriminante *de E, como el número:*

$$\Delta = -16 \cdot (4A^3 + 27B^2)$$

(compárese con el Teorema 10).

5 Curvas Elípticas sobre Cuerpos Finitos

Sea $E/\mathbb{Q}$ una curva elíptica de ecuación $y^2 = x^3 + Ax + B$ con coeficientes enteros, $A, B \in \mathbb{Z}$. Sea p un número primo. Si reducimos cada uno de los coeficientes modulo p, obtenemos la ecuación de una curva cúbica $\widetilde{E}_p$ definida sobre el cuerpo finito $\mathbb{F}_p$ (esto es, el cuerpo que consta de p elementos, $\mathbb{Z}/p\mathbb{Z}$). Recordemos que una de las propiedades de E es ser no singular en todo punto. Sin embargo, esto no garantiza que $\widetilde{E}_p$ no tenga singularidades sobre $\mathbb{F}_p$.

Definición 13. *Decimos que una curva elíptica E tiene buena reducción modulo p si $\widetilde{E}_p$ es una curva no singular. Si $\widetilde{E}_p$ es singular en algún punto, entonces decimos que E tiene mala reducción en p y diferenciamos dos casos:*

1. *Si $\widetilde{E}_p\colon y^2 = (x-\alpha)^2(x-\beta) \mod p$, donde $\alpha, \beta \in \overline{\mathbb{F}_p}$ y $\alpha \neq \beta \mod p$ entonces decimos que E tiene reducción multiplicativa (o semiestable);*
2. *Si $\alpha \equiv \beta \mod p$ entonces E tiene reducción aditiva (o inestable).*

Por lo tanto, para aquellos números primos tales que E tiene buena reducción, $\widetilde{E}_p$ es una curva elíptica definida sobre $\mathbb{F}_p$. Por supuesto, el estudio de curvas sobre cuerpos finitos es mucho más sencillo. Por ejemplo, es fácil encontrar todas las soluciones pues sólo hay p^2 puntos en el plano.

Dada una curva $E/\mathbb{Q}$ sólo un número finito de primos tienen mala reducción y estos son fáciles de encontrar.

Proposición 14. *Sea E una curva elíptica y sea Δ su discriminante. Un número primo p es de mala reducción si y sólo si Δ es divisible por p.*

Las curvas definidas sobre cuerpos finitos han sido estudiadas en profundidad[13] pues la información *local* (cuerpos finitos $\mathbb{F}_q$, cuerpos locales $\mathbb{Q}_p$) de una curva proporciona información fundamental sobre la curva definida sobre cuerpos *globales* ($\mathbb{Q}$, cuerpos de números). Supongamos que $\widetilde{E}$ es una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$, donde $q = p^r$ denota el número de elementos ($p \in \mathbb{Z}$ es un primo). El siguiente teorema nos proporciona una

[13] Las curvas elípticas definidas sobre cuerpos finitos tienen aplicaciones computacionales de gran interés, como la construcción de sistemas de encriptación, algoritmos de factorización o tests de primalidad.

cota de N_q, el número de soluciones de $\widetilde{E}$ sobre dicho cuerpo. El resultado fue conjeturado por Emil Artin (en su tesis) y demostrado por Helmut Hasse en la decada de 1930.

Teorema 15 **(Hasse)**. $q+1-2\sqrt{q} < N_q < q+1+2\sqrt{q}$.

Helmut Hasse (1898-1979)

Las conexiones entre los números N_p y el grupo global $E(\mathbb{Q})$ son numerosas y de gran interés. La relación más sorprendente es la que constituye la conocida conjetura de Birch y Swinnerton-Dyer que relaciona el crecimiento de N_p (al cambiar p) con el rango de la curva elíptica sobre $\mathbb{Q}$ (ver sección 6.2).

En la proposición siguiente detallamos otra interesante conexión. Usamos la siguiente notación: dado un grupo abeliano G, el subgrupo de puntos de torsión de orden m es denotado por $G[m]$.

Proposición 16. *Supongamos que $E/\mathbb{Q}$ es una curva elíptica, sea p primo y m un número natural no divisible por p. Cuando la curva E tiene buena reducción en p, la función inducida al reducir modulo p cada coordenada*

$$E(\mathbb{Q})[m] \longrightarrow \widetilde{E}(\mathbb{F}_p)$$

es un homomorfismo inyectivo de grupos conmutativos. En particular el número de elementos de $E(\mathbb{Q})[m]$ divide al número de elementos de $\widetilde{E}(\mathbb{F}_p)$.

Esta proposición puede resultar muy útil para calcular $E(\mathbb{Q})_{\text{torsión}}$. Veamos una aplicación practica.

Ejemplo 17. *Definamos $E/\mathbb{Q}$: $y^2 = x^3 + 3$. El discriminante de esta curva es $\Delta = -3888 = -2^4 \cdot 3^5$. Recordemos que si p es un primo de mala reducción entonces $p \mid \Delta$. Por tanto los únicos primos de mala reducción son $2, 3$, y $\widetilde{E}_p$ es suave para todo $p \geq 5$. Cuando $p = 5$ obtenemos*

$$\widetilde{E}_5(\mathbb{Z}/5\mathbb{Z}) = \{\widetilde{O}, (1,2), (1,3), (2,1), (2,4), (3,0)\}$$

donde todas las coordenadas son consideradas modulo 5 *(¡y no olvidemos el punto en el infinito!). De modo que la curva* $\widetilde{E}_5$ *sólo tiene* 6 *puntos,* $N_5 = |\widetilde{E}(\mathbb{Z}/5\mathbb{Z})| = 6$. *De manera similar podemos comprobar que* $N_7 = 13$.

Ahora, si $q \neq 5, 7$ *es un número primo, entonces* $E(\mathbb{Q})[q]$ *es trivial. En efecto, la Proposición 16 implica que* $|E(\mathbb{Q})[q]|$ *divide a* $N_5 = 6$ *y a* $N_7 = 13$, *así que* $|E(\mathbb{Q})[q]|$ *debe dividir* $\mathrm{mcd}(6, 13) = 1$.

En el caso de $q = 5$ *sabemos que* $|E(\mathbb{Q})[5]|$ *divide* $N_7 = 13$ *y es fácil probar que si* $E(\mathbb{Q})[p]$ *es no trivial entonces* p *divide su cardinal, y como* 13 *no es divisible por* 5, *concluimos que* $E(\mathbb{Q})[5]$ *es trivial. De manera similar* $E(\mathbb{Q})[7]$ *también es trivial. Por tanto el subgrupo de torsión de* $E(\mathbb{Q})$ *es trivial.*

Nótese que $P = (1, 2) \in E(\mathbb{Q})$ *es un punto obvio en la curva. Como acabamos de probar que* E *no tiene ningún punto de orden finito, se desprende que* P *es de orden infinito, y hemos demostrado que* E *tiene infinitas soluciones racionales* $(\pm P, \pm 2P, \pm 3P, \dots)$. *De hecho:*

$$E(\mathbb{Q}) \cong \mathbb{Z}$$

y $(1, 2)$ *es un generador del grupo.*

6 El Rango y la Parte Libre

Hasta ahora hemos sido capaces de proveer al lector con algoritmos eficientes para determinar el subgrupo de torsión de $E(\mathbb{Q})$. Recordemos que el teorema de Mordell-Weil dice

$$E(\mathbb{Q}) \cong E_{\text{torsión}} \oplus \mathbb{Z}^{R_E}.$$

Así que hemos de encontrar un método para encontrar R_E generadores de la parte "libre" del grupo, los puntos de orden infinito. Desgraciadamente, hasta la fecha no se ha encontrado ningún método. Toda la complejidad aritmética, *endiablada* en multitud de ocasiones, se concentra en este problema. Ni siquiera tenemos a nuestra disposición una fórmula para determinar R_E, el rango de la curva, aunque podemos obtener cotas superiores para cada curva dada E.

Uno podría tener la esperanza de que si los coeficientes de la curva elíptica fueran "pequeños" entonces los generadores (sus coordenadas) deberían ser "pequeños" también, y quizá una búsqueda rápida de puntos proporcionaría todos los generadores. Sin embargo, Bremner y Cassels encontraron un sorprendente contratiempo: la curva elíptica $y^2 = x^3 + 877x$ tiene rango 1, y la coordenada x de un generador P es

$$x(P) = (612776083187947368101/78841535860683900210)^2.$$

Aun así, en [Lan83] Serge Lang propuso vencer este obstáculo, conjeturando que para todo $\epsilon > 0$ existe una constante C_ϵ tal que hay un sistema de generadores $\{P_i : i = 1, \dots, R_E\}$ de $E(\mathbb{Q})$ que satisfacen

$$\hat{h}(P_i) \leq C_\epsilon \cdot |\Delta|^{1/2+\epsilon}$$

donde $\hat{h}$ es la función de altura canónica[14] y Δ es el discriminante de E. Recordemos que la altura de P es básicamente la mitad del logaritmo del máximo entre el numerador y denominador de $x(P)$. Nótese que en el ejemplo anterior $\hat{h}(P) = 47,9901...$ mientras que $|\Delta|^{1/2} = 207773,1275....$ De modo que la conjetura dice que las coordenadas de generadores pueden crecer de manera exponencial con el discriminante de la curva.

6.1 Cotas Superiores del Rango

La demostración del teorema débil de Mordell-Weil se basa en incluir el grupo $A = E(\mathbb{Q})/2E(\mathbb{Q})$ en otro grupo B (normalmente $B \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$ ó $B = S^2(E,\mathbb{Q})$, un grupo de Selmer, ver sección 6.3) y se establece una cota explícita del orden de B, que fácilmente nos ofrece información sobre R_E, el rango de E. Por ejemplo, el siguiente resultado es consecuencia de los métodos que veremos en 6.3:

Teorema 18 **([Mil96], Proposición 16.8)**. *Sea $E/\mathbb{Q}$ una curva elíptica definida por la ecuación:*

$$E\colon y^2 = x(x-c)(x-d), \text{ con } c,d \in \mathbb{Z}$$

y supongamos que E tiene $s = m + a$ primos de mala reducción, siendo m y a el número de primos de reducción multiplicativa y aditiva respectivamente. Entonces:

$$R_E \leq m + 2a - 1.$$

Ejemplo 19. *Pierre de Fermat demostró que $n = 1$ no es un número congruente usando la ecuación $x^4 + y^4 = z^2$, la cual no tiene soluciones (este es un caso particular de su "último" teorema para el que si que encontró un margen suficientemente ancho y escribió una demostración completa). Como aplicación del teorema anterior, podemos probar que la curva*

$$E_1\colon y^2 = x^3 - x = x(x-1)(x+1)$$

no tiene más que las soluciones triviales de orden 2. En efecto, el discriminante de E_1 es $\Delta = 64$, por tanto $p = 2$ es el único primo de mala reducción, y ésta es multiplicativa. El teorema 18 nos permite concluir que $R_{E_1} = 0$ y E_1 sólo tiene puntos de torsión. Finalmente, el teorema de Nagell-Lutz implica que los únicos puntos de torsión son de orden 2.

[14] La función de altura canónica satisface $2\hat{h}(P) = H(P) + O(1)$ donde H es la función de altura definida en la nota (8). En concreto $\hat{h}(P) = \frac{1}{2}\lim_{N\to\infty} 4^{-N} H(2^N \cdot P)$.

6.2 La Conjetura de Birch y Swinnerton-Dyer

Comenzamos esta sección definiendo una función de manera analítica que incluye información "local" sobre la curva elíptica $E/\mathbb{Q}$: la función[15] L de E. Sea p un primo de buena reducción de E (esto es, $p \nmid \Delta$), N_p el número de puntos en $\widetilde{E}_p(\mathbb{F}_p)$, y definamos la función L local:

$$L_p(T) = 1 - a_p T + pT^2$$

donde $a_p = p + 1 - N_p$ es lo que se denomina traza de la función de *Frobenius*. De modo similar, se definen factores $L_p(T)$ para los primos de mala reducción ($L_p(T) = 1$ si la reducción es aditiva, y $1 - T$ ó $1 + T$ si es multiplicativa, dependiendo si es *split* o no, ver [Sil86], pg. 180, 360). La función L de E se define como:

$$L(E/\mathbb{Q}, s) = \prod_p L_p(p^{-s})^{-1}.$$

El producto converge y la función así definida es holomorfa para todo $s \in \mathbb{C}$ con parte real mayor que $3/2$. La conjetura de Shimura-Taniyama, demostrada por Breuil, Conrad, Diamond, Taylor y Wiles [BCD01], [Wil95], implica que $L(E/\mathbb{Q}, s)$ tiene una continuación analítica a todo el plano complejo y satisface la ecuación funcional:

$$\Lambda(s) = w_E \cdot \Lambda(2 - s) \tag{4}$$

donde $w_E = \pm 1$ y $\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s)$, para cierto número natural N, llamado el *conductor* de E.

En 1963, B. Birch y Sir H. P. F. Swinnerton-Dyer [BSD63] publicaron datos sobre el estudio de un gran número de curvas elípticas, que les llevó a proponer la siguiente famosa conjetura:

Conjetura 20 **(Birch y Swinnerton-Dyer)**. *La función $L(E/\mathbb{Q}, s)$ tiene un cero en $s = 1$ con multiplicidad exactamente igual al rango de E. En otras palabras, la serie de Taylor de L en el punto $s = 1$ satisface:*

$$L(E/\mathbb{Q}, s) = c \cdot (s - 1)^{R_E} + O((s - 1)^{R_E + 1}), \quad c \neq 0.$$

Se ha logrado caracterizar el residuo de L en $s = 1$ (el número c) como el producto de ciertos conocidos invariantes de la curva. La conjetura ha sido comprobada en numerosos casos, y demostrada sólo en casos muy particulares[16]:

[15] La notación de las *funciones L* fue introducida por Dirichlet, cuyo nombre completo era Johann Peter Gustav Lejeune-Dirichlet. La función L para curvas elípticas fue introducida por Hasse y Weil.

[16] Recientemente Douglas Ulmer [Ulm02] ha demostrado que la conjetura es cierta para cierta familia de curvas elípticas definidas sobre $\mathbb{F}_p(T)$ y entre las cuales se encuentran curvas con rango arbitrariamente grande.

Teorema 21 **(B. Gross, V. Kolyvagin, D. Zagier)**.

1. $L(E/\mathbb{Q},1) \neq 0 \Rightarrow R_E = 0$,
2. $L(E/\mathbb{Q},1) = 0, L'(E/\mathbb{Q},1) \neq 0 \Rightarrow R_E = 1$.

Ejemplo 22. *Sea $E/\mathbb{Q}$ la curva elíptica $y^2 = x^3 - 157^2 x$. El teorema 18 indica que $R_E \leq 1$ y una búsqueda rápida por ordenador no revela ningún punto racional no trivial. Sin embargo, el mismo ordenador nos dice que $L(E,1) \cong 10^{-28}$ y $\frac{d}{ds}L(E,s)|_{s=1} = 11,4259444....$ El teorema de Kolyvagin et al. nos hace pensar que debemos volver a buscar puntos, esta vez con más paciencia, hasta que encontramos uno cuya coordenada x es:*

$$x(P) = \left(\frac{2244035177043369699245575130906748631609484720 41}{1782466453785771917605107035793432714003296166 0}\right)^2$$

y por tanto $n = 157$ es un número congruente. Si uno no es tan paciente como para buscar por tanto tiempo (el numerador de $x(P)$ tiene 94 dígitos), se ha de utilizar el método del 2-descenso.

La conjetura de Birch y Swinnerton-Dyer tiene muchas e importantes consecuencias, como por ejemplo la *conjetura de la paridad*:

Conjetura 23. *Si el rango R_E de una curva elíptica E es par, entonces el signo de la ecuación funcional (4) es $w_E = 1$ y si R_E es impar $w_E = -1$.*

Si asumimos esta conjetura entonces se puede demostrar que un número natural n es congruente si y sólo si $n \equiv 5,\ 6$ ó $7 \mod 8$.

6.3 El Grupo de Selmer y el 2-Descenso

Como hemos mencionado, para poder formular con precisión su famosa conjetura, Birch y S.-Dyer necesitaron analizar una cantidad ingente (para la época) de curvas elípticas haciendo uso del ordenador EDSAC II de la Universidad de Cambridge. Por supuesto, les era imprescindible averiguar el rango de cada curva y calcular el grupo de Mordell-Weil. Para ello, perfeccionaron un método de J. W. S. Cassels, el algoritmo de *descenso*. Aunque es la mejor herramienta a nuestra disposición, no es un algoritmo[17] en el sentido estricto de la palabra, pues no está garantizado que este termine en tiempo finito. En esta sección describimos un caso particular, el *Descenso via 2-isogenia*.

El método es, básicamente, una demostración muy explícita del teorema débil de Mordell-Weil. El objetivo, determinar $E(\mathbb{Q})$ y/o R_E, se cumple si somos capaces de calcular un sistema de generadores de $A_2 = E(\mathbb{Q})/2E(\mathbb{Q})$.

[17] J. Cremona ha implementado el algoritmo en un programa, *mwrank*, que se puede obtener en su web [Cre04] y que maximiza la eficiencia del método.

El grupo A_2 puede ser incluido en un grupo de naturaleza cohomológica, el *grupo de Selmer* $S^{(2)}(E/\mathbb{Q})$, más fácil de calcular[18]. Estos grupos forman una secuencia exacta:

$$0 \longrightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow S^{(2)}(E/\mathbb{Q}) \longrightarrow TS(E/\mathbb{Q})[2] \longrightarrow 0$$

donde $TS(E/\mathbb{Q})$ es el *grupo de Tate-Shafarevich* (la notación $G[n]$ indica el subgrupo de n-torsión de G). Cada elemento del grupo de Selmer puede ser interpretado como un *espacio homogéneo*, una curva auxiliar que tiene soluciones p-ádicas (en $\mathbb{Q}_p$) para todo primo p. Aquellos espacios homogéneos que tienen una solución racional (en $\mathbb{Q}$) proporcionan un punto no trivial en A_2 y por tanto en $E(\mathbb{Q})$. El grupo $TS(E/\mathbb{Q})$ está formado por aquellos espacios homogéneos que no poseen puntos racionales a pesar de ser localmente resolubles y, por tanto, el grupo de Tate-Shafarevich constituye el mayor obstáculo a la hora de calcular $E(\mathbb{Q})$.

El lector puede consultar una versión extendida de este artículo en la *web* del autor, donde se describe el método del 2-descenso y se definen los grupos de Selmer y Tate-Shafarevich en detalle.

Lecturas Recomendadas

Los excelentes libros de J. Silverman [Sil86], [Sil94] son la referencia estándar y de lectura obligada. En internet y de forma gratuita se encuentran dos libros también muy recomendables, [Mil96] y [Ivo04]. En 2002, Rubin y Silverberg [RuS02] publicaron una exposición sobre rangos de curvas que cuenta con una extraordinaria bibliografía actualizada. Por último, los algoritmos para curvas elípticas se pueden encontrar (con muchas mejoras y sugerencias para su implementación) en [Cre04] y [Coh00].

Agradecimientos

Quisiera dar las gracias a Julio Lozano y David Rohrlich por leer el manuscrito. Sus comentarios fueron de gran utilidad en la redacción del artículo.

Referencias

[Bak90] Alan Baker, *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1990.

[18] El método de *descenso* en general estudia los grupos $E(\mathbb{Q})/2^nE(\mathbb{Q})$ incluidos en los grupos de Selmer $S^{2^n}(E/\mathbb{Q})$.

[BSD63] B. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves (I) and (II), *J. Reine Angew. Math.* **212** (1963), 7–25 and **218** (1965), 79–108.

[BCD01] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[Coh00] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, New York, 2000.

[Cre97] John Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997 (disponible en su web).

[Cre04] John Cremona, Página *web*: `http://www.maths.nott.ac.uk/personal/jec/`

[Duj04] Andrej Dujella, Página *web*: `http://www.math.hr/∼duje/`

[Har77] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977.

[Ivo04] Carlos Ivorra Castillo, *Curvas Elípticas*. Disponible en: `http://www.uv.es/∼ivorra/Libros/Elipticas.pdf`

[Kub76] Daniel S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc. (3)* **33** (1976) 193–237.

[Lan83] Serge Lang, *Conjectured Diophantine estimates on elliptic curves*, Progress in Math. 35, Birkhäuser, 1983.

[Lut37] E. Lutz, Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps p-adic, *J. Reine Angew. Math.* **177** (1937), 431–466.

[Mat93] Yuri V. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, Massachusetts, 1993.

[Maz77] Barry Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[Maz78] Barry Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[Mil96] James Milne, *Elliptic Curves*, notas de su curso en la web, V 1.01, 1996, `http://www.jmilne.org/math/CourseNotes/math679.html`

[Nag35] T. Nagell, *Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre*, Wid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[RuS02] Karl Rubin, Alice Silverberg, Ranks of Elliptic Curves, *Bull. Amer. Math. Soc.* **39** (2002), no. 4, 455–474.

[Ser97] J.P. Serre, *Galois Cohomology*, Springer-Verlag, New York, 1997.

[ShT67] I. R. Shafarevich, J. Tate, The rank of elliptic curves, *AMS Transl.* **8** (1967), 917–920.

[Shi71] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, Princeton, New Jersey, 1971.

[Sil86] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.

[SiT92] Joseph H. Silverman, John Tate, *Rational Points on Elliptic Curves*. Springer-Verlag, New York, 1992.

[Ulm02] Douglas Ulmer, Elliptic curves with large rank over function fields, *Ann. of Math.* **155** (2002), 295–315.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, *Ann. of Math.* **141** (1995), no. 3, 443–551.

Álvaro Lozano Robledo
Department of Mathematics
Colby College
Mayflower Hill 5830
Waterville, ME 04901
Estados Unidos de América
Correo electrónico:alozano@colby.edu