Computing Selmer groups of Jacobians
Edward Schaefer, Santa Clara University

Let $C$ be a curve over $K$, a number field. We want to determine $C(K)$, the $K$-rational points on $C$. General program (Bruin, Flynn, Macallum, Poonen, S., Stoll, Wetherell, etc.):

Let $J$ be the Jacobian of $C$. $J = \text{Div}^0(C)/\text{Princ}(C)$. Note $J = J(\overline{K})$. Elliptic curves are Jacobians: $E \cong \text{Div}^0(E)/\text{Princ}(E)$ by $P \mapsto [P - 0]$.

We know $J(K) \cong \mathbb{Z}^r \oplus J(K)_{\text{tors}}$ where $r$ and $\#J(K)_{\text{tors}}$ are finite.

1. Determine $J(K)_{\text{tors}}$. Easy in practice.
2. Find a Selmer group to give an upper bound for $r$. (Focus of this talk.)
3. Find independent points of infinite order in $J(K)$ to give a lower bound for $r$.
4. Use pseudo-generating points and a Chabauty argument on $C$ if $r < \text{genus}(C)$ on covers of $C$ if $r \geq \text{genus}(C)$ to determine $C(K)$ (not guaranteed to work).

How to use a Selmer group to find an upper bound for $r$ when $J(K) \cong \mathbb{Z}^r \oplus J(K)_{\text{tors}}$. Let $p$ be prime. Assume we know $J(K)_{\text{tors}}$. If we knew $J(K)/pJ(K)$ then we’d know $r$. There is no known effective algorithm for determining $J(K)/pJ(K)$. There is an effectively computable (in theory) group called the Selmer group containing this group.

We have an exact sequence $0 \to J(\overline{K})[p] \to J(\overline{K}) \xrightarrow{\delta} J(\overline{K}) \to 0$ of $\text{Gal}(\overline{K}/K)$-modules. Taking $\text{Gal}(\overline{K}/K)$-invariants gives us

\[
\ldots J(K) \xrightarrow{\delta} J(K) \xrightarrow{\delta} H^1(\text{Gal}(\overline{K}/K), J[p]) \to H^1(\text{Gal}(\overline{K}/K), J(\overline{K})) \xrightarrow{\delta} H^1(\text{Gal}(\overline{K}/K), J(\overline{K})) \ldots
\]

Giving us a short exact sequence $0 \to J(K)/pJ(K) \xrightarrow{\delta} H^1(K, J[p]) \to H^1(K, J)[p] \to 0$.

(Note abbreviation of $\text{Gal}(\overline{K}/K)$ in $H^1$.)

We’d like to find $J(K)/pJ(K)$. Equivalently, find its image in $H^1(K, J[p])$. Let $S$ be the set of primes of $K$ containing primes over $p$, primes of bad reduction of $C$ and if $p = 2$, infinite primes. Image of $J(K)/pJ(K)$ is contained in $H^1(K, J[p]; S)$, a finite group (this is the subgroup of cocycle classes unramified outside $S$).

Approximate image locally.
\[
J(K)/pJ(K) \xrightarrow{\delta} H^1(K,J[p];S) \\
\downarrow \prod \alpha_s \quad \downarrow \prod \text{res}_s \\
\prod_{s \in S} J(K_s)/pJ(K_s) \xrightarrow{\prod \delta_s} \prod_{s \in S} H^1(K_s,J[p])
\]

Want image of \( J(K)/pJ(K) \) in \( H^1(K,J[p];S) \). Define \( S^p(K,J) = \{ \gamma \in H^1(K,J[p];S) \mid \text{res}_s(\gamma) \in \delta_s(J(K_s)/pJ(K_s)) \quad \forall \ s \in S \} \).

Problems: 1) \( H^1(K,J[p];S) \) hard to work in.
2) \( \delta_s \) hard to evaluate.

Solution: Replace group and map.

Replace \( H^1(K,J[p]) \):

Let \( \overline{A} \) be the étale \( K \)-algebra that is the set of maps from \( J[p] \setminus 0 \) to \( \overline{K} \). Let \( A \) be its \( \text{Gal}(\overline{K}/K) \)-invariants.

What does it look like? Let \( J[p] \setminus 0 = \{ T_1, \ldots, T_l \} \). Concretely, \( A = \prod^\circ K(T_i) \) where \( \prod^\circ \) means take one representative from each \( \text{Gal}(\overline{K}/K) \)-orbit of \( \{ T_1, \ldots, T_l \} \).

Let \( \mu_p(\overline{A}) \) be the maps from \( J[p] \setminus 0 \) to \( \mu_p \).

Let \( w : J[p] \to \mu_p(\overline{A}) \) by \( P \mapsto (T_i \mapsto e_p(P,T_i)) \).

This induces a map \( \hat{w} : H^1(K,J[p]) \to H^1(K,\mu_p(\overline{A})) \).

Kummer theory induces an isomorphism \( k : H^1(K,\mu_p(\overline{A})) \to A^\times/(A^\times)^p \).

Have \( H^1(K,J[p]) \xrightarrow{\hat{w}} H^1(K,\mu_p(\overline{A})) \xrightarrow{k} A^\times/(A^\times)^p \).

Concerns: 1) Sure helps if \( \hat{w} \) is injective (doesn’t have to be, though \( w \) is).
2) Need to find image of \( H^1(K,J[p]) \) in \( A^\times/(A^\times)^p \) (can be difficult if smallest Galois-invariant spanning set of \( J[p] \) is much larger than a basis).
3) Really need image of \( H^1(K,J[p];S) \) in \( A(S,p) \subset A^\times/(A^\times)^p \). Requires class group/unit group information in number fields making up \( A \). (Note if \( L \) is a number field then \( L(S,p) \) is the subgroup of \( L^\times/L^{xp} \) of elements for which if you adjoin a \( p \)-th root, you get an extension unramified outside of prime lying over primes in \( S \). Since \( A \) is a product of number fields, we extend this definition to \( A \).

Let’s assume \( \hat{w} \) is injective and we’ve found the image of \( H^1(K,J[p];S) \) in \( A(S,p) \). (I predict having a non-trivial kernel of \( \hat{w} \) will be a problem for this general method in the future.)

Have isomorphic image of \( H^1(K,J[p];S) \) in \( A(S,p) \subset A^\times/(A^\times)^p \). Need to replace map \( J(K)/pJ(K) \xrightarrow{\delta} H^1(K,J[p]) \xrightarrow{\hat{w}} H^1(K,\mu_p(\overline{A})) \xrightarrow{k} A^\times/(A^\times)^p \).

Assume \( C(K) \) non-empty. Then can choose divisors \( D_1, \ldots, D_l \), with \( [D_i] = T_i \in J[p] \setminus 0 \) and \( pD_i = \text{div}_{K} \) and where \( \{ f_i \} \cong J[p] \setminus 0 \) as \( \text{Gal}(\overline{K}/K) \)-sets.

We call \( D \) a good divisor if \( D \in \text{Div}^0(C)(K) \) and its support does not intersect any of the \( \text{div}_{K} \)’s.

Define \( f : \{ \text{good divisors} \} \to A^\times \) by \( D \mapsto (T_i \mapsto f_i(D)) \).
Theorem: The map $f$ induces a well defined homomorphism from $J(K)/pJ(K) \to A(S, p) \subset A^\times/(A^\times)^p$ that is the same as $k\hat{J}$.

Equivalently we have

$$J(K)/pJ(K) \to \prod_{i} K(T_i)(S, p) \subset K(T_i)^\times/(K(T_i)^\times)^p.$$ 

Note, we have $A(S, p) = \prod K(T_i)(S, p)$.

$$J(K)/pJ(K) \xrightarrow{f} A(S, p)$$

$$\downarrow \prod \alpha_s \quad \downarrow \prod \beta_s$$

$$\prod_{s \in S} J(K_s)/pJ(K_s) \xrightarrow{f} \prod_{s \in S} A_s^\times/(A_s^\times)^p$$

We have $S^\circ(K, J) = \{ \gamma \in \text{image of } H^1(K, J[p]) \text{ in } A(S, p) \mid \beta_s(\gamma) \in f(J(K_s)/pJ(K_s)), \forall s \in S \}$.

Notes:

1. If have isogeny $\phi : B \to J$ over $K$ where $B$ is an abelian variety then can use this technique to find $S^\circ(K, B)$.

2. Instead of using all of $J[p] \setminus \{0\}$ can use a Galois-invariant spanning set of $J[p]$. Will get lower degree $A$.

Important related method.

Above, had $\text{div}(f_i) = pD_i$. What if $\text{div}(f_i) = pD_i - D'$ where $D_i$ effective and $D'/K$?

Example: Hyperelliptic curve. Generically, a hyperelliptic curve of genus $g$ has equation $y^2 = h(x)$, where $h(x)$ has degree $2g + 2$.

Let $h(\alpha_i) = 0$ and consider $f_i = x - \alpha_i$ then $\text{div}(f_i) = 2(\alpha_i, 0) - (\infty^+ + \infty^-)$. Then $\text{div}(f_i) = 2(\alpha_i, 0) - (\infty^+ + \infty^-)$.

Note their differences are $\{2(\alpha_i, 0) - 2(\alpha_j, 0)\}$ and the set $\{[(\alpha_i, 0) - (\alpha_j, 0)]\}$ spans $J[2]$.

Let $\overline{A}$ be the set of maps from $\{2(\alpha_i, 0) - (\infty^+ - \infty^-)\}$ to $\overline{K}$. So $A \cong K[T]/(h(T))$ and $f = x - T$. (Note the degree of $A$ over $K$ is $2g + 2$ whereas a typical 2-torsion point is defined over an extension of degree $(2g + 2)(2g + 1)/2$, and so if we did the previous method, we would probably work in number fields of much higher degree.)

$$J(K)/2J(K) \xrightarrow{x-T} A^\times/(A^{\times 2}K^\times).$$

Has kernel of size 1 or 2, depending on Galois-action on roots of $h$.

Example: Let $C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1$. Find $C(\mathbb{Q})$.

Easy to find $\{(0, \pm 1), (-3, \pm 1), \infty^+, \infty^-\} \subseteq C(\mathbb{Q})$.

$\#J(\mathbb{F}_3) = 9$ and $\#J(\mathbb{F}_5) = 41$ so $J(\mathbb{Q})_{\text{tors}} = 0$. Thus $J(\mathbb{Q}) \cong \mathbb{Z}^\times$.

We have $A = \mathbb{Q}[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1)$, a sextic number field. Bad primes are $S = \{\infty, 2, 3701\}$.

$$J(\mathbb{Q})/2J(\mathbb{Q}) \quad \xrightarrow{x-T} \quad A^\times/(A^{\times 2}\mathbb{Q}^\times)$$

$$\prod_{p \in S} J(\mathbb{Q}_p)/2J(\mathbb{Q}_p) \xrightarrow{x-T} \prod_{p \in S} A_p^\times/(A_p^{\times 2}\mathbb{Q}_p^\times)$$
Define $S^2_{\text{fake}}(Q, J) = \{ \gamma \in \ker N : A(S, 2)/Q(S, 2) \to Q^x/Q^{x^2} \mid \beta_p(\gamma) \in (x-T)(J(Q_p)), \forall p \in S \}$.

From Galois action on zeros of sextic, turns out $\dim_{F_2} S^2(Q, J) = \dim_{F_2} S^2_{\text{fake}}(Q, J) + 1$.

Basis of $A(S, 2)$ is $\{-1, u_1, u_2, u_3, \alpha, \beta_1, \beta_2, \beta_3\}$ with norms $\{1, 1, 1, -1, 2^3, 3701, -3701, 3701^3\}$.

Basis of $\ker N : A(S, 2)/Q(S, 2) \to Q^x/Q^{x^2}$ is $\{u_1, u_3\beta_1\beta_2\}$.

So $S^2_{\text{fake}}(Q, J) \subseteq \langle u_1, u_3\beta_1\beta_2 \rangle$.

The image of $J(Q_{3701})$ in $A^x_{3701}/(A^x_{3701}Q^x_{3701})$ is the image of $[(-4, \sqrt{185}) - \infty^-]$. It is a unit in each component. So $u_3\beta_1\beta_2$ and $u_1u_3\beta_1\beta_2$ do not map to $(x-T)J(Q_{3701})$. Thus $S^2_{\text{fake}}(Q, J) \subseteq \langle u_1 \rangle$.

The image of $J(Q_2)$ in $A^x_2/(A^x_2Q^x_2)$ is the image of $[(2, \sqrt{881}) - \infty^-]$ and $u_1$ does not map to that.

So $S^2_{\text{fake}}(Q, J)$ is trivial.

Since $\dim_{F_2} S^2(Q, J) = \dim_{F_2} S^2_{\text{fake}}(Q, J) + 1$, we have $\dim_{F_2} S^2(Q, J) = 1$.

Since $J(Q)/2J(Q) \subseteq S^2(Q, J)$, we have $\dim_{F_2} J(Q)/2J(Q) \leq 1$.

It’s easy to show that $[\infty^+ - \infty^-]$ has infinite order. So $1 \leq \dim_{F_2} J(Q)/2J(Q)$. Thus $\dim_{F_2} J(Q)/2J(Q) = 1$. Since $J(Q) \cong \mathbb{Z}^r$ we have $J(Q) \cong \mathbb{Z}$.

References.

General case:


$y^2 = f(x)$ case:


$y^p = f(x)$ case: