Distribution of traces of genus 3 curves over finite fields

R. Lercier, C. Ritzenthaler, Florent Rovetta, Jeroen Sijsling and Ben Smith

IRMAR (Rennes 1)

Linz, November 2013

Overview

- Existence of a curve with a given Weil polynomial
- Distribution of curves with respect to their Weil polynomial
- How to span curves?

How (much) does geometry rule arithmetic?

Case $g = 0$.

- Riemann-Roch: $\ell(-\kappa) = 2 - g + 1 + \ell(2\kappa) = 3$. Let x, y, z be a basis of $\mathcal{L}(-\kappa)$
- Riemann-Roch: $\ell(-2\kappa) = 4 - g + 1 + \ell(3\kappa) = 5$. $\mathcal{L}(-2\kappa)$ contains $x^2, xy, xz, y^2, yz, z^2 \Rightarrow C$ is a plane conic
- Chevalley-Warning: $C \simeq \mathbb{P}^1$
- $\#C(\mathbb{F}_{p^n}) = p^n + 1$

C : smooth projective absolutely irreducible curve of genus $g > 0$ over a finite field $k = \mathbb{F}_p$ with $p > 3$.

Weil polynomial

$$\chi_C(X) = \prod_{i=1}^{g}(X - \sqrt{p}e^{i\theta_i})(X - \sqrt{p}e^{-i\theta_i}) \in \mathbb{Z}[X], \quad \theta_i \in [0, \pi].$$

$$\#C(\mathbb{F}_{p^n}) = 1 + p^n - 2 \cdot p^{n/2} \cdot \sum_{i=1}^{g} \cos(\theta_i^n).$$

Case $g = 1$.

- $\chi_C(X) = X^2 - tX + p$ with $|t| \leq 2\sqrt{p}$ (Hasse bound).
- (Deuring 41, Waterhouse 69): all values of t are possible.

The general strategy for small g

C : smooth projective absolutely irreducible curve of genus $g > 1$ over $k = \mathbb{F}_p$ with $p > 3$.

$$\begin{array}{ccccc} \{\text{hyp. curves}\}_{/\simeq_{\bar{k}}} & \subset & \{\text{curves}\}_{/\simeq_{\bar{k}}} & \to & \{\text{abelian var. of dim. } g\}_{/\simeq_{\bar{k}}} \\ & & C & \mapsto & \mathrm{Jac}(C) \end{array}$$

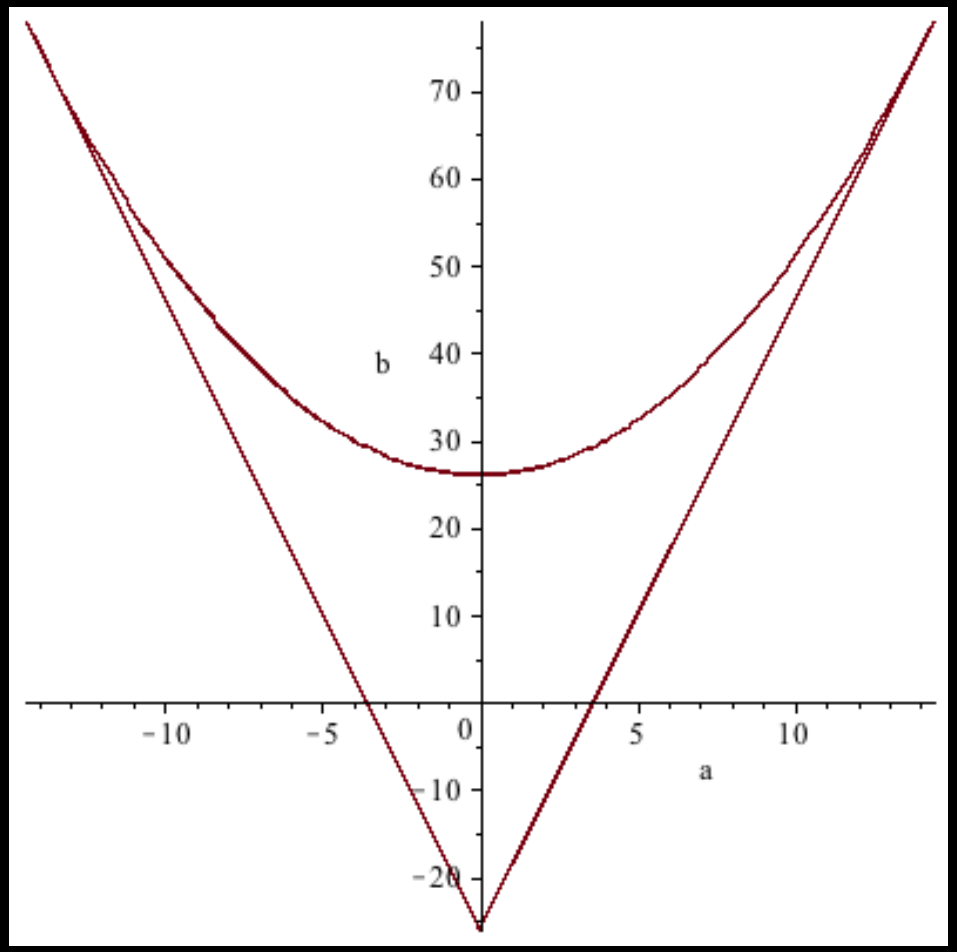
$2g-1$	$3g-3$	$\frac{g(g+1)}{2}$	dim.
3	3	3	$g=2$
5	6	6	$g=3$
7	9	10	$g=4$

(Honda-Tate 66-68) : any Weil polynomial is a Weil polynomial of an abelian variety over k.

(Rück 90, Xing 94, Haloui-Singh 11) complete description for $g \leq 4$ over $\mathbb{F}_q$.

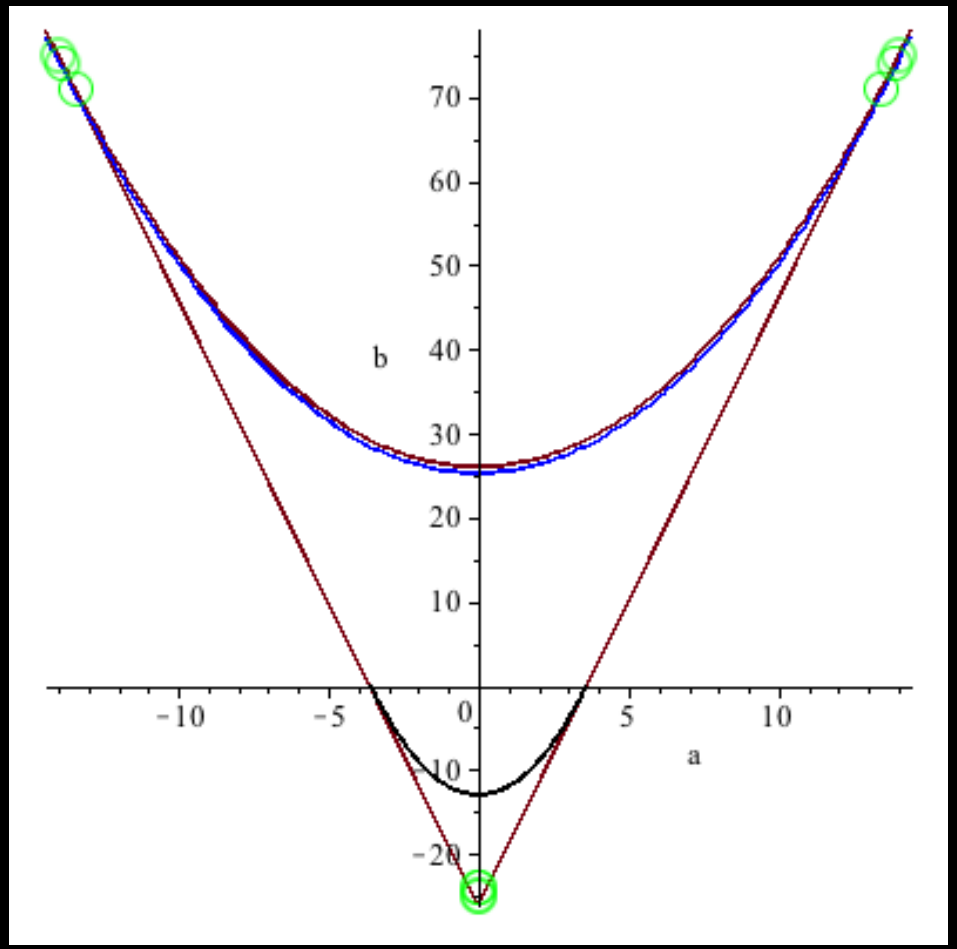
(Honda-Tate 66-68) : any Weil polynomial is a Weil polynomial of an abelian variety over k.

Case $g = 2$. $\chi_A(X) = X^4 + aX^3 + bX^2 + paX + p^2$



(Honda-Tate 66-68) : any Weil polynomial is a Weil polynomial of an abelian variety over k.

Case $g = 2$. (Serre 83, Rück 90, McGuire-Voloch 05, Maisner-Nart 07, Howe 08, Howe-Nart-R. 09)



Serre's obstruction: $g \geq 3$

Serre (1983) : "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

$\mathcal{A}_g(k) =$ the set of abelian varieties of dim. g over k which are non hyperelliptic Jacobians over $\bar{k}$.

$$\begin{array}{ccc} \mathcal{A}_g(k) & \to & k^*/(k^*)^2 \simeq \{\pm 1\} \\ A & \mapsto & \epsilon \end{array}$$

Serre's obstruction : $A \in \mathcal{A}_g(k)$ is a Jacobian (over k) if and only if $\epsilon = 1$.

Consequence

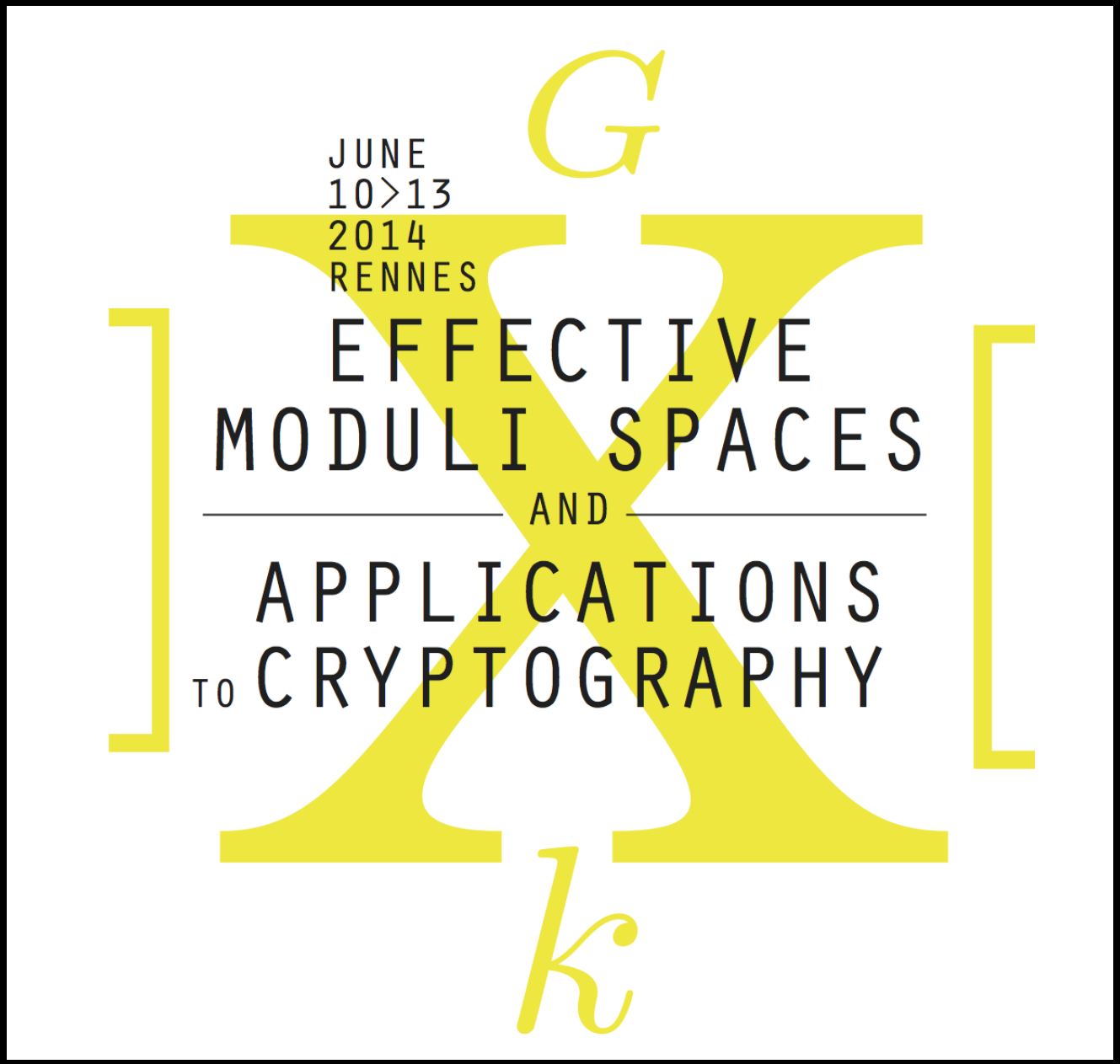
$A \in \mathcal{A}_g(\mathbb{F}_p)$ with trace t gives a curve of genus g over k with $1 + p - \epsilon \cdot t$ rational points.

(Lauter 02) : $\forall p$, there exists C of genus 3 over $\mathbb{F}_p$ such that

$$|\#C(\mathbb{F}_p) - (p+1)| \geq 3\lfloor 2\sqrt{p} \rfloor - 3.$$

Question: close formula for $N_p(3) = \max_{C/\mathbb{F}_p}(\#C(\mathbb{F}_p))$?

Partial solutions: (Howe-Leprevost-Poonen 00, Nart-R. 08,10, R. 10, Alekseenko-Aleshnikov-Markin-Zaytsev 11, Mestre 13, R.-Robert work in progress).

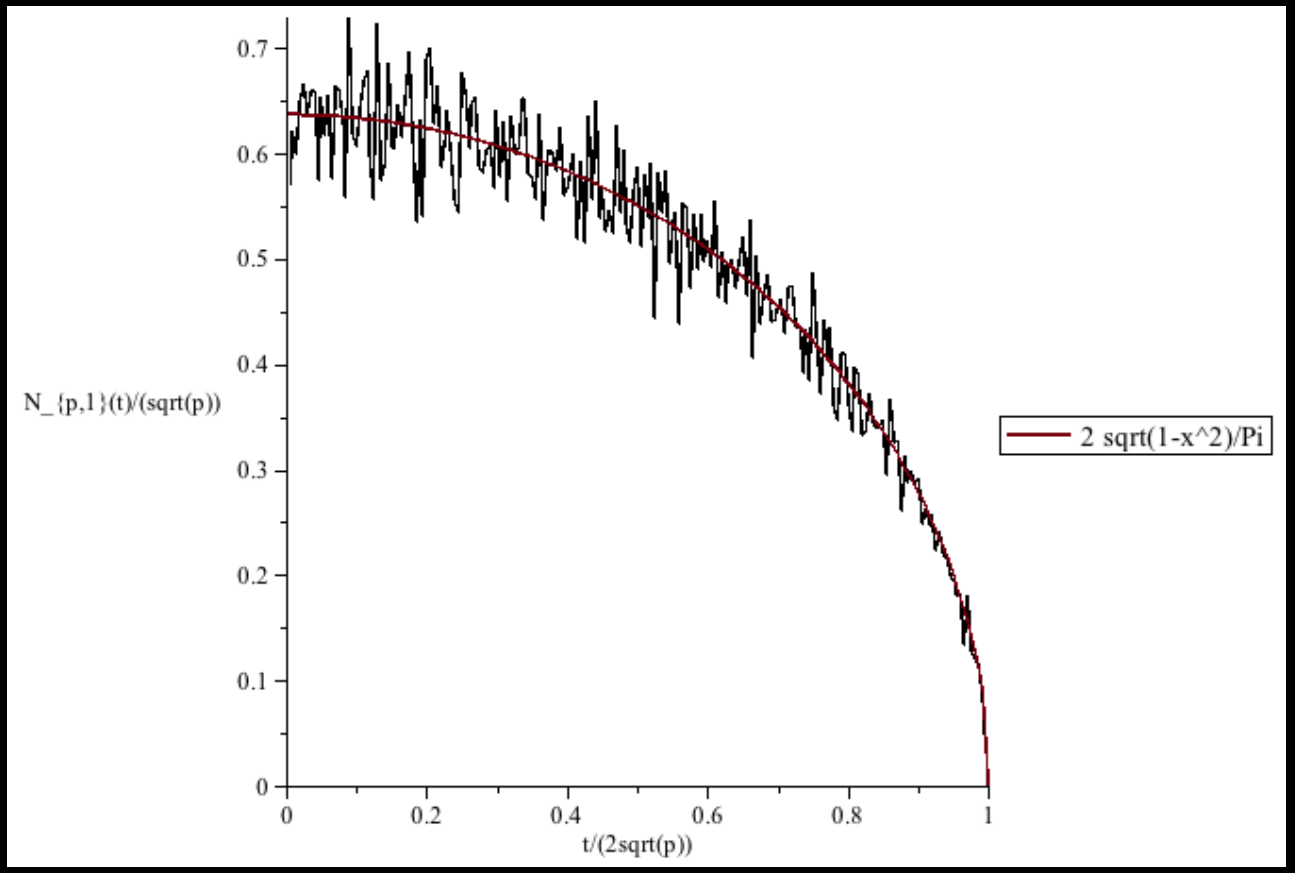


http://www.lebesgue.fr/SEMESTRE2014/

Distribution: case $g = 1$

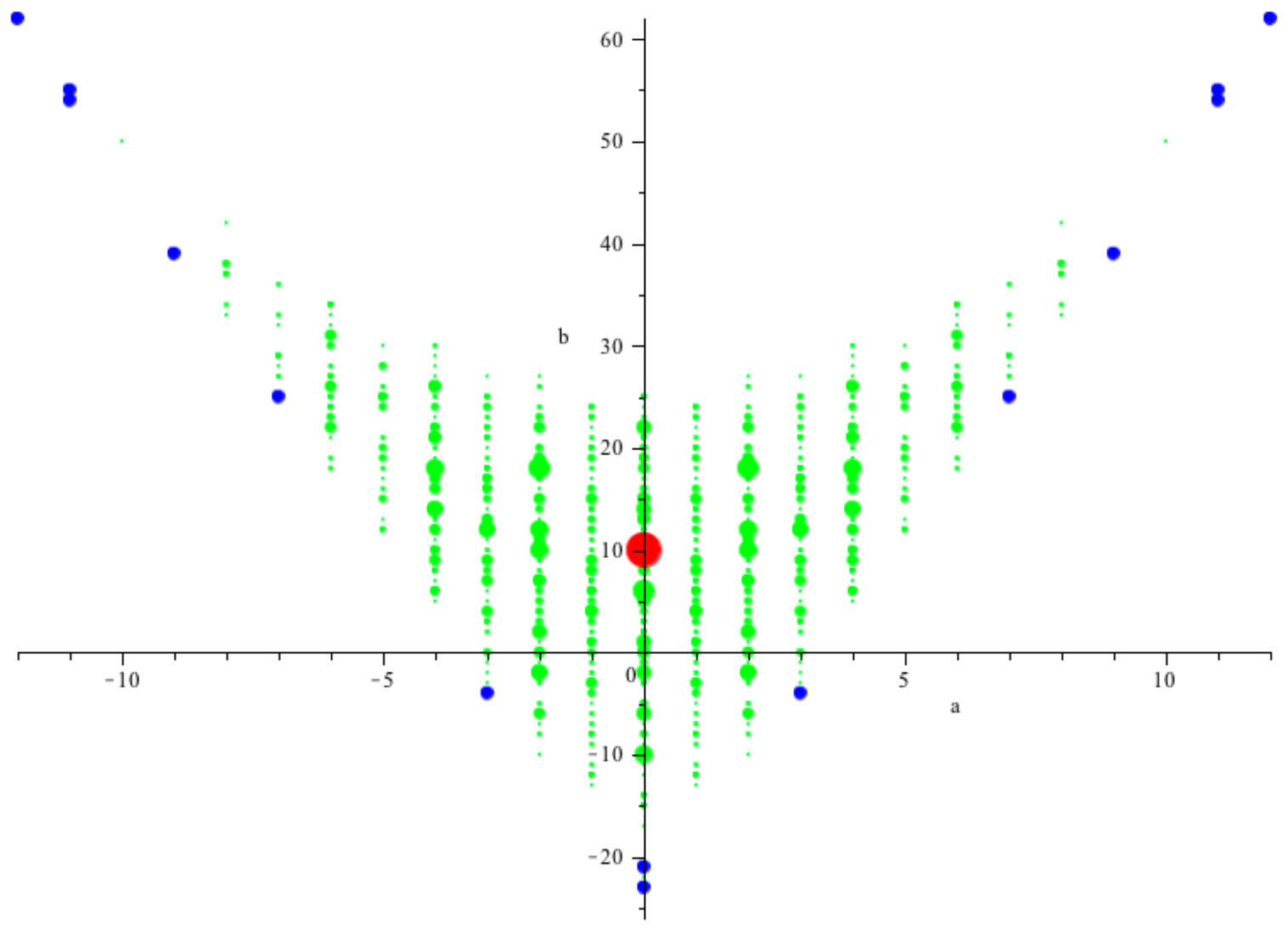
(Deuring 41) : for any $|t| \leq 2\sqrt{p}$,

$$N_{p,1}(t) := \#\{\text{genus } 1\ C/\mathbb{F}_p \text{ s.t. } \mathrm{trace}(C) = t\}_{/\simeq} = \mathcal{H}(t^2 - 4p)$$

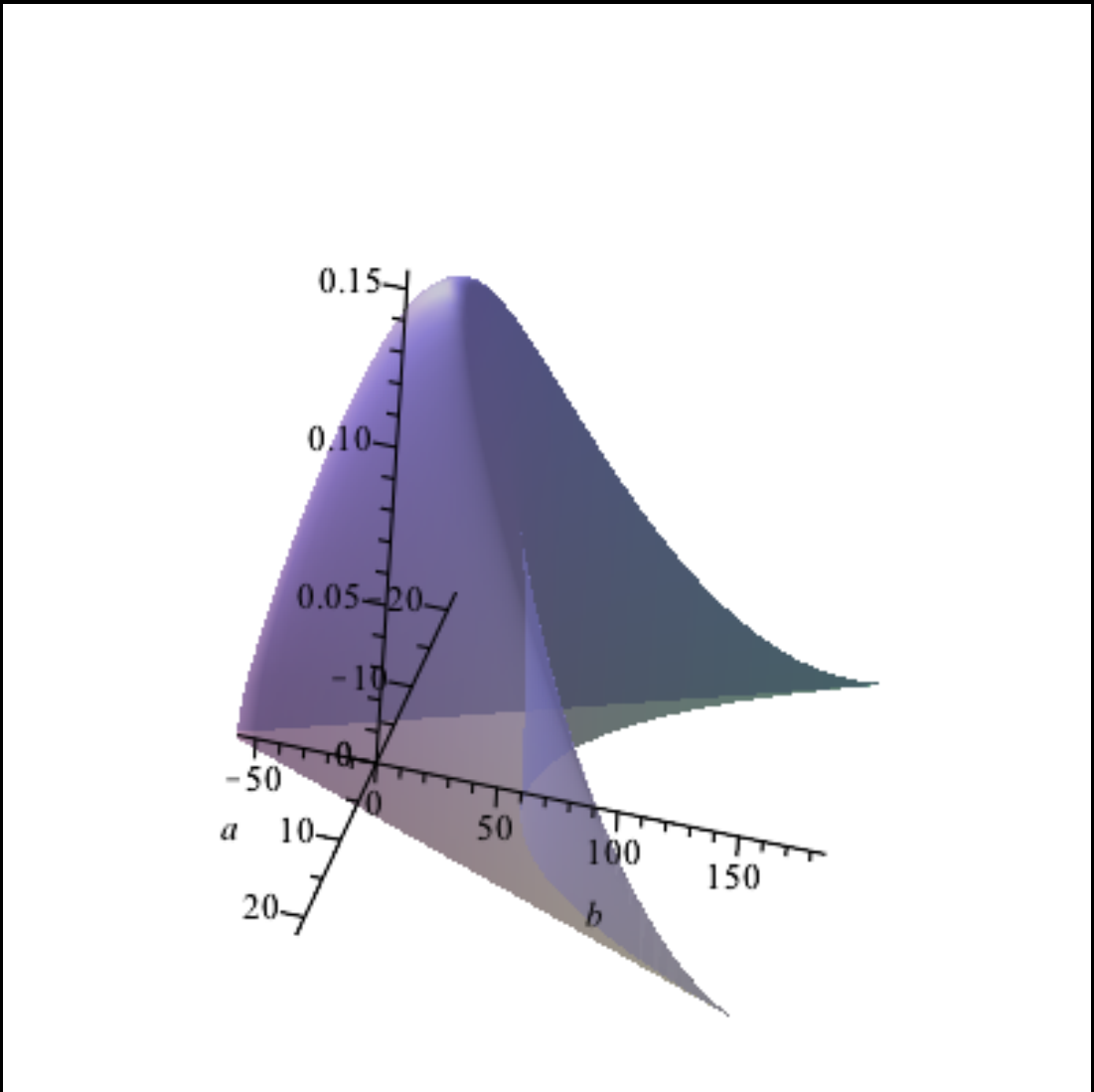


Asymptotic distribution (Birch 68, Gekeler 03, Katz 09)

Distribution: case $g = 2$, $X^4 + aX^3 + bX^2 + paX + p^2$



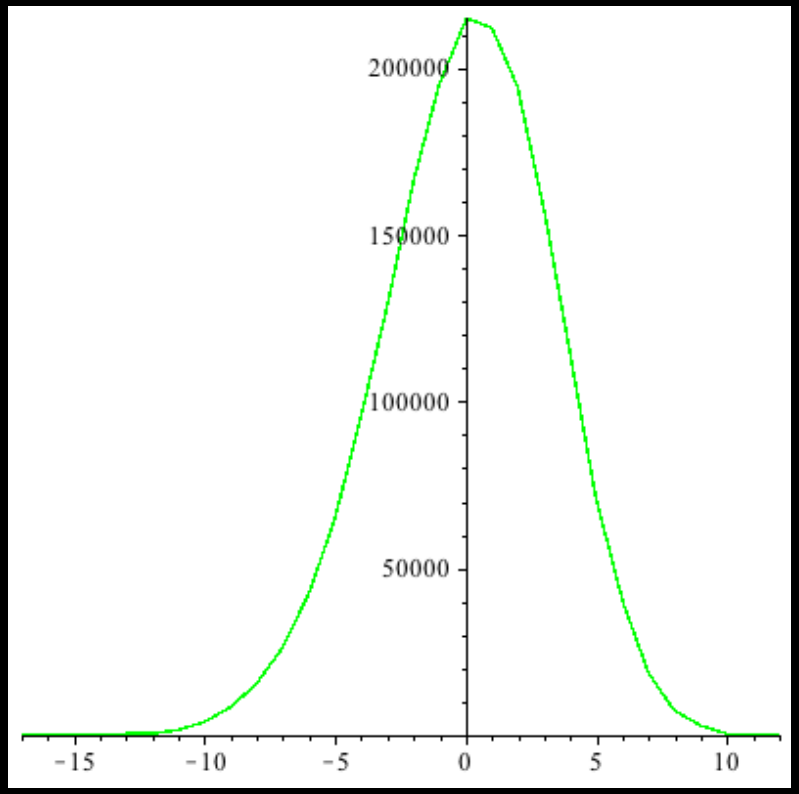
Distribution: case $g = 2$, $X^4 + aX^3 + bX^2 + paX + p^2$



(Katz-Sarnak 91, Williams 12, Howe, Achter-Howe work in progress)

Distribution of the trace for $g = 3$

$$N_{p,3}(t) = \#\{C/\mathbb{F}_p \text{ genus 3 non hyp. with } \mathrm{trace}(C) = t\}_{/\simeq}$$

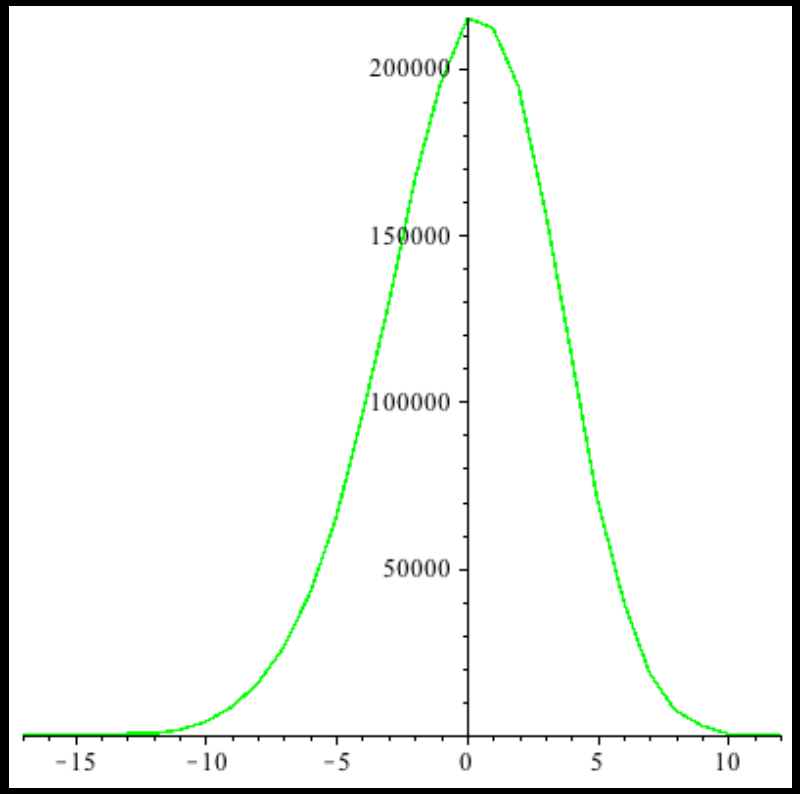


Graph of $N_{11,3}(t)$

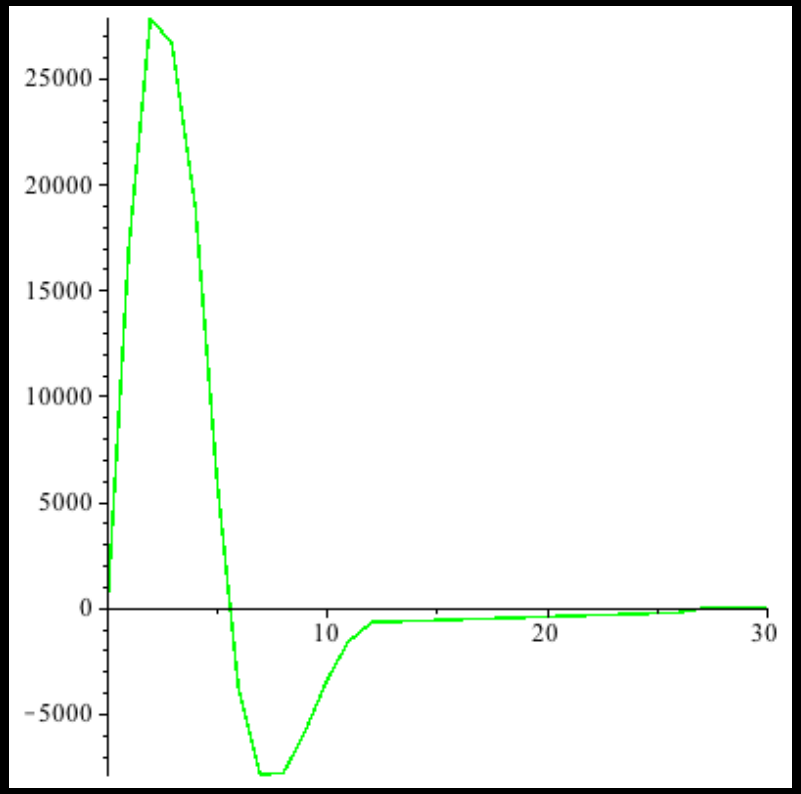
Distribution of the trace for $g = 3$

$$N_{p,3}(t) = \#\{C/\mathbb{F}_p \text{ genus 3 non hyp. with } \mathrm{trace}(C) = t\}_{/\simeq}$$

$\Rightarrow V_{p,3}(t) = N_{p,3}(t) - N_{p,3}(-t)$



Graph of $N_{11,3}(t)$

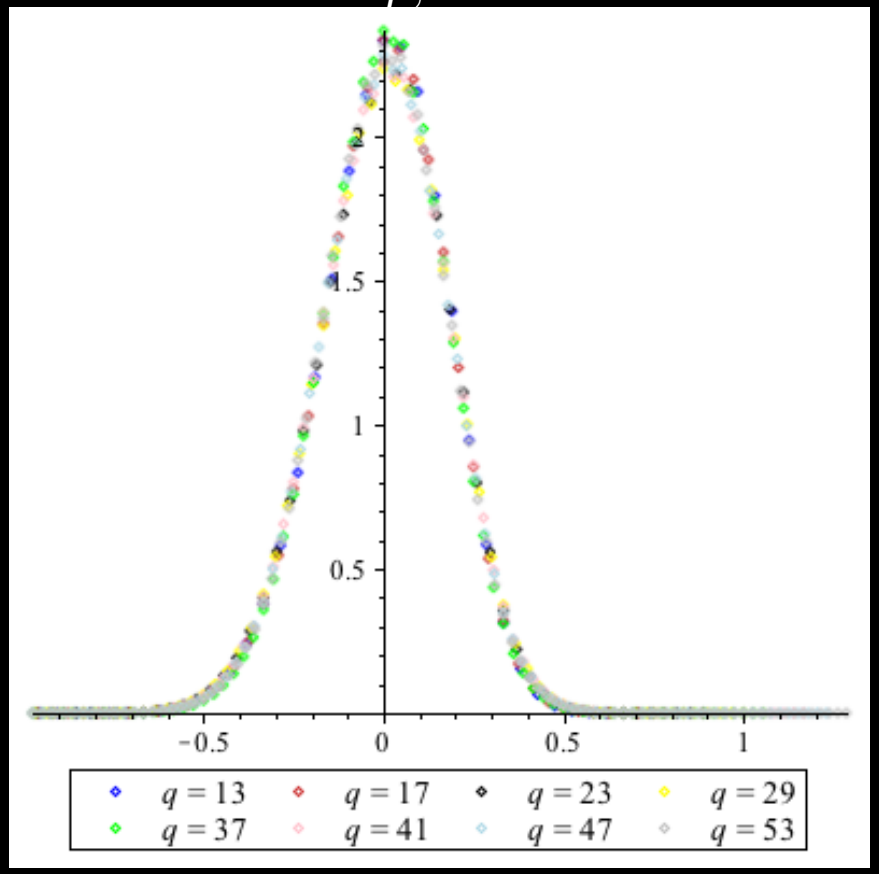


Graph of $V_{11,3}(t)$

Normalization in p

$$N_{p,3}^{\mathrm{KS}}(x) = 6 \cdot p^{-11/2} \cdot N_{p,3}(t), \quad t = \lfloor 6\sqrt{p} \cdot x \rfloor, \quad x \in [-1, 1]$$

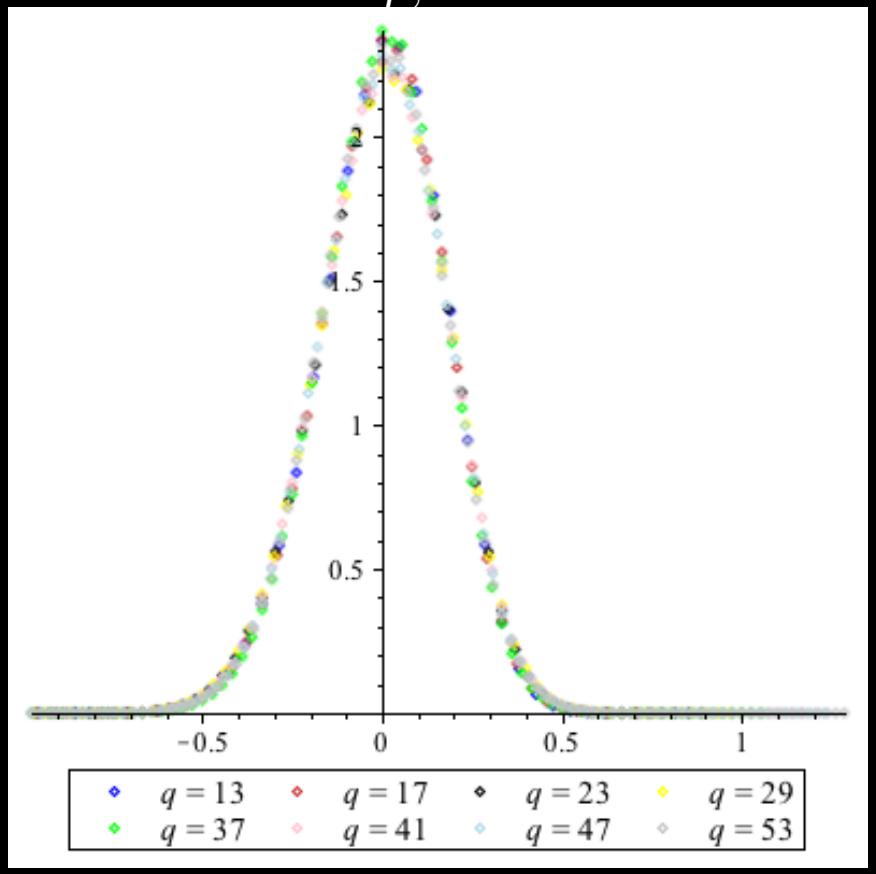
$N_{p,3}^{\mathrm{KS}}(x)$



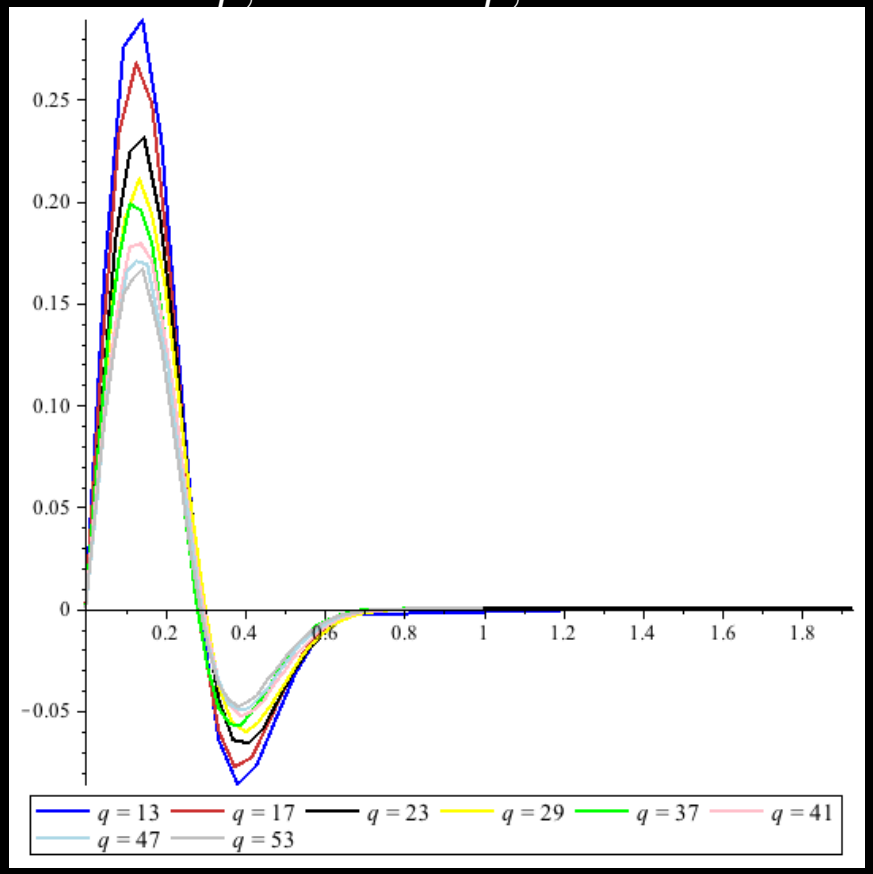
Normalization in p

$$N_{p,3}^{\mathrm{KS}}(x) = 6 \cdot p^{-11/2} \cdot N_{p,3}(t), \quad t = \lfloor 6\sqrt{p} \cdot x \rfloor, \quad x \in [-1, 1]$$

$N_{p,3}^{\mathrm{KS}}(x)$



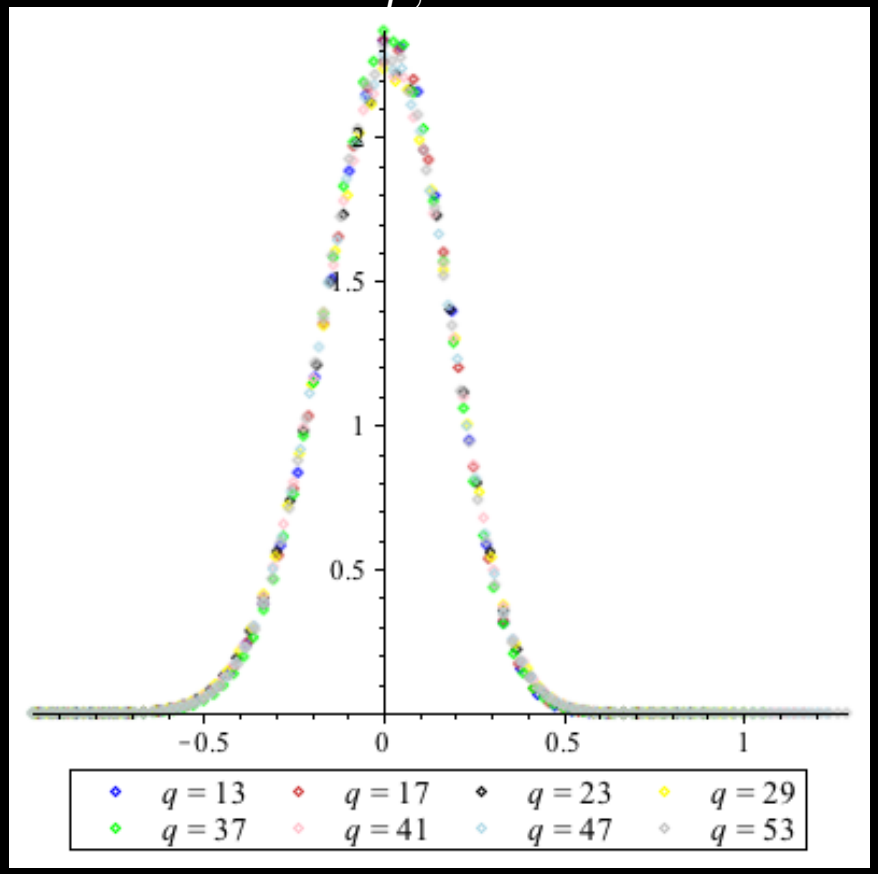
$N_{p,3}^{\mathrm{KS}}(x) - N_{p,3}^{\mathrm{KS}}(-x)$



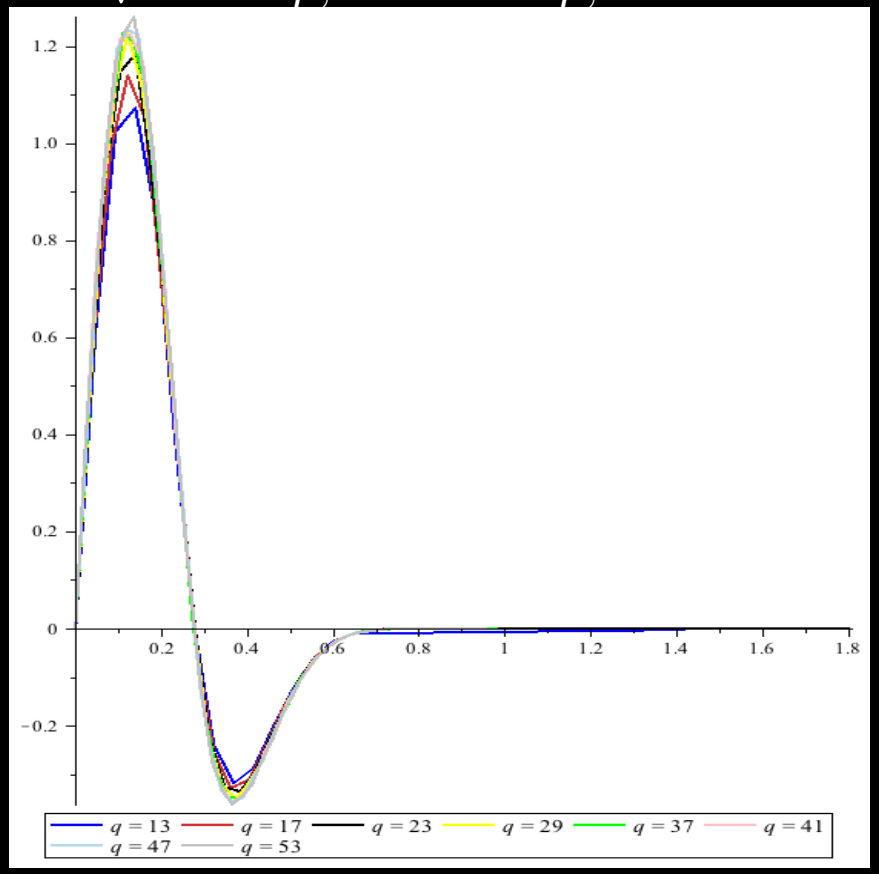
Normalization in p

$$N_{p,3}^{\mathrm{KS}}(x) = 6 \cdot p^{-11/2} \cdot N_{p,3}(t), \quad t = \lfloor 6\sqrt{p} \cdot x \rfloor, \quad x \in [-1, 1]$$

$N_{p,3}^{\mathrm{KS}}(x)$



$\sqrt{p} \cdot (N_{p,3}^{\mathrm{KS}}(x) - N_{p,3}^{\mathrm{KS}}(-x))$



Send applications to Kohel, Ritzenthaler and Shparlinski

How to span curves over $\mathbb{F}_p$?

Hyperelliptic curves:

- Genus ≤ 3: use invariants + twists (Lercier-R. 09,12)
- In general: contained in 3 families with $2g$ coefficients
- Check isomorphisms (Lercier-R.-Sijsling 13)

Non hyperelliptic (non trigonal, $g \neq 6$) curves:

- (Petri 22) intersection in $\mathbb{P}^{g-1}$ of

$$\frac{g(g+1)}{2} - (3g-3) = \frac{(g-2)(g-3)}{2}$$

  quadrics $\Rightarrow \frac{(g+1)g(g-2)(g-3)}{4} = O(g^4)$ coefficients

- Over $\bar{k}$: $\frac{(g-1)(g-2)(g-3)}{2} = O(g^3)$ coefficients (Saint-Donat 73)

Genus 3 non hyperelliptic curves

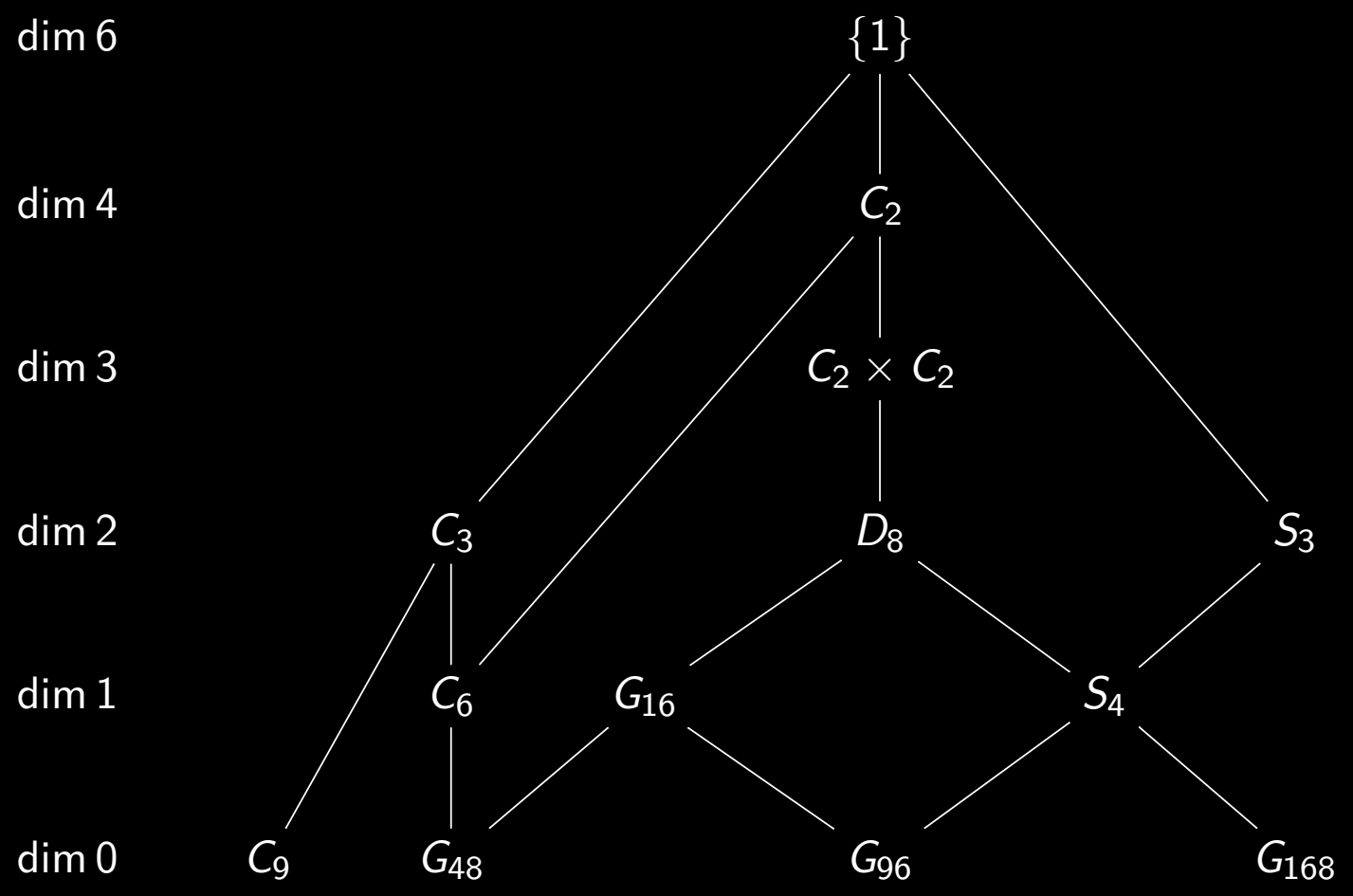
It is not possible to compute the classes naively

- too many plane smooth quartics $\approx p^{14}$
- Magma function `IsIsomorphic()` is bugged and too slow

It is not possible to do it as for hyperelliptic curves of genus $g \leq 3$

- no reconstruction of a generic quartic from its 13 Dixmier-Ohno invariants

Automorphism strata after (Henn 76, Vermeulen 83, Magaard et al. 05, Bars 06 $(\mathrm{char}(k) \neq 2, 3))$:



How to describe the strata?

Given a locus $S \subset \mathrm{M}_g$, $\mathcal{C}/\mathcal{S}$ is a geometrically normal family for S/k if $\dim S = \dim \mathcal{S}$ and $\phi : \mathcal{S} \to S$ is surjective.

4	C_2	$x^4 + x^2(ay^2 + byz + cz^2) + zy^3 + \frac{y^2z^2}{4} - \frac{36yz^3}{j-1728} - \frac{z^4}{j-1728}$
3	$C_2 \times C_2$	$ax^4 + by^4 + cz^2 + \epsilon x^2y^2 + y^2z^2 + z^2x^2$, $\epsilon = 0, 1$
2	C_3	$\begin{cases} x^3z + y^4 + ay^2z^2 + ayz^3 + bz^4 & a \neq 0 \\ x^3z + y^4 + ayz^3 + az^4 & a \neq 0 \end{cases}$
2	S_3	$x^3z + y^3z + x^2y^2 + axyz^2 + bz^4$
2	D_8	$x^4 + y^4 + z^4 + ax^2y^2 + bxyz^2$
1	C_6	$z^3y + x^4 + ax^2y^2 + y^4$
1	G_{16}	$x^4 + y^4 + z^4 + ay^2z^2$
1	S_4	$x^4 + y^4 + z^4 + a(x^2y^2 + y^2z^2 + z^2x^2)$
0	C_9	$x^4 + xy^3 + yz^3$
0	G_{48}	$x^3y + y^4 + z^4$
0	G_{96}	$x^4 + y^4 + z^4$
0	G_{168}	$x^3y + y^3z + z^3x$

Not good enough:

1. if $s \in S(k)$, none of the fibers $\mathcal{C}_{\phi^{-1}(s)}$ may be defined over k
2. ϕ may not be injective

Definition

Given a locus $S \subset \mathrm{M}_g$ over a field k, $\mathcal{C}/\mathcal{S}$ is a universal family for S if ϕ is an isomorphism.

Rem.: injectivity implies that the field of moduli is a field of definition.

For quartics: the field of moduli is a field of definition if $\mathrm{Aut}(C) \not\simeq C_2$ (Artebani, Quispe 12).

Theorem

We give explicit universal families for all strata in M_3 *but* $\mathrm{Aut}(C) \simeq \{1\}$ *and* $\mathrm{Aut}(C) \simeq C_2$ *(5 coefficients).*

Rem./Questions: in the case $\mathrm{Aut}(C) \simeq \{1\}$

- geometrically normal families are known (Weber 1876, Shioda 93)
- we use a family found by Bergström with 7 coefficients
- down to 6?