Calgary workshop on abelian varieties: June 2016
Pries - sample problems about supersingular curves

Review material
Let p be an odd prime and let $k = \overline{\mathbb{F}}_p$.

Supersingular elliptic curves:
Let $h(x) \in k[x]$ be a degree 3 polynomial with no repeated roots. Let E/k be the elliptic curve with equation $y^2 = h(x)$.

Fact 1: The elliptic curve E is supersingular if and only if $c_{p-1} = 0$ where c_{p-1} is the coefficient of x^{p-1} in $h(x)^{(p-1)/2}$.

Fact 2: If E has complex multiplication by a quadratic imaginary field K and p is inert in $\mathcal{O}_K$ then E is supersingular.

Review problems:

1. Use Fact 1 to determine the set of primes for which E is supersingular when:
   A. $h(x) = x^3 - x$;
   B. $h(x) = x^3 + 1$;
2. Use Fact 2 to find the primes for which E is supersingular ($h(x)$ as in Problem 1).
3. Consider the Hermitian curve $X : y^q + y = x^{q+1}$ where $q = p^a$.
   (a) Find the genus of X. Hint: Riemann-Hurwitz formula.
   (b) Find the number of points in $X(\mathbb{F}_{q^2})$. Hint: LHS is the trace map $\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ and RHS is the norm map $N : \mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$.
   (c) Show that X is maximal over $\mathbb{F}_{q^2}$. Hint: Hasse-Weil bound.
4. If X is maximal (resp. minimal) over $\mathbb{F}_{q^2}$, prove that X is supersingular. Hint: show that its L-polynomial is
$$L(T) := L(X/\mathbb{F}_{q^2}, T) = (1 + qT)^{2g} \text{ (resp. } (1 - qT)^{2g}).$$
   For $0 \leq i \leq 2g$, let κ_i be the coefficient of x^i in $L(T)$. Show that $v_p(\kappa_i)/2a \geq i/2$ and show the Newton polygon of $L(T)$ is a line segment of slope $1/2$.
5. For $g = 3, 4, 5$, find all the possible Newton polygons of an abelian variety A/k of dimension g and draw a graph showing how they are partially ordered.

Harder problems about supersingular curves: rachelpries@gmail.com

If you make progress on these problems after the workshop, please let me know!

1. Supersingular curves in characteristic 2.

   A. Read Van der Geer and Van der Vlugt's paper *On the Existence of Supersingular Curves of Given Genus* http://xxx.lanl.gov/abs/alg-geom/9404007 .

   B. Pick a genus g and use their method to construct a supersingular curve of genus g defined over $\overline{\mathbb{F}}_2$.

   C. When p is odd, why does their method not produce a supersingular curve of every genus over $\overline{\mathbb{F}}_p$?

   D. Can you improve this result?

   Karemaker/Pries: Let $g = Gp(p-1)^2/2$ where $G = \sum_{i=1}^{t} p^{s_i}(1+p+\cdots p^{r_i})$. Then there exists a supersingular curve over $\overline{\mathbb{F}}_p$ of genus g.

   E. Other references: Bouw et al *Zeta functions of a class of Artin-Schreier curves with many automorphisms* https://arxiv.org/abs/1410.7031

2. For which p and d is the Fermat curve $x^d + y^d = 1$ supersingular over $\overline{\mathbb{F}}_p$?

   Helpful reference: Yui On the Jacobian variety of the Fermat curve

3. Suppose X is a curve of genus g having complex multiplication by a field K (of dimension $2g$). Under what conditions on p is X supersingular? Generate families of supersingular curves with complex multiplication.

   Helpful reference: Sugiyama On a generalization of Deuring's results.

4. Let ℓ be an odd prime. For which p is $y^2 = x^{2\ell+1} - x$ supersingular?

   Helpful reference Gonzales Hasse-Witt matrices for the Fermat curves of prime degree: http://projecteuclid.org.ezproxy2.library.colostate.edu:2048/euclid.tmj/1178225144

5. Learn about Katz's sharp slope estimate.

   (a) How it can be used to find the first slope of the Newton polygon?

   (b) In what situations has it been used to prove that curves are supersingular?

   (c) In what situations has it been used to prove that no supersingular curve of a certain type exists?

   (d) Find a new example where it gives information about the Newton polygon.

6. Under what congruence conditions on p are any of the following curves supersingular: $y^2 = x^9 - x$, $y^2 = x^9 - 1$, $y^2 = x^{10} - 1$?

Calgary workshop on abelian varieties: June 2016
Pries - sample problems about p-ranks of curves

Review material: The p-rank of a hyperelliptic curve:

Let X/k be a smooth hyperelliptic curve of genus g. Then X has an equation of the form $y^2 = h(x)$ for a polynomial $h(x) \in k[x]$ having degree $2g+1$ or $2g+2$ which has distinct roots. A basis for the set of holomorphic 1-forms on X is $\{x^i dx/y \mid 0 \leq i \leq g-1\}$.

Let c_s denote the coefficient of x^s in the expansion of $h(x)^{(p-1)/2}$. For $0 \leq \ell \leq g-1$, let M_ℓ be the $g \times g$ matrix whose ijth entry is $(c_{ip-j})^{p^\ell}$. The matrix M_0 is the Hasse-Witt matrix of X. The Cartier-Manin matrix is $M = M_{g-1}M_{g-2}\cdots M_0$.

Fact 3: X is not ordinary if and only if M_0 has determinant 0.

Fact 4: The p-rank of X is $\sigma_X = \mathrm{rank}(M)$.

Review problems:

1. Prove that M_0 is the matrix for the Cartier operator on $X : y^2 = h(x)$ with respect to the basis $\{x^i dx/y \mid 0 \leq i \leq g-1\}$ for $H^0(X, \Omega^1)$.
2. Check that the Cartier operator has rank 0 on the Hermitian curve $y^p + y = x^{p+1}$.
3. Prove there exists (or find) a smooth curve of genus 3 which has p-rank 0 but is not supersingular.
4. Let ℓ be prime and let $1 \leq a \leq \ell - 1$. Let X be the curve with affine equation $y^\ell = x^a(x-1)$.
   (a) What is the genus of X? Hint: use Riemann-Hurwitz.
   (b) Show that X admits a $\mathbb{Z}/\ell$-cover $\phi : X \to \mathbb{P}^1$. What is the Galois action?
   (c) Show that ϕ is branched at $n = 3$ points and compute the inertia type.
   (d) Show that any $\mathbb{Z}/\ell$-cover $\phi : X \to \mathbb{P}^1$ branched at 3 points is isomorphic to one of these.
   (e) Compute the number of isomorphism classes of such curves, in terms of ℓ.

Harder problems about the p-ranks of curves: rachelpries@gmail.com

If you make progress on these problems after the workshop, please let me know!

1. There is a bug in the current SAGE algorithm to find the p-rank of a hyperelliptic curve. The problem is the formula for the Cartier-Manin matrix in Yui's paper is erroneously listed as $M = M_0 M_1 \cdots M_{g-1}$ (wrong) rather than $M = M_{g-1} \cdots M_1 M_0$ (correct).

   (a) Fix the implementation. Also implement the algorithm for $h(x)$ with even degree.

   (b) Implement Elkin's algorithm for the p-rank of a $\mathbb{Z}/\ell$-cover of the projective line.

2. Let $p \geq 5$ odd and X a generic hyperelliptic curve with genus $g = 3$ and p-rank 0. Does the Cartier matrix on $H^0(X, \Omega^1)$ have rank 2?

   Write $X : y^2 = h(x)$ with $h(x) = x^7 + ax^6 + bx^5 + cx^4 + dx^3 + ex^2 + x$. The condition $M_2 M_1 M_0 = [0]$ is true for a dimension 2 subspace in (a, b, c, d, e). For each component, does M_0 generically have rank 2? (Start with $p = 5$)

3. Let $\ell \neq p$ be prime and let $1 \leq a \leq \ell - 1$. Under what conditions on p, ℓ and a is the curve $y^\ell = x^a(x-1)$ not ordinary?

   Use formulae of Elkin to compute the matrix M_0 for the Cartier operator, starting with the cases (i) $\ell = 5$ and $a = 1$, (ii) $\ell = 7$ and $a = 1, 2$, and (iii) $\ell = 11$ and $a = 1, 2$. When is M_0 not invertible?

   Reference Elkin: The rank of the Cartier operator on cyclic covers of the projective line: https://arxiv.org/pdf/0708.0431.pdf