HOW TO OBTAIN GLOBAL INFORMATION FROM COMPUTATIONS OVER FINITE FIELDS

MICHAEL STOLL

ABSTRACT. This is an extended version of the talk I gave at the summer school in Göttingen in July 2007.

We discuss the Mordell-Weil Sieve and some applications.

1. The Problem

Let A be an abelian variety over $\mathbb{Q}$ (for simplicity; we could work over an arbitrary number field instead), and let $V \subset A$ be a "transversal" subvariety, i.e., a subvariety that does not contain a translate of a nontrivial subabelian variety of A.

Our goal is to obtain information on $V(\mathbb{Q})$, the set of rational points on V. For example, we would like to prove that $V(\mathbb{Q}) = \emptyset$.

The standard example for this situation is when we have a curve C over $\mathbb{Q}$ of genus $g \geq 2$. If we we know a rational divisor class D of degree 1 on C, then we can use D as a base-point for an embedding $\iota : C \hookrightarrow J$, $P \mapsto [P] - D$. Here $A = J$ is the Jacobian variety of C, and $V = \iota(C) \subset A$.

2. The Idea

Our approach is to combine global and local information in the following way. The *global* input is the knowledge of the Mordell-Weil group $A(\mathbb{Q})$. This means that we need to know explicit generators of this group (which is a finitely generated abelian group, by the Mordell-Weil Theorem). Note that it requires some nontrivial computations and a bit of luck to obtain this information. If A is the Jacobian of a curve of genus 2, it is usually possible to perform the necessary computations successfully. This includes a 2-descent on A as described in [St01], a search for rational points on A (see for example [BS07b]), possibly visualization computations to improve the upper bound for the rank obtained by 2-descent (see [Br04] and [BF06]) and canonical height computations in order to make sure that one has generators of the full group (see [St99] and [St02]). The latter part, which is currently only available for genus 2 Jacobians, can be replaced by a computation that checks that the index of the known subgroup is prime to a finite set of primes. Compare the genus 3 example from [PSS07] discussed in Section 7 below.

Date: December 1, 2007.

The *local* input is obtained by looking at the situation over $\mathbb{F}_p$, for a suitable finite set S of primes p. We assume (for now) that p is a prime of good reduction for A and V. We can then compute the finite abelian group $A(\mathbb{F}_p)$ and determine its subset $V(\mathbb{F}_p)$. Denote by

$$\alpha_p : V(\mathbb{F}_p) \hookrightarrow A(\mathbb{F}_p)$$

the inclusion map.

Since we assume we know generators of $A(\mathbb{Q})$, we can also compute the group homomorphism

$$\beta_p : A(\mathbb{Q}) \to A(\mathbb{F}_p)\,.$$

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

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

We now combine the information we obtain from all the primes in the set S. Consider the following commutative diagram.

$$\begin{tikzcd}
V(\mathbb{Q}) \arrow[r, hook] \arrow[d] & A(\mathbb{Q}) \arrow[d, "\beta = \prod_{p \in S} \beta_p"] \\
\prod_{p \in S} V(\mathbb{F}_p) \arrow[r, hook, "\alpha = \prod_{p \in S} \alpha_p"] & \prod_{p \in S} A(\mathbb{F}_p)
\end{tikzcd}$$

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

In particular, if $\operatorname{im}(\alpha) \cap \operatorname{im}(\beta) = \emptyset$, then this *proves* that $V(\mathbb{Q}) = \emptyset$.

This technique is called the *Mordell-Weil Sieve*. It appears first in Scharaschkin's thesis [Sc99]. It was later applied to many genus 2 curves by Flynn [Fl04], and more recently used and improved by Bruin and Stoll [BS07a] in a project whose aim it was to decide for all genus 2 curves $C : y^2 = f(x)$, where f has integral coefficients of absolute value ≤ 3, whether C has rational points or not; see Section 4 below.

3. The Poonen Heuristic

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* [Po06].

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

For $\rho > 0$, there is a number $\delta_\rho > 0$ such that there are at least $\delta_\rho B^\rho$ *B-smooth* integers $\leq B^\rho$, for B large. (An integer is "B-smooth" if all its prime divisors are $\leq B$.)

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

Assumption 1. *Let*

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

Then

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

By the Weil bounds, we have

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

If the group orders $\#A(\mathbb{F}_p)$ behave like random integers in this range, then the assumption should be valid, by the result on the density of B-smooth numbers up to B^ρ (taking $\rho = 2\dim A$).

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

$$\prod_{q\le B} q^{\lfloor \log_q \#A(\mathbb{F}_p)\rfloor} \le B^{2\pi(B)\dim A}(1+o(1)) \approx e^{2B\dim A}\,.$$

The inequality comes from $q^{\lfloor \log_q \#A(\mathbb{F}_p)\rfloor} \le \#A(\mathbb{F}_p) \le B^{2\dim A}(1+o(1))$, and for the estimate, we use the Prime Number Theorem $\pi(x) \sim x/\log x$.

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 $c\,e^{2rB\dim A}$ for some constant c. This is because each generator of $A(\mathbb{Q})$ maps to an element of order $\ll e^{2B\dim A}$.

On the other hand, for B large, we have

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

where $\delta_B = \dfrac{\#S_B}{\pi(B^2)} \ge \delta > 0$, 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 $\approx e^{2\delta_B B^2\dim V}$. Recall the diagram of maps

$$\begin{tikzcd}
V(\mathbb{Q}) \arrow[r, hook] \arrow[d] & A(\mathbb{Q}) \arrow[d, "\beta_B"] \\
\prod_{p\in S_B} V(\mathbb{F}_p) \arrow[r, hook, "\alpha_B"] & \prod_{p\in S_B} A(\mathbb{F}_p)
\end{tikzcd}$$

We have seen that we have the following estimates.

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

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

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

(This is in fact the expected size of the intersection, which gives an upper bound for the relevant probability.) Since $\delta_B \geq \delta > 0$, this tends to zero when $B \to \infty$. Thus we obtain the following result.

Proposition 3. *Under Assumptions 1 and 2, the Mordell-Weil Sieve will be successful with probability 1.*

Note that Assumption 2 will not be valid when $V(\mathbb{Q}) \neq \emptyset$, since in this case, $V(\mathbb{F}_p)$ will always contain the images of the global points in $V(\mathbb{Q})$. Of course, the Mordell-Weil Sieve computation cannot succeed in this case. On the other hand, in the absence of global points, there does not seem to be any reason for a non-random behavior of the sets $V(\mathbb{F}_p)$, and so Assumption 2 should make sense in this case. In any case, if we perform the computation and it succeeds, this will prove *unconditionally* that $V(\mathbb{Q}) = \emptyset$; the assumptions are only necessary to convince us that we will succeed eventually.

4. Application: Proving that Curves Do Not Have Rational Points

In a joint project with Nils Bruin [BS07a], we considered all "small" curves of genus 2:

$$C : y^2 = f_6 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0$$

with $f_0, f_1, \ldots, f_6 \in \{-3, -2, -1, 0, 1, 2, 3\}$.

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

Among the $\approx 200\,000$ isomorphism classes of such curves, there were $\approx 1\,500$, for which more straight-forward approaches (searching for rational points, checking for local points, performing a "2-cover descent"; for details see [BS07a]) were unsuccessful.

We were able to determine generators of $J(\mathbb{Q})$ for these curves (this is conditional on the Birch and Swinnerton-Dyer Conjecture in 42 cases). We then applied the *Mordell-Weil Sieve* to these curves and their Jacobians; for *all* of them, we could prove in this way that $C(\mathbb{Q}) = \emptyset$.

5. Practical Considerations and Improvements

In practice, the computation suggested by the heuristic is infeasible. The sets we have to deal with would be much too large.

Instead, we pick a smooth number N and work with

$$\begin{tikzcd}
V(\mathbb{Q}) \arrow[r] \arrow[d] & \dfrac{A(\mathbb{Q})}{NA(\mathbb{Q})} \arrow[d, "\beta^{(N)}"] \\
\prod_{p \in S} V(\mathbb{F}_p) \arrow[r, "\alpha^{(N)}"] & \prod_{p \in S} \dfrac{A(\mathbb{F}_p)}{NA(\mathbb{F}_p)}
\end{tikzcd}$$

where S is a set of primes such that $A(\mathbb{F}_p)/NA(\mathbb{F}_p)$ is reasonably large (i.e., such that a large part of the exponent divides N).

Instead of computing the subset of $A(\mathbb{Q})/NA(\mathbb{Q})$ of elements that map under $\beta^{(N)}$ into the image of $\alpha^{(N)}$ directly in one go, we build N successively as a product of prime factors, keeping track of the sets $\Sigma(N') = (\beta^{(N')})^{-1}\big(\mathrm{im}(\alpha^{(N')})\big)$ at each step. If we go from N' to $N'q$, we then only have to check all possible lifts to $A(\mathbb{Q})/N'qA(\mathbb{Q})$ of the elements of $\Sigma(N')$. The number of such checks is $q^r \#\Sigma(N')$, and the total complexity will be much less than N^r (which corresponds to the one-step approach) if we can make sure that the sets $\Sigma(N')$ are considerably smaller than $(N')^r$. For more details on our implementation, see [BS07c].

The procedure as decribed so far works well when the rank is at most 2. To go further than this, we need to use more information than just what we can obtain mod p for primes p of good reduction. For the method, this restriction is unnecessary, and we can work more generally with finite quotients of $A(\mathbb{Q}_p)$ in place of $A(\mathbb{F}_p)$. 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 a prime p of bad reduction can provide useful information.

These improvements make the Mordell-Weil Sieve practical for a curve sitting in an abelian surface when $r \leq 3$ and maybe even $r = 4$ (but the evidence in this case is too sparse to say something definite).

6. A Variation

Even when V does have 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 $nA(\mathbb{Q})$.

(These two kinds of condition are actually equivalent: via the maps $A(\mathbb{Q}) \to A(\mathbb{Q}_p)/A(\mathbb{Q}_p)_n$ and $C(\mathbb{Q}_p) \to A(\mathbb{Q}_p)/A(\mathbb{Q}_p)_n$, congruence conditions mod p^n can be translated into coset conditions mod $eA(\mathbb{Q})$, where e is the exponent of $A(\mathbb{Q}_p)/A(\mathbb{Q}_p)_n$, and conversely. Here $A(\mathbb{Q}_p)_n$ is the nth kernel of reduction.)

To deal with the first kind of condition, we restrict to the relevant subset of $V(\mathbb{Q}_p)$ for the primes p dividing n.

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

If we can determine an integer n such that no two points in $V(\mathbb{Q})$ are in the same coset mod $nA(\mathbb{Q})$, then this refinement of the Mordell-Weil Sieve allows us (assuming a suitably modified version of the Poonen Heuristic) to *determine* the set $V(\mathbb{Q})$ in the following way. For each coset of $nA(\mathbb{Q})$, we search for points in this coset that are on V, and at the same time, we run the Mordell-Weil Sieve in an attempt to show that no such point exists. One of the two procedures should be successful, and so we will either have shown that there is no point on V in the coset, or else we will have found such a point, and then we know that it must be the only one.

If V is a curve in its Jacobian A, and $r < \dim A$ (which is the genus of the curve), then we can use *Chabauty's method* to obtain such a "separating" integer n. For details, see [BS07c].

7. An Example

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 [PSS07].)

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 of the Néron model at these primes. We find

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

$$J(\mathbb{Q}_3) \twoheadrightarrow \Phi_3 \cong \frac{\mathbb{Z}}{7\mathbb{Z}}$$

The congruence conditions on $P \in C(\mathbb{Q})$ correspond to subsets of size 3 and 1, respectively.

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. Thus we have shown that no rational points on C exist that satisfy the congruences mod 2 and mod 3.

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. In particular, it is not necessary to know that we actually have generators of $J(\mathbb{Q})$. Since there is no explicit theory of canonical heights available for Jacobians of genus 3 curves, we would not be able to prove that we do have generators. On the other hand, we can verify that the index of the subgroup generated by the points we know is prime to a given prime number q, by considering maps $J(\mathbb{Q}) \to J(\mathbb{F}_p)$ for primes p such that $q \mid \#J(\mathbb{F}_p)$.

8. 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 $A(\mathbb{Q})$. More precisely, if at some stage in the computation, we find that the set $\Sigma(N) \subset A(\mathbb{Q})/NA(\mathbb{Q})$ of elements that are consistent with the local information coincides with the image of the known points in $V(\mathbb{Q})$, then this implies that for any unknown point $P \in V(\mathbb{Q})$, there must be a known point $Q \in V(\mathbb{Q})$ such that $P \in Q + NA(\mathbb{Q})$. Since (by assumption), $P \neq Q$, this implies that $\hat{h}(P) \gg N^2$, and so any unknown point in $V(\mathbb{Q})$ must be extremely large (if N is not very small).

In some cases, we can use Baker's Method to get a (very large) bound on the height of *integral points* on V. We can then combine this with the Mordell-Weil Sieve information to show that we know all the integral points on V. This is ongoing work of Bugeaud, Mignotte, Siksek, Stoll, and Tengely, see [BMS+]. For example, we can determine the set of integral points on the curve

$$C : y^2 - y = x^5 - x\,.$$

The Jacobian J of C has Mordell-Weil rank 3. The Mordell-Weil Sieve computation gave

$N = 444932978061474820647297268617994065251575448327430679656821404800 0,$

and after another step based on similar ideas that replaces $NJ(\mathbb{Q})$ be a sublattice of much larger index, this can be used to show that

$$\log x(P) \geq 0.95 \times 10^{2159}$$

for every unknown integral point P on C. This turned out to be much more than sufficient to contradict the upper bound, and so we can conclude that there are no unknown integral points. The complete list of integral points is therefore given by

$$(x,y) = (-1,0),\ (-1,1),\ (0,0),\ (0,1),\ (1,0),\ (1,1),\ (2,-5),\\ (2,6),\ (3,-15),\ (3,16),\ (30,-4929),\ (30,4930).$$

References

[BMS+] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely: *Integral points on hyperelliptic curves,* in preparation.

[Br04] N. Bruin: *Visualisation of Sha[2] in Abelian Surfaces,* Math. Comp. **73**, no. 247, 1459–1476 (2004).

[BF06] N. Bruin and E.V. Flynn: *Exhibiting Sha[2] on Hyperelliptic Jacobians,* Journal of Number Theory **118**, 266–291 (2006).

[BS07a] N. Bruin and M. Stoll: *Deciding existence of rational points on curves: an experiment,* to appear in Experiment. Math.

[BS07b] N. Bruin and M. Stoll: *Finding Mordell-Weil generators on genus 2 Jacobians,* in preparation.

[BS07c] N. Bruin and M. Stoll: *The Mordell-Weil sieve: Proving non-existence of rational points on curves,* in preparation.

[Fl04] E.V. Flynn: *The Hasse Principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115**, 437–466 (2004).

[Po06] B. Poonen: *Heuristics for the Brauer-Manin obstruction for curves,* Experiment. Math. **15**, 415–420 (2006).

[PSS07] B. Poonen, E.F. Schaefer, and M. Stoll: *Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$,* Duke Math. J. **137**, 103–158 (2007).

[Sc99] V. Scharaschkin: *Local-global problems and the Brauer-Manin obstruction*, Ph.D. thesis, University of Michigan (1999).
See also *The Brauer-Manin obstruction for curves*, Manuscript (1998).

[St99] M. Stoll: *On the height constant for curves of genus two*, Acta Arith. **90** (1999), 183–201.

[St01] M. Stoll: *Implementing 2-descent on Jacobians of hyperelliptic curves,* Acta Arith. **98**, 245–277 (2001).

[St02] M. Stoll: *On the height constant for curves of genus two, II*, Acta Arith. **104** (2002), 165–182.

School of Engineering and Science, Jacobs University Bremen P.O.Box 750561, 28725 Bremen, Germany.

E-mail address: m.stoll@jacobs-university.de