Miscelánea Matemática **42** (2006) 1–17 SMM

Del teorema de Pitágoras a la aritmética de curvas elípticas

Felipe Zaldívar

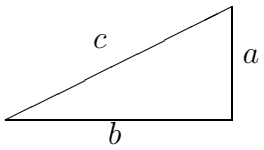
Departamento de Matemáticas

Universidad Autónoma Metropolitana-I

fzc@oso.izt.uam.mx

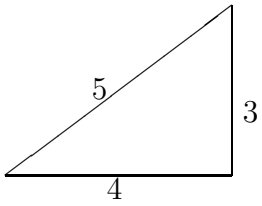
Dado un número racional $A > 0$, ¿existe un *triángulo rectángulo* (a, b, c) con lados racionales tal que A sea el área de ese triángulo?:

$$a^2 + b^2 = c^2 \qquad A = \frac{ab}{2}$$



Usaremos la notación (a, b, c) para el triángulo rectángulo con catetos $a < b$ e hipotenusa c.

Ejemplo 1. El triángulo $(3, 4, 5)$ tiene área $A = 6$:



$$A = \frac{ab}{2} = 6$$

En un resumen de algunos de sus trabajos sobre teoría de números que envió a Huygens en 1659, Fermat afirma que ha demostrado, por un *método singular* que él llama *descenso infinito*, entre otros teoremas, que *no existe un triángulo rectángulo con lados enteros cuya área*

sea el cuadrado de un entero. En esta carta Fermat sólo bosqueja la idea general del método de descenso infinito y para los detalles se excusa afirmando que *alargarían demasiado la carta*. Afortunadamente esta vez los detalles de la demostración de este resultado sí cupieron en el margen de su ejemplar de la Arithmetica de Diofanto, junto a la última proposición de esta obra. Esencialmente el argumento se puede variar probando primero que la ecuación $x^4 - y^4 = z^2$ no tiene soluciones enteras no triviales, un resultado que Fermat demuestra usando el método de descenso infinito, en forma análoga a como se demuestra que la ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras no triviales y luego la usa para concluir que la ecuación $x^4 + y^4 = z^4$ no tiene soluciones enteras no triviales.

Teorema 1 (Fermat). *Ningún cuadrado de un entero puede ser el área de un triángulo rectángulo con lados enteros.*

Demostración: Supongamos que el área de un triángulo rectángulo (a, b, c) con lados enteros tiene área el cuadrado de un entero m, i.e., que $(1/2)ab = m^2$. Entonces,

$$(a + b)^2 = a^2 + b^2 + 2ab = c^2 + 4m^2$$

y

$$(a - b)^2 = a^2 + b^2 - 2ab = c^2 - 4m^2$$

de donde se sigue que

$$(a^2 - b^2)^2 = (a - b)^2(a + b)^2 = c^4 - (2m)^4$$

por lo que la ecuación $z^2 = x^4 - y^4$ tendría la solución no trivial $x = c$, $y = 2m$, $z = a^2 - b^2$, en contradicción con el resultado de Fermat mencionado antes. □

Números congruentes. Los matemáticos árabes del siglo X formulaban el problema anterior de la forma siguiente: si $A > 0$ es un racional positivo, tal que existe un triángulo rectángulo (a, b, c) con lados racionales y área A, entonces:

$$A = \frac{ab}{2} \qquad \text{y} \qquad a^2 + b^2 = c^2$$

de tal forma que los racionales A, a, b, c deben satisfacer estas dos ecuaciones. Sumando o restando 4 veces la primera ecuación a la segunda obtenemos

$$(a \pm b)^2 = c^2 \pm 4A$$

que dividiendo entre 4 queda:

$$(*) \qquad \frac{1}{4}(a \pm b)^2 = \left(\frac{c}{2}\right)^2 \pm A$$

y poniendo $x = (c/2)^2$ se tiene que

$$x \pm A = \left(\frac{1}{2}(a \pm b)\right)^2$$

es decir, $x + A$ y $x - A$ son cuadrados de números racionales. Como x también es el cuadrado de un racional, hemos probado que, *dado $A > 0$ un racional, existe un racional x tal que $x - A, x, x + A$ son cuadrados de racionales*. En otras palabras, dado el racional $A > 0$, existen tres cuadrados racionales en progresión aritmética con diferencia común (*congruum*, en latín) A. Se dice entonces que el racional $A > 0$ es un *número congruente*. Recíprocamente, dado $A > 0$ un racional tal que existe $x \in \mathbb{Q}$ con la propiedad de que $x - A, x, x + A$ son cuadrados de racionales, entonces $\sqrt{x - A}$, $\sqrt{x}$ y $\sqrt{x + A}$ son racionales por lo que

$$a = \sqrt{x + A} - \sqrt{x - A}, \quad b = \sqrt{x + A} + \sqrt{x - A} \quad \text{y} \quad c = 2\sqrt{x}$$

son racionales. Se tiene además que

$$a^2 + b^2 = (\sqrt{x + A} - \sqrt{x - A})^2 + (\sqrt{x + A} + \sqrt{x - A})^2 = 4x = c^2$$

y

$$\frac{1}{2}ab = \frac{1}{2}(\sqrt{x + A} - \sqrt{x - A})(\sqrt{x + A} + \sqrt{x - A}) = \frac{1}{2}(2A) = A$$

por lo que A es el área de un triángulo rectángulo (a, b, c) con lados racionales. Finalmente, si (a, b, c) y (a', b', c') son dos triángulos rectágulos con lados racionales tales $x = (c/2)^2 = (c'/2)^2$, entonces $c = c'$ ya que ambos son positivos. Así, $a^2 + b^2 = a'^2 + b'^2$ y como además $(1/2)ab = (1/2)a'b'$, entonces $2ab = 2a'b'$ por lo que

$$(a + b)^2 = (a' + b')^2$$

de donde se sigue que $a + b = a' + b'$ ya que ambos son positivos. Similarmente se prueba que $a - b = a' - b'$. Sumando y restando estas dos últimas igualdades se sigue que $a = a'$ y $b = b'$. Hemos así probado el teorema siguiente:

Teorema 2. *Dado un racional $A > 0$, existe una biyección entre los triángulos rectángulos (a, b, c) con lados racionales y área A y los racionales x tales que $x - A, x, x + A$ son cuadrados de racionales.* □

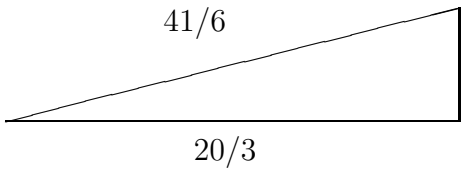
Observemos ahora que, sin perder generalidad, el racional $A > 0$ se puede suponer que es un *entero libre de cuadrados*. En efecto, dado el racional $A > 0$ podemos encontrar $s \in \mathbb{Q}$ tal que $D = s^2 A$ es un entero positivo libre de cuadrados. Ahora, si A es un número congruente, entonces existe un triángulo racional (a, b, c) tal que $A = (1/2)ab$. Se sigue que el triángulo racional (as, bs, cs) satisface que

$$\frac{1}{2}(asbs) = \frac{1}{2}abs^2 = As^2 = D,$$

por lo que D es un número congruente.

Con la reformulación en el teorema 2, podemos ahora recordar cómo se obtuvo, antes de Fermat, un ejemplo no trivial de un número congruente, a saber, el número 5. Este ejemplo se suele atribuir a Leonardo de Pisa, Fibonacci, quien nació en Pisa, Italia alrededor del año 1170 y por temporadas vivió en el norte de Africa y en Constantinopla y también visitó en otras ocasiones Siria y Egipto a finales del siglo XII, donde muy probablemente tuvo contactos con los matemáticos de esos lugares, antes de establecerse en su ciudad natal. En alguna ocasión, cuando el emperador Federico II visitó Pisa, Leonardo fue invitado a su corte para participar en los diálogos y discusiones intelectuales en presencia del emperador, como se estilizaba entonces, y se sabe que Fibonacci fue retado a encontrar tres cuadrados racionales en progresión aritmética con diferencia común 5. La respuesta de Fibonacci se encuentra en su *Liber Quadratorum* de 1225, una obra no tan conocida como su *Liber Abaci* pero que contiene muchas gemas como la de este ejemplo. Fibonacci comienza observado que el área de un triángulo rectángulo pitagórico debe ser un múltiplo de 6; por lo tanto, dice, podemos tomar como el cuadrado del entero, digamos m, un múltiplo de 6. Tomando $m = 6$, Fibonacci escribe el triángulo $(9, 40, 41)$ cuya área es $(1/2)(9)(40) = 180 = 5 \times 36$. Dividiendo entre 36 obtiene el triángulo rectángulo con lados racionales $(3/2, 20/3, 41/6)$ cuya área es 5. Siendo la corte de Federico II un punto de encuentro de las herencias de las culturas griega y latina con la cultura árabe y aún cuando no hay evidencia de que Fibonacci estuviera familiarizado con todos estos lenguajes y sus conocimientos matemáticos, es plausible suponer que ciertamente conocía la reformulación del problema de los números congruentes en términos geométricos.

Ejemplo 2. El triángulo $(3/2, 20/3, 41/6)$ tiene área $A = 5$:



$$A = \frac{ab}{2} = 5$$

Tabla de ejemplos. Los ejemplos anteriores más algunos otros los resumimos en la tabla siguiente:

A	Triángulo (a, b, c) con área A
1	no hay
2	no hay
3	no hay
5	$(3/2, 20/3, 41/6)$
6	$(3, 4, 5)$
7	$(24/25, 7/12, 337/300)$
41	$(40/3, 123/20, 881/60)$

Puntos racionales en ciertas cúbicas. Supongamos ahora que A es un entero libre de cuadrados y es un número congruente. Por el teorema 2 existe un racional x tal que $x-A$, x, $x+A$ son cuadrados de racionales y como A es libre de cuadrados entonces x es diferente de cero y de $\pm A$. Se sigue que el producto de estos tres números es un cuadrado también, i.e., $x^3 - A^2x = y^2$, para $y \in \mathbb{Q}$. En otras palabras, el punto (x, y) con coordenadas racionales está en la curva definida por la ecuación cúbica

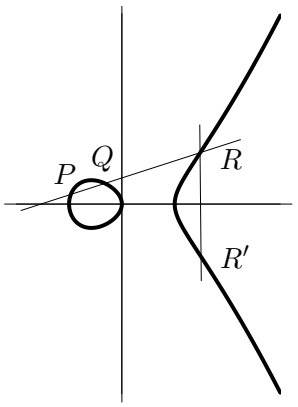
$$y^2 = x^3 - A^2x$$

y además no es uno de los puntos obvios: $(0, 0)$, $(-A, 0)$, $(A, 0)$. Hemos así probado el teorema siguiente. La afirmación recíproca la demostraremos después de recordar algunos hechos sobre curvas en el párrafo siguiente.

Teorema 3. *Sea $A > 0$ un racional positivo. Si existe un triángulo rectángulo (a, b, c) con lados racionales y área A, entonces la ecuación cúbica $y^2 = x^3 - A^2x$ tiene una solución racional (x, y) distinta de $(0, 0), (-A, 0), (A, 0)$.* □

Curvas elípticas. La curvas cúbicas anteriores satisfacen que el polinomio en x (en el lado derecho de $y^2 = x^3 - A^2x$) tiene sus tres raíces

diferentes y por lo tanto son curvas lisas y más aún, son curvas de género $g = 1$, al considerarlas no como curvas afines sino como curvas en el plano proyectivo $\mathbb{P}^2$ al tomar el polinomio homogéneo asociado $y^2z = x^3 - A^2xz^2$, que sigue siendo un polinomio con coeficientes racionales. Esta curva proyectiva contiene al punto racional (i.e., con coordenadas racionales) $\mathbf{0} := (0, 1, 0) \in E$; se dice entonces que E es una *curva elíptica* definida sobre $\mathbb{Q}$. Nos interesa entonces el conjunto $E(\mathbb{Q})$ de puntos con coordenadas racionales de E. El conjunto $E(\mathbb{Q})$ puede ser *finito* o *infinito*, dependiendo de la curva elíptica en consideración. Sin embargo, hay una propiedad adicional de E (y de $E(\mathbb{Q})$) que no tienen las otras curvas de género distinto de 1. Dicho rápidamente: el conjunto de puntos de E tiene estructura de *grupo conmutativo* con operación definida como sigue: dados dos puntos P, Q en E, considerando la recta secante que pasa por ellos (tangente, si $P = Q$), sea R el tercer punto donde esta recta corta a E (este punto existe por el teorema de Bezout) y luego consideremos la recta que pasa por R y el punto $\mathbf{0}$ y sea R' el tercer punto donde esta recta (que hemos dibujado como una recta vertical en la figura siguiente) intersecta a E. La suma $P + Q$ se define como R'. Se prueba directamente que, con esta operación, E es un grupo abeliano, donde la única parte laboriosa es la demostración de la asociatividad de la operación, pero todo lo anterior se puede simplificar mediante una demostración más conceptual usando los elementos de la geometría algebraica.



La operación de grupo. Para la curva elíptica E_A dada por $y^2 = x^3 - A^2x$ con polinomio homogéneo asociado $y^2z = x^3 - A^2xz^2$, el *punto al infinito* $\mathbf{0} = (0, 1, 0)$ servirá como *elemento neutro* ya que es un *punto de inflexión* de E_A por lo que la recta tangente que pasa por

$\mathbf{0} = (0,1,0)$ corta a E_A en $\mathbf{0} = (0,1,0)$ y así $\mathbf{0} + \mathbf{0} = \mathbf{0}$. El *inverso aditivo* de $P \in E_A$ está dado por el punto $-P$ obtenido como el tercer punto donde la recta por P y $\mathbf{0} = (0,1,0)$ corta a E_A. Por lo tanto, si $P = (x_0, y_0)$, como la recta por P y $\mathbf{0} = (0,1,0)$ tiene ecuación $x = x_0$ (es vertical), entonces se tiene que $-P = (x_0, -y_0)$. Se sigue que los puntos de orden 2 de E_A, los cuales satisfacen que $-P = P$, son los puntos sobre el eje X y así hay 3 de estos puntos que son los obvios $(0,0)$, $(A,0)$ y $(-A,0)$.

Dados ahora dos puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ en E_A queremos una fórmula explícita para las coordenadas (x_3, y_3) de la suma $P+Q$ en E_A. Note que podemos suponer que $Q \neq -P$, i.e., que P y Q no están en una recta vertical, porque de lo contrario al considerar la recta que pasa por P y Q el tercer punto de intersección con E_A sería el punto al infinito $\mathbf{0}$. Denotemos con R al punto donde la recta siguiente corta a la curva E_A:

$$\mathcal{L} : y = mx + b = \begin{cases} \text{recta secante que pasa por } P \text{ y } Q & \text{si } P \neq Q, \\ \text{recta tangente que pasa por } P & \text{si } P = Q, \end{cases}$$

procedemos a calcular la pendiente m y la ordenada b en cada uno de los dos casos anteriores:

En el caso $P \neq Q$,

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

y substituyendo este valor de m y las coordenadas de $P = (x_1, y_1)$ en $y = mx + b$, obtenemos la ordenada

$$b = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Finalmente, en el caso $P = Q$, calculamos $m = dy/dx$ mediante derivación implícita de $y^2 = x^3 - A_2 x$ para obtener $2yy' = 3x^2 - A^2$ de donde despejamos y' substituyendo (x, y) por (x_1, y_1) de tal forma que

$$m = y' = \frac{3x_1^2 - A^2}{2y_1}$$

y substituyendo este valor de m y los valores (x_1, y_1) en $y = mx + b$ despejamos la ordenada b para obtener

$$b = y_1 - \Big(\frac{3x_1^2 - A^2}{2y_1}\Big)x_1 = \frac{2y_1^2 - 3x_1^3 + A^2 x_1}{2y_1}$$

y como $y_1^2 = x_1^3 - A^2x_1$, entonces

$$b = \frac{2(x_1^3 - A^2x_1) - 3x_1^3 + A^2x_1}{2y_1} = \frac{-x_1^3 - A^2x_1}{2y_1}.$$

Podemos ahora calcular $P + Q$ explícitamente, escribiendo primero el polinomio que define a la curva E_A como $F(x, y) = x^3 - A^2x - y^2$ y substituyendo $y = mx + b$ para obtener

$$(*) \qquad F(x, mx + b) = x^3 - A^2x - (mx + b)^2$$

donde P, Q, R están en la recta $\mathcal{L}$ y en la curva E_A por lo que las coordenadas x_1, x_2, x_3 de estos puntos satisfacen la ecuación anterior y, contando multiplicidades, estas deben ser las tres raíces de $(*)$. Se sigue que

$$(x - x_1)(x - x_2)(x - x_3) = F(x, mx + b) = x^3 - A^2x - (mx + b)^2$$

de donde desarrollando los productos de los dos lados y comparando los términos con x^2 se obtiene que $-(x_1 + x_2 + x_3) = -m^2$ por lo que

$$x_3 = m^2 - x_1 - x_2$$

y así

$$y_3 = mx_3 + b$$

de donde se sigue que: para el caso $P \neq Q$, las coordenadas del punto $P + Q = R' = (x', y')$ son

$$\begin{aligned} x' = x_3 &= \Big(\frac{y_2 - y_1}{x_2 - x_1}\Big)^2 - x_1 - x_2 \\ y' = -y_3 &= -mx_3 - b. \end{aligned}$$

Finalmente, en el caso $P = Q$, para calcular las coordenadas de $2P = P + P$, usando los valores obtenidos previamente para m y b se tiene que la abscisa $x(2P)$ de $2P$ es:

$$\begin{aligned} x(2P) = m^2 - x_1 - x_2 &= \Big(\frac{3x_1^2 - A^2}{2y_1}\Big)^2 - 2x_1 \\ &= \frac{9x_1^4 - 6A^2x_1^2 + A^4 - 8x_1y_1^2}{4y_1^2} \\ &= \frac{x_1^4 + 2A^2x_1^2 + A^4}{4x_1^3 - 4A^2x_1} \end{aligned}$$

(usando que $y_1^2 = x_1^3 - A^2x_1$). Una consecuencia importante de estas fórmulas es el recíproco del teorema 3:

Teorema 4. *Sea A un entero libre de cuadrados y supongamos que existe un punto racional $P = (x_1, y_1)$ en E_A diferente de los cuatro puntos obvios $(0,0), (-A,0), (A,0)$ y $\mathbf{0}$. Entonces, A es un número congruente.*

Demostración: Como $P = (x_1, y_1)$ es diferente de los puntos obvios, entonces $y_1 \neq 0$ y P no tiene orden 1 ó 2. Se sigue que $2P \neq \mathbf{0}$ y si escribimos $2P = (x_2, y_2)$, si $y = mx + b$ es la recta tangente a E_A en P, de las fórmulas de duplicación anterior se tiene que $y_2 = -mx_2 - b$ y como (x_2, y_2) satisface la ecuación $y^2 = x^3 - A^2x$ entonces $(x_2, -y_2)$ también satisface la misma ecuación. Más aún, el punto $(x_2, -y_2)$ también está en la recta $y = mx+b$ porque $y_2 = -mx_2 - b$ por las fórmulas de duplicación. Se sigue que los dos puntos (x_1, y_1) y $(x_2, -y_2)$ satisfacen las ecuaciones $y^2 = x^3 - A^2x$ y $y = mx + b$, por lo que satisfacen la igualdad

$$(\dagger) \qquad x(x-A)(x+A) = x^3 - A^2x = (mx+b)^2$$

y como $y = mx + b$ es tangente a E_A en x_1, se sigue que la raíz x_1 de $(\dagger)$ es de multiplicidad 2, por lo que las tres raíces de $(\dagger)$ son x_2, x_1, x_1 y por lo tanto

$$x(x-A)(x+A) - (mx+b)^2 = (x-x_2)(x-x_1)^2$$

y poniendo $x = 0$ se sigue que $-(b)^2 = (-x_2)(-x_1)^2 = -x_2x_1^2$, y como x_1 es distinto de 0 porque P es diferente de los puntos obvios, podemos despejar a x_2 de la última igualdad para obtener que $x_2 = (b/x_1)^2$ es el cuadrado de un racional. Similarmente se prueba que $x_2 - A$ y $x_2 + A$ también son cuadrados de racionales y hemos mostrado así que $x_2 - A, x_2, x_2 + A$ son cuadrados en $\mathbb{Q}$ y por lo tanto A es un número congruente. □

Ejemplo 3. (Fermat) El entero $A = 2$ no es un número congruente. En efecto, si 2 fuera congruente la ecuación $y^2 = x^3 - 4x$ tendría una solución diferente de las 4 obvias. Transformando esta ecuación mediante el cambio de variables

$$x = \frac{2}{Y - X^2} \qquad y = \frac{4X}{Y - X^2}$$

la ecuación anterior queda

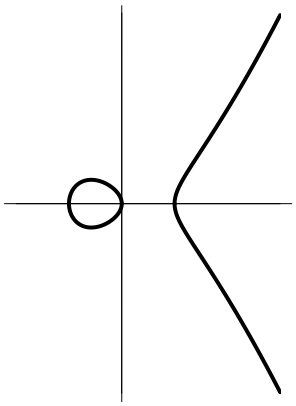
$$\frac{16X^2}{(Y-X^2)^2} = \frac{8}{(Y-X^2)^3} - \frac{8}{Y-X^2}$$

i.e.,

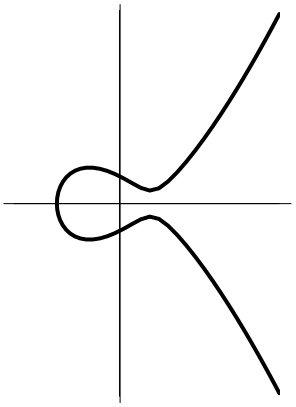
$$16X^2(Y - X^2) = 8 - 8(Y - X^2)^2$$

de donde se sigue que $Y^2 = X^4 + 1$ tendría una solución racional no trivial, la cual podemos escribir como $X = u/v$, $Y = w/v$. Substituyendo en $Y^2 = X^4+1$ obtenemos que $(w/v)^2 = 1+(u/v)^4$, i.e., $(vw)^2 = v^4+u^4$ por lo que la ecuación $x^4+y^4 = z^2$ tendría una solución en $\mathbb{Z}$ no trivial, en contradicción con el resultado de Fermat recordado al principio.

Para cualquier curva elíptica E definida sobre los racionales, al graficar sus partes reales se tienen dos casos, ilustrados por los ejemplos siguientes:



$y^2 = x^3 - x$



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

y al proyectivizar añadiendo el punto al infinito $\mathbf{0}$ a la parte real de la curva, topológica y diferenciablemente se obtienen uno o dos círculos, lo cual quiere decir que el grupo $E(\mathbb{R})$ de puntos reales de E es el grupo S^1 ó el grupo $S^1 \oplus \mathbb{Z}/2$. Se sigue que el grupo de puntos con coordenadas racionales $E(\mathbb{Q})$ es un subgrupo de S^1 ó de $S^1 \oplus \mathbb{Z}/2$. Poincaré conjeturó el teorema siguiente cuya primera demostración la obtuvo Mordell y que aquí sólo citaremos, remitiendo al lector a las referencias para su demostración:

Teorema 5 (Mordell, 1922). *El grupo $E(\mathbb{Q})$ es finitamente generado.* □

Así, el grupo $E(\mathbb{Q})$ se puede separar en un subgrupo finito o de torsión $E(\mathbb{Q})_{\text{tor}}$ y un subgrupo libre de rango finito $\mathbb{Z}^r$:

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tor}} \oplus \mathbb{Z}^r$$

donde al entero $r \geq 0$ se le llama el *rango* de $E(\mathbb{Q})$.

Regresando ahora a la curva elíptica $E_A:\ y^2 = x^3 - A^2x$ que nos interesa, calcularemos su subgrupo de torsión, para después probar un criterio, en términos del rango del grupo $E_A(\mathbb{Q})$ para que A sea o no congruente. Con este objetivo, necesitaremos los resultados siguientes:

Reducción módulo p. Si p es un primo, el morfismo $r_p : \mathbb{Z} \to \mathbb{Z}/p =: \mathbb{F}_p$ de reducción módulo p se puede extender al plano proyectivo para definir una función $r_p : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$, simplemente observando que si $P = (a, b, c) \in \mathbb{P}^2(\mathbb{Q})$, multiplicando por un entero adecuado se puede suponer que a, b, c son enteros sin un factor en común. Si denotamos con una barra a la reducción módulo p, observemos que como p no divide a los tres enteros a, b, c, entonces $\overline{P} = (\overline{a}, \overline{b}, \overline{c}) \in \mathbb{P}^2(\mathbb{F}_p)$ es un punto en el plano proyectivo con coordenadas en el campo finito $\mathbb{F}_p$. Más aún, si $P \in E(\mathbb{Q})$ entonces $\overline{P} \in E(\mathbb{F}_p)$. Observemos ahora que, dada una curva elíptica

$$E:\ y^2 = x^3 - ax - b$$

siempre se puede escoger un modelo de ella definida sobre $\mathbb{Z}$ (mínimo en un cierto sentido) y reduciendo sus coeficientes módulo el primo p podemos considerar la curva reducida $\widetilde{E}:\ y^2 = x^3 - \overline{a}x - \overline{b}$ definida ahora sobre el campo finito $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Pueden suceder dos cosas:

- $\widetilde{E}$ sigue siendo lisa y por lo tanto es una curva elíptica. En este caso decimos que E tiene *buena reducción* en p.
- $\widetilde{E}$ no es lisa. En este caso decimos que E tiene *mala reducción* en p.

Note que si $y^2 = x^3 - ax - b$ es el polinomio con coeficientes enteros que define a la curva E y si Δ es el discriminante del polinomio en x anterior, el hecho de que E sea lisa es equivalente a que $\Delta \neq 0$. Más aún, el discriminate $\overline{\Delta}$ del polinomio $y^2 = x^3 - \overline{a}x - \overline{b}$ que define a $\widetilde{E}$, es la reducción módulo p de Δ. Observamos ahora que, si p no divide al discriminante Δ de E, entonces la función $r_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$ es un homomorfismo. El lema siguiente identifica su núcleo:

Lema. *Sean p un primo, E una curva elíptica sobre $\mathbb{Q}$ tal que p no divide al discriminante de E y $r_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)$ el homomorfismo anterior. Si $P, Q \in E(\mathbb{Q})$, entonces $\overline{P} = \overline{Q}$ si y sólo si el producto vectorial $P \times Q$ (vistos como vectores en $\mathbb{R}^3$) tiene coordenadas divisibles por p.*

Demostración: Si $P = (x_1, y_1, z_1)$ y $Q = (x_2, y_2, z_2)$, $P \times Q = (y_1z_2 - y_2z_1, x_2z_1 - x_1z_2, x_1y_2 - x_2y_1)$ y si suponemos que p divide a las coordenadas de $P \times Q$, consideremos dos casos:

(1). El primo p divide a x_1. En este caso, p divide a x_2z_1 y a x_2y_1 y por lo tanto divide a x_2 porque no puede dividir a x_1, y_1 y z_1 ya que estamos suponiendo que las coordenadas proyectivas de P no tienen un divisor común. Sin perder generalidad podemos suponer que $p \nmid y_1$. Entonces, como $\overline{x}_1 = 0 = \overline{x}_2$,

$$\begin{aligned}\overline{Q} &= (0, \overline{y}_2, \overline{z}_2)\overline{y}_1 = (0, \overline{y}_2\overline{y}_1, \overline{z}_2\overline{y}_1) = (0, \overline{y}_1\overline{y}_2, \overline{y}_2\overline{z}_1) = (0, \overline{y}_1, \overline{z}_1)\overline{y}_2 \\ &= (0, \overline{y}_1, \overline{z}_1) = \overline{P}\end{aligned}$$

la primera igualdad porque $\overline{y}_1 \neq 0$, la tercer igualdad porque la primera coordenada de $P \times Q$ es cero mód p, la cuarta igualdad porque $\overline{y}_2 \neq 0$, ya que de lo contrario, de la primera coordenada de $P \times Q$ se tendría que $p | y_1z_2$ y así $p|z_2$, por lo que p dividiría a x_2, y_2, z_2, lo cual no es posible.

(2). Si el primo p no divide a x_1. En este caso,

$$\begin{aligned}\overline{Q} &= (\overline{x}_2, \overline{y}_2, \overline{z}_2)\overline{x}_1 = (\overline{x}_1\overline{x}_2, \overline{x}_1\overline{y}_2, \overline{x}_1\overline{z}_2) = (\overline{x}_1\overline{x}_2, \overline{x}_2\overline{y}_1, \overline{x}_2\overline{z}_1) \\ &= (\overline{x}_1, \overline{y}_1, \overline{z}_1)\overline{x}_2 = \overline{P}\,.\end{aligned}$$

Recíprocamente, si $\overline{P} = \overline{Q}$, sin perder generalidad supongamos que $p \nmid x_1$ por lo que $p \nmid x_2$ también (un argumento similar aplica si $p \nmid y_1$ ó $p \nmid z_1$). Entonces, de $(\overline{x}_1, \overline{y}_1, \overline{z}_1) = (\overline{x}_2, \overline{y}_2, \overline{z}_2)$ se sigue que

$$(\overline{x}_1\overline{x}_2, \overline{x}_1\overline{y}_2, \overline{x}_1\overline{z}_2) = \overline{Q} = \overline{P} = (\overline{x}_2\overline{x}_1, \overline{x}_2\overline{y}_1, \overline{x}_2\overline{z}_1)$$

y como las primeras coordenadas son iguales, se sigue que las otras dos también lo son, i.e., $\overline{x_1y_2} = \overline{x_2y_1}$ y $\overline{x_1z_2} = \overline{x_2z_1}$, por lo que p divide a $x_1y_2 - x_2y_1$ y a $x_1z_2 - x_2z_1$, es decir, p divide a las dos últimas coordenadas de $P \times Q$. Para ver que p divide a la primer coordenada $y_1z_2 - y_2z_1$, si sucediera que ambos y_1 y z_1 son divisibles por p, ya acabamos. Si $p \nmid y_1$ ó $p \nmid z_1$, repetimos el argumento de arriba con x_1, x_2 reemplazados por y_1, y_2 ó z_1, z_2. □

Corolario. *Sea E una curva elíptica definida sobre $\mathbb{Z}$ y supongamos que p es un primo suficientemente grande de tal manera que no divide a las coordenadas de todos los productos vectoriales de los puntos en $E(\mathbb{Q})_{\text{tor}}$ ni al discriminante de E. Entonces, la restricción del morfismo de reducción, $r_p : E(\mathbb{Q})_{\text{tor}} \to E(\mathbb{F}_p)$, es inyectiva.* □

Lema. *Para la curva elíptica $E_A : \ y^2 = x^3 - A^2x$, si p es un primo tal que p no divide al discriminante de E_A, $p \geq 7$ y $p \equiv 3 \pmod 4$, entonces $E_A(\mathbb{F}_p)$ tiene exactamente $p + 1$ puntos.*

Demostración: Para comenzar, $E_A(\mathbb{F}_p)$ contiene a los cuatro puntos $(0,0)$, $(-A,0)$, $(A,0)$ y $\mathbf{0}$. Observemos ahora que si $x \neq 0, A, -A$, considerando el par $\{x,-x\}$ notamos que, como $f(x) = x^3 - A^2x$ es una función impar y como $p \equiv 3 \pmod 4$ por lo que -1 no es un cuadrado módulo p, entonces exactamente uno de los elementos $f(x)$ ó $f(-x) = -f(x)$ es un cuadrado en $\mathbb{F}_p$ y por lo tanto se tienen dos raíces cuadradas que dan lugar a dos puntos $(x, \pm\sqrt{f(x)})$ ó $(x, \pm\sqrt{f(-x)})$, lo cual nos da un total de $p-3$ puntos extra en $E_A(\mathbb{F}_p)$ que junto con los cuatro obvios nos dan los $p+1$ puntos deseados. □

Teorema 6. *$E_A(\mathbb{Q})_{\text{tor}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. De hecho,*

$$E_A(\mathbb{Q})_{\text{tor}} = \{(0,0), (-A,0), (A,0), \mathbf{0}\}.$$

Demostración: Basta mostrar que el orden de $E_A(\mathbb{Q})_{\text{tor}}$ divide a 4. Por el corolario anterior, si p es suficientemente grande, el orden de $E_A(\mathbb{Q})_{\text{tor}}$ divide al orden de $E(\mathbb{F}_p)$ y por el lema anterior este último orden es $p+1$ si $p \equiv 3 \pmod 4$. Usaremos ahora el teorema de Dirichlet, sobre la existencia de un número infinito de primos en cualquier progresión de la forma $an+b$ con a, b coprimos, para mostrar que los divisores del orden de $E_A(\mathbb{Q})_{\text{tor}}$ están restringidos.

Comenzamos viendo que 8 no divide a $|E_A(\mathbb{Q})_{\text{tor}}|$. En efecto, por el teorema de Dirichlet existen primos suficientemente grandes tales que $p \equiv 3 \pmod 8$. Si sucediera que 8 divide a $|E_A(\mathbb{Q})_{\text{tor}}|$, entonces 8 dividiría a $p+1$. Pero como $p \equiv 3 \pmod 8$, entonces $p+1 \equiv 4 \pmod 8$ y así $8 \nmid p+1$, una contradicción.

En forma similar se muestra que 3 no divide a $|E_A(\mathbb{Q})_{\text{tor}}|$, considerando primos $p \equiv 7 \pmod{12}$ y usando que esta congruencia implica que $p \equiv 3 \pmod 4$.

Análogamente, si $q > 3$ es cualquier primo, se muestra que q no divide a $|E_A(\mathbb{Q})_{\text{tor}}|$ usando ahora primos $p \equiv 3 \pmod{4q}$, lo cual implica que $p \equiv 3 \pmod 4$.

Por lo tanto, los únicos divisores de $|E_A(\mathbb{Q})_{\text{tor}}|$ son 1,2, 4 y como $E_A(\mathbb{Q})_{\text{tor}}$ contiene a los cuatro puntos obvios, entonces su orden es 4. □

Recordemos ahora que si $A > 0$ es un entero libre de cuadrados, los teoremas 3 y 4 dicen que: *A es un número congruente si y sólo si la curva elíptica $y^2 = x^3 - A^2x$ tiene un punto racional (x,y) diferente de los cuatro obvios.* Así, por el teorema previo $(x,y) \notin E_A(\mathbb{Q})_{\text{tor}}$ y por lo tanto los puntos que queremos deben ser de orden infinito:

Teorema 7. *Sea $A > 0$ entero libre de cuadrados. Entonces, A es un número congruente si y sólo si la curva elíptica $y^2 = x^3 - A^2x$ tiene rango $r \geq 1$, o lo que es lo mismo, si y sólo si $E_A(\mathbb{Q})$ es infinito.*

Demostración: Sólo falta probar la suficiencia y para ésto, si $E_A(\mathbb{Q})$ tiene rango cero, entonces es un grupo de torsión y por el teorema 6 debe ser $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ y por lo tanto cualquier punto racional en esta curva debe ser de los triviales y por el teorema 3 se sigue que A no es congruente. □

El problema es entonces ¿cómo determinar si $E_A(\mathbb{Q})$ es infinito? Hasta este momento, la exposición ha sido elemental, excepto a lo más por el teorema de Mordell, y en lo que resta del artículo sólo bosquejaremos las ideas involucradas para culminar con una formulación de una versión de las conjeturas de Birch y Swinnerton-Dyer, no sólo de relevancia para el problema de los números congruentes que hemos estado estudiando, sino de una profundidad y consecuencias mayores. Todo lo anterior ha sido una excusa para motivar una parte de estas conjeturas importantes.

La función L de Hasse-Weil de una curva elíptica. En nuestro contexto el problema fundamental es: si $E/\mathbb{Q}$ es una curva elíptica, determinar si el grupo $E(\mathbb{Q})$ es infinito. Para ésto, dada la curva elíptica

$$E:\ y^2 = x^3 - ax - b$$

escogiendo un modelo de ella definida sobre $\mathbb{Z}$ (mínimo en un cierto sentido) y reduciendo sus coeficientes módulo un primo p podemos considerar la curva reducida $\widetilde{E}:\ y^2 = x^3 - \overline{a}x - \overline{b}$ definida ahora sobre el campo finito $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, la cual puede o no ser lisa. En cualquier caso, como $\mathbb{F}_p$ es finito podemos contar el número de puntos con coordenadas en $\mathbb{F}_p$ que tiene la curva $\widetilde{E}$. Esto lo hacemos también con todas las extensiones finitas $\mathbb{F}_{p^n}$ de $\mathbb{F}_p$ y lo denotamos con $\#\widetilde{E}(\mathbb{F}_{p^n})$. La idea es considerar la función generadora asociada a la sucesión de enteros $\#\widetilde{E}(\mathbb{F}_{p^n})$:

$$Z(E,u) := \exp\left(\sum_{n=1}^{\infty} \frac{\#\widetilde{E}(\mathbb{F}_{p^n})}{n} \cdot u^n\right)$$

Se prueba que esta función zeta es de la forma siguiente:

$$Z(E,u) = \begin{cases} \dfrac{1-a_p u + pu^2}{(1-u)(1-pu)} & \text{si } E \text{ tiene buena reducción en } p \\ \\ \dfrac{1-a_p u}{(1-u)(1-pu)} & \text{si } E \text{ tiene mala reducción en } p \end{cases}$$

donde $a_p = p+1-\#\widetilde{E}(\mathbb{F}_p)$. Notamos entonces que en esta función zeta sólo el entero a_p depende de la curva E por lo que sólo los numeradores nos dan información sobre la curva. Tomando estos numeradores, variando los primos p y substituyendo $u = p^{-s}$, para $s \in \mathbb{C}$ se define la función L de Hasse-Weil de E como:

$$L(E,s) := \prod_{p \text{ malos}} \frac{1}{1-a_p p^{-s}} \prod_{p \text{ buenos}} \frac{1}{1-a_p p^{-s}+p^{1-2s}}$$

y con respecto a la convergencia de este producto infinito se tiene:

Teorema 8 (Hasse). (1)*: Para todo primo p se tiene que $|a_p| < 2\sqrt{p}$.* (2): *$L(E,s)$ converge para $Re(s) > 3/2$.* □

Conjetura [Hasse]. *La función $L(E,s)$ tiene una continuación analítica a todo $\mathbb{C}$ y satisface una ecuación funcional de la forma*

$$L(E,s) \sim L(E,2-s)$$

donde $\sim$ denota igualdad salvo factores gamma elementales.

Para el caso de curvas elípticas con multiplicación compleja (por ejemplo, si $A > 0$ es un entero positivo libre de cuadrados, entonces la curva elíptica $E_A : \ y^2 = x^3 - A^2 x$ tiene multiplicación compleja por el anillo de enteros gaussianos), Deuring y Hecke probaron la conjetura de Hasse. El año 1999, continuando el trabajo de Wiles-Taylor en su demostración de la conjetura de Fermat, se anunció la demostración de la conjetura de Shimura-Taniyama-Weil [2] y como consecuencia de ésto se tiene que la conjetura de Hasse es verdadera: para toda curva elíptica $E/\mathbb{Q}$, la función $L(E,s)$ se extiende a una función entera.

Tiene entonces sentido hablar de si $s = 1$ es o no cero de $L(E,s)$ y se tiene la pregunta: ¿Qué pasa con el valor de $L(E,s)$ en $s = 1$? (equidistante de s y $2-s$): A principios de los años 1960's (¡cuando aún no se sabía que $L(E,s)$ estaba definida en $s = 1$!), Birch y Swinnerton-Dyer formularon unas conjeturas asombrosas:

Conjeturas [Birch-Swinnerton-Dyer]:

(1) $E(\mathbb{Q})$ *es infinito* $\Leftrightarrow L(E,1)=0$.

(2) *Más precisamente:* $\mathrm{ord}_{s=1}L(E,s)=r$, *donde* $r=\mathrm{rango}(E(\mathbb{Q}))$.

Resultados. Los avances más importantes hacia la demostración de estas conjeturas son:

Teorema 9 (Coates-Wiles, 1977). *Sea $E/\mathbb{Q}$ una curva elíptica con multiplicación compleja. Si $E(\mathbb{Q})$ es infinito, entonces $L(E,1)=0$.*

Teorema 10 (Gross-Zagier-Rubin, 1983). *Sea $E/\mathbb{Q}$ una curva elíptica con multiplicación compleja.*

- *Si $L(E,1)\neq 0$, entonces $E(\mathbb{Q})$ es finito.*
- *Si $L(E,1)=0$ y $L'(E,1)\neq 0$, entonces* $\mathrm{rango}(E(\mathbb{Q}))=1$.

Estos resultados se aplican a la curva $y^2=x^3-A^2x$ ya que ésta tiene multiplicación compleja.

Ya para terminar, regresando al problema diofantino original, para la curva elíptica asociada se tiene el siguiente teorema:

Teorema 11 (Tunnel, 1983). *Si $A>0$ es un entero libre de cuadrados y $E_A: y^2=x^3-A^2x$ es la curva elíptica correspondiente, entonces:*

$$L(E_A,1)=\frac{a(n-2m)^2}{\sqrt{d}}C_0$$

donde $C_0=0{,}163878597\ldots$ es una constante y

$$a=\begin{cases}1 & \text{si } A \text{ es impar}\\ 2 & \text{si } A \text{ es par}\end{cases}$$

$$n=\#\{(x,y,z)\in\mathbb{Z}^3\ :\ x^2+2ay^2+8z^2=A/a\}$$

y

$$m=\#\{(x,y,z)\in\mathbb{Z}^3\ :\ x^2+2ay^2+32z^2=A/a\}.$$

Se sigue que:

- *Si $n\neq 2m$ entonces no existe un triángulo rectángulo con lados racionales y área A.*
- *¿Qué pasa si $n=2m$? Para comenzar, $s=1$ sería un cero de $L(E_A,s)$. Pero como todavía no sabemos que la conjetura de BSD sea cierta, entonces no podemos concluir que el rango de $E_A(\mathbb{Q})$ es ≥ 1 para deducir de ésto la existencia de un triángulo rectángulo con lados racionales y área A.*

Referencias

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

[2] Breuil, C., Conrad, B., Diamond, F. and Taylor, R., *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*. J. Amer. Math. Soc. **14** (2001), 843–939.

[3] Coates, J. and Wiles, A., *On the conjecture of Birch and Swinnerton-Dyer*. Inv. Math. **39** (1977), 223–351.

[4] Gross, B. H. and Zagier, D., *Heegner points and derivatives of L-series*. Inv. Math. **84** (1986), 225–320.

[5] Knapp, A. Elliptic Curves, Princeton University Press, Princeton, 1992.

[6] Koblitz, N. Introduction to elliptic curves and modular forms. Springer Verlag, Berlin, 1993.

[7] Rubin, K., *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Inv. Math. **89** (1987), 527–560.

[8] Tunnel, J., *A classical Diophantine problem and modular forms of weight* 3/2. Inv. Math. **72** (1983), 323–334.

[9] Weil, A., Number Theory: An approach through history from Hammurapi to Legendre. Birkhäuser Verlag, Basel, 1984.