A geometric quadratic Chabauty computation on $X_0(67)^+$

Juanita Duque-Rosero and Sachi Hashimoto
joint work with Pim Spelier

Simons collaboration meeting, September 11, 2021

Our goal

Motivation:
We want to apply the geometric quadratic Chabauty of Edixhoven and Lido method to find an upper bound for the number of rational points on $X_0(67)^+ = X_0(67)/\langle w_{67} \rangle$.

Let X be the weighted homogenization of

$$y^2 + (x^3 + x + 1)y = x^5 - x.$$

Fact: X is a regular model for $X_0(67)^+$ over $\mathbb{Z}$.

Proposition

The integer points $X(\mathbb{Z})$ reducing to $(0, -1) \in X(\mathbb{F}_7)$ are contained in the set

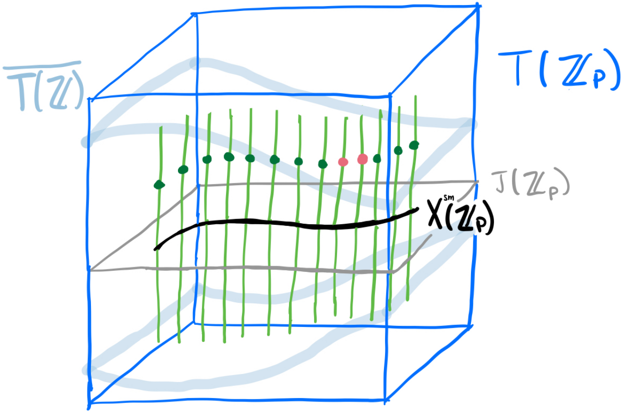
$$\{(0, -1), (4 \cdot 7 + O(7^2), 6 + O(7^2))\}.$$

Note: $X(\mathbb{Q}) = X(\mathbb{Z})$.
$X(\mathbb{Q})$ has been determined by Balakrishnan, Best, Bianchi, Lawrence, Müller, Triantafillou, and Vonk.

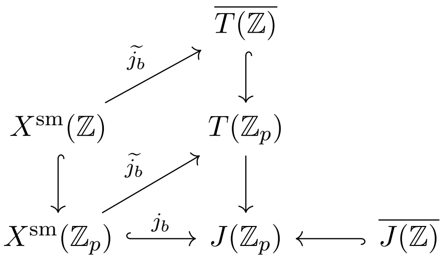
Overview

$J/\mathbb{Z}$ Néron model for the Jacobian of X,
T a $\mathbb{G}_m$-torsor over J,
$j_b : X^{\mathrm{sm}} \to J$ Abel–Jacobi at basepoint $b = (1,0) \in X(\mathbb{Z})$.

Note: $X(\mathbb{Q}) = X(\mathbb{Z}) = X^{\mathrm{sm}}(\mathbb{Z})$.



“Chabauty’s Theorem”



“Chabauty’s Theorem”*

$\widetilde{j_b}(X^{\mathrm{sm}}(\mathbb{Z}_p)) \cap \overline{T(\mathbb{Z})} \subset T(\mathbb{Z}_p)$ is finite.

*This is neither a theorem, nor Chabauty’s.

Work residue disk by residue disk. Consider disk of $P = (0, -1)$.

Strategy

Our strategy:

- Construct a homeomorphism $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$ given by convergent power series
- Compute the embedding $\widetilde{j_b} : X^{\mathrm{sm}} \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ via a section
- Give a map $\kappa : \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$
- Intersect $\varphi \circ \kappa$ and $\varphi \circ \widetilde{j_b}$ in $\mathbb{Z}_p^3$
- A Hensel-like lemma implies that precision p^2 is enough

Construction of T

We need an nontrivial trace 0 endomorphism $f : J \to J$. We use an element of the Hecke algebra of J.

We pull back the universal $\mathbb{G}_m$-torsor $\mathcal{M}^\times$ over $J \times J$ by $(1, \alpha)$ where $\alpha = \mathrm{tr}_c \circ f$ and c is uniquely determined so that $T := (1, \alpha)^* \mathcal{M}^\times$ over J is trivial over X.

We compute equations for a correspondence $D_f \subset X \times X$ inducing the endomorphism f, using the code of Costa, Mascot, Sijsling, and Voight.

One of the challenging aspects is to work with the divisor

$$A_\alpha := D_f - D_f|_{X \times b} \times X + X \times D_f|_{X \times b} - X \times D_f|_\Delta$$

explicitly.

The equations for D_f

```
[7605023584402176072496*x^8*u^2 + 276848668324194788374*x^8*u + 2162467398048698636700*x^7*u^2 -
6272554892698832692599*x^6*y*u^2 - 4626446567682633747828*x^8*v - 1168446771586826201673*x^8 -
9165162915676858733619*x^7*u + 2241777840578137196064*x^6*y*u - 8418141092008037071834*x^6*u^2 -
13292836185052144419762*x^5*y*u^2 + 754031123597981360894*x^7*v + 6328906343710703634915*x^6*y*v +
2615195628519325252191*x^7 + 1831262799801461507208*x^6*y + 2756070458250784948869*x^6*u + 15428857376010803153841*x^5*y*u
- 11784051570902048135703*x^5*u^2 - 7230872538984499657093*x^4*y*u^2 + 16912156368781966844899*x^6*v +
8794134244461097697655*x^5*y*v + 13382241469127150196465*x^6 + 4082469582390924565047*x^5*y +
21852540598540798087489*x^5*u + 13245519579554143163167*x^4*y*u - 22985066915160029536074*x^4*u^2 -
23255128704790712417887*x^3*y*u^2 + 13682822171560412185605*x^5*v - 165783020433170604550*x^4*y*v -
6931902302166164206278*x^5 - 5083451259029072420619*x^4*y - 11826350429569203951840*x^4*u -
19199699515311811452213*x^3*y*u - 28484484698745046075669*x^3*u^2 - 17690076715222265602489*x^2*y*u^2 +
17805473443696348827856*x^4*v + 675202808346140479378*x^3*y*v + 6675814886892603310402*x^4 + 5577161777751351740903*x^3*y
+ 19969878692979973055652*x^3*u + 18120117063433135735083*x^2*y*u + 936713375105971953531*x^2*u^2 +
11466853454037386066020*x*y*u^2 + 10542523972242190209720*x^3*v + 8824421921807720328364*x^2*y*v +
11877160806671853672804*x^3 + 13363913247174903062953*x^2*y + 14059453652617340471247*x^2*u +
10218057833893227356605*x*y*u - 308361787245220032444*x*u^2 - 5322779956111165805354*y*u^2 + 5505912629321680476560*x^2*v
- 4290695327689320279111*x*y*v - 7612900075627672207215*x^2 - 14312446660999532149696*x*y + 4434640084437900284987*x*u +
3704885128833955385271*y*u - 993796068912520397282*u^2 + 575350421007770819831*x*v + 3829830430486931582408*y*v +
5885803647094172346013*y + 960790192851544016507*u + 281506727438003913980*v + 113825130829311801917,
790135714013668417211*x^8*u^2 - 52199251698889313788*x^8*u + 445626397822123380960*x^7*u^2 -
484065148072652139393*x^6*y*u^2 - 355589770017865569639*x^8*v - 97839554801178078020*x^8 - 678398566039036992539*x^7*u +
155198586393263487818*x^6*y*u - 113052264818131543479*x^6*u^2 - 874765196307671212424*x^5*y*u^2 +
50893236050896468243*x^7*v + 549806068461932423405*x^6*y*v + 245852373764948827027*x^7 + 222973665578085376766*x^6*y -
186006391998859651031*x^6*u + 918135020900189841469*x^5*y*u - 523150712434256670561*x^5*u^2 -
328927822772590067729*x^4*y*u^2 + 1388867642711454788442*x^6*v + 882684613081080621057*x^5*y*v +
1142791546745352334216*x^6 + 533732004549278022010*x^5*y + 394464353147344850914*x^5*u + 874586564270896523236*x^4*y*u -
1503623861758469781638*x^4*u^2 - 1118256877330123036794*x^3*y*u^2 + 962253617070423872834*x^5*v +
260675420287904377496*x^4*y*v - 73108557049802456668*x^5 - 177841514864980758518*x^4*y - 1357965873921914116106*x^4*u -
1595337468013963640622*x^3*y*u - 1882558303840937888797*x^3*u^2 - 1293922634022119677492*x^2*y*u^2 +
1390753692690189767706*x^4*v + 246438908010171275168*x^3*y*v + 793691222208583979104*x^4 + 499223278514256382778*x^3*y +
645256167770372257021*x^3*u + 984786145000107598929*x^2*y*u - 280718524673749556697*x^2*u^2 +
779933023636684223799*x*y*u^2 + 842189446494471065427*x^3*v + 558551444022004233780*x^2*y*v + 913241896994237593431*x^3 +
1244963363551342949690*x^2*y + 727117765460043207926*x^2*u + 1012441030923028187282*x*y*u - 21753359867708939458*x*u^2 -
344942106360625888966*y*u^2 + 353025200232170583936*x^2*v - 211033121948623991455*x*y*v - 163875785683850219832*x^2 -
617198754625174179093*x*y + 597830134728356122829*x*u + 169901861802716830954*y*u - 82203224665107226192*u^2 +
82310455430799619016*x*v + 191169787322405231086*y*v + 341475392487935405751*x + 350318508927358217032*y -
21028731891073941584*u - 9558514495942700720*v, x^5 - x^3*y - x*y - y^2 - x - y, u^5 - u^3*v - u*v - v^2 - u - v,
1120*x^20*u^4 - 2068*x^20*u^3 + 8124*x^19*u^4 + 2407*x^20*u^2 - 16894*x^19*u^3 + 35279*x^18*u^4 - 1641*x^20*u +
18092*x^19*u^2 - 67012*x^18*u^3 + 102591*x^17*u^4 + 378*x^20 - 8178*x^19*u + 58447*x^18*u^2 - 173283*x^17*u^3 +
216476*x^16*u^4 + 774*x^19 - 14247*x^18*u + 103331*x^17*u^2 - 297137*x^16*u^3 + 334741*x^15*u^4 + 1458*x^18 - 31130*x^17*u
+ 180514*x^16*u^2 - 358567*x^15*u^3 + 360468*x^14*u^4 + 10605*x^17 - 90380*x^16*u + 290195*x^15*u^2 - 395289*x^14*u^3 +
240873*x^13*u^4 + 20415*x^16 - 159334*x^15*u + 394529*x^14*u^2 - 407100*x^13*u^3 + 44248*x^12*u^4 + 22701*x^15 -
112959*x^14*u + 418497*x^13*u^2 - 493887*x^12*u^3 - 105112*x^11*u^4 + 25606*x^14 - 115611*x^13*u + 111265*x^12*u^2 -
417580*x^11*u^3 - 92961*x^10*u^4 + 1092*x^13 - 103527*x^12*u + 145152*x^11*u^2 - 88490*x^10*u^3 - 92811*x^9*u^4 +
48856*x^12 + 186438*x^11*u + 267721*x^10*u^2 - 155622*x^9*u^3 - 45395*x^8*u^4 - 27776*x^11 - 191295*x^10*u -
178159*x^9*u^2 - 70489*x^8*u^3 + 16905*x^7*u^4 - 61956*x^10 - 74059*x^9*u + 378244*x^8*u^2 + 232801*x^7*u^3 +
15979*x^6*u^4 + 74366*x^9 + 338472*x^8*u + 227589*x^7*u^2 - 74613*x^6*u^3 - 16012*x^5*u^4 - 87675*x^8 - 182672*x^7*u -
189206*x^6*u^2 + 26802*x^5*u^3 + 25133*x^4*u^4 - 85989*x^7 - 42976*x^6*u + 119160*x^5*u^2 + 38380*x^4*u^3 - 14569*x^3*u^4
+ 57369*x^6 + 50376*x^5*u - 22878*x^4*u^2 - 26236*x^3*u^3 + 5653*x^2*u^4 - 19638*x^5 - 66959*x^4*u + 10199*x^3*u^2 +
7737*x^2*u^3 - 1185*x*u^4 - 18109*x^4 + 33891*x^3*u - 10338*x^2*u^2 + 126*x*u^3 + 90*u^4 + 8894*x^3 - 13882*x^2*u +
3365*x*u^2 - 189*u^3 - 1493*x^2 + 903*x*u - 105*u^2 - 176*x + 18*u + 4]
```

Describing T

Let $p > 2$.

To work with the residue disks of T, we construct a homeomorphism $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$ given by convergent power series.
This map factors through a homomorphism from $\mathcal{M}^\times(\mathbb{Q}_p)$ to the trivial biextension $\mathbb{Q}_p^2 \times \mathbb{Q}_p^2 \times \mathbb{Q}_p$, which can be written using p-adic heights.

In this trivial biextension, the section $\widetilde{j_b}(z)$ is

$$(\log([z-b]), \log([A_\alpha|_{z\times X}]), h_p(z-b, A_\alpha|_{z\times X})) \in \mathbb{Q}_p^2 \times \mathbb{Q}_p^2 \times \mathbb{Q}_p.$$

Working in the trivial biextension makes our computations much easier. The hard part will be computing $h_p(z-b, A_\alpha|_{z\times X})$.

Embedding the curve

Let $p = 7$.
Recall $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$ is our constructed homeomorphism.

Proposition

Let $\mathbb{Z}_p \to X(\mathbb{Z}_p)_{\overline{P}}$ be the parametrization of the residue disk with parameter equal to the x-coordinate. Define the map $\lambda : \mathbb{Z}_p \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ to be the composition of this parametrization $\mathbb{Z}_p \to X(\mathbb{Z}_p)_{\overline{P}}$ and $\widetilde{j_b}$. Then the map $\varphi \circ \lambda$ is given by convergent power series and modulo p is

$$\nu \mapsto (2\nu, 0, 6 - \nu).$$

Computing $\widetilde{j}_b$

To get λ mod p, we parametrize

$$\begin{aligned} \{0, ..., p-1\} &\to X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}} \\ \nu &\mapsto P_\nu := (\nu p, -1). \end{aligned}$$

To compute $\widetilde{j}_b(P_\nu)$, we will compute $\widetilde{j}_b(P_0)$ and $\widetilde{j}_b(P_1)$ and interpolate.
An easier calculation shows $\varphi \circ \widetilde{j}_b(P_0) = (0, 0, 6)$. We discuss $\varphi \circ \widetilde{j}_b(P_1)$ the more general example.

Local heights

Recall: the hard part of finding $\varphi \circ \widetilde{j_b}(P_1)$ is computing $H := h_p(P_1 - b, A_\alpha|_{P_1 \times X})$.

Sage and Magma have an implementation of local heights based on an algorithm by Balakrishnan and Besser.

Implementation requires $A_\alpha|_{P_1 \times X}$ can be written as a sum of $\mathbb{Q}_p$-points, which is not possible.

Local heights cont.

Over $\mathbb{Z}/p^2\mathbb{Z}$, we have $A_\alpha|_{P_1\times X} = D_f|_{P_1\times X} + D_f|_{b\times X} - D_f|_\Delta$. Using "explicit Cantor's algorithm" (with code by Sutherland) we can write

$$2D_f|_{P_1\times X} = \sum_i Q_i + \operatorname{Div} g_1.$$

Over $\mathbb{Q}$ we have

$$D_f|_{b\times X} - D_f|_\Delta = \sum_j R_j + \operatorname{Div} g_2.$$

Altogether:

$$H = 1/2 h_p(P_1 - b, \sum_i Q_i + 2\sum_j R_j)$$
$$+ 1/2\log(g_1(P_1 - b)) + \log(g_2(P_1 - b)).$$

Yields $\varphi(\widetilde{j_b}(P_1)) = (2, 0, 5)$.

Integer points on T

We construct a map $\kappa : \mathbb{Z}_p^2 \to T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})}$ with image exactly $\overline{T(\mathbb{Z})}_{\widetilde{j_b}(\overline{P})}$.

Proposition

Recall the bijection $\varphi : T(\mathbb{Z}_p)_{\widetilde{j_b}(\overline{P})} \to \mathbb{Z}_p^3$. The map $\varphi \circ \kappa : \mathbb{Z}_p^2 \to \mathbb{Z}_p^3$ is given by convergent power series, and modulo p is given by

$$(n_1, n_2) \mapsto (n_1, -n_1 - 2n_2, -3n_1^2 - n_1 n_2 - n_1 + n_2 - 1).$$

We use the biextension structure to construct many integer points in $T(\mathbb{Z})$ lying over integer points in $J(\mathbb{Z})$.

An upper bound

Recall that modulo p

$$
\begin{aligned}
(\varphi \circ \kappa)(n_1, n_2) =& (n_1, -n_1 - 2n_2, -3n_1^2 - n_1 n_2 - n_1 + n_2 - 1), \\
(\varphi \circ \lambda)(\nu) =& (2\nu, 0, 6 - \nu).
\end{aligned}
$$

Intersect $\widetilde{j_b}(X(\mathbb{Z}/p^2\mathbb{Z})_{\overline{P}})$ and $T(\mathbb{Z}/p^2\mathbb{Z})_{\widetilde{j_b}(\overline{P})}$. Get two solutions:

$$
(\nu, n_1, n_2) \in \{(0,0,0), (4,1,3)\}.
$$

Proposition

The integer points $X(\mathbb{Z})$ reducing to $(0,-1) \in X(\mathbb{F}_7)$ are contained in the set

$$
\{(0,-1), (4 \cdot 7 + O(7^2), 6 + O(7^2))\}.
$$