LES CONTRIBUCIONS DE POINCARÉ A L'ARITMÈTICA

PILAR BAYER

Índex

Date: 17 de gener de 2005.
Partially supported by MCYT BFM2003-01898.

INTRODUCCIÓ

Desitjo felicitar la Facultat de Matemàtiques i Estadística de la Universitat Politècnica de Catalunya per la iniciativa de commemorar el 150è aniversari del naixement d'Henri Poicaré, i agrair la invitació del professor Sebastià Xambó per participar en la jornada en honor d'aquest científic, permanentment vinculat a la universitat i a l'escola politècnica.

0.1. **Perfil biogràfic de Poincaré.** Jules Henri Poincaré (1854-1912) naixé a Nancy en el si d'una família benestant. El seu pare, Léon Poincaré, era metge i professor de la Facultat de Medicina. Fins a l'edat de 8 anys, Poincaré fou educat per la seva mare, Eugénie Launois. La seva escolarització s'inicià al *Lycée Impérial* de Nancy. L'any 1873 ingressà l'*École Polytechnique*; l'any 1875 ho feu a l'*École National Supérieure des Mines*, on hi cursà els seus estudis d'enginyer. En finalitzar-los, viatjà per Àustria-Hongria, Suècia i Noruega.

El mes de març de 1879 Poincaré fou nomenat enginyer de mines a la ciutat de Vesoul; el mes d'agost assolí el grau de Doctor en Ciències Matemàtiques per la Universitat de París, sota la direcció de Charles Hermite (1822-1901); el mes de desembre del mateix any obtingué el càrrec de professor *Chargé du Cours d'Analyse* a la Facultat de Ciències de la Universitat de Caen.

Quan comptava 27 anys, Poincaré es casà amb Louise Poulain d'Andecy. La família fixà la seva residència a París, i del matrimoni naixeren tres filles i un fill.

L'any 1881 Poincaré obtingué la plaça de *Maître de Conférences d'Analyse* a la Facultat de Ciències de la Universitat de París. Més endavant compaginaria la docència a la *Sorbonne* amb la docència a l'*École Polytechnique*. L'any 1887 ingressà a l'*Académie de Sciences*; i l'any 1908 ho feu a l'*Académie française*.

En el decurs de la seva vida acadèmica, Poincaré fou nomenat professor de física i mecànica experimental, física matemàtica i teoria de la probabilitat, astronomia i mecànica celest, i electricitat teòrica. L'amplitud del seu coneixement es reflecteix en la diversitat de temes que componen la seva recerca. L'obra matemàtica de Poincaré fou editada entre 1916 i 1956 per Gauthier-Villars, i ocupa un total d'onze volums (cf. [Poincaré, *Oeuvres*]).

A més de les publicacions matemàtiques, Poincaré també ens llegà una part significativa de les seves reflexions sobre filosofia de la ciència. Els opuscles *La Science et l'Hypothèse* (1902), *Science et Méthode* (1905), *La Valeur de la Science* (1908) i *Dernières pensées* (1913) (aquest en edició pòstuma) gaudiren d'una popularitat que ultrapassà l'àmbit estrictament matemàtic per esdevenir obres de referència en l'estudi del pensament científic. Poincaré fou alhora un matemàtic, un enginyer i un filòsof.

0.2. **Els treballs aritmètics.** El caràcter polièdric de l'obra de Poincaré permet el seu estudi des de vessants diferents. El nostre propòsit és posar de manifest la seva influència en l'aritmètica.

Poincaré opinava que la seva aportació a l'aritmètica es reduïa gairebé en exclusiva a la teoria de formes:

> *Mes recherches arithmétiques ont presque exclusivement porté sur la théorie des formes.*
>
> Poincaré [*Oeuvres*, t. V, p. 6].

Els treballs de Poincaré específicament aritmètics s'aplegaren en el volum V de les *Oeuvres.* En una vintena d'articles, Poincaré estudia les formes quadràtiques binàries, ternàries i quaternàries; precisa la noció de gènere; defineix grups fuchsians associats a formes quadràtiques ternàries; tracta les fraccions contínues; i inicia un estudi de formes cúbiques, ternàries i quaternàries. El volum V conté també un important treball sobre l'aritmètica de corbes algebraiques.

Altres contribucions de Poincaré, recopilades majoritàriament en els volums d'anàlisi, formen part de les arrels de l'aritmètica d'avui. Destaquem en aquest sentit les següents:

ŒUVRES, Tome II: Analyse pure. Conté l'estudi de funcions fuchsianes, grups fuchsians, grups kleinians i funcions thetafuchsianes.

ŒUVRES, Tome III: Analyse pure. Conté la integració algebraica d'equacions diferencials, integrals abelianes, i grups continus de transformacions.

ŒUVRES, Tome IV: Analyse pure. Théorie des fonctions. Conté la uniformització de funcions analítiques, la teoria del potencial i funcions abelianes, i funcions theta.

ŒUVRES, Tome V: Algèbre et Arithmétique. Conté l'estudi d'invariants aritmètics, grups fuchsians, substitucions automorfes de formes quadràtiques, funcions fuchsianes associades, el teorema d'addició, i l'aritmètica de corbes algebraiques.

ŒUVRES, Tome XI: Mémoires divers. Conté part de la correspondència matemàtica de Poincaré.

El procés de lectura dels clàssics és ple d'entrebancs. Per facilitar-lo, és bo proveir-se d'un petit diccionari de butxaca que n'actualitzi la terminologia. Esmentem, a tall d'exemple, que l'equivalent del terme *faisceau* de Poincaré és el nostre grup abelià. Quan Poincaré parla de *nombres quelconques* es refereix a nombres complexos. Un *groupe de substitutions linéaires* és un subgrup del grup lineal $\mathrm{GL}(n, \mathbb{C})$. Un *groupe continu de substitutions linéaires* és un subgrup de $\mathrm{GL}(n, \mathbb{R})$. Quan Poincaré esmenta els *invariants algébriques* es refereix a objectes invariants per l'acció de subgrups de $\mathrm{GL}(n, \mathbb{C})$; els *invariants arithmétiques* ho són respecte de subgrups discrets de $\mathrm{GL}(n, \mathbb{R})$. Un *groupe de substitutions semblables des formes quadratiques* és un grup d'isotropia de formes quadràtiques. Un *système de nombres complexos* és una àlgebra finitament generada. Sovint, Poincaré designa les matrius com *quadres de coeficients*. Les *fonctions fuchsiennes* de Poincaré corresponen a les avui anomenades funcions automorfes; les *fonctions thétafuchsiennes* han esdevingut les formes automorfes.

Per tal de no perdre el referent històric, en aquest escrit emprarem la terminologia de Poincaré, però en facilitarem la seva traducció quan ho creguem necessari.

1. FORMES QUADRÀTIQUES I GRUPS FUCHSIANS

1.1. **Formes quadràtiques binàries.** L'estudi de la representació dels enters per formes quadràtiques fou emprès per Gauss (1777-1855) en les *Disquisitiones arithmeticae* [Ga1801]. En aquesta obra de joventut, Gauss se centrà especialment en el cas binari. Prosseguint una recerca iniciada per Fermat (1601-1665), Euler (1707-1783) i Legendre (1752-1833), Gauss s'ocupa de l'estudi de les solucions enteres de les equacions $aX^2 + 2bXY + cY^2 = m$, on $a, b, c, m \in \mathbb{Z}$. La forma binària $f(X, Y) = aX^2 + 2bXY + cY^2$ és denotada per (a, b, c); quan $\mathrm{mcd}(a, b, c) = 1$, la forma rep el nom de primitiva.

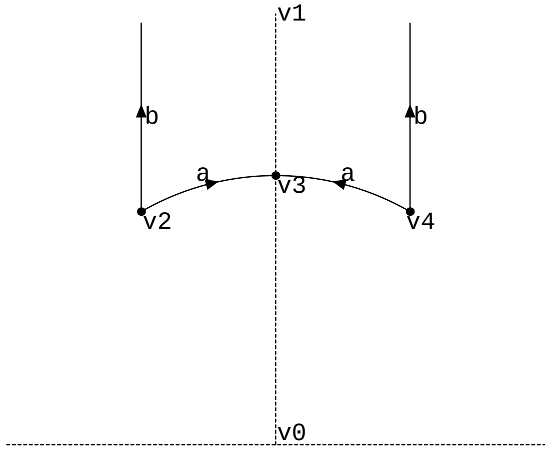

FIGURA 1. El domini fonamental $\mathcal{F}(\mathrm{SL}(2,\mathbb{Z}))$

Per delimitar i resoldre el problema, Gauss utilitza de manera implícita grups, accions de grups en conjunts, relacions d'equivalència, estructures quocient, grups cíclics, grups abelians finits, caràcters de grau 1, etc., anticipant-se uns quants anys a la formalització del càlcul matricial i de la teoria de grups.

Gauss classifica les formes i les representacions dels enters per formes mitjançant canvis de coordenades

$$\begin{cases} X' &= \alpha X + \beta Y \\ \\ Y' &= \gamma X + \delta Y \,, \end{cases}$$

en els quals $\alpha, \beta, \gamma, \delta$ pertanyen a $\mathbb{Z}$ i $\alpha\delta - \beta\gamma = 1$. Per tant, els canvis són donats per matrius $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ del grup modular $\mathrm{SL}(2,\mathbb{Z})$.

En definir una llei de composició de classes de formes binàries, enteres, primitives, de discriminant $D = b^2 - ac$ donat, i definides positives (o bé indefinides), Gauss obté un grup, $H(D)$, que és abelià i finit. El seu ordre, $h(D)$, és l'anomenat nombre de classes.

Gauss distribueix les classes de formes en gèneres, que defineix per mitjà de caràcters. Els gèneres proporcionen una partició del grup $H(D)$ equivalent a la consideració del grup quocient $H(D)/H(D)^2$. El nombre de gèneres és determinat per Gauss i facilita una primera informació sobre $h(D)$, quantitat molt més inassequible a mesura que D creix.

El grup especial lineal $\mathrm{SL}(2,\mathbb{R})$ opera transitivament per mitjà de transformacions lineals fraccionàries $z \mapsto \dfrac{az+b}{cz+d}$ en el semiplà superior complex

$$\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}.$$

L'acció factoritza a través del grup $\mathrm{PSL}(2,\mathbb{R}) = \mathrm{SL}(2,\mathbb{R})/\{\pm 1_2\}$. El grup de les rotacions $\mathrm{SO}(2)$ és el grup d'isotropia de la unitat imaginària, i, per la qual cosa

$$\mathrm{SO}(2)\backslash\mathrm{SL}(2,\mathbb{R}) \xrightarrow{\sim} \mathcal{H}.$$

El grup $\mathrm{SL}(2,\mathbb{Z})$ és un subgrup discret de $\mathrm{SL}(2,\mathbb{R})$ i, com a tal, opera en $\mathcal{H}$. La figura 1 mostra un domini fonamental $\mathcal{F} = \mathcal{F}(\mathrm{SL}(2,\mathbb{Z}))$ per a aquesta acció. És format a partir de la unió del triangle hiperbòlic de vèrtexs $v_1 = \infty$, $v_2 = \exp(2\pi i/3)$, $v_3 = i$, i el seu simètric respecte l'eix imaginari. A fi que cada punt de $\mathcal{H}$ tingui un representant únic en $\mathcal{F}$, cal identificar dos a dos els costats dels triangles: $[v_2, v_1] \sim [v_4, v_1]$, $[v_2, v_3] \sim [v_4, v_3]$, tal com s'indica a la figura. La identificació d'aquests costats es realitza per mitjà de la translació T i de la simetria S, definides per

$$T : z \mapsto z+1, \qquad S : z \mapsto -\frac{1}{z}.$$

Observem que S i T proporcionen un sistema de generadors del grup $\mathrm{PSL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})/\{\pm 1_2\}$.

Donat un discriminant $D < 0$, cada forma $f = (a,b,c)$ definida positiva ($a > 0$) determina un punt $z(f)$ de $\mathcal{H}$, igual al zero de part imaginària positiva del polinomi $f(X,1)$,

$$z(f) = \frac{-b+\sqrt{D}}{a}.$$

Gauss representa les classes de $H(D)$ per mitjà de formes reduïdes, en les quals el zero $z(f)$ és un punt de $\mathcal{F}$. Quan $z(f)$ és un punt de l'interior de $\mathcal{F}$, la classe de f conté una única forma reduïda. Quan $z(f)$ és un punt de la frontera de $\mathcal{F}$, la classe de f conté dues formes reduïdes, els zeros de les quals s'identifiquen d'acord amb la figura 1. Per tant, cada discriminant D aïlla un total de $h(D)$ punts de $\mathcal{F}$, no equivalents sota l'acció de $\mathrm{SL}(2,\mathbb{Z})$.

Les recerques de Gauss sobre les formes foren continuades de manera immediata per Dirichlet (1805-1859), Eisenstein (1823-1852), Dedekind (1831-1916) i Hermite (1822-1901). Més tard, ho serien per Poincaré.

1.2. **Grups fuchsians aritmètics.** Per la seva pròpia complexitat, les recerques de Poincaré sobre les formes no constitueixen una teoria autocontinguda, com fou la de Gauss en el seu moment, però són un referent per comprendre treballs posteriors, deguts bàsicament a Minkowski (1864-1909), Brandt (1886-1954), Hecke (1887-1947) i Siegel (1896-1981).

En reflexionar sobre la definició escaient de gènere, Poincaré conclou que dues formes quadràtiques de coeficients enters pertanyen al mateix gènere si, i només si, són equivalents mòdul n, per a tot n. Aquest punt de vista resultà del tot encertat. Els anys 1920, la teoria del gènere quedaria clarificada amb la introducció per part de Hensel (1861-1941) dels nombres p-àdics i amb la noció d'equivalència en tots els anells d'enters p-àdics com a definidora del gènere. Una cèlebre fórmula obtinguda per Siegel expressa el nombre de representacions d'un enter per un gènere de formes en termes de densitats p-àdiques. La fórmula de Siegel clarifica el paper dels gèneres en l'estudi de les formes quadràtiques de coeficients enters i d'un nombre de variables qualsevol.

Tal com hem dit més amunt, Poincaré emprengué l'estudi de formes de grau superior. Procedí a una classificació de formes cúbiques ternàries i cercà les formes cúbiques ternàries i les formes cúbiques quaternàries invariants ja per una transformació lineal donada ja per un grup abelià de transformacions. L'estudi d'aquestes formes el conduí a la consideració de grups de transformacions del pla continguts en el grup multiplicatiu d'àlgebres no commutatives:

> [...] *Parmi les groupes continus dont je vient de parler, les plus intéressants sont ceux qui donnent naissance à un système de nombres complexes à multiplication non commutative* (*comme sont, par exemple les quaternions*).
>
> Poincaré [*Oeuvres*, t. V, p. 2].

Tota forma quadràtica ternària, real i indefinida,

$$F(X,Y,Z) = aX^2+bY^2+cZ^2+dYZ+eXZ+fXY, \quad a,b,c,d,e,f \in \mathbb{R},$$

és equivalent sota l'acció de $\mathrm{SL}(3,\mathbb{R})$ a la forma $Y^2 - XZ$, o bé a la seva oposada. Poincaré prova que el grup d'isotropia d'aquesta forma consta de les transformacions

$$S = \begin{bmatrix} \alpha^2 & -2\alpha\beta & \beta^2 \\ -\alpha\gamma & \alpha\delta+\beta\gamma & -\beta\delta \\ \gamma^2 & -2\gamma\delta & \delta^2 \end{bmatrix},$$

on $\alpha, \beta, \gamma, \delta$ pertanyen a $\mathbb{R}$ i $\alpha\delta - \beta\gamma = 1$. Quan els coeficients de la forma F són nombres enters, Poincaré s'interessa per les matrius de coeficients enters del grup d'isotropia. En considerar les matrius $s = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ que en resulten, obté un subgrup discret $\Gamma(F)$ de $\mathrm{SL}(2, \mathbb{R})$, associat a un objecte aritmètic.

En molts treballs de Poincaré s'aprecia la seva gran competència en geometria hiperbòlica, tot just desenvolupada arran de les investigacions de Gauss (1744-1855), Bolyai (1775-1856) i Lobatxevski (1793-1856).

Recordem que la distància hiperbòlica $\rho(z_1, z_2)$ entre dos punts z_1, z_2 de $\mathcal{H}$ es defineix per

$$\cosh \rho(z_1, z_2) = 1 + \frac{|z_1 - z_2|^2}{2 \operatorname{Im}(z_1) \operatorname{Im}(z_2)}.$$

En termes de la mesura de Lebesgue, la mesura hiperbòlica de $\mathcal{H}$ és donada per

$$d\mu z = \frac{dx\, dy}{y^2}.$$

El semiplà superior dotat de la distància hiperbòlica és un model del pla hiperbòlic. El grup projectiu especial $\mathrm{PSL}(2, \mathbb{R})$ en proporciona el grup de tots els moviments hiperbòlics directes. En molts textos, $\mathcal{H}$ rep el nom de semiplà de Poincaré.

Poincaré elaborarà una teoria general de grups discrets de transformacions, anomenant fuchsians els subgrups discrets Γ de $\mathrm{SL}(2, \mathbb{R})$. Els subgrups discrets de $\mathrm{SL}(2, \mathbb{R})$ coincideixen amb els subgrups discontinus d'aquest grup, els quals es caracteritzen pel fet que cap òrbita Γz, $z \in \mathcal{H}$, no conté punts d'acumulació en $\mathcal{H}$.

L'acció de qualsevol grup fuchsià Γ en $\mathcal{H}$ determina dominis fonamentals $\mathcal{F} = \mathcal{F}(\Gamma)$. Com en el cas del grup modular, els costats dels dominis són semirectes perpendiculars a l'eix real o arcs de circumferència de centre en $\mathbb{R}$. Es tracta, doncs, de polígons hiperbòlics. El càlcul d'un domini fonamental és equivalent al càlcul d'un sistema de generadors de Γ, els elements del qual identificaran dos a dos els costats del polígon. En desplaçar $\mathcal{F}$ segons tots els moviments de Γ, s'obté un mosaic de $\mathcal{H}$. De manera equivalent, el mosaic pot visualitzar-se a l'interior del disc unitat, en fixar prèviament un isomorfisme analític de l'interior del disc en $\mathcal{H}$.

En certa manera, els grups fuchsians són al pla hiperbòlic el que els grups cristal·logràfics són al pla euclidià. La diferència, però, és notable: la finitud del nombre de classes d'isomorfia de mosaics euclidians es contraposa a l'infinitud del nombre de classes d'isomorfia de mosaics hiperbòlics.

Poincaré expressa el seu convenciment que les formes quadràtiques, incloses les binàries, s'haurien de classificar per altres grups discrets, a més dels lineals habituals.

1.3. **Invariants aritmètics.** En un article escrit en memòria de Dirichlet, que titula *Sur les invariants arithmétiques* [*Oeuvres*, t. V, p. 203], Poincaré associa a una forma quadràtica binària (a, b, c), definida positiva, l'invariant aritmètic

$$F(q) := \sum_{x,y\in\mathbb{Z}} q^{ax^2+2bxy+cy^2}, \text{ on } \quad q(t) := e^{-t}.$$

En escriure

$$2\,(aX^2 + 2bXY + cY^2) = (\alpha X + \gamma Y)^2 + (\beta X + \delta Y)^2,\ \alpha\delta - \beta\gamma = E,$$

obté que $b^2 - ac = -\dfrac{1}{4}E^2$. Quan la forma és de coeficients enters, la funció

$$\Phi(u) := F(e^{-2\pi i u}), \quad t = 2\pi i u,$$

satisfà les igualtats

$$\Phi(u+1) = \Phi(u), \quad \Phi(u) = -\frac{i}{Eu}\Phi\left(-\frac{1}{E^2u}\right).$$

Les fórmules anteriors posen de manifest que $\Phi^2(u)$ és una funció quasiperiòdica respecte del grup generat per les transformacions

$$u \mapsto u+1, \quad u \mapsto -\frac{1}{E^2u},$$

(cf. Secció 2.5). En un fragment de l'article esmentat, Poincaré creu que els grups fuchsians haurien de proporcionar informació aritmètica sobre les formes quadràtiques:

> *L'étude de ce groupe fuchsien jetterait sans doute quelque lumière sur les propriétés arithmétiques des formes quadratiques.*
>
> Poincaré [*Oeuvres*, t. V, p. 238].

L'estudi de la representació d'enters per formes conduí Poincaré vers la representació geomètrica dels nombres enters algebraics. Per comprendre la divisibilitat d'aquests nombres, utilitzà xarxes de $\mathbb{R}^n$. En contribucions diferents, Poincaré deixà constància dels seus intents per familiaritzar-se amb l'aritmètica dels anells d'enters dels cossos de nombres, d'acord amb la teoria desenvolupada per Dedekind a partir del 1871.

En un altre ordre d'idees, Poincaré també es preocupà d'estendre el teorema de Txebixev (1821-1894) sobre la densitat dels nombres primers en el conjunt de tots els nombres naturals. L'any 1891 demostrà un teorema similar, però formulat en l'anell $\mathbb{Z}[i]$ dels enters de Gauss (cf. [Poi1891]). El resultat obtingut li permeté comparar la densitat dels nombres primers congrus amb 1 mòdul 4 amb la dels congrus amb 3 mòdul 4, en el conjunt de tots els nombres primers. A banda del teorema dels nombre primers, la llei que regeix la distribució dels ideals primers en un cos de nombres galoisià qualsevol havia estat conjecturada l'any 1880 per Frobenius (1849-1917), en un article que no es publicà fins l'any 1896. El teorema de densitat corresponent seria demostrat per Txebotarev (1894-1947) l'any 1922 i, amb el temps, esdevindria una de les eines més potents proporcionada per la teoria global de cossos de classes.

2. FUNCIONS FUCHSIANES

2.1. **Les funcions circulars.** Com és ben sabut, les funcions circulars sinus i cosinus són funcions enteres que satisfan les relacions de periodicitat

$$\sin(z+2\pi) = \sin(z), \quad \cos(z+2\pi) = \cos(z), \quad \text{per a tot } z \in \mathbb{C}.$$

Les funcions circulars poden definir-se per mitjà de la inversió d'integrals:

$$z = \int_0^{\sin(z)} \frac{dt}{\sqrt{1-t^2}}.$$

Els seus períodes, $\Lambda = 2\pi\mathbb{Z}$, són un $\mathbb{Z}$-mòdul lliure de rang 1. En considerar els zeros d'aquestes funcions, Euler (1707-1783) n'obtingué el seu desenvolupament en forma de producte infinit:

$$\sin(z) = z\prod_{n\geq 1}\left(1-\frac{z^2}{\pi^2 n^2}\right), \quad \cos(z) = \prod_{n\geq 1}\left(1-\frac{4z^2}{\pi^2(2n-1)^2}\right).$$

Si ara tenim en compte que

$$\cos^2(z) + \sin^2(z) = 1,$$

veiem que entre el sinus i el cosinus se satisfà una relació algebraica. Notem que el cosinus és un traslladat del sinus per una fracció del període:

$$\cos(z) = \sin\left(z + \frac{\pi}{2}\right).$$

La relació algebraica anterior posa de manifest que les funcions sinus i cosinus proporcionen un sistema de funcions coordenades de la circumferència unitat:

$$X^2 + Y^2 = 1.$$

Veurem més endavant que altres corbes algebraiques i altres varietats algebraiques admeten uniformitzacions per funcions especials. Quan això és així, la recerca en aquestes varietats de punts amb propietats diofantines específiques pot beneficiar-se de l'estudi de valors especials de les seves funcions coordenades. En aquest sentit, fixem-nos que els vèrtexs dels polígons regulars són nombres algebraics que s'obtenen en avaluar les funcions sinus i cosinus en els punts de divisió del període.

2.2. **Funcions el·líptiques.** S'anomenen el·líptiques les funcions complexes d'una variable meromorfes i doblement periòdiques. El seu estudi es remunta a Fagnano (1682-1766), Euler (1707-1783), Legendre (1752-1833), Gauss (1777-1855), Abel (1802-1829), Jacobi (1804-1851), Weierstrass (1815-1897) i Klein (1849-1925).

Les funcions el·líptiques san, can, dan s'obtenen per inversió d'integrals el·líptiques:

$$\begin{aligned}
x &= \int_0^{\mathrm{sn}(x,k)} \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}, \\
x &= \int_{\mathrm{cn}(x,k)}^1 \frac{dt}{\sqrt{(1-t^2)(k'^2-k^2t^2)}}, \\
x &= \int_{\mathrm{dn}(x,k)}^1 \frac{dt}{\sqrt{(1-t^2)(t^2-k'^2)}}.
\end{aligned}$$

Foren estudiades per Jacobi (cf. [Ja1829]). Els paràmetres k i k' designen el mòdul i el mòdul complementari, respectivament. Se satisfà que $k^2 + k'^2 = 1$.

La funció theta bàsica es defineix per

$$\vartheta(z,\tau) := \sum_{n\in\mathbb{Z}} \exp(2\pi i n z + \pi i n^2 \tau), \quad z \in \mathbb{C},\ \tau \in \mathcal{H}.$$

Es tracta d'una funció analítica en les dues variables que és quasiperiòdica en la primera variable:

$$\vartheta(z+1,\tau) = \vartheta(z,\tau), \quad \vartheta(z+\tau,\tau) = e^{-\pi i\tau - 2\pi i z}\vartheta(z,\tau).$$

La funció ϑ admet el desenvolupament en producte infinit:

$$\vartheta(z) = \prod_{n=1}^{\infty}(1-q^{2n})(1-q^{2n-1}p^2)(1-q^{2n-1}p^{-2}),$$

on $p := e^{\pi i z}$, $q := e^{\pi i \tau}$.

Un precedent de la funció ϑ es troba en l'estudi que realitzà Fourier de l'equació de la calor (cf. [Fou1822]). Notem que la lletra ϑ és la inicial de $\vartheta\varepsilon\varrho\mu o\tau\eta\varsigma$, substantiu grec que significa calor; l'adjectiu $\vartheta\varepsilon\varrho\mu o\varsigma$ significa calent. L'arrel grega *thermo* és present en paraules com termodinàmica, termòmetre, etc.

Les funcions theta de Jacobi, $\vartheta_i(z,\tau)$, són funcions analítiques en les dues variables que es defineixen a partir de la funció theta bàsica. En particular es té que $\vartheta_3 = \vartheta$.

En tenir en compte els zeros i els pols de les funcions san, can, dan, Jacobi n'obtingué expressions en forma de quocients de productes infinits, donats per funcions theta:

$$\mathrm{sn}(x,k) = \frac{\vartheta_3(0)}{\vartheta_2(0)}\cdot\frac{\vartheta_1(z)}{\vartheta_4(z)}, \quad \mathrm{cn}(x,k) = \frac{\vartheta_4(0)}{\vartheta_2(0)}\cdot\frac{\vartheta_2(z)}{\vartheta_4(z)},$$

$$\mathrm{dn}(x,k) = \frac{\vartheta_4(0)}{\vartheta_3(0)}\cdot\frac{\vartheta_3(z)}{\vartheta_4(z)},$$

on

$$z = \frac{x}{\pi\vartheta_3^2(0)}, \quad k^2 = \frac{\vartheta_2^4(0)}{\vartheta_3^4(0)}, \quad \vartheta_i(z) = \vartheta_i(z,\tau),$$

per a $\tau = iK'/K$, essent $4K$, $2iK'$ els períodes de la funció $\mathrm{sn}(x,k)$.

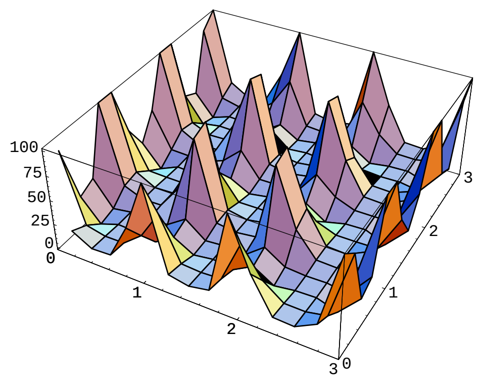

FIGURA 2. Una funció $|\wp|$ de Weierstrass, doblement periòdica

Sigui $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ un $\mathbb{Z}$-mòdul lliure de rang 2, $\lambda_i \in \mathbb{C}$. El conjunt de totes les funcions el·líptiques de xarxa de períodes Λ constitueix un cos, que denotem per $\mathbb{C}(\Lambda)$.

Les funcions de Weierstrass:

$$\wp(z,\Lambda) := \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right), \quad \wp'(z,\Lambda) = -2\sum_{\lambda\in\Lambda} \frac{1}{(z-\lambda)^3}$$

proporcionen un sistema de generadors del cos $\mathbb{C}(\Lambda)$; és a dir, tota funció Λ-periòdica s'expressa racionalment en funció de $\wp, \wp'$:

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Entre una funció $\wp$ i la seva derivada $\wp'$ se satisfà una relació algebraica:

$$\wp'^2(z) = 4\wp^3(z) - g_2\,\wp(z) - g_3, \quad \Delta := g_2^3 - 27g_3^2 \neq 0,$$

que posa de manifest que el grau de transcendència del cos $\mathbb{C}(\Lambda)$ és igual a 1. Les funcions de Weierstrass uniformitzen doncs una corba el·líptica, d'equació

$$Y^2 = 4X^3 - g_2X - g_3.$$

Aquí Δ denota el discriminant del polinomi de tercer grau $4X^3 - g_2X - g_3$. Els coeficients g_2, g_3 s'obtenen a partir de les sèries d'Eisenstein de pesos 4 i 6, respectivament, avaluades en la xarxa de períodes:

$$g_2(\Lambda) = 60 \sum_{\lambda\in\Lambda\setminus\{0\}} \lambda^{-4}, \quad g_3(\Lambda) = 140 \sum_{\lambda\in\Lambda\setminus\{0\}} \lambda^{-6}.$$

El problema de la uniformització euclidiana de les corbes el·líptiques consisteix en saber si tota corba el·líptica complexa

$$Y^2 = 4X^3 - AX - B, \quad A^3 - 27B^2 \neq 0,$$

admet una uniformització per funcions de Weierstrass. La resposta és afirmativa. La demostració d'aquest fet s'obté a partir de propietats de la funció modular el·líptica, que veurem a continuació.

2.3. **Funcions modulars.** S'anomenen modulars les funcions meromofes de $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ que són periòdiques respecte d'un subgrup discret Γ de $\mathrm{SL}(2,\mathbb{Z})$. Són molt diferents de les funcions el·líptiques que acabem de considerar en la mesura que les funcions el·líptiques són periòdiques respecte de subgrups discrets de moviments euclidans i les funcions modulars ho són respecte de subgrups discrets de moviments hiperbòlics.

La funció j és la funció modular bàsica. Els seus orígens es remunten a Dedekind i a Klein. Es tracta d'una funció meromorfa en $\mathcal{H}$ amb un únic pol, simple i de residu igual a 1, situat a l'infinit. A l'entorn de l'infinit, la funció j és desenvolupable en sèrie de Fourier:

$$\begin{aligned} j(z) &= \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 \\ &\quad +20245856256q^4 + 333202640600q^5 + \mathrm{O}(q^6), \end{aligned}$$

on $q(z) := e^{2\pi i z}$, $z \in \mathcal{H}$. Notem que els coeficients de Fourier de j són nombres enters.

Les relacions satisfetes per aquesta funció,

$$j(z+1) = j(z), \quad j(-1/z) = j(z),$$

posen de manifest la seva periodicitat respecte de tot el grup modular:

$$j(\gamma(z)) = j(z), \quad \text{per a tot } \gamma \in \mathrm{SL}(2, \mathbb{Z}).$$

En particular, la funció j queda determinada pels seus valors en el domini fonamental $\mathcal{F}(\mathrm{SL}(2,\mathbb{Z}))$ que hem trobat en l'estudi de les formes quadràtiques binàries, enteres i definides positives (cf. figura 1). La funció j proporciona un isomorfisme analític

$$j : \mathrm{SL}(2,\mathbb{Z})\backslash\mathcal{H}^* \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

A més, aquesta funció és un generador del cos de totes les funcions invariants per $\mathrm{SL}(2,\mathbb{Z})$:

$$\mathbb{C}(\mathrm{SL}(2,\mathbb{Z})) = \mathbb{C}(j).$$

Per la seva relació amb les integrals el·líptiques, la funció j es coneix amb el nom de funció modular el·líptica. La relació s'obté en assignar a cada punt $z \in \mathcal{H}$ la classe d'isomorfia de la corba el·líptica E_z de xarxa de períodes $\langle 1, z\rangle$. Aleshores,

$$\begin{array}{ccc} \mathbb{C}/\langle 1, z\rangle & \xrightarrow{\sim} & E_z(\mathbb{C}) \\ u & \mapsto & (\wp(u), \wp'(u), 1), \\ 0 & \mapsto & (0,1,0), \end{array}$$

i el valor $j(z)$ és l'invariant de la classe d'isomorfia de E_z donat per

$$j(z) = \frac{g_2^3(z)}{\Delta(z)}.$$

La igualtat anterior, unida a les propietats de la funció j, permet demostrar que tota corba el·líptica complexa E és uniformitzable per mitjà de funcions el·líptiques. La xarxa Λ s'obté a partir dels períodes de les integrals el·líptiques associades a l'equació algebraica de la corba. L'isomorfisme que en resulta

$$(\wp, \wp') : \mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$$

és un isomorfisme de grups abelians: els arguments el·líptics se sumen per la llei d'addició quocient i els punts de la corba se sumen mitjançant el mètode de la tangent i de la secant, familiar a Euler i a Fermat.

Considerem el subgrup de congruència de nivell N:

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : c \equiv 0 \pmod N \right\}.$$

La funció $j_N(z) := j(Nz)$ és invariant per $\Gamma_0(N)$. Entre les funcions j i j_N se satisfà una relació algebraica:

$$\Phi_N(j, j_N) = 0,$$

coneguda pels clàssics amb el nom d'equació modular. El polinomi $\Phi_N(X, Y)$ és de coeficients enters. Les funcions j, j_N constitueixen un sistema de generadors del cos de totes les funcions modulars per a $\Gamma_0(N)$:

$$\mathbb{C}(\Gamma_0(N)) = \mathbb{C}(j, j_N).$$

El grup $\Gamma_0(N)$ conté transformacions parabòliques (translacions), la qual cosa comporta que les funcions de $\mathbb{C}(\Gamma_0(N))$ siguin desenvolupables en sèrie de Fourier a l'entorn de les puntes d'un domini fonamental $\mathcal{F}(\Gamma_0(N))$.

A poc a poc, l'estudi del grup modular i dels seus subgrups de congruència derivà cap a l'estudi de les anomenades corbes modulars. Sobresurten les corbes modulars $X_0(N), X_1(N), X(N)$, definides per diferents subgrups de congruència de nivell N. En particular, l'equació modular clàssica

$$\Phi_N(X, Y) = 0$$

proporciona un model afí de la corba modular $X_0(N)$, de nivell N. El lligam de l'invariant j amb les corbes el·líptiques permet interpretar les corbes modulars com a espais de moduli de corbes el·líptiques dotades d'estructures de nivell. Aquesta interpretació és especialment útil a l'hora d'estudiar propietats diofantines d'aquestes corbes.

Des del punt de vista aritmètic, la funció j gaudeix de propietats remarcables. Els valors $j(z(f))$, obtinguts en avaluar-la en els zeros de les formes quadràtiques binàries, enteres i definides positives, són enters algebraics. Les corbes el·líptiques $E_{z(f)}$ posseeixen més endomorfismes que els habituals, degut a multiplicacions complexes que operen en les xarxes $\langle 1, z(f) \rangle$. Les classes d'isomorfia de les corbes el·líptiques amb multiplicació complexa contenen models de Weierstrass de coeficients algebraics.

Les funcions modulars havien estat estudiades per Kronecker (1823-1891), Weber (1842-1913), Klein (1849-1925) i Fricke (1861-1930). Convé fer notar que Hermite havia aconseguit la resolució de l'equació de grau 5 mitjançant funcions modulars.

Les funcions modulars constitueixen un precedent de les funcions fuchsianes estudiades per Poincaré.

2.4. **Equacions diferencials fuchsianes.** En els treballs [Fu1866] i [Fu1876], Fuchs (1833-1902) estudia equacions diferencials ordinàries, lineals, homogènies i de coeficients variables

$$\frac{d^n w}{dz^n} + p_1(z)\frac{d^{n-1}w}{dz^{n-1}} + \dots p_{n-1}(z)\frac{dw}{dz} + p_n(z)w = 0.$$

Suposa que les funcions $p_i(z)$ són meromorfes en una regió T simplement connexa del pla complex. D'acord amb Weierstrass, el seu mestre, Fuchs anomena punts singulars de l'equació diferencial els pols dels coeficients:

> *Diejenigen Punkte innerhalb T, für welche eine oder mehrere der Functionen p unstetig sind, werden wir im Folgenden, nach dem Vorgange von Weierstrass, singuläre Punkte nennen.*
>
> Fuchs [Fu1866].

Per simplificar l'exposició, centrem-nos en les equacions diferencials de segon ordre:

$$\frac{d^2w}{dz^2} + p(z)\,\frac{dw}{dz} + q(z)\,w = 0.$$

Suposem que $z = 0$ és un punt singular de l'equació diferencial. Fuchs considera un camí tancat amb base en un punt no singular $z_0 \in T$,

$$\gamma : [0,1] \to T, \quad \gamma(0) = \gamma(1) = z_0,$$

i que encercla l'origen, $z = 0$, exactament una vegada. Seguint un procediment habitual en Riemann, estudia el comportament d'un sistema fonamental de solucions de l'equació diferencial, $\{w_1, w_2\}$, en ser perllongat analíticament al llarg de γ. La transformació, dita de monodromia,

$$\begin{cases} v_1(z) = a_{11}w_1(z) + a_{12}w_2(z) \\ v_2(z) = a_{21}w_1(z) + a_{22}w_2(z), \end{cases}$$

té cura d'aquest comportament. A partir de la matriu de monodromia A associada al sistema, obté l'equació característica

$$\det(A - \sigma \mathrm{I}_2) = 0.$$

Anomena nombres característics les arrels σ_1, σ_2 de l'equació anterior. Fuchs considera els nombres ρ_1, ρ_2 definits per les igualtats $e^{2\pi i \rho_i} = \sigma_i$, per a $i = 1, 2$. Per obtenir la forma general de les solucions de l'equació diferencial, distingeix dos casos:

Cas 1: $\sigma_1 \neq \sigma_2$. Aleshores, $\rho_1 - \rho_2 \notin \mathbb{Z}$, i existeix un sistema fonamental de solucions tal que:

$$w_1(z) = z^{\rho_1}\varphi_1(z), \quad w_2(z) = z^{\rho_2}\varphi_2(z).$$

Cas 2: $\sigma_1 = \sigma_2$. Aleshores existeix un sistema fonamental de solucions tal que:

$$w_1(z) = z^{\rho}\varphi_1(z), \quad w_2(z) = z^{\rho}\varphi_1(z)\log z + z^{\rho}\varphi_2(z),$$

on $\sigma = \sigma_i$, $e^{2\pi i \rho} = \sigma$.

Suposem que, com a molt, p té un pol simple i q té un pol doble en $z = 0$:

$$p(z) = \sum_{n \geq -1}^{\infty} p_n z^n, \quad q(z) = \sum_{n \geq -2}^{\infty} q_n z^n.$$

Aleshores les funcions φ_i del sistema fonamental no presenten cap singularitat essencial a l'origen. En aquest cas, el punt $z = 0$ s'anomena un punt singular regular de l'equació diferencial.

Es diu que una equació diferencial lineal és de tipus fuchsià quan totes les seves singularitats són punts singulars regulars.

La paraula *monodromia* deriva del substantiu grec $\delta\varrho o\mu o\varsigma$, que significa volta de passeig o cursa (recordi's hipòdrom, canòdrom, etc.). Fixem-nos que la monodromia proporciona una representació lineal del grup fonamental de l'espai que s'obté en llevar de T els punts singulars de l'equació diferencial.

A l'article [Fu1880], Fuchs introdueix una nova classe de funcions mitjançant la resolució d'un problema d'inversió similar al de Jacobi, però que parteix de les integrals de les solucions d'equacions diferencials lineals de coeficients funcions racionals. Fuchs, limitant-se al cas d'ordre 2, considera la funció $z(\zeta)$ que resulta en invertir el quocient

$$\zeta = \frac{f(z)}{\varphi(z)}$$

de dues solucions de l'equació diferencial donada.

Arran dels treballs d'Hermite sobre la resolució de la quíntica, Fuchs i Hermite es posaren en contacte. Els treballs de Fuchs influirien en Jordan (1838-1921), Frobenius (1849-1917) i, tal com veurem, en el propi Poincaré.

2.5. **Funcions fuchsianes.** El 29 de maig de l'any 1880, Poincaré inicià una correspondència amb Fuchs, qüestionant-li alguns dels seus resultats. Poincaré desitjava caracteritzar quan el quocient

$$z = \frac{w_1(x)}{w_2(x)}$$

de dues solucions independents d'una equació diferencial de segon ordre

$$\frac{d^2w}{dx^2} - Qw = 0$$

definia, per inversió, una funció meromorfa $x(z)$. Per aquest camí, Poincaré arribaria a la seva descoberta particular de les funcions fuchsianes.

Considerant que les funcions periòdiques en el pla euclidià s'esgoten amb les funcions el·líptiques −d'acord amb un teorema degut a Kronecker−, Poincaré cercarà funcions periòdiques en el pla hiperbòlic, entenent aquest com a un mitjà molt més idoni per a la formulació dels seus resultats. Poincaré designa amb el nom de fuchsianes les funcions meromorfes en un disc (equivalentment en $\mathcal{H}$) amb periodicitats donades pels elements d'un grup fuchsià:

$$f(\gamma(z)) = f(z), \quad \text{per a tot } \gamma \in \Gamma.$$

Per a Poincaré, les funcions fuchsianes són a la geometria de Lobatxevski allò que les funcions doblement periòdiques són a la geometria d'Euclides.

En una carta adreçada a Fuchs, escrita a Caen el 20 de març del 1881, Poincaré li anuncia que ben aviat publicarà els seus resultats sobre les funcions fuchsianes, que apleguen com a casos particulars les funcions el·líptiques i la funció modular el·líptica:

> *J'ai continué à m'occuper des fonctions auxquelles j'ai donné votre nom et j'espère publier prochainement mes résultats. Ces fonctions comprennent comme cas particulier les fonctions elliptiques d'une part, et d'autre part la fonction modulaire.*
>
> Poincaré [*Oeuvres*, t. XI, p. 25].

La primera contribució de Poincaré a l'estudi de les funcions fuchsianes és una nota enviada al *Comptes rendus de l'Académie des Sciences* ([Poi1881]). En ella llegim:

> *Le but que je me propose dans le travail que j'ai l'honneur de présenter à l'Académie, est de rechercher s'il n'existe pas des fonctions analytiques analogues aux fonctions elliptiques et permettant d'intégrer diverses équations différentielles linéaires à coefficients algébriques. Je suis arrivé à démontrer qu'il existe une classe très étendue de fonctions qui satisfont à ces conditions et auxquelles j'ai donné le nom de* fonctions fuchsiennes*, en honneur de M. Fuchs, dont les travaux m'ont servi très utilement dans ces recherches.*
>
> Poincaré [*Oeuvres*, t. II, p. 1].

En el decurs d'un any, Poincaré publicaria en la mateixa revista tretze notes més sobre aquest tema, aplegant finalment els resultats obtinguts en dues memòries que publicà a *Acta mathematica* (cf. [*Oeuvres*, t. II]).

A Poincaré li cal resoldre el problema de l'existència de funcions fuchsianes no constants respecte d'un grup fuchsià Γ arbitrari. Per ferho, reprèn l'antiga idea de Jacobi de representar les funcions el·líptiques com a quocient de funcions theta i cerca les funcions fuchsianes en els quocients de sèries específiques, que anomena thetafuchsianes. Segons Poincaré, l'expressió general d'una sèrie thetafuchsiana és

$$\Theta(z) = \sum_{\gamma \in \Gamma} h(\gamma(z)) \left(\frac{d\gamma(z)}{dz} \right)^k, \quad k > 1,$$

on $h(z)$ denota una funció racional arbitrària. Les sèries thetafuchsianes defineixen funcions quasiperiòdiques; més concretament, satisfan que

$$\Theta(\gamma(z)) = \Theta(z) \left(\frac{d\gamma(z)}{dz} \right)^{-k}, \quad \text{per a tot } \gamma \in \Gamma.$$

Per tant, el quocient de dues funcions thetafuchsianes del mateix pes k i respecte del mateix grup fuchsià és una funció fuchsiana respecte d'aquest grup.

En analogia amb el cas de l'equació modular, Poincaré investiga les possibles relacions algebraiques entre dues funcions fuchsianes:

> [...] *quand $F(z)$ se réduit à la fonction modulaire J,* [...] *nous savons qu'il y a une relation algébrique entre $F(z)$*

> *et* $F\left(\frac{z}{n}\right)$*; c'est cette relation algébrique qui est bien connue sous le nom d'équation modulaire dans la théorie de la transformation des fonctions elliptiques.*
>
> Poincaré [*Oeuvres*, t. II, p. 509].

En un salt qualitatiu impressionant, aïlla el motiu que possibilita l'existència d'una relació algebraica entre una funció fuchsiana i una transformada seva: cal que els grups de períodes respectius comparteixin un subgrup d'índex finit:

> *Pour qu'il y ait une relation algébrique entre une fonction fuchsienne* $F(z)$ *de groupe* G *et sa transformée* $F(z \cdot S)$ *par la substitution* S*, il faut et il suffit que les deux groupes* G *et* $S^{-1}GS$ *soient commensurables.*
>
> Poincaré [*Oeuvres*, t. II, p. 508].

Poincaré demostra que tota funció fuchsiana $x = x(z)$ permet integrar una equació diferencial de coeficients algebraics. Si

$$t_1 := \sqrt{\frac{dx}{dz}}, \quad t_2 := z\sqrt{\frac{dx}{dz}},$$

aleshores t_1, t_2 satisfan una equació diferencial

$$\frac{d^2t}{dx^2} = \varphi(x, y)t,$$

en la qual $\varphi(x, y)$ és una funció racional.

Aquest teorema de Poincaré resultarà molt important a l'hora de realitzar càlculs efectius. Suposem donat un grup fuchsià Γ del qual en coneixem un domini fonamental $\mathcal{F}(\Gamma)$. Si $\mathcal{F}(\Gamma)$ ens permet el càlcul de la funció $\varphi(x, y)$, i integrem l'equació diferencial anterior, el quocient de dues integrals de la mateixa proporcionarà, per inversió, una funció Γ-fuchsiana (cf. Secció 5).

En el treball [Poi1887], Poincaré, tenint present segurament els resultats d'Hermite, intueix que els nous transcendents aritmètics (és a dir, les funcions fuchsianes o thetafuchsianes associades a grups fuchsians aritmètics) proporcionaran en l'estudi de certes classes d'equacions algebraiques serveis anàlegs als de la funció modular en l'estudi de la quíntica:

> *Cela peut faire concevoir l'espoir que ces transcendantes arithmétiques rendront, dans la théorie de certaines classes d'équations algébriques, des services analogues à ceux*

> *qu'a rendus la fonction modulaire dans l'étude de l'équation du cinquième degré.*
>
> Poincaré [*Oeuvres*, t. V, p. 290].

Tenint en compte que els treballs de Riemann, Schwarz, Dedekind i Klein sobre funcions periòdiques eren previs a l'estudi de les funcions fuchsianes per part de Poincaré, i que Fuchs no tenia cap publicació específica sobre aquest tema, Klein proposà a Poincaré en repetides ocasions la substitució del nom *funcions fuchsianes* pel nom *funcions automorfes*, a fi de treure'n tota referència personal. Però la recomanació de Klein no fou presa en consideració per Poincaré, qui argumentà que els treballs de Fuchs li havien proporcionat la inspiració necessària. Recordem el cèlebre episodi de *Science et méthode* [Poi1908] on Poincaré, molts anys després, explica la gènesi del procés creatiu a través de la *seva* descoberta de les funcions fuchsianes!

No obstant l'obstinació de Poincaré, el temps ha donat la raó a Klein: avui anomenem funcions automorfes les funcions fuchsianes, i anomenem formes automorfes les sèries thetafuchsianes. Però seguim designant amb l'adjectiu fuchsians els grups discrets de moviments hiperbòlics.

2.6. **Corbes de Shimura.** L'estudi dels grups fuchsians aritmètics (modulars o no) i de les funcions automorfes associades (modulars o no) conduí cap a l'estudi de les corbes de Shimura (modulars o no). En un dels seus primers treballs sobre aquest tema, Shimura dedica una línia als clàssics:

> [...] *part of the paper is devoted to the theory of a certain type of automorphic functions of one variable known in the literature as functions belonging to indefinite ternary quadratic forms* [cf. Poincaré 1887], [cf. Fricke-Klein, 1897]. *They occur as moduli of abelian varieties of dimension 2 whose endomorphism rings are isomorphic to an order of an indefinite quaternion algebra.*
>
> Shimura [Shi1975].

En general, una àlgebra de quaternions $H = \left(\dfrac{a,b}{F}\right)$ de centre un cos F és un F-espai vectorial de dimensió 4, de base $\{1, \mathrm{I}, \mathrm{J}, \mathrm{K}\}$, amb un producte definit per les regles

$$\mathrm{I}^2 = a,\ \mathrm{J}^2 = b,\ \mathrm{IJ} = -\mathrm{JI} = K, \quad a, b \in F^*.$$

Els grups fuchsians Γ que defineixen les corbes de Shimura són grups fuchsians aritmètics, que generalitzen el grup modular i els seus subgrups de congruència. Considerem una àlgebra de quaternions H de centre un cos de nombres K. Els subanells de H de rang quatre sobre l'anell d'enters de K se solen designar, encara avui, amb el nom antic d'ordres. Suposem que el cos K és totalment real i que l'àlgebra H és no ramificada exactament en una plaça real de K. Els grups fuchsians Γ són subgrups d'índex finit del grup d'unitats de norma 1, d'ordres $\mathcal{O}$ de H.

L'àlgebra de quaternions indefinida més senzilla de centre $\mathbb{Q}$ és l'àlgebra de matrius $H = M(2, \mathbb{Q})$. El seu discriminant és $D = 1$. Les matrius de coeficients enters $\mathcal{O} = M(2, \mathbb{Z})$ en constitueixen un ordre maximal. El grup multiplicatiu de les unitats de norma 1 d'aquest ordre és, exactament, el grup modular: $\mathcal{O}_1^* = \mathrm{SL}(2, \mathbb{Z})$.

Donat un grup fuchsià aritmètic Γ, el cos $\mathbb{C}(\Gamma)$ de totes les funcions Γ-automorfes és el cos de funcions d'una corba algebraica, $X(\Gamma)$, dita de Shimura. Les corbes modulars són doncs un cas particular de les corbes de Shimura, però entre les corbes de modulars (definides pels grups fuchsians estudiats per Klein) i les corbes de Shimura no modulars (definides pels grups fuchsians estudiats per Poincaré) hi ha diferències notables. Per apreciar-les, començarem per fixar-nos en els mosaics hiperbòlics de les figures 3 i 4.

Una tessel·la fonamental del mosaic 3 s'obté per la unió de dos triangles hiperbòlics: el d'angles $(\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{\infty})$ i el seu simètric; i equival, doncs, al domini fonamental de la figura 1. Una tessel·la fonamental del mosaic 4 s'obté per la unió de dos triangles hiperbòlics, el d'angles $(\frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{7})$ i el seu simètric.

En el primer cas, tots els triangles tenen un vèrtex en la circumferència unitat; en el segon, no. Paral·lelament, el grup fuchsià del primer mosaic conté translacions, però el del segon, no. Com a conseqüència, les funcions automorfes associades a cadascun d'aquests mosaics són desenvolupables en sèrie de Fourier únicament en el primer cas.

Shimura interpreta les corbes $X(\Gamma)$ com a espais de moduli de superfícies abelianes dotades de multiplicació quaterniònica, i dotades d'estructures de nivell (cf. Secció 3), generalitzant d'aquesta manera la interpretació clàssica de les corbes modulars com a espais de moduli de corbes el·líptiques amb estructures de nivell. Aquesta interpretació

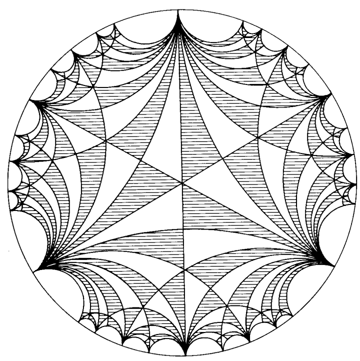

FIGURA 3. Mosaic hiperbòlic $\mathrm{T}(2,3,\infty)$

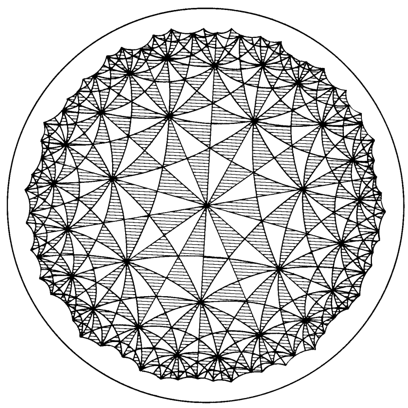

FIGURA 4. Mosaic hiperbòlic $\mathrm{T}(2,3,7)$

és especialment escaient a l'hora d'estudiar els models enters de les corbes.

Les corbes modulars han donat lloc a una extensa literatura. Tant les corbes modulars com la seva generalització, les corbes de Shimura, han esdevingut objectes imprescindibles en el tractament actual de problemes aritmètics (cf. Secció 4). Els treballs de Shimura publicats fins a avui han estat recopilats en quatre volums per l'editorial Springer (cf. [Shimura, CP]).

3. FUNCIONS ABELIANES

3.1. **Funcions abelianes.** Les integrals hiperel·líptiques generalitzen les integrals el·líptiques. Són de la forma

$$\int \frac{R(x)}{\sqrt{P(x)}}\, dx,$$

on $R \in \mathbb{C}(x)$ denota una funció racional i $P \in \mathbb{C}[x]$, un polinomi de grau menor o igual que 6.

Amb analogia amb el problema estudiat per Jacobi de la inversió de les integrals el·líptiques, Göpel (1812-1847), Weierstrass (1815-1897) i Rosenhain (1816-1887), entre d'altres, estudiaren el problema de la inversió de les integrals hiperel·líptiques. Les integrals hiperel·líptiques

$$u_1 \equiv \int_{p_1}^{z_1} \omega_1 + \int_{p_2}^{z_2} \omega_1, \quad u_2 \equiv \int_{p_1}^{z_1} \omega_2 + \int_{p_2}^{z_2} \omega_2$$

estan definides mòdul una xarxa de períodes

$$\Lambda = \langle \oint_{\alpha_1} \omega, \oint_{\alpha_2} \omega, \oint_{\beta_1} \omega, \oint_{\beta_2} \omega \rangle, \quad \omega = (\omega_1, \omega_2).$$

El problema de la inversió planteja expressar les funcions z_1, z_2 en funció de les funcions (multivaluades) u_1, u_2. En fer-ho, s'obtenen dues funcions analítiques en dues variables i de quatre períodes independents:

$$z_i = z_i(u_1, u_2) : \quad \mathbb{C}^2/\Lambda \to \mathbb{C} \cup \{\infty\}, \quad i = 1, 2.$$

Les integrals hiperel·líptiques són casos particulars de les integrals abelianes. La forma general d'una integral abeliana és

$$\int f(x, y)\, dx, \quad f(X, Y) \in \mathbb{C}(X, Y),$$

on les funcions x, y satisfan una relació algebraica. És a dir, se suposa que existeix un polinomi irreductible i no constant $F(X, Y) \in \mathbb{C}[X, Y]$ tal que $F(x, y) = 0$.

La teoria de Riemann permet associar al polinomi $F(X, Y)$ una superfície analítica compacta i g diferencials holomorfes independents:

$$\omega = (\omega_1, \ldots, \omega_g),$$

essent g el gènere de la superfície topològica subjacent. Podem ara considerar les integrals abelianes,

$$(u_1, \ldots, u_g) \equiv (\sum_{k=1}^{g} \int_{p_k}^{z_k} \omega_1, \ldots, \sum_{k=1}^{g} \int_{p_k}^{z_k} \omega_g),$$

definides mòdul una xarxa de períodes $\Lambda \simeq \mathbb{Z}^{2g}$ de $\mathbb{C}^g$.

Les funcions abelianes s'obtenen en resoldre el problema de la inversió de les integrals abelianes. En fer-ho, s'obtenen g funcions de g arguments, Λ-periòdiques:

$$z_i = z_i(u): \quad \mathbb{C}^g/\Lambda \to \mathbb{C} \cup \{\infty\}, \quad 1 \leq i \leq g.$$

Sigui $\mathcal{C}$ la corba projectiva, no singular, de model afí $F(X,Y) = 0$. El tor complex $\mathbb{C}^g/\Lambda$ és algebraic; és a dir, podem interpretar-lo com el conjunt de punts d'una varietat algebraica, $J(\mathcal{C})$, anomenada la varietat jacobiana de la corba:

$$\mathbb{C}^g/\Lambda \xrightarrow{\sim} J(\mathcal{C})(\mathbb{C}).$$

En particular, i per transport d'estructura, el conjunt $J(\mathcal{C})(\mathbb{C})$ esdevé un grup abelià.

Riemann demostrà que les funcions abelianes $\{z_1, \ldots, z_g\}$ anteriorment obtingudes són les solucions de l'equació

$$\Theta(z) = \vartheta\left(\int_{p_0}^{z} \omega - u - \kappa, Z\right) = 0,$$

on $\Lambda = \langle 1_g, Z\rangle$ denota la normalització de la xarxa de períodes de la corba, obtinguda prèvia elecció d'una base simplèctica de l'homologia respecte de l'aparellament d'intersecció (cf. [Rie1857]). La matriu Z és una matriu $g \times g$, simètrica, de part imaginària definida positiva; i κ és l'anomenat vector de Riemann.

3.2. **El teorema de Poincaré-Picard.** Si ara partim d'una xarxa arbitrària Λ de $\mathbb{C}^n$, $n > 1$, el més probable és que les úniques funcions Λ-periòdiques siguin constants. Recordem que aquest fet no es presenta quan $n = 1$ (cf. Secció 2.2).

Una aportació remarcable en aquest context és l'anomenat teorema de Poincaré-Picard, procedent d'una publicació conjunta d'aquests dos autors (cf. [Poi-Pic1883]). El teorema precisa resultats familiars a Weierstrass, Riemann i Hermite. Poincaré i Picard demostren que, donada una xarxa Λ de $\mathbb{C}^n$, existeixen funcions de n variables, no constants, i periòdiques de xarxa de períodes Λ si, i només si, Λ satisfà les anomenades relacions de Riemann respecte d'una forma hermítica H positiva. En aquest cas, $E = \mathrm{Im}H$ és una forma alternada que pren valors enters sobre la xarxa. Si H és definida positiva, aleshores el nombre de funcions és màxim.

Suposem que la forma de Riemann és no degenerada. L'obtenció d'una base simplèctica de la xarxa permet la substitució de la xarxa original per una xarxa normalitzada:

$$\Lambda \sim \langle 1_n, Z \rangle.$$

Les funcions periòdiques en qüestió s'obtenen com a quocient de funcions theta de dues variables amb característiques:

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (u, Z) := \sum_{m \in a + \mathbb{Z}^n} \exp(\pi i ({}^t m Z m + 2 {}^t m (u + b))),$$

${}^t a, {}^t b \in \mathbb{R}^g$, $u \in \mathbb{C}^n$. La variable u, que s'anomena l'argument, és un vector de $\mathbb{C}^n$. La variable Z, que s'anomena el mòdul, és una matriu $n \times n$, simètrica, de part imaginària definida positiva (que cal substituir pel valor que dóna la xarxa). Les característiques a, b proporcionen una àmplia generalització de les diferents funcions theta que, en el seu dia, havia considerat Jacobi en dimensió $n = 1$.

Poincaré i Picard demostren que tota funció periòdica de xarxa de períodes (Λ, H) és quocient de funcions theta abelianes; és a dir, de funcions theta construïdes a partir de xarxes de períodes d'integrals abelianes:

> *Nous avons démontré* [...] *M. Picard et moi, qu'un système* quelconque *de fonctions abéliennes peut être déduit par réduction d'un système analogue, engendré par une courbe algébrique.*
>
> Poincaré [*Oeuvres*, t. IV, p. 315].

No menys important és l'estudi portat a terme per Poincaré sobre reducció d'integrals abelianes, que conduiria també al concepte d'isogènia entre varietats abelianes i a l'anomenat teorema de Poincaré de reductibilitat completa. Vegem part d'aquests resultats en les seves pròpies paraules:

> *J'ai donné moi-même, à ce sujet, un théorème, d'après lequel, quand il y a réduction, on peut, par une transformation d'ordre k, changer la fonction Θ à reduire en un produit de fonctions Θ, d'un moindre nombre de variables. L'entier k est alors le nombre caractéristique de la réduction.*
>
> Poincaré [*Oeuvres*, t. IV, p. 314].

3.3. **Varietats abelianes.** Els treballs de Poincaré sobre les integrals abelianes es compten entre la llarga sèrie de treballs clàssics que tingueren una repercussió directa en el naixement i posterior desenvolupament de la teoria de les varietats abelianes.

Les varietats abelianes complexes són tors complexos que són, a més, varietats algebraiques projectives. Estan dotades d'una llei d'addició algebraica, commutativa, que reflecteix l'existència d'un isomorfisme

$$\mathbb{C}^n/\Lambda \xrightarrow{\sim} A(\mathbb{C}),$$

on A és la varietat en qüestió. Les corbes el·líptiques són les varietats abelianes de dimensió 1. Altres exemples són les varietats jacobianes de les corbes, que són varietats abelianes de dimensió igual al gènere g de la corba. L'any 1921 Lefschetz donava la definició següent d'aquestes varietats:

> *An* Abelian *variety of genus p, V_p, is a variety whose non-homogeneous point coordinates are equal to $2p$-ply periodic meromorphic functions of p arguments $u_1, \ldots, u_p$, or whose homogeneous point coordinates are proportional to theta's of the same order and continuous characteristic. The variety is algebraic* (*Weierstrass*) *and of dimensionality p. When the periods are those of an algebraic curve of genus p, V_p is called a* Jacobi *variety.*
>
> Lefschetz [Lef1921].

A poc a poc, el punt de vista analític cedí pas al llenguatge algebraic. Es precisaren les definicions de varietat abeliana sobre un cos qualsevol i de jacobiana d'una corba; s'introduí el concepte de polarització d'una varietat abeliana; es creà una teoria *ad hoc* de funcions theta, divisors, fibrats, etc. L'estudi de les varietats abelianes des d'aquest punt de vista seria posat a punt per Weil (1906-1998) (cf. [We1948], [We1958]).

En l'estudi aritmètic de les varietats abelianes definides sobre cossos de nombres, o sobre cossos p-àdics, es consideren, a més, els models enters d'aquestes varietats. Es tracta d'esquemes sobre l'anell d'enters del cos corresponent. Les seves fibres proporcionen informació aritmètica important. Aquests models enters i les seves reduccions han estat especialment estudiats en les jacobianes $J(X(\Gamma))$ de les corbes modulars i, més generalment, de les corbes de Shimura.

4. PUNTS RACIONALS DE CÚBIQUES

4.1. **Corbes el·líptiques racionals.** En el treball [Poi1901], Poincaré s'ocupa de l'estructura del subgrup dels punts de coordenades racionals d'una corba el·líptica definida sobre el cos dels nombres racionals. El treball conté la que fou anomenada conjectura de Poincaré per a corbes el·líptiques, segons la qual, donada una corba el·líptica sobre $\mathbb{Q}$,

$$E: \quad Y^2 = X^3 + a_4 X + a_6, \quad a_i \in \mathbb{Q},$$

el grup abelià $E(\mathbb{Q})$ dels seus punts de coordenades racionals és finitament generat.

De fet, en el treball esmentat, Poincaré no formula explícitament cap conjectura. Es limita a constatar un fet:

> *Si les points d'arguments elliptiques* $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_q$ *sont rationnels, il en est de même de tous les points dont les arguments elliptiques sont compris dans la formule*
>
> $$(1) \quad \alpha + 3n\alpha + p_1(\alpha_1 - \alpha) + p_2(\alpha_2 - \alpha) + \cdots + p_q(\alpha_q - \alpha)$$
>
> *où* n *et les* p *sont entieres. On peut se proposer de choisir les arguments* (2) $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_q$ *de telle façon que la formule* (1) *comprenne tous les points rationnels de la cubique. Les* $q+1$ *points rationnels qui ont les arguments* (2) *forment alors ce que nous appellerons un* système de points rationnels fondamentaux.
>
> Poincaré [*Oeuvres*, t. V, p. 492].

Fixem-nos amb què un "sistema de punts racionals fonamentals" es tradueix en un sistema de generadors del grup abelià $E(\mathbb{Q})$.

La conjectura de Poincaré fou demostrada per Mordell l'any 1922 [Mo1922]. En ser el grup abelià $E(\mathbb{Q})$ finitament generat, té, pel teorema d'estructura, una part lliure i una part de torsió:

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

Per definició, l'enter $r = \operatorname{rg} E(\mathbb{Q}) \geq 0$ és el rang de la corba el·líptica.

El teorema de Mordell fou generalitzat per Weil els anys 1928 i 1929. D'una banda, Weil estengué el resultat de Mordell a totes les corbes el·líptiques definides sobre cossos de nombres. D'altra banda, Weil estengué el resultat anterior a les varietats abelianes de dimensió qualsevol definides sobre cossos de nombres.

L'any 1977, Mazur [Ma1977] obtingué un resultat fonamental sobre la torsió de les corbes el·líptiques definides sobre $\mathbb{Q}$, que completava resultats parcials d'altres autors. Mazur demostrà que tota corba el·líptica $E/\mathbb{Q}$ té, com a màxim, 16 punts de torsió racionals, i precisà les possibles estructures del grup de torsió:

$$E(\mathbb{Q})_{\mathrm{tor}} \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z}, \ 1 \leq N \leq 10, \ N = 12, \\ \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \ 1 \leq N \leq 4\,. \end{cases}$$

El problema resolt per Mazur es tradueix en un problema diofantí relatiu a corbes modulars $X_0(N)$. Degut a la interpretació de les corbes modulars com a espais de moduli de corbes el·líptiques amb estructures de nivell, els valors de N que se citen més amunt provenen de valors M per als quals la corba modular $X_0(M)$ té punts racionals, diferents de les puntes.

4.2. **La conjectura de Birch i Swinnerton-Dyer.** Seguint el model proporcionat per la funció zeta de Riemann en l'estudi dels nombres primers, l'any 1933 Hasse associà a tota corba el·líptica $E/\mathbb{Q}$ una funció

$$L(E/\mathbb{Q}, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

on

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

La funció L de E conté informació aritmètica de la corba el·líptica, en tant que té en compte el nombre de punts de la seves reduccions $\widetilde{E}$ en els diferents primers. Se satisfà que $|a_p| < 2p^{1/2}$, amb la qual cosa el producte infinit convergeix absolutament i uniformement sobre els compactes situats en el semiplà $\mathrm{Re}(s) > 3/2$. Per tant, $L(E, s)$ és una funció holomorfa i sense zeros en el semiplà esmentat.

Com en el cas de la funció zeta de Riemann, cal completar la funció L amb factors proporcionats per la funció Γ d'Euler:

$$\Lambda(E/\mathbb{Q}, s) := N^{s/2}(2\pi)^{-s}\Gamma(s)L(E/\mathbb{Q}, s). \quad \mathrm{Re}(s) > 3/2.$$

La constant $N = N_E$ es determina per mitjà de l'estudi de les fibres de reducció dolenta de la corba, i s'anomena el conductor de E.

Recordem que la funció zeta de Riemann s'estén en una funció meromorfa del pla amb un únic pol, simple, en $s = 1$. Per analogia amb aquest fet, l'any 1967 Hasse i Weil conjecturaren que la funció $\Lambda(E/\mathbb{Q}, s)$ admetria una prolongació analítica en una funció entera i satisfaria una equació funcional:

$$\Lambda(E/\mathbb{Q}, 2 - s) = w(E)\Lambda(E/\mathbb{Q}, s), \quad s \in \mathbb{C}, \quad w(E) = \pm 1.$$

La conjectura de Hasse-Weil fou provada per Deuring en el cas de les corbes el·líptiques amb multiplicació complexa. Més endavant, es veié que la conjectura era certa per a totes les corbes el·líptiques uniformitzables per funcions modulars.

En els anys 1963 i 1965, Birch i Swinnerton-Dyer posaren de manifest mitjançant experiències numèriques realitzades en corbes amb multiplicació complexa, que el rang r de $E/\mathbb{Q}$ anava coincidint amb l'ordre en el punt $s = 1$ del zero de la funció $L(E/\mathbb{Q}, s)$. Conjecturaren que aquest podria molt bé ser un fet general:

$$r \stackrel{?}{=} \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s).$$

En el moment de la seva formulació, la conjectura de Birch i Swinnerton-Dyer semblava excessivament agosarada, atès que comparava una quantitat desconeguda amb una quantitat que ni tan sols estava definida (car $1 < 3/2$).

Els resultats parcials coneguts en favor de la conjectura de Birch i Swinnerton-Dyer inclouen dos teoremes esplèndids: el teorema de Coates-Wiles, de l'any 1977, i el teorema de Gross-Zagier, de l'any 1983.

Coates i Wiles demostraren que si $E/\mathbb{Q}$ és una corba el·líptica dotada de multiplicació complexa per un cos quadràtic de nombre de classes 1, aleshores

$$L(E/\mathbb{Q}, 1) \neq 0 \Rightarrow \mathrm{rg} E(\mathbb{Q}) = 0.$$

Gross i Zagier demostraren que

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) = 1 \Rightarrow \mathrm{rg} E(\mathbb{Q}) \geq 1$$

per a totes les corbes el·líptiques $E/\mathbb{Q}$ uniformitzables mitjançant funcions modulars.

La conjectura de Birch i Swinnerton-Dyer segueix essent avui un problema obert i, com a tal, figura proposat en la llista de l'Institut Clay dels Set Problemes del Mil·leni.

4.3. **Uniformització modular de corbes el·líptiques.** La conjectura de Shimura-Taniyama-Weil (STW), formulada en els anys 1960, proporcionà un camí per provar la conjectura de Hasse-Weil. La conjectura STW afirma que tota corba el·líptica $E/\mathbb{Q}$ és uniformitzable per funcions modulars. Més concretament, si el conductor de $E/\mathbb{Q}$ és igual a N, la corba E ha de ser isògena sobre $\mathbb{Q}$ a un factor de la jacobiana $J_0(N)$ de la corba modular $X_0(N)$. En particular, les integrals el·líptiques associades a corbes el·líptiques definides sobre $\mathbb{Q}$ s'han de poder obtenir per reducció d'integrals abelianes associades a corbes modulars. Si això és així, aleshores la funció L admet una representació integral de nucli integral donat per una funció thetafuchsiana de pes 2:

$$L(E/\mathbb{Q}, s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z},$$

on $f(z)dz \in H^0(X_0(N), \Omega^1)$. Aquesta representació integral permet la prolongació analítica de la funció L i la prova de l'equació funcional (com en el cas de la funció zeta de Riemann).

La conjectura STW adquirí una rellevància inesperada quan, gràcies a teoremes de Frey [1986], de Serre [1987] i de Ribet [1990], es posà de manifest que no solament implicava la conjectura de Hasse-Weil sinó que, a més, implicava el Teorema de Fermat. Com és ben sabut, STW esdevingué un teorema, degut a Wiles [1993], Taylor-Wiles [1993], Diamond [1996], Conrad-Diamond-Taylor [1998] i Breuil-Conrad-Diamond-Taylor [1999].

En una primera apreciació hom pot pensar que els grups fuchsians que intervenen en STW són únicament els subgrups de congruència del grup modular i les corbes modulars. Però el fet és que la resta de subgrups fuchsians aritmètics, tal com els entenia Poincaré, i les corbes de Shimura associades intervenen per partida doble en la demostració del Teorema de Fermat. D'una banda, s'utilitzen per demostrar que STW implica Fermat. D'altra banda, s'utilitzen en la prova mateixa de STW. Els punts essencials (i més difícils) provenen de comparar les fibres de models enters de jacobianes de corbes modulars amb les fibres de models enters de jacobianes de corbes de Shimura.

5. EXEMPLES

En aquesta darrera secció mostrem alguns exemples numèrics que il·lustren conceptes considerats en les seccions anteriors. Apleguen una part de resultats obtinguts conjuntament amb Alsina, Guàrdia i Travesa en el context de les corbes de Shimura i de la seva interpretació com a espais de moduli (cf. [Al2000], [Al-Ba2004], [Ba-Gu2004] i [Ba-Tr]). En la realització d'aquests treballs, la lectura de Poincaré resultà especialment reveladora.

L'àlgebra $\mathbb{H}_6 = \left(\frac{3, -1}{\mathbb{Q}}\right)$, de discriminant $D = 6$, és la $\mathbb{Q}$-àlgebra de quaternions ramificada de discriminant més petit que és isomorfa a una subàlgebra de $\mathbf{M}(2, \mathbb{R})$. En el que segueix considerarem fixada la immersió

$$\begin{array}{rcl}\Phi : \mathbb{H}_6 & \longrightarrow & \mathbf{M}(2,\mathbb{R}) \\ x + y\mathrm{I} + z\mathrm{J} + t\mathrm{K} & \mapsto & \begin{bmatrix} x + y\sqrt{3} & z + t\sqrt{3} \\ -(z - t\sqrt{3}) & x - y\sqrt{3} \end{bmatrix}. \end{array}$$

La traça reduïda i la norma reduïda d'un quaternió es definiexen per

$$\mathrm{tr}(x + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}) = 2x, \quad \mathrm{n}(x + y\mathrm{I} + z\mathrm{J} + t\mathrm{K}) = x^2 - 3y^2 + z^2 - 3t^2,$$

i coincideixen amb la traça i el determinant de la matriu imatge per Φ.

Tots els ordres maximals de $\mathbb{H}_6$ són conjugats. Fixem el representant en aquesta classe de conjugació:

$$\mathcal{O}_6 = \mathbb{Z}\left[1, \mathrm{I}, \mathrm{J}, \frac{1 + \mathrm{I} + \mathrm{J} + \mathrm{K}}{2}\right].$$

Sigui $(\mathcal{O}_6)_1^* = \{\gamma \in \mathcal{O}_6 : \mathrm{n}(\gamma) = 1\}$ el grup de les unitats de norma reduïda igual a 1.

El grup $\Gamma_6 := \Phi((\mathcal{O}_6)_1^*)$ és un grup fuchsià aritmètic, que admet la descripció següent:

$$\Gamma_6 = \left\{\gamma = \frac{1}{2}\begin{bmatrix} \alpha & \beta \\ -\beta' & \alpha' \end{bmatrix} : \alpha, \beta \in \mathbb{Z}[\sqrt{3}], \det\gamma = 1, \ \alpha \equiv \beta \pmod 2\right\},$$

on α' denota la conjugació de Galois no trivial d'un element α del cos quadràtic $\mathbb{Q}(\sqrt{3})$.

La figura 5 mostra un domini fonamental $\mathcal{F}(\Gamma_6)$ per l'acció de Γ_6 en $\mathcal{H}$. El grup Γ_6 és un grup fuchsià sense transformacions parabòliques. La corba completa i no singular $X_6 := X(\Gamma_6)$ és de gènere zero i definida sobre $\mathbb{Q}$.

Sigui R un ordre quadràtic de discriminant d_R contingut de manera òptima en l'ordre $\mathbb{Z}+2\mathcal{O}_6$ de $\mathbb{H}_6$. Associat a R tenim la família següent de formes quadràtiques binàries i primitives de discriminant d_R i de coeficients enters algebraics:

$$\Big\{(a + b\sqrt{3}, 2c\sqrt{3}, a - b\sqrt{3}) : \quad a, b, c \in \mathbb{Z}, \ a \equiv b \equiv c \pmod 2,$$

$$\mathrm{disc}(f) = d_R, \ \mathrm{mcd}\left(\frac{c+b}{2}, \frac{a+b}{2}, b\right) = 1\Big\}.$$

En classificar aquestes formes per l'acció de Γ_6, obtindrem per a cada R un conjunt finit de classes. Els seus zeros proporcionaran punts de multiplicació complexa en el domini fonamental $\mathcal{F}(\Gamma_6)$. En particular,

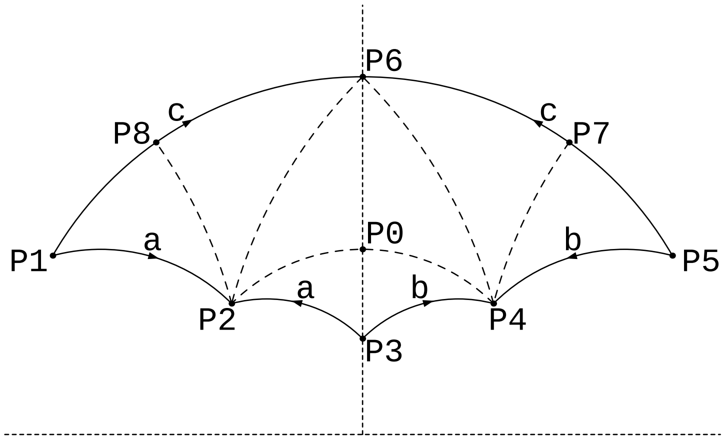

FIGURA 5. Domini fonamental $\mathcal{F}(\Gamma_6)$

l'ordre màxim del cos quadràtic $\mathbb{Q}(\sqrt{-6})$ proporciona el dos punts de multiplicació complexa especials:

$$P_0 = \frac{i(\sqrt{6}-\sqrt{2})}{2}, \quad P_7 = \frac{\sqrt{3}+i\sqrt{6}}{3} \sim P_8.$$

La teoria de la multiplicació complexa garanteix que les funcions fuchsianes del model de Shimura prenen valors algebraics en aquests punts.

La figura 5 mostra els punts de multiplicació complexa especials en el domini de la corba X_6 i una partició del domini en triangles i quadrilàters hiperbòlics obtinguda gràcies a aquests punts. La consideració d'aquests polígons hiperbòlics permet interpretar la corba X_6 com a una corba recobridora de quatre corbes més, també de gènere zero.

La funció fuchsiana t_6 que uniformitza la corba X_6 fou obtinguda a partir del teorema de Poincaré per integració d'una equació diferencial fuchsiana. L'equació en qüestió, escrita mitjançant la informació proporcionada pel domini fonamental, conté d'entrada 8 constants que cal determinar. La consideració conjunta dels recobriments subordinats a la corba porta a un conjunt de cinc equacions diferencials, que s'obtenen a partir de plegaments escaients del domini. Entre totes proporcionen dades suficients per determinar les constants cercades de l'equació diferencial de partida i de les equacions auxiliars. L'equació diferencial fuchsiana satisfeta per t_6 és donada per

$$D_a(t,z) = \frac{27t^4+74t^2+27}{36t^2(t^2-1)^2},$$

on $D_a(t,z)$ denota la derivada automorfa.

La funció fuchsiana t_6 és determinada pel seu valor en tres punts del domini fonamental. Pot ésser desenvolupada a l'entorn de qualsevol punt del domini, però no admet desenvolupaments en sèrie de Fourier perquè Γ_6 no conté transformacions parabòliques. Qüestions diofantines condueixen cap a normalitzacions convenients, tant de la funció t_6 com dels paràmetres d'uniformització locals.

Situem-nos al voltant del punt P_6 i fixem t_6 de manera que tingui un pol en aquest punt (amb analogia a la funció j de Klein, del cas $D=1$). A l'entorn del vèrtex $P=P_6$, la funció fuchsiana normalitzada

$$j_6(P, q_P; z) := \frac{1}{384} t_6$$

admet el desenvolupament en sèrie

$$j(P, q_P; z) = \sum_{n=-1}^{\infty} c_n \frac{q_P(z)^n}{(2e_P(n+2))!}, \quad \text{on} \quad q_P(z) = \frac{1}{\nu_P}\left(k_P \frac{z-P}{z-\overline{P}}\right)^{e_P},$$

$$e_P = 2, \quad k_P = \frac{\sqrt{3}(1-i)}{4\sqrt{2}} \frac{\Gamma(1/3)\Gamma(2/3)\Gamma(1/4)}{\Gamma(3/4)\Gamma(7/12)\Gamma(11/12)}, \quad \nu_P = 2^4.$$

Els coeficients c_n $(-1 \leq n \leq 10)$ del desenvolupament són

$$\begin{array}{r}
1 \\
0 \\
18480 \\
0 \\
12803590800 \\
0 \\
-817993722627081000 \\
0 \\
-1560789298453265580199500000 \\
0 \\
1228599534077201106792411793803450000 \\
0
\end{array}$$

L'elecció del paràmetre d'uniformització local q_P obeeix a raons proporcionades per la isotropia local. Cal un paràmetre escaient a fi que els coeficients siguin enters, i cal que aquest paràmetre estigui convenientment escalat a fi que la funció prengui valors algebraics en els punts de multiplicació complexa.

La corba X_6 és l'espai groller de moduli de les superfícies abelianes amb multiplicació quaterniònica per $\mathcal{O}_6$. Aquestes superfícies abelianes són jacobianes de corbes de gènere 2. L'elecció d'una polarització, d'estructures de nivell convenients i la utilització de funcions ϑ permet el càlcul efectiu d'aquestes corbes.

Considerem, com abans, els punts de multiplicació complexa especials

$$P_0 = \frac{i(\sqrt{6}-\sqrt{2})}{2}, \quad P_7 = \frac{\sqrt{3}+i\sqrt{6}}{3}.$$

Calculant els períodes normalitzats de les integrals abelianes associades s'obtenen les xarxes $\langle 1_2, Z_k \rangle$, on

$$Z_1 = \begin{bmatrix} \frac{-1+3i\sqrt{6}}{5} & \frac{-2+i\sqrt{6}}{5} \\ \frac{-2+i\sqrt{6}}{5} & \frac{6+2i\sqrt{6}}{5} \end{bmatrix}, \; Z_2 = \begin{bmatrix} \frac{-1+2i\sqrt{6}}{5} & \frac{-2-i\sqrt{6}}{5} \\ \frac{-2-i\sqrt{6}}{5} & \frac{6+3i\sqrt{6}}{5} \end{bmatrix}.$$

Aquests períodes determinen sengles varietats jacobianes, J_k, els punts complexos de les quals són donats per

$$\mathbb{C}^2/\langle 1_2, Z_k \rangle \simeq J_k(\mathbb{C}), \quad k = 1, 2.$$

La recuperació de les corbes algebraiques que tenen per jacobianes les varietats abelianes anteriors es porta a terme mitjançant funcions theta amb característiques. En l'exemple concret que ens ocupa s'obtenen les corbes hiperel·líptiques:

$$Y^2 = X^5 - 2i\sqrt{2}X^4 - \frac{11}{3}X^3 + 2i\sqrt{2}X^2 + X,$$

$$Y^2 = X^5 + 2\sqrt[4]{-5+2\sqrt{6}}X^4 - \frac{10}{3}i\sqrt{2}X^3 + 2i\sqrt[4]{-5-2\sqrt{6}}X^2 + X.$$

Adonem-nos que les classes d'isomorfia d'aquestes corbes posseeixen models algebraics perquè els períodes Z_k han estat obtinguts a partir de punts de multiplicació complexa del domini; és a dir, en última instància, mitjançant zeros de classes de formes quadràtiques binàries construïdes d'acord amb Poincaré.

Referències

[Al2000] Alsina, M.: *Aritmètica d'ordres quaterniònics i uniformització hiperbòlica de corbes de Shimura*. Tesi UB, 2000. ISBN: 84-475-2491-4.

[Al-Ba2004] Alsina, M.; Bayer, P.: *Quaternion orders, quadratic forms and Shimura curves*. CRM Monograph Series **22**. AMS, 2004 (198 + ix p.). ISBN: 0-8218-3359-6.

[Bak1897] Baker, H. F.: *Abelian Functions*. Cambridge University Press, 1995. Primera ed.: Cambridge University Press, 1897.

[Ba2002] Bayer, P.: Uniformization of certain Shimura curves. In *Differential Galois Theory*, T. Crespo and Z. Hajto (eds.). Banach Center Publications **58** (2002), 13-26.

[Ba-Gu2003] Bayer, P.; Guàrdia, J. (eds.): *Funcions theta*. Notes del Seminari de Teoria de Nombres (UB-UAB-UPC) **10**, 2003. ISBN 84-923250-7-0.

[Ba-Gu2004] Bayer, P.; Guàrdia, J.: On equations defining fake elliptic curves. *J.* de Théorie des nombres de Bordeaux 2004, per aparèixer.

[Ba-Tr] Bayer, P.; Travesa, A.: *Uniformizing functions for certain Shimura curves, in the case* $D = 6$, pre-publicació 2004.

[De1877] Dedekind, R.: Schreiben an Herrn *Borchardt* über die Theorie der elliptischen Modul-Functionen. *J. für reine u. angew. Math.* **83** (1877), 265-292.

[For1902] Forsyth, A. R.: *Theory of Differential Equations*, v. III. Cambridge University Press, 1902.

[Fou1822] Fourier, J-B. J.: *Théorie analytique de la chaleur.* Paris, 1822.

[Fri-Kl1897-1912] Fricke, R.; Klein, F.: *Vorlesungen ueber die Theorie der automorphen Funktionen* v. I–II. Teubner, 1897; 1912. Reimpressió: Johnson Reprint, 1965.

[Fu1866] Fuchs, L.: Zur Theorie der linearen Differential Gleichungen mit veränderlichen Coefficienten. *J. für reine u. angew. Math.* **66** (1866), 121-160.

[Fu1876] Fuchs, L.: Ueber die linearen Differential Gleichungen zweiter Ordnung, welche algebraische Integrale basitzen, und eine neue Anwendung del Invariantentheorie. *J. für reine u. angew. Math.* **81** (1876), 97-142.

[Fu1880] Fuchs, L.: Ueber eine Klasse von Funktionen mehrerer Variablen, welche durch Umkehrung der Integrale von Lösungen der linearen Differential Gleichungen mit rationalen Coeffizienten entstehen *J. für reine u. angew. Mathematik*, **89** (1880), 151-169.

[Ga1801] Gauss, C. F.: *Disquisitiones arithmeticæ*. Leipzig, 1801. *Disquisicions aritmètiques*, traducció de G. Pascual. SCM, 1996.

[Gra1986] Gray, J.: *Linear Differential Equations and Group Theory from Riemann to Poincaré.* Birkhäuser, 1986.

[Ja1829] Jacobi, C. G. J.: *Fundamenta nova theoriae functionum ellipticarum*, 1829. Gesammelte Werke Bd. 1. Berlin, 1881.

[Klein, GMA] Klein, F.: *Gesammelte Mathematische Abhandlungen*, v. III. R. Fricke; H. Vermeil; E. Bessel-Hagen (eds.). Springer, 1923. Reimpressió: Springer, 1973.

[Kl-Fri1890] Klein, F.; Fricke, R.: *Vorlesungen ueber die Theorie der elliptischen Modulfunctionen*, v. I–II. Teubner, 1890. Reimpressió: Johnson Reprint, 1965.

[Kra1903] Krazer, A.: *Lehrbuch der Thetafunktionen.* Chelsea, 1970. Primera ed.: Leipzig, 1903.

[Lan-Bir1992] Lange, H.; Birkenhake, C.: *Complex Abelian Varieties.* GMW **302**. Springer, 1992.

[Law1998] Lawden, D. F.: *Elliptic Functions and Applications.* Colledge Press, 1998.

[Lef1921] Lefschetz, S.: On certain numerical invariants of algebraic varieties with application to abelian varieties. *Trans. Amer. Math. Soc.* **22** no. 3 (1921), 327-406; **22** no. 4 (1921), 407-482.

[Ma1977] Mazur, B.: Modular curves and the Eisenstein ideal. *Publications mathématiques de l'I.H.E.S.* **47** (1977), 33-186.

[Mo1922] Mordel, L. J.: On the rational solutions of the indeterminate equations of the third and four degrees. *Proc. Cambridge Phil. Soc.* **22** (1922), 179-192

[Mum1983] Mumford, D.: *Tata Lectures on Theta I.* Progress in Math. **28**. Birkhäuser, 1983.

[Mum1984] Mumford, D.: *Tata Lectures on Theta II.* Progress in Math. **43**. Birkhäuser, 1984.

[Mum1991] Mumford, D.; Nori, M.; Norman, P.: *Tata Lectures on Theta III.* Progress in Math. **97**. Birkhäuser, 1991.

[Poi1881] Poincaré, H.: Sur les fonctions fuchsiennes. *Comptes rendus de l'Académie des Sciences* **92** (1881), 333-335.

[Poi1884] Poincaré, H.: Sur la réduction des intégrales abéliennes. *Bull. Soc. Mat. France* **12** (1884), 124-143.

[Poi1887] Poincaré, H.: Les fonctions fuchsiennes et l'arithmétique. *Journal de Mathématiques* **3** (1887), 405-464.

[Poi1891] Poincaré, H.: Extension aux nombres premiers complexes des théorèmes de M. Tchebicheff. *Journal de Mathématiques* **8** (1891), 25-68.

[Poi1901] Poincaré, H.: Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques* t. **7** (1901), 161-233.

[Poi1904] Poincaré, H.: Sur les fonctions abéliennes. *Acta Math.* **26** (1904), 43-98.

[Poi1908] Poincaré, H.: *Science et méthode.* Flammarion. Paris, 1908. *Ciencia y método*; traducció de M. García Miranda y L. Alonso. Colección austral, **409**. Espasa Calpe, 1963.

[Poincaré, *Oeuvres*] Poincaré, H.: *Oeuvres*, 11 v. Gauthier-Villars. Paris, 1916-1956.

[Poi-Pic1883] Poincaré, H.; Picard, E.: Sur un théorème de Riemann relatif aux fonctions de n variables indépendentes admettant $2n$ systèmes de périodes. *Comptes rendus de l'Académie des Sciences* **97** (1883), 1284-1287.

[Rie1857] Riemann, B.: *Theorie der Abel'schen Functionen.* Gesammelte mathematische Werke. Teuber, 1892.

[Rot2003] Rotger, V.: *Abelian varieties with quaternionic multiplication and their moduli.* Tesi UB, 2003.

[Rot2004] Rotger, V.: Modular Shimura varieties and forgetful maps. *Trans. Amer. Math. Soc.* **356** (2004), 1535-1550.

[Sa-Ge1969] Sansone, G.; Gerretsen, J.: *Lectures on the Theory of Functions of a Complex Variable. II Geometric Theory.* Wolters-Noordhoff Publishing Groningen, 1969.

[Scor1916] Scorza, G.: Intorno alla teoria generale delle matrici di Riemann. *Rend. Circ. Mat. Palermo* **41** (1916), 263-379.

[Shi1971] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions.* Iwanami Shoten and Princeton University Press, 1971.

[Shi1975] Shimura, G.: On the real points of an arithmetic quotient of a bounded symmetric domain. *Math. Ann.* **215** (1975), 135-164.

[Shi1976] Shimura, G.: Theta Functions with Complex Multiplication. *Duke Math. J.* **43** (1976), 673-696.

[Shi1998] Shimura, G.: *Abelian Varieties with Complex Multiplication and Modular Functions.* Princeton Mathematical Series **46**. Princeton University Press, 1998.

[Shimura, CP] Shimura, G.: *Collected Papers*; v. I (1954-1966); v. II (1967-1977); v. III (1978-1988); v. IV (1989-2001);

[Sw-Dy1974] Swinnerton-Dyer, H. P. F.: *Analytic Theory of Abelian Varieties.* London Math. Soc., Lecture Notes Series **14**. Cambridge University Press, 1974.

[We1948] Weil, A.: *Courbes algébriques et variétés abéliennes*. Hermann, 1971. Primera ed.: Hermann, 1948.

[We1958] Weil, A.: *Variétés kähleriennes*. Hermann, 1971. Primera ed.: Hermann, 1958.

[Weil, *Oeuvres*] Weil, A.: *Oeuvres scientifiques. Collected Papers*, Vols. I, II, III. Springer, 1979.

[Yo1987] Yoshida, M.: *Fuchsian Differential Equations*. Max-Planck-Institut für Mathematik. Vieweg & Sohn, 1987.

P. Bayer. Facultat de Matemàtiques. Universitat de Barcelona. Gran Via de les Corts Catalanes 585. E-08007, Barcelona

E-mail address: `bayer@ub.edu`