Rational Points on Curves

Michael Stoll
Universität Bayreuth

Journées Arithmétiques, Saint-Étienne
July 9, 2009
The Problem

Let $C$ be a (geometrically integral) 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 focus of this talk is on the practical aspects, in the case of genus $\geq 2$. 
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.
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 \( \mathbb{P}^1 \rightarrow C \).
Genus One

The Hasse Principle may fail.

If we can’t find a rational point, but \( C \) has points “everywhere locally”, we can try \((n-)\)coverings.

Coverings can be used to show that \( C(\mathbb{Q}) \) is empty, or they can help find a point \( P_0 \in C(\mathbb{Q}) \).

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

- \( y^2 = \text{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 $r = \dim_{\mathbb{Q}} E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Computation of the $n$-Selmer group of $E$ gives an upper bound on $r$. This $n$-descent is feasible for $n = 2, 3, 4, 8$; $n = 9$ is current work.

A search for independent points gives a lower bound on $r$. However, generators may be very large. Descent can help find them. When $r = 1$, Heegner points can be used.
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, we expect points to be small:

**Conjecture** (A consequence of Vojta’s Conjecture: Su-Ion Ih). If $C \to B$ is a family of higher-genus curves, then there is $\kappa$ such that

$$H_C(P) \ll H_B(b)^\kappa$$

for all $P \in C_b(\mathbb{Q})$ if the the fiber $C_b$ is smooth.
Examples

Consider a curve

\[ C : y^2 = f_6x^6 + \cdots + f_1x + f_0 \]

of genus 2, with \( f_j \in \mathbb{Z} \).

Then the conjecture says that there are \( \gamma \) and \( \kappa \) such that the \( x \)-coordinate \( p/q \) of any point \( P \in C(\mathbb{Q}) \) satisfies

\[ |p|, |q| \leq \gamma \max\{|f_0|, |f_1|, \ldots, |f_6|\}^\kappa. \]

Example (Bruin-St).
Consider curves of genus 2 as above 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 \( |p|, |q| \leq 1519 \).

We will call these curves small genus 2 curves.
Local Points

If we do not find a rational point on $C$, we can check for local points (over $\mathbb{R}$ and $\mathbb{Q}_p$). We have to consider primes $p$ that are small or sufficiently bad.

Example (Poonen-St).
About 84–85% of all curves of genus 2 have points everywhere locally.

Conjecture.
0% of all curves of genus 2 have rational points.

So in many cases, checking for local points 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.
To resolve these cases, we can use coverings.

**Example.**
Consider \( C : y^2 = g(x)h(x) \) with \( \deg g, \deg h \) not both odd.

Then \( D : u^2 = g(x), v^2 = h(x) \)
is an unramified \( \mathbb{Z}/2\mathbb{Z} \)-covering of \( C \).

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

Every rational point on \( C \) lifts to one of the twists,
and there are only finitely many twists
such that \( D_d \) 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 among
\[ du^2 = -x^2 - x + 1, \quad dv^2 = x^4 + x^3 + x^2 + x + 2 \]
where \( d \) is one of 1, -1, 19, -19. (The resultant is 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 (Fermat, Chevalley-Weil, . . . ).**

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:

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

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

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

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

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

We call such a covering an $n$-covering of $C$; the set of all $n$-coverings with points everywhere locally is denoted $\text{Sel}^{(n)}(C')$. 
It is feasible to compute $\text{Sel}^{(2)}(C)$ 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 1492 curves $C$ without rational points and such that $\text{Sel}^{(2)}(C) \neq \emptyset$. 
Conjecture 1.
If \( C(\mathbb{Q}) = \emptyset \), then \( \text{Sel}^{(n)}(C) = \emptyset \) for some \( n \geq 1 \).

Remarks.

- In principle, \( \text{Sel}^{(n)}(C) \) is computable for every \( n \).
  The conjecture therefore implies that “\( C(\mathbb{Q}) = \emptyset ? \)” is decidable.
  (Search for points by day, compute \( \text{Sel}^{(n)}(C) \) by night.)
- The conjecture implies that the Brauer-Manin obstruction is the only obstruction against rational points on curves.
  (In fact, it is equivalent to this statement.)
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 $J 
i P \mapsto nP + Q \in J$, with $Q \in J(\mathbb{Q})$; the shift $Q$ is only determined modulo $nJ(\mathbb{Q})$.

The set we are interested in is therefore

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

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.

$$
\begin{array}{ccc}
C(\mathbb{Q}) & \xrightarrow{\iota} & J(\mathbb{Q}) \\
\downarrow & & \downarrow \\
\prod_{p \in S} C(F_p) & \xrightarrow{\iota} & \prod_{p \in S} J(F_p) \\
\alpha & & \beta \\
\prod_{p \in S} J(F_p) & \xrightarrow{\iota} & \prod_{p \in S} J(F_p) / nJ(F_p) \\
\end{array}
$$

We can compute the maps $\alpha$ and $\beta$. 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.
A carefully optimized version of the Mordell-Weil sieve works well when $r = \text{rank } J(\mathbb{Q})$ is not too large.

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

**Note:** It suffices to have generators of a subgroup of $J(\mathbb{Q})$ of finite index prime to $n$.
This is easier to obtain than a full generating set, which is currently possible only for genus 2.
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 $(\mathbb{Q} + NJ(\mathbb{Q})) \cap \iota(C) = \emptyset$, then there are $n \in NZ$ 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 $C(\mathbb{Q}) \xrightarrow{l} J(\mathbb{Q}) \rightarrow J(\mathbb{Q})/NJ(\mathbb{Q})$ 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

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

Since 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.
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.

**Example (Bruin-St).**
For the 46 436 small genus 2 curves with rational points and $r = 1$, we determined $C(\mathbb{Q})$. The computation takes about 8–9 hours.
When \( r \geq g \), we can still use the Mordell-Weil Sieve to show that we know all rational points up to very large height.

For smaller height bounds, we can also use lattice point enumeration.

**Example (Bruin-St).**
Unless there are points of height \( > 10^{100} \), the largest point on a small genus 2 curve has height 209 040.

**Note.**
For these applications, we need to know generators of the full Mordell-Weil group. Therefore, this is currently restricted to genus 2.
Integral Points

If \( C \) is hyperelliptic, we can compute bounds for integral points using Baker's method.

These bounds are of a flavor like \( |x| < 10^{10^{600}} \).

If we know generators of \( J(\mathbb{Q}) \), we can use the Mordell-Weil Sieve to prove that there are no unknown rational points below that bound. This allows us to determine the set of integral points on \( C \).

Example (Bugeaud-Mignotte-Siksek-St-Tengely).
The integral solutions to
\[
\binom{y}{2} = \binom{x}{5}
\]
have \( x \in \{0, 1, 2, 3, 4, 5, 6, 7, 15, 19\} \).
Genus Larger Than 2

The main practical obstacle is the determination of \( J(\mathbb{Q}) \):

- **Descent** is only possible in special cases.
- There is no explicit theory of heights.

**Example (Poonen-Schaefer-St).**
In the course of solving \( x^2 + y^3 = z^7 \), one has to determine the set of rational points on certain **twists of the Klein Quartic**. Descent on \( J \) is possible here; Chabauty+MWS is successful.

**Example (St).**
The curve \( X^\text{dyn}_0(6) \) classifying 6-cycles under \( x \mapsto x^2 + c \) has genus 4. Assuming BSD for its Jacobian, we can show that \( r = 3 \); Chabauty's method then allows to **determine** \( X^\text{dyn}_0(6)(\mathbb{Q}) \).