JACOBS
UNIVERSITY

How to Determine the Set of Rational Points on a Curve

Michael Stoll

Jacobs University Bremen

MEGA 2007, Strobl, June 28, 2007

The Problem

Let C be a curve defined over $\mathbb{Q}$.

(We take $\mathbb{Q}$ for simplicity; we could use an arbitrary number field instead.)

Problem.
Determine $C(\mathbb{Q})$, the set of rational points on C !

Since a curve and its smooth projective model
only differ in a computable finite set of points,
we will assume that C is smooth and projective.

The Structure of the Solution Set

The structure of the set $C(\mathbb{Q})$ is determined by the genus g of C.
("Geometry determines arithmetic")

- $g = 0$:
  Either $C(\mathbb{Q}) = \emptyset$, or if $P_0 \in C(\mathbb{Q})$, then $C \cong \mathbb{P}^1$.
  The isomorphism parametrizes $C(\mathbb{Q})$.
- $g = 1$:
  Either $C(\mathbb{Q}) = \emptyset$, or if $P_0 \in C(\mathbb{Q})$, then (C, P_0) is an elliptic curve.
  In particular, $C(\mathbb{Q})$ is a finitely generated abelian group.
  $C(\mathbb{Q})$ is described by generators of the group.
- $g \geq 2$:
  $C(\mathbb{Q})$ is finite.
  $C(\mathbb{Q})$ is given by listing the points.

Genus Zero

A smooth projective curve of genus 0
is (computably) isomorphic to a smooth conic.

Conics C satisfy the Hasse Principle :
If $C(\mathbb{Q}) = \emptyset$, then $C(\mathbb{R}) = \emptyset$ or $C(\mathbb{Q}_p) = \emptyset$ for some prime p.

We can effectively check this condition:
we only need to check $\mathbb{R}$ and $\mathbb{Q}_p$ when p divides the discriminant.
For a given p, we only need finite p-adic precision.

(Note: we need to factor the discriminant!)

At the same time, we can find a point in $C(\mathbb{Q})$, if it exists.
Given $P_0 \in C(\mathbb{Q})$, we can compute an isomorphism $\mathbb{P}^1 \to C$.

Genus One

Given a curve C of genus 1,
we can still check effectively whether C has points over $\mathbb{R}$ and over all $\mathbb{Q}_p$.

However, the Hasse Principle may fail.

If we can't find a rational point, but C has points "everywhere locally",
we can try coverings.

Over $\bar{\mathbb{Q}}$, C is isomorphic to an elliptic curve E.
We consider coverings $D \to C$ that over $\bar{\mathbb{Q}}$ are isomorphic to $E \xrightarrow{\cdot n} E$.

Up to $\mathbb{Q}$-isomorphism, there are only finitely many such n-coverings
such that D has points everywhere locally.
If this finite set is empty, then $C(\mathbb{Q}) = \emptyset$.

Genus One — Coverings

If C has a rational point P,
it will lift to one of the n-coverings D,
where it should be “smaller”, hence can be found more easily.

In general, we can repeat the procedure with the covering curves D.

If the Shafarevich-Tate group of the Jacobian elliptic curve E is “nice” (e.g., finite — this is a conjecture), then eventually, we will be successful.

In practice, this is feasible only in a few cases:

- $y^2 =$ quartic in x and $n = 2$;
- intersections of two quadrics in $\mathbb{P}^3$ and $n = 2$;
- plane cubics and $n = 3$ (current PhD project).

Elliptic Curves

Now assume that we have found a rational point P_0 on C.
Then (C, P_0) is an elliptic curve, which we will denote E.

We know that $E(\mathbb{Q})$ is a finitely generated abelian group;
the task is now to find explicit generators.

The hard part is to determine the rank $r = \dim_{\mathbb{Q}} E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

$E(\mathbb{Q})/nE(\mathbb{Q})$ injects into the set of n-coverings of E
with points everywhere locally.
This gives us upper bounds on r.

The bound may fail to be sharp:
the obstruction comes from the Shafarevich-Tate group of E.

Elliptic Curves — Finding Points

To get lower bounds on r, we can search for points on E.

However, generators may be very large and cannot be found by search.

We can use the coverings to find rational points on E:
every point in $E(\mathbb{Q})$ lifts to an n-covering, where it is much smaller.

To make use of this idea,
we need explicit and nice models of the covering curves.

There is some interesting algebraic geometry behind these methods, see
J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll:
Explicit n-descent on elliptic curves.

This "n-descent" is feasible for $n = 2, 3, 4, 8$; $n = 9$ is current work.

Higher Genus — Finding Points

Now consider a curve C of genus $g \geq 2$.

The first task is to decide whether C has any rational points.

If there is a rational point, we can find it by search.
Unlike the genus 1 case, there seems to be a reasonably small point.

Example (Bruin-St).
Consider $\quad C : y^2 = f_6 x^6 + \cdots + f_1 x + f_0 \quad$ of genus 2
such that $f_j \in \{-3, -2, \ldots, 3\}$.

If C has rational points,
then there is one whose x-coordinate is p/q with $|p|, |q| \leq 1519$.

Higher Genus — Local Points

If we don't find a rational point on C,
we can again check for local points (over $\mathbb{R}$ and $\mathbb{Q}_p$).

Example (Poonen-St).
We expect about 85 % of all curves of genus 2
to have points everywhere locally.

So in many cases, this will not suffice to prove that $C(\mathbb{Q}) = \emptyset$.

Example (Bruin-St).
Among the 196 171 isomorphism classes of "small" genus 2 curves,
there are 29 278 that are counterexamples to the Hasse Principle.

Coverings Again

To resolve these cases, we can again use coverings.

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 an unramified $\mathbb{Z}/2\mathbb{Z}$-covering of C.

Its twists are $D_d : d\,u^2 = g(x),\ d\,v^2 = h(x)$, $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Every rational point on C lifts to one of the twists,
and there are only finitely many twists
such that D_d has points everywhere locally.

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 there are no relevant twists, and $C(\mathbb{Q}) = \emptyset$.

Descent

More generally, we have the following result.

Descent Theorem.
Let $D \xrightarrow{\pi} C$ be an unramified and geometrically Galois covering.
Its twists $D_\xi \xrightarrow{\pi_\xi} C$ are parametrized by $\xi \in H^1(\mathbb{Q}, G)$
(a Galois cohomology set), where G is the Galois group of the covering.

We then have the following:

- $C(\mathbb{Q}) = \bigcup\limits_{\xi \in H^1(\mathbb{Q},G)} \pi_\xi\Big(D_\xi(\mathbb{Q})\Big)$.
- $\text{Sel}^\pi(C) := \Big\{\xi \in H^1(\mathbb{Q}, G) : D_\xi \text{ has points everywhere locally}\Big\}$
  is finite (and computable). This is the Selmer set of C w.r.t. π.

(Fermat, Chevalley-Weil, . . .)

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

Abelian Coverings

A covering $D \to C$ is abelian if its Galois group is abelian.

Let J be the Jacobian variety of C.
Assume for simplicity that there is an embedding $\iota : C \to J$.

Then all abelian coverings of C are obtained from n-coverings of J:

$$\begin{tikzcd}
D \arrow[r] \arrow[d, "\pi"'] & X \arrow[r, dashed, "\cong/\bar{\mathbb{Q}}"] \arrow[d] & J \arrow[dl, "\cdot n"] \\
C \arrow[r, "\iota"] & J &
\end{tikzcd}$$

We call such a covering an n-covering of C;
the set of all n-coverings with points everywhere locally
is denoted $\mathrm{Sel}^{(n)}(C)$.

Practice — Descent

It is feasible to compute $\mathrm{Sel}^{(2)}(C)$ for hyperelliptic curves C (Bruin-St).

This is a generalization of the $y^2 = g(x)h(x)$ example,
where all possible factorizations are considered simultaneously.

Example (Bruin-St).
Among the “small” genus 2 curves, there are only 1 492 curves C without rational points and such that $\mathrm{Sel}^{(2)}(C) \neq \emptyset$.

Example (Bruin-St).
It appears that for large coefficients, there is a fraction of 7–8 % of all genus 2 curves C such that $\mathrm{Sel}^{(2)}(C)$ is non-empty, but C has no rational points.

A Conjecture

These encouraging results motivate the following.

Conjecture 1.
If $C(\mathbb{Q}) = \emptyset$, then Sel$^{(n)}(C) = \emptyset$ for some $n \geq 1$.

Remarks.

- In principle, Sel$^{(n)}(C)$ is computable for every n.
  Hence, the conjecture implies that "$C(\mathbb{Q}) = \emptyset$?" is decidable.
  (Search for points by day, compute Sel$^{(n)}(C)$ by night.)
- (For the experts:)
  The conjecture implies that the Brauer-Manin obstruction is the only obstruction against rational points on curves.

An Improvement

Assume we know generators of the Mordell-Weil group $J(\mathbb{Q})$ (a finitely generated abelian group again).
Then we can restrict to n-coverings of J that have rational points.

They are of the form $J \ni P \mapsto nP + Q \in J$, with $Q \in J(\mathbb{Q})$;
the shift Q is only determined modulo $nJ(\mathbb{Q})$.

The set we are interested in is

$$\Big\{Q + nJ(\mathbb{Q}) : (Q + nJ(\mathbb{Q})) \cap \iota(C) \neq \emptyset\Big\} \subset J(\mathbb{Q})/nJ(\mathbb{Q})\,.$$

We approximate the condition by testing it modulo p for a set of primes p.

The Mordell-Weil Sieve

Let S be a finite set of primes of good reduction for C.

Consider the following diagram.

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

We can compute the maps α and β.

If their images do not intersect, then $C(\mathbb{Q}) = \emptyset$.

(Scharaschkin, Flynn, Bruin-St)

Poonen Heuristic/Conjecture:

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

Practice — Generators

We can try to find generators of $J(\mathbb{Q})$ by descent again.
This is feasible for hyperelliptic curves when $n = 2$.
Large generators can be a problem, however.

Example (Bruin-St).
For $\quad C : y^2 = -3\,x^6 + x^5 - 2\,x^4 - 2\,x^2 + 2\,x + 3$,
$J(\mathbb{Q})$ is infinite cyclic, generated by $[P_1 + P_2 - W]$,
where the x-coordinates of P_1 and P_2 are the roots of

$$x^2 + \tfrac{37482925498065820078878366248457300623}{34011049811816647384141492487717524243}\,x + \tfrac{581452628280824306698926561618393967033}{544176796989066358146263879803480387888}\,,$$

and W is a canonical divisor.

The canonical logarithmic height of this generator is 95.26287.

Practice — Mordell-Weil Sieve

A carefully optimized version of the Mordell-Weil sieve
works well when $r = \operatorname{rank} J(\mathbb{Q}) \le 3$ and perhaps also for $r = 4$.
For larger ranks, combinatorial explosion is a major problem.

Example (Bruin-St).
For all the 1 492 remaining "small" genus 2 curves C,
a Mordell-Weil sieve computation proves $C(\mathbb{Q}) = \emptyset$.
(For 42 curves,
we need to assume the Birch and Swinnerton-Dyer Conjecture.)

A Refinement

Taking n as a multiple of N,
the Mordell-Weil sieve gives us a way of proving
that a given coset of $NJ(\mathbb{Q})$ does not meet $\iota(C)$.

Conjecture 2.
If $(Q + NJ(\mathbb{Q})) \cap \iota(C) = \emptyset$, then there are $n \in N\mathbb{Z}$ and S such that the Mordell-Weil sieve with these parameters proves this fact.

So if we can find an N that separates the rational points on C,
i.e., such that the composition $C(\mathbb{Q}) \xrightarrow{\iota} J(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective,
then we can effectively determine $C(\mathbb{Q})$ if Conjecture 2 holds for C:

For each coset of $NJ(\mathbb{Q})$, we either find a point on C mapping into it,
or we prove that there is no such point.

Chabauty's Method

Chabauty's method allows us to compute a separating N when the rank r of $J(\mathbb{Q})$ is less than the genus g of C.

Let p be a prime of good reduction for C. There is a pairing

$$\Omega^1_J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p\,, \qquad (\omega, R) \longmapsto \int_0^R \omega = \langle \omega, \log R \rangle\,.$$

Since $\operatorname{rank} J(\mathbb{Q}) = r < g = \dim_{\mathbb{Q}_p} \Omega^1_J(\mathbb{Q}_p)$, there is a differential $0 \neq \omega_p \in \Omega_C(\mathbb{Q}_p) \cong \Omega^1_J(\mathbb{Q}_p)$ that kills $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$.

Theorem.
If the reduction $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$ and $p > 2$, then each residue class mod p contains at most one rational point.

This implies that $N = \#J(\mathbb{F}_p)$ is separating.

Practice — Chabauty + MW Sieve

When $g = 2$ and $r = 1$, we can easily compute $\bar{\omega}_p$.

Heuristically (at least if J is simple),
we expect to find many p satisfying the condition.

In practice, such p are easily found;
the Mordell-Weil sieve computation then determines $C(\mathbb{Q})$ very quickly.

Summary

- The case $g = 0$ is solved completely.
- For $g = 1$, we have a good (though not complete) theoretical understanding.

  The theoretical obstacle lies in the Shafarevich-Tate group.

  We can do quite something in practice;
  the obstacle against progress lies in number theoretical computations.
- For $g = 2$, we can already do many things.

  We can verify that $C(\mathbb{Q}) = \emptyset$ in many cases.

  If we can find generators of $J(\mathbb{Q})$, we can apply the Mordell-Weil sieve and deal with more cases.
  If $r \leq 1$, we can even determine $C(\mathbb{Q})$ in practice.
- For $g \geq 3$, we cannot do much yet.