Butlletí de la Societat Catalana de Matemàtiques
Vol. 39, núm. 1-2, 2024. Pàg. 73–102. DOI: 10.2436/20.2002.01.115

Punts racionals en corbes el·líptiques

Xavier Guitart i Marc Masdeu

Resum: Les corbes el·líptiques són un dels objectes més estudiats en teoria de nombres actualment. Es descriuen per equacions cúbiques i allò que les distingeix de la resta de corbes—i les fa tan fascinants—és l'estructura algebraica tan rica que presenta el conjunt de les seves solucions. Aquest article té com a objectiu explicar què són les corbes el·líptiques i explorar algunes de les seves propietats més importants, que sovint es troben entre els resultats més rellevants de les matemàtiques dels segles XX i XXI, així com algunes de les conjectures encara obertes i que guien gran part de la recerca actual. Per situar-les en un context històric i conceptual més ampli, les presentem com un cas particular d'equacions diofàntiques, un tema fonamental i transversal dins la teoria de nombres.

Paraules clau: equacions diofàntiques, corbes el·líptiques, punts de Heegner, integració p-àdica, punts de Stark-Heegner.

Classificació MSC2020: 14H52, 11G05.

1 Equacions diofàntiques

Un dels temes centrals en teoria de nombres és l'estudi de les *equacions diofàntiques*, en què hom està interessat en les solucions enteres o racionals d'equacions polinòmiques amb coeficients enters. De manera més precisa, una equació diofàntica és una equació de la forma

$$F(x_1, \dots, x_n) = 0, \tag{1.1}$$

on F és un polinomi amb coeficients enters, i volem determinar les solucions en què totes les components viuen a $\mathbb{Z}$ o, alternativament, a $\mathbb{Q}$. Per exemple, $(-1, 0)$ és una solució entera de l'equació diofàntica

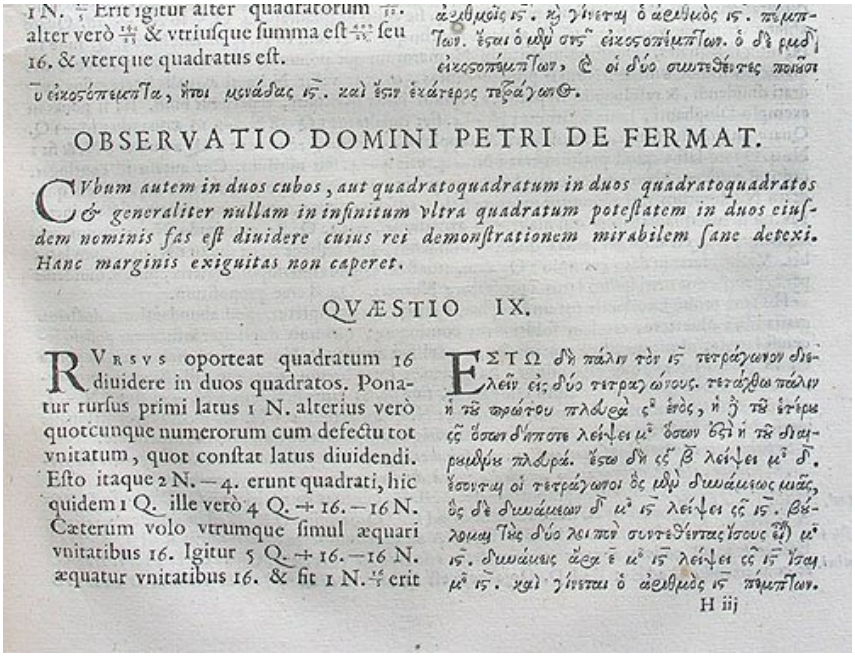
$$x^2 + y^2 - 1 = 0, \tag{1.2}$$

i $(-3/5, 4/5)$ n'és una solució racional. De fet, i això ho veurem més endavant, aquesta equació diofàntica té infinites solucions racionals.

El terme *diofàntic* fa referència al matemàtic Diofant d'Alexandria, que visqué durant el segle III i feu, entre altres, un tractat d'aritmètica en què estudià problemes que es resolen amb aquestes equacions. Veiem, doncs, que l'interès per les equacions diofàntiques ve de molt lluny. Al llarg dels segles, matemàtics il·lustres, com ara Fermat, Euler o Gauss, n'han tractat casos concrets i, de fet, sovint han estat la motivació d'algunes nocions algebraiques que han acabat formant part del cos teòric de la matemàtica actual. Un dels casos més famosos és el de l'equació de Fermat

$$F_n : x^n + y^n - z^n = 0, \tag{1.3}$$

on n és un natural fixat. Fermat deixà anotat en un marge d'un dels seus llibres d'estudi, justament un volum de l'*Aritmètica* de Diofant (vegeu figura 1), que, si $n \geq 3$, aleshores l'equació (1.3) no té solucions enteres no trivials; és a dir, no té solucions (x, y, z) amb $x, y, z \in \mathbb{Z}$ tots tres no nuls. Aquest enunciat, d'aparença innocent, romangué sense demostrar durant més de 300 anys, i moltes de les nocions i tècniques matemàtiques actuals provenen dels intents d'aquells que van succeir Fermat en la tasca de provar l'enunciat.[1]



1 N. $\frac{1}{1}$ Erit igitur alter quadratorum $\frac{16}{1}$. alter verò $\frac{15}{1}$ & vtriusque summa est $\frac{31}{1}$ seu 16. & vterque quadratus est.

ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄. πέμπτων. ἔστι δὲ ὑφ' ἑαυτὸν εἰκοσοπέμπτων. ὁ δὲ ἑαυτὸν εἰκοσοπέμπτων, ᾧ οἱ δύο συντεθέντες ποιοῦσι ῡ εἰκοσόπεμπτα, ἤτοι μονάδας ις̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rurſus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot conſtat latus diuidendi. Eſto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque ſimul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

ΕΣΤΩ δὴ πάλιν τὸν ις̄ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τοῦ πρώτου πλευρὰ ς̲ ἑνός, ἡ δὲ τοῦ ἑτέρου ς̲ ὅσων δήποτε λείψει μ̲ ὅσων ὅσοι ἡ τοῦ διαιρεθέντος πλευρά. ἔστω δὴ ς̲ β̲ λείψει μ̲ δ̲. ἔσονται οἱ τετράγωνοι ὃς μὲν δωδάκις μδ̲, ὃς δὲ δωδάκις δ̲ μ̲ ις̄ λείψει ς̲ ις̄. βέλομαι τοὺς δύο λοιπὸν συντεθέντας ἴσους εἶναι μ̲ ις̄. δωδάκις ἄρα ε̲ μ̲ ις̄ λείψει ς̲ ις̄ ἴσας μ̲ ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄ πέμπτων.

H iij

FIGURA 1: Edició posterior de l'*Aritmètica* de Diofant, amb l'observació de Fermat. (Font: `https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem`.)

1 Fermat afirmà que n'havia trobat una demostració, però que el marge on escrivia era massa petit per a encabir-la-hi. Aquesta suposada prova no es va trobar mai, i aquest és, en part, el motiu pel qual tants matemàtics provaren de demostrar l'anomenat *darrer teorema de Fermat.*

Per exemple, la teoria general d'ideals en anells sorgí de l'estratègia ideada per Kummer per a atacar el problema; o, més recentment, els treballs de Wiles [37] i Taylor i Wiles [35] sobre la conjectura de modularitat, de la qual parlarem més endavant, foren el pas definitiu que resolgué el problema l'any 1994.

No es pot dir que hi hagi hagut sempre al llarg de la història un interès per una teoria general de les equacions diofàntiques, sinó que més aviat es tractaven de manera fragmentada, cas per cas. Un dels primers a plantejar la necessitat de sistematitzar-ne l'estudi fou Hilbert, que a la seva llista de 23 problemes que presentà al congrés internacional de matemàtiques de París l'any 1900, inclogué com a problema número 10 el següent:

> Donada una equació diofàntica amb qualsevol nombre de quantitats desconegudes i amb coeficients numèrics enters: Idear un procés segons el qual es pugui determinar, en un nombre finit d'operacions, si l'equació és resoluble en nombres enters.

Aquest procés en un nombre finit de passos de què parlava Hilbert és el que avui en dia coneixem com a *algoritme*. El problema, tal i com el va plantejar Hilbert amb solucions enteres, resulta que no té solució. El 1970 Matiyasevich ([25]) donà una família d'equacions diofàntiques per a les quals no pot existir cap algoritme que pugui decidir si tenen solucions enteres o no. Això no obstant, el problema anàleg per a solucions racionals segueix obert. De fet, a partir d'ara ens centrarem en solucions racionals, de manera que, quan parlem d'equacions diofàntiques, ens hi referirem en el sentit de solucions racionals.

Malgrat ser més generals que les enteres, les solucions racionals solen presentar més estructura, la qual cosa n'acostuma a facilitar l'estudi. Un primer exemple d'això és el fet que una equació com (1.1) dona lloc a una varietat algebraica, i podem emprar les eines provinents de la geometria algebraica. Una conseqüència terminològica d'aquest punt de vista és que pensem les solucions $(x_1, \ldots, x_n)$ com a punts de l'espai afí (o de l'espai projectiu, si el polinomi que defineix l'equació és homogeni). Així doncs, sovint ens referirem a una solució de (1.1) com a un punt, entenent que ens referim a un punt de la varietat definida per l'equació. Per exemple, l'equació (1.2) defineix una circumferència al pla afí, i les solucions racionals es corresponen als punts de la circumferència amb les dues components racionals.

Seguint amb l'esperit del problema de Hilbert, algunes de les preguntes més generals que podem plantejar per a equacions diofàntiques són:

1. Existeix algun algoritme que, donada una equació diofàntica, decideixi si aquesta té alguna solució racional?
2. Si l'equació té solucions, hi ha algun algoritme per a calcular-les totes? O, en qualsevol cas, per a calcular-ne alguna?
3. Podem dir alguna cosa sobre el nombre de solucions? Per exemple, decidir si és finit o infinit i donar-ne una fita en el cas finit?

Aquests problemes segueixen oberts, no només per al cas general, sinó, fins i tot, per al cas particular, molt restringit però, tot i això, molt interessant, de corbes planes, que serà en el que ens centrarem a partir d'ara.

Una *corba plana*[2] ve donada per un polinomi en dues variables $f(x,y)=0$ en el cas afí, o per un polinomi homogeni en tres variables $F(X,Y,Z)=0$ en el cas projectiu.[3] De fet, l'exemple (1.2) és una corba plana afí i (1.3) és una corba plana projectiva.

L'invariant més important d'una corba és el seu *gènere*, que podem pensar en primera instància com una noció topològica. Considerem una corba C donada per una equació de la forma

$$C : f(x,y) = 0.$$

Com a equació diofàntica, estem interessats en les solucions racionals o, dit d'una altra manera, en el conjunt de punts racionals de C, que denotarem amb $C(\mathbb{Q})$. Més concretament,

$$C(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}\times\mathbb{Q} : f(x,y) = 0\}.$$

Però també té sentit considerar el conjunt de punts de C amb components complexes; és a dir,

$$C(\mathbb{C}) = \{(x,y) \in \mathbb{C}\times\mathbb{C} : f(x,y) = 0\}.$$

Clarament $C(\mathbb{Q}) \subseteq C(\mathbb{C})$ i $C(\mathbb{C})$ admet una estructura topològica que governa determinats aspectes aritmètics de $C(\mathbb{Q})$. Per començar, vist com a subespai de $\mathbb{C}\times\mathbb{C}$, resulta que $C(\mathbb{C})$ és una superfície. Una manera de pensar-ho és escrivint les variables complexes x i y com $x = a+bi$ i $y = c+di$ amb $a,b,c,d \in \mathbb{R}$, i observant que l'equació $f(x,y)=0$ dona lloc a dues equacions de nombres reals (una per a la part real i una per a la part imaginària) en les quatre variables reals a, b, c, d; dues equacions en quatre variables reals defineixen una superfície. La compactificació d'aquesta superfície és una superfície orientable compacta que és, doncs, homeomorfa a un tor amb g forats per a algun $g \geq 0$; aquest g és el *gènere* de la corba. Per exemple, si la corba $C(\mathbb{C})$ és homeomorfa a l'esfera, aleshores $g=0$; i si és homeomorfa al tor estàndard, $g=1$.

En el cas de corbes planes, el gènere està relacionat amb un altre invariant important, que és el grau: si la corba és no singular[4] de grau d, el gènere de la

2 Ens restringirem al cas de corbes planes per simplicitat, però tot el que direm en aquesta secció també és cert per a corbes algebraiques més generals, no necessàriament planes (és a dir, que no estiguin contingudes necessàriament al pla afí o al pla projectiu, sinó en espais de dimensió superior).

3 En el cas projectiu, com que el polinomi $F(X,Y,Z)$ és homogeni, si $(X_0,Y_0,Z_0) \neq (0,0,0)$ és solució, aleshores també ho és $(\lambda X_0, \lambda Y_0, \lambda Z_0)$ per a tot $\lambda \in \mathbb{Q}$ no nul; totes aquestes solucions s'identifiquen amb un únic punt de l'espai projectiu.

4 Una corba és no singular si tot punt té una única recta tangent. La fórmula per al gènere que donem només val per a corbes planes que segueixen essent no singulars quan les pensem al pla projectiu.

corba és $(d-1)(d-2)/2$. Per exemple, la corba de Fermat F_n té gènere $(n-1)(n-2)/2$; en particular, F_2 té gènere 0 i F_3 té gènere 1.

Doncs bé, aquest invariant topològic permet distingir tres comportaments aritmètics molt diferenciats en les corbes, i és que dona informació molt important sobre el conjunt de punts racionals.

En primer lloc, les corbes de gènere 0 són còniques planes; és a dir, venen donades per $f(x,y)=0$, on f és un polinomi de grau 2. Per a aquestes corbes, existeix un algoritme que permet decidir si hi ha algun punt racional. En cas que n'hi hagi algun, aleshores n'hi ha infinits i es poden trobar tots a partir d'un d'ells. Per exemple, en el cas de l'equació (1.2), que té gènere 0, podem partir del punt racional $(-1,0)$. Aleshores, la recta que passa per aquest punt i té pendent t ve descrita per l'equació

$$y = t(x+1). \tag{1.4}$$

Aquesta recta talla la corba en un altre punt P_t (vegi's la figura 2). Substituint (1.4) a (1.2), obtenim que

$$P_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

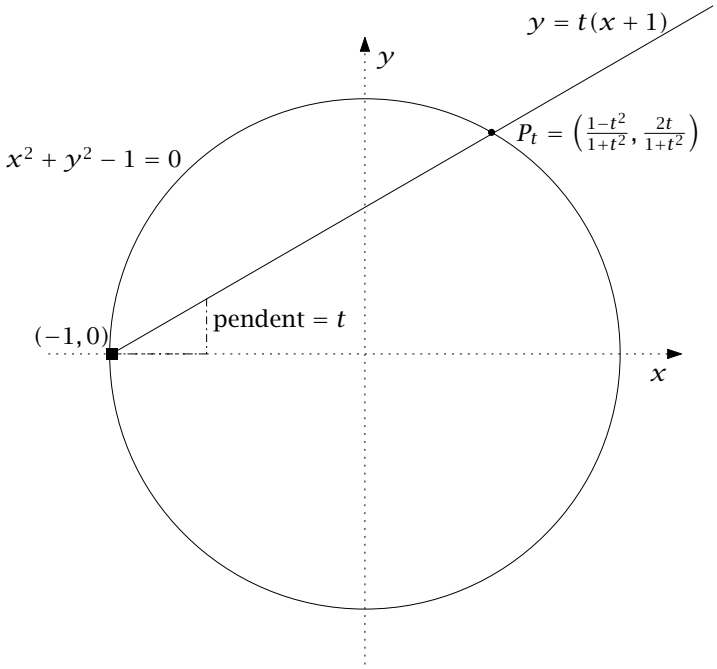


FIGURA 2: A partir del punt racional $(-1,0)$ del cercle, podem trobar tots els altres amb rectes de pendent racional.

D'aquí es pot veure que P_t té coordenades racionals si i només si t és racional, i que si P' és un punt racional de la corba, aleshores es correspon a un punt de la forma P_t per algun valor $t \in \mathbb{Q}$. Hem vist, doncs, que la corba té infinits punts racionals i que els podem calcular explícitament si en coneixem un. El mateix procediment funciona per a qualsevol corba de gènere 0.

El cas següent serien les corbes de gènere 1, però aquest el deixarem per al final i ara parlarem de què succeeix amb les corbes de gènere més gran o igual que 2. Mordell va conjecturar l'any 1922 que, si una corba té gènere $g \geq 2$, aleshores té un nombre finit de punts racionals. Aquesta conjectura va ser demostrada per Faltings el 1983 [12], en un resultat que li va valer una medalla Fields l'any 1986. També hi ha resultats que donen una fita pel nombre de punts. Un dels més recents, de Dimitrov-Gao-Habegger [11], ens diu que

$$\#C(\mathbb{Q}) \leq c_g^{1+r(C)},$$

on c_g és una constant que només depèn de g i $r(C)$ és un invariant de C (el rang del grup de punts racionals de la seva jacobiana). Tot i que aquests resultats ens donen molta informació sobre el conjunt de punts d'una corba de gènere ≥ 2, avui dia encara no es coneix cap algoritme per a determinar si una corba de gènere ≥ 2 té algun punt racional o no, ni per a calcular-los tots en cas que en tingui.

Ens queda, doncs, veure quina és la situació en el cas de corbes de gènere 1. Hem vist que una corba de gènere 0 o bé no té punts o bé en té infinits, i que una corba de gènere ≥ 2 té un nombre finit de punts. Les corbes de gènere 1 exhibeixen un comportament encara diferent. En primer lloc, de manera semblant al cas de gènere ≥ 2, no es coneix cap algoritme per a determinar si una corba de gènere 1 té punts racionals o no. Però, a diferència dels casos de gènere 0 o gènere ≥ 2, si en té, tant en pot tenir un nombre finit com un nombre infinit. De fet, una corba de gènere 1 amb algun punt racional és, justament, el que es coneix amb el nom de *corba el·líptica*, i el conjunt dels seus punts racionals admet una estructura molt especial que li confereix un seguit de propietats molt notables. Aquestes són les corbes o, si es vol, les equacions diofàntiques, a què dedicarem la resta de l'article.

2 Corbes el·líptiques

Una *corba el·líptica sobre* $\mathbb{Q}$ és una corba projectiva no singular de gènere 1 amb un punt racional distingit. Aquesta definició pot semblar una mica abstracta, però es pot veure que tota corba el·líptica es pot descriure, de fet, per una equació afí de la forma[5]

$$E : y^2 = x^3 + ax + b, \text{ amb } a, b \in \mathbb{Q} \text{ i } 4a^3 + 27b^2 \neq 0. \tag{2.1}$$

5 Tot i que el nom pugui dur a confusió, les corbes el·líptiques no són el·lipses, com es veu d'aquesta descripció: l'equació d'una el·lipse és de grau 2, mentre que la d'una corba el·líptica és de grau 3. Des del punt de vista històric sí que hi ha, però, una certa relació, a través de les funcions el·líptiques, que apareixen en el càlcul de la longitud de l'arc de les el·lipses i que es troben a l'origen del terme *corba el·líptica*.

La corba projectiva associada ve donada per l'equació

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

La condició $4a^3 + 27b^2 \neq 0$ és equivalent al fet que la corba sigui no singular, i la quantitat $\Delta_E = -16(4a^3 + 27b^2)$ s'anomena *discriminant* de la corba. De l'equació projectiva veiem que el punt $O = [0 : 1 : 0]$ és un punt racional de E; s'anomena *punt de l'infinit*, ja que és l'únic punt de la corba a la recta de l'infinit en el pla projectiu (és a dir, és l'únic punt de la corba projectiva que no veiem al model afí (2.1)).

L'equació (2.1) s'anomena *equació de Weierstrass* de la corba el·líptica. Sovint és convenient treballar amb equacions una mica més generals, de la forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.2}$$

que s'anomenen *equacions generalitzades de Weierstrass*. Si treballem sobre $\mathbb{Q}$, com és el nostre cas, tota equació de la forma (2.2) es pot transformar mitjançant un canvi de variables en una de la forma (2.1). Però en cossos de característica 2 o 3 no sempre és possible, per això cal admetre també equacions generalitzades.

Seguint amb el plantejament de la secció 1, estem interessats en E com a equació diofàntica; és a dir, ens interessen els punts racionals de E:

$$E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\} \cup \{O\}.$$

Com que hem definit els punts racionals fent servir l'equació afí, ens cal afegir-hi el punt O, que no veiem al model afí. Alternativament, podríem haver definit els punts racionals directament com els punts de l'espai projectiu que satisfan l'equació projectiva de la corba.

Ja ens hem trobat amb un exemple de corba el·líptica. Recordem que a la secció 1 hem vist que la cúbica de Fermat

$$F_3 : X^3 + Y^3 = Z^3$$

té gènere 1. Com que té punts racionals (per exemple, el punt $[1 : -1 : 0]$), és una corba el·líptica. De fet, el canvi de variables

$$x = \frac{12Z}{X + Y}, \quad y = \frac{36(X - Y)}{X + Y}$$

transforma l'equació F_3 en

$$E_3 : y^2 = x^3 - 432,$$

que és de la forma (2.1). Fixem-nos que el canvi de variables involucra funcions racionals amb coeficients a $\mathbb{Q}$; per tant, transforma punts racionals de E_3 en punts racionals de F_3 i estableix, de fet, una bijecció entre els punts racionals de les dues corbes.

La propietat més important de les corbes el·líptiques és que, a partir de dos punts racionals, podem fabricar-ne un altre amb un procediment geomètric. Ho explicarem amb un exemple. Suposem que tenim la corba el·líptica

$$E : y^2 = x^3 - 16x + 16. \tag{2.3}$$

Per ajudar-nos a visualitzar el procés, és útil dibuixar els punts reals de la corba, de manera semblant a com hem fet amb l'exemple del cercle anteriorment. Podem veure el resultat a la figura 3. Remarquem que d'aquests punts amb coordenades reals, les solucions racionals de l'equació diofàntica $y^2 = x^3 - 16x - 16$ es corresponen amb els punts de la gràfica amb les dues components racionals. Per exemple, els dos punts

$$P = (0, 4), \quad Q = (4, 4)$$

són punts racionals de la corba, és a dir, $P, Q \in E(\mathbb{Q})$, ja que tenen components racionals i satisfan l'equació.

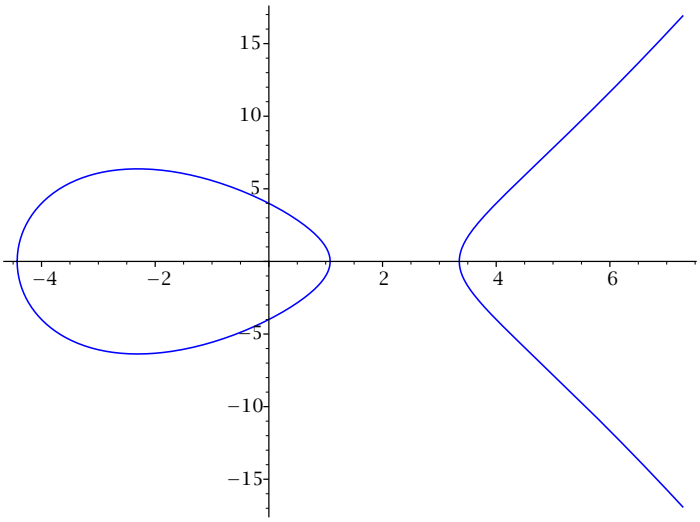


FIGURA 3: Els punts reals de la corba $y^2 = x^3 - 16x - 16$.

Resulta que la recta que passa per P i Q talla la corba E en un tercer punt. Escrivint l'equació de la recta $\overline{PQ}$ i substituint-la a l'equació de E, podem calcular que aquest tercer punt (vegeu la figura 4) és el $(-4, 4)$, que també té coordenades racionals i que anomenarem $P \star Q$.

Aquest procediment funciona per a tota corba el·líptica E i per a tot parell de punts racionals P i Q: la recta $\overline{PQ}$ ve donada per una equació de grau 1, i E per una de grau 3, de manera que la recta i la corba es tallen en tres punts. A més, un càlcul explícit permet veure que, si P i Q tenen coordenades racionals, el nou punt $P \star Q$ també.

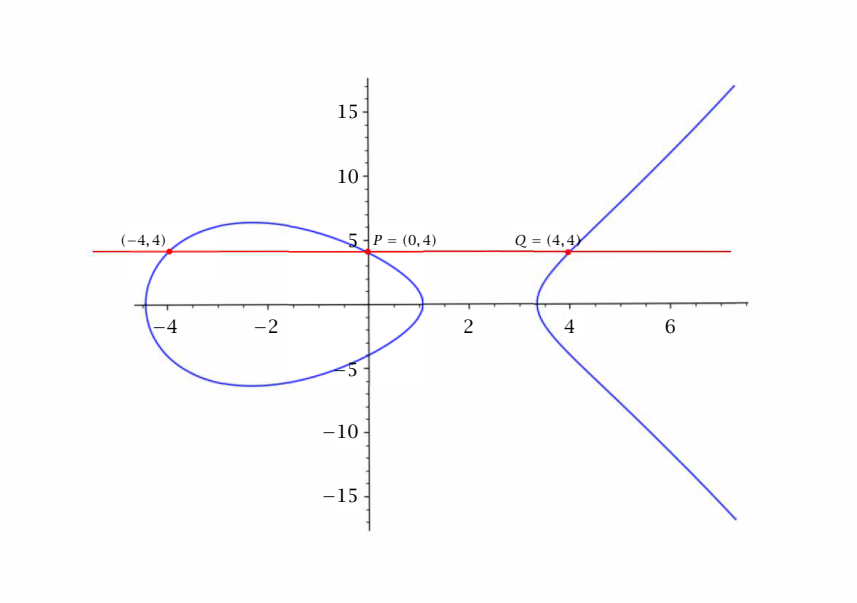


FIGURA 4: A partir dels punts racionals $P = (0, 4)$ i $Q = (4, 4)$ podem trobar el punt $(-4, 4)$, prenent la intersecció de la corba E amb la recta que passa per P i Q.

Per tant, donats dos elements de $E(\mathbb{Q})$, podem fabricar un altre element de $E(\mathbb{Q})$ amb aquest procediment geomètric, i això dona lloc a una llei de composició; és a dir, a una aplicació

$$\begin{aligned} E(\mathbb{Q}) \times E(\mathbb{Q}) &\longrightarrow E(\mathbb{Q}) \\ (P, Q) &\longmapsto P \star Q. \end{aligned}$$

Bé, hi ha un parell de detalls pendents que no hem tractat. El primer és què passa si prenem $P = Q$, ja que en aquest cas no té sentit parlar de la recta que uneix P i Q. Però, com que la corba és no singular, podem prendre la corba tangent a E que passa per P (si la corba fos singular en P, hi hauria més d'una recta tangent i això no tindria sentit). Podem repetir l'argument anterior amb aquesta recta tangent: la seva intersecció amb E ens dona un punt $P \star P$, que també és un punt racional.

El segon detall pendent és què passa si un dels punts que sumem és el punt O, que no veiem al model afí. La resposta és que aquest punt el podem pensar com «la direcció vertical»; per exemple, si volem calcular $P \star O$, prendrem com a recta $\overline{PO}$ la recta vertical que passa per P.

A aquest procediment per a construir nous punts a partir de punts coneguts se'l coneix com a *mètode de la secant i la tangent*, però la llei de composició que hem descrit cal modificar-la una mica per tal que tingui millors propietats

algebraiques. En comptes de $P \star Q$, prenem un altre punt definit de la manera següent: fem la recta vertical que passa per $P \star Q$ i considerem el punt d'intersecció d'aquesta recta amb E (vegeu la figura 5). Es pot veure que aquest punt, que anomenarem $P + Q$, també té coordenades racionals. Obtenim, doncs, una nova llei de composició

$$\begin{aligned} +\colon E(\mathbb{Q}) \times E(\mathbb{Q}) &\longrightarrow E(\mathbb{Q}) \\ (P, Q) &\longmapsto P + Q. \end{aligned}$$

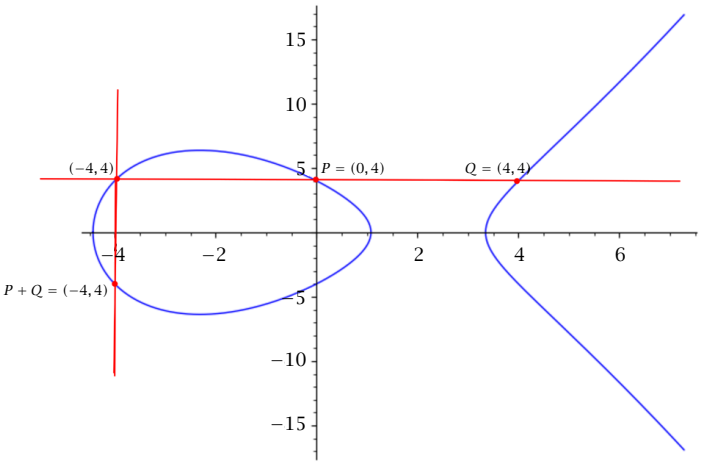


FIGURA 5: A partir del punt $P \star Q = (-4, 4)$, trobem un nou punt racional fent la recta vertical que passa per $P \star Q$ i tallant amb E. Aquest nou punt, en aquest cas el $(-4, -4)$, és el que anomenem $P + Q$.

Poincaré va demostrar que aquesta operació $+$ satisfà un seguit de propietats molt rellevants:

1. Per a tot $P \in E(\mathbb{Q})$ se satisfà que $P + O = O$. És a dir, O és un element neutre per a l'operació.
2. Tot element té un invers: per a tot $P \in E(\mathbb{Q})$, existeix un únic punt Q tal que $P + Q = O$. Aquest punt l'anomenarem $-P$.
3. L'operació és associativa: $(P + Q) + R = P + (Q + R)$.
4. L'operació és commutativa: $P + Q = Q + P$.

Veiem, doncs, que $E(\mathbb{Q})$ amb l'operació $+$ satisfà els axiomes de grup abelià.[6] Aquest és el primer resultat clau de la teoria de corbes el·líptiques [30].

TEOREMA 2.1 (POINCARÉ, 1901). *L'operació $P, Q \mapsto P + Q$ dona una estructura de grup abelià al conjunt $E(\mathbb{Q})$.*

6 En canvi, l'operació $P, Q \mapsto P \star Q$ no compleix els axiomes d'una llei de grup, ja que no és associativa.

Poincaré també va conjecturar al mateix article[7] que sempre podem trobar un conjunt finit de punts racionals a partir dels quals es pot construir qualsevol altre punt racional aplicant repetidament el mètode de la secant i la tangent. Dit amb terminologia moderna de teoria de grups, Poincaré conjecturà que $E(\mathbb{Q})$ és un grup finitament generat. Això fou demostrat per Mordell [28] un quart de segle després.

TEOREMA 2.2 (MORDELL, 1922). *$E(\mathbb{Q})$ és un grup finitament generat.*

Aquest resultat ja ens proporciona molta informació sobre l'estructura de $E(\mathbb{Q})$. El teorema de classificació de grups abelians finitament generats ens diu que es té un isomorfisme de la forma

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T,$$

on T és un grup finit i $r \in \mathbb{Z}_{\geq 0}$. El grup T es correspon amb els punts racionals de E d'ordre finit, o punts de torsió; és a dir, punts $P \in E(\mathbb{Q})$ tals que per a algun $n \in \mathbb{Z}_{>0}$ es té que[8] $nP = O$. L'enter r denota el nombre màxim de punts d'ordre infinit linealment independents, i es coneix com a *rang* de E.

EXEMPLE 2.3. Per la corba E_3 corresponent a la cúbica de Fermat, resulta que

$$E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}.$$

És a dir, $T = \mathbb{Z}/3\mathbb{Z}$ (hi ha tres punts racionals) i el rang és 0 (no hi ha cap punt d'ordre infinit). De fet,

$$E_3(\mathbb{Q}) = \{(12, 36), (12, -36)\} \cup \{O\}.$$

El punt $(12, 36)$ té ordre 3, i es compleix que $2(12, 36) = (12, -36)$ i $3(12, 36) = O$.

EXEMPLE 2.4. La corba E de (2.3) satisfà que

$$E(\mathbb{Q}) \simeq \mathbb{Z}.$$

És a dir, l'únic punt de torsió és O, i hi ha un punt d'ordre infinit a partir del qual es poden obtenir totes els altres punts racionals. El punt $P = (0, 4)$ és un generador; alguns dels seus múltiples són:

$$2P = (4, 4), \quad 3P = (-4, -4), \quad 4P = (8, -20), \quad 5P = (1, -1), \quad 6P = (24, 116).$$

Podria semblar que sempre obtindrem punts amb coordenades enteres. Però això no és cert; ja al següent múltiple de P veiem que $7P = (-20/9, 172/27)$ i a partir d'aquí tots els altres múltiples tenen coordenades racionals no enteres.

7 Per a una visió més completa de les contribucions de Poincaré a l'aritmètica, podeu consultar [1].

8 Com és habitual en els grups abelians, nP denota $P + P + \overset{n)}{\cdots} + P$.

EXEMPLE 2.5. Podem considerar ara la corba

$$E : y^2 = x^3 - 15\,058\,251x + 21\,601\,366\,470,$$

que satisfà que $E(\mathbb{Q}) \simeq \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Els generadors són

$$(51, 27), \quad (45, 153), \quad (-124, 62), \quad (9, 594).$$

Els dos primers punts tenen ordre infinit, el tercer té ordre 2 i el darrer té ordre 4.

Veiem, doncs, una propietat que havíem avançat a la secció 1: una corba el·líptica tant pot tenir un nombre finit de punts racionals com un nombre infinit. Però, gràcies a l'estructura algebraica del conjunt de punts, ara podem precisar molt més aquesta qüestió: podem preguntar-nos quina és l'estructura de grup de $E(\mathbb{Q})$. De manera natural, el problema es pot desglossar en dos, corresponents a la part de torsió i a la part lliure:

1. Quina és l'estructura del grup de punts de torsió?
2. Quin és el rang de E?

També ens podem preguntar, és clar, sobre com calcular els generadors de $E(\mathbb{Q})$. Novament, en aquest problema podem distingir els generadors d'ordre finit i els d'ordre infinit.

Relacionat amb el punt 1 hi ha la qüestió sobre quins possibles grups apareixen com a grups de torsió de corbes el·líptiques. Això va quedar completament resolt gràcies a un resultat de Mazur [26] que havia estat conjecturat el 1908 per Levi.

TEOREMA 2.6 (MAZUR, 1977). *Sigui E una corba el·líptica sobre $\mathbb{Q}$. Aleshores $E(\mathbb{Q})$ és isomorf a algun dels grups següents:*

- $\mathbb{Z}/N\mathbb{Z}$ *amb* $1 \leq N \leq 10$ *o* $N = 12$.
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ *amb* $1 \leq N \leq 4$.

A més, se sap que cadascun d'aquests 15 grups apareix com a grup de torsió d'infinites corbes el·líptiques.

En canvi, el rang és un invariant de les corbes el·líptiques del qual sabem molt menys. Per exemple, no se sap si hi ha corbes el·líptiques de rang arbitràriament gran. Abans hem mostrat exemples de corbes de rang 1 i 2. La corba el·líptica de rang més gran que es coneix[9] va ser trobada per Elkies-Klagsbrun el 2024 i té rang ≥ 29. El rècord anterior era una corba de rang ≥ 28, i havia estat trobada per Elkies el 2006.

9 És la corba d'equació:

$$y^2 = x^3 - 3500001348115367519509130918030550010505939878989991990933965098 7x + 257811997977142991685197145612331535766533036449554194813576383387631020408149548710623489711696 6.$$

No se sap si hi ha corbes de rang més gran. Un argument heurístic de Park-Poonen-Voight-Wood [29] suggereix que els possibles rangs haurien d'estar fitats i, de manera més precisa, que només hi ha un nombre finit de corbes el·líptiques de rang més gran que 21.

Un dels problemes oberts més importants en teoria de nombres és, doncs, el de determinar el rang de les corbes el·líptiques, ja sigui des d'un punt de vista algorítmic o mitjançant alguna fórmula que permeti entendre millor la naturalesa d'aquest invariant. Aquest segon punt de vista és, precisament, el que persegueix la conjectura de Birch i Swinnerton-Dyer, que forma part de la llista de set problemes del mil·lenni presentats per la Fundació Clay l'any 2000. Abans de parlar d'aquesta conjectura, però, hem de fer un petit parèntesi en el nostre estudi de les solucions a $\mathbb{Q}$ i parlar, breument, de les solucions en cossos finits.

3 Punts sobre cossos finits

Suposem que tenim una corba el·líptica com ara, per exemple,

$$E : y^2 = x^3 - x + 1. \tag{3.1}$$

Si p és un nombre primer, podem pensar a trobar solucions de l'equació (3.1) mòdul p. Per exemple, per a $p = 3$ resulta que el punt $(2, 1)$ és una solució mòdul 3. En efecte, si substituïm $x = 2$ i $y = 1$ a l'equació de la corba, no obtenim una igualtat de nombres enters, però sí una congruència mòdul 3:

$$1^2 \equiv 2^3 - 2 + 1 \pmod 3. \tag{3.2}$$

El costat esquerre de (3.2) val 1 i el costat dret val 7, i $7 \equiv 1 \pmod 3$ o, el que és el mateix, $7 - 1$ és múltiple de 3. Fixem-nos que $(2, 1)$ no és un punt racional de la corba, ja que, com hem dit, quan substituïm $x = 2$ i $y = 1$ a l'equació de la corba no obtenim una igualtat de nombres racionals. Però sí que obtenim una congruència mòdul 3; equivalentment, obtenim una igualtat de classes a $\mathbb{Z}/3\mathbb{Z}$. Diem que $(2, 1)$ és un punt de E a $\mathbb{Z}/3\mathbb{Z}$. De fet, és fàcil trobar tots els punts de E a $\mathbb{Z}/3\mathbb{Z}$, ja que les úniques classes de residus mòdul 3 que cal considerar per a x i y són 0, 1 i 2, i podem provar totes les possibilitats i quedar-nos amb aquelles que proporcionin punts mòdul 3. Fent una cerca exhaustiva veiem que

$$E(\mathbb{Z}/3\mathbb{Z}) = \{(0, 1), (0, 2), (1, 1), (2, 1), (2, 2)\} \cup \{O\}.$$

El cos $\mathbb{Z}/p\mathbb{Z}$ es denota habitualment amb $\mathbb{F}_p$, i és l'únic cos finit de cardinal p, llevat d'isomorfisme. Per a cada nombre primer p, podem considerar la quantitat N_p de punts mòdul p; és a dir, $N_p = \#E(\mathbb{F}_p)$. Per a l'exemple (3.1) hem calculat N_p per als primers valors de p:

p	2	3	5	7	11	13	17	19	23	29	31	37
N_p	3	7	8	12	10	19	14	22	23	37	35	36

Podem observar que N_p creix aproximadament al mateix ritme que p. De fet, un argument heurístic ens mostra que podem esperar que el valor de N_p estigui al voltant de $p+1$. Per veure si $(x_0, y_0) \in \mathbb{F}_p \times \mathbb{F}_p$ pertany a $E(\mathbb{F}_p)$, substituïm x_0 a la part de la dreta de l'equació (3.1). Si el valor $x_0^3 - x_0 + 1$ és 0 a $\mathbb{F}_p$, aleshores $(x_0, 0)$ serà un punt; si és diferent de 0, aleshores trobarem dos punts si aquest valor és un quadrat a $\mathbb{F}_p$ i no trobarem cap punt si no és un quadrat. Com que la meitat dels valors no nuls de $\mathbb{F}_p$ són quadrats i la meitat són no quadrats, per a cadascun dels p valors possibles de x_0 esperem trobar un punt, en mitjana. Això ens dona p punts en total, que, si hi sumem el punt O, ens dona $p+1$ com a valor esperat de N_p. Aquest argument és heurístic perquè no sabem quina és la distribució dels valors de $x_0^3 - x_0 + 1$ quan x_0 recorre $\mathbb{F}_p$. En qualsevol cas, podem esperar que la quantitat $a_p = a_p(E) = p + 1 - N_p$, que mesura la diferència entre el nombre de punts real i l'esperat, serà petita. A la figura 6 veiem representada la quantitat $p + 1 - \#E(\mathbb{F}_p)$ respecte als primers p en l'interval $2 \leq p \leq 10^5$, i veiem que no només aquest valor és petit respecte a p, sinó que sembla sempre confinat a una paràbola. Això és cert, i és el contingut d'aquest resultat conjecturat per Artin a la seva tesi i demostrat per Hasse.

TEOREMA 3.1 (HASSE, 1936). *Sigui E una corba elíptica sobre $\mathbb{Q}$, p un primer i posem $a_p = p + 1 - \#E(\mathbb{F}_p)$. Aleshores, $|a_p| \leq 2\sqrt{p}$.*

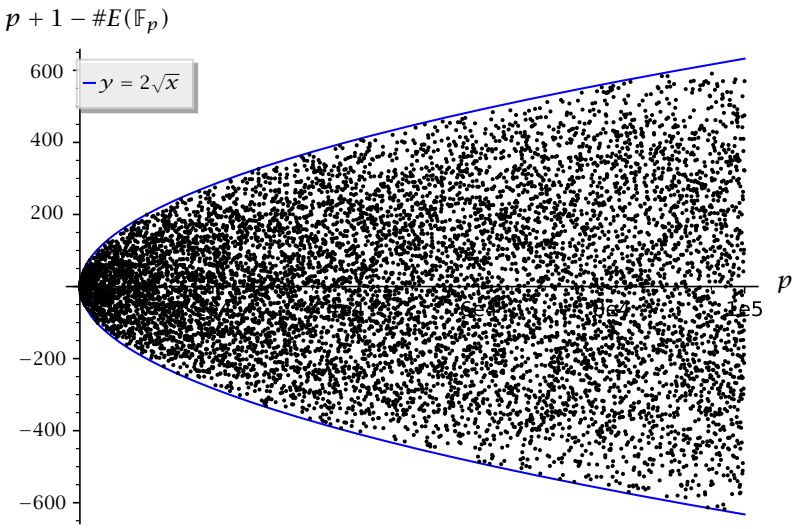


FIGURA 6: Il·lustració del teorema de Hasse.

No es coneix una fórmula tancada que, donada una corba E, calculi la quantitat a_p. En certa manera, la funció $p \mapsto a_p$ es comporta de manera aleatòria, i el que sí que coneixem és la distribució de probabilitat que segueix. Per

formalitzar aquest fet, comencem observant que per la fita de Hasse del teorema 3.1 la quantitat $\overline{a}_p = a_p/\sqrt{p}$ és un nombre real que cau a l'interval $[-2,2]$. Podem preguntar-nos per la «distribució de probabilitat» de la quantitat $\overline{a}_p$, quan pensem p com una quantitat aleatòria. Dit d'una altra manera, donat un subinterval $[\alpha,\beta]$ de l'interval $[-2,2]$, quina és la probabilitat que, si prenem un primer p a l'atzar, el corresponent $\overline{a}_p$ caigui a l'interval $[\alpha,\beta]$?

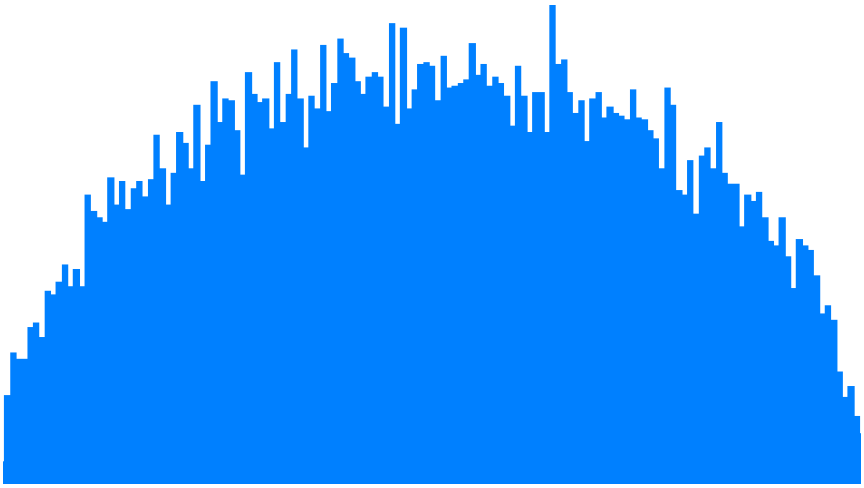


FIGURA 7: Il·lustració de la conjectura de Sato-Tate. Font: [33].

Observem a la figura 7 un histograma (per la corba $y^2 = x^3 + x + 1$) on s'han repartit els valors $\overline{a}_p$ entre 151 subintervals de $[-2,2]$ per a $2 \le p \le 2^{18}$. L'any 1960 Sato i Tate, de manera independent, van conjecturar que la distribució de probabilitat venia donada per un semicercle d'entre -2 i 2; és a dir, era la funció $\frac{4}{\pi}\sqrt{4-x^2}$. La conjectura de Sato-Tate fou finalment demostrada a finals de la primera dècada del segle XXI [34, 20].

TEOREMA 3.2 (CLOZEL-HARRIS-SHEPHERD-BARRON-TAYLOR, 2008). *Si E és «genèrica», aleshores*

$$\lim_{x\to\infty} \frac{\#\{p \le x : \overline{a}_p \in [\alpha,\beta]\}}{\#\{p \le x\}} = \frac{4}{\pi}\int_\alpha^\beta \sqrt{4-x^2}\,dx.$$

El terme *genèrica* fa referència al fet que la corba no tingui multiplicació complexa. Per no allargar-nos excessivament no en donarem la definició precisa (el lector interessat pot consultar [8, § 3.1]), però, en el cas en què la corba no sigui genèrica, també se sap quina és la distribució de probabilitat i, de fet, el resultat és anterior al del cas genèric.

4 La conjectura de Birch i Swinnerton-Dyer

La intuïció darrere la conjectura de Birch i Swinnerton-Dyer (d'ara en endavant, BSD) és que un rang gran de E hauria de donar lloc a molts punts mòdul p; és a dir, esperaríem que N_p fos sistemàticament més gran que el nombre de punts esperat en general, que és $p+1$. Per tal de quantificar aquesta idea, a finals de la dècada dels 1950 Birch i Swinnerton-Dyer van estudiar experimentalment la funció

$$C_E(x) = \prod_{p \leq x} \frac{N_p(E)}{p}, \tag{4.1}$$

on per a cada valor real de x el producte recorre tots els nombres primers p menors o iguals que x.

Emprant un dels primers ordinadors electrònics de la història, l'EDSAC, de la Universitat de Cambridge, van comprovar que per a corbes de rang 0 la funció $C_E(x)$ semblava comportar-se asimptòticament com una constant. En canvi, per a corbes de rang $r > 0$ la funció semblava tendir a infinit quan $x \to \infty$, i l'observació clau fou que ho feia proporcionalment a la funció $(\log x)^r$, com podem veure a la figura 8, on s'il·lustra amb corbes de rang fins a tres.[10] És a dir, semblava que el rang de E es manifestava en l'ordre de creixement de la funció $C_E(x)$. Això va donar lloc a una primera versió de la conjectura [4].

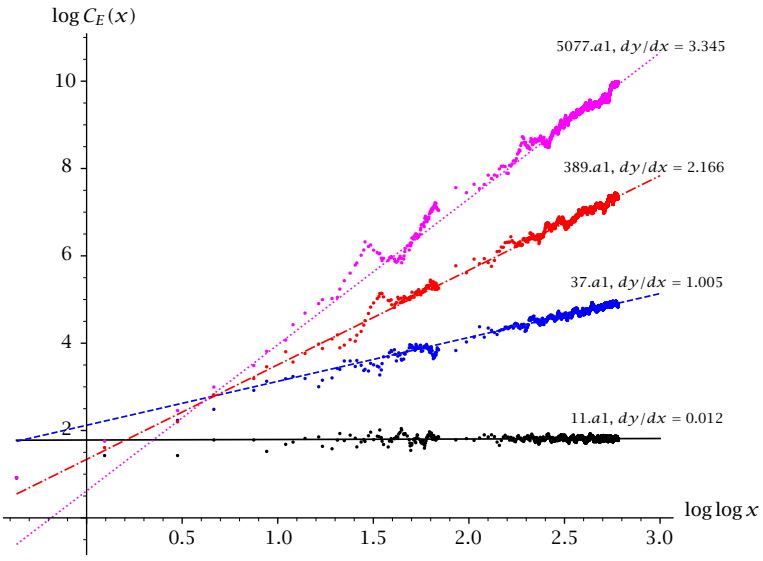


FIGURA 8: Il·lustració de la conjectura BSD, per les corbes 11.a1, 37.a1, 389.a1 i 5077.a1, de rangs 0, 1, 2 i 3, respectivament.

10 Les corbes anomenades `11.a1`, `37.a1`, `389.a1` i `5077.a1` es poden trobar a `https://www.lmfdb.org`, i són les «primeres» que tenen rangs 0, 1, 2 i 3, respectivament.

A l'enunciat següent, el símbol $\sim$ denota que el quocient de les dues funcions tendeix a 1 quan $x \to \infty$.

CONJECTURA 4.1 (BIRCH I SWINNERTON-DYER). *Si E és una corba el·líptica sobre $\mathbb{Q}$ de rang r, aleshores existeix una constant α_E tal que*

$$C_E(x) \sim \alpha_E (\log x)^r.$$

La formulació d'aquesta conjectura és un exemple de com les matemàtiques també poden tenir una component experimental essencial, i és que el càlcul computacional i l'observació de les dades obtingudes fou el que revelà la relació precisa entre el nombre de punts sobre cossos finits i el rang. De fet, una eina fonamental en l'estudi de les corbes el·líptiques són les taules que recullen exemples concrets de corbes i alguns dels seus invariants més notables (rang, punts de torsió, etc.), com ara les taules d'Anvers [3], les taules de Cremona [6] o la base de dades online LMFDB [22], accessible a `https://www.lmfdb.org/`.

La funció $C_E(x)$ resulta ser complicada de controlar des del punt de vista analític. Per això, habitualment la conjectura BSD s'enuncia en termes d'una altra funció amb millors propietats analítiques, que s'anomena *funció L de E* i és, de fet, una funció de variable complexa.[11] Aquesta funció es defineix com un producte infinit de funcions analítiques de variable complexa, indexades pels nombres primers i en què la contribució corresponent a un primer p incorpora la informació sobre el nombre de punts mòdul p, via la quantitat $a_p(E)$. De manera més precisa, si E ve donada per una equació

$$E : y^2 = x^3 + ax + b,$$

la funció L incompleta de E es defineix com a

$$L(E, s) = \prod_p \frac{1}{1 - a_p(E)p^{-s} + p^{1-2s}}, \tag{4.2}$$

on $s \in \mathbb{C}$ és la variable de la funció i p recorre tots els primers senars que no divideixen $4a^3 + 27b^2$. Es pot veure que la fita de Hasse $|a_p(E)| \leq 2\sqrt{p}$ implica que aquest producte infinit convergeix a una funció analítica en el semiplà del pla complex format pels nombres de part real més gran que $3/2$. De fet, Hasse també va conjecturar que $L(E, s)$ admet continuació analítica a tot el pla complex. Això està demostrat avui en dia, com a conseqüència del teorema de modularitat, demostrat per Breuil-Conrad-Diamond-Taylor el 2001 [5] amb les tècniques introduïdes per Wiles i Taylor i Wiles en la seva demostració del darrer teorema de Fermat.

En particular, té sentit avaluar $L(E, s)$ en $s = 1$. No podem fer-ho directament a la fórmula (4.2), ja que el producte infinit només convergeix per a part real

11 Una altra funció de variable complexa que apareix de manera notable en aritmètica és la funció ζ de Riemann [31]. De fet, hi ha una construcció general que permet associar funcions L a objectes geomètrics i obtenir $\zeta(s)$ i $L(E, s)$ com a casos particulars, així que podem pensar en $L(E, s)$ com una determinada generalització de $\zeta(s)$.

de s més gran que $3/2$. Però, si ens oblidem per un moment del problema amb la convergència i substituïm formalment $s = 1$ al producte infinit, multiplicant i dividint el terme p-èsim per p obtenim que

$$L(E,1)\text{« = »}\prod_p \frac{1}{1 - a_p(E)p^{-1} + p^{-1}}\text{« = »}\prod_p \frac{p}{N_p(E)}.$$

Les cometes als signes d'igualtat indiquen que l'argument és heurístic i no són igualtats rigoroses. Però, tolerant aquest inconvenient, si comparem amb (4.1), veiem que això hauria de correspondre a l'invers del valor $\lim_{x\to\infty} c_E(x)$. Per tant, sembla que el comportament de $L(E,s)$ en $s = 1$ hauria de reflectir el comportament asimptòtic de $c_E(x)$, i, com que un és l'invers de l'altre, com més gran sigui el rang r, més ràpid hauria de tendir a 0 la funció en $s = 1$. Això és, justament, el que diu la versió més habitual de la conjectura BSD; per exemple, la que apareix en la descripció oficial del problema del mil·lenni de la Fundació Clay [38].

CONJECTURA 4.2 (BSD). *Si E té rang r, aleshores $L(E,s)$ té un zero d'ordre r en $s = 1$. És a dir,*

$$L(E,s) = c(s-1)^r + \textit{termes d'ordre superior},$$

per a determinada constant $c \neq 0$.

Malgrat que a primer cop d'ull pugui semblar el contrari, aquesta conjectura no ens ajuda gaire en el problema algorítmic del càlcul del rang, ja que no es coneixen algoritmes per a calcular l'ordre d'anul·lació de $L(E,s)$ en $s = 1$ quan aquest ordre és més gran que 3. De fet, avui dia no coneixem cap corba el·líptica E per la qual puguem demostrar que l'ordre d'anul·lació de $L(E,s)$ és 4.

Hi ha una «versió forta» de la conjectura, que involucra la funció L completa (en què s'incorporen també termes corresponents a $p \mid 2(4a^3 + 27b^2)$, que són una mica més complicats de definir). En aquest cas la conjectura prediu el valor de la constant c en el primer terme del desenvolupament de Taylor en funció de certs invariants aritmètics i geomètrics de E. Si aquesta versió forta fos certa, això sí que donaria lloc a un algoritme per a calcular el rang i un conjunt de generadors de $E(\mathbb{Q})$.

La conjectura BSD, fins i tot en la seva «versió dèbil» que hem enunciat, encara està oberta en completa generalitat. Això no obstant, se'n coneixen alguns resultats parcials. El més important des del punt de vista del present article és, sens dubte, el que es deriva dels treballs de Gross, Zagier i Kolyvagin de finals de la dècada del 1980 [16, 21].

TEOREMA 4.3 (GROSS-ZAGIER 1986, KOLYVAGIN 1988). *Si l'ordre d'anul·lació de la funció $L(E,s)$ en $s = 1$ és 0 o 1, aleshores la conjectura BSD per a E és certa.*

Dit d'una altra manera: si $L(E,1) \neq 0$, el rang és 0; i si $L(E,1) = 0$ i $L'(E,1) \neq 0$, el rang és 1. En particular, si $L(E,1) = 0$ i $L'(E,1) \neq 0$, aleshores hi ha un punt d'ordre infinit a E. Aquesta és la part del resultat que van provar Gross i Zagier, i per a la qual van resoldre el problema clau: donada una corba el·líptica amb $L(E,1) = 0$ i $L'(E,1) \neq 0$, com construir un punt racional d'ordre infinit? L'eina fonamental que van emprar són els anomenats *punts de Heegner*, introduïts uns anys abans per Birch i que, en certa manera, ja havien estat descoberts per Heegner en un context lleugerament diferent.

5 Punts de Heegner i exemples

Com ja hem avançat més amunt, els punts de Heegner són punts definits a la corba el·líptica E que són d'ordre infinit quan l'ordre d'anul·lació de la funció $L(E,s)$ és exactament 1, i, per tant, en aquesta secció assumirem que aquest és el cas. A més, ens cal utilitzar el fet que E és *modular*, així que primer veurem què vol dir que una corba el·líptica sigui modular. De fet, una manera ràpida de dir-ho és dir que la corba E està associada a una forma modular. Però aleshores ens cal explicar què és una forma modular, i què vol dir que E hi estigui associada.

Considerem, doncs, el semiplà superior de Poincaré $\mathbb{H}$, que simplement és conjunt de complexos amb part imaginària positiva:

$$\mathbb{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}.$$

Aquest espai, que també s'anomena *semiplà hiperbòlic*, té una mètrica associada donada per

$$ds = \frac{dx\,dy}{y^2}, \quad z = x + iy.$$

Les isometries de $\mathbb{H}$ venen donades justament pel grup

$$\mathrm{PSL}_2(\mathbb{R}) = \{\gamma \in \mathrm{M}_2(\mathbb{R}) \mid \det \gamma = 1\}/\{\pm 1\},$$

on l'acció d'una matriu $\gamma = \left(\begin{smallmatrix} a & b \\ c & c \end{smallmatrix}\right)$ és per una transformació fraccionària lineal

$$z \longmapsto \frac{az+b}{cz+d}.$$

En particular, el grup $\mathrm{SL}_2(\mathbb{R})$ actua a $\mathbb{H}$, i ens interessa estudiar funcions que es comporten de manera molt simètrica respecte a determinats subgrups. Concretament, en el cas de les corbes el·líptiques fixarem un enter positiu N i considerarem el grup

$$\Gamma_0(N) = \left\{\left(\begin{smallmatrix} a & b \\ c & c \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}) \mid ad - bc = 1,\, N \mid c\right\},$$

és a dir, en el grup de matrius dos per dos a coeficients enters, determinant 1 i amb l'entrada inferior esquerra divisible per N.

DEFINICIÓ 5.1. Una forma modular de nivell N (cuspidal i de pes 2) és una funció holomorfa $f\colon \mathbb{H} \to \mathbb{C}$ tal que:

1. $f(\gamma z) = (cz + d)^2 f(z)$ per a tota $\gamma = \left(\begin{smallmatrix} a & b \\ c & c \end{smallmatrix}\right) \in \Gamma_0(N)$, i
2. $\lim_{z \to i\infty} (cz + d)^{-2} f(\gamma z) = 0$ per a tota $\gamma = \left(\begin{smallmatrix} a & b \\ c & c \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

Com que la matriu $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ pertany a $\Gamma_0(N)$ sigui quin sigui N, tota forma modular f és 1-periòdica, i, per tant, té una sèrie de Fourier. De fet, com que f és holomorfa, podem escriure

$$f(z) = \sum_{n=1}^{\infty} a_n(f) e^{2\pi i n z}, \quad a_n(f) \in \mathbb{C}.$$

Sovint s'abreuja $q = e^{2\pi i z}$ i s'anomena $\sum_{n=1}^{\infty} a_n(f) q^n$ la q-expansió de f. Evidentment és temptador considerar la sèrie de Dirichlet associada a aquests coeficients, que no és més que la funció

$$L(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}.$$

Un teorema de Hecke ens assegura que per a tot primer p es té $|a_p(f)| = O(p)$, i, com a conseqüència dels resultats de Deligne sobre les conjectures de Weil, sabem que, de fet, $|a_p(f)| \leq 2\sqrt{p}$. En tot cas, la sèrie $L(f, s)$ convergeix per $\mathrm{Re}(s)$ suficientment gran. A més, la simetria de f ens permet continuar analíticament $L(f, s)$ a una funció holomorfa a tot $\mathbb{C}$.

TEOREMA 5.2 (TAYLOR-WILES, WILES, BREUIL-CONRAD-DIAMOND-TAYLOR). *Donada una corba el·líptica E, hi ha un enter positiu N_E i una forma modular f_E de nivell N_E, de manera que per a tot primer p es té*

$$a_p(f_E) = p + 1 - \#E(\mathbb{F}_p).$$

La quantitat N_E s'anomena *conductor* de la corba, i hi ha algoritmes que el calculen de manera senzilla a partir de l'equació de Weierstrass. A més, els primers que divideixen N_E són essencialment els mateixos que divideixen el discriminant de E. És més, la funció $L(E, s)$ es pot definir de manera que també incorpori els primers que divideixen el discriminant, i aleshores el teorema de modularitat ens diu que hi ha una forma modular f_E tal que $L(f_E, s) = L(E, s)$.

Tal com l'hem enunciat, no està clar com es pot aprofitar aquest teorema per a construir punts a la corba el·líptica, que recordem que és el nostre objectiu.

Per a entendre com l'existència de la forma modular f_E ens permet trobar punts a E ens caldria entendre l'estructura algebraica que hi ha al darrere del quocient analític $Y_0(N) = \Gamma_0(N) \backslash \mathbb{H}$. En aquesta nota, però, ens conformarem amb la següent conseqüència.

Tal com hem vist a la secció 1, els punts complexos, que denotem amb $E(\mathbb{C})$, formen una superfície a l'espai de dimensió (real) 4 que és $\mathbb{C} \times \mathbb{C}$, que s'anomena

superfície de Riemann, ja que fou Riemann qui primer estudià aquest tipus de superfícies. En el cas que ens ocupa, es pot calcular un reticle

$$\Lambda_E = \{m + n\tau_E \mid m, n \in \mathbb{Z}\} \subset \mathbb{C}$$

per a un determinat element $\tau_E \in \mathbb{H}$, i es té un isomorfisme analític[12]

$$\mathbb{C}/\Lambda_E \xrightarrow{\cong} E(\mathbb{C}).$$

L'aplicació

$$\tau \longmapsto \int_{i\infty}^{\tau} 2\pi i f_E(z)\, dz$$

envia $Y_0(N)$ a $\mathbb{C}/\Lambda$, on Λ és homotètic a Λ_E. Això fa que, reescalant la integral anterior, puguem considerar una aplicació analítica

$$\Phi_N \colon Y_0(N) \longrightarrow E(\mathbb{C}),$$

que anomenarem *parametrització modular*. Val a dir que aquesta funció (o una aproximació arbitràriament bona) es pot calcular a partir de la q-expansió de f_E, i que s'ha fet molta recerca per a aconseguir que aquest càlcul sigui molt eficient.

L'últim ingredient que ens falta, doncs, per a obtenir punts a $E(\mathbb{Q}) \subset E(\mathbb{C})$ és trobar punts adequats a $Y_0(N)$. La funció Φ_N és altament transcendent, i, per tant, en principi no esperaríem que punts algebraics a $\mathbb{H}$ donin lloc a punts algebraics a $E(\mathbb{C})$, cosa que gairebé no passa mai. Tot i així, la teoria de multiplicació complexa garanteix que, si $\tau \in \mathbb{H}$ és un quadràtic imaginari (és a dir, satisfà una equació de la forma $A\tau^2 + B\tau + C = 0$ amb $A, B, C \in \mathbb{Z}$ i $B^2 - 4AC < 0$), aleshores $\Phi_N(\tau) \in E(\mathbb{C})$ té coordenades definides[13] en una extensió algebraica de $\mathbb{Q}(\tau)$. La situació és semblant al que passa amb les funcions trigonomètriques: la funció $x \mapsto \sin(2\pi x)$ és transcendent, però resulta que, si x és racional, aleshores $\sin(2\pi x)$ és un nombre algebraic.[14]

Vegem un exemple que ens ajudarà a clarificar la construcció que hem fet. Considerem la corba el·líptica[15]

$$E : y^2 + y = x^3 - x,$$

que és la corba el·líptica «més simple» de rang 1. La forma modular f_E associada a E per modularitat té q-expansió

$$f_E(q) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + \cdots$$

12 Un isomorfisme analític és aquell que ve donat per funcions holomorfes amb inversa holomorfa.

13 Per tal que això sigui cert ens cal assumir una condició tècnica, coneguda com la «hipòtesi de Heegner»: els primers divisors de N no poden ser *inerts* a $\mathbb{Q}(\tau)$.

14 De fet, la teoria de Galois ens permet predir en quina extensió de $\mathbb{Q}$ està definit $\sin(2\pi x)$ en aquest cas.

15 `https://www.lmfdb.org/EllipticCurve/Q/37/a/1`.

Considerem ara

$$\tau = \frac{-21 + \sqrt{-3}}{74} \in \mathbb{H}.$$

Calculem de manera aproximada $\Phi_N(\tau)$ i obtenim

$$\Phi_N(\tau) \simeq \left(-1.000\,000, 1.11 \cdot 10^{-16}\right) \in E(\mathbb{C}).$$

Podem comprovar que $(-1,0) = 3(0,-1) + (0,1)$, i que $E(\mathbb{Q}) = \{O, (0,1)\} \times \langle (0,-1) \rangle$. Així doncs, la construcció dels punts de Heegner ens ha donat lloc al punt d'ordre infinit l'existència del qual hauríem pogut predir (gràcies a la conjectura BSD) del fet que la L-sèrie $L(E,s)$ tingués un zero (simple) a $s = 1$.

Observem que en aquest cas el punt que hem obtingut té coordenades racionals, però això prové del fet que $\operatorname{rang} E(\mathbb{Q}) = \operatorname{rang} E(\mathbb{Q}(\sqrt{-3})) = 1$.

Vegem per acabar un altre exemple que mostra com els punts de Heegner tenen coordenades a extensions (potser trivials) de cossos quadràtics imaginaris. En aquest cas, considerem la corba[16] donada per l'equació

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$

que té conductor 11 i forma modular associada

$$f_E = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + \cdots$$

En aquest cas prenem

$$\tau = \frac{-9 + \sqrt{-7}}{22},$$

que genera el cos quadràtic imaginari $\mathbb{Q}(\sqrt{-7})$, i calculem

$$\Phi_N(\tau) \simeq \left(0.500\,000 - 1.322\,876\sqrt{-1}, -2.000\,00 - 5.291\,502\,6\sqrt{-1}\right).$$

El punt obtingut és molt proper a

$$P_{\sqrt{-7}} = \left(\frac{1 + \sqrt{-7}}{2}, -2 + 2\sqrt{-7}\right) \in E(\mathbb{Q}(\sqrt{-7})),$$

que es pot escriure com a

$$P_{\sqrt{-7}} = \left(-6, \frac{-1 - 11\sqrt{-7}}{2}\right) + (5,5).$$

Es pot veure que $E(\mathbb{Q}(\sqrt{-7}))$ és isomorf (com a grup abelià) a $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}$, amb generador de $\mathbb{Z}/5\mathbb{Z}$ donat per $(5,5)$ i generador de la part lliure donat per $(-6, \frac{-1-11\sqrt{-7}}{2})$.

16 https://www.lmfdb.org/EllipticCurve/Q/11/a/2.

6 Corbes el·líptiques sobre els p-àdics

A finals del segle passat, Darmon proposà a [7] una construcció anàloga a la dels punts de Heegner, en el cas que l'extensió quadràtica que considerem sigui real. En aquesta secció i la propera intentarem donar una idea d'aquesta construcció, que, a diferència de la construcció de punts de Heegner, dona lloc a punts que—avui dia—encara no sabem demostrar que siguin algebraics.

Ja d'entrada ens adonem fàcilment que la construcció de Heegner no funcionarà en aquesta situació, ja que, si τ és real, aleshores segur que no pertany a $\mathbb{H}$ (recordem que $\mathbb{H}$ està format per complexos amb part imaginària *estrictament* positiva). La idea brillant de Darmon va ser considerar un altre tipus de semiplà que sí que contindria aquests punts reals. Així, substituí $\mathbb{H}$ per un pla p-àdic, on p és un primer divisor del conductor de la corba. Per tal de simplificar l'exposició suposarem que el conductor de la corba el·líptica que considerem és primer.

Els nombres p-àdics, que habitualment s'escriuen com a $\mathbb{Q}_p$, s'obtenen a partir dels racionals de manera anàloga a com se n'obtenen els nombres reals, és a dir, prenent una compleció dels racionals respecte d'un valor absolut. Si prenem el valor absolut usual, obtenim els reals $\mathbb{R}$, però, si prenem el valor absolut p-àdic (que veurem seguidament), aleshores obtindrem els nombres p-àdics.

El valor absolut p-àdic, que denotarem amb $|\cdot|_p$, es defineix en els enters com a

$$|a|_p = p^{-v_p(a)}, \quad v_p(a) = \max\{k \mid p^k \text{ divideix } a\}.$$

Per exemple, com que 3^2 divideix 18 i 3^3 no, tenim $|18|_3 = 1/9$. Així, si pensem 3-àdicament, el nombre 18 és *més petit que* el nombre 1 (per a qualsevol p, es té $|1|_p = 1$). De manera semblant, els nombres $3, 9, 27, \ldots, 3^n, \ldots$ tendeixen a zero 3-àdicament, encara que amb el valor absolut usual ens sembli que es fan grans.

El valor absolut p-àdic es pot estendre de manera directa als racionals, definint

$$\left|\frac{a}{b}\right|_p = \frac{|a|_p}{|b|_p},$$

i així obtenim un valor absolut que respecta la multiplicació: per a tot $x, y \in \mathbb{Q}$, tenim $|xy|_p = |x|_p|y|_p$.

De la mateixa manera que podem aproximar qualsevol real no nul mitjançant un enter multiplicat per una potència de 10, també podem aproximar qualsevol p-àdic no nul mitjançant un enter multiplicat per una potència de p. En aquest cas, dos enters seran molt propers (p-àdicament) si la seva diferència és divisible per una potència molt gran de p. Per exemple, els nombres 14 i 500 són bastant propers a $\mathbb{Q}_3$, ja que la seva diferència és $486 = 2 \cdot 3^5$, que té valor absolut 3-àdic igual a $3^{-5} \simeq 0.004\,115$. D'altra banda, 14 està a distància 1 de 2, ja que $|14 - 2|_3 = |13|_3 = 1$.

De la mateixa manera que per a definir els punts de Heegner no n'hem tingut prou amb els reals i hem hagut de considerar els nombres complexos, en

el cas p-àdic també ens caldrà considerar un cos més gran que $\mathbb{Q}_p$. Recordem que per construir els complexos adjuntem una arrel del polinomi x^2+1, que és irreductible si el pensem en els reals. Així, considerarem una extensió $\mathbb{C}_p$ de grau 2 de $\mathbb{Q}_p$, que es pot obtenir, per exemple, adjuntant l'arrel d'un polinomi mònic de grau 2 amb coeficients a $\mathbb{Z}$ que sigui irreductible mòdul p.[17]

Hi ha una teoria de corbes el·líptiques sobre $\mathbb{Q}_p$, i resulta que també donen lloc a tors (en aquest cas, tors p-àdics), però en aquesta situació ens cal una versió multiplicativa. Fixem-nos que, en el cas complex, la funció exponencial $z \mapsto e^{2\pi i z}$ dona lloc a un isomorfisme $\mathbb{C}/\Lambda_E \cong \mathbb{C}^\times/q_E^{\mathbb{Z}}$, on $q_E = e^{2\pi i \tau_E}$ i

$$q_E^{\mathbb{Z}} = \{q_E^n \mid n \in \mathbb{Z}\}.$$

En el cas p-àdic, es té un isomorfisme analític (donat per sèries de potències amb coeficients p-àdics)

$$\eta_{\mathrm{Tate}} \colon \mathbb{C}_p^\times/q_E^{\mathbb{Z}} \longrightarrow E(\mathbb{C}_p),$$

on $q_E \in \mathbb{Q}_p^\times$, que s'anomena *període de Tate*, s'obté també de manera senzilla a partir de l'equació de E.

Fins aquí hem intentat convèncer el lector de substituir els punts complexos de la corba el·líptica $E(\mathbb{C})$ pels punts p-àdics $E(\mathbb{C}_p)$. Ens hem de preguntar, doncs, per quins objectes anàlegs substituirem el semiplà de Poincaré $\mathbb{H}$ i el grup $\Gamma_0(p)$. D'entrada, podem pensar que $\mathbb{H} = (\mathbb{C} \setminus \mathbb{R})^+$, on el símbol $+$ fa referència a la component connexa formada pels complexos amb part imaginària positiva. Així, no ens sorprendrà que definim el *semiplà p-àdic* $\mathbb{H}_p$ com a $\mathbb{C}_p \setminus \mathbb{Q}_p$ (en aquest cas, no té sentit considerar una component «positiva»). El grup $\mathrm{PSL}_2(\mathbb{Q}_p)$ actua a $\mathbb{H}_p$ per transformacions fraccionàries lineals, i el grup anàleg a $\Gamma_0(p)$ que considerà Darmon, seguint Ihara, és el grup

$$\Gamma = \mathrm{SL}_2(\mathbb{Z}[1/p]) = \left\{\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}[1/p])) \mid \det \gamma = 1\right\}.$$

La notació $\mathbb{Z}[1/p]$ significa l'anell format pels racionals a/b, on b és una potència de p. Ara ja tenim definits objectes p-àdics $\Gamma\backslash\mathbb{H}_p$ i $E(\mathbb{C}_p)$, i ens resta per veure:

1. Quin és l'anàleg p-àdic de l'aplicació Φ_N de la secció anterior, i
2. Quins punts interessants es poden definir a $\Gamma\backslash\mathbb{H}_p$ que donin lloc a punts algebraics a $E(\mathbb{C}_p)$?

En la secció següent veurem que el camí no és tan directe, i ens veurem obligats a combinar la teoria p-àdica amb la complexa per definir els punts que cerquem a $E(\mathbb{C}_p)$.

17 A la literatura sovint s'escriu $\mathbb{C}_p$ per a referir-se a la compleció de la clausura algebraica de $\mathbb{Q}_p$, que aquí no farem servir.

7 Punts de Stark-Heegner i exemples

Recordem que el teorema de modularitat ens permet associar a una corba el·líptica E una certa forma modular f_E. De fet, el que acabem integrant és una 1-forma diferencial $\omega_E = 2\pi i f(z)\,dz$. La propietat de simetria per al grup $\Gamma_0(p)$ (recordem que estem assumint que el conductor $N_E = p$ és primer) fa que ω_E sigui invariant per a aquest grup i, per tant, la forma diferencial ω_E és una forma a $Y_0(p)$.

Un dels punts clau de la construcció de Darmon consisteix a considerar el producte $\mathbb{H}_p \times \mathbb{H}$, on actua el grup Γ de manera diagonal, i a associar a E una $(1,1)$-forma diferencial Ω_E a $X_\Gamma = \Gamma\backslash(\mathbb{H}_p \times \mathbb{H})$. Val a dir que el llenguatge que estem fent servir no és gaire precís, ja que $\mathbb{H}_p$ és totalment disconnex amb la topologia p-àdica i la diferenciabilitat no funciona com amb els complexos. Per fer-ho precís hauríem de recórrer a la geometria rigidoanalítica, però en aquest article l'analogia ens servirà.

De manera anàloga a com en la secció anterior hem integrat una 1-forma diferencial al llarg d'un camí complex $i\infty \rightsquigarrow \tau$, aquesta nova $(1,1)$-forma diferencial l'haurem d'integrar sobre una 2-cadena. Fixem-nos que el camí complex $i\infty \rightsquigarrow \tau$ té com a vora la 0-cadena tancada $(\tau) - (i\infty)$. Així, si volem seguir l'analogia, hauríem de trobar un 1-cicle exacte, és a dir, que sigui la vora d'una 2-cadena. Heus ací com podem procedir: donat un punt $\tau \in \mathbb{H}_p$ que satisfaci una equació $A\tau^2 + B\tau + C = 0$ amb $B^2 - 4AC > 0$, es pot considerar el subgrup estabilitzador

$$\Gamma_\tau = \{\alpha \in \Gamma \mid \alpha\tau = \tau\},$$

que resulta estar generat per una matriu γ. També es pot veure que una certa potència[18] de γ es pot escriure com a producte de commutadors:

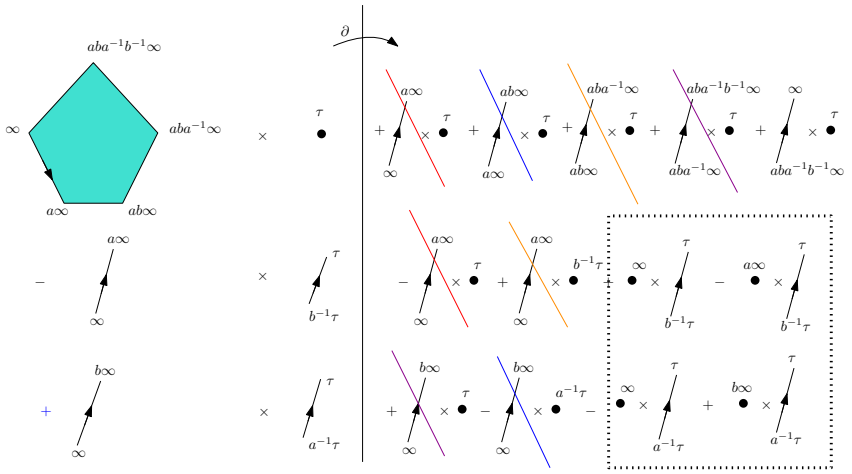
$$\gamma^e = [a_1, b_1][a_2, b_2] \cdots [a_t, b_t].$$

El cicle que considera Darmon és

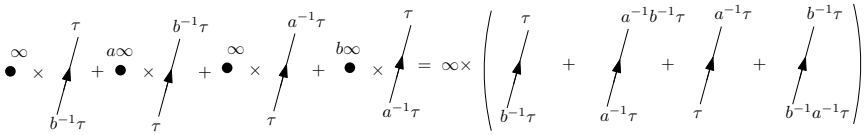
$$\Theta = (\gamma^e \infty \rightsquigarrow \infty) \times \{\tau\} \in \Gamma\backslash(\mathbb{H} \times \mathbb{H}_p).$$

Aquest cicle és tancat, i, de fet, es pot veure que és exacte, és a dir, que hi ha una 2-cadena Δ tal que $\partial\Delta = \Theta$. Per fer-ho suposem, per tal de simplificar la notació, que només apareix un commutador en la descomposició de γ^e, així que $\gamma^e = aba^{-1}b^{-1}$. El diagrama següent mostra la 2-cadena corresponent:

18 En general, cal modificar γ fent servir uns operadors determinats coneguts com a *operadors de Hecke*, però podem obviar aquest detall en aquesta primera aproximació.



Observem que molts dels termes es cancel·len. D'altra banda, la part que apareix enquadrada es pot reescriure com a



Però, com que

$$a^{-1}b^{-1}\tau = b^{-1}a^{-1}aba^{-1}b^{-1}\tau = b^{-1}a^{-1}\gamma\tau = b^{-1}a^{-1}\tau,$$

aquesta 1-cadena és nul·la. En conclusió, tots els termes excepte un es cancel·len i, per tant,

$$\Theta = \partial\Big(\pentagon \times \{\tau\} - (\infty \to a\infty) \times (b^{-1}\tau \to \tau) + (\infty \to b\infty) \times (a^{-1}\tau \to \tau)\Big).$$

Podem definir la integral

$$J_\tau = \int_\infty^{a\infty} \int_\tau^{b^{-1}\tau} \Omega_E - \int_\infty^{b\infty} \int_\tau^{a^{-1}\tau} \Omega_E \in \mathbb{C}_p.$$

Per exemple, considerem la corba el·líptica de l'apartat anterior

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$

de conductor $p = 11$. Com que $x^2 - 13$ no té arrels mòdul 11, podem escollir

$$\tau = \frac{3 - \sqrt{13}}{2} \in \mathbb{H}_{11}.$$

Calculem una aproximació de la integral anterior, que dona lloc al punt

$$J_\tau = 275\,514\,415\,488\,849\,148\,207\tau + 302\,729\,526\,018\,381\,608\,293 \pmod{11^{20}}.$$

Aplicant l'isomorfisme a $E(\mathbb{C}_{11})$, obtenim

$$\eta_{\mathrm{Tate}}(J_\tau) \simeq \Big(645\,077\,502\,996 + 732\,103\,938\,720\tau + O(11^{20}),\\ 4\,172\,141\,459\,976\,479 + 4\,172\,141\,459\,976\,479\tau + O(11^{20})\Big),$$

que és proper al punt algebraic d'ordre infinit

$$2\cdot\Big(-8\,071\,272/139\,129\tau + 52\,783\,800/139\,129,\\ 109\,494\,875\,952/51\,895\,117\tau - 329\,723\,275\,860/51\,895\,117\Big) \in E(\mathbb{Q}(\sqrt{13})).$$

Com hem remarcat a la secció anterior, una diferència important entre la teoria de punts de Heegner de la secció 5 i la teoria de punts de Stark-Heegner que hem vist en aquesta secció és que aquesta darrera és una teoria encara majoritàriament conjectural. Això es deu al fet que la construcció que hem explicat de punts de Heegner és la vessant analítica d'una teoria geomètrica de punts de Heegner, que permet demostrar que els punts obtinguts no només són punts amb components complexes, sinó que, de fet, són punts amb components algebraiques. La construcció de punts de Stark-Heegner es pot veure com un anàleg analític p-àdic de la construcció complexa de punts de Heegner, però en el cas de Stark-Heegner no es coneix l'anàleg de la construcció geomètrica.

Tot i així, al llarg dels anys han aparegut molts resultats que donen evidència de la validesa d'aquesta conjectura, tant de caire computacional i experimental ([9, 17]), en què es comprova en nombrosos exemples que els punts de Stark-Heegner són molt propers a punts racionals d'ordre infinit, com de caire teòric ([27, 23, 2, 24, 10]), en què es demostren casos particulars de la conjectura.

8 Epíleg

La construcció original de Darmon s'ha generalitzat en múltiples direccions en les més de dues dècades que han passat des de l'article fundacional [7]. La hipòtesi de Heegner (sobre el comportament en el cos quadràtic dels divisors del conductor) es pot relaxar a canvi de considerar subgrups de $\mathrm{SL}_2(\mathbb{R})$ o $\mathrm{SL}_2(\mathbb{Q}_p)$ donats per àlgebres de quaternions en comptes dels grups $\Gamma_0(N)$ ([15]), i es poden considerar corbes el·líptiques sobre cossos de nombres diferents de $\mathbb{Q}$, com ara cossos quadràtics imaginaris ([36]). Avui en dia, disposem de construccions conjecturals de punts algebraics sempre que el signe de l'equació funcional de $L(E/K, s)$ sigui senar, i les conjectures prediuen que aquestes construccions donen lloc a punts algebraics d'ordre infinit sempre que l'ordre d'anul·lació de $L(E/K, s)$ a $s = 1$ sigui exactament 1. Per a més detalls, convidem el lector a consultar [19] i [18], en què la construcció es presenta des del punt de vista més general.

També cal mencionar l'existència de generalitzacions que van més enllà de la situació de corbes el·líptiques de rang 1 tractada en aquest article. Per

exemple, els cicles de Stark-Heegner ([32]) o, més recentment, els anomenats *punts plèctics*, que, inspirats per les construccions de Darmon, proporcionen invariants p-àdics en certes situacions de rang > 1 ([13, 14]).

En aquest article hem volgut fer un tast d'algunes conjectures sobre corbes el·líptiques i les corresponents respostes parcials que sabem donar. Concretament, la conjectura de Birch i Swinnerton-Dyer segueix essent una font d'inspiració per a la teoria de nombres del segle XXI, i les construccions explícites que va introduir Heegner i ha generalitzat Darmon i altres contemporanis ens proveeixen d'una petita ajuda a l'hora d'entendre aquesta misteriosa relació entre l'anàlisi de les L-sèries i l'aritmètica dels punts racionals. Segurament caldran altres idees fonamentalment noves per a poder demostrar la conjectura en casos de rangs superiors a 1, on fins avui tenim ben pocs resultats teòrics.

Referències

[1] BAYER, P. «Les contribucions de Poincaré a l'aritmètica». *Butlletí de la Societat Catalana de Matemàtiques*, 21 (1) (2006), 5–38.

[2] BERTOLINI, M.; DARMON, H. «The rationality of Stark-Heegner points over genus fields of real quadratic fields». *Ann. of Math. (2)*, 170 (1) (2009), 343–370.

[3] BIRCH, B. J.; KUYK, W. (ED.). *Modular Functions of One Variable. IV.* Proceedings of the International Summer School, University of Antwerp, July 17–August 3, 1972. Berlín; Nova York: Springer-Verlag, 1975. (Lecture Notes in Math.; 476)

[4] BIRCH, B. J.; SWINNERTON-DYER, H. P. F. «Notes on elliptic curves. II». *J. Reine Angew. Math.*, 218 (1965), 79–108.

[5] BREUIL, C.; CONRAD, B.; DIAMOND, F.; TAYLOR, R. «On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises». *J. Amer. Math. Soc.*, 14 (4) (2001), 843–939.

[6] CREMONA, J. E. *Algorithms for Modular Elliptic Curves*. 2a ed. Cambridge: Cambridge University Press, 1997.

[7] DARMON, H. «Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications». *Ann. of Math. (2)*, 154 (3) (2001), 589–639.

[8] DARMON, H. *Rational Points on Modular Elliptic Curves*. Washington, DC: Conference Board of the Mathematical Sciences; Providence, RI: American Mathematical Society, 2004. (CBMS Reg. Conf. Ser. Math.; 101)

[9] DARMON, H.; POLLACK, R. «Efficient calculation of Stark-Heegner points via overconvergent modular symbols». *Israel J. Math.*, 153 (2006), 319–354.

[10] DARMON, H.; ROTGER, V. «Stark-Heegner points and diagonal classes». A: *Heegner Points, Stark-Heegner Points, and Diagonal Classes. Astérisque*, 434 (2022), 1–28.

[11] DIMITROV, V.; GAO, Z.; HABEGGER, P. «Uniformity in Mordell-Lang for curves». *Ann. of Math. (2)*, 194 (1) (2021), 237–298.

[12] Faltings, G. «Endlichkeitssätze für abelsche Varietäten über Zahlkörpern». *Invent. Math.*, 73 (3) (1983), 349–366.

[13] Fornea, M.; Gehrmann, L. «Plectic Stark-Heegner points». *Adv. Math.*, 414 (2023), article núm. 108861, 42 p.

[14] Fornea, M.; Guitart, X.; Masdeu, M. «Plectic p-adic invariants». *Adv. Math.*, 406 (2022), article núm. 108484, 26 p.

[15] Greenberg, M. «Stark-Heegner points and the cohomology of quaternionic Shimura varieties». *Duke Math. J.*, 147 (3) (2009), 541–575.

[16] Gross, B. H.; Zagier, D. B. «Heegner points and derivatives of L-series». *Invent. Math.*, 84 (2) (1986), 225–320.

[17] Guitart, X.; Masdeu, M. «Elementary matrix decomposition and the computation of Darmon points with higher conductor». *Math. Comp.*, 84 (292) (2015), 875–893.

[18] Guitart, X.; Masdeu, M.; Molina, S. «An automorphic approach to Darmon points». *Indiana Univ. Math. J.*, 69 (4) (2020), 1251–1274.

[19] Guitart, X.; Masdeu, M.; Şengün, M. H. «Darmon points on elliptic curves over number fields of arbitrary signature». *Proc. Lond. Math. Soc. (3)*, 111 (2) (2015), 484–518.

[20] Harris, M.; Shepherd-Barron, N.; Taylor, R. «A family of Calabi-Yau varieties and potential automorphy». *Ann. of Math. (2)*, 171 (2) (2010), 779–813.

[21] Kolyvagin, V. A. «Euler systems». A: *The Grothendieck Festschrift, Vol. II*. Boston, MA: Birkhäuser Boston, Inc., 1990, 435–483. (Progr. Math.; 87)

[22] LMFDB, «The L-functions and modular forms database (LMFDB)». Publicat en línia (2024). `https://www.lmfdb.org`.

[23] Longo, M.; Martin, K.; Hu, Y. «Rationality of Darmon points over genus fields of non-maximal orders». *Ann. Math. Qué.*, 44 (1) (2020), 173–195.

[24] Longo, M.; Vigni, S. «The rationality of quaternionic Darmon points over genus fields of real quadratic fields». *Int. Math. Res. Not. IMRN*, 2014 (13) (2014), 3632–3691.

[25] Matiyasevich, Ju. V. «The Diophantineness of enumerable sets». *Dokl. Akad. Nauk SSSR*, 191 (2) (1970), 279–282. [En rus]

[26] Mazur, B. «Modular curves and the Eisenstein ideal». Amb un apèndix de B. Mazur i M. Rapoport. *Inst. Hautes Études Sci. Publ. Math.*, 47 (1977), 33–186.

[27] Mok, C. P. «On a theorem of Bertolini-Darmon on the rationality of Stark-Heegner points over genus fields of real quadratic fields». *Trans. Amer. Math. Soc.*, 374 (2) (2021), 1391–1419.

[28] Mordell, L. J. «On the rational solutions of the indeterminate equations of the third and fourth degrees». *Proc. Cambridge Philos. Soc.*, 21 (1922/23), 179–192.

[29] Park, J.; Poonen, B.; Voight, J.; Wood, M. M. «A heuristic for boundedness of ranks of elliptic curves». *J. Eur. Math. Soc. (JEMS)*, 21 (9) (2019), 2859–2903.

[30] Poincaré, H. «Sur les propriétés arithmétiques des courbes algébriques». *J. Math. Pures Appl.*, 7 (3) (1901), 161–233.

[31] Quer, J. «La funció ζ de Riemann». *Butlletí de la Societat Catalana de Matemàtiques*, 22 (2) (2007), 197–228.

[32] Rotger, V.; Seveso, M. A. «$\mathcal{L}$-invariants and Darmon cycles attached to modular forms». *J. Eur. Math. Soc. (JEMS)*, 14 (6) (2012), 1955–1999.

[33] Sutherland, A. V. «Sato-Tate distributions in genus 1». `https://math.mit.edu/~drew/g1SatoTateDistributions.html`. [Consulta: 10 setembre 2024].

[34] Taylor, R. «Automorphy for some l-adic lifts of automorphic mod l Galois representations. II». *Publ. Math. Inst. Hautes Études Sci.*, 108 (2008), 183–239.

[35] Taylor, R.; Wiles, A. «Ring-theoretic properties of certain Hecke algebras». *Ann. of Math. (2)*, 141 (3) (1995), 553–572.

[36] Trifković, M. «Stark-Heegner points on elliptic curves defined over imaginary quadratic fields». *Duke Math. J.*, 135 (3) (2006), 415–453.

[37] Wiles, A. «Modular elliptic curves and Fermat's last theorem». *Ann. of Math. (2)*, 141 (3) (1995), 443–551.

[38] Wiles, A. «The Birch and Swinnerton-Dyer conjecture». A: *The Millennium Prize Problems*. Cambridge, MA; Clay Mathematics Institute, 2006, 31–41.

Xavier Guitart
Departament de Matemàtiques i Informàtica
Universitat de Barcelona
`xevi.guitart@gmail.com`

Marc Masdeu
Departament de Matemàtiques
Universitat Autònoma de Barcelona
`marc.masdeu@uab.cat`