El mètode de Chabauty-Coleman

Xavier Xarles

14 de març de 2005

Introducció

L'any 1941, C. Chabauty [3] va desenvolupar un mètode que permetia demostrar la conjectura de Mordell (o teorema de Faltings) per a certes corbes de gènere superior a 1 sobre $\mathbb{Q}$, concretament per les que el grup de punts racionals de la jacobiana tenia rang menor que el gènere. Aquest resultat, àmpliament superat per la demostració de Faltings (i posteriorment les de Votja i Bombieri), ha resultat ser un dels pocs resultats aplicables per a trobar efectivament tots els punts de una corba donada i també, per a trobar cotes molt bones pel nombre de punts que una corba pot tenir. El mètode de Chabauty va ser "oblidat"durant un llarg període de temps fins que Robert Coleman va publicar a l'any 1985 un article on relacionava aquest mètode amb la integració p-àdica de corbes que ell mateix havia desenvolupat. Coleman va poder demostrar així que el resultat ens donava una cota molt bona per a les corbes verificant la condició de Chabauty, i va donar varis exemples de com utilitzar el mètode per a calcular tots els punts de certes corbes de gènere 2 (vegis l'exemple ?).

La idea darrera del mètode és relativament senzilla. Prenem C una corba de genere $g > 1$ definida sobre un cos de nombres, i suposem que el grup de Mordell-Weil de la jacobiana J de C té rang menor que el gènere. Prenem $\wp$ un primer de K i sigui $K_\wp$ el completat respecte aquest primer, amb anell d'enters $\mathcal{O}_\wp$. Aleshores $J(K_\wp)$ és un grup de Lie sobre $K_\wp$ de dimensió g, i per tant localment és un $\mathcal{O}_\wp$-mòdul finit generat de rang g. Considerem $J_\wp$ la clausura topològica (p-àdica) de $J(K_\wp)$ generada per $J(\mathbb{Q})$, i denotem per $r_\wp$ la seva dimensió com a subgrup de Lie p-àdic; per la condició de Chabauty sabem que $r_\wp < g$. Localment $J_\wp$ és un $\mathcal{O}_\wp$-mòdul finit generat de rang $r_\wp$.

Tenim que

$$C(K) \subseteq C(K_\wp) \cap J_\wp$$

i, d'altre banda, $C(K_\wp)$ és un subespai analític ($\wp$-àdic) de $J(K_\wp)$ de dimensió 1. Tenim així que $C(\mathbb{Q})$ està contingut en la intersecció d'un subespai analític amb un subgrup de Lie de dimensió $< g$, i per tant ha de ser finit (per "Bezout").

Veurem que aquest resultat, juntament amb el càlcul explicit de aquesta intersecció, es dedueix del teorema de Strassman, utilitzant grups formals (seguint el mètode de Chabauty) o bé integració p-àdica (seguint el mètode de Coleman).

Notació 1. *Fixem les notacions que farem servir tota l'estona. Denotarem per K un cos de nombres, amb anell d'enters $\mathcal{O}$. Sigui $\wp$ un primer de K (una plaça finita) sobre de p un nombre primer, i prenem $K_\wp$ la completació de K respecte $\wp$. Sigui $\mathcal{O}_\wp$ l'anell d'enters de $K_\wp$, amb cos residual k. Denotarem per π un uniformitzant de $\mathcal{O}_\wp$ i per $|\ |$ el valor absolut tal que $|p| = p^{-1}$; aleshores $|\pi| = p^{-1/e}$ on e és l'index de ramificació absolut de $K_\wp$. Per a tot objecte O definit sobre $\mathcal{O}_\wp$, posarem $\widetilde{O}$ la seva reducció a k.*

1 Grups formals i el mètode de Chabauty

Considerem A una varietat abeliana de dimensió g sobre un cos de global o un cos local K amb anell d'enters $\mathcal{O}$, i prenem $\mathcal{A}$ el seu model de Néron sobre $\mathcal{O}$. Considerem ara $\widehat{A}$ la completació formal respecte la secció zero de $\mathcal{A}$; és un esquema en grups formal llis i connex, i per tant es de la forma $\mathrm{Spf}(\mathcal{O}[[X_1, \cdots, X_n]])$. La operació de grup de $\widehat{A}$ ens dona una estructura de algebra de Hopf a $\mathcal{O}[[X_1, \cdots, X_n]]$, que ve determinada per una g-tuple de series formals $F := (F_1, \cdots, F_g)$ a $\mathcal{O}[[X_1, \cdots, X_n]]$ verificant les propietats ven conegudes dels grups formals de Lie. Anomenem F el grup formal (de Lie) associat a A.

Per exemple, si A és una corba el·líptica donada per una equació de Weierstrass minimal, aleshores el grup formal és el grup formal definit com al llibre del Silverman [11].

Exemple 1. *Prenem la corba C de gènere 2 donada per la equació hiperel·líptica*

$$Y^2 = F(X) := f_6X^6 + f_5X^5 + f_4X^4 + f_3X^3 + f_2X^2 + f_1X + f_0,$$

on els f_i són tots elements de K, $f_6 \neq 0$ i el discriminant de $F(X)$ és diferent de zero.

Sigui J la jacobiana de C; els seus punts K-racionals (a part del 0) és corresponent amb parelles $\{(x,y),(u,v)\}$ de punts de la corba, la parella definida sobre K, i $y \neq 0$ o bé $y = 0$ i $x \neq u$. Això vol dir que o bé els dos punts estan definits sobre K o bé estan definits sobre una extensió quadràtica de K i són conjugats sobre K.

Identifiquem C a dins de J com els punts de la forma $\{P,P\}$ (de fet aquesta aplicació no és injectiva doncs envia els punts de Weierstrass a 0). Tenim aleshores el següent resultat: un punt $\{(x,y),(u,v)\}$ de J és de C si i només si

$$(x+u)^2 - 4xu = 0.$$

Definim ara a_2 i a_1 com

$$a_2 := (G(x,u))y - G(u,x)v)/((x-u)^3)$$

$$a_1 := (H(x,u)y - H(u,x)v)/((x-u)^3)$$

on G i H són

$$\begin{aligned} G(x,u) := \quad & f_0 4 + f_1(x+3u) + f_2(2xu+2u^2) + f_3(3xu^2+u^3) \\ + \quad & f_4(4xu^3) + f_5 x(xu^3+3u^4) + f_6 2x(xu^4+u^5) \\ H(x,u) := \quad & f_0 2(x+u) + f_1 u(3x+u) + f_2 4xu^2 + f_3 xu^2(x+3u) \\ + \quad & f_4 2xu^3(x+u) + f_5 xu^4(3x+u) + f_6 4x^2u^5 \end{aligned}$$

Sigui ara

$$a_0 := (F_0 - 2yv)^2/((x-u)^4)$$

on F_0 és

$$F_0 := 2f_0 + f_1(x+u) + 2f_2xu + f_3(x+u)xu + 2f_4(xu)^2 + f_5(x+u)(xu)^2 + 2f_6(xu)^3.$$

Aleshores $s_1 := a_1/a_0$ i $s_2 = a_2/a_0$ ens donen un parell de paràmetres locals de J al voltant del zero.

Considerem ara $\{(x',y'),(u',v')\}$ un altre punt de J amb paràmetres locals $t1$ i $t2$. Aleshores els paràmetres locals de la suma $\{(x,y),(u,v)\} + \{(x',y'),(u',v')\}$ com a punts de J estan donats per un parell de series de potencies F_1 i F_2 en s_1, s_2, t_1 i t_2 amb coeficients a K (de fet a $\mathbb{Z}[f_0,\ldots,f_6]$).

La parella F_1 i F_2 ens dona el grup formal de J a $\mathcal{O}_\wp$ si p no divideix el discriminant de $F(X)$ (més en general, si l'equació ens dóna un model regular de la corba C).

Per exemple, els termes fins a grau 3 són

$$F_1 = s_1 + t_1 + 2f_4 s_1^2 t_1 + 2f_4 s_1 t_1^2 - f_1 s_2^2 t_2 - f_1 s_2 t_2^2 + \dots$$

$$F_2 = s_2 + t_2 + 2f_2 s_2^2 t_2 + 2f_2 s_2 t_2^2 - f_5 s_1^2 t_1 - f_5 s_1 t_1^2 + \dots$$

La relació entre el grup formal i els punts K-racionals quan K és un cos local és ven coneguda per a les corbes el·líptiques; un resultat similar és cert també en general. La següent proposició no és molt difícil de demostrar.

Proposició 1. *Suposem que K és un cos local, amb anell d'enters $\mathcal{O}_\wp$, ideal maximal $\wp$ i cos residual k, i sigui $\mathcal{A}$ el model de Néron de A. Considerem el morfisme reducció*

$$red : A(K) \cong \mathcal{A}(\mathcal{O}_\wp) \longrightarrow \mathcal{A}_k.$$

Aleshores el nucli del morfisme reducció és isomorf al grup de punts de F sobre $\mathcal{O}_\wp$, es a dir a $(\wp)^g$ amb l'estructura de grup donada per les series formals F_1, ..., F_g.

Recordem que tot grup formal de Lie sobre un cos de característica zero és isomorf al grup formal additiu; l'isomorfisme amb el grup formal additiu s'anomena el seu logaritme, i la seva inversa l'exponencial; venen donats per a series de potencies en g-variables.

Exemple 2. *En l'exemple anterior, el logaritme del grup formal construït venen donats fins a grau 3 per*

$$log \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} s_1 - \frac{2}{3}s_1^3 f_4 + \frac{1}{3}f_1 s_2^3 + \dots \\ s_2 - \frac{2}{3}s_2^3 f_2 + \frac{1}{3}f_5 s_1^3 + \dots \end{pmatrix}$$

Es poden trobar tots els termes fins a grau 7 al fitxer log del lloc ftp: ftp.liv.ac.uk/pub/genus2/jacobian.variety/

Per a simplificar l'exposició suposarem a partir d'ara que $A = J$ és la jacobiana d'una corba C que té gènere 2. Si el rang del grup de Mordell-Weil de J és zero, els punts K-racionals de C sols poden ser punts de torsió de J, que són fàcilment calculables. Per tant suposarem que el rang és

1, i que coneixem un generador D de $J(K)$ (en segons quins casos no és necessari conèixer un generador, sols cal un punt d'ordre infinit verificant certes condicions). Fixem també un primer $\wp$ de K de bona reducció per J.

Denotem per $\widetilde{D}$ la imatge de D per el morfisme reducció, i sigui m l'ordre de $\widetilde{D}$; aleshores $D' := mD$ està en el nucli del morfisme reducció. Tenim així que tot punt Q de $J(K)$ s'expressa de la forma $P = A + nD'$, on

$$A \in \mathcal{S} := \{B + iD \mid B \in J(K)_{tors} \text{ i } \ 0 \leq i \leq m-1\}$$

i $n \in \mathbb{Z}$. Ara, utilitzant el logaritme i l'exponencial del grup formal F tenim que el subgrup analític de $J(K_\wp)$ que conté $J(K)$ és igual a

$$J_\wp = \{A + \exp(N \log(D')) \mid A \in \mathcal{S} \text{ i } \ |N| \leq 1\}.$$

Així els punts de $C(K)$ estan continguts a $J_\wp$; de fet només cal considerar els $A \in \mathcal{S}$ tals que la seva reducció està a l'imatge de C dins J. Donat un tal A, definim per a cada N enter $\wp$-àdic el punt de J donat per

$$h_A(N) := A + \exp(N \log(D')).$$

Aquest punt l'expressem de la forma $\{(x, y), (u, v)\}$ i denotem per $\theta_A(N) := (x+u)^2 - 4xu$. Tenim que

$$\theta_A(N) = c_0 + c_1 N + c_2 N^2 + \cdots \in K_\wp[[N]],$$

on els coeficients c_i tendeixen a zero a $K_\wp$. Aquest coeficients es poden calcular en principi efectivament donats D' i A (i la corba C) mòdul $\wp^n$ per n tant gran com es vulgui. Per a fer-ho cal poder passar de l'expressió en els paràmetres locals a una expressió de la forma $\{(x, y), (u, v)\}$, el que no és gens fàcil en principi. Però Flynn a [6] i Cassels i Flynn a [2] ho fan utilitzant una immersió concreta de la corba en la varietat de Kummer.

A la pràctica només ens interessarà saber la valoració dels c_i, o com a mínim una cota prou bona d'aquesta valoració. Per això tenim el següent resultat del Flynn [6], Theorem 2.9.

Teorema 1. *Denotem per* $\delta := \max\{|s_1(D')| \ , \ |s_2(D')|\} \leq p^{-1/e}$, *i suposem que l'index de ramificació de* $K_\wp$ *sobre* $\mathbb{Q}_p$ *és menor que* $p-1$. *Aleshores*

$$|c_j| \leq \delta^j p^{(j-m)/(p-1)},$$

on m *és el minim grau de* $\theta_A(N)$ *respecte* N.

En resum: els punts P de C, identificats a dins de J com $\{P, P\}$, tals que la seva reducció mòdul $\wp$ sigui igual que la reducció de A es corresponent tots a zeros de la serie $\theta_A(N)$ dins de $\mathcal{O}_\wp$. Però les series de potencies convergents a la bola unitat tenen un nombre finit de zeros a la bola unitat, tal com es dedueix del següent resultat de Strassman.

Teorema 2. *Sigui $\theta(X) := c_0 + c_1X + c_2X^2 + \cdots \in K_\wp[[X]]$ tal que $c_i \longrightarrow 0$ a $K_\wp$, o sigui que $|c_i|_\wp \longrightarrow 0$ (aquesta es la condició necessària per tal que la serie convergeixi a $\mathcal{O}_\wp$). Definim k com l'únic enter que verifica que $|c_k|_\wp \geq |c_i|_\wp$ per a tot $i \geq 0$ i que $|c_k|_\wp > |c_i|_\wp$ per a tot $i > k$. Aleshores la serie $\theta(X)$ té com a molt k zeros a $\mathcal{O}_\wp$.*

La demostració del teorema no és difícil, i pot ser deduïda o bé de la teoria de polígons de Newton o bé del teorema de preparació de Weierstrass (formal o p-àdic).

Anem a explicar la estratègia per a trobar una cota per el nombre de punts, i, si hi ha sort, per a trobar-los tots.

Prenem $A \in \mathcal{S}$; si $red(A)$ no és un punt de la corba (i.e. no és de la forma $\{P, P\}$), és clar que cap punt de la corba pot reduir a A. Així sols cal considerar els punts que al reduir són de la corba.

Ara, si el propi A és de la corba, aleshores la serie de potencies té terme inicial 0:

$$\theta_A(N) = c_1N + c_2N^2 + \dots.$$

Si podem calcular la k tal que ens dona la cota de Strassman, tindrem que hi ha com a molt k punts de la corba amb reducció igual a la de A. Per a fer-ho sols ens cal calcular la valoració dels coeficients c_i fins a un i fixat que ens permeti acotar la valoració del reste de c_j's i calcular la k.

Per a la majoria dels punts de corbes que ens trobarem, tenim que les series $\theta_A(N)$ tenen sols un zero a $\mathcal{O}_\wp$. Per exemple, tenim el següent resultat.

Corol·lari 1. *Suposem que estem en les condicions del teorema de Flynn i que A és un punt de la corba C. Aleshores $\theta_A(N) = c_1N + c_2N^2 + \dots$. Suposem que $c_1 \neq 0$ i que a més $|c_1| = \delta < p^{-1/(p-1)}$. Aleshores A és l'únic punt de C que redueix a $\widetilde{A}$.*

Demostració. Pel teorema del Flynn, donat que $m = 1$, tenim que

$$|c_j| \leq \delta^j p^{(j-1)/(p-1)} < \delta p^{(-j-1)/(p-1)} p^{(j-1)/(p-1)} = \delta p^{-2/(p-1)} < \delta = |c_1|$$

i per tant $k = 1$ en el teorema de Strassman. □

Exemple 3. *Anem a intentar fer un exemple seguint l'article de Flynn. Prenem C la corba donada per l'equació:*

$$y^2 = F(x) = (x^2+1)(x^2+2)(x^2+2x+2).$$

Primer cal saber que el grup de Mordell-Weil està generat pels punts de 2-torsió (els punts de Weierstrass) i el punt $D := \{\infty^+, \infty^+\}$. Així la corba té rang 1.

Prenem p=3, doncs 3 no divideix el discriminant. Aleshores la reducció de D té ordre 5 i per tant

$$D' := 5D = \{(-1/2, 15/8), (-1/2, 15/8)\}$$

està en el nucli de la reducció.

Calculem els paràmetres locals de D' aplicant les formules donades: són $s_1 = 6225/22472$ i $s_2 = -555/11236$, i tenen valoració 1 en p=3. Així $\delta := |s_1| = |s_2| = 3^{-1}$.

Considerem el conjunt

$$\mathcal{S} := \{B + i \cdot D \mid B \in J(\mathbb{Q})_{tors} \quad i \quad 0 \leq i \leq 4\}.$$

Aquest conjunt té 20 elements, però sols 5 d'ells al reduir ens donen un punt de la forma $\{P, P\}$: $\{\infty^+, \infty^+\}$, $\{\infty^-, \infty^-\}$, $\{(0,2),(0,2)\}$, $\{(0,-2),(0,-2)\}$ i 0.

Prenem $A = \{\infty^+, \infty^+\}$; la idea és que es pot arribar a calcular $\theta_A(N)$ mòdul p^r per el r que ens faci falta. Flynn calcula que $\theta_A(N) = 3N (mod\ 9)$, i per tant $|c_1| = 3^{-1}$ i $|c_i| < 3^{-1}$ per a tot $i > 1$. Així sols tenim un punt P que redueix a $\widetilde{A}$. Com que ja en teniem un, $P = \infty^+$, ja estem.

De la mateixa manera es pot veure que sols hi ha un punt que redueixi a $\widetilde{A}$ per a $A \neq 0$ en la llista anterior.

Finalment, tractem el cas $A = 0$. En aquest cas tenim que $\theta_A(N) = c_6 N^6 + \ldots$ (sempre que estem en el cas $A = 0$ resulta que $m = 6$). Tenim que $|c_6| = 3^{-7}$ i per tant no podem concloure. Calculant més coeficients tenim que $|c_8| = 3^{-7}$ i d'aquí podem deduir, utilitzant el teorema de Flynn, que $|c_j| < 3^{-7}$ per a $j > 8$. Així tenim que $\theta_A(N)$ té com a molt 8 zeros; 6 corresponent a 0 (repetit). Ara bé, els punts $D' = \{(-1/2, 15/8), (-1/2, 15/8)\}$ i $-D' = \{(-1/2, -15/8), (-1/2, -15/8)\}$ també redueixen a 0 (corresponent a $N = 1$ i a $N = -1$). Per tant ja tenim els 8 zeros.

En resum:

$$C(\mathbb{Q}) = \{\infty^+, \infty^-, (0, \pm 2), (-1/2, \pm 15/8)\}.$$

2 Integració p-àdica

En l'article [5], Robert Coleman va introduir la integració p-àdica per poder donar cotes efectives del nombre de punts d'una corba de gènere ≥ 2 amb bona reducció en un primer p en funció del gènere i de p. La idea és interpretar el logaritme p-àdic en funció de l'integració de formes diferencials.

Considerem A una varietat abeliana sobre un cos p-àdic $K_\wp$; aleshores tenim un morfisme analític natural (pel fet de ser un grup de Lie p-àdic)

$$\log : A(K_\wp) \longrightarrow T_0(A)(K_\wp),$$

on $T_0(A)(K_\wp)$ denota l'espai tangent de A al 0. De fet aquest morfisme és un isomorfisme local i tenim una successió exacte

$$0 \longrightarrow A(K_\wp)_{tors} \longrightarrow A(K_\wp) \xrightarrow{\log} T_0(A)(K_\wp)$$

que ens dona un isomorfisme

$$\log\colon A(K_\wp) \otimes \mathbb{Q} \xrightarrow{\sim} T_0(A)(K_\wp).$$

Anem primer a determinar el morfisme log en termes de integració p-àdica. Per a fer-ho necesitem recordar que per a una varietat abeliana tenim un isomorfisme natural entre $T_0(A)(K_\wp)$ i el dual de l'espai de formes diferencials glodals $\Gamma(A, \Omega^1_{A/K_\wp})$ (o, dit d'una altre manera, entre l'espai cotangent i l'espai de formes diferencials globals). De fet, aquest resultat és cert també sobre l'anell $\mathcal{O}_\wp$ i el model de Néron $\mathcal{A}$ de A.

Així el morfisme logaritme ens determina un aparellament

$$\lambda\colon \Gamma(A, \Omega^1_{A/K_\wp}) \times A(K_\wp) \longrightarrow K_\wp.$$

Lemma 1. *Sigui $\omega \in \Gamma(A, \Omega^1_{A/K_\wp})$ una forma diferencial global. Aleshores hi ha un únic morfisme analític $\lambda_\omega\colon A(K_\wp) \to K_\wp$ tal que $d(\lambda_\omega) = \omega$.*

Demostració. És conegut que $d\omega = 0$, i per tant que localment al voltant del zero ω es la derivada d'un funció analítica. Concretament, si $z_1, \ldots, z_g$ és un sistema de coordenades local de A al 0, tenim una única serie de potencies $\lambda_\omega \in K_\wp[[z_1, \ldots, z_g]]$ tal que $\lambda_\omega(0) = 0$ i $d(\lambda_\omega) = \omega$ en certa bola oberta B al voltant del 0. A més podem suposar que B és un subgrup de A, i per tant d'index finit (és obert).

Usant que ω és invariant per translacions, podem veure que λ_ω és un morfisme de grups, i estendre la definició a tot $A(K_\wp)$ via la fórmula $\lambda_\omega(a) := \lambda_\omega(na)/n$, on $n := [A(K_\wp) : B]$. □

Notació 2. *És habitual denotar*

$$\int_a^b \omega := \lambda_\omega(b) - \lambda_\omega(a).$$

Aquesta integral compleix les propietats usuals de la integració.

Definim ara l'aparellament λ com $\lambda(\omega, a) := \lambda_\omega(a)$. És clar aleshores que l'aparellament és no degenerat a l'esquerra i que tenim les successions exactes anteriors.

Suposem ara que A/K és la jacobiana d'una corba C/K, i prenem una aplicació $f_D\colon C \to A$ donada per un divisor D K-racional de grau r (o sigui, $f_D(P) := [rP - D]$). Un resultat estàndar de la teoria de corbes ens diu que l'aplicació

$$f^* := \frac{1}{r} f_D\colon \Gamma(A, \Omega^1_{A/K_\wp}) \to \Gamma(C, \Omega^1_{C/K_\wp})$$

és un isomorfisme independent de D. Utilitzarem aquest morfisme per identificar les formes diferencials en A i en C.

Donada una forma diferencial η en C, prenem $\omega := f^{*-1}(\eta)$ i definim

$$\lambda_{\eta,D}(P) := \lambda_\omega([rP - D]).$$

De la mateixa manera, si P i Q són punts de $C(K_\wp)$, definim

$$\int_P^Q \eta := \lambda_{\eta,P}(Q) = \int_0^{[Q-P]} f^{*-1}\eta.$$

Aquesta integració coincideix, si C té bona reducció, amb la integració p-àdica de Coleman definida a [4] per a afinoïdes amb bona reducció utilitzant anàlisi rígida i el principi de continuació analítica al llarg del Frobenius de Dwork.

Tenim que $\lambda_{\eta,D}$ ens dona una funció analítica en C, amb diferencial $r\eta$. A més es pot calcular localment: si fixem Q_0 un punt de $C(K_\wp)$, tenim una bola oberta B de Q_0 i una coordenada local u tal que $\eta = F(u)du$ en B, on $F(u) \in K_\wp[[u]]$ convergeix a B. Aleshores la integral formal $G(u)$ de $rF(u)$ convergeix també a B i es igual a $\lambda_{\eta,D}$ fora d'una constant additiva. Aquesta constant es pot calcular fàcilment si $D = P$ és un divisor de grau 1 efectiu, i si P està a B: és igual a $-G(P)$, ja que $\lambda_{\eta,P}(P) = 0$.

El punt clau del càlcul efectiu està en el fet que podem prendre les boles B on $\lambda_{\eta,D}$ és representable per una serie de potencies convergent iguals a les classes de residus.

Notació 3. *Donat un esquema $\mathcal{X}$ propi sobre $\mathcal{O}_\wp$, amb fibra genèrica X sobre $K_\wp$ i fibra especial $\widetilde{\mathcal{X}}$, tenim un morfisme reducció*

$$red : X(\overline{K_\wp}) \longrightarrow \widetilde{\mathcal{X}}(\overline{k}).$$

Donat ara un punt $P \in X(\overline{K_\wp})$, denotarem per $B_P := red^{-1}(red(P))$, la classe de residus de P.

En general la classe de residus d'un punt P és un obert per a la topologia rígida analítica, i de fet és un obert afinoïde. En el cas que $\widetilde{\mathcal{X}}$ sigui no singular a P és de fet isomorf a una bola tancada. Per exemple, en el cas que $\mathcal{X}$ sigui el model de Néron d'una varietat abeliana i P sigui el 0, ja em vist aquest resultat.

Anem a veure que $\lambda_{\eta,D}$ és representable per una serie de potencies convergent en cada classe de residus si tenim que $\mathcal{X}$ és un model regular de X. La idea és que, multiplicant si cal η per un enter, podem suposar que η és un diferencial en el model $\mathcal{X}$, o sigui que $\eta \in \Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/\mathcal{O}_\wp})$, que és un $\mathcal{O}_\wp$ mòdul de rang 1. Aleshores, per la regularitat de $\mathcal{X}$, tot punt de X redueix a un punt no singular de $\widetilde{\mathcal{X}}$, i per tant la classe de residus és isomorf a una bola tancada. Prenem u un paràmetre local en la classe de residus, o sigui $u\colon B_P \to \wp\mathcal{O}_\wp$ ens dóna un isomorfisme analític. Així $\eta = F(u)du$ en la classe de residus i $F(u) \in \mathcal{O}_\wp[[u]]$. Per tant $\lambda_{\eta,D}$ és igual en aquesta bola a la integral formal $G(u)$ de $F(u)$, i per tant és de la forma

$$\lambda_{\eta,D} = c_0 + \sum_{i\geq 1} \frac{c_i}{i} u^i.$$

on $F(u) = \sum_{i\geq 1} c_i u^{i-1} \in \mathcal{O}_\wp[[u]]$ i c_0 és la constant d'integració.

Exemple 4. *Prenem C una corba hiperel·líptica donada per una equació del tipus $y^2 = f(x)$, on $f(x)$ és un polinomi sense arrels multiples de grau $2g+1$ o $2g+2$. Aleshores una base per les diferencials globals en C be donada per $\eta_i = \frac{x^i dx}{y}$ amb $i = 0 \ldots g-1$. Si prenem un punt (a,b) de C tal que $b \neq 0$, aleshores $x-a$ és un paràmetre local en (a,b) i podem expressar els diferencials η_i en funció de series en $x-a$: sols hem de calcular $1/y = 1/\sqrt{f}$ com a serie en $x-a$.*

Per exemple, a la corba

$$y^2 = -2x^5 + 4x^4 + 6x^3 - 4x^2 - 4x$$

tenim el punt $P = (-1/2, 3/4)$*, i denotant* $u = x + \frac{1}{2}$ *obtenim que*

$$\frac{1}{y} = \frac{1}{\sqrt{f(x)}} = \frac{4}{3} - \frac{20}{9}u + \frac{98}{9}u^2 - \frac{2738}{81}u^3 + \frac{66083}{486}u^4 - \frac{81923}{162}u^5 + \frac{5876989}{2916}u^6 -$$

$$-\frac{69679147}{8748}u^7 + \frac{2251499083}{69984}u^8 - \frac{246360165799}{1889568}u^9 + O(u^{10}).$$

Aleshores tenim que $\eta_i = f_i(u)du$ *al voltant de* P *amb* $f_0(u)$ *la serie anterior i*

$$f_1(u) = -\frac{2}{3} + \frac{22}{9}u - \frac{23}{3}u^2 + \frac{2251}{81}u^3 - \frac{98939}{972}u^4 + \frac{377935}{972}u^5 - \frac{8826217}{5832}u^6 +$$

$$+\frac{104941081}{17496}u^7 - \frac{3366365435}{139968}u^8 + \frac{367941116281}{3779136}u^9 + O(u^{10}),$$

on em utilitzat que $x = u - \frac{1}{2}$*.*

Observem que l'equació que em donat de la corba té bona reducció fora del 2 i el 3 (més encara, en el 2 i en el 3 no ens dona una equació regular). Així les series que em donat tenen coeficients a $\mathbb{Z}_p$ *per a tot primer* $p \neq 2, 3$*.*

Per a calcular $\lambda_{\eta_i,P}$ *sols cal integrar formalment les series anteriors (recordem que* $\lambda_{\eta_i,P}(P) = 0$ *i per tant la constant d'integració és zero).*

Observem finalment que podem calcular integrals a J si sabem calcular integrals a C. En efecte, si tenim $D = [\sum Q_i - \sum P_i]$ és un punt de J, aleshores

$$\int_0^D \omega = \sum \int_{P_i}^{Q_i} f^*\omega.$$

Per exemple, si $P \in C(K_\wp)$ és un punt de la corba, i tenim D un punt de la jacobiana amb reducció 0, podem aleshores escriure $D = [\sum_{i=1}^g Q_i - gP]$, on $red(Q_i) = red(P)$ per a tot i. Considerem η un diferencial i calculem $\lambda_{\eta,P} = c_0 + \sum_{j\geq 1} \frac{c_j}{j} u^j$, on u és un paràmetre local en P. Aleshores

$$\lambda_\eta(D) = \sum_{i=1}^g \lambda_{\eta,P}(Q_i) = c_0 + \sum_{j\geq 1} \frac{c_i}{i} s_i,$$

on

$$s_j = \sum_{i=1}^g u(Q_i)^j.$$

3 El mètode de Coleman

La idea del mètode, tal com ja em explicat, és la següent. Fixem una corba X sobre K un cos de nombres, i denotem per A la seva jacobiana. Prenem un primer $\wp$ de K i un model regular $\mathcal{X}$ de X sobre $\mathcal{O}_\wp$. Suposarem per simplificar l'exposició que $X(K_\wp) \neq \emptyset$ (si fos buit ja tindríem tots els punts K-racionals determinats!), i fixem D un divisor de grau 1 de $X/K_\wp$ (si voleu, determinat per un punt $K_\wp$-racional).

Veurem que si el rang del grup de Mordell-Weil de A és més petit que g, existeix una forma diferencial ω de $X/K_\wp$ tal que $\lambda_{\eta,D}$ s'anul·la a $X(K)$. Veurem que d'aquí podem determinar cotes molt bones per el nombre de punts i, fins hi tot, trobar-los tots.

Comencem primer per a definir un invariant més bo que el rang del grup de Mordell-Weil per el que ens interessa.

Definició 1. *Sigui A una varietat abeliana sobre un cos de nombres K i sigui $K_\wp$ la completació en un primer $\wp$. Definim el rank de Chabauty de A en $\wp$ com*

$$Chab(A, K, \wp) := \dim_{K_\wp}(\log(A(K)) \otimes_{\mathbb{Z}} K_\wp).$$

Observem que

$$\mathrm{Chab}(A, K, \wp) \leq \min\{g, \mathrm{rang}_{\mathbb{Z}}(A(K))\}$$

ja que la dimensió de l'espai tangent al zero com a $K_\wp$-espai vectorial és sempre g.

Ara, direm que A compleix la condició de Chabauty $\wp$ si $\mathrm{Chab}(A, K, \wp) < g$. El punt clau és que si A compleix la condició de Chabauty en $\wp$, aleshores existeix una (o més) forma diferencial $\eta \in \Gamma(A, \Omega^1_{A/K_\wp})$ tal que el morfisme $\lambda_\eta : A(K_\wp) \to K_\wp$ s'anul·la a $A(K)$, i per tant que $\lambda_{\eta,D}$ s'anul·la a $C(K)$. Suposarem d'ara en endavant que $\eta \in \Gamma(\mathcal{X}, \Omega^1_{\mathcal{X}/\mathcal{O}_\wp})$.

Exemple 5. *Considerem la corba anterior*

$$y^2 = -2x^5 + 4x^4 + 6x^3 - 4x^2 - 4x$$

i el punt $P = (-1/2, 3/4)$. Prenem el morfisme de C a J induït per P: $f_P(Q) := [Q - P]$.

El punt de la jacobiana $\{(0,0),P\}$ té ordre infinit i, junt amb la torsió, genera el grup de Mordell-Weil. Per a simplificar els càlculs prendrem enlloc d'aquest punt el punt

$$D := \{(0,0),P\} + \{\infty,(-1,0)\} = \{(-\frac{1}{2}+\frac{1}{2}\sqrt{-15},12),(-\frac{1}{2}-\frac{1}{2}\sqrt{-15},12)\}.$$

Considerem $p=5$, doncs la corba té bona reducció en p amb model donat per l'equació anterior. Aleshores $\widetilde{D}$ téordre 3, i per tant

$$D' = 3D = \{Q,Q'\}$$

on

$$Q = (\frac{-197}{10}+\frac{1}{10}\sqrt{34185},\frac{32652}{5}-\frac{4416}{125}\sqrt{34185})$$

i Q' és el seu conjugat de Galois.

Ara, volem expressar D' com $[R_1+R_2-2P]$, així que sumem

$$\{Q,Q'\}+\{P,P\} = \{(-\frac{1}{2}+\frac{1}{2}\sqrt{-15},-12),(-\frac{1}{2}-\frac{1}{2}\sqrt{-15},-12)\}.$$

Aleshores $R_1 = (-\frac{1}{2}+\frac{1}{2}\sqrt{-15},-12)$ i R_2 el seu conjugat. Ens interessen els nombres $u_1 = u(R_1) = x(R_1)+1/2 = \frac{1}{2}\sqrt{-15}$ i $u_2 = u(R_2) = -\frac{1}{2}\sqrt{-15}$.

Per a calcular $\lambda_{\eta_i,P}(D')$ per a $i=0,1$ el que farem es calcular primer les funcions elementals en u_1 i u_2, per a poder calcular després $s_j = u_1^j + u_2^j$ per a j's tant grans com calgui. Tenim $\sigma_1 = u_1+u_2 = 0$ i $\sigma_2 = u_1u_2 = \frac{15}{4}$, i per tant $s_j = 0$ si j és senar i $s_2 = -\frac{15}{2}$, $s_4 = \frac{225}{8}$, $s_6 = -\frac{3375}{32}$, $s_8 = \frac{50625}{128}$, etc.

Finalment podem substituir en les formules per $\lambda_{\eta_i,P}$ obtenides anteriorment integrant formalment f_i:

$$\lambda_{\eta_0,P}(D') = \frac{4}{3}s_1 - \frac{10}{9}s_2 + \frac{98}{27}s_3 - \frac{1369}{162}s_4 + \frac{66083}{2430}s_5 - \frac{81923}{972}s_6 + \frac{5876989}{20412}s_7 - \frac{69679147}{69984}s_8 + \frac{2251499083}{629856}s_9 - \frac{246360165799}{18895680}s_{10} + \dots$$

$$\lambda_{\eta_1,P}(D') = -\frac{2}{3}s_1 - \frac{11}{9}s_2 + \frac{23}{9}s_3 - \frac{2251}{324}s_4 + \frac{98939}{4860}s_5 - \frac{377935}{5832}s_6 + \frac{8826217}{40824}s_7 - \frac{104941081}{139968}s_8 + \frac{3366365435}{1259712}s_9 - \frac{367941116281}{37791360}s_{10} + \dots$$

Observem que els coeficients b_j de $\lambda_{\eta,P}$ tenen sempre valoració $v(b_j) = v(c_j) - v(j) \geq -v(j)$, ja que c_j són enters p-àdics. D'altre banda, com que

la valoració 5-àdica de σ_2 és 1 (i $\sigma_1 = 0$), la valoració de s_j és $j/2$ si j és parell. Per tant, per a calcular $\lambda_{\eta,P}(D')$ mòdul 5^r per un r fixat sols ens cal calcular la serie anterior fins a s_t, on $t := 2\sum_{i\geq 0}[r/5^i]$. Per exemple, per a calcular-ho mòdul 5^6 només ho hem de calcular fins a s_{10}. En aquest cas obtenim

$$\lambda_{\eta_0,P}(D') = 150908497330975/7962624 = 5^2 \cdot 11 (mod\ 5^6)$$

i

$$\lambda_{\eta_1,P}(D') = -225346728509665/15925248 = -5 \cdot 3 \cdot 2^5 (mod\ 5^6)$$

Per tant, el diferencial $\eta := 55\eta_1 + 96\eta_0$ verifica que $\lambda_{\eta,P}$ anul·la D' mòdul 5^6. Així podrem utilitzar la funció $\lambda_{\eta,P}$ per a veure que no hi ha cap més punt de $C(\mathbb{Q})$ que té la mateixa reducció que P. Tenim

$$\lambda_{\eta,P}(u) = \frac{274}{3}u - \frac{355}{9}u^2 + \frac{1871}{9}u^3 - \frac{139043}{324}u^4 +$$
$$\frac{7246291}{4860}u^5 - \frac{26401223}{5832}u^6 + \frac{642939953}{40824}u^7 -$$
$$\frac{7606636769}{139968}u^8 + \frac{247137725011}{1259712}u^9 - \frac{27064390437953}{37791360}u^{10} + O(u^{11})$$

En resum: aquesta serie anterior es convergent a la bola $5\mathbb{Z}_5$, i val zero en tots els u's que corresponen a punts $\mathbb{Q}$-racionals de la corba (que estan dins d'aquesta bola), o sigui els punts $\mathbb{Q}$-racionals que redueixen a P mòdul 5.

Pels altres punts, només cal calcular els zeros de la funció analítica $\lambda_{\eta,P}$, desenvolupant en serie en les altres classes de residus (boles) al voltant dels altres punts (el fet que tenim un punt racional a dins de cada classe de residus pot ajudar).

Fixem ara $P \in X(K_\wp)$ un punt i prenem $B = B_P$. La idea és acotar el nombre de zeros de $\lambda_{\eta,D}$ en B (que ens donarà una cota per el nombre de punts de $X(K)$ amb reducció $\widetilde{P}$). Recordem que

$$\lambda_{\eta,D} = c_0 + \sum_{i\geq 1} \frac{c_i}{i} u^i = \sum_{i\geq 0} b_i X^i,$$

on, fixat π un uniformitzant de $\mathcal{O}_\wp$, em posat $X = u/\pi$, $b_0 = c_0$ i $b_i = c_i\pi^i/i$. La serie $\sum_{i\geq 0} b_i X^i$ és convergent a la bola unitat $\mathcal{O}_\wp$ i per tant podem aplicar el teorema de Strassman per a calcular el nombre de zeros.

Per exemple, si la reducció de η, $\widetilde{\eta}$, té ordre 0 a $\widetilde{P}$ (o sigui, $\widetilde{c_1} \neq 0$, o equivalentment $|c_1| = 1$), i si $e < p-1$, aleshores $|b_1| = |c_1| \cdot |\pi| = p^{-1/e}$ i

$$|b_i| \leq \frac{|\pi|^i}{|i|} = \frac{p^{-\frac{i}{e}}}{|i|} \leq p^{-2/e}$$

per $i \geq 2$, ja que $|i| \geq p^{\frac{2-i}{e}}$. Pel teorema de Strassman obtenim que $\lambda_{\eta,D}$ té com a molt un zero a B_P.

Exemple 6. *En el nostre exemple anterior, tenim que la serie $\lambda_{\eta,P}(u)$ té terme de grau 1 no múltiple de 5, i per tant com a molt té un zero en la bola $5\mathbb{Z}_5$. O sigui, no hi ha cap punt de $C(\mathbb{Q})$ que tingui la mateixa reducció mòdul 5 que P a part de P.*

Més en general, si $\mathrm{ord}_{\widetilde{P}}(\widetilde{\eta}) = k-1$, denotem per

$$n(\widetilde{\eta}, \widetilde{P}) := \max\{n \,:\, |\pi|^n/|n| \geq |\pi|^k/|k|\}.$$

Aleshores el teorema de Strassman ens implica que $\lambda_{\eta,D}$ té com a molt $n(\widetilde{\eta}, \widetilde{P})$ zeros a B_P.

Si ara definim $N(\widetilde{\eta}) := \sum n(\widetilde{\eta}, \widetilde{P})$, on la suma la prenem respecte tots els punts de la reducció de C, obtenim una cota per el nombre de zeros de $\lambda_{\eta,D}$, i per tant per el nombre de punts K-racionals de C. En general es difícil calcular $N(\eta)$, però el podem acotar sota certes condicions per el nombre de zeros de η a la bola unitat, i, en el cas de bona reducció, per el nombre de zeros de $\widetilde{\eta}$.

Denotem per

$$i(\eta, P) := \min\{m \,:\, |a_m| = 1\ \}.$$

És clar que, si $i(\eta, P) > 0$, aleshores $i(\eta, P) - 1$ és la cota de Strassman per el nombre de zeros de la derivada de $\lambda_{\eta,P}$.

Lemma 2. *Suposem que $p > 2$, que $e = 1$ i que $i(\eta, P) < p^2 - 2$. Aleshores $n(\eta, P) \leq i(\eta, P) + 1$, i, si p no divideix $i(\eta, P) + 1$, de fet $n(\eta, P) \leq i(\eta, P)$.*

La demostració d'aquest fet us la deixem com a exercici.

Ara, tenim el següent resultat sobre el nombre de zeros de la derivada de $\lambda_{\eta,P}$.

Proposició 2. *Multiplicant si cal η per un element de K podem suposar que l'expansió local de η en P es de la forma $\eta = \sum_{i\geq 1} c_i u^{i-1} du$, amb $c_m \in \mathcal{O}_\wp$ i*

$$i(\eta, P) - 1 = \sum_{red(Q)=red(P)} [K_\wp(Q) : K_\wp] ord_\wp(\eta)$$

Ara, utilitzant que el nombre de zeros d'una forma diferencial és com a molt $2g-2$ (comptats amb multiplicitat), podem deduir una cota general per les corbes.

Teorema 3. *(Coleman) Sigui C una corba de gènere g definida sobre un cos de nombres K, i sigui $\wp$ un primer tal que $K_\wp$ és no ramificat sobre $\mathbb{Q}_p$, i prenem $\mathcal{C}$ un model regular i propi de C sobre $\mathcal{O}_\wp$. Suposem que verifica la condició de Chabauty i que $p^2 > 2g+1$. Aleshores*

$$\#C(K) \leq \#(\mathcal{C}_{ns}(k)) + \frac{p-1}{p-2}(2g-2)$$

La idea de la demostració es que

$$\sum_{\widetilde{P}} (i(\eta, P) - 1) =$$

$$\sum_{\widetilde{P}} \sum_{red(Q)=\widetilde{P}} [K_\wp(Q) : K_\wp] \mathrm{ord}_\wp(\eta) \leq 2g-2 < p^2 - 3$$

on la suma és sobre tots els punts $\widetilde{P}$ a $\mathcal{C}_{ns}(k)$.

Ara, del teorema de Strassman tenim que

$$\#C(K) \leq \sum_{\widetilde{P}} n(\eta, P) \leq$$

$$\sum_{p \mid (i(\eta,P)+1)} (i(\eta, P)+1) + \sum_{p \nmid (i(\eta,P)+1)} i(\eta, P)$$

$$\leq \sum_{\widetilde{P}} i(\eta, P) + (2g-2)/(p-2)$$

ja que si $p \mid (i(\eta,P)+1)$, aleshores $i(\eta,P)-1 > p+2$ i $\sum (i(\eta,P)-1) < 2g-2$, com a molt hi ha $(p+2)/(2g-2)$ punts verificant aquesta condició.

Per tant tenim que

$$\#C(K) \leq \sum_{\widetilde{P}} (i(\eta, P) - 1) + \#(\mathcal{C}_{ns}(k)) + \frac{p+2}{2g-2} \leq$$

$$2g - 2 + \#(\mathcal{C}_{ns}(k)) + \frac{p+2}{2g-2}$$

Corol·lari 2. *Sota les mateixes condicions del Teorema, si a més $p > 2g$, aleshores*

$$\#C(K) \leq \#(\mathcal{C}_{ns}(k)) + (2g - 2)$$

Per exemple, si la corba té gènere 2, aleshores té com a molt 2 punts més K-racionals que a la reducció.

Exemple 7. *La corba $y^2 = x(x-1)(x-2)(x-5)(x-6)$ té rang 1 i bona reducció en el 7. És fàcil trobar els següents punts racionals: ∞, $(0,0)$, $(1,0)$, $(2,0)$, $(3,\pm 6)$, $(5,0)$, $(6,0)$, $(10,\pm 120)$. Però $\#\mathcal{C}(\mathbb{F}_7) = 8$, per tant $\#C(\mathbb{Q}) \leq 10$. Com que tenim 10 punts, ja els tenim tots.*

Referències

[1] *Nils Bruin*, Chabauty methods and covering techniques applied to generalised Fermat equations, PhD dissertation, Leiden, 1999. In http://www.cecm.sfu.ca/∼bruin/.

[2] *J. W. S. Cassels and E. V. Flynn*, Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2, Cambridge Univ. Press, Cambridge, 1996.

[3] *C. Chabauty* Sur les points rationnels des courbes algébriques de genre supérieur à l'unité, C. R. Acad. Sci. Paris 212 (1941), 882–885.

[4] *Robert F. Coleman*, Torsion points on curves and p-adic Abelian integrals. Annals of math. 121 (1985), 111–168.

[5] *Robert F. Coleman*, Effective Chabauty. Duke Math. J. 52 (1985), 765–780.

[6] *E. Victor Flynn*, A flexible method for applying Chabauty's Theorem, Compositio Math. 105 (1997), 79–94.

[7] *E. Victor Flynn and Joseph L. Wetherell* Covering collections and a challenge problem of Serre. Acta Arith. 98 (2001), no. 2, 197–205.

[8] *Dino Lorenzini and Thomas J. Tucker*, Thue equations and the method of Chabauty-Coleman. Invent. Math. 148 (2002), no. 1, 47–77.

[9] *William G. McCallum*, The arithmetic of Fermat curves. Math. Ann. 294 (1992), 503–511.

[10] *Bjorn Poonen*, Computing racional points on curves, preprint 2001, in http://math.berkeley.edu/∼poonen/.

[11] *J. H. Silverman*, The Arithmetic of Elliptic Curves, Springer, New York, 1986.

[12] *Joseph L. Wetherell*, Bounding the number of rational points on certain curves of high rank, PhD dissertation, Univ. of California at Berkeley, 1997. Es pot trobar a http://swc.math.arizona.edu/∼swcenter/notes/AWS99.html