Computation of p-torsion of Jacobians of hyperelliptic curves

Rachel Pries

Colorado State University
pries@math.colostate.edu

Sage Days 26
December 9, 2010

Abstract

An elliptic curve defined over $k = \overline{\mathbb{F}}_p$ can be ordinary or supersingular;

this distinction measures certain properties of its p-torsion.

The p-torsion of the Jacobian of a curve of higher genus can be classified by interesting combinatorial invariants, such as the p-rank, Newton polygon, a-number, and Ekedahl-Oort type.

Algorithms to compute these invariants exist but some have not been implemented.

I will explain how to compute these invariants and describe the lag in producing explicit curves with given p-torsion invariants.

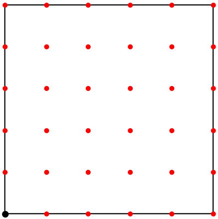
Complex elliptic curves and p-torsion

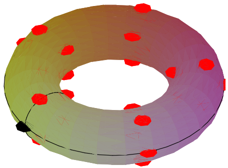
Let E be a complex elliptic curve.

$E \simeq \mathbb{C}/L$ for a lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.
(Thus E is an abelian group).

Torsion points: $E[p](\mathbb{C}) = \{Q \in E(\mathbb{C}) \mid pQ = 0_E\}$.

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

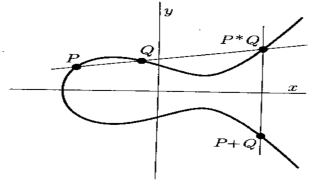




If X is a complex curve of genus $g \geq 2$, its Jacobian J_X is a p.p. abelian variety of dimension g and $J_X[p](\mathbb{C}) \simeq (\mathbb{Z}/p)^{2g}$.

Elliptic curves - algebraic version

Let $E : y^2 = x^3 + ax^2 + bx + c$ be an elliptic curve over $k = \overline{\mathbb{F}}_p$ with algebraic group law.



The ℓ-torsion of E is $\mathrm{Ker}[\ell]$ where $[\ell] : E \to E$ is mult.by-ℓ.

$E[\ell](k) := \{Q \in E(k) \mid \ell Q = 0_E\} \simeq (\mathbb{Z}/\ell)^2$ if $p \nmid \ell$.

Torsion points - example

Let $E : y^2 = x^3 + ax^2 + bx + c$ and $\ell = 3$.

A point Q has order 3 iff $x(2Q) = x(Q)$.

This occurs iff $x(Q)$ is a root of the 3-division polynomial.

$P. < a, b, c >= PolynomialRing(ZZ, 3)$
$E = EllipticCurve(P, [0, a, 0, b, c])$
$d_3 = E.division\_polynomial(3, x = None)$

$3 * x^4 + 4 * a * x^3 + 6 * b * x^2 + 12 * c * x - b^2 + 4 * a * c$

If $p \neq 3$, then $d_3(x)$ has 4 distinct roots so E has 8 points of order 3 and $|E[3](k)| = 9$.

Collapsing torsion points - example

What if $p = 3$?

$d_3 = 3 * x^4 + 4 * a * x^3 + 6 * b * x^2 + 12 * c * x - b^2 + 4 * a * c$.

Collapsing torsion points - example

What if $p = 3$?

$d_3 = 3*x^4 + 4*a*x^3 + 6*b*x^2 + 12*c*x - b^2 + 4*a*c$.

$P3. < a, b, c >= PolynomialRing(GF(3), 3)$

$r_3 = d_3.change\_ring(P3)$

$+a*x^3 - b^2 + a*c$

Mod p binomial thm: In $k[x]$, $(x+\alpha)^p = x^p + \alpha^p$.

So $r_3 = a*x^3 - b^2 + a*c$ has

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

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

Reduction of division polynomials of $y^2 = x^3 + b * x + c$

p	r_p
5	$+2*b*x^{10} - b^2*c*x^5 + b^6 - 2*b^3*c^2 - c^4$
7	$+3*c*x^{21} + 3*b^2*c^2*x^{14} +$ $(-b^7*c - 2*b^4*c^3 + 3*b*c^5)*x^7$ $-b^{12} - b^9*c^2 + 3*b^6*c^4 - b^3*c^6 + 2*c^8$

The number of roots of r_p in $k[x]$ is at most:

Reduction of division polynomials of $y^2 = x^3 + b*x + c$

p	r_p
5	$+2*b*x^{10} - b^2*c*x^5 + b^6 - 2*b^3*c^2 - c^4$
7	$+3*c*x^{21} + 3*b^2*c^2*x^{14} +$
	$(-b^7*c - 2*b^4*c^3 + 3*b*c^5)*x^7$
	$-b^{12} - b^9*c^2 + 3*b^6*c^4 - b^3*c^6 + 2*c^8$

The number of roots of r_p in $k[x]$ is at most:

$$(p-1)/2.$$

Ordinary/Supersingular

The points of order p on $E : y^2 = h(x)$ collapse in char. p.

The p-torsion of an elliptic curve E/k contains either p points or 1 point.

Def:

$$E \text{ is } \begin{cases} \text{ordinary} & \text{if } |E[p](k)| = p \\ \text{supersingular} & \text{if } |E[p](k)| = 1 \end{cases}$$

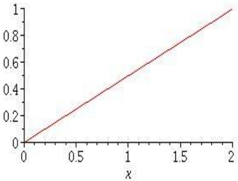
E is supersingular iff the coeff of x^{p-1} in $h(x)^{(p-1)/2}$ is 0.
Igusa: $y^2 = x(x-1)(x-\lambda)$ is supersingular for $(p-1)/2$ choices of $\lambda \in k$.

Supersingular elliptic curves - revisited

If $E/\mathbb{F}_p$ is elliptic curve, then $\#E(\mathbb{F}_p) = p+1-a$.
The zeta function of E is $Z(t) = (1-at+pt^2)/(1-t)(1-pt)$.

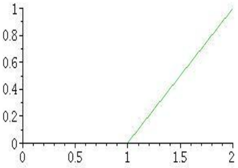
Fact: $a = 0$ iff E supersingular.

E supersingular, Newton polygon of $1+pt^2$ has slopes $1/2$.



called $G_{1,1}$.

E ordinary, then Newton polygon has slopes 0 and 1.



called $G_{0,1} \oplus G_{1,0}$.

Sage - computing supersingularity

$E = EllipticCurve(GF(5), [0, 1, 0, 2, 0])$
Elliptic Curve defined by $y^2 = x^3 + x^2 + 2 * x$ over Finite Field of size 5
$E.is\_supersingular()$
True
$E.hasse\_invariant()$
0
$E.trace\_of\_frobenius()$
0
$F = E.frobenius()$
$C = F.absolute\_charpoly()$
$x^2 + 5$
$C.newton\_slopes(5)$
$[1/2, 1/2]$

Multiple meanings

For elliptic curves, supersingular means:

p-rank - no points of order p.

Newton polygon - slopes $1/2$

group scheme -
$E[p]$ is a group scheme of rank p^2.
$E[p] \simeq \mathbb{Z}/p \oplus \mu_p$ if E ordinary.
If E supersingular, then $0 \to \alpha_p \to E[p] \to \alpha_p \to 0$ (non-split).

a-number - presence of α_p.

For curves of genus $g \geq 2$, these are all different!

Supersingular elliptic curves in cryptography

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

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

Recent research in cryptography involves Jacobians of (hyperelliptic) curves of larger genus.

Similar security phenomena occur for supersingular abelian varieties, Galbraith.

There are open problems on security parameters for larger genus.

Jacobians of curves of higher genus

Let X be a smooth proj. conn. k-curve of genus $g = \dim(H^0(\Omega_1))$.

Its Jacobian J_X is p.p. abelian variety of dim. g.

$J_X[\ell] := \mathrm{Ker}[\ell] \simeq (\mathbb{Z}/\ell)^{2g}$ if $p \nmid \ell$.

The p-torsion points collapse mod p.

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

The p-rank of X

Fact:

If X is a k-curve of genus g,
then $|J_X[p](k)| = p^f$ for some $0 \leq f \leq g$.

Def. Call f the *p-rank* of X.

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

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

Hyperelliptic curves

Assume p odd.

Hyperelliptic curves are $\mathbb{Z}/2$-covers $\phi : Y \to \mathbb{P}^1_k$.

If ϕ is branched at ∞ and Y is smooth of genus g,

then Y has an equation $y^2 = h(x)$ where $h(x) \in k[x]$ has degree $d = 2g+1$ and no repeated roots.

Basis for $H^0(Y, \Omega^1)$ is $\{dx/y, xdx/y, \ldots, x^{g-1}dx/y\}$.

Project - implement algorithm

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.

One can compute f given p, X, and a basis of $H^0(X, \Omega^1)$.

Yui worked this out when X hyperelliptic.
Consider $X : y^2 = h(x)$ where $\deg(h(x)) = 2g + 1$.
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:

X is ordinary if and only if $\det(A_g) \neq 0$.

The p-rank of X is $f = \mathrm{rank}(M)$ where $M = \prod_{i=0}^{g-1}(A_g^{(p^i)})$.

Voloch - algorithm for plane curves in terms of separating variable.

Theoretical results

For all p and $g \geq 3$ and $0 \leq f \leq g$, there exists:

1: curve X of genus g with p-rank f Faber/Van der Geer.

2: hyperelliptic curve X of genus g with p-rank f Glass/P, Zhu/P

The proofs here are all geometric; there is no information about the field of definition.

Open questions

These questions could use some experimentation:
for $g \geq 4$, p, $0 \leq f \leq g$:

1: does there exist (hyperelliptic) X curve of genus g with p-rank f defined over $\mathbb{F}_p$?

2: over $\mathbb{F}_{p^a}$, how many are there?

This gives information about the number of components of moduli space.

Nart = $p = 2$, $g = 3$.

Definition of Newton polygon

Zeta function of $\mathbb{F}_q$-curve X is $Z(t) = L(t)/(1-t)(1-qt)$

where $L(t) = \prod_{i=1}^{2g}(1-w_i t) \in \mathbb{Z}[t]$ and $|w_i| = \sqrt{q}$.

The Newton polygon of X is the Newton polygon of $L(t)$.

Find p-adic valuation v_i of coefficient of t^i in $L(t)$.
Draw lower convex hull of $(i, v_i/a)$ where $q = p^a$.

Example: The curve $Y : y^p - y = x^{p+1}$ has $g = p(p-1)/2$ and is maximal over $\mathbb{F}_{p^2}$.

$L(t) = (1+pt)^{2g} = \sum_{i=1}^{2g} \binom{2g}{i} (pt)^i$.

Newton polygon is line through $(i, i/2)$ for $1 \leq i \leq 2g$.

All slopes equal $1/2$ so Y is supersingular.

More on Newton polygons

Facts: The NP goes from $(0,0)$ to $(2g,g)$.
There is a partial ordering on Newton polygons;
NP line segments break at points with integer coefficients;
If slope λ occurs with length m_λ, so does slope $1-\lambda$.

More abstract definition:
If X is a k-curve, look at the p-divisible group $J_X[p^\infty]$.
There is an isogeny $J_X[p^\infty] \sim \oplus_\lambda H_\lambda^{m_\lambda}$.
Here $\lambda \in \mathbb{Q} \cap [0,1]$ and $\lambda = c/d$ and, by Manin,
H_λ is a p-divisible group of dimension c and height d.
The Dieudonné module D_λ for H_λ is a $W(k)$-module.
Over $\mathrm{Frac}(W(k))$, there is a basis $x_1, \ldots, x_d$ for D_λ s.t. $F^d x_i = p^c x_i$.
Newton polygon: lower convex hull made from line segments of slope λ and length m_λ.

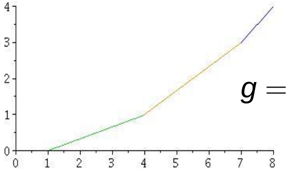
$P. < x >= PolynomialRing(GF(67))$
$X = HyperellipticCurve(x^7 + x^3 + x)$
$X.genus()$
3
$C = X.frobenius\_polynomial()$
$x^6 + 57 * x^4 + 3819 * x^2 + 300763$
$C.newton\_slopes(67)$
$[1, 1, 1/2, 1/2, 0, 0]$
So the p-rank is 2.

A generic Newton polygon

Given $g \geq 3$ and $f = g - 3$, let $\nu_{g,g-3}$ be the NP with slopes: 0 and 1 with mult. $g - 3$ and $1/3$ and $2/3$ with mult. 3.

Also $\nu_{g,g-3} = G_{0,1}^{g-3} \oplus G_{1,2} \oplus G_{2,1} \oplus G_{1,0}^{g-3}$.

This is the most generic Newton polygon with p-rank $f = g - 3$.



$g = 4$, $f = 1$.

Corollary: Achter/P

If $g \geq 3$, then there exists a curve X of genus g whose Jacobian has Newton polygon $\nu_{g,g-3}$.

Supersingular

Let A be a p.p. abelian variety of dimension g.

Def: We say A is *supersingular* if its Newton polygon has all slopes equal $1/2$.

Def: An *isogeny* of abelian varieties is a group homomorphism $\sim$ with finite kernel.

Fact:
Then A is supersingular iff $A \sim \times_{i=1}^{g} E_i$,
for some supersingular elliptic curves $E_1, \ldots E_g$.

This is 'smallest' Newton polygon under partial ordering.

Earlier results

Which Newton polygons occur for Jacobians of curves?

For $g = 1$ both, $g = 2$ all three, $g = 3$ all five.

For $g \geq 4$ and $f \geq g - 2$, the p-rank determines the Newton polygon, and thus this Newton polygon occurs.

Same for hyperelliptic curves (see Oort for $g = 3$).

Zhu: If $p = 2$ and $g = 2^n - 1$, then no supersingular hyperelliptic curve exists.

Supersingular versus p-rank 0

Fact: If A is supersingular then A has p-rank 0.

Fact: If $g \in \{1,2\}$ and A has p-rank 0 then A is supersingular.

Fact: If $g \geq 3$, a generic abelian variety A of dimension g and p-rank 0 is not supersingular.

Thm. (Oort) If $g = 3$, then the Jacobian of a generic hyperelliptic curve of genus 3 and p-rank 0 has slopes $\{1/3, 2/3\}$ (not supersingular).

Proof: study intersection of two codim 1 conditions in $\mathcal{M}_3^0$.

Results and questions

Achter/P:

If $g \geq 3$, there exists a (hyperelliptic) curve of genus g and p-rank 0 which is not supersingular.

For $g \geq 4$, p, $f = 0$:
Q1: Find example of non-supersingular curve.
Q2: Which Newton polygons occur?
Conj (Oort) Not all Newton polygons occur for Jacobians.
Q 3: If $g \geq 4$, what is the Newton polygon of a generic (hyperelliptic) curve of genus g and p-rank 0?
Expectation: slopes $1/g$ and $(g-1)/g$.

Egregious open case

Case: Curves of genus 4 and p-rank 0.

Note: $\dim(M_4) + 1 = \dim(A_4)$.

Theorem: Achter/P

For all p, there exists a curve of genus 4 with Newton slopes $1/4$, $3/4$.

Proof: if $p \neq 3$, look at $y^3 = \deg 6$. Look at moduli space of abelian 4-folds with action by $\mathbb{Z}[\zeta_3]$ (Shimura variety). Newton polygons understood when p splits in $\mathbb{Q}(\zeta_3)$ (Montovan) or when p inert (Wedhorn).
What about $p = 3$?

The search!

Find: curve of genus 4 defined over $\mathbb{F}_3$ whose Newton polygon has slopes $1/4$ and $3/4$.

Try: $y^2 =$
$x^9 + a_8x^8 + a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x$.
$P. < x >= PolynomialRing(GF(3))$
$V = VectorSpace(GF(3), 8)$
$Z = matrix(P, 4, 4)$
$M = matrix(P, 4, 4)$
$L = []$
Claim: There are 12 hyperelliptic curves of genus 4, p-rank 0, and a-number 1 defined over $\mathbb{F}_3$.

search - 3-rank 0 and a-number 1

$$for\ a\ inV\ :$$
$$\quad f = x^9 + add(a[k]*x^{k+1} for\ k\ in\ range(8))$$
$$\quad if\,\mathrm{is\_squarefree}(f):$$
$$\quad\quad for\ i\ in\ range(4):$$
$$\quad\quad\quad for\ j\ in\ range(4):$$
$$\quad\quad\quad\quad t = 3*i+3-j-1$$
$$\quad\quad\quad\quad if(t<10)and(t>-1):$$
$$\quad\quad\quad\quad\quad M[i,j] = f.coeffs()[3*i+3-j-1]$$
$$\quad\quad d = M.determinant()$$
$$\quad\quad if(d==0):$$
$$\quad\quad\quad M3 = M*M*M$$
$$\quad\quad\quad if\ not\ (M3 == Z):$$
$$\quad\quad\quad\quad M4 = M3*M$$
$$\quad\quad\quad\quad if(M4 == Z):$$
$$\quad\quad\quad\quad\quad L.append(f)$$

Candidates for $y^2 = f(x)$ with slope $1/4$, $3/4$

L is a list of 24 polynomials.

L[0]

$x^9 + x^7 + x^6 + x^5 + 2*x^3 + 2*x^2 + 2*x$

L[1]

$x^9 + x^7 + x^6 + 2*x^5 + x^4 + 2*x^3 + x^2 + x$

The change of variables $x \to 1/cx$ permutes these.

There are 12 candidates for a hyperelliptic curve of genus 4 defined over $\mathbb{F}_3$ with slopes $1/4$ and $3/4$.

X=HyperellipticCurve(L[0])

Hyperelliptic Curve over Finite Field of size 3 defined by $y^2 = x^9 + x^7 + x^6 + x^5 + 2*x^3 + 2*x^2 + 2*x$

F=X.frobenius_polynomial()

ValueError: In the current implementation, p must be greater than (2g+1)(2N-1) = 117

Search - matching zeta function

$$R. < T >= PolynomialRing(Integers())$$
$$var('a,b,c,d')$$
$$g = 1 + a*T + b*T^2 + c*T^3 + d*T^4 + 3*c*T^5 + 9*b*T^6 + 27*a*T^7 + 81*T^8$$
$$z = g/((1-T)*(1-3*T))$$
$$z4 = taylor(z,T,0,4).truncate()$$

$$(40*a + 13*b + 4*c + d + 121)*T^4 + (13*a + 4*b + c + 40)*T^3 + (4*a + b + 13)*T^2 + (a+4)*T + 1$$

$$S. < t >= PowerSeriesRing(Integers())$$
$$zeta = X.zeta\_series(4,t)$$
$$p4 = zeta.truncate(5).subs(t = T)$$

$$184*T^4 + 58*T^3 + 16*T^2 + 4*T + 1$$

search - finding the slopes

$coeff = [], for\ i\ inrange(5):$
$\quad coeff.append(z4.coeffs()[i][0] - p4.coeffs()[i])$

$[0, a, 4*a+b-3, 13*a+4*b+c-18, 40*a+13*b+4*c+d-63, 0, a, 4*a+b-3, 13*a+4*b+c-18, 40*a+13*b+4*c+d-63]$

$h = solve([coeff[1] == 0, coeff[2] == 0, coeff[3] == 0, coeff[4] == 0], a, b, c, d)[0]$
$[a == 0, b == 3, c == 6, d == 0]$

$g0 = g.subs(h[0]).subs(h[1]).subs(h[2]).subs(h[3])$
$gp = g0.polynomial(Integers())$
$gp.newton\_slopes(3))$
Slopes are $1/3$, $1/2$, $2/3$.

Automating slope computation


```
for i in range(23):
X=HyperellipticCurve(L[i])
zeta=X.zeta_series(4,t).truncate(5).subs(t=T)
diffpoly=zeta-z4
eqns=[diffpoly.expand().coeff(T,j)==0 for j in
range(diffpoly.degree(T)+1)]
h=solve(eqns,a,b,c,d)[0]
g0=g.subs(h[0]).subs(h[1]).subs(h[2]).subs(h[3])
gp=g0.polynomial(Integers())
print(i, gp.newton_slopes(3))
```

Slopes 1/4, 3/4 or 1/3, 1/2, 2/3, or supersingular all occur.

A new invariant

Example when $g = 2$
$X : y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)$

There are 3 variables $\lambda_i \in k$ to choose.

The parameter space $\mathcal{M}_2$ for choices of X has dimension 3.

There are 4 possibilities for $J_X[p]$.
Look at subspace of $\mathcal{M}_2$ such that:

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

What distinguishes between the last two columns?

The a-number

The *a-number* is the dimension of the kernel of the Cartier operator on $H^0(\Omega_1)$.

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

Now $a + f \leq g$. If $f < g$, then $a \geq 1$.

Unlike the p-rank, 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 $a = 1$.

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 $g = (j-1)/2$.
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 $a = \lfloor (g+1)/2 \rfloor$.

Superspecial $\Rightarrow$ Supersingular $\Rightarrow f = 0$

Def: An abelian variety A is *superspecial* if $A \simeq \times_{i=1}^{g} E_i$ where E_i are supersingular elliptic curves.

Then $a = g$ iff A superspecial.

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

Def: 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 $1/2$.

If A is superspecial, then A is supersingular.
The converse is false for $g \geq 2$.

If A is supersingular, then the p-rank of A is 0.
The converse is false for $g \geq 3$.

More examples

The curve $X : y^p - y = x^{p+1}$ is maximal over $\mathbb{F}_{p^2}$;

(number of points in $X(\mathbb{F}_{p^2})$ realizes Hasse-Weil bound).

It can be used to construct a good error-correcting code.

This curve has $g = p(p-1)/2$ by Riemann-Hurwitz, $f = 0$ by Deuring-Shafarevich, and $a = g$.

If $p \equiv 1 \bmod j$ instead, then $y^p - y = x^j$ has $g = (j-1)(p-1)/2$ and $f = 0$ and (P):

$$a = \begin{cases} (p-1)j/4 & \text{if j even} \\ (p-1)(j-1)(j+1)/4j & \text{if j odd} \end{cases}$$

Open questions

Expect a-number is usually small

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

The conditions p-rank f and a-number 1 determine a unique group scheme of rank p^{2g}. Its covariant Dieudonné module has relation $F^r = V^r$.

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

Analogous result for hyp. curves when $f = g - 2$ if $p > 2$.

Question: find explicit equations for curves with p-rank 0 and given a-number.

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 $a_Y = 1$. (i.e. J_Y is a supersingular non-superspecial abelian surface).

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 $p \nmid \ell$).

Each of these yields an unramified $\mathbb{Z}/\ell$-cover $X \to Y$ s.t. X has genus g and $J_Y \subset J_X$.

By a result of Raynaud about theta divisors, one of these curves X has p-rank $g - 2$.

Group schemes

If A is a p.p. abelian variety, then $A[p]$ is a group scheme.

Then $f = \dim_{\mathbb{F}_p} \mathrm{Hom}(\mu_p, A[p])$ where $\mu_p \simeq \mathrm{Spec}(k[x]/(x^p - 1))$ is the kernel of Frobenius on $\mathbb{G}_m$;
and $a = \dim_k \mathrm{Hom}(\alpha_p, A[p])$ where $\alpha_p \simeq \mathrm{Spec}(k[x]/x^p)$ is the kernel of Frobenius on $\mathbb{G}_a$.

The p-rank and the a-number do not determine the isomorphism class of $A[p]$ if $g \geq 3$.

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

Classification by Newton polygon does not match up well.

$g = 1$:

$A[p]$	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	$[0,1,1,2]$	$\{4,2\}$
$I_{2,1} \oplus I_{2,1}$	7	0	2	$[0,0,1,2]$	$\{4,3\}$
$I_{1,1} \oplus I_{3,2}$	7	0	3	$[0,1,1,1]$	$\{4,2,1\}$
$I_{4,3}$	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.

Open questions

For a p.p. abelian variety of dimension g, there are 2^g possibilities for the group scheme $A[p]$.
Let $\mathbb{G}$ be one of these.

Q1: Does $\mathbb{G}$ occur as the p-torsion of a Jacobian J_X?

Q2: 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 $J_X[p] \simeq (\mathbb{Z}/p \oplus \mu_p)^{g-1} \oplus I_{1,1}$ and $a_X = 1$.

For $g \geq 4$ and $f \geq g - 3$, all occur, P

Egregious open case

Hyperelliptic curves with $g = 3$ and $f = 0$.

Note: $\dim(H_3) + 1 = \dim(A_3)$.

The moduli space $\mathcal{H}_3^0$ has dimension 2.

Is it irreducible?

Yes, when $p = 3$, Elkin/P

Open questions - arithmetic

Q 1: For all $g \geq 3$ and $0 \leq f \leq g$, does there exist an $\mathbb{F}_p$-curve X with genus g and p-rank f?

Note: earlier application shows slopes are not all $1/2$.

Note: the case $f = 0$ is crucial; can reduce the calculation of generic Newton polygon of $\mathcal{M}_g^f$ to that of $\mathcal{M}_{g-f}^0$.

Open questions - geometric

Q 3: How many irreducible components does $\mathcal{M}_g^f$ have?

Known that $\mathcal{M}_g^f$ is irreducible for all p when $g = 2$ and $f \geq 1$ and when $g = 3$.

If $g > 3$ and $f = g$, then $\mathcal{M}_g^f$ is irreducible for all p.

Q 4: How many irreducible components does $\mathcal{H}_g^f$ have?

The case $g = 3$, $f = 0$ could improve results on $\mathcal{H}_g^0$, $\mathcal{H}_g^{g-3}$.

Already the case $g = 3$, $f = 0$ with $p \geq 5$ is unknown.