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. $J = \mathrm{Div}^0(C)/\mathrm{Princ}(C)$.

Note $J = J(\overline{K})$.

Elliptic curves are Jacobians: $E \cong \mathrm{Div}^0(E)/\mathrm{Princ}(E)$ by $P \mapsto [P - 0]$.

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

1. Determine $J(K)_{\mathrm{tors}}$. 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 $r < \mathrm{genus}(C)$
on covers of C	if $r \geq \mathrm{genus}(C)$

to determine $C(K)$ (not guaranteed to work).

How to use a Selmer group to find an upper bound for r when $J(K) \cong \mathbf{Z}^r \oplus J(K)_{\mathrm{tors}}$.

Let p be prime. Assume we know $J(K)_{\mathrm{tors}}$. 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

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

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

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

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

$\to H^1(\mathrm{Gal}(\overline{K}/K), J(\overline{K})) \xrightarrow{p} H^1(\mathrm{Gal}(\overline{K}/K), J(\overline{K}))\ldots$

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 $\mathrm{Gal}(\overline{K}/K)$ 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.

$$\begin{array}{ccc} J(K)/pJ(K) & \stackrel{\delta}{\hookrightarrow} & H^1(K, J[p]; S) \\ \downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \mathrm{res}_{\mathfrak{s}} \\ \prod\limits_{\mathfrak{s}\in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \stackrel{\prod \delta_{\mathfrak{s}}}{\hookrightarrow} & \prod\limits_{\mathfrak{s}\in S} H^1(K_{\mathfrak{s}}, J[p]) \end{array}$$

Want image of $J(K)/pJ(K)$ in $H^1(K, J[p]; S)$.

Define $S^p(K, J) = \{\gamma \in H^1(K, J[p]; S) \mid$

$\quad \mathrm{res}_{\mathfrak{s}}(\gamma) \in \delta_{\mathfrak{s}}\big(J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}})\big) \quad \forall\, \mathfrak{s} \in S\}.$

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

2) $\delta_{\mathfrak{s}}$ 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 $\mathrm{Gal}(\overline{K}/K)$-invariants.

What does it look like?

Let $J[p] \setminus 0 = \{T_1, \ldots, T_l\}$.

Concretely, $A \cong \prod^{\diamondsuit} K(T_i)$ where $\prod^{\diamondsuit}$ means take one representative from each $\mathrm{Gal}(\overline{K}/K)$-orbit of $\{T_1, \ldots, T_l\}$.

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

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

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

$A(S, p) \subset A^\times/(A^\times)^p$. Need to replace map

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

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 $pD_i = \mathrm{div}_{f_i}$ and where

$\{f_i\} \cong J[p] \setminus 0$ as $\mathrm{Gal}(\overline{K}/K)$-sets.

We call D a good divisor if $D \in \mathrm{Div}^0(C)(K)$ and its support does not intersect any of the div_{f_i}'s.

Define $f : \{$ good divisors $\} \to A^*$

by $D \mapsto \big(T_i \mapsto f_i(D)\big)$.

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

$J(K)/pJ(K) \xrightarrow{\prod^\diamondsuit f_i} \prod^\diamondsuit K(T_i)(S, p)$
where $K(T_i)(S, p) \subset K(T_i)^\times/(K(T_i)^\times)^p$.

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

Let $A_\mathfrak{s} = A \otimes_K K_\mathfrak{s}$.

$$\begin{array}{ccc} J(K)/pJ(K) & \stackrel{f}{\hookrightarrow} & A(S,p) \\ \downarrow \prod \alpha_{\mathfrak{s}} & & \downarrow \prod \beta_{\mathfrak{s}} \\ \prod_{\mathfrak{s}\in S} J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}}) & \stackrel{f}{\hookrightarrow} & \prod_{\mathfrak{s}\in S} A_{\mathfrak{s}}^{\times}/(A_{\mathfrak{s}}^{\times})^p \end{array}$$

We have $S^p(K,J) = \{\gamma \in \text{image of } H^1(K,J[p];S) \text{ in } A(S,p) \mid$

$\beta_{\mathfrak{s}}(\gamma) \in f\big(J(K_{\mathfrak{s}})/pJ(K_{\mathfrak{s}})\big),\ \ \forall \mathfrak{s} \in S\}$.

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 $\mathrm{div}(f_i) = pD_i$.

What if $\mathrm{div}(f_i) = pD_i - D'$ 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

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

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 $f = x - T$.

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

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 $C(\mathbf{Q})$.

Easy to find $\{(0,\pm1),\ (-3,\pm1),\ \infty^+, \infty^-\} \subseteq C(\mathbf{Q})$.

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

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

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

$$\begin{array}{ccc} J(\mathbf{Q})/2J(\mathbf{Q}) & \stackrel{x-T}{\to} & A^\times/(A^{\times 2}\mathbf{Q}^\times) \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_{p\in S} J(\mathbf{Q}_p)/2J(\mathbf{Q}_p) & \stackrel{x-T}{\to} & \prod_{p\in S} A_p^\times/(A_p^{\times 2}\mathbf{Q}_p^\times) \end{array}$$

Define $S^2_{\mathrm{fake}}(\mathbf{Q}, J) = \{\gamma \in \ker N : A(S,2)/\mathbf{Q}(S,2) \to$

$\mathbf{Q}^\times/\mathbf{Q}^{\times 2} \mid \beta_p(\gamma) \in (x-T)\big(J(\mathbf{Q}_p)\big),\ \forall p \in S\}$.

From Galois action on zeros of sextic, turns out
$\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = \dim_{\mathbf{F}_2} S^2_{\mathrm{fake}}(\mathbf{Q}, J) + 1$.

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

$$\begin{array}{ccc} J(\mathbf{Q})/2J(\mathbf{Q}) & \stackrel{x-T}{\to} & A^\times/(A^{\times 2}\mathbf{Q}^\times) \\ \downarrow & & \downarrow \prod \beta_p \\ \prod_{p\in S} J(\mathbf{Q}_p)/2J(\mathbf{Q}_p) & \stackrel{x-T}{\to} & \prod_{p\in S} A_p^\times/(A_p^{\times 2}\mathbf{Q}_p^\times) \end{array}$$

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

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

The image of $J(\mathbf{Q}_{3701})$ in $A^\times_{3701}/(A^{\times 2}_{3701}\mathbf{Q}^\times_{3701})$ is generated

by 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
$(x-T)J(\mathbf{Q}_{3701})$. Thus $S^2_{\mathrm{fake}}(\mathbf{Q}, J) \subseteq \langle u_1\rangle$.

The image of $J(\mathbf{Q}_2)$ in $A_2^\times/(A_2^{\times 2}\mathbf{Q}_2^\times)$ is the image of

$\langle[(2, \sqrt{881}) - \infty^-]\rangle$ and u_1 does not map to that.

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

Since $\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = \dim_{\mathbf{F}_2} S^2_{\mathrm{fake}}(\mathbf{Q}, J) + 1$,

we have $\dim_{\mathbf{F}_2} S^2(\mathbf{Q}, J) = 1$.

Since $J(\mathbf{Q})/2J(\mathbf{Q}) \subseteq S^2(\mathbf{Q}, J)$,

we have $\dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q}) \le 1$.

It's easy to show that $[\infty^+ - \infty^-]$ has infinite order.

So $1 \le \dim_{\mathbf{F}_2} J(\mathbf{Q})/2J(\mathbf{Q})$.

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

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

Let us use a Chabauty argument to prove that for

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

we have $C(\mathbf{Q}) = \{(0, \pm 1), (-3, \pm 1), \infty^\pm\}$.

Note that $r = 1 < g = 2$ and $g = 2$ gives the dimension of J.

J has good reduction at 3.

Let ω be a holomorphic 1-form on $J(\mathbf{Q}_3)$.

Define a homomorphism $\lambda_\omega \colon J(\mathbf{Q}_3) \to \mathbf{Q}_3$

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 $J(\mathbf{Q}_3)$.)

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

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

Of the 9 elements of $J(\mathbf{F}_3)$, exactly 4 are in the image

of $\iota C(\mathbf{F}_3)$, namely the reductions of

$\{(0, \pm 1), \infty^\pm\}$.

So if $R \in C(\mathbf{Q})$ then R is in the same residue class

mod 3 of one of those 4 points.

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

Closure of $J(\mathbf{Q})$ in $J(\mathbf{Q}_3)$ has dimension 1 so let's find a

1-form ω on $J(\mathbf{Q}_3)$ killing $J(\mathbf{Q})$ and hence $C(\mathbf{Q})$.

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 $\mathbf{Q}_3[[x]]\, dx$ (x is unif'r at $(0, 1)$).

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

Then for $j = 1, 2$, we compute

$\int_0^{[P_1+P_2-2(0,1)]} \iota_*\omega_j$

$= \int_{(0,1)}^{P_1} \omega_j + \int_{(0,1)}^{P_2} \omega_j \in \mathbf{Q}_3$.

Find a, b such that $a \int_0^{[P_1+P_2-2(0,1)]} \iota_*\omega_1 + b \int_0^{[P_1+P_2-2(0,1)]} \iota_*\omega_2 = 0$.

So $\eta = \frac{adx+bxdx}{2y} \in \mathbf{Q}_3[[x]]\, dx$ kills $J(\mathbf{Q})$.

Let $R \in C(\mathbf{Q})$ with $R \equiv (0,1) (\bmod 3)$.

Have $0 = \int_0^{[R-(0,1)]} \iota_*\eta = \int_{(0,1)}^{R} \eta$

$= \alpha_1 x(R) + \alpha_2 x(R)^2 + \ldots$

$= \alpha_1 3t + \alpha_2 (3t)^2 + \ldots$, with $\alpha_i \in \mathbf{Z}_3$.

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 $\mathbf{Z}_3$ 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 $C(\mathbf{Q})$ 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 $C(\mathbf{Q})$ 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 $C(\mathbf{F}_3)$ in $J(\mathbf{F}_3)$ by $R \mapsto [R - (0, 1)]$ was equal to the image of the known rational points,

we have $C(\mathbf{Q}) = \{(0, \pm 1), (-3, \pm 1), \infty^{\pm}\}$.

References.

General case:

Schaefer, E.F. *Computing a Selmer group of a Jacobian using functions on the curve*, Mathematische Annalen, **310**, 1998, 447–471.

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

Flynn, E.V., Poonen, B. and Schaefer, E.F. *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Mathematical Journal, **90**, 1997, 435–463.

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

Poonen, B. and Schaefer, E.F. *Explicit Descent for Jacobians of cyclic covers of the projective line*, Journal für die reine und angewandte Mathematik, **488**, 1997, 141–188.

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