Aritmètica: a les portes de la terra promesa

Enric Nart

Introducció[1]

De les diverses qüestions que concerneixen l'aritmètica em centraré en aquesta xerrada en la resolució d'equacions diofantines. Una equació diofantina és simplement un sistema d'equacions polinòmiques:

$$\left.\begin{array}{c} F_1(X_1, \cdots, X_n) = 0 \\ \cdots\cdots\cdots\cdots \\ F_m(X_1, \cdots, X_n) = 0 \end{array}\right\}$$

El terme *diofantina* emfasitza que ens interessem per les solucions enteres de l'equació. Resoldre l'equació equival, doncs, a trobar totes les n-ples $(x_1, \cdots, x_n)$ de nombres enters que satisfacin simultàniament totes les equacions. El més usual és que els polinomis $F_i(X_1,..., X_n)$ tinguin també coeficients enters.

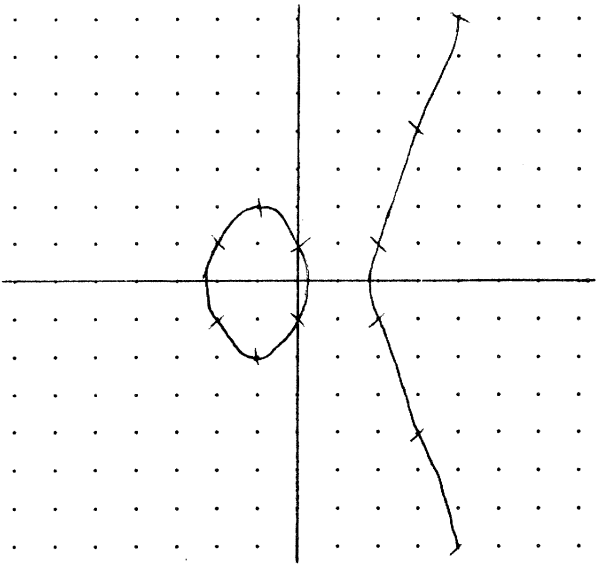
Aquesta qüestió té una interpretació geomètrica clara. Per exemple, una equació en dues variables com:

$$Y^2 = X^3 - 4X + 1, \tag{1}$$

podem pensar-la com una corba en el pla XY, i resoldre la corresponent equació diofantina equival a trobar totes les interseccions de la corba amb la xarxa de punts de coordenades enteres.

Tot i que discutirem el cas general, per fixar les idees convé tenir sempre present l'equació determinada per un sol polinomi en dues variables: $f(X, Y) = 0$. És el cas no-trivial més senzill i il·lustra prou bé les dificultats inherents a la resolució d'equacions diofantines.

Cal admetre també com a genuïnament diofantí el problema de determinar les solucions racionals d'un sistema d'equacions polinòmiques. En efecte, les solucions racionals d'una equació estan (gairebé) en correspondència bijectiva amb les solucions enteres de l'equació obtinguda homogeneïtzant tots els polinomis involucrats.



Per exemple, les solucions racionals d'(1) es corresponen amb les solucions enteres de:

$$Y^2 Z = X^3 - 4XZ^2 + Z^3. \tag{2}$$

A tota solució entera (x, y, z) d'aquesta darrera equació li podem associar una solució racional $(\frac{x}{z}, \frac{y}{z})$ d'(1). La correspondència és bijectiva si identifiquem les solucions homotètiques de (2) ($(mx, my, mz) \sim (x, y, z)$ si m enter) i si excloem les solucions amb $Z = 0$.

El punt de vista geomètric

En la primera part de la conferència vull fer una breu revisió històrica del desenvolupament que varen experimentar les qüestions diofantines a partir del 1890.

En aquest període l'aritmètica es troba en un moment de gran esplendor. Després dels treballs iniciàtics de Fermat al segle XVII, els primers després de l'*Aritmètica* de Diofant d'Alexandria (segle III), a qui deuen el seu nom les equacions diofantines, han seguit contribucions importants d'Euler, Legendre, Lagrange i Gauss. Al prinicpi del segle XIX Gauss va publicar les *Disquisitiones Aritmeticae* i a mitjan segle s'ha viscut el *boom* de la teoria de la divisibilitat per a nombres algebraics, amb les cèlebres contribucions de Kummer, Dirichlet, Dedekind i Kronocker, que han comportat la introducció d'importants conceptes d'àlgebra i anàlisi com les sèries de Dirichlet o els

conceptes de mòdul i d'ideal. Doncs bé, el 1890 l'aritmètica viu encara una nova revolució transcendental: Hilbert i Hurwitz apliquen a les qüestions diofantines tècniques de geometria algebraica.

Una equació com (1) defineix una corba C del pla. Estudiar la *geometria* de la corba és estudiar les propietats del punts de la corba, o dels sistemes de punts de la corba, invariants per transformacions biracionals. Si la corba està definida sobre $\mathbb{Q}$ (notació: $C_{|\mathbb{Q}}$), té sentit estudiar el que Hilbert i Hurwitz anomenen l'*aritmètica* de la corba [Hi-Hu]; és a dir, les propietats dels *punts racionals* de la corba, o dels sistemes de punts racionals, invariants per transformacions biracionals definides per equacions amb coeficients racionals.

Un punt racional de la corba és una solució (x, y) de l'equació amb $x, y \in \mathbb{Q}$. Si denotem per $C(\mathbb{Q})$ el conjunt de punts racionals de la corba, és clar que el conjunt $C(\mathbb{Q})$ és invariant per transformacions biracionals racionals i, per tant, el problema diofantí de la determinació de $C(\mathbb{Q})$ cau dintre d'aquesta aritmètica de la corba de Hilbert i Hurwitz. Per *invariant* vull dir simplement que si tenim una transformació biracional entre dues corbes:

$$C \to C', \quad (x, y) \to \left(\frac{p(x, y)}{q(x, y)}, \frac{u(x, y)}{v(x, y)}\right),$$

i els polinomis involucrats tenen tots coeficients racionals, aleshores la transformació envia $C(\mathbb{Q})$ a $C'(\mathbb{Q})$.

Una primera conseqüència important d'aquest nou punt de vista és que els problemes diofantins $f(X, Y) = 0$ han de ser classificats segons el *gènere* de la corba corresponent i no segons el grau de $f(X, Y)$ com es feia fins aleshores. El gènere d'una corba és un nombre natural $g \geq 0$. És un invariant biracional que mesura la complexitat de la geometria de la corba. Les corbes de gènere zero són les biracionalment equivalents a la recta projectiva $\mathbb{P}^1$. Per tant, la resolució del problema diofantí per a aquestes corbes es redueix a explicar un isomorfisme biracional (racional) amb $\mathbb{P}^1$, el qual ja proporciona una parametrització del conjunt de punts racionals. Per exemple, la corba $Y^2 = X^3$, tot i ser una cúbica, és de gènere zero i l'equivalència biracional:

$$\mathbb{P}^1 \to C, \quad t \to (t^2, t^3),$$

ens proporciona (per a valor finits de t) una parametrització de $C(\mathbb{Q})$.

Evidentment, el nou punt de vista suggereix també treballar preferentment amb varietats projectives, que tindran invariants geomètrics globals interessants. Així per exemple, l'estudi d'(1) requerirà treballar amb l'equació (2), que representa una corba del pla projectiu. Noteu que el concepte de punt de l'espai projectiu en coordenades homogènies ja comporta la identificació de solucions homotètiques que ens interessava i permet també no haver de distinguir més entre solucions racionals i solucions enteres (de l'equació (2)). Noteu també que aquest punt de vista permet tractar el problema de trobar les solucions racionals d'(1), però no pas les seves solucions enteres!

Com passa sempre amb les veritables revolucions, això fou només el principi. El principi d'una època de canvis revolucionaris en aritmètica, i també de canvis revolucionaris en geometria algebraica. La història d'aquests canvis té dos protagonistes indiscutibles: André Weil i Alexander Grothendieck. Al meu parer, dos dels més grans matemàtics de tots els temps, per la influència tan profunda que exerceixen les seves idees en camps molt diversos de la matemàtica. No puc fer cap repàs mínimament digne de les seves contribucions en elpoc temps que tinc. Em vull limitar a il·lustrar amb algun exemple concret la forta influència que s'han exercit mútuament l'aritmètica i la geometria algebraica. Per fer-ho he decidit centrar-me en la figura d'André Weil a qui, en certa manera, està dedicada aquesta conferència.

André Weil

André Weil neix a París el 1906. Estudia a l'Escola Normal Superior i ja en la seva època d'estudiant queda fortament impressionat amb la lectura de dos autors: Riemann i Fermat. Somnia la possibilitat d'aplicar la potència extraordinària de les idees de Riemann a les qüestions diofantines i aquesta obsessió no l'abandona en tota la seva vida científica posterior.

El 1928 llegeix la seva tesi doctoral: *L'aritmétique sur les courbes algébriques* [We, p. 11]. És una obra cabdal en la història de la geometria algebraica aritmètica, on introdueix tècniques que avui en dia considerem bàsiques, com la tècnica de les altures o la de les distribucions. L'objectiu principal de la tesi és provar el que coneixem avui com a:

TEOREMA DE MORDELL-WEIL. *Si* $C|_{\mathbb{Q}}$ *és una corba projectiva no-singular de gènere* $g \geq 1$ *i* $C(\mathbb{Q}) \neq \phi$, *aleshores* $J_C(\mathbb{Q})$ *és un grup commutatiu finit-generat.*

JC és una variant de dimensió g anomenada la *varietat jacobiana* de C. És la varietat dels *sistemes de g punts* de la corba, en el llenguatge clàssic. Hi ha una addició natural entre els punts complexos de la jacobiana que fa que tinguin una estructura de grup commutatiu. Si la corba C està definida sobre $\mathbb{Q}$, l'addició de punts racionals de J_C torna a proporcionar punts racionals, de manera que $J_C(\mathbb{Q})$ és un subgrup. L'afirmació interessant del teorema de Mordell-Weil és, per tant, la finita-generació d'aquest subgrup.

Resolt per Hilbert i Hurwitz el problema diofantí de la determinació dels punts racionals de corbes de gènere zero, el cas de gènere 1 fou estudiat per Poincaré. Les corbes de gènere 1 tenen una addició natural de punts (coincideix la corba amb la jacobiana) i, en un treball de 1901 [Po], Poincaré introdueix el concepte de *rang* de la corba com el nombre mínim de punts racionals necessari per generar tots els altres punts racionals mitjançant addició. En el mateix treball Poincaré s'adona que l'estudi de corbes de gènere superior exigeix treballar amb els *sistemes de g punts*. El 1922 Mordell provà que el rang d'una corba de gènere 1 és sempre finit, i Weil generalizà

aquest resultat a gènere qualsevol (i per a corbes definides sobre un cos de nombres arbitrari).

La intenció inicial de Weil era la de provar en la seva tesi la:

CONJECTURA DE MORDELL (1922). *$C_{|\mathbf{Q}}$ té gènere $\geq 2 \Rightarrow C(\mathbb{Q})$ és finit.*

Com que la corba viu dins la seva jacobiana, $C \hookrightarrow J_C$, Weil pensà que quan la dimensió de J_C és estrictament més gran que 1, només un nombre finit dels punts del grup finitament-generat $J_C(\mathbb{Q})$ podien «caure» a C. No obstant això, la idea fou insuficient i no pogué derivar la finitud de $C(\mathbb{Q})$ de la finita-generació de $J_C(\mathbb{Q})$. Hadamard, com a supervisor de la tesi, li aconsellà «que no publiqués un treball a mitges», però Weil no li va fer cas i va donar la seva tesi per acabada preveient la profunditat del problema: «*We face here a series of important and difficult problems whose solution will perhaps require the efforts of more than one generation.*» [We, p. 126]. Avui podem jutjar que obrà encertadament, perquè la conjectura de Mordell no ha pogut ser provada fins al 1983 per G. Faltings [Fal], utilitzant tècniques ben allunyades de l'abast de Weil en aquella època.

Aquest resultat de Weil és un avenç important, però no constitueix de cap manera la revolució anunciada. Mentre ens movem amb cossos de característica zero no calen modificacions essencials de les tècniques clàssiques per adaptar-les als problemes aritmètics. No passa el mateix, però, quan volem treballar amb varietats definides sobre un cos de característica positiva. La qüestió és: volem treballar en característica positiva? La resposta: i tant que volem!

És un principi ben clàssic que es pot obtenir informació interessant sobre una equació diofantina estudiant les diferents equacions obtingudes reduint mòdul els diferents nombres primers. I reduint mòdul un primer passem a obtenir equacions definides sobre un cos finit. Què vol dir en aquest cas «estudiar» l'equació? Essencialment: *comptar el nombre de solucions*. Això ens porta, doncs, de manera natural, a considerar també aquest problema com a genuïnament diofantí. Remarco que no és pas un problema colateral o «en sintonia» amb el nostre planteig inicial, sinó ben al contrari: les dades del nombre de solucions d'una equació mòdul els diferents primers es poden recollir en un objecte global, la L-sèrie de l'equació; és una funció de variable complexa que conté informació precisa sobre les solucions enteres de l'equació.

Geometria sobre cossos finits: les conjectures de Weil

La funció zeta d'una varietat definida sobre un cos finit és l'objecte més adequat per tractar les qüestions que facin referència al «nombre de punts» de la varietat. Considerem per simplicitat el cas d'una corba projectiva i no singular C definida sobre el cos $\mathbb{F}_p$ de p elements. La funció zeta de C és la següent sèrie formal en una indeterminada t:

$$Z(C,t) = \exp\Big(\sum_{1}^{\infty} \frac{1}{n} \sharp C(\mathbb{F}_{p^n}) t^n\Big) \in \mathbb{Z}[[t]].$$

Aquesta definició s'entén millor si sabem que $Z(C,t)$ admet una expressió com a producte infinit:

$$Z(C,t) = \prod_{x \in C} \frac{1}{1 - t^{\deg(x)}},$$

on x recorre els «punts tancats» de C. En aquesta expressió endevinem una similitud amb la funció zeta de Riemann. Si substituïm els punts tancats x de C pels nombres primers q (que són els punts tancats de $\mathrm{Spec}(\mathbb{Z})$), considerem que el grau és sempre 1 i canviem t per q^{-s}, on considerem s ara com una variable complexa, obtenim el producte infinit d'Euler, que convergeix a la funció zeta de Riemann a la regió $\mathrm{Re}(s) > 1$:

$$\prod_{q} \frac{1}{1 - q^{-s}} = \sum_{1}^{\infty} \frac{1}{n^s} = \zeta(s), \quad \mathrm{Re}(s) > 1.$$

Aquesta analogia és només formal. La funció zeta $Z(C, t)$ és un objecte infinitament més senzill i transparent que $\zeta(s)$. Una aplicació elemental del teorema de Riemann-Roch permet provocar que $Z(C, t)$ és una funció racional:

$$Z(C,t) = \frac{(1 - \alpha_1 t) \cdot \ldots \cdot (1 - \alpha_{2g} t)}{(1 - t)(1 - pt)},$$

on g és el gènere de C i els α_i són nombres complexos.

Aquesta funció zeta fou introduïda per Artin a la seva tesi. En analogia amb la funció zeta de Riemann, Artin formulà també una *hipòtesi de Riemann*. La hipòtesi de Riemann clàssica preveu que els zeros no trivials de $\zeta(s)$ han de tenir forçosament $\mathrm{Re}(s) = \frac{1}{2}$. Si pensem que l'analogia formal amb $Z(C, t)$ s'ha obtingut fent $t = p^{-s}$, la hipòtesi de Riemann es tradueix en: $|\frac{1}{\alpha_i}| = p^{-1/2}$ o equivalentment en : $|\alpha_i| = p^{1/2}$.

La relació $\#C(\mathbb{F}_{p^n}) - 1 - p^n = \sum_i \alpha_i^n$ ens fa veure com la hipòtesi de Riemann té una conseqüència immediata sobre el nombre de punts:

$$\left|\#C(\mathbb{F}_{p^n}) - 1 - p^n\right| \leq 2gp^{n/2}.$$

Dóna una fórmula asimptòtica universal, amb una estimació precisa del terme d'error.

Weil va tenir una idea genial per provar la hipòtesi de Riemann per a corbes. El nombre $\#C(\mathbb{F}_p)$ coincideix amb el nombre de punts fixos del morfisme de Frobenius:

$$C \longrightarrow C, \quad (x_1, \cdots, x_n) \mapsto (x_1^p, \cdots, x_n^p).$$

I si pensem aquest morfisme com una correspondència de C en si mateixa, el nombre de punts fixos ha de coincidir amb el nombre d'intersecció de la correspondència amb la diagonal. Amb aquesta filosofia, Weil va dissenyar un procediment per obtenir la hipòtesi de Riemann com una conseqüència de la desigualtat de Castelnuovo.

admetent que fos possible desenvolupar una teoria de les correspondències per varietats sobre cossos finits amb propietats anàlogues a la teoria clàssica. Aquesta genial intuïció fou concebuda a la presó de Rouen, on s'hi va estar quatre mesos l'any 1940 «per discrepàncies amb les autoritats militars». L'any següent s'instal·là a Princeton. Hermann Weyl, aleshores *chairman* de l'IAS, en assabentar-se de les circumstàncies en les quals Weil havia desenvolupat les seves idees, li oferí la seva influència perquè el portessin a la presó per tal que pogués finalitzar el seu treball amb les mateixes condicions, que li havien resultat tan productives.

Els anys següents, a Princeton, Weil es dedica amb intensitat a la teoria d'intersecció per varietats en característica positiva. Fou aquesta una tasca extremament delicada que el portà a reconsiderar tots els mètodes clàssics. En paraules del mateix Weil extretes de les seves *Obres completes*:

«*A rewriting of the whole theory (of correspondences of Severi) is a necessary preliminary to the applications we have in view.*»

«*... je commençais à apercevoir qu'une notable partie de la géometrie italienne reposait exclusivement sur la théorie des intersections.*»

«*Je voyais bien que, pour s'assurer de la validité des methodes italiennes en caracteristique p, toutes les foundations seraient à reprendre.*»

Aquesta refundació de la geometria algebraica culmina el 1946 amb l'aparició de les seves famoses *Foundations of Algebraic Geometry* [We2]. Weil hi redefineix els principis més bàsics de la geometria algebraica per tal de poder fer geometria sobre un cos arbitrari. Desenvolupa la teoria de la intersecció fins a un punt que li permet provar la hipòtesi de Riemann per a corbes definides sobre un cos finit. També trobem a les *Foundations* la primera definició de varietat abstracta, imitant la definició intrínseca de la varietat diferenciable. Això li permet construir, també per primera vegada, la jacobiana d'una corba definida sobre un cos arbitrari; és obtinguda com una varietat abstracta i desconeix si es pot submergir en un espai projectiu, qüestió que fou provada afirmativament per Chow l'any 1950.[2]

El 1949 Weil publica un altre article fonamental: «Number of solutions of equations in finite fields» [We, p. 399]. En ell prova que la funció zeta de les varietats definides per equacions de la forma:

$$a_1 X_1^{n_1} + \cdots + a_r X_r^{n_r} = b,$$

tenia propietats anàlogues a la de la funció zeta de les corbes, i formula les seves cèlebres conjectures. Si q és una potència de p i $V_{|\mathbb{F}_q}$ és una varietat projectiva no singular de dimensió n, Weil preveu:

CONJECTURES DE WEIL

W1. La funció zeta, Z(V, t) és racional:

$$Z(V,t) = \frac{P_1(t) \cdot \ldots \cdot P_{2n-1}(t)}{P_0(t) \cdot \ldots \cdot P_{2n}(t)}, \quad P_r(t) = \prod_{i=1}^{b_r} (1 - \alpha_i^{(r)} t).$$

W2. $Z(V, t)$ satisfà l'equació funcional:

$$Z(V, \frac{1}{q^n t}) = \pm q^{n\chi/2} t^{\chi} Z(V, t),$$

on χ és la característica d'Euler-Poincaré de V (nombre d'intersecció de la diagonal $V \times V$ amb ella mateixa).

W3. Hipòtesi de Riemann: $|\alpha_i^{(r)}| = p^{r/2}$.

W4. Els nombres b_r, anomenats els «nombres de Betti» de V, han de satisfer la relació usual: $\chi = \sum_r (-1)^r b_r$. *Si existeix una varietat projectiva i no-singular V_0 definida sobre un cos de nombres tal que V és isomorfa a la reducció de V_0 mòdul algun ideal, aleshores els b_r han de coincidir amb els nombres de Betti usuals de $V_0 \otimes C$.*

Ens trobem davant d'una altra de les genials intuïcions de Weil: si imaginem la varietat definida per la reducció mòdul un primer d'unes equacions amb coeficients enters, la complicació de la topologia de la varietat complexa que defineixen aquestes mateixes equacions té una influència ben precisa en el nombre de solucions mòdul p.

Geometria sobre anells

Aquestes conjectures, juntament amb la conjectura de Mordell, guien l'activitat de recerca en aritmètica durant els 40 anys següents. Per a la seva resolució fou necessari que la geometria algebraica patís una altra revolució fonamental: una nova refundació, duta a terme per A. Grothendieck a la fi dels anys 50 inspirat en idees de J. P. Serre.

L'objectiu essencial del nou punt de vista introduït per Grothendieck era fer geometria sobre un anell i no necessàriament sobre un cos [GroDi][Gro]. Això comportà, altra vegada, una revisió completa dels principis més bàsics. Les varietats algebraiques cedeixen el rol «d'objecte bàsic d'estudi» als esquemes. En certa manera, el treball de Grothendieck dóna vida a la idea de Kronecker de desenvolupar una branca de la matemàtica que contingui la teoria de nombres i la geometria algebraica com a casos especials.

La nova geometria s'imposa lentament gràcies als éxits en el tractament de problemes on els mètodes anteriors havien fracassat o mostrat la seva insuficiència. Mencionem el tractament de l'esquema de Picard, de l'esquema de Hilbert i, evidentment, la prova de les conjectures de Weil.

Grothendieck mateix provà totes les conjectures,[3] excepte la hipòtesi de Riemann, utilitzant, en el marc dels esquemes, una de les seves invencions més notables: la *cohomologia étale*. Sens dubte una de les joies més importants que ha aportat l'aritmètica a la matemàtica. Amb l'esperit bíblic del títol de la conferència es pot ben dir que amb l'aparició de la *cohomologia étale* l'aritmètica va cabar la seva travessia pel desert.

Grothendieck formulà també unes conjectures sobre cicles algebraics (sempre teoria de la intersecció!) que implicarien la hipòtesi de Riemann, però aquestes conjetures són d'una profunditat extraordinària i romanen sense provar. No obstant això, l'any 1973 Pierre Deligne [De] culmina el programa de Grohtendieck provant la hipòtesi de Riemann, tot utilitzant, d'una manera especialment brillant i imaginativa, tècniques de *cohomologia étale*.

D'altra banda, ja he mencionat que la conjectura de Mordell fou provada per Faltings el 1983, utilitzant també els mètodes de Grothendieck en tota la seva extensió.

Geometria d'Arakelov

Una nova geometria, encara? per què?

D'entrada cal observar que només per a corbes tenim resultats plenament satisfactoris, mentre que la nostra comprensió de les propietats aritmètiques de varietats de dimensió superior és molt més limitada.

Però, fins i tot per a corbes! Els mètodes geomètrics només funcionen satisfactòriament per varietats completes (projectives). Així, ens poden proporcionar informació sobre les solucions racionals (i enteres) de (2) i per tant sobre les solucions racionals d'(1), però no sobre les solucions enteres d'(1)! Per exemple, per provar que l'equació (1) té exactament les 22 solucions:

$$(x, \pm y) = (-2, 1), (-1, 2), (0, 1), (2, 1), (3, 4), (4, 7), (10, 31)$$
$$(12, 41), (20, 89), (114, 1217), (1274, 45473),$$

calen mètodes d'aproximació diofantina [Tza-deWe]. Amb aquestes tècniques, C. L. Siegel provà el 1929 que tota corba afí de gènere positiu té un nombre finit de solucions enteres [Sie]. No és possible cap demostració «geomètrica» d'aquest resultat . . . si no és en el context de la geometria d'Arakelov.

Però, fins i tot per a corbes projectives! L'equació de Fermant:

$$X^n + Y^n = Z^n,$$

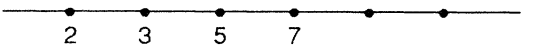
és una corba projectiva no-singular de gènere > 1 si $n > 3$. La prova de Faltings de la conjectura de Mordell ens perment assegurar que, per a cada n, la corba té només un nombre finit de punts racionals. Però això no resol encara l'enigma de Fermat, qui afirmà que només n'hi ha tres: $(X, Y, Z) = (1, 0, 1), (0, 1, 1)$ i $(1, -1, 0)$, si n és senar (i només els dos primers si n és parell).

Tenim, doncs, una qüestió pendent: l'EFECTIVITAT. Un criteri per decidir si una equació té un nombre finit o infinit de solucions i, en el primer cas, un procediment per obtenir cotes efectives per la dimensió de les solucions. La geometria de Grothendieck és insuficient per obtenir aquesta mena de resultats, entre d'altres coses perquè no és capaç de desenvolupar una teoria de la intersecció per a varietats definides sobre $\mathbb{Z}$.

Idea germinal de la teoria d'Arakelov: Weil 1939

Des del punt de vista geomètric, $\mathbb{Z}$ és un objecte anàleg a una corba sobre un cos finit. Ja hem observat traces d'aquest fenomen quan comparàvem les respectives funcions zeta.

Expliquem amb més detall aquesta analogia. L'objecte geomètric associat a l'anell $\mathbb{Z}$ és l'esquema Spec($\mathbb{Z}$). Com a espai topològic, Spec ($\mathbb{Z}$) és el conjunt d'ideals primers de $\mathbb{Z}$ amb la topologia de Zariski: els tancats no-trivials són els conjunts finits de punts que no contenen el punt corresponent a l'ideal primer «zero». Es pot representar com una sèrie de punts sobre una línia, sent representat el punt «zero» per la mateixa línia que uneix tots els punts. Aquesta imatge reflecteix el fet que el «zero» és un punt genèric de Spec($\mathbb{Z}$), és a dir, la seva ahereència és tot l'espai.



Així és com Spec($\mathbb{Z}$) és imaginat com una corba pels aritmètics. Valesn per a aquesta corba els resultats clàssics que es tenen per a corbes definides sobre un cos? No. No podem ni tan sols aspirar a aplicar-hi les técniques clàssiques ja que és una corba no completa. És una corba afí i, per tant, mancada d'invariants globals interessants. Una idea molt antiga, formulada amb precisió per Weil el 1939 [We, p. 236], és la de completar-la afegint els *primers de l'infinit*.

De la mateixa manera com els punts del model projectiu no-singular d'una corba estan en correspondència bijectiva amb les valoracions del cos de funcions, el model «complet i no-singular» de Spec($\mathbb{Z}$) hauria de tenir els punts que corresponen als valors abosults no-arquimedians de $\mathbb{Q}$, un per a cada nombre primer, i un punt més, corresponent al valor absolut $|\ |$ ordinari. Imaginant la corba completa amb l'afegit formal d'aquest punt de l'infinit, Weil provà una versió feble del teorema de Riemann-Roch per Spec($\mathbb{Z}$) (de fet, per a l'anell d'enters d'un cos de nombres). El problema de Riemann-Roch consisteix a estudiar l'existència de funcions amb zeros i pols prefixats. Sobre Spec($\mathbb{Z}$), estudia l'existència de «funcions» $x \in \mathbb{Q}$ amb divisibilitat prefixada per un nombre finit de primers i amb condicions de dimensió per a $|x|$.

El paper de Weil sobre el significat d'aquestes idees ens mostra altre cop la seva capacitat visionària [We, p. 447]:

«... *if we apply this idea to an algebraic number field (also a onedimensional problem), we obtain satisfactory formulations for global theorems, entirely analogous to the theorems on algebraic curves, provided we allow for «archimedean» valuations with somewhat weaker properties than those of algebraic geometry and that the p-adic valuations on number fields, viz., those for which the completed field is the field of real or that of complex numbers. Thus it appears that algebraic geometry over the complex number-field is, after all, a legitimate object o study, no less neces-*

sary or useful than geometry over p-adic fields; and so the door is open to toplogy, function-theory, differential geometry, and partial differential equations.»

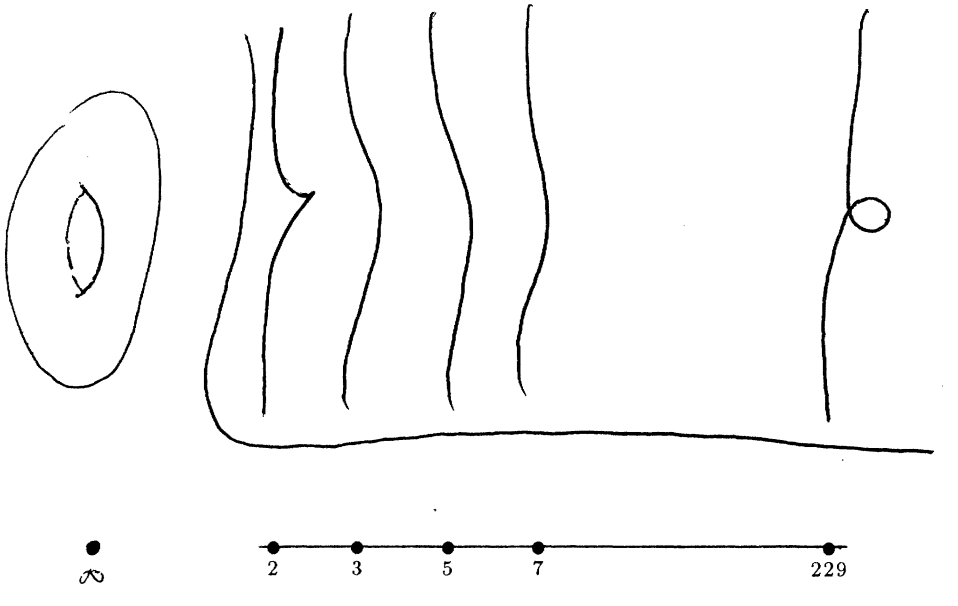
Intersecció sobre superfícies aritmètiques

Aquesta filosofia fou estesa per Arakelov el 1974 [Ar] al cas de corbes definides sobre $\mathbf{Z}$, p. e. el que els aritmètics anomenen *superfícies aritmètiques*. Una corba com (1) és en llenguatge geomètric una «fibració» sobre la «corba» Spec($\mathbf{Z}$):

$$C := \mathrm{Spec}(\mathbf{Z}[X, Y]/Y^2 - X^3 + 4X - 1) \to \mathrm{Spec}(\mathbf{Z})$$

Parlem d'una *superfície* perquè les fibres són corbes. La fibra en el punt p és isomorfa, com a esquema, a la corba sobre el cos finit $\mathbf{F}_p$ determinada per la reducció d'(1) mòdul p. La fibra en el punt genèric és isomorfa a la corba sobre $\mathbf{Q}$ determinada per la mateixa equació (1). Aquesta és la manera de visualitzar les varietats sobre $\mathbf{Z}$: són famílies de varietats sobre cossos, però de diferent característica!

Completar C significa, d'una banda, considerar la clausura projectiva de la varietat (p. e. la varietat definida per (2)) i, de l'altra, afegir formalment una fibra C_∞ sobre el punt de l'infinit de Spec($\mathbf{Z}$). Aquesta fibra ha de ser la superfície de Riemann compacta associada a la corba sobre $\mathbf{C}$ determinada per (1). Tenim, doncs, una part finita i una infinita en les varietats, i la filosofia de la geometria d'Arakelov consisteix a analitzar la varietat utilitzant geometria algebraica sobre la part finita i geometria diferencial sobre la part infinita d'una manera simultània.



Arakelov materialitzà aquesta filosofia desenvolupant una teoria d'intersecció per a superfícies aritmètiques. Els objectes geomètrics han de ser dotats de *mètriques a l'infinit*. Un fibrat d'Arakelov consisteix a donar un fibrat vectorial E sobre C i una mètrica hermitiana sobre el fibrat vectorial $E \otimes C$ sobre C_∞ induït de manera natural per E. Un divisor d'Arakelov és una combinació formal amb coeficients enters de subvarietats irreductibles de C, però comptant també la fibra C_∞ com una d'aquestes subvarietats i admetent que el seu coeficient sigui un nombre real. Un divisor d'Arakelov, D, ha de donar lloc a un fibrat de línia d'Arakelov, $O(D)$. La metrització de $O(D)$ cal fer-la d'una manera coherent, en variar el divisor. Això s'aconsegueix mitjançant la utilització d'una funció de Green adequada. Les funcions de Green són funcionals:

$$g : C_\infty \times C_\infty \longrightarrow \mathbb{C},$$

amb singularitats logarítmiques al llarg de la diagonal, associades a certs operadors diferencials. Amb aquests ingredients, Arakelov reïx a definir un aparellament d'intersecció amb valors reals:

$$(D, D') \mapsto D \cdot D' \in \mathbb{R},$$

amb propietats anàlogues a les de l'aparellament d'intersecció clàssic de les superfícies complexes. Faltings [Fa2] prossegueix aquesta línia provant alguns dels resultats clàssics de superfícies complexes: teorema de Riemann-Roch, teorema de l'índex de Hodge, fórmula d'adjunció, per a superfícies aritmètiques.
Aquesta geometria d'Arakelov ens acosta a l'efectivitat desitjada en la mesura que proporciona eines que permeten adquirir un cert control sobre la dimensió de les solucions. Com a il·lustració d'aquest fet mencionaré simplement que, per unes idees de Parshin, la prova per a superfícies aritmètiques de la desigualtat entre classes de Chern:

$$c_1^2 \leq 3c_2,$$

implicaria el teorema de Fermat asimptòtic, p. e. que la família d'equacions: $X^n + Y^n = Z^n$, $n > 2$, té en conjunt només un nombre finit de solucions no-trivials. L'any 1977 fou provada aquesta desigualtat per a superfícies complexes de tipus general per Miyaoka i Yau independentment (versions més febles havien estat provades abans per Van de Ven i Bogomolov). La prova recent (i falsa) del teorema de Fermat anunciada per Miyaoka passava per la convicció (errònia) d'haver provat aquesta desigualtat en el cas aritmètic.

Epíleg

H. Gillet i C. Soulé han elaborat en els darrers ays una proposta molt precisa de generalització de la geometria d'Arakelov a dimensions superiors. Diversos símptomes indiquen que podríem estar al davant de la versió definitiva de la geometria sobre $\mathbf{Z}$ que somniaven Kronecker i Weil. Almenys aquesta és l'opinió del mateix Weil. En una conversa recent amb Soulé, Weil li manifestà que aparentment la història li havia

reservat el mateix paper que a Moisès: després d'alliberar l'aritmètica de l'esclavitud dels mètodes clàssics i guiar-la en la seva travessia pel desert, li és permès d'arribar, ja ancià, a les mateixes portes de la terra promesa però, ben probablemet, s'haurà de quedar sense veure-la.

Referències

[Ar] S. Arakelov, Intersection theory of divisors on an arithmetic surface, Izv. Akad. Nauk. SSSR, Ser. Mat. 38 (1974); AMS Translations 8 (1974).

[Hi-Hu] D. Hilbert - A. Hurwitz, Über die diophantischen Gleichungen vom Geschlecht Null, Acta Math. 14 (1890).

[De] P. Deligne, La conjeture de Weil I, II, Publ. Math. IHES 43 (1974), 52 (1980).

[Fa1] G. Faltings, Endilichkeitssätze für abelsche Varietäten über Zahlkörpern, Inv. Math. 73 (1983).

[Fa2] G. Faltings, Calculus on arithmetic surfaces, Ann. of Math. 119 (1984).

[Gro-Di] A. Grothendieck - J. Dieudonné, Élements de Géométrie Algébrique, Publ. Math. IHES 8 (1961), 11 (1961), 17 (1963), 20 (1964), 24 (1965), 28 (1966), 32 (1967).

[Gro] A. Grothendieck et al., Séminaire de Géométrie Algébrique, Lecture Notes in Mathematics 224, 225, 269, 270, 288, 305, 340, 569, 589, Springer Verlag.

[Po] H. Poincaré, Sur les propriétés arithmétiques des coures algébriques, J. de Liouville 7 (1901).

[Sie] C. l. Siegel, Über einige Anwendungen diophantischer Approximationen, Gesammelte Abhadlungen, Vol. I, Springer Verlag, New York-Heidelberg-Berlin, 1966.

[Tza-deWè] N. Tzanakis - B. M. M. de Weger, On the practical solution of the Thue equation, J. Number Theory 31 (1989).

[We2] A. Weil, Collected papers, Vol. I, Springer Verlag, New York-Heidelberg-Berlin, 1979.

[We2] A. Weil, Foundations of Algebraic geometry, AMS Colloq. Publ. Vol. XXIX, New York, 1946.

Notes

1. En la redacció d'aquesta nota he mantingut l'estil informal de l'exposició oral. El contingut ha estat dividit en diferents paràgrafs per facilitar-ne la lectura.

2. Amb aquesta refundació de la geometria algebraica es va superar en certa manera la polèmica entre l'escola italiana (Severi, Castelnuovo,...) i l'alemanya (Van der Waerden, Noether,...) sobre el rigor i la metodologia que havia d'utilitzar la geometria algebraica. Es va considerar, en contra del propi pensament de Weil expressat a la introducció de les Foundations, que l'algebra havia "guanyat", i el mètodes dels italians van quedar injustament arraconats.

3. La racionalitat de la funció zeta havia estat provada per Dwork utilizant anàlisi p-àdica. No obstant, la prova de Grothendieck d'aquest fet és la que permet una aproximació correcta al problema i obre el camí que menà a la seva completa resolució.