

p -torsion of curves in characteristic p

(in part with Darren Glass and with June Hui Zhu)

April 24, Galois theory workshop
University of Pennsylvania

Abstract

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Understanding the p -torsion of Jacobians of curves in characteristic p is a fantastic problem in number theory.

This topic has applications to codes, cryptography, and Galois covers and representations.

There are many open problems about the existence of curves whose p -torsion has given invariants such as p -rank, a -number, group scheme, or Newton polygon.

In this talk, I will introduce these problems, give a survey of the literature, give a proof of some recent results, and describe some open questions.

Preview - more precise later

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Every component of the moduli space of hyperelliptic curves of genus g with p -rank f has dimension $g + f - 1$, (Glass-P for $p \geq 3$, Zhu for $p = 2$).

Look at the moduli space of curves of genus g with p -rank f . When $f = g - 2$ or $f = g - 3$, the generic point of every component has a -number 1, and the analogous result is true for hyperelliptic curves with $f = g - 2$, (P).

When $f = g - 2$, there exist (hyperelliptic) curves with a -number 2 (and family of these has expected dimension). When $f = g - 3$, all four types of p -torsion occur, (P).

These results lead us to open questions which can be tackled with many approaches (computational, geometric).

p -torsion in the complex case

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Let $E = \mathbb{C}/L$ be a complex elliptic curve (genus 1).

E is an abelian group.

The p -torsion $E[p]$ is the kernel of multiplication by p .

Then $E[p] = \frac{1}{p}L/L \simeq (\mathbb{Z}/p)^2$.

More generally,

Let X be a Riemann surface of genus g with Jacobian J_X .

Then J_X is a p.p. abelian variety of dimension g .

Also $J_X[p] \simeq (\mathbb{Z}/p)^{2g}$.

p -torsion in characteristic p

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Now, let k be an algebraically closed field of characteristic p .

If E is an elliptic curve over k , then $|E[p](k)| < p^2$.

Typically, $|E[p](k)| = p$ and E is *ordinary*.

Otherwise, $|E[p](k)| = 1$ and E is *supersingular*.

There are exactly $(p-1)/2$ choices of λ for which the elliptic curve $y^2 = x(x-1)(x-\lambda)$ is supersingular, Igusa.

(These are the solutions to a hypergeometric differential equation.)

The p -rank of $J_X[p]$

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Let X be a smooth projective k -curve of genus g .

Its Jacobian J_X is a p - p . abelian variety of dimension g .

Then $|J_X[p](k)| = p^{f_X}$ for some $0 \leq f_X \leq g$.

We say that f_X is the p -rank of X .

Also $f_X = \max\{f \in \mathbb{N} \mid \exists \text{ étale } Z \xrightarrow{(\mathbb{Z}/p)^f} X\}$.

The p -rank can only decrease under specialization, Katz.

For fixed p and X , one can compute $f_X = \dim(\text{im } C^g)$ where C is the Cartier operator on $H^0(X, \Omega_1)$.

Calculations are tricky since C is only semi-linear.

Yui: hyperelliptic curves

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Consider $Y : y^2 = h(x)$ where $h(x) = \prod_{i=1}^{2g+1} (x - \lambda_i)$.

Let c_r be the coefficient of x^r in the expansion of $h(x)^{(p-1)/2}$.

Let A_g be the $g \times g$ matrix whose ij th entry is c_{ip-j} .

Yui: Y is ordinary if and only if $D = \det(A_g) \neq 0$.

The p -rank of Y is $f_Y = \text{rank}(M)$ where $M = \prod_{i=0}^{g-1} (A_g^{(p^i)})$.

One expects that decreasing f_Y by one gives exactly one new restriction on $\{\lambda_i\}$.

Without more information, it is not clear how to use this even to guarantee the existence of a hyperelliptic curve with genus g and p -rank f for every p, g, f .

Moduli spaces

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Consider the moduli space \mathcal{M}_g of k -curves of genus g or the moduli space \mathcal{H}_g of hyperelliptic k -curves of genus g . (All curves are smooth, connected, and projective.)

Recall $\dim(\mathcal{M}_g) = 3g - 3$ and $\dim(\mathcal{H}_g) = 2g - 1$.

Let $V_{g,f} \subset \mathcal{M}_g$ consist of all curves with p -rank $f_X \leq f$.

$$V_{g,0} \subset V_{g,1} \subset \dots \subset V_{g,g-1} \subset V_{g,g} = \mathcal{M}_g.$$

Oort's purity result implies that $\text{codim}(V_{g,f-1}, V_{g,f}) \leq 1$.

Faber & Van der Geer: every component of $V_{g,f}$ has codimension $g - f$ in \mathcal{M}_g (dimension $2g + f - 3$).

Intersection with the hyperelliptic locus

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

For every p , $g \geq 1$ and $0 \leq f \leq g$, there exists a smooth hyperelliptic curve of genus g with p -rank f :

Theorem

(Glass, P): For $p \geq 3$, every component of $V_{g,f} \cap \mathcal{H}_g$ has codimension $g - f$ in \mathcal{H}_g .

So every component of $V_{g,f} \cap \mathcal{H}_g$ has dimension $g + f - 1$.

We skip the proof. It is by induction (first on g with $f = 0$, and then on f). It uses Oort's purity result and results of F & VdG that $V_{g,0} \cap \mathcal{H}_g$ is non-empty and $V_{g,f}$ intersects the boundary $\partial\mathcal{H}_g$. We do a dimension count at different components Δ_i and Δ_0 of $\partial\mathcal{H}_g$.

Zhu: same for $p = 2$; also $\exists X \in \mathcal{H}_g \cap V_{g,f}$ with $\text{Aut}(X) = \mathbb{Z}/2$.

The p -rank of Artin-Schreier curves

(this slide is joint with June Hui Zhu)

Consider $Y : y^p - y = f(x)$ for $f(x) \in k(x)$.

Consider $D = \text{div}_\infty(f) = \sum_{i=0}^r d_i P_i$ with $p \nmid d_i$.

Then $g_Y = (\sum_{i=0}^r (d_i + 1) - 2)(p - 1)/2$ (Riemann-Hurwitz)
and the p -rank is $f_Y = r$ (Düring-Shafarevich).

Let \mathcal{AS}_g be moduli space of Art-Sch curves of genus g .

For $p = 2$, components of $\mathcal{AS}_g \cap V_{g,f}$ have dim. $g + f - 1$.

Can increase p -rank in deformation that splits branch points.

For $p = 3$, components of $\mathcal{AS}_g \cap V_{g,f}$ have different dimensions, but can still deform to increase p -rank.

For $p \geq 5$, components have different dimensions and deformation property appears false, $V_{g,f-1} \not\subset \delta V_{g,f}$.

$E[p]$ as a group scheme

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

If E is ordinary, $E[p] \simeq \mathbb{Z}/p \oplus \mu_p$.

If E is supersingular, there is a unique isomorphism class for $E[p]$ which we denote I_1 . There is a non-split exact sequence $1 \rightarrow \alpha_p \rightarrow I_1 \rightarrow \alpha_p \rightarrow 1$.

Here \mathbb{Z}/p is the constant group scheme;

$\mu_p \simeq \text{Spec}(k[x]/(x-1)^p)$ is the kernel of Frobenius on \mathbb{G}_m ;
and $\alpha_p \simeq \text{Spec}(k[x]/x^p)$ is the kernel of Frobenius on \mathbb{G}_a .

The p -torsion $J_X[p]$ is a group scheme of rank p^{2g} .

Technically, $J_X[p]$ is a symmetric BT_1 group scheme (finite commutative group scheme annihilated by p having actions by Frobenius and Verschiebung homomorphisms).

The p -rank and a -number

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

The p -rank of X is $f_X = \dim_{\mathbb{F}_p} \text{Hom}(\mu_p, J_X)$.

The a -number of X is $a_X = \dim_k \text{Hom}(\alpha_p, J_X)$.

Unlike the p -rank, the a -number is not an isogeny invariant.
The a -number can only increase under specialization, Oort.
Also, $a_X = g_X - \dim_k(\text{im}(C))$ where C is Cartier operator.
Also, $a_X + f_X \leq g_X$.

Genus 2: $y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$

There are 4 possibilities for $J_X[p]$.

The p -rank f	2	1	0	0
The a -number a	0	1	1	2
Dimension in \mathcal{M}_2	3	2	1	0

Some points of common confusion

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

If X is superspecial ($a_X = g_X$) then X is supersingular (all slopes of the Newton polygon equal $1/2$).

The converse is false for $g \geq 2$.

If X is supersingular then the p -rank is $f_X = 0$.

The converse is false for $g \geq 3$.

The Newton polygon of X does not determine the group scheme $J_X[p]$ for $g \geq 2$.

The group scheme $J_X[p]$ does not determine the Newton polygon of X for $g \geq 3$.

Construction for $f = g - 2$ and $a = 2$:

For $i = 1, 2$, let $\phi_i : C_i \rightarrow \mathbb{P}^1$ be hyperelliptic, branched at B_i .
Let $\phi : D \rightarrow \mathbb{P}^1$ be the normalized fibre product of ϕ_1 and ϕ_2 .
It is a $(\mathbb{Z}/2)^2$ -cover.

Its third hyperelliptic quotient $\phi_3 : C_3 \rightarrow \mathbb{P}^1$ is branched at $B_3 = (B_1 \cup B_2) - (B_1 \cap B_2)$.

Prop. If $p > 2$, then $J_D[p] \cong J_{C_1}[p] \oplus J_{C_2}[p] \oplus J_{C_3}[p]$
(isomorphism, not isogeny as in Kani-Rosen)

Prop. Given g , if $p \geq 5$, there exist B_1, B_2 s.t. $f_{C_i} = g_{C_i} - 1$
for $i = 1, 2$, $g_{C_3} = 0$, $g_D = g$, (not obvious, uses Yui, Igusa).

Theorem

(Glass, P): For $p \geq 5$ and $g \geq 2$, there is a hyperelliptic curve D with $J_D[p] \cong (\mu_p \oplus \mathbb{Z}/p\mathbb{Z})^{g-2} \oplus (I_1)^2$.

Questions

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Consider $g \geq 1$ and $0 \leq f \leq g$.

It is now natural to ask:

Which a -numbers and which group schemes occur for (hyperelliptic) curves of genus g with p -rank f ?

If a certain group scheme occurs, describe the sublocus of \mathcal{M}_g of curves with that group scheme: for example, how many components? what are their dimensions?

If $f = g$, then $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^g$ and $a_X = 0$.

If $f = g - 1$, then $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^{g-1} \oplus I_1$ and $a_X = 1$.

For arbitrary g and $f \leq g - 2$, there are not many results.

Non-existence results

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

For small p , not all types of p -torsion occur.

Ekedahl: If X is superspecial ($a = g$), then $g \leq (p^2 - p)/2$.
(generalized by Re).

When $p = 2$, there are no supersingular hyperelliptic curves
with $g = 2^n - 1$, Zhu.

When $p = 2$, if $X \in \mathcal{H}_g \cap V_{g,0}$ then $a_X = \lfloor (g+1)/2 \rfloor$, VdG.

The automorphism group of X puts restrictions on $J_X[p]$,
e.g. Bouw.

The generic group scheme for p -rank f

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Suppose X has genus g and p -rank f where $f \leq g - 1$.
Then $J_X[p] = (\mathbb{Z}/p \oplus \mu_p)^f \oplus \mathbb{G}$ where there are 2^{g-f-1}
possibilities for \mathbb{G} .

Let I_{g-f} be the unique choice of \mathbb{G} with a -number 1.
Here I_{g-f} has rank $p^{2(g-f)}$, p -rank 0, and a -number 1.

I_1 occurs as the p -torsion for a supersingular elliptic curve.
 I_2 , for a supersingular non-superspecial abelian surface.

The Ekedahl-Oort type for I_{g-f} is $[0, 1, \dots, r - 1]$.
The covariant Dieudonné module has relation $F^r = V^r$.

Conj. Generically, one expects $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^f \oplus I_{g-f}$.
This is clearly true when $f = g - 1$.

When $g \geq 2$ and $f = g - 2$

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Then $J_X[p]$ is (A) $(\mathbb{Z}/p \oplus \mu_p)^{g-2} \oplus I_2$ (with $a_X = 1$) or
(B) $(\mathbb{Z}/p \oplus \mu_p)^{g-2} \oplus (I_1)^2$ (with $a_X = 2$).

Let $T_{g,2} \subset \mathcal{M}_g$ be the locus of curves X with $a_X \geq 2$.

Theorem

(P): Case (A) occurs for the generic point of every component of $V_{g,g-2} \cap \mathcal{M}_g$ and (for $p \geq 3$) of $V_{g,g-2} \cap \mathcal{H}_g$.

If $p \geq 5$, then every component of $T_{g,2}$ has codimension 3 in \mathcal{M}_g and case (B) occurs for generic point of every component.

So case (A) occurs in codim 2 in \mathcal{M}_g (and in \mathcal{H}_g for $p \geq 3$).

The generic curve with $a_X \geq 2$ has $f_X = g - 2$.

Case (B) occurs with dimension $3g - 6$ (codim 3 in \mathcal{M}_g).

When $g \geq 3$ and $f = g - 3$

Then $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^{g-3} \oplus \mathbb{G}$ where \mathbb{G} is:

(i) $\mathbb{G} = I_3$, (ii) $\mathbb{G} = I'_3$, (iii) $\mathbb{G} = I_2 \oplus I_1$, or (iv) $\mathbb{G} = (I_1)^3$.

Theorem

(P): Case (i) (p -rank $g - 3$ and $a_X = 1$) occurs for the generic point of every component of $V_{g,g-3} \cap \mathcal{M}_g$.

Let $p \geq 3$. Let g be odd, $g \not\equiv 1 \pmod{p}$, and $g \geq 6(p - 1) + 1$. Then cases (ii), (iii) and (iv) all occur for a curve X of genus g and p -rank $g - 3$.

So case (i) occurs with dimension $3g - 6$ (codim 3 in \mathcal{M}_g).
For cases (ii)-(iv), X is produced as an étale cover of a genus 3 curve, using a result of Raynaud. This leads to restrictions on g .

Also, case (ii) occurs when $p = 2$ and $g \equiv 1 \pmod{4}$ and $g \geq 7$.

Outline of proof using boundary

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

The proofs are by induction using the compactification $\overline{\mathcal{M}}_g$.

In the initial case, when $g_0 = 2$ or $g_0 = 3$,
the Torelli maps $\mathcal{M}_2 \rightarrow \mathcal{A}_2$ and $\mathcal{M}_3 \rightarrow \mathcal{A}_3$ are finite.
Abelian varieties of dim. $g_0 \leq 3$ are well-understood, Oort.

Unfortunately very little is known for $g_0 \geq 4$ and $f = 0$.

Inductive result. If the generic curve of genus g_0 and p -rank 0 has a -number 1 then so does the generic curve of genus $g = g_0 + r$ and p -rank r .

This yields case (A) for $f = g - 2$ and case (i) for $f = g - 3$.
Case (B) for $f = g - 2$ follows, with a similar method.

Difficulty of problem related to codimension of loci.

Proof of inductive result

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Let X be the generic point of a component W of $V_{g,f} \cap \mathcal{M}_g$.

Now $\dim(W) = 2g - 3 + f > \dim(W \cap V_{g,f-1})$, so $f_X = f$.

Assume $a_X > 1$. By Diaz/Looijenga, \overline{W} intersects Δ_0 .

Then $\dim(\overline{W} \cap T_{g,2}) \leq \dim(\overline{W} \cap T_{g,2} \cap \Delta_0) + 1$.

The generic point of $\overline{W} \cap T_{g,2} \cap \Delta_0$ yields a smooth curve X_0 with $g_{X_0} = g - 1$, $f_{X_0} = f - 1$, $a_{X_0} \geq 2$, identified at 2 points.

So $\dim(\overline{W} \cap T_{g,2} \cap \Delta_0) = \dim(V_{g-1,f-1} \cap T_{g-1,2}) + 2$.

By induction, $\dim(V_{g-1,f-1} \cap T_{g-1,2}) < 2g + f - 6$.

Then $\dim(\overline{W} \cap T_{g,2}) < 2g + f - 3$.

This is too small to be generic in W . Thus $a_X = 1$.

Open questions for small genus

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Hyperelliptic curves of genus 3 and p -rank 0

- 1 How many components does $V_{3,0} \cap \mathcal{H}_3$ have?
- 2 Does the generic point of each component have a -number 1? (so far, yes for at least 1 component).
- 3 Does supersingular locus intersect each component?

Curves of genus $g \geq 4$

- 1 Does there exist a curve with p -rank 0 and a -number 1?
- 2 Does there exist a curve with p -rank $g - 3$ and $a = 3$?

Computational evidence for many p should be feasible. Is there a systematic way to produce these curves for all g, p ?

Transversality questions

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

These results imply that some loci are in general position relative to the stratification of \mathcal{A}_g by p -torsion type.

Thm. 1 \implies transversality of \mathcal{H}_g and $V_{g,f}$.

Thm. 3 \implies transversality of $T_{g,2}$ with $V_{g,g-2}$ or $V_{g,g-2} \cap \mathcal{H}_g$.

Thm. 4 \implies transversality of $T_{g,2}$ with $V_{g,g-3}$.

There is a new interpretation of the classification of $J_X[p]$ in terms of Chow classes, VdG & E. There are results on intersection theory of Chow classes, Faber.

How can this be used to study which group schemes occur as the p -torsion of Jacobians of (hyperelliptic) curves?

Summary

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

- We use (Galois) covers to find curves X with interesting p -torsion $J_X[p]$. The Cartier operator is useful for computing $J_X[p]$.
- We use geometric methods to study the dimension of the moduli space of curves of genus g with p -rank f (which are hyperelliptic or Artin-Schreier).
- In some cases, we can show the generic points of components of these moduli space have a -number 1.

Thanks!

Fun approach for $g = 5$ and $a = 3$

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Let $\lambda_1, \lambda_2, \lambda_3$ be distinct supersingular values;
(i.e. each $E_i : y^2 = x(x-1)(x-\lambda_i)$ is supersingular).
There are $\binom{(p-1)/2}{3}$ ways to choose $\{\lambda_i\}_{i=1}^3$.

Which of the 4 possibilities for $J_Y[p]$ occur for the resulting
genus two curve $Y : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$?

For all p , we expect $\{\lambda_i\}_{i=1}^3$ exists so Y is ordinary;
(this is verified by Ritzenthaler for $7 \leq p < 100$).

If so, the fibre product of $\{E_i\}_{i=1}^3$ is a hyperelliptic curve of
genus 5, with p -rank 2 and a -number 3.

For some p , there does not exist $\{\lambda_i\}_{i=1}^3$ so Y has p -rank 0.

Open questions on hyperelliptic curves

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Recall $Y : y^2 = \prod_{i=1}^{2g+1} (x - \lambda_i)$ is ordinary iff $D \neq 0$.

View $D \in k[\lambda_1, \dots, \lambda_{2g+1}]$. It is invariant under S_{2g+1} -action.

One can show that D has degree $d = g(p-1)/2$ in each λ_i .

For generic $\lambda_1, \dots, \lambda_{2g}$ does D have d distinct roots?

We show at least $(p-1)/2$ distinct roots using Igusa.

Are \mathcal{H}_g and $V_{g,g-1}$ *strictly* transversal in \mathcal{M}_g ?

For every choice of $\lambda_1, \dots, \lambda_{2g}$, does there exist λ_{2g+1} so that $D \neq 0$ and Y is ordinary?

Can you deform any hyperelliptic curve to the ordinary locus by moving only one branch point?

Example: Artin-Schreier covers

p -torsion of
curves in
characteristic

p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

For any j so that $p \nmid j$, consider the curve $Y : y^p - y = x^j$.

Then the genus is $g_Y = (p-1)(j-1)/2$ (Riemann-Hurwitz) and the p -rank is $f_Y = 0$ (Düring-Shafarevich).

If $j \mid (p+1)$ then $a_Y = g_Y$ and Y is superspecial.

If $j \mid (p-1)$ then a_Y is about $g_Y/2$.

The Newton polygon of Y has slopes $\{1/j, \dots, (j-1)/j\}$ occurring with equal multiplicity, Katz. (See also Zhu).

There is a messy formula for a_Y when $j \nmid (p \pm 1)$.

Example: Hermitian curve

p -torsion of
curves in
characteristic
 p

Rachel Pries

Introduction

The p -rank

Group
schemes

Summary and
open
questions

Let $q = p^r$ and $X : y^q - y = x^{q+1}$.

Then $g_X = (q^2 - q)/2$ by Riemann-Hurwitz,
and $f_X = 0$ by Düring-Shafarevich, and $a_X \sim g_X/2$.

X is maximal, $\#X(\mathbb{F}_{q^2}) = q^2 + 1 + 2g_X$.

No maximal \mathbb{F}_{q^2} -curve has larger genus, Ihara.

X is the unique maximal curve of this genus, Rück/Stichten.

The $SL_2(\mathbb{F}_q)$ -cover $\phi : X \rightarrow \mathbb{P}_k^1$ has $B = \{0, \infty\}$.

All deformations of ϕ are isotrivial, (P).

If $q = p$, X is the unique such $SL_2(\mathbb{F}_p)$ -curve, Bouw/Wewers.