

Equacions de Thue: Models regulars i fites uniformes.

Xavier Xarles

Seminari de Teoria de Nombres

1 de Febrer de 2007

Equacions de Thue

$F(X, Y) \in \mathbb{Z}[X, Y]$ homogénea, de grau $n \geq 3$, i tal que $F(x, 1)$ no té arrels repetides.

Equacions de Thue

$F(X, Y) \in \mathbb{Z}[X, Y]$ homogénea, de grau $n \geq 3$, i tal que $F(x, 1)$ no té arrels repetides.

Una equació de Thue és una equació de la forma, per $h \in \mathbb{Z}$,

$$F(X, Y) = h.$$

Equacions de Thue

$F(X, Y) \in \mathbb{Z}[X, Y]$ homogénea, de grau $n \geq 3$, i tal que $F(x, 1)$ no té arrels repetides.

Una equació de Thue és una equació de la forma, per $h \in \mathbb{Z}$,

$$F(X, Y) = h.$$

Teorema (Thue 1909)

Les equacions de Thue tenen un nombre finit de solucions $(x, y) \in \mathbb{Z}^2$.

Observació

Una equació de Thue (tal com l'he definit) ens determina una corba (plana) no singular $X_{F,h}$, de gènere

$$g(X_F) = \frac{(n-1)(n-2)}{2}$$

(anomenada corba superel·líptica).

Observació

Una equació de Thue (tal com l'he definit) ens determina una corba (plana) no singular $X_{F,h}$, de gènere

$$g(X_F) = \frac{(n-1)(n-2)}{2}$$

(anomenada corba superel·líptica).

Teorema(Faltings 1982)

Les equacions de Thue amb $n \geq 4$ tenen un nombre finit de solucions racionals ($(x, y) \in \mathbb{Q}^2$).

Conjectura Solucions primitives

Conjectura(Erdős, Steward, Tijdeman)

Per a tota $n \geq 3$, existeix una constant $C(n)$ que només depèn de n tal que

$$\#\{(x, y) \in \mathbb{Z}^2 \mid F(x, y) = h \text{ i } (x, y) = 1\} \leq C(n)$$

per a tota equació de Thue $F(X, Y) = h$ de grau n .

Conjectura solucions racionals

Conjectura(Caporaso, Harris, Mazur)

Per a tota $n \geq 4$, existeix una constant $C(n)$ que només depèn de n tal que

$$\#\{(x, y) \in \mathbb{Q}^2 \mid F(x, y) = h\} \leq C(n)$$

per a tota equació de Thue $F(X, Y) = h$ de grau n .

Resultats Coneguts

Notació

$$N(F, h) = \#\{(x, y) \in \mathbb{Z}^2 \mid F(x, y) = h \text{ i } (x, y) = 1\}$$

Resultats Coneguts

Notació

$$N(F, h) = \#\{(x, y) \in \mathbb{Z}^2 \mid F(x, y) = h \text{ i } (x, y) = 1\}$$

Teorema (Bombieri-Schmidt 1987)

Suposem $F(x, 1)$ irreductible. Existeix una constant B_1 (que podem prendre igual a 215 si n és gran), tal que

$$N(F, h) \leq B_1 n^{\omega(h)+1}$$

on $\omega(h)$ és el nombre de factors primers de h

Resultats Coneguts

Denotem per $r(X_{F,h})$ el rank del grup de punts racionals de la Jacobiana de $X_{F,h}$.

Resultats Coneguts

Denotem per $r(X_{F,h})$ el rank del grup de punts racionals de la Jacobiana de $X_{F,h}$.

Teorema(Silverman 1983)

Existeix una constant (inefectiva) $h(F)$ tal que per tota $h > h(F)$ lliure de potències enèsimes,

$$N(F, h) \leq n^{2n^2} (8n^3)^{r(X_{F,h})}$$

Lorenzini-Tucker 2002

Teorema

Si $r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}$, aleshores

$$N(F, h) \leq 2n^3 - 2n - 3.$$

(Per certs casos especials obtenen una fita del ordre $O(n^2)$).

Lorenzini-Tucker 2002

Teorema

Si $r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}$, aleshores

$$N(F, h) \leq 2n^3 - 2n - 3.$$

(Per certs casos especials obtenen una fita del ordre $O(n^2)$).

Observació La fita que s'obté del resultat del Silverman és exponencial en n .

Mètode de Chabauty-Coleman

Idea a retenir Si $r(X) < g(X)$, i $p > 2g$, aleshores

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

on $\overline{\mathcal{X}}$ és la reducció mòdul p de qualsevol model regular $\mathcal{X}$ de X sobre $\mathbb{Z}_p$, i ns indica els punts no singulars.

Mètode de Chabauty-Coleman

Idea a retenir Si $r(X) < g(X)$, i $p > 2g$, aleshores

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

on $\overline{\mathcal{X}}$ és la reducció mòdul p de qualsevol model regular $\mathcal{X}$ de X sobre $\mathbb{Z}_p$, i ns indica els punts no singulars.

Generalització Val pels cossos de nombres K amb completació en un primer no ramificada sobre $\mathbb{Q}_p$.

Comentaris

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

- Coleman va provar això només per bona reducció.

Comentaris

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

- Coleman va provar això només per bona reducció.
- La fita donada pot ser molt gran si la reducció és molt dolenta

Comentaris

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + 2g(X) - 2$$

- Coleman va provar això només per bona reducció.
- La fita donada pot ser molt gran si la reducció és molt dolenta
- Necessitem una millora per estudiar els punts que ens interessin (no tots els punts racionals)

Notacions

$X/\mathbb{Q}$ corba de gènere $g > 2$.

Notacions

$X/\mathbb{Q}$ corba de gènere $g > 2$.

$\mathcal{X}$ un model regular sobre $\mathbb{Z}_p$

Notacions

$X/\mathbb{Q}$ corba de gènere $g > 2$.

$\mathcal{X}$ un model regular sobre $\mathbb{Z}_p$

$\overline{\mathcal{X}}$ la fibra especial de $\mathcal{X}$ a $\mathbb{F}_p$

Notacions

$X/\mathbb{Q}$ corba de gènere $g > 2$.

$\mathcal{X}$ un model regular sobre $\mathbb{Z}_p$

$\overline{\mathcal{X}}$ la fibra especial de $\mathcal{X}$ a $\mathbb{F}_p$

$red_p : X(\mathbb{Q}_p) \rightarrow \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ el morfisme reducció.

Notacions

$X/\mathbb{Q}$ corba de gènere $g > 2$.

$\mathcal{X}$ un model regular sobre $\mathbb{Z}_p$

$\overline{\mathcal{X}}$ la fibra especial de $\mathcal{X}$ a $\mathbb{F}_p$

$red_p : X(\mathbb{Q}_p) \rightarrow \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ el morfisme reducció.

Exercici: La imatge sempre cau dins els punts no singulars

Chabauty-Coleman General

Prenem $X/\mathbb{Q}$ corba de gènere $g > 2$. Suposem $r(X) < g$

Chabauty-Coleman General

Prenem $X/\mathbb{Q}$ corba de gènere $g > 2$. Suposem $r(X) < g$

Sigui $d < p$ tal que $p^d > 2g + 1 - d$. (Prendrem $d=2$)

Chabauty-Coleman General

Prenem $X/\mathbb{Q}$ corba de gènere $g > 2$. Suposem $r(X) < g$

Sigui $d < p$ tal que $p^d > 2g + 1 - d$. (Prendrem $d=2$)

Sigui $U \subseteq \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ un subconjunt qualsevol.

Chabauty-Coleman General

Prenem $X/\mathbb{Q}$ corba de gènere $g > 2$. Suposem $r(X) < g$

Sigui $d < p$ tal que $p^d > 2g + 1 - d$. (Prendrem $d=2$)

Sigui $U \subseteq \overline{\mathcal{X}}_{ns}(\mathbb{F}_p)$ un subconjunt qualsevol.

Aleshores

$$\#red_p^{-1}(U) \cap X(\mathbb{Q}) \leq \#U + \left(\frac{p-1}{p-d} \right) (2g-2)$$

Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Aleshores $p^2 > 2g(X_{F,h}) - 1$.

Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Aleshores $p^2 > 2g(X_{F,h}) - 1$.

Trobem U a la reducció en p d'un model regular de $X_{F,h}$ que contingui totes les imatges de punts primitius sobre $\mathbb{Z}$.

Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Aleshores $p^2 > 2g(X_{F,h}) - 1$.

Trobem U a la reducció en p d'un model regular de $X_{F,h}$ que contingui totes les imatges de punts primitius sobre $\mathbb{Z}$.

Fitem superiorment el nombre de punts de U en funció de n i p i apliquem el teorema anterior.

Idea

Considerem un nombre primer p tal que $n < p < 2n$.

Aleshores $p^2 > 2g(X_{F,h}) - 1$.

Troblem U a la reducció en p d'un model regular de $X_{F,h}$ que contingui totes les imatges de punts primitius sobre $\mathbb{Z}$.

Fitem superiorment el nombre de punts de U en funció de n i p i apliquem el teorema anterior.

Substituïm p per $2n$. I ja està!

Notacions

$F(X, Y)$ polinomi homogeni amb coeficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

Notacions

$F(X, Y)$ polinomi homogeni amb coeficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

$d(F) \in \mathbb{Z}$ discriminant de $F(x, 1)$.

Notacions

$F(X, Y)$ polinomi homogeni amb coeficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

$d(F) \in \mathbb{Z}$ discriminant de $F(x, 1)$.

$h \in \mathbb{Z}$ enter lliure de potències enèsimes (si en té podem fer un canvi de variables per treure-la)

Notacions

$F(X, Y)$ polinomi homogeni amb coeficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

$d(F) \in \mathbb{Z}$ discriminant de $F(x, 1)$.

$h \in \mathbb{Z}$ enter lliure de potències enèsimes (si en té podem fer un canvi de variables per treure-la)

Suposem que $X := X_{F,h}$ té $r(X) < g(X)$.

p un nombre primer $n < p < 2n$.

Notacions

$F(X, Y)$ polinomi homogeni amb coeficients a $\mathbb{Z}$ de grau $n > 3$ sense arrels repetides a $\overline{\mathbb{Q}}$.

$d(F) \in \mathbb{Z}$ discriminant de $F(x, 1)$.

$h \in \mathbb{Z}$ enter lliure de potències enèsimes (si en té podem fer un canvi de variables per treure-la)

Suposem que $X := X_{F,h}$ té $r(X) < g(X)$.

p un nombre primer $n < p < 2n$.

Casos a estudiar

1. $p \nmid d(F)$ i $p \nmid h$ (Cas bona reducció).

Casos a estudiar

1. $p \nmid d(F)$ i $p \nmid h$ (Cas bona reducció).
2. $p \mid d(F)$ i $p \nmid h$ (Cas mala reducció).

Casos a estudiar

1. $p \nmid d(F)$ i $p \nmid h$ (Cas bona reducció).
2. $p \mid d(F)$ i $p \nmid h$ (Cas mala reducció).
3. $p \nmid d(F)$ i $p \mid h$ (Cas bona reducció potencial)

Casos a estudiar

1. $p \nmid d(F)$ i $p \nmid h$ (Cas bona reducció).
2. $p \mid d(F)$ i $p \nmid h$ (Cas mala reducció).
3. $p \nmid d(F)$ i $p \mid h$ (Cas bona reducció potencial)
4. $p \mid d(F)$ i $p \mid h$ (Cas molt mala reducció)

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + \left(\frac{p-1}{p-2}\right) (2g - 2).$$

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + \left(\frac{p-1}{p-2}\right) (2g - 2).$$

$$\text{Tenim } \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) \leq (n - 1)(p + 1) + 1.$$

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + \left(\frac{p-1}{p-2}\right) (2g - 2).$$

$$\text{Tenim } \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) \leq (n - 1)(p + 1) + 1.$$

$$p \leq 2n - 1 \Rightarrow (2g - 2) \left(\frac{p-1}{p-2}\right) \leq 2g + n - 5.$$

1. $p \nmid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{X}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model redueix a una corba no singular. El model és llis, i per tant regular.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#\overline{\mathcal{X}}_{ns}(\mathbb{F}_p) + \left(\frac{p-1}{p-2}\right) (2g - 2).$$

$$\text{Tenim } \overline{\mathcal{X}}_{ns}(\mathbb{F}_p) \leq (n - 1)(p + 1) + 1.$$

$$p \leq 2n - 1 \Rightarrow (2g - 2) \left(\frac{p-1}{p-2}\right) \leq 2g + n - 5.$$

$$\text{Obtenim finalment que } \#X(\mathbb{Q}) \leq 3n^2 - 4n - 2.$$

2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model no és regular! Ara bé, la part afí U de la reducció $\bar{\mathcal{C}}$ corresponent a $F(X, Y) = h$ és llisa.

2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model no és regular! Ara bé, la part afí U de la reducció $\bar{\mathcal{C}}$ corresponent a $F(X, Y) = h$ és llisa.

Tota solució primitiva $(a, b) \in \mathbb{Z}^2$ de $F(X, Y) = h$ cau a dins de U al reduir.

2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model no és regular! Ara bé, la part afí U de la reducció $\bar{\mathcal{C}}$ corresponent a $F(X, Y) = h$ és llisa.

Tota solució primitiva $(a, b) \in \mathbb{Z}^2$ de $F(X, Y) = h$ cau a dins de U al reduir.

Prenem $\varphi : \mathcal{X} \rightarrow \mathcal{C}$ model regular obtingut resolent $\mathcal{C}$. Aleshores $\bar{\varphi}^{-1}(U) \cong U$.

2. $p \mid d(F)$ i $p \nmid h$

Prenem el model $\mathcal{C}$ de X sobre $\mathbb{Z}_p$ donat per $F(X, Y) = hZ^n$.

Aquest model no és regular! Ara bé, la part afí U de la reducció $\bar{\mathcal{C}}$ corresponent a $F(X, Y) = h$ és llisa.

Tota solució primitiva $(a, b) \in \mathbb{Z}^2$ de $F(X, Y) = h$ cau a dins de U al reduir.

Prenem $\varphi : \mathcal{X} \rightarrow \mathcal{C}$ model regular obtingut resolent $\mathcal{C}$. Aleshores $\bar{\varphi}^{-1}(U) \cong U$.

Per tant $N(F, h) \leq (2g - 2)(p - 1)/(p - 2) + \#U \leq (2g - 2)(p - 1)/(p - 2) + np \leq 3n^2 - 3n - 3$.

3. $p \mid d(F)$ i $p \nmid h$

Prenem $K = \mathbb{Q}_p(\sqrt[n]{h})$. Aleshores

$$X \otimes_{\mathbb{Q}_p} K \cong X_{F,1}$$

que té bona reducció pel cas 1.

3. $p \mid d(F)$ i $p \nmid h$

Prenem $K = \mathbb{Q}_p(\sqrt[n]{h})$. Aleshores

$$X \otimes_{\mathbb{Q}_p} K \cong X_{F,1}$$

que té bona reducció pel cas 1.

Idea: Prenem model $\mathcal{Y}$ sobre $\mathcal{O}_K$ llis, i fem quocient per l'acció de $Gal(K/\mathbb{Q}_p)$. Resolem el model obtingut.

3. $p \mid d(F)$ i $p \nmid h$

Prenem $K = \mathbb{Q}_p(\sqrt[n]{h})$. Aleshores

$$X \otimes_{\mathbb{Q}_p} K \cong X_{F,1}$$

que té bona reducció pel cas 1.

Idea: Prenem model $\mathcal{Y}$ sobre $\mathcal{O}_K$ llis, i fem quocient per l'acció de $Gal(K/\mathbb{Q}_p)$. Resolem el model obtingut.

Problema: $K/\mathbb{Q}_p$ no és cíclica, ni tant sols Galois.

3. $p \mid d(F)$ i $p \nmid h$

Prenem $K = \mathbb{Q}_p(\sqrt[n]{h})$. Aleshores

$$X \otimes_{\mathbb{Q}_p} K \cong X_{F,1}$$

que té bona reducció pel cas 1.

Idea: Prenem model $\mathcal{Y}$ sobre $\mathcal{O}_K$ llis, i fem quocient per l'acció de $Gal(K/\mathbb{Q}_p)$. Resolem el model obtingut.

Problema: $K/\mathbb{Q}_p$ no és cíclica, ni tant sols Galois.

Idea: Prenem $L = \mathbb{Q}_p^{nr}(\sqrt[n]{h})/\mathbb{Q}_p^{nr}$ que és Galois, cíclica, moderadament ramificada.

Construcció quocient: Cas llis

Tenim $\mathcal{Y}$ llis sobre $\mathcal{O}_L$, el model anterior:

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - Z^n)$$

Construcció quocient: Cas lli

Tenim $\mathcal{Y}$ lli sobre $\mathcal{O}_L$, el model anterior:

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - Z^n)$$

L'acció de $G := \text{Gal}(L/\mathbb{Q}_p^{nr}) = \langle \sigma \rangle$ sobre X_L dóna acció sobre $\mathcal{Y}$:

$$\sigma(X) = X, \sigma(Y) = Y, \sigma(Z) = \xi_m Z$$

ξ_m arrel primitiva enèsima de 1, $m := n/\text{ord}_p(h)$,
 $L = \mathbb{Q}_p^{nr}(\xi_m)$.

Construcció quotient: Cas lls

Tenim $\mathcal{Y}$ lls sobre $\mathcal{O}_L$, el model anterior:

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - Z^n)$$

L'acció de $G := \text{Gal}(L/\mathbb{Q}_p^{nr}) = \langle \sigma \rangle$ sobre X_L dóna acció sobre $\mathcal{Y}$:

$$\sigma(X) = X, \sigma(Y) = Y, \sigma(Z) = \xi_m Z$$

ξ_m arrel primitiva enèsima de 1, $m := n/\text{ord}_p(h)$,
 $L = \mathbb{Q}_p^{nr}(\xi_m)$.

El morfisme $q : \mathcal{Y} \rightarrow \mathcal{Y}/G$ redueix al morfisme
 $\bar{q} : \bar{\mathcal{Y}} \rightarrow \bar{\mathcal{Y}}/G$.

Estudi del quocient

El quocient $\mathcal{Y}/G$ és un esquema sobre $\mathbb{Z}_p^{nr}$, normal, els seus punts singulars estan a la fibra especial i són "singularitats quocient".

Estudi del quocient

El quocient $\mathcal{Y}/G$ és un esquema sobre $\mathbb{Z}_p^{nr}$, normal, els seus punts singulars estan a la fibra especial i són "singularitats quocient".

Els punts singulars són els punts ramificats de $\bar{q} : \bar{\mathcal{Y}} \rightarrow \bar{\mathcal{Y}}/G$.

Estudi del quocient

El quocient $\mathcal{Y}/G$ és un esquema sobre $\mathbb{Z}_p^{nr}$, normal, els seus punts singulars estan a la fibra especial i són "singularitats quocient".

Els punts singulars són els punts ramificats de $\bar{q} : \bar{\mathcal{Y}} \rightarrow \bar{\mathcal{Y}}/G$.

O sigui els punts $q(P)$ amb $P = [x : y : 0]$, i n'hi ha n . A més $q^{-1}(P)$ només conté el punt tancat P .

Desingularització de quocient

Prenem $\nu : \mathcal{X}' \rightarrow \mathcal{Y}/G$ la desingularització sobre $\mathbb{Z}_p^{nr}$.

Desingularització de quocient

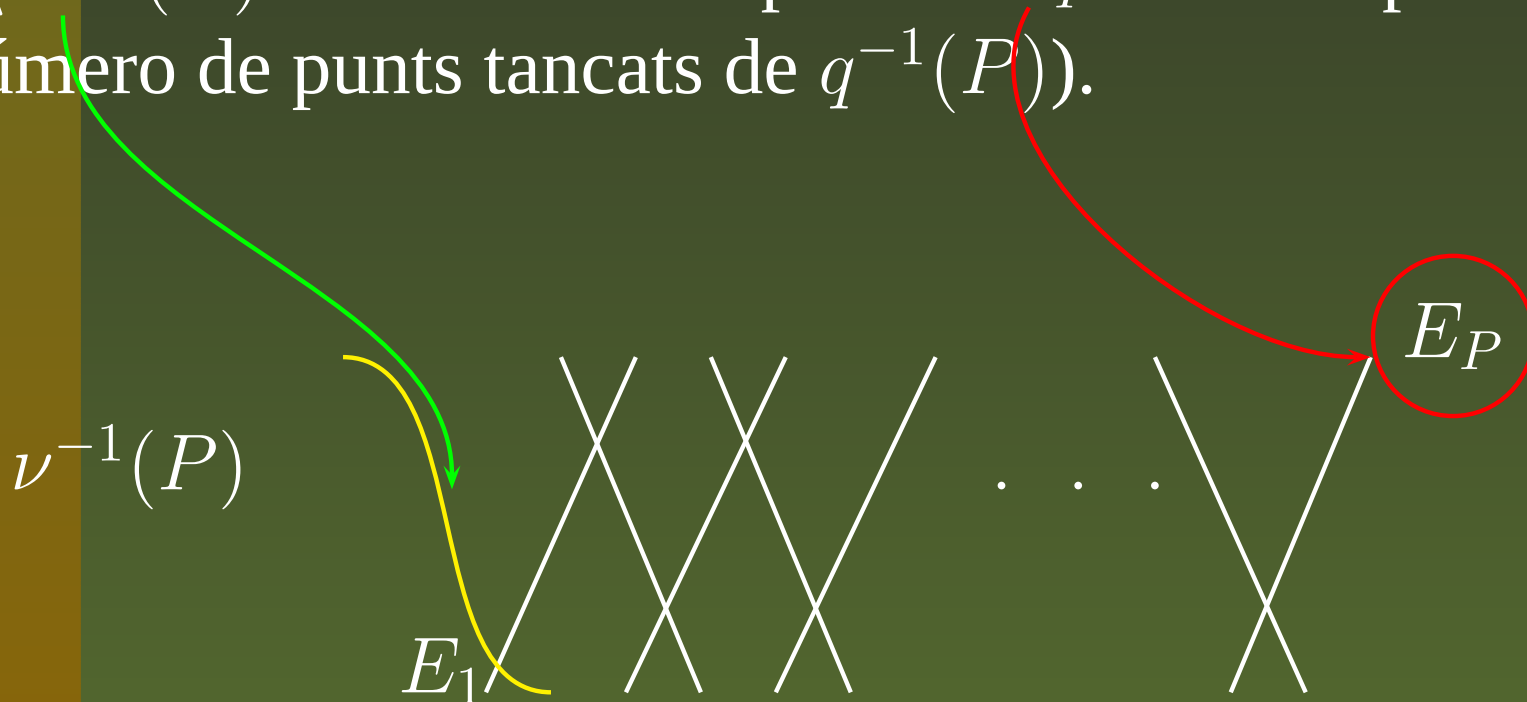
Prenem $\nu : \mathcal{X}' \rightarrow \mathcal{Y}/G$ la desingularització sobre $\mathbb{Z}_p^{nr}$.

Donat $P \in (\overline{\mathcal{Y}}/G)_{sing}$, $\nu^{-1}(P)$ és una cadena de corbes llises i racionals, amb una sola E_1 interseccan $\overline{\mathcal{X}'} \setminus \nu^{-1}(P)$ i la última component E_P de multiplicitat 1 (=número de punts tancats de $q^{-1}(P)$).

Desingularització de quocient

Prenem $\nu : \mathcal{X}' \rightarrow \mathcal{Y}/G$ la desingularització sobre $\mathbb{Z}_p^{nr}$.

Donat $P \in (\overline{\mathcal{Y}}/G)_{sing}$, $\nu^{-1}(P)$ és una cadena de corbes llises i racionals, amb una sola E_1 intersecció $\overline{\mathcal{X}'} \setminus \nu^{-1}(P)$ i la última component E_P de multiplicitat 1 (=número de punts tancats de $q^{-1}(P)$).



3. $p \mid d(F)$ i $p \nmid h$ (Cont.)

Un punt $[x : y : z]$ de $X(\mathbb{Q})$ ens dóna un punt $[x : y : \sqrt[n]{h}z]$ de $\mathcal{Y}$.

3. $p \mid d(F)$ i $p \nmid h$ (Cont.)

Un punt $[x : y : z]$ de $X(\mathbb{Q})$ ens dóna un punt $[x : y : \sqrt[n]{h}z]$ de $\mathcal{Y}$.

Que correspon a un del n punts $[x : y : 0]$ de $\overline{\mathcal{Y}}$, singular a $\overline{\mathcal{Y}}/G$.

3. $p \mid d(F)$ i $p \nmid h$ (Cont.)

Un punt $[x : y : z]$ de $X(\mathbb{Q})$ ens dóna un punt $[x : y : \sqrt[n]{h}z]$ de $\mathcal{Y}$.

Que correspon a un del n punts $[x : y : 0]$ de $\overline{\mathcal{Y}}$, singular a $\overline{\mathcal{Y}}/G$.

Per tant, al reduir a través de $\mathcal{X}'$ un punt en una de les n components llises i racionals de $\overline{\mathcal{X}}'$ de multiplicitat 1.

3. $p \mid d(F)$ i $p \nmid h$ (Cont.)

Un punt $[x : y : z]$ de $X(\mathbb{Q})$ ens dóna un punt $[x : y : \sqrt[n]{h}z]$ de $\mathcal{Y}$.

Que correspon a un del n punts $[x : y : 0]$ de $\overline{\mathcal{Y}}$, singular a $\overline{\mathcal{Y}}/G$.

Per tant, al reduir a través de $\mathcal{X}'$ un punt en una de les n components llises i racionals de $\overline{\mathcal{X}}'$ de multiplicitat 1.

Que necessàriament ha de ser una de les $\leq n$ components llises i racional de $\overline{\mathcal{X}}$ de multiplicitat 1.

3. $p \mid d(F)$ i $p \nmid h$ (Final)

Prenem $U \subseteq \overline{\mathcal{X}}$ la unió d'aquestes components racionals.

3. $p \mid d(F)$ i $p \nmid h$ (Final)

Prenem $U \subseteq \overline{\mathcal{X}}$ la unió d'aquestes components racionals.

Aleshores $red^{-1}(U) \cap X(\mathbb{Q}) = X(\mathbb{Q})$.

3. $p \mid d(F)$ i $p \nmid h$ (Final)

Prenem $U \subseteq \overline{\mathcal{X}}$ la unió d'aquestes components racionals.

Aleshores $red^{-1}(U) \cap X(\mathbb{Q}) = X(\mathbb{Q})$.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#U + \left(\frac{p-1}{p-2} \right) (2g - 2) \leq np + 2g + n - 5$$

3. $p \mid d(F)$ i $p \nmid h$ (Final)

Prenem $U \subseteq \overline{\mathcal{X}}$ la unió d'aquestes components racionals.

Aleshores $red^{-1}(U) \cap X(\mathbb{Q}) = X(\mathbb{Q})$.

Chabauty-Coleman:

$$\#X(\mathbb{Q}) \leq \#U + \left(\frac{p-1}{p-2}\right) (2g-2) \leq np + 2g + n - 5$$

$$\#X(\mathbb{Q}) \leq 3n^2 - 3n - 3$$

4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.

4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.
 $p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

4. $p \nmid d(F)$ i $p \nmid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.
 $p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

Per a cada arrel α de $F(x, 1)$, es construeixen oberts
llisos U_α de $\mathcal{Y}$ sobre $\mathcal{O}_L$.

4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.
 $p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

Per a cada arrel α de $F(x, 1)$, es construeixen oberts
llisos U_α de $\mathcal{Y}$ sobre $\mathcal{O}_L$.

Aquests oberts tenen acció de $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$ natural.

4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.
 $p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

Per a cada arrel α de $F(x, 1)$, es construeixen oberts
llisos U_α de $\mathcal{Y}$ sobre $\mathcal{O}_L$.

Aquests oberts tenen acció de $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$ natural.

Considerem $Z_P = U_P/G$ i s'estudia la reducció de la
seva desingularització.

4. $p \mid d(F)$ i $p \mid h$

No té pot. bona reducció. Prenem un model enter $\mathcal{Y}$ de X sobre L , cos de descomposició de $F(x, 1)$ sobre $\mathbb{Q}_p^{nr}$.
 $p > n \Rightarrow L/\mathbb{Q}_p^{nr}$ moderada.

Per a cada arrel α de $F(x, 1)$, es construeixen oberts
llisos U_α de $\mathcal{Y}$ sobre $\mathcal{O}_L$.

Aquests oberts tenen acció de $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$ natural.

Considerem $Z_P = U_P/G$ i s'estudia la reducció de la
seva desingularització.

Es prova que tot punt primitiu P de X està en un U_α

Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i lli de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua.
Prenem $q : \mathcal{U} \rightarrow \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i lli de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua.

Prenem $q : \mathcal{U} \rightarrow \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Existeix un esquema regular $\mathcal{X}$ sobre $\mathbb{Z}_p^{nr}$ i un morfisme birracional $\nu : \mathcal{X} \rightarrow \mathcal{Z}$ induint iso entre $\mathcal{X}_{ns}$ i $\mathcal{Z}_{ns}$.

Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i llis de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua.
Prenem $q : \mathcal{U} \rightarrow \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Existeix un esquema regular $\mathcal{X}$ sobre $\mathbb{Z}_p^{nr}$ i un morfisme birracional $\nu : \mathcal{X} \rightarrow \mathcal{Z}$ induint iso entre $\mathcal{X}_{ns}$ i $\mathcal{Z}_{ns}$.

Per a tot punt $z \in \mathcal{Z}_{sing}$, $\nu^{-1}(z)$ és una cadena $\{E_1, \dots, E_z\}$ connexa de corbes racionals i llises.

Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i llis de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua.
Prenem $q : \mathcal{U} \rightarrow \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Existeix un esquema regular $\mathcal{X}$ sobre $\mathbb{Z}_p^{nr}$ i un morfisme birracional $\nu : \mathcal{X} \rightarrow \mathcal{Z}$ induint iso entre $\mathcal{X}_{ns}$ i $\mathcal{Z}_{ns}$.

Per a tot punt $z \in \mathcal{Z}_{sing}$, $\nu^{-1}(z)$ és una cadena $\{E_1, \dots, E_z\}$ connexa de corbes racionals i llises.

U llis, per tant la cadena sols interseca el resta de la fibra $\overline{\mathcal{X}}$ en un punt a E_1 .

Construcció quocient: Cas general

$\mathcal{U}$ sub-esquema obert i llis de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on G actua.
Prenem $q : \mathcal{U} \rightarrow \mathcal{Z} := \mathcal{U}/G$, $\mathcal{Z}$ esquema sobre $\mathbb{Z}_p^{nr}$.

Existeix un esquema regular $\mathcal{X}$ sobre $\mathbb{Z}_p^{nr}$ i un morfisme birracional $\nu : \mathcal{X} \rightarrow \mathcal{Z}$ induint iso entre $\mathcal{X}_{ns}$ i $\mathcal{Z}_{ns}$.

Per a tot punt $z \in \mathcal{Z}_{sing}$, $\nu^{-1}(z)$ és una cadena $\{E_1, \dots, E_z\}$ connexa de corbes racionals i llises.

U llis, per tant la cadena sols interseca el resta de la fibra $\overline{\mathcal{X}}$ en un punt a E_1 .

El conjunt de punts singulars és igual als punts de ramificació de q . E_z té multiplicitat $= \#q^{-1}(z)$.

Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

$$\mathcal{V}_\alpha := \text{Spec}(\mathcal{O}_L[z', y](F_\alpha(z', y) - h/\pi^{u_\alpha}))$$

on π uniformitzant de L .

Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

$$\mathcal{V}_\alpha := \text{Spec}(\mathcal{O}_L[z', y](F_\alpha(z', y) - h/\pi^{u_\alpha}))$$

on π uniformitzant de L .

Fent $z_0 = x - \alpha y$, obtenim $F_0(z_0, y)$ de $F(x, y)$.

Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

$$\mathcal{V}_\alpha := \text{Spec}(\mathcal{O}_L[z', y](F_\alpha(z', y) - h/\pi^{u_\alpha}))$$

on π uniformitzant de L .

Fent $z_0 = x - \alpha y$, obtenim $F_0(z_0, y)$ de $F(x, y)$.

$z' := z_0/\pi^t$, on t és cert enter.

Oberts adequats

Per a cada arrel α de $F(x, 1)$, construïm $\mathcal{V}_\alpha$ obert de $\mathcal{Y}$ sobre $\mathcal{O}_L$, on

$$\mathcal{Y} := \text{Proj}(\mathcal{O}_L[X, Y, Z]/(F(X, Y) - hZ^n).$$

$$\mathcal{V}_\alpha := \text{Spec}(\mathcal{O}_L[z', y](F_\alpha(z', y) - h/\pi^{u_\alpha}))$$

on π uniformitzant de L .

Fent $z_0 = x - \alpha y$, obtenim $F_0(z_0, y)$ de $F(x, y)$.

$z' := z_0/\pi^t$, on t és cert enter.

$F_\alpha(z_\alpha, y) = F_0(z_0, y)\pi^{-u_\alpha}$ amb u_α un cert enter.

Oberts adequats (continuació)

Proposició $\mathcal{V}_\alpha$ és un esquema llis, obert de $\mathcal{Y}$. Igualment per

$$\mathcal{U}_\alpha := \bigcap_{\tau \in G} \tau(\mathcal{V}_\alpha)$$

que a més és invariant per $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$.

Oberts adequats (continuació)

Proposició $\mathcal{V}_\alpha$ és un esquema llis, obert de $\mathcal{Y}$. Igualment per

$$\mathcal{U}_\alpha := \bigcap_{\tau \in G} \tau(\mathcal{V}_\alpha)$$

que a més és invariant per $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$.

Per a tot P solució primitiva de $F(X, Y) = h$, existeix un α tal que $P \in \mathcal{U}_\alpha$.

Oberts adequats (continuació)

Proposició $\mathcal{V}_\alpha$ és un esquema llis, obert de $\mathcal{Y}$. Igualment per

$$\mathcal{U}_\alpha := \bigcap_{\tau \in G} \tau(\mathcal{V}_\alpha)$$

que a més és invariant per $G := \text{Gal}(L/\mathbb{Q}_p^{nr})$.

Per a tot P solució primitiva de $F(X, Y) = h$, existeix un α tal que $P \in \mathcal{U}_\alpha$.

Concretament, $P = (a, b)$, aleshores $P \in \mathcal{U}_\alpha$ si i només si

$$t := v(a - \alpha b) = \max_{\beta} (a - \beta b).$$

on β es mou dins les arrels de $F(x, 1) = 0$.

4. $p \mid d(F)$ i $p \mid h$ (cont)

Fem el mateix raonament que el cas 3, però pels $\mathcal{U}_\alpha$.

$$\mathcal{U}_\alpha \rightarrow \mathcal{Z}_\alpha \leftarrow \mathcal{X}_\alpha$$

4. $p \mid d(F)$ i $p \mid h$ (cont)

Fem el mateix raonament que el cas 3, però pels $\mathcal{U}_\alpha$.

$$\mathcal{U}_\alpha \rightarrow \mathcal{Z}_\alpha \leftarrow \mathcal{X}_\alpha$$

Si $\mathcal{X}$ model regular sobre $\mathbb{Z}_p$, tenim $\mathcal{X}_\alpha \rightarrow \mathcal{X} \otimes \mathbb{Z}_p^{nr}$.

4. $p \mid d(F)$ i $p \mid h$ (cont)

Fem el mateix raonament que el cas 3, però pels $\mathcal{U}_\alpha$.

$$\mathcal{U}_\alpha \rightarrow \mathcal{Z}_\alpha \leftarrow \mathcal{X}_\alpha$$

Si $\mathcal{X}$ model regular sobre $\mathbb{Z}_p$, tenim $\mathcal{X}_\alpha \rightarrow \mathcal{X} \otimes \mathbb{Z}_p^{nr}$.

Fet clau: Com a molt np punts de la imatge de $\mathcal{Z}_\alpha$ a $\overline{\mathcal{X}}$ poden ser reducció de punts primitius.

4. $p \mid d(F)$ i $p \mid h$ (Final)

En resum:

Si U és la unió de les imatges de $\mathcal{U}_\alpha$ a $\overline{\mathcal{X}}$, aleshores

4. $p \mid d(F)$ i $p \mid h$ (Final)

En resum:

Si U és la unió de les imatges de $\mathcal{U}_\alpha$ a $\overline{\mathcal{X}}$, aleshores

Chabauty-Coleman:

$$N(F, h) \leq \#U + \left(\frac{p-1}{p-2} \right) (2g - 2) \leq n^2 p + 2g + n - 5.$$

4. $p \mid d(F)$ i $p \mid h$ (Final)

En resum:

Si U és la unió de les imatges de $\mathcal{U}_\alpha$ a $\overline{\mathcal{X}}$, aleshores

Chabauty-Coleman:

$$N(F, h) \leq \#U + \left(\frac{p-1}{p-2} \right) (2g - 2) \leq n^2 p + 2g + n - 5.$$

$$N(F, h) \leq 2n^3 - 2n - 3$$

Resum definitiu

Tenim en el cas general que si

$r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}$, aleshores

$$N(F, h) \leq 2n^3 - 2n - 3.$$

Resum definitiu

Tenim en el cas general que si

$$r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}, \text{ aleshores}$$

$$N(F, h) \leq 2n^3 - 2n - 3.$$

Si $\exists p \nmid d(F)$ tal que $n < p < 2n$, aleshores

$$\#X_{F,h}(\mathbb{Q}) \leq 3n^2 - 3n - 3.$$

Resum definitiu

Tenim en el cas general que si

$$r(X_{F,h}) < g(X_F) = \frac{(n-1)(n-2)}{2}, \text{ aleshores}$$

$$N(F, h) \leq 2n^3 - 2n - 3.$$

Si $\exists p \nmid d(F)$ tal que $n < p < 2n$, aleshores

$$\#X_{F,h}(\mathbb{Q}) \leq 3n^2 - 3n - 3.$$

Si $\exists p \nmid h$ tal que $n < p < 2n$, aleshores

$$N(F, h) \leq 3n^2 - 3n - 3.$$

*L'espai singular
s'enrama tot de branques
mentre no el miro.*

