Computing Selmer groups
of Jacobians

Edward Schaefer
Mzuzu University
and
Santa Clara University

Let $C$ be a curve over $K$, a number field. We want to determine $C(K)$, the $K$-rational points on $C$, when $C(K) \neq \emptyset$.

General program (Bruin, Flynn, Poonen, Schaefer, Stoll, Wetherell, etc.):

Let $J$ be the Jacobian of $C$. $J = \text{Div}^0(C)/\text{Princ}(C)$.

Note $J = J(K)$.

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 $r$.

If those bounds are the same, then you have $r$ and a set of points in $J(K)$ generating a subgroup of finite index. Let’s assume this.

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

\[ 0 \to J(K)[p] \to J(K) \xrightarrow{p} J(K) \to 0 \]

of $\text{Gal}(\overline{K}/K)$-modules.

Taking $\text{Gal}(\overline{K}/K)$-invariants gives us

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

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

Approximate image locally.

\[
\begin{array}{c}
J(K)/pJ(K) \\
\downarrow \prod \alpha_s \\
\prod_{s \in S} J(K_s)/pJ(K_s) \\
\downarrow \prod \text{res}_s \\
\prod_{s \in S} H^1(K_s, J[p])
\end{array} \xrightarrow{\prod \delta_s} \prod_{s \in S} H^1(K_s, J[p])
\]

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, \( A \cong \prod \hat{\phi} K(T_i) \) where \( \prod \hat{\phi} \) means take one representative from each \( \text{Gal}(\overline{K}/K) \)-orbit of \( \{ T_1, \ldots, T_l \} \).

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

Let \( w : J[p] \rightarrow \mu_p(\overline{A}) \) 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 \( A \).

Let’s assume \( \hat{w} \) is injective and we’ve found the image of \( H^1(K, J[p]; S) \) in \( A(S, p) \).

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

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

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}_f(T)'s.

Define \( f : \{ \text{good divisors} \} \to A^* \)
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 \( k\hat{w}\delta \).

Equivalently we have
\[
J(K)/pJ(K) \xrightarrow{\prod f_i} \prod K(T_i)(S, p)
\]
where \( K(T_i)(S, p) \subset K(T_i)^\times/(K(T_i)^\times)^p \).

Note, we have \( A(S, p) = \prod K(T_i)(S, p) \).
Let \( A_s = A \otimes K_s \).
We have $S^p(K, J) = \{ \gamma \in \text{image of } H^1(K, J[p]; S) \text{ in } A(S, p) | \beta_s(\gamma) \in f(J(K_s)/pJ(K_s)), \forall s \in S \}$.

Notes:

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

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

$\text{div}(f_i) = 2(\alpha_i, 0) - (\infty^+ + \infty^-)$.

Note their differences are $\{2(\alpha_i, 0) - 2(\alpha_j, 0)\}$ and the set $\{[(\alpha_i, 0) - (\alpha_j, 0)]\}$ spans $J[2]$. So we have the necessary spanning property. However, the divisors $2(\alpha_i, 0) - (\infty^+ + \infty^-)$ are defined over a field of lower degree than the divisors $2(\alpha_i, 0) - 2(\alpha_j, 0)$.

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 $f = x - T$.

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

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

\[
\begin{align*}
J(K)/pJ(K) & \xrightarrow{f} A(S, p) \\
\prod_{s \in S} J(K_s)/pJ(K_s) & \xrightarrow{f} \prod_{s \in S} A_s^\times/(A_s^\times)^p
\end{align*}
\]
#J(F_3) = 9 and #J(F_5) = 41 so J(Q)_{tors} = 0. Thus J(Q) \cong \mathbb{Z}^7.

We have
\[A = Q[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1),\]
a sextic number field.

Bad primes are \( S = \{\infty, 2, 3701\} \).

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

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

We have \( A = Q[T]/(T^6 + 8T^5 + 22T^4 + 22T^3 + 5T^2 + 6T + 1) \) - a sextic number field.

\[
J(Q)/2J(Q) \xrightarrow{x - T} A^\times/(A^\times^2 Q^\times) \quad \downarrow
\]
\[
\prod_{p \in S} J(Q_p)/2J(Q_p) \xrightarrow{x - T} \prod_{p \in S} A^\times_p/(A^\times^2 Q^\times_p)
\]

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 \( \ker N : A(S, 2)/Q(S, 2) \twoheadrightarrow Q^\times/Q^\times 2 \) 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 \( A^\times_{3701}/(A^\times^2_{3701} Q^\times_{3701}) \) is generated by the image of \( \{(-4, \sqrt{185}) - \infty^\cdot \} \). 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 \( A^\times_2/(A^\times^2 Q^\times_2) \) is the image of \( \langle (2, \sqrt{881}) - \infty^\cdot \rangle \) 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 \(1 \leq \dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q})\).

Thus \(\dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) = 1\).

Since \(J(\mathbb{Q}) \cong \mathbb{Z}^r\) we have \(J(\mathbb{Q}) \cong \mathbb{Z}\).

Let us use a Chabauty argument to prove that for the curve

\[ C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 5x^2 + 6x + 1, \]

we have \(J(\mathbb{Q}) = \{(0, \pm 1), (-3, \pm 1), \infty^\pm\}\).

Note that \(r = 1 < g = 2\) and \(g = 2\) gives the dimension of \(J\).

\(J\) has good reduction at 3.

Let \(\omega\) be a holomorphic 1-form on \(J(\mathbb{Q}_3)\).

Define a homomorphism \(\lambda_\omega : J(\mathbb{Q}_3) \to \mathbb{Q}_3\)

by \(T \mapsto \int_0^T \omega\).

(Can be defined on a neighborhood of 0 using the formal group, and then extended linearly to all of \(J(\mathbb{Q}_3)\).)

We have \(J(\mathbb{F}_3) \cong \mathbb{Z}/9\mathbb{Z}\).

Map \(\iota : C \to J\) by \(R \mapsto [R - (0, 1)]\).

Of the 9 elements of \(J(\mathbb{F}_3)\), exactly 4 are in the image of \(\iota C(\mathbb{F}_3)\), namely the reductions of \(\{(0, \pm 1), \infty^\pm\}\).

So if \(R \in C(\mathbb{Q})\) then \(R\) is in the same residue class mod 3 of one of those 4 points.

We’ll bound the number of points in \(C(\mathbb{Q})\) in the residue class of each of those 4 points.

Closure of \(J(\mathbb{Q})\) in \(J(\mathbb{Q}_3)\) has dimension 1 so let’s find a 1-form \(\omega\) on \(J(\mathbb{Q}_3)\) killing \(J(\mathbb{Q})\) and hence \(C(\mathbb{Q})\).

A basis for the space of holomorphic differentials on \(C\) is \(\omega_1 = \frac{dx}{2y}\) and \(\omega_2 = \frac{x dx}{2y}\).

Express each as element of \(\mathbb{Q}_3[[x]] dx\) (\(x\) is uniform at \((0, 1)\)).

Compute \(9[(-1, -1) - (0, 1)] = [P_1 + P_2 - 2(0, 1)]\), where \(P_1 + P_2 \equiv 2(0, 1)\) (mod 3). (Note all the points are in a neighborhood of \((0, 1)\).)

Then for \(j = 1, 2\), we compute
\[
\int_{0}^{[P_1+P_2-2(0,1)]} t_* \omega_j
g\int_{(0,1)} \omega_j + p \int_{(0,1)} \omega_j \in \mathbb{Q}_3.
\]

Find \(a, b\) such that
\[
a \int_{0}^{[P_1+P_2-2(0,1)]} t_* \omega_1 + b \int_{0}^{[P_1+P_2-2(0,1)]} t_* \omega_2 = 0.
\]
So \(\eta = \frac{adx+bxdx}{2y} \in \mathbb{Q}_3[[x]] dx\) kills \(J(\mathbb{Q})\).

Let \(R \in C(\mathbb{Q})\) with \(R \equiv (0, 1)(\text{mod } 3)\).

Have 0 = \(\int_{0}^{[R-(0,1)]} t_* \eta = \int_{(0,1)} \eta\)
\[
= \alpha_1 x(R) + \alpha_2 x(R)^2 + \ldots
\]
\[
= \alpha_1 3t + \alpha_2 (3t)^2 + \ldots, \text{ with } \alpha_i \in \mathbb{Z}_3.
\]

Let \(i\) be the greatest index of the coefficients with the minimum 3-adic valuation.

From Strassman’s theorem, the number of zeros of this power series in \(\mathbb{Z}_3\) is at most \(i\).

Here \(i = 2\) unit). So only there are exactly two zeros, coming from \((0, 1)\) and \((-3, 1)\). So there are only two points of \(C(\mathbb{Q})\) in the residue class of \((0, 1)\) mod 3.

Do the same thing for \(P = (0, -1), \infty^\pm\), using \(\eta = \frac{adx+bxdx}{2y}\), expanded each time respect to a uniformizer at \(P\).

For \(P = (0, -1)\) we find there are two points of \(C(\mathbb{Q})\) in that residue class, namely \((0, -1)\) and \((-3, -1)\). For \(P = \infty^\pm\) we find there is only one point in the residue class of each.

Since the image of \(C(\mathbb{F}_3)\) in \(J(\mathbb{F}_3)\) by \(R \mapsto [R-(0,1)]\) was equal to the image of the known rational points,
we have \(C(\mathbb{Q}) = \{(0, \pm 1), (-3, \pm 1), \infty^\pm\}\).

References.

General case:

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

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

There isn’t really a good reference on the Chabauty looking like what I did yet. Eventually, when Poone, Schaefer, Stoll (on \(X^2 + Y^3 = Z^7\)) comes out, there will be.