p-torsion of Curves in Characteristic p

Colin Weir
Simon Fraser University

West Coast Number Theory
December 2013

Outline

Complex Riemann Surfaces

Elliptic Curves (genus 1)

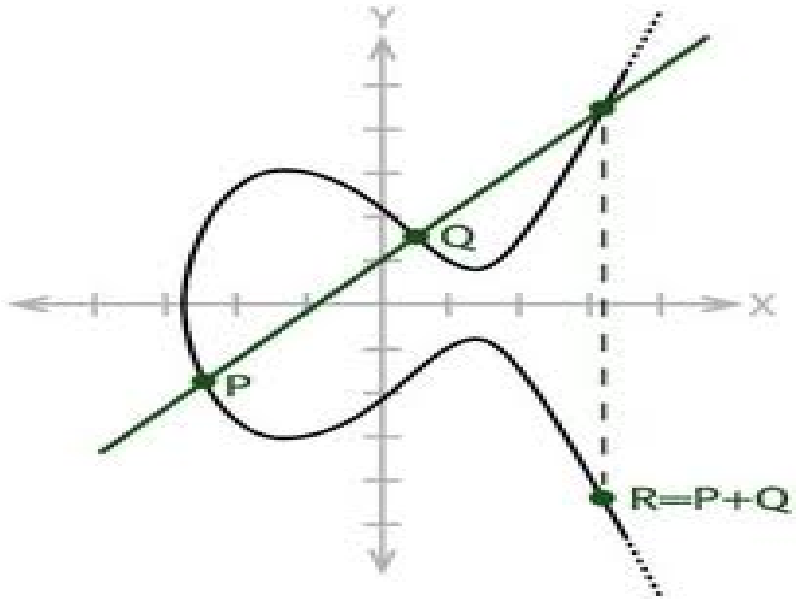
- Let E be an elliptic curve - i.e. $\mathbb{C}/L$
- E is an abelian group.
- The p-torsion $E[p]$ is the kernel of mult. by p
- Then $E[p] = \frac{1}{p}L/L \cong (\mathbb{Z}/p)^2$.

Higher Genus Curves

- Let X be a Riemann Surface of genus g
- It's Jacobian J_X is a g dimensional abelian variety.
- $J_X[p] \cong (\mathbb{Z}/p)^{2g}$

Elliptic Curves in Characteristic p

- Let E be an elliptic curve over $k = \bar{\mathbb{F}}_q$.
- Then $E : y^2 = x^3 + ax^2 + bx + c$ for $p > 2$.
- Algebraic groups law:



- $[\ell] : E \to E$ be mult. by ℓ morphism.
- The ℓ-torsion of E is $E[\ell] = Ker[\ell]$.

Computing the 3 torsion

Recall $E : y^2 = x^3 + ax^2 + bx + c$.

The case $\ell = 3$

$$3Q = Id \Leftrightarrow 2Q = -Q$$
$$\Leftrightarrow x(Q) \text{ is a root of the 3-division polynomial}$$

The 3-division polynomial is

$$\Psi_3(X) := 3X^4 + 4aX^3 + 6bX^2 + 12cX + 4ac - b^2$$

Computing the 3 torsion

Recall $E : y^2 = x^3 + ax^2 + bx + c$.

The case $\ell = 3$

$$3Q = Id \Leftrightarrow 2Q = -Q$$
$$\Leftrightarrow x(Q) \text{ is a root of the 3-division polynomial}$$

The 3-division polynomial is

$$\Psi_3(X) := 3X^4 + 4aX^3 + 6bX^2 + 12cX + 4ac - b^2$$

$p \neq 3$

$\Psi_3(X)$ has 4 roots, so $E[3](k) \cong (\mathbb{Z}/9)^2$.

$p = 3$

$\Psi_3(X) \equiv aX^3 + (ac - b^2) \mod 3$
So $E[3](k) \cong 1$ or $\mathbb{Z}/3$ (whether or not $a \equiv 0 \mod 3$)

Higher Genus Curves

Let X be an (adjectives) curve over k of genus g.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:

$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

Higher Genus Curves

Let X be an (adjectives) curve over k of genus g.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:

$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

$J_X[p](k) \cong (\mathbb{Z}/p)^f$ for some $0 \leq f \leq g$. The value f is called the *p-rank* of X.

Higher Genus Curves

Let X be an (adjectives) curve over k of genus g.
Its Jacobian J_X is a p.p. abelian variety of dimension g.

When $\ell \neq p$:

$J_X[\ell](k) := Ker[\ell] \cong (\mathbb{Z}/\ell)^{2g}$.

When $\ell = p$:

$J_X[p](k) \cong (\mathbb{Z}/p)^f$ for some $0 \leq f \leq g$. The value f is called the *p-rank* of X.

Does each p-rank actually occur? How often?
We should look closer at $Ker[p]$

Multiplication by p

In general...

- As J_X is an projective abelian variety
- $[n]$ is given by homogeneous equations over k of degree n^{2g}.
- $[p]$ is **inseparable** in characteristic p.

How to understand the p-torsion:

- Want to understand $Ker[p]$ better.
- It's a group...
- We have equations for it...

Multiplication by p

In general...

- As J_X is an projective abelian variety
- $[n]$ is given by homogeneous equations over k of degree n^{2g}.
- $[p]$ is **inseparable** in characteristic p.

How to understand the p-torsion:

- Want to understand $Ker[p]$ better.
- It's a group...
- We have equations for it... It's a group scheme!
  (a p-torsion group scheme of rank p^{2g})

p-torsion Group Schemes in General

Let $A[p]$ be a finite group scheme annihilated by p, with two morphisms, the Frobenius F and the Verschiebung V (F's dual) where

$$[p] = F \circ V,$$

How many isomorphism types have rank p^{2g}?

p-torsion Group Schemes in General

Let $A[p]$ be a finite group scheme annihilated by p, with two morphisms, the Frobenius F and the Verschiebung V (F's dual) where

$$[p] = F \circ V,$$

How many isomorphism types have rank p^{2g}?

Defintion

There exists a filtration $N_1 \subset N_2 \subset \cdots \subset N_{2g} = A[p]$ stable under V and F^{-1}, such that $\dim_k(N_i) = i$. Set $v_i := \dim_k(VN_i)$. The Ekedahl - Oort type is $v := [v_1, \ldots, v_g]$.

- It is nec/suff that $v_i \leq v_{i+1} \leq v_i + 1$.
- Thus there are 2^g possibilities for $J_X[p]$.
- For $g > 1$, this is more than the $g + 1$ possible p-ranks.

Curves with a given EO-type

- How many curves have a given p-rank?

Theorem (Faber/Van der Geer, and Glass/Pries)

For p prime, $g \geq 1$ and $0 \leq f \leq g$ there exists a smooth projective connected (HE) curve of genus g and p-rank f over k. (Codimension g-f in both cases).

- Which EO types occur?

Curves with a given EO-type

- How many curves have a given p-rank?

Theorem (Faber/Van der Geer, and Glass/Pries)

For p prime, $g \geq 1$ and $0 \leq f \leq g$ there exists a smooth projective connected (HE) curve of genus g and p-rank f over k. (Codimension g-f in both cases).

- Which EO types occur?

Example: Hyperelliptic curves in characteristic 2

- For genus 2: Only 3 of the 4 EO types occur.
- Only 1 of the 2^{g-1} types occurs for h.e. curves with 2-rank 0.

In general, not much is known. It would help to have an algorithm to compute EO types of Jacobians.

Isomorphic Viewpoints

We use the follow equivalences:

BT-1 groups schemes of rank p^{2g}

$J_X[p]$ is one of these.

$\updownarrow$

Dieudonné modules of dim $2g$ (mod p)

Module over $\mathbb{E}$ a non-commutative ring with generated by semi-linear operators F and V on k such that $FV = VF = 0$.

$\updownarrow$

$H^1_{dR}(X)$ with F,V actions

'Concrete' space with explicit actions.
Goal: Compute this as an F, V module.

$H^1_{dR}(X)$

In General:

$$0 \to H^0(X, \Omega_1) \to H^1_{dR}(X) \to H^1(X, \mathcal{O}) \to 0$$

These spaces have dimensions

$$\dim(H^1_{dR}(X)) = 2g, \quad \dim(H^0(X, \Omega_1)) = g = \dim(H^1(X, \mathcal{O})).$$

Idea

- This sequence is non-split as F, V modules.
- It does split as $\mathbb{F}_p$ vector spaces.
- So compute each piece and a good vec. space splitting
- Compute F and V on this space (the splitting).

Computing the Pieces

Computing $H^0(X, \Omega_1)$

$L(D) =$ Riemann-Roch space of the canonical divisor. (MAGMA can compute this).

Computing $H^1(X, \mathcal{O})$

- Let $\pi : X \to \mathbb{P}^1$.
- Set $U_0 = X \setminus \{\pi^{-1}(0)\}$.
- Set $U_\infty = X \setminus \{\pi^{-1}(\infty)\}$.
- Set $\Gamma(U)$ denote functions regular on U.

Then,

$$H^1(X, \mathcal{O}) = \frac{\Gamma(U_0 \cap U_\infty)}{\Gamma(U_0) + \Gamma(U_\infty)}$$

Computing the Pieces

Let D_* be the divisor

$$D_* = \sum_{P \in \{\pi^{-1}(*)\}} P.$$

Then,

$$\begin{aligned} H^1(X, \mathcal{O}) &= \frac{\Gamma(U_0 \cap U_\infty)}{\Gamma(U_0) + \Gamma(U_\infty)} \\ &= \lim_{n \to \infty} \frac{L(n(D_0 + D_\infty))}{L(n(D_0)) + L(n(D_\infty))} \end{aligned}$$

It's finite dim'l so we can take n sufficiently large....$n = 2g$.

Computing the Pieces

Let D_* be the divisor

$$D_* = \sum_{P \in \{\pi^{-1}(*)\}} P.$$

Then,

$$\begin{aligned} H^1(X, \mathcal{O}) &= \frac{\Gamma(U_0 \cap U_\infty)}{\Gamma(U_0) + \Gamma(U_\infty)} \\ &= \lim_{n \to \infty} \frac{L(n(D_0 + D_\infty))}{L(n(D_0)) + L(n(D_\infty))} \end{aligned}$$

It's finite dim'l so we can take n sufficiently large....$n = 2g$.

Computing $H^1_{dR}(X)$

Recall:

$$0 \to H^0(X, \Omega_1) \to H^1_{dR}(X) \to H^1(X, \mathcal{O}) \to 0$$

The suitable splitting:

$H^1_{dR}(X) := (f, (\omega_0, \omega_\infty))/\{(f_0, (df_0, 0)) + (f_\infty, (0, df_\infty))\}$

- $H^0(X, \Omega_1) \mapsto (0, (\omega, \omega))$
- $H^1(X, \mathcal{O}) \mapsto (f, (df|_{U_0}, df|_{U_\infty}))$

So we have a basis!

The maps F and V are given by:

- $F[f, [\omega_0, \omega_\infty)] = [f^p, (0, 0)]$
- $V[f, [\omega_0, \omega_\infty)] = [0, (C\omega_0, C\omega_\infty)]$, with C the Cartier map.

The maps are easily computable!

Suzuki Curves: Supersingular Example in Char 2

Let $m \in \mathbb{N}$, $q = 2^{2m+1}$, $q_0 = 2^m = \sqrt{\frac{q}{2}}$.

The Suzuki curve S_m in $\mathbb{P}^2$ is defined over $\mathbb{F}_q$ by the equation

$$W^{q_0}(Z^q + ZW^{q-1}) = Y^{q_0}(Y^q + YW^{q-1}).$$

- Smooth.
- Irreducible.
- Genus $g = q_0(q-1)$.
- $|S_m(\mathbb{F}_q)| = q^2 + 1$.
- $\mathrm{Aut}(S_m) = S(q)$ the Suzuki Group.
- Maximal: S_m meets Hasse-Weil bound over $\mathbb{F}_{q^4}$.
- Its Jacobian has no points of order 2.

Examples

Example: $m = 1$ (g=14)

$$J_1[2] \cong \left(\frac{k[F,V]}{(F^2+V^2)}\right) \oplus \left(\frac{k[F,V]}{(F^3+V^3)}\right)^4$$

Example: $m = 2$ (g=124)

$$J_1[2] \cong \left(\frac{k[F,V]}{(F+V)}\right) \oplus \left(\frac{k[F,V]}{(F^3+V^3)}\right) \oplus \left(\frac{k[F,V]}{(F^5+V^5)}\right)^{16}$$
$$\oplus \left(\text{A Module of dim } 20 \text{ with } a\# = 3\right)^4$$

Example: m=3 (g=1016)

Takes about an hour on my laptop... a little to ugly to write down.

General m

Work in progress with R. Pries and E. Malmskog.

Thanks