Computing the p-torsion of curves in characteristic p

Rachel Pries

Colorado State University

Computational challenges arising in algorithmic number theory and cryptography
Fields Institute, October 31, 2006

Abstract

New invariants occur for the p-torsion of Jacobians of curves in characteristic p, such as the p-rank and a-number.

Some of these invariants are relevant for cryptography.

In this talk, I will describe these invariants and explain how to compute them.

I will give some results about the construction of curves with given invariants.

If time permits, I will describe the geometry of the moduli spaces of curves with given invariants.

p-torsion in the complex case

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

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

Let $k = \overline{\mathbb{F}}_p$, 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.

The elliptic curve $y^2 = h(x)$ is supersingular iff the coefficient of x^{p-1} in $h(x)^{(p-1)/2}$ is 0.

Example of points of order p collapsing mod p

$E : y^2 = x^3 + ax^2 + bx + c$.
A point $Q \in E$ has order 3 iff $x(2Q) = x(Q)$.

This occurs iff $x(Q)$ is a root of

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

Now $\psi_3(x)$ has 4 distinct roots in $\mathbb{C}$ so $|E_{\mathbb{C}}[3]| = 9$.

Let $p = 3$. Then $\psi_3(x) \equiv ax^3 + (ac - b^2)$ mod 3

$$\psi_3(x) \text{ has } \begin{cases} \text{a triple root} & a \not\equiv 0 \bmod 3 \\ \text{no roots} & a \equiv 0 \bmod 3 \end{cases}$$

So $|E[3](k)|$ divides 3.

Supersingular elliptic curves in cryptography

Introduction

Invariants

Computing invariants

Constructing curves

Moduli spaces

Summary and open questions

Due to Frey-Rück attack, supersingular elliptic curves are weak for cryptography, Menezes-Okamato-Vanstone.

Similar phenomenon occurs for supersingular abelian varieties, Galbraith.

Rubin/Silverberg: "For some cryptographic applications [identity based encryption, short signature schemes] supersingular elliptic curves turn out to be very good."

There is active research on the security parameters of these abelian varieties.

What are the invariants of the p-torsion for these abelian varieties?

The p-rank of $J_X[p]$

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.

Note: we count the number of points over k not over $\mathbb{F}_q$.

Also, $f_X = \dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, J_X[p])$.
$\mu_p \simeq \mathrm{Spec}(k[x]/(x^p - 1))$ is the kernel of Frobenius on $\mathbb{G}_m$.

Def: X is *ordinary* if $f = g$ and this happens generically.

The p-rank can only go down under specialization, Katz.

Supersingularity and points of order p

Def: An abelian variety A is supersingular if A is isogenous to $\times_1^g E_i$ where E_i are supersingular elliptic curves.

A supersingular iff the slopes of Newton polygon are all $1/2$.

The p-rank is an isogeny invariant.

If A is supersingular, then the p-rank of A is 0.

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

Let $p = 2$ and $g = 2^n - 1$.
Let $y^2 + y = h(x)$ with $h(x) \in k[x]$ and $\deg(h(x)) = 2g + 1$.
This has genus g and p-rank 0, but there are no supersingular hyperelliptic curves of this genus (Zhu).

The a-number

The *a-number* of X is $a_X = \dim_k \mathrm{Hom}(\alpha_p, J_X[p])$.

$\alpha_p \simeq \mathrm{Spec}(k[x]/x^p)$ is the kernel of Frobenius on $\mathbb{G}_a$.

The a-number measures the intersection of the image of F and V on the Dieudonné module.

The a-number can only increase under specialization, Oort.

If $f = 0$, then $a \geq 1$. Also $a + f \leq g$.

Let $E_1, \ldots, E_g$ be supersingular elliptic curves.
Then $a = g$ iff $A \simeq \times_{i=1}^{g} E_i$ (*A superspecial*).

Superspecial curves are rare.
They occur only if $g \leq (p^2 - p)/2$, Ekedahl (see also Re).

More about the a-number

The a-number is not an isogeny invariant.

Let E_1, E_2 be supersingular elliptic curves.

If $A \simeq E_1 \times E_2$, then $a = 2$.

If A isogenous to $E_1 \times E_2$ but $A \not\simeq E_1 \times E_2$ then $a = 1$.

The p-rank and the a-number do not determine the isomorphism class of the group scheme $A[p]$.

The group scheme $A[p]$ can be described using Dieudonné modules, Ekedahl-Oort types ν, Young diagrams μ, or cycle classes.

$g = 1$:

$A[p]$	codim	f	a	ν	μ	cycle class
L	0	1	0	[1]	$\emptyset$	λ_0
$I_{1,1}$	1	0	1	[0]	$\{1\}$	$(p-1)\lambda_1$

Group schemes:

$L = \mathbb{Z}/p \oplus \mu_p$.

$I_{1,1}$ given by $0 \to \alpha_p \to I_{1,1} \to \alpha_p \to 0$ (non-split).

Occur as p-torsion:

If E is an ordinary elliptic curve then $E[p] \simeq L$.

If E is a supersingular elliptic curve, then $E[p] \simeq I_{1,1}$.

Dieudonné modules:

$D(\mathbb{Z}/p \oplus \mu_p) \simeq k[F,V]/(F, 1-V)_\ell \oplus k[F,V]/(V, 1-F)_\ell$.

$D(I_{1,1}) \simeq k[F,V]/(F+V)_\ell$.

$g = 2$:

$A[p]$	codim	f	a	ν	μ	cycle class
L^2	0	2	0	$[1,2]$	$\emptyset$	λ_0
$L \oplus I_{1,1}$	1	1	1	$[1,1]$	$\{1\}$	$(p-1)\lambda_1$
$I_{2,1}$	2	0	1	$[0,1]$	$\{2\}$	$(p-1)(p^2-1)\lambda_2$
$I_{1,1}^2$	3	0	2	$[0,0]$	$\{2,1\}$	$(p-1)(p^2+1)\lambda_1\lambda_2$

Group scheme:
Here $\alpha_p \subset H \subset I_{2,1}$ where $H/\alpha_p \simeq \alpha_p \oplus \alpha_p$, and $I_{2,1}/H \simeq \alpha_p$.

Dieudonné module:
$D(I_{2,1}) \simeq k[F,V]/(F^2+V^2)_\ell$.

Newton polygons:
$2G_{1,1}$ (supersingular) occurs for both $(I_{1,1})^2$ and $I_{2,1}$.

$g = 3$:

$A[p]$	codim	f	a	ν	μ
L^3	0	3	0	$[1,2,3]$	$\emptyset$
$L^2 \oplus I_{1,1}$	1	2	1	$[1,2,2]$	$\{1\}$
$L \oplus I_{2,1}$	2	1	1	$[1,1,2]$	$\{2\}$
$L \oplus I_{1,1}^2$	3	1	2	$[1,1,1]$	$\{2,1\}$
$I_{3,1}$	3	0	1	$[0,1,2]$	$\{3\}$
$I_{3,2}$	4	0	2	$[0,1,1]$	$\{3,1\}$
$I_{1,1} \oplus I_{2,1}$	5	0	2	$[0,0,1]$	$\{3,2\}$
$I_{1,1}^3$	6	0	3	$[0,0,0]$	$\{3,2,1\}$

If $A[p] \simeq I_{3,1}$, then $NP(A) = G_{1,2} + G_{2,1}$ (slopes $1/3$ and $2/3$) usually but $NP(A) = 3G_{1,1}$ (supersingular) also occurs.
$D(I_{3,1}) \simeq k[F,V]/(F^3 + V^3)_\ell$.
$D(I_{3,2}) \simeq k[F,V]/(F^2 - V)_\ell \oplus k[F,V]/(V^2 - F)_\ell$.

$g = 4$:

There are 16 possibilities for $A[p]$ if $g = 4$.
Here are the ones with $f = 0$.

$g = 4,\ f = 0$	codim	f	a	ν	μ
$I_{4,1}$	4	0	1	$[0,1,2,3]$	$\{4\}$
$I_{4,2}$	5	0	2	$[0,1,2,2]$	$\{4,1\}$
$I_{1,1} \oplus I_{3,1}$	6	0	2	$[0,1,1,2]$	$\{4,2\}$
$I_{1,1} \oplus I_{3,2}$	7	0	3	$[0,1,1,1]$	$\{4,2,1\}$
$I_{2,1} \oplus I_{2,1}$	7	0	2	$[0,0,1,2]$	$\{4,3\}$
$I_{4,3}$	8	0	3	$[0,0,1,1]$	$\{4,3,1\}$
$I_{1,1}^2 \oplus I_{2,1}$	9	0	3	$[0,0,0,1]$	$\{4,3,2\}$
$I_{1,1}^4$	10	0	4	$[0,0,0,0]$	$\{4,3,2,1\}$

It is not known if these occur for all p as the p-torsion $J_X[p]$ of a curve X of genus 4.

Computing the p-rank and a-number

Let C be the Cartier (semi-linear) operator on $H^0(X, \Omega^1)$.

The p-rank is $f = \dim(\mathrm{im} C^g)$, Manin.

The a-number is $a = g - r$ where r is the rank of C.

Thus, for fixed p and X, one can compute f_X and a_X.

Yui worked out C when X hyperelliptic.
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 ijth 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 $f_Y = \mathrm{rank}(M)$ where $M = \prod_{i=0}^{g-1}(A_g^{(p^i)})$.

An example of the Cartier operator when $p = 2$.

Let $X : y^2 + y = h(x)$ with $h(x) \in k[x]$ of odd degree j.

All hyperelliptic curves with 2-rank 0 have this form.

This includes some supersingular curves whose security parameters are as good as possible.
Galbraith: $y^2 + y = x^5 + x^3$, $y^2 + y = x^9 + x^4 + 1$.

Then $g = (j-1)/2$ and $f = 0$ by Deuring-Shafarevich.

A basis for $H^0(X, \Omega^1)$ is $\{dx, xdx, \ldots, x^{g-1}dx\}$.

$C(x^{2b}dx) = 0$ and $C(x^{2b+1}dx) = x^b dx$.

C nilpotent so $f = 0$, and $a = \lfloor (g+1)/2 \rfloor$.

More examples

Curves found in Galbraith, a-number computed by Elkin.
$p=3$, $y^2=x^6+x+2$ has $g=2$, $f=0$, $a=1$.
$p=3$, $y^2=x^7+1$ has $g=3$, $f=0$, and $a=1$.
$p=5$, $y^2=x^5+2x^4+x^3+x+3$ has $g=2$, $f=0$, $a=1$.
$p=2$, $y^3=x^5+1$ has $g=4$, $f=0$, and $a=2$.
$p=2$, $y^3=x^5+x+1$ has $g=4$, $f=0$, and $a=2$.

The curve $y^p-y=x^{p+1}$ is related to error-correcting codes.
It has $g=p(p-1)/2$, $f=0$, and $a=g$.

(P) If $p\equiv 1 \bmod j$ and $y^p-y=x^j$, then $a=(p-1)j/4$ if j even and $a=(p-1)(j-1)(j+1)/4j$ if j odd.

Geometric existence results

For every $p \geq 2$, for every $g \geq 1$, for every $0 \leq f \leq g$ there exists a curve X over $k = \overline{\mathbb{F}}_p$ with:

genus g and p-rank f, Faber-van der Geer.
genus g and p-rank f with X hyperelliptic if $p \geq 3$, Glass-P.
genus g and p-rank f with X hyperelliptic if $p = 2$, Zhu.

P: existence results for curves with large p-rank:
genus $g \geq 2$ with $f = g - 2$ and $a = 1$.
genus $g \geq 2$ with $f = g - 2$ and $a = 2$ if $p \geq 5$.
genus $g \geq 3$ with $f = g - 3$ and $a = 1$.

Only Zhu's proof is constructive.
The other proofs are all geometric. There are families of these curves and the results include the dimension of the families.

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

Let $\phi_i : C_i \to \mathbb{P}^1$ be a hyperelliptic cover branched at B_i for $i = 1, 2$. Let $\phi_3 : C_3 \to \mathbb{P}^1$ be the hyperelliptic cover branched at $B_3 = (B_1 \cup B_2) - (B_1 \cap B_2)$.

Let $\phi : D \to \mathbb{P}^1$ be the normalized fibre product of ϕ_1 and ϕ_2. It is a $(\mathbb{Z}/2)^2$-cover.

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)

Theorem

(Glass, P): For $p \geq 5$ and $g \geq 2$, we construct a hyperelliptic curve D with p-rank $g - 2$ and a-number 2.

Proof. For g even, there exist $B_1 \neq B_2$ s.t. $g_{C_1} = g_{C_2} = g/2$ and $g_{C_3} = 0$ and $f_{C_1} = f_{C_2} = g/2 - 1$ (uses Yui, Igusa).
If g is odd, the proof is similar.

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

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.

Method to construct curves with $f = g - 2$ and $a = 1$.

Goal: produce X genus g with $f_X = g - 2$ and $a_X = 1$.

Start with Y genus 2 with $f_Y = 0$ and $a_Y = 1$.

Ex: $p = 2$, look at $y^2 + y = x^5$.
$p = 3$, look at $y^2 = x^6 + x + 2$.
$p = 5$, look at $y^2 = x^5 + 2x^4 + x^3 + x + 3$.

Find points of order $\ell = g + 1$ on J_Y (ok if $p \nmid \ell$).

One of these yields an unramified $\mathbb{Z}/\ell$-cover $X \to Y$ with invariants as above.

Constructing curves with $f = g - 3$

All four possibilities for the p-torsion of a curve of genus 3 with $f = 0$ do occur.

Prop.[P] Let $p \geq 3$. Let g be odd, $g \not\equiv 1 \bmod p$, and $g \geq 6(p-1)+1$. Then all four possibilities for the p-torsion of a curve X of genus g with p-rank $g-3$ do occur.

Proof: X is produced as an unramified cover of a curve of genus 3, using a result of Raynaud about theta divisors. This leads to restrictions on g.

Questions

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

Let X be a curve of genus g with p-rank f.

Then $J_X[p] = (\mathbb{Z}/p \oplus \mu_p)^f \oplus \mathbb{G}$ where there are 2^{g-f-1} possibilities for the group scheme $\mathbb{G}$.

It is now natural to ask:

which a-numbers and group schemes $\mathbb{G}$ actually occur?

If $\mathbb{G}$ occurs, describe the corresponding sublocus of $\mathcal{M}_g$: 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.

The generic group scheme for p-rank f

Conj. A generic curve of genus g and p-rank f has a-number 1 if $f \leq g - 1$.

[P] proved when $f \geq g - 3$ and reduced proof in other cases to the base case $f = 0$.

The conditions p-rank f and a-number 1 determine a unique group scheme: $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^f \oplus I_{g-f,1}$.
Here $I_{r,1}$ is the unique choice of $\mathbb{G}$ with rank p^{2r}, p-rank 0, and a-number 1.

$I_{1,1}$ occurs as the p-torsion for a supersingular elliptic curve.
$I_{2,1}$, for a supersingular non-superspecial abelian surface.

The covariant Dieudonné module for $I_{r,1}$ has relation $F^r = V^r$.

Open questions for small genus

Hyperelliptic curves of genus 3 and p-rank 0

1. How many components does this space have?
2. Does supersingular locus intersect each component?

Curves of genus $g \geq 4$

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

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?

Summary

- The Cartier operator is useful for computing invariants of the p-torsion $J_X[p]$.
- We construct curves X with interesting p-torsion $J_X[p]$.
- We use geometric methods to show there exist (hyperelliptic) curves of genus g with p-rank f.
- In some cases, we can find the a-number of these curves.

Thanks!

Moduli spaces

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 $f_X \leq f$.

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

Oort described the stratification of $\mathcal{A}_g$ by p-rank.

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

(Glass, P): For $p \geq 3$, every component of $V_{g,f} \cap \mathcal{H}_g$ has codimension $g - f$ in $\mathcal{H}_g$ (dim $g + f - 1$).

Boundary approach: when $g \geq 2$ and $f = g - 2$

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 $a_X = 2$).

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 case (B) occurs with codimension 3 in $\mathcal{M}_g$.

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

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

Every component of $T_{g,2}$ has dimension $3g - 6$.

The generic point of every component of $T_{g,2}$ has type (B).

Boundary approach: 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 $V_{g,g-3} \cap \mathcal{M}_g$.

So case (i) occurs with dimension $3g - 6$ (codim 3 in $\mathcal{M}_g$).