How to Obtain Global Information From Computations Over Finite Fields

Michael Stoll
Jacobs University Bremen

Göttingen, July 5, 2007

The Goal

Let A be an abelian variety over $\mathbb{Q}$,
and let $V \subset A$ be a subvariety
that does not contain a translate of a nontrivial subabelian variety of A.

Goal.
Obtain information on $V(\mathbb{Q})$, the rational points on V!
For example, prove that $V(\mathbb{Q}) = \emptyset$!

Example.
Let C be a curve of higher genus over $\mathbb{Q}$,
and assume we know a rational divisor class of degree 1 on C.
Then $C \hookrightarrow J$, where J is the Jacobian variety of C.

The Idea

We know that $A(\mathbb{Q})$ is a finitely generated abelian group.

Assumption.
We know explicit generators of $A(\mathbb{Q})$.

If p is a prime of good reduction for A and V,
we can then compute (the images of) the following maps:

$$\alpha_p : V(\mathbb{F}_p) \hookrightarrow A(\mathbb{F}_p) \qquad \text{and} \qquad \beta_p : A(\mathbb{Q}) \to A(\mathbb{F}_p)$$

If $P \in A(\mathbb{Q})$ is in $V(\mathbb{Q})$, then $\beta_p(P) \in \alpha_p\Big(V(\mathbb{F}_p)\Big)$.

Thus we obtain congruence conditions on the coefficients of P
with respect to our generators of $A(\mathbb{Q})$.

Using Several Primes

We can extend this to more than one prime.

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

$$\begin{array}{ccc} V(\mathbb{Q}) & \hookrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \beta = \prod_{p \in S} \beta_p \\ \prod_{p \in S} V(\mathbb{F}_p) & \xhookrightarrow{\alpha = \prod_{p \in S} \alpha_p} & \prod_{p \in S} A(\mathbb{F}_p) \end{array}$$

As before, if $P \in A(\mathbb{Q})$ is in $V(\mathbb{Q})$, then $\beta(P) \in \text{im}(\alpha)$.

In particular, if $\text{im}(\alpha) \cap \text{im}(\beta) = \emptyset$, then $V(\mathbb{Q}) = \emptyset$.

This technique is called the Mordell-Weil Sieve.

Poonen Heuristic (1)

Assuming that indeed $V(\mathbb{Q}) = \emptyset$,
what are our chances to prove this fact in the way just described?

The following considerations are due to Bjorn Poonen.

Let B be some large integer.
We will consider all primes $p < B^2$.

For $r > 0$, there is a number $\delta_r > 0$ such that there are at least $\delta_r B^r$ B-smooth integers $\leq B^r$, for B large.
("B-smooth" means that all prime divisors are $\leq B$.)

We assume that a similar statement is true for the set $\{\#A(\mathbb{F}_p) : p < B^2\}$.

Poonen Heuristic (2)

More precisely, we make the following

Assumption 1.
Let $S_B = \{p < B^2 : p \text{ good and } \#A(\mathbb{F}_p) \text{ is } B\text{-smooth}\}$. Then

$$\liminf_{B\to\infty} \frac{\#S_B}{\pi(B^2)} > 0\,.$$

Remarks.

(1) $\#A(\mathbb{F}_p) \le (\sqrt{p}+1)^{2\dim A} \le B^{2\dim A}(1+o(1))$.

(2) For a fixed prime q, $\#A(\mathbb{F}_p)$ is more likely to be divisible by q than a random integer.

The exponent of $A(\mathbb{F}_p)$ for $p \in S_B$ divides

$$\prod_{q\le B} q^{\lfloor \log_q \#A(\mathbb{F}_p)\rfloor} \le B^{\pi(B)\dim A}(1+o(1)) \approx e^{B\dim A}.$$

Poonen Heuristic (3)

Let r be the rank of $A(\mathbb{Q})$.
Then the image of $A(\mathbb{Q})$ in $\prod_{p \in S_B} A(\mathbb{F}_p)$ has size at most $c\, e^{rB \dim A}$.

On the other hand, for B large, we have

$$\# \prod_{p \in S_B} A(\mathbb{F}_p) \approx e^{\delta_B B^2 \dim A},$$

where $\delta_B = \dfrac{\# S_B}{\pi(B^2)} \geq \delta > 0$, by Assumption 1.

We now make the following

Assumption 2.
$V(\mathbb{F}_p)$ behaves like a random subset of $A(\mathbb{F}_p)$ of size $\approx p^{\dim V}$.

Then $\prod_{p \in S_B} V(\mathbb{F}_p)$ is a random subset of $\prod_{p \in S_B} A(\mathbb{F}_p)$ of size $\approx e^{\delta_B B^2 \dim V}$.

Poonen Heuristic (4)

$$\begin{array}{ccc} V(\mathbb{Q}) & \hookrightarrow & A(\mathbb{Q}) \\ \downarrow & & \downarrow \beta_B \\ \prod_{p \in S_B} V(\mathbb{F}_p) & \xhookrightarrow{\alpha_B} & \prod_{p \in S_B} A(\mathbb{F}_p) \end{array}$$

$$\# \prod_{p \in S_B} A(\mathbb{F}_p) \approx e^{\delta_B B^2 \dim A}, \quad \#\mathrm{im}(\alpha_B) \approx e^{\delta_B B^2 \dim V}, \quad \#\mathrm{im}(\beta_B) < c\, e^{rB \dim A}$$

So the probability that $\mathrm{im}(\alpha) \cap \mathrm{im}(\beta) \neq \emptyset$ is (roughly)

$$\frac{\#\mathrm{im}(\alpha_B) \cdot \#\mathrm{im}(\beta_B)}{\# \prod_{p \in S_B} A(\mathbb{F}_p)} < c\, e^{rB \dim A - \delta_B B^2 (\dim A - \dim V)}.$$

Since $\delta_B \geq \delta > 0$, this tends to zero when $B \to \infty$.

Conclusion.

With probability 1, the Mordell-Weil Sieve will be successful.

Example

In a joint project with Nils Bruin,
we considered all ‘small’ curves of genus 2:

$$C : y^2 = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

with $f_0, f_1, \dots, f_6 \in \{-3, -2, \dots, 3\}$.

Our goal was to decide whether C has rational points,
for all such curves C.

Among the $\approx 200\,000$ isomorphism classes, there were $\approx 1\,500$,
for which more straight-forward approaches were unsuccessful.

We applied the Mordell-Weil Sieve to these curves and their Jacobians;
for all of them, we could prove that $C(\mathbb{Q}) = \emptyset$.

(See my talk at the Summer School 2006 for more information.)

Practice

In practice, the computation suggested by the heuristic is infeasible.

Instead, we pick a smooth number N and work with

$$\begin{array}{ccc} V(\mathbb{Q}) & \longrightarrow & \dfrac{A(\mathbb{Q})}{NA(\mathbb{Q})} \\ \big\downarrow & & \big\downarrow \beta \\ \prod_{p \in S} V(\mathbb{F}_p) & \xrightarrow{\alpha} & \prod_{p \in S} \dfrac{A(\mathbb{F}_p)}{NA(\mathbb{F}_p)} \end{array}$$

where S is a set of primes such that $A(\mathbb{F}_p)/NA(\mathbb{F}_p)$ is large.

We build N successively as a product of prime factors,
keeping track of $\beta^{-1}\big(\mathrm{im}(\alpha)\big)$ at each step.

It is an interesting problem to find a good strategy for this procedure.

Improvements

Instead of just looking at primes of good reduction,
we can work more generally with finite quotients of $A(\mathbb{Q}_p)$.

In this way, we can include information at bad primes
and 'deep' information modulo higher powers of p.

For example, the component group of the Néron model of A at p
can provide useful information.

These improvements make the Mordell-Weil Sieve practical
for a curve sitting in an abelian surface when $r \leq 3$ or 4.

Refinement

Even when V has rational points,
we can use the Mordell-Weil Sieve to rule out rational points on V
with certain additional properties.

For example, we can show that there is no $P \in V(\mathbb{Q})$ such that

- P is in a certain residue class mod n, or
- P is in a certain coset mod $nA(\mathbb{Q})$.

(Both kinds of condition are equivalent.)

In the first case, we restrict to the relevant subset of $V(\mathbb{Q}_p)$
for the primes p dividing n.

In the second case, we use values of N that are multiples of n
and restrict to the relevant cosets in $A(\mathbb{Q})/NA(\mathbb{Q})$.

Example (1)

Consider the smooth plane quartic curve

$$C : -2x^3y - 2x^3z + 6x^2yz + 3xy^3 - 9xy^2z + 3xyz^2 - xz^3 + 3y^3z - yz^3 = 0\,.$$

It has the known rational points

$$(1:0:0)\,, \quad (0:1:0)\,, \quad (0:0:1)\,, \quad (1:1:1)\,.$$

Any point $P \in C(\mathbb{Q})$ such that

$$P \equiv (0:1:0) \bmod 3 \quad \text{and} \quad P \equiv (1:0:0) \text{ or } (1:1:1) \bmod 2$$

would lead to a primitive integral solution of $x^2 + y^3 = z^7$.

Note that the known points do not satisfy this condition.

We want to prove that no rational point on C satisfies the condition.

(This was the last step in the complete solution of $x^2 + y^3 = z^7$, see Poonen, Schaefer, Stoll, Duke Math. J. 2007.)

Example (2)

Let J be the Jacobian of C.
We can prove that the rank of $J(\mathbb{Q})$ is 3,
and we find generators of a subgroup of $J(\mathbb{Q})$ of finite index prime to 14.

We need to use information at the bad primes 2 and 3;
we will use the component groups.

We find

$$J(\mathbb{Q}_2) \longrightarrow\!\!\!\!\rightarrow \Phi_2 \cong \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$$

$$J(\mathbb{Q}_3) \longrightarrow\!\!\!\!\rightarrow \Phi_3 \cong \frac{\mathbb{Z}}{7\mathbb{Z}}$$

The conditions correspond to subsets of size 3 and 1, respectively.

Example (3)

With the additional information coming from

$$J(\mathbb{F}_{23}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{16\mathbb{Z}} \times \frac{\mathbb{Z}}{16\mathbb{Z}} \times \frac{\mathbb{Z}}{32\mathbb{Z}}$$

$$J(\mathbb{F}_{97}) \cong \frac{\mathbb{Z}}{98\mathbb{Z}} \times \frac{\mathbb{Z}}{98\mathbb{Z}} \times \frac{\mathbb{Z}}{98\mathbb{Z}}$$

$$J(\mathbb{F}_{13}) \longrightarrow\!\!\!\!\rightarrow \frac{\mathbb{Z}}{14\mathbb{Z}}$$

we get a contradiction.

Since we are working in $J(\mathbb{Q})/NJ(\mathbb{Q})$ with $N = 2^a \cdot 7^b$,
it suffices to know that the known points in $J(\mathbb{Q})$
generate a subgroup of index prime to 14.

Another Application

We can use the Mordell-Weil Sieve to show
that for every $P \in V(\mathbb{Q})$ there is a known point $Q \in V(\mathbb{Q})$
such that $P - Q$ is in a subgroup of very large index in $A(\mathbb{Q})$.

This implies in particular that any unknown point in $V(\mathbb{Q})$
must be extremely large.

In some cases, we can get a (quite large) bound
on the height of integral points on V.

We can combine this with the MW Sieve information
to show that we know all integral points.

(This is ongoing work of Bugeaud, Siksek, Stoll, Tengely.)

Summary

- The Mordell-Weil Sieve is a method that gives information on the rational points of a subvariety of an abelian variety.
- It combines global information on the Mordell-Weil group with information over the finite fields $\mathbb{F}_p$.
- The Poonen heuristic predicts that we can always verify that there are no rational points on the subvariety.
- With a suitable compuational strategy and some improvements, the method is practical when the MW rank is not too large.
- It has been successfully applied in various contexts and is likely to have more applications in the future.