FINITE COVERINGS AND RATIONAL POINTS

MICHAEL STOLL

1. Introduction

Basic Question.
Given a (smooth projective) curve C over a number field k, can we determine explicitly the set $C(k)$ of rational points?

This problem splits naturally into several parts.

Problem 1.
Decide if $C(k)$ is empty or not!

Problem 2.
Knowing that $C(k)$ is nonempty, find a point $P \in C(k)$!

Problem 3.
Knowing a point $P \in C(k)$, describe $C(k)$!

Problem 2 is easily solved *in principle*: we just have to do a systematic search until we hit a point.

Problem 3 is easy for a genus 0 curve. For a genus 1 curve, which we can turn into an elliptic curve by declaring P to be the origin, it comes down to the determination of the Mordell-Weil rank (and then we have to find explicit generators, but this is again just a matter of search). For curves of higher genus, the set $C(k)$ is finite, and the main difficulty is to know when we have found all the points.

Let us first consider Problem 1.

There are some obvious approaches we can take.

- Look for a small rational point. If found, we have solved Problems 1 and 2.
- Check for local solubility. If $C(k_v)$ is empty for some place v of k, $C(k)$ is empty as well. Note that this is a finite computation.
- Use *descent*.

Date: Talk given in Oberwolfach, July 19, 2005.

Example.

Consider the genus 2 curve (over $\mathbb{Q}$)

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

We don't find a rational point on it, and it has points everywhere locally (note that $f(0) = 2$, $f(1) = -6$, $f(-2) = -3 \cdot 2^2$, $f(18)$ is a 2-adic square, and $f(4)$ is a 3-adic square). Now, by a standard procedure, for any rational point (x, y), we must have

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

(and $y = d\,uv$), where d is a squarefree integer dividing the resultant of the two factors, which is 19. So d is one of $1, -1, 19, -19$. If $d < 0$, the second equation has no solution, and if $d = 1$ or 19, the pair of equations has no solution over $\mathbb{F}_3$. (The first implies that x mod 3 is one of 0 or -1, whereas the second implies that x mod 3 is one of 1 or ∞.)

More generally, given an *unramified covering* $D \xrightarrow{\pi} C$ that is *geometrically Galois*, by standard theory, there are only finitely many *twists* $D_j \xrightarrow{\pi_j} C$ of this covering (up to isomorphism over k) such that D_j has points everywhere locally, and

$$C(k) = \coprod_j \pi_j(D_j(k))\,.$$

Moreover, the set of these twists is computable (at least in principle).

In particular, if it turns out that there are *no* such twists, then this proves that $C(k)$ is empty (like in the example above).

2. The Conjecture

Let me now state a conjecture that essentially says that this should always work. Actually, there will be two versions, a weaker and a stronger one, and they will be a little bit more general. Namely, we want them to also apply when $C(k)$ is not necessarily empty.

Let us define a *residue class* on C to be a subset of the adelic points

$$C(\mathbb{A}_k) = \prod_v C(k_v)$$

given by specifying conditions "modulo powers of v" at finitely many finite places and perhaps conditions to lie on certain connected components at some of the (real) infinite places. (I.e., a clopen subset.)

Main Conjecture (weak version).

If $X \subset C(\mathbb{A}_k)$ is a residue class such that $X \cap C(k) = \emptyset$, then there exists an unramified covering $D \xrightarrow{\pi} C$ such that for all twists $D_j \xrightarrow{\pi_j} C$, we have

$$\pi_j(D_j(\mathbb{A}_k)) \cap X = \emptyset\,.$$

In other words, we can actually *prove* that $X \cap C(k) = \emptyset$ using some unramified covering.

Main Conjecture (strong version).
Same as before, but we require the unramified covering $D \to C$ to be abelian.

Here are some consequences.

- The weak version implies that we can solve Problem 1: we search for a point by day and run through the coverings by night (they can be enumerated), until one of the two attacks is successful.
- When $C(k)$ is empty, the strong version is equivalent to saying that the Brauer-Manin obstruction is the only obstruction against rational points on C.

It is also very likely that the strong version implies that we can solve Problems 2 and 3 when the "Chabauty condition" holds for C, i.e., the Mordell-Weil rank of the Jacobian is less than the genus. If it is true that the Chabauty condition holds eventually for abelian coverings, then we can solve Problem 3 for all curves of genus at least 2.

3. Evidence

Now I want to give some evidence for these conjectures.

First a few general facts.

- The strong conjecture is true for curves of genus zero. (Use Hasse Principle and weak approximation.)
- Let C be a curve of genus 1, with Jacobian E. If C represents an element of $Ш(k, E)$ that is not divisible, then the strong conjecture is true for C. It is true for E if and only if the divisible subgroup of $Ш(k, E)$ is trivial.
- Similarly, if C is of genus ≥ 2 and Pic^1_C is a non-divisible element in $Ш(k, J)$ (where J is the Jacobian of C), then the strong conjecture holds for C. (Scharaschkin, in the context of the Brauer-Manin obstruction)
- If $C \to A$ is a nonconstant morphism into an abelian variety A such that $A(k)$ is finite and $Ш(k, A)_{\mathrm{div}} = 0$, then the strong conjecture is true for C. (Stoll, partial results by Colliot-Thélène and Siksek)
- Bjorn Poonen has heuristic arguments supporting an even stronger version of the conjecture in case $C(k)$ is empty.

From this and by other means, we get a number of concrete examples.

- The strong conjecture is true for all modular curves $X_0(N)$, $X_1(N)$ and $X(N)$ over $\mathbb{Q}$. (Use Mazur's results to show that if N is large, $X_0(N)$ maps into a modular abelian variety of analytic rank zero, plus William Stein's tables to check the remaining cases.)

- Computations have shown the strong conjecture to hold for all but 1488 genus 2 curves of the form $y^2 = f(x)$, where f has integral coefficients of absolute value at most 3, such that the curve does not have a rational point (here $k = \mathbb{Q}$). Under the assumption that $Ш(k, J)_{\text{div}} = 0$ for the Jacobian J of such a curve, the strong conjecture holds for 1383 out of these 1488 curves. Assuming in addition the Birch and Swinnerton-Dyer conjecture (plus standard conjectures on L-series), the strong conjecture holds for 42 of the remaining 105 curves. We hope to be able to deal with the other 63 curves in due course. (Bruin, Stoll)
- Successful Chabauty computations verify the strong conjecture for residue classes defined in terms of just one place v.

There are also some relative statements that allow us to conclude that some version of the conjecture holds for one curve, if we know it for one or more other curves.

- If either version of the conjecture holds for C/K, where K/k is a finite extension, and $C(K)$ is finite, then it holds for C/k. (Stoll)
- If $C(k)$ is finite and $D \to C$ is a nonconstant morphism, and either version of the conjecture holds for C, then it also holds for D. (Stoll, partial result by Colliot-Thélène)
- If $D \to C$ is an unramified covering, $C(k)$ is finite, and the weak version of the conjecture holds for all twists D_j (such that $D_j(\mathbb{A}_k)$ is nonempty), then it also holds for C. (Stoll)

This allows us to show that one of the two versions holds for a given curve in many cases.

We can also use these results to prove a statement of a somewhat different flavor.

- If the weak conjecture holds for $y^2 = x^6 + 1$ over all number fields k, then it also holds for all hyperelliptic curves of genus ≥ 2 (and many more, perhaps all curves with $g \geq 2$) over any number field. (Use results of Bogomolov-Tschinkel on coverings.)

4. More Conjectures

Let me state two more rather plausible conjectures.

"Strong Chabauty" Conjecture.
Assume that $C \to A$ is a nonconstant morphism into an abelian variety such that the image of C is not contained in a proper abelian subvariety. Also assume that $\operatorname{rank} A(k) \leq \dim A - 2$. *Then there is a set of places v of k of density* 1 *and a zero-dimensional subscheme $Z \subset C$ such that $C(k_v)$ intersects the topological closure of $J(k)$ in $J(k_v)$ only in points from Z.*

The motivation for this conjecture comes from the fact that in this situation, the system of equations for the intersection is overdetermined. Hence you do not expect solutions unless there is a good reason for them.

I suggest to do some numerical experiments with hyperelliptic genus 3 curves (with a rational Weierstrass point, say) such that the Mordell-Weil rank of the Jacobian is 1, in order to test this conjecture.

- If C satisfies assumptions and conclusion of the above conjecture, and $Ш(k, A)_{\mathrm{div}} = 0$, then the strong version of the main conjecture is true for C. (Stoll)

"Eventually Small Rank" Conjecture.
Let C be a curve of genus ≥ 2. Then there is some $n \geq 1$ such that for all twists D_j of the multiplication-by-n covering of C with $D_j(\mathbb{A}_k) \neq \emptyset$, the Jacobian of D_j has a factor A such that $\operatorname{rank} A(k) \leq \dim A - 2$.

Since the genus of the D_j grows rapidly with n, this essentially says that one does not expect Mordell-Weil ranks to be large compared to the dimension. (This conjecture (even with $\dim A - 2$ replaced by $\dim A - 1$) also implies Mordell's Conjecture.)

- Assume
  (1) $Ш(k, A)_{\mathrm{div}} = 0$ for all abelian varieties,
  (2) the "Strong Chabauty" conjecture,
  (3) the "Eventually Small Rank" conjecture.
  Then the weak version of the main conjecture holds for all curves over k, and Problem 3 can be solved.

5. Reference

See the paper on *Finite descent and rational points on curves*, available from my homepage at `http://www.faculty.iu-bremen.de/stoll/schrift.html`

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

E-mail address: `m.stoll@iu-bremen.de`