Coverings and Mordell-Weil Sieve

Michael Stoll

International University Bremen

(Jacobs University as of soon)

Banff, February 6, 2007

Local Obstruction

Let $C/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 2$.

Goal:
Determine $C(\mathbb{Q})$!

Sub-Goal 1:
Decide if $C(\mathbb{Q}) = \emptyset$!

Sub-Goal 2:
If $C(\mathbb{Q}) \neq \emptyset$, find all the points (and prove that these are all)!

Easy Case for Sub-Goal 1:
$C(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$ for some prime p.
This is equivalent to $C(\mathbb{A}_{\mathbb{Q}}) = \emptyset$.

Coverings

Let $\pi : D \to C$ be a finite étale, geometrically Galois covering
(more precisely: a C-torsor under a finite $\mathbb{Q}$-group scheme G).

This covering has *twists* $\pi_\xi : D_\xi \to C$ for $\xi \in H^1(\mathbb{Q}, G)$.

More concretely, a twist $\pi_\xi : D_\xi \to C$ of $\pi : D \to C$ is another covering of C that over $\bar{\mathbb{Q}}$ is isomorphic to $\pi : D \to C$.

Example. Consider $C : y^2 = g(x)h(x)$ with $\deg g$, $\deg h$ even.
Then $D : u^2 = g(x),\ v^2 = h(x)$ is a C-torsor under $\mathbb{Z}/2\mathbb{Z}$,
and the twists are $D_d : u^2 = d\,g(x),\ v^2 = d\,h(x),\quad d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Every rational point on C lifts to one of the twists,
and there are only finitely many twists such that $D_d(\mathbb{Q}_v) \neq \emptyset$ for all v.

Coverings

Let $\pi : D \to C$ be a finite étale, geometrically Galois covering (more precisely: a C-torsor under a finite $\mathbb{Q}$-group scheme G).

This covering has *twists* $\pi_\xi : D_\xi \to C$ for $\xi \in H^1(\mathbb{Q}, G)$.

More concretely, a twist $\pi_\xi : D_\xi \to C$ of $\pi : D \to C$ is another covering of C that over $\bar{\mathbb{Q}}$ is isomorphic to $\pi : D \to C$.

Example. Consider $C : y^2 = g(x)h(x)$ with $\deg g$, $\deg h$ even.
Then $D : u^2 = g(x),\ v^2 = h(x)$ is a C-torsor under $\mathbb{Z}/2\mathbb{Z}$,
and the twists are $D_d : u^2 = d\,g(x),\ v^2 = d\,h(x)$, $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Every rational point on C lifts to one of the twists,
and there are only finitely many twists such that $D_d(\mathbb{Q}_v) \neq \emptyset$ for all v.

Descent

More generally, we have the following result.

Theorem.

- $C(\mathbb{Q}) = \bigcup_{\xi \in H^1(\mathbb{Q},G)} \pi_\xi(D_\xi(\mathbb{Q}))$.
- $\mathrm{Sel}^\pi(C) := \{\xi \in H^1(\mathbb{Q}, G) : D_\xi(\mathbb{A}_\mathbb{Q}) \neq \emptyset\}$ is finite (and computable).

(Fermat, Chevalley-Weil, . . .)

If we find $\mathrm{Sel}^\pi(C) = \emptyset$, then $C(\mathbb{Q}) = \emptyset$.

Example

Consider the genus 2 curve

$$C : y^2 = -(x^2 + x - 1)(x^4 + x^3 + x^2 + x + 2) = f(x)\,.$$

C has points everywhere locally
($f(0) = 2,\ f(1) = -6,\ f(-2) = -3 \cdot 2^2,\ f(18) \in (\mathbb{Q}_2^\times)^2,\ f(4) \in (\mathbb{Q}_3^\times)^2$).

The relevant twists of the obvious $\mathbb{Z}/2\mathbb{Z}$-covering are

$$d\,u^2 = -x^2 - x + 1\,, \qquad d\,v^2 = x^4 + x^3 + x^2 + x + 2$$

where d is one of $1, -1, 19, -19$.
If $d < 0$, the second equation has no solution in $\mathbb{R}$;
if $d = 1$ or 19, the pair of equations has no solution over $\mathbb{F}_3$.

So the Selmer set is empty, and $C(\mathbb{Q}) = \emptyset$.

First Conjectures

This should always work. More precisely:

Conjecture 1
If $C(\mathbb{Q}) = \emptyset$, then there is a covering π of C such that $\mathrm{Sel}^{\pi}(C) = \emptyset$.

Conjecture 2
If $C(\mathbb{Q}) = \emptyset$, then there is an abelian covering π of C such that $\mathrm{Sel}^{\pi}(C) = \emptyset$.

(A covering is abelian if its Galois group is abelian.)

Conjecture 2 is stronger than Conjecture 1.
The Section Conjecture implies Conjecture 1.
Poonen has a heuristic argument that supports Conjecture 2.

Abelian Coverings

By Geometric Class Field Theory, all (connected) abelian coverings "come from the Jacobian".

More precisely, let $V = \mathrm{Pic}^1_C$ be the principal homogeneous space for $J = \mathrm{Pic}^0_C$ that has a natural embedding $C \to V$.

Then every abelian covering $D \to C$ is covered by an n-covering for some $n \geq 1$.

An n-covering is obtained by pull-back from an n-covering of V; geometrically, this is just multiplication by n: $J \to J$.

Let $\mathrm{Sel}^{(n)}(C) \subset H^1(\mathbb{Q}, J[n])$ denote the corresponding Selmer set.

Conjecture 2: $C(\mathbb{Q}) = \emptyset$ implies $\mathrm{Sel}^{(n)}(C) = \emptyset$ for some n.

Refinement

Consider local conditions on C,
given by a closed and open subset $X \subset C(\mathbb{A}_{\mathbb{Q}})$.
(Concretely: congruence conditions, connected components of $C(\mathbb{R})$.)

Then we can consider $\mathrm{Sel}^{\pi}(C; X)$,
the subset of $\mathrm{Sel}^{\pi}(C)$ consisting of twists
that have adelic points whose image on C is in X.

Conjecture 1'.
For all X as above, if $C(\mathbb{Q}) \cap X = \emptyset$,
then there is a covering π of C such that $\mathrm{Sel}^{\pi}(C; X) = \emptyset$.

Conjecture 2'.
For all X as above, if $C(\mathbb{Q}) \cap X = \emptyset$,
then there is some $n \geq 1$ such that $\mathrm{Sel}^{(n)}(C; X) = \emptyset$.

Comments

- The Section Conjecture implies Conjecture 1',
  which is equivalent to Conjecture 1.

- Conjecture 2' implies Conjecture 1' and Conjecture 2.

- Evidence for Conjecture 2 in many examples (see my other talk).

- Conjecture 2' is true for $X_0(N)$, $X_1(N)$, $X(N)$, if genus is positive.

- "Abelian descent information" is equivalent
  to "Brauer group information".

  Conjecture 2 implies that the Brauer-Manin obstruction
  is the only one against rational points.

- See my paper Finite descent obstructions ...

Mordell-Weil Sieve 1

Now assume that we know generators of $J(\mathbb{Q})$
and that we fix a basepoint $O \in C(\mathbb{Q})$
(or a a rational divisor class of degree 1 on C).

Then we have the usual embedding $C \to J$.

We only need to consider n-coverings of C
that are pull-backs of n-coverings of J that have rational points;
they are of the form $J \to J$, $P \mapsto Q + nP$ for $Q \in J(\mathbb{Q})$.

We are then interested in the rational points on C
that map into a given coset $Q + nJ(\mathbb{Q})$.

Mordell-Weil Sieve 2

Let S be a finite set of primes of good reduction.
Consider the following diagram.

$$\begin{tikzcd}
C(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{Q})/nJ(\mathbb{Q}) \arrow[d] \arrow[dd, bend left, "\beta"] \\
C(\mathbb{A}_\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{A}_\mathbb{Q}) \arrow[r] \arrow[d] & J(\mathbb{A}_\mathbb{Q})/nJ(\mathbb{A}_\mathbb{Q}) \arrow[d] \\
\prod_{p\in S} C(\mathbb{F}_p) \arrow[r] \arrow[rr, bend right, "\alpha"'] & \prod_{p\in S} J(\mathbb{F}_p) \arrow[r] & \prod_{p\in S} J(\mathbb{F}_p)/nJ(\mathbb{F}_p)
\end{tikzcd}$$

We can compute the maps α and β.
If their images do not intersect, then $C(\mathbb{Q}) = \emptyset$.

Poonen Heuristic:
If $C(\mathbb{Q}) = \emptyset$, then this will be the case when n and S are sufficiently large.

Mordell-Weil Sieve 3

We can also bring in a local condition.
This is equivalent with requiring $P \in C(\mathbb{Q})$ to be mapped to certain cosets in $J(\mathbb{Q})/NJ(\mathbb{Q})$, for some N.

We can then use the procedure above with n a multiple of N and restricting to these cosets.

Conjecture 2".
Let $Q \in J(\mathbb{Q})$. If no $P \in C(\mathbb{Q})$ maps into $Q + NJ(\mathbb{Q})$, then the procedure will prove that (for S and $n \in N\mathbb{Z}$ large enough).

Conjecture 2" is slightly stronger than Conjecture 2'.

Consequence:
If C satisfies Conjecture 2" and $N \geq 1$, then we can decide whether $Q + NJ(\mathbb{Q})$ contains a point from C.

Effective Mordell?

Given $O \in C(\mathbb{Q})$ and generators of $J(\mathbb{Q})$, here is a tentative procedure.

1. Find $N \geq 1$ such that $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective (Minhyong).
2. For each coset, decide if it is in the image (Mordell-Weil sieve).

We can attempt the second step,
and if Conjecture 2'' is satisfied, we will be successful.
(Otherwise, the procedure will not terminate.)

Question.
Is there an N for step 1 that only depends on the genus?

Chabauty

In the Chabauty situation, the first step can be done as follows.

Let $\omega \in \Omega_C(\mathbb{Q}_p)$ be a differential killing $J(\mathbb{Q})$.
If the reduction $\bar{\omega}$ does not vanish on $C(\mathbb{F}_p)$ and $p > 2$,
then each residue class contains at most one rational point.

This implies that $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective, where $N = \#J(\mathbb{F}_p)$.

Heuristically, the set of primes p satisfying this condition
should have positive density (at least when J is simple).

In practice, this works very well for $g = 2$ and $r = 1$.