Triangles rectangles de costats racionals*

PILAR BAYER **

A qui, un dia, va voler saber si de la Teoria de Nombres era més bonica la teoria o eren més bonics els nombres.

En un manuscrit anònim grec, datat entre Euclides i Diofant, hom posa de manifest que l'àrea del triangle rectangle de costats 9, 40, 41 val $5 \cdot 36$ i, per tant, que l'àrea del triangle

$$\left(\frac{9}{6}, \frac{40}{6}, \frac{41}{6}\right) = \left(1 + \frac{1}{2}, 6 + \frac{2}{3}, 6 + \frac{5}{6}\right)$$

és igual a 5.

Si (a, b, c) és un triangle rectangle de costats racionals i designem per n la seva àrea, tindrem que

$$a^2 + b^2 = c^2 \quad , \quad ab = 2n.$$

Per tant, $(a \pm b)^2 = c^2 \pm 4n$; i veiem que

$$\left(\frac{c}{2}\right)^2 - n, \quad \left(\frac{c}{2}\right)^2, \quad \left(\frac{c}{2}\right)^2 + n$$

són tres nombres de $\mathbf{Q}^{*2}$ en progressió aritmètica.

El problema de caracteritzar els nombres naturals que, com el 5, poden ésser àrea de triangles racionals, o bé el problema equivalent de trobar ternes de quadrats en progressió aritmètica, fascinà als àrabs. El trobem plantejat en un manuscrit del segle X, on Mohammed Ben Alhocain el qualifica de «objectiu principal de la teoria dels triangles rectangles racionals».

Clàssicament hom ha anomenat *congruents* els nombres naturals que són àrea de triangles rectangles racionals. Sigui $\boldsymbol{C}$ el conjunt corresponent. És fàcil veure

* Conferència inaugural del curs de la Societat Catalana de Ciències, Secció de Matemàtiques, impartida el 13 de novembre del 1986.

** Departament d'Àlgebra i Geometria de la Universitat de Barcelona.

que un nombre natural n pertany a $\boldsymbol{C}$ si i solament si pertany a $\boldsymbol{C}$ la seva part lliure de quadrats. És a dir, si escrivim $n = n_0 t^2$, amb $n_0, t \in \mathrm{N}$, n_0 no divisible per cap quadrat, tenim que $n \in \boldsymbol{C}$ sii $n_0 \in \boldsymbol{C}$. Per tant, en l'estudi de $\boldsymbol{C}$ podem restringir-nos a la classe dels enters lliures de quadrats.

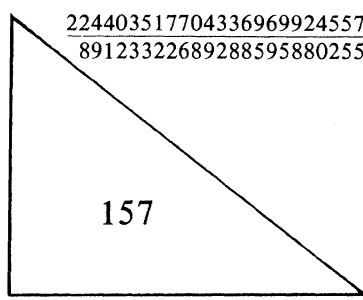
El àrabs donaren en el segle X la següent llista de 30 nombres congruents lliures de quadrats:

5	34	210	429	2730
6	65	221	546	3570
14	70	231	1155	4290
15	110	286	1254	5610
21	154	330	1785	7854
30	190	390	1995	10374.

Si observem, detingudament, la llista anterior a fi d'inferir condicions perquè un nombre sigui congruent, el més probable és que no en sapiguem dir res. La raó, bàsicament, és deguda al fet següent: la llista dels àrabs és altament incompleta; el que un nombre no hi figuri no vol dir, ni molt menys, que no sigui congruent; vol dir simplement que o bé no és congruent, o bé que per als àrabs fou massa difícil trobar un triangle que el tingués per àrea. Un triangle rectangle pot tenir uns costats racionals petits, però requerint molts dígits per ésser expressats. Un exemple que parla per si sol el proporciona el primer triangle rectangle que té per àrea 157 (l'exemple és degut a Zagier):

$$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

$$\frac{6803298487826435051217540}{4113405192277161493832 03}$$



$$\frac{4113405192277161493832 03}{21666555693714761309610}$$

El primer en demostrar que $1 \notin \boldsymbol{C}$ o, equivalentment, que no existeixen triangles rectangles i quadrats de costats racionals amb la mateixa àrea, fou Fermat. La demostració de Fermat (val a dir, l'única que hom li coneix) és per descens. Fermat prova per a tal fi que l'equació $X^2 = Z^4 - Y^4$ no té solucions enteres no trivials; la qual cosa implica, a la vegada, que l'equació de Fermat $X^4 + Y^4 = Z^4$ no té solució, llevat de les trivials.

L'ús dels ordinadors, bàsicament, permeteren millorar una mica les taules de nombres congruents. L'estat d'aquest problema, l'any 1983, era el següent: hom disposava d'una taula de nombres $n \in \boldsymbol{C}, n \leq 1.000$, tret potser de 8 casos en què el caràcter congruent o no del nombre en qüestió no havia pogut ésser decidit. El fet que aquesta taula fos molt més completa que la dels àrabs permeté formular conjectures: Tots els enters n lliures de quadrats, $n \equiv 5, 6, 7 \pmod 8$ sortien congruents; els primers $p \equiv 1, 3 \pmod 8$ no ho eren mai, etc.

El problema dels nombres congruents canvià totalment d'aspecte gràcies al treball de J. B. Tunnell *A Classical Diophantine Problem and Modular Forms of Weight 3/2*, Invent. Math. *72* (1983), 323-334. L'avenç produït en aquest sentit es pot resumir en dos punts:

1) Avui disposem d'una taula (completa!) de nombres congruents $n \leq 2.000$.
2) Tenim un criteri que, donat un nombre n permet, mitjançant un càlcul algebraic que involucra $O(n^{3/2})$-passos, decidir conjecturalment si n és congruent o no.

Per explicar el criteri de Tunnell car reformular el problema que ens hem proposat. Clarament un nombre n és congruent si i solament si la corba donada per la intersecció de les quadràtiques:

$$a^2 + b^2 = c^2$$
$$ab = 2nt^2$$

té un punt racional no trivial. Com és ben sabut, les solucions de la primera equació (que són les ternes pitagòriques) poden parametritzar-se en la forma

$$(a, b, c) = (\lambda^2 - 1,\ 2\lambda,\ \lambda^2 + 1)$$

on $\lambda \in \mathbf{Q}^*$. Si portem aquests valors a la segona de les quadràtiques, obtenim que $(\lambda^2 - 1)\lambda = nt^2$; és a dir

$$nt^2 = \lambda^3 - \lambda$$

i veiem, per tant, que la corba el·líptica

$$\mathsf{E}_n : nY^2 = X^3 - X$$

té un punt racional $(x, y) = (\lambda, t)$, en el qual $t \neq 0$. Designem per $\mathsf{E}_n(\mathbf{Q})$ el conjunt dels punts racionals de E_n:

$$\mathsf{E}_n(\mathbf{Q}) = \{(x, y) \in \mathbf{Q}^2 \mid ny^2 = x^3 - x\} \cup \{P_\infty\}.$$

És ben conegut que el conjunt $\mathsf{E}_n(\mathbf{Q})$ té estructura de grup abelià quan sumem els

seus punts segons la regla usual en les cúbiques (tres punts sumen zero si i solament si estan en línea recta). Segons un cèlebre teorema degut a Mordell, $\mathsf{E}_n(\mathbf{Q})$ és un grup abelià de tipus finit; per tant descompon en suma directa

$$\mathsf{E}_n(\mathbf{Q}) \simeq \mathsf{E}_n(\mathbf{Q})_{\text{tor}} \oplus \mathbf{Z}^r,$$

d'un grup abelià de torsió i d'un grup abelià lliure de rang $r \geq 0$. És fàcil veure que, en el nostre cas,

$$\mathsf{E}_n(\mathbf{Q})_{\text{tor}} = \{P_\infty, (-1, 0), (0, 0), (1, 0)\},$$

amb la qual cosa, tots els punts de $\mathsf{E}_n(\mathbf{Q})$ que tenen la segona component no nul·la són d'ordre infinit. Recíprocament, si tenim un punt $(x, y) \in \mathsf{E}_n(\mathbf{Q}) \otimes \mathbf{Q}$, diferent de P_∞, podem fer-li correspondre el triangle d'àrea ny^2 donat per $(x^2 - 1, 2x, x^2 + 1)$. En conseqüència obtenim el

1r. criteri per reconèixer si un nombre és congruent: Donat un nombre natural n, tenim que

$$n \in \boldsymbol{C} \leftrightarrow \operatorname{rg} \mathsf{E}_n(\mathbf{Q}) > 0,$$

on $\operatorname{rg} \mathsf{E}_n(\mathbf{Q})$ designa el rang del grup de Mordell-Weil de la corba el·líptica.

La correspondència esmentada entre els triangles d'àrea n i els punts d'ordre infinit de $\mathsf{E}_n(\mathbf{Q})$ és molt rica: d'una banda, posa de manifest que si un nombre és congruent, tenim infinits triangles rectangles racionals que el tenen per àrea i permet obtenir una llei recurrent per obtenir-los (basta anar sumant amb si mateix el punt de la cúbica). D'altra banda, el rang del grup de Mordell-Weil dóna compta de quants triangles tinc d'àrea n «independents». Però el que la fa més interessant és que el rang del grup de Mordell-Weil de les corbes el·líptiques és molt més controlable que la possible existència de triangles d'àrea donada, com veurem tot seguit. L'instrument idoni per portar a terme aquest control és la funció L de Hasse-Weil de E_n.

D'entrada pensem, donat un primer $p \nmid 2n$, la corba el·líptica E_n com una equació definida sobre el cos finit $\mathbf{F}_p$ $(= \mathbf{Z}/p\mathbf{Z})$ i posem:

$$a_{\mathsf{E}_n} = 1 + p - \#\, \mathsf{E}_n\,(\mathbf{F}_p).$$

Aquests nombres es calculen tots. Vénen donats per:

$$a_{\mathsf{E}_n, p} = \left(\frac{n}{p}\right) a_p,$$

on $a_p = 0$ si $p \equiv 3 \pmod 4$, $a_p = 2(-1)^v u$ si $p \equiv 1 \pmod 4$, $p = u^2 + 4v^2$ i $u \equiv 1 \pmod 4$. El producte infinit

$$\mathsf{L}(\mathsf{E}_n, s) = \prod_{\substack{p \text{ primer} \\ p \nmid 2n}} \frac{1}{1 - a_{\mathsf{E}_n, p}\, p^{-s} + p^{1-2s}}$$

convergeix per a $Re(s) > 3/2$ i defineix una funció holomorfa en aquesta regió del pla. Definim

$$N_n = \begin{cases} 32n^2 & \text{si } 2 \nmid n \\ 16n^2 & \text{si } 2 \mid n. \end{cases}$$

(N_n és l'anomenat *conductor* de la corba el·líptica E_n). Expressant $\mathsf{L}(\mathsf{E}_n, s)$ com una transformada integral d'una «funció theta» convenientment definida, hom prova que la funció precedent admet una continuació analítica a tot el pla complex i satisfà l'equació funcional

$$\left(\frac{N_n}{2\pi}\right)^s \Gamma(s)\, \mathsf{L}(\mathsf{E}_n, s) = w_n \left(\frac{N_n}{2\pi}\right)^{2-s} \Gamma(2-s)\, \mathsf{L}(\mathsf{E}_n, 2-s),$$

on

$$w_n = \begin{cases} +1 & \text{si } n \equiv 1, 2, 3 \pmod 8 \\ -1 & \text{si } n \equiv 5, 6, 7 \pmod 8. \end{cases}$$

Veiem que el centre de simetria de l'equació funcional es troba en el punt $s = 1$ i que aquesta posa de manifest que, quan $n \equiv 5, 6, 7 \pmod 8$, aleshores $\mathsf{L}(\mathsf{E}_n, 1) = 0$. D'altra banda, recordem que hom sospitava que aquests valors eren tots nombres congruents i que, per tant, el rang del grup de Mordell-Weil de E_n seria positiu.

La corba el·líptica E_n és una corba el·líptica «molt bona» en el sentit que admet una multiplicació complexa:

$$\begin{aligned} i\colon \mathsf{E}_n(\mathbf{C}) &\longrightarrow \mathsf{E}_n(\mathbf{C}) \\ (x, y) &\longmapsto (-x, iy). \end{aligned}$$

En general, per a tota corba el·líptica E dotada de multiplicació complexa, hom sospita que el rang del seu grup de Mordell-Weil $\mathsf{E}(\mathbf{Q})$ ha d'ésser controlable via el comportament de la seva funció L en el punt $s = 1$. (La filosofia és la següent: una acumulació de punts mòdul p per a tots els p, ha de traduir l'existència de punts globals d'ordre infinit.) Més concretament, hom creu que és certa la:

Conjectura de Birch i Swinneron-Dyer. Si E és una corba el·líptica definida sobre $\mathbf{Q}$ i dotada de multiplicació complexa, aleshores

$$\text{ordre}_{s=1}\, \mathsf{L}(\mathsf{E}, s) = \text{rg}\, \mathsf{E}(\mathbf{Q}).$$

Pel que fa al nostre problema ens interessen especialment els següents resultats parcials vers la seva demostració:

Teorema. Sigui $E/\mathbf{Q}$ una corba el·líptica dotada de multiplicació complexa. Aleshores:

I) $\operatorname{ord}_{s=1} L(E, s) = 0 \quad \Rightarrow \quad \operatorname{rg} E(\mathbf{Q}) = 0.$

II) $\operatorname{ord}_{s=1} L(E, s) = 1 \quad \Rightarrow \quad \operatorname{rg} E(\mathbf{Q}) \geq 1.$

La part I) del teorema és deguda a Coates-Wiles (1977); la part II), a Gross-Zagier (1983). Així podem passar a formular el

2n. criteri per al reconeixement de nombres congruents: Donat un nombre natural n, tenim que

I) $L(E_n, 1) \neq 0 \quad \Rightarrow \quad n \notin \boldsymbol{C}.$

II) $L(E_n, 1) = 0, L'(E_n, 1) \neq 0 \quad \Rightarrow \quad n \in \boldsymbol{C}.$

III) La validesa de la conjectura *BSD* implica que

$$L(E_n, 1) = 0 \quad \Leftrightarrow \quad n \in \boldsymbol{C}.$$

En aquest punt, direm que per als $n \leq 2.000$, $n \equiv 5, 6, 7 \pmod 8$, la funció $L(E_n, s)$ presenta un zero simple en el punt $s = 1$, llevat del cas $n = 1254$ en què el zero és d'ordre 3. El 1254 figurava ja en la relació dels àrabs i és, per tant, un nombre congruent. Notem que en aquest cas la conjectura de Birch i Swinnarton-Dyer prediu la presència d'una família triplement infinita de triangles que tenen per àrea 1254. En efecte, hom constata que els punts

$$\left(\frac{-198}{1254}, \frac{17424}{1254^2}\right), \left(\frac{-171}{1254}, \frac{16245}{1254^2}\right), \left(\frac{-98}{1254}, \frac{12376}{1254^2}\right)$$

són tots de $E_{1254}(\mathbf{Q})$ i linealment independents sobre Z.

Passem ara a descriure el procediment seguit per a l'avaluació de la funció $L(E_n, s)$ en el punt $s = 1$.

Desenvolupant el producte infinit que defineix $L(E_n, s)$ quan $Re(s) > 3/2$ obtenim una sèrie de Dirichlet:

$$L(E_n, s) = \prod_{p \nmid 2n} (1 - a_{E_n, p} p^{-s} + p^{1-2s})^{-1} = \sum_{m=1}^{\infty} b_{n,m} m^{-s}.$$

No és difícil veure que per a $n \equiv 1, 2, 3 \pmod 8$ és

$$L(E_n, 1) = 2 \sum_{m=1}^{\infty} \frac{b_{n,m}}{m} e^{-2\pi m/\sqrt{N_n}}.$$

En aquesta sèrie es satisfà $|b_{n,m}| \leq \sigma_0(m)m^{1/2}$, essent $\sigma_0(m)$ igual al nombre de divisors de m. La convergència d'aquesta sèrie és ràpida i pot servir, quan n no és massa gran, per detectar el seu caràcter no congruent. Per exemple, si $n = 1$ i avaluem el primer sumand veiem que

$$L(E_1, 1) = 0.6586... + R_5$$

amb $|R_5| < 0.023$ i, per tant, $L(E_1, 1) \neq 0$ (la qual cosa és coherent amb el fet que $1 \notin \boldsymbol{C}$). Però quan n és gran, el treballar amb la sèrie anterior és, d'una banda, lent i, d'altra banda, no permet provar que $L(E_1, 1) = 0$, per a un n concret, car no tenim la certesa de que un zero obtingut amb l'ordinador sigui un zero veritable.

El principal mèrit del treball de Tunnell abans esmentat és el d'aconseguir donar el valor $L(E_n, 1)$ de manera compacta. Concretament tenim el següent:

Teorema (Tunnell, 1983). Sigui n un enter lliure de quadrats. Sigui

$$\beta = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} = 2.622 \ldots$$

el «període real» de la corba el·líptica E_1. Posem

$$2c_n = \begin{cases} \sum_{n=2x^2+y^2+8z^2} (-1)^z & \text{si } 2 \nmid n \\ \sum_{n/2=4x^2+y^2+8z^2} (-1)^z & \text{si } 2 \mid n. \end{cases}$$

Aleshores

$$L(E_n, 1) = \begin{cases} \frac{\beta}{\sqrt{n}} \left(\frac{c_n}{2}\right)^2 & \text{si } 2 \nmid n \\ \frac{\beta}{\sqrt{n}} \frac{c_n^2}{2} & \text{si } 2 \mid n. \end{cases}$$

En particular, $L(E_n, 1) = 0$ si i solament si $c_n = 0$.

Notem ara que, fent ús del Teorema de Tunnell, el decidir si $L(E_n, 1)$ val o no zero pot ésser sempre portat a terme amb $O(n^{3/2})$ passos.

L'haver obtingut per primera vegada una expressió compacta per al valor $L(E_n, 1)$ cal mirar-ho com un altre èxit més de la teoria de les formes modulars. Són aquestes, funcions de variable complexa definides en el semiplà superior $\mathbf{H}$ i gaudint de certes propietats de periodicitat; la propietat més remarcable que tenen és la

de posseir un desenvolupament en sèrie de Fourier en el qual els seus coeficients entren de manera decisiva en l'estudi de múltiples qüestions aritmètiques. Si considerem la sèrie de Dirichlet $L(E_1, s)$ donada per

$$L(E_1, s) = \sum_{m=1}^{\infty} \frac{b_{1,m}}{m^s} = 1 - 2 \cdot 5^{-s} - 3 \cdot 9^{-s} + 6 \cdot 13^{-s} + 2 \cdot 17^{-s} + \sum_{m \geq 25} \frac{b_{1,m}}{m^s},$$

quan $\mathrm{Re}(s) \geq 3/2$, i definim la funció

$$f_{E_1}(z) = \sum_{m=1}^{\infty} b_{1,m} q^m = 1 - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} + \sum_{m \geq 25} b_{1,m} q^m,$$

on $q = e^{2\pi i z}$, $\mathrm{Im}(z) \geq 0$, obtenim que f_{E_1} és una forma modular parabòlica «de pes 2» i «de nivell 32».

L'estudi de les formes modulars de pes enter és un tema clàssic (que s'inicia pràcticament amb Jacobi) i prossegueix amb Poincaré, Klein, Fricke, Ramanujan, Hecke, Siegel, etc. L'estudi de les formes modulars de pes semienter, pel contrari, no fou emprès fins els anys 70 de manera sistemàtica. L'any 1973 aparegué l'important article de Shimura *On modular forms of half-integral weight.* Part fonamental d'aquest article és la que tracta l'anomenada aplicació de Shimura (*Shimura's lifting*). L'aplicació de Shimura associava a certes formes parabòliques de pes fraccionari $k/2$ una forma parabòlica de pes enter $k - 1$. L'aplicació de Shimura fou estesa, generalitzada i reformulada per diversos autors: Niwa (1975), Shintani (1975), Waldspurger (1980, 1981).

Especialment destacables per als nostres propòsits són els dos treballs de Waldspurger, publicats en el J. Math. Pures et Appl. En el primer, de 133 pàgines, Waldspurger interpreta la correspondència de Shimura en termes de representacions sobre un cos local del grup metaplectic $\tilde{S}$, que és un revestiment de dos fulles de SL_2. En el segon, de 109 pàgines, dóna una aplicació del primer: Donada una forma modular f de pes parell $k - 1$, de nivell M i «nova» en el sentit d'Atkin-Lehner, Waldspurger descriu un sistema de generadors de l'espai $S_{k/2}(N, \chi, f)$ de formes parabòliques de pes fraccionari, nivell N i caràcter χ que, per l'aplicació de Shimura, tenen per imatge f. Per a cada $n \geq 1$ els coeficients de Fourier de les funcions φ_i són de la forma:

$$a_n(\varphi_i) = A(f, n) \prod_p d_p(\varphi_i, n).$$

Les funcions $d_p(\varphi_i, n)$ vénen donades per una fórmula i són iguals a 1, quasi per a tot primer p. El valor $A(f, n)$ és el terme interessant. Waldspurger no el determina explícitament, però veu que $A(f, n) = A(f, n_0)$ essent n_0 la part de n lliure de quadrats, i que $A(f, n_0)^2$ coincideix amb el valor en el centre de simetria de la sèrie L associada a la forma modular $f \otimes \chi_{n_0}$; és a dir, a la forma modular que s'obté torçant f amb el caràcter quadràtic associat a l'extensió $\mathbb{Q}(\sqrt{n_0})$.

Coneixent el resultat de Waldspurger, Tunnell començà la recerca de formes parabòliques de pes 3/2 que, per l'aplicació de Shimura, tinguessin per imatge f_{E_1}. En nivel 64 (el primer que la teoria prediu) no en trobà cap; en nivell 128 la situació fou més favorable car

$$S_{3/2}(128,\ 1, f_{E_1}) \neq \varnothing \qquad \text{i} \qquad S_{3/2}(128,\ \chi_2, f_{E_1}) \neq \varnothing.$$

Posem

$$\theta_t = \sum_{m=-\infty}^{m=\infty} q^{tm^2}.$$

La funció θ_t és una forma modular de pes 1/2, nivell 128 i caràcter χ_t. Per resultats de Serre i de Stark sabem que

$$\langle \theta_2, \theta_8, \theta_{32} \rangle = S_{1/2}(128, \chi_2),$$
$$\langle \theta_1, \theta_4, \theta_{16} \rangle = S_{1/2}(128,\ 1).$$

Així per conèixer els espais $S_{3/2}(128, \chi_2)$, $S_{3/2}(128,\ 1)$ Tunnell necessità construir una forma modular de pes 1, nivell 128 i caràcter χ_{-2}. El teorema de Deligne-Serre sobre formes modulars de pes 1, dels anys 70, posa de manifest que aquestes formes són tals que la seva sèrie L associada és la sèrie L d'Artin d'una representació irreduïble de dimensió 2, de conductor 128 i de determinant χ_{-2}. Sabent això, arribà a la conclusió que

$$g = \sum (-1)^{m+n} q^{(4m+1)^2+8n^2} \qquad , \qquad (m,\ n) \in \mathbf{Z} \times \mathbf{Z},$$

era la funció escaient. Aleshores

$$\langle g\theta_2, g\theta_8, g\theta_{32} \rangle = S_{3/2}(128,\ 1),$$
$$\langle g\theta_1, g\theta_4, g\theta_{16} \rangle = S_{3/2}(128, \chi_8).$$

i, a més,

$$\langle g\theta_2, g\theta_8 \rangle = S_{3/2}(128,\ 1, f_{E_1}),$$
$$\langle g\theta_4, g\theta_{16} \rangle = S_{3/2}(128,\ \chi_2, f_{E_1}).$$

El pas següent consistí en comparar els generadors de Waldspurger amb els de Tunnell, en aquest cas concret. Posem

$$g\theta_2 = \sum_{n=1}^{\infty} a_n q^n.$$

Si $n \equiv 5$ ò $7 \pmod 8$, tenim que $a_n = 0$ i això dóna $A(f_{E_1}, n) = 0$, és a dir $L(E_n,\ 1) = 0$, la qual cosa ens era coneguda. Si $n \equiv 1$ ò $3 \pmod 8$, el càlcul de les constants d_p de Waldspurger proporciona l'existència de constants λ_1, λ_3 tals que

$$a_n = \lambda_1 A(f_{E_1}, n)n^{1/4} \quad , \quad \text{si } n \equiv 1 \pmod 8,$$
$$a_n = \lambda_3 A(f_{E_1}, n)n^{1/4} \quad , \quad \text{si } n \equiv 3 \pmod 8.$$

Birch i Swinnerton-Dyer sabien que

$$L(E_1, 1) = \frac{\beta}{4}$$

i que

$$L(E_3, 1) = \frac{\beta}{\sqrt{3}}$$
$$L(E_n, 1) = \frac{\beta}{\sqrt{n}} \kappa_n,$$

essent κ_n un nombre racional. Com que $a_1 = 1$ i $a_3 = 2$, podem calcular els valors de λ_1 i de λ_3, obtenint que

$$L(E_n, 1) = A(f_{E_1}, n)^2 = \frac{\beta}{\sqrt{n}} \left(\frac{a_n}{2}\right)^2,$$

si $n \equiv 1$ ò $3 \pmod 8$. De manera semblant, per tractar el cas $n \equiv 2 \pmod 8$ hom escriu

$$g\theta_4 = \sum a'_n q^n.$$

El coneixement dels valors $L(E_2, 1)$, $L(E_{10}, 1)$ permet provar que

$$L(E_{2n}, 1) = \frac{\beta}{\sqrt{2n}} \frac{a'^2_n}{2}.$$

Ara cal explicitar el càlcul de a_n, a'_n. No és difícil veure que

$$g = (\theta_1 - \theta_4)(\theta_{32} - \frac{1}{2}\theta_8)$$

i que, a partir d'ací:

$$a_n = \text{coef. } n\text{-èssim de } (\theta_2\theta_1\theta_{32} - \frac{1}{2}\theta_2\theta_1\theta_8)$$
$$= \text{coef. } n\text{-èssim de} \left(\sum_{x,y,z \in \mathbf{Z}} q^{2x^2+t^2+32z^2} - \frac{1}{2} \sum_{x,y,z \in \mathbf{Z}} q^{2x^2+y^2+8z^2} \right)$$
$$= \#\{x, y, z \in Z \mid n = 2x^2 + y^2 + 32z^2\} - \frac{1}{2}\#\{x, y, z \in Z \mid n = 2x^2 + y^2 + 8z^2\}$$
$$= \frac{1}{2} \sum_{n=2x^2+y^2+8z^2} (-1)^y,$$

si n és senar. També:

$$\begin{aligned} a'_n &= \text{coef. } n\text{-èssim de } (\theta_4\theta_1\theta_{32} - \frac{1}{2}\theta_4\theta_1\theta_8) \\ &= \text{coef. } n\text{-èssim de } \left(\sum_{x,y,z\in\mathbf{Z}} q^{4x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbf{Z}} q^{4x^2+y^2+8z^2}\right) \\ &= \#\{x, y, z \in \mathbf{Z} \mid n = 4x^2 + y^2 + 32z^2\} - \frac{1}{2}\#\{x, y, z \in \mathbf{Z} \mid n = 4x^2 + y^2 + 8z^2\} \\ &= \frac{1}{2}\sum_{n=4x^2+y^2+8z^2} (-1)^y, \end{aligned}$$

si n és, tanmateix, senar. Per obtenir el criteri de Tunnell basta doncs definir

$$c_n = \begin{cases} a_n & \text{si } 2 \nmid n \\ a'_{n/2} & \text{si } 2 \mid n. \end{cases}$$

REFERÈNCIES

COATES, J., WILES, A.: On the conjecture of Birch and Swinneron-Dyer. *Invent. math.* **39** (1977), 223-251.

DICKSON, L. E.: *History of the Theory of Numbers.* Chelsea, 1952.

GROSS, B. H., ZAGIER, D.: Heegner points and derivatives of L-series. *Invent. math.* **84** (1986), 225-320.

KOBLITZ, N.: *Introduction to Elliptic Curves and Modular Forms.* Springer, 1984.

KRAMARZ, G.: All Congruent Numbers Less than 2000. *Math. Ann.* **273** (1986), 337-340.

TUNNELL, J. B.: A classical Diophantine Problem and Modular Forms of Weight 3/2. *Invent. math.* **72** (1983), 323-334.