Rational Points on Curves in Practice

Michael Stoll
Universität Bayreuth

Journées Algophantiennes Bordelaises

Université de Bordeaux

June 8, 2017

The Problem

Let C be a smooth projective and geometrically irreducible curve over $\mathbb{Q}$ of genus $g \geq 2$, given by explicit equations.

Example.

$$C_1 : x^2(x+1)y^3 - (5x^2+x+1)y^2 - x(x^2-2x-7)y + (x+1)(x-3) = 0$$

considered as a curve of type $(3,3)$ in $\mathbb{P}^1 \times \mathbb{P}^1$, with $g = 4$.

By Faltings' Theorem, the set $C(\mathbb{Q})$ of rational points on C is finite.

Problem.

Determine $C(\mathbb{Q})$ explicitly!

Example.

$$C_1(\mathbb{Q}) = \{(\infty,-1),(\infty,0),(\infty,1),(-1,\infty),(-1,-\tfrac{4}{5}),(-1,0),(0,\infty),(1,2),(2,1),(3,0)\}$$

General Strategy

Search for rational points on $C \rightsquigarrow C(\mathbb{Q})_{\text{known}}$

[We expect that $C(\mathbb{Q})_{\text{known}} = C(\mathbb{Q})$, so we try to prove that]

if $C(\mathbb{Q})_{\text{known}} = \emptyset$ **then**

Try to show that $C(\mathbb{Q}) = \emptyset$

else

Let J be the Jacobian of C

Let $P_0 \in C(\mathbb{Q})_{\text{known}} \rightsquigarrow i\colon C \hookrightarrow J,\ P \mapsto [P - P_0]$

Determine $r = \operatorname{rk} J(\mathbb{Q})$ and find r independent points in $J(\mathbb{Q})$

if $r < g$ **then**

Apply Chabauty and Mordell-Weil Sieve $\rightsquigarrow C(\mathbb{Q}) = C(\mathbb{Q})_{\text{known}}$

else

Try something else (or give up)

end if

end if

Showing that $C(\mathbb{Q}) = \emptyset$

- Test for local points: $C(\mathbb{R}) = \emptyset$? $\exists p$: $C(\mathbb{Q}_p) = \emptyset$?

- Descent: Find étale and geometrically Galois morphism $\pi\colon D \to C$ and show that $\mathrm{Sel}^{\pi}(C) = \emptyset$.

Example.
$C\colon y^2 = -(x^2 + x - 1)(x^4 + x^3 + x^2 + x + 2)$ has points everywhere locally.
$\exists \mathbb{Z}/2\mathbb{Z}$-covering $\pi\colon D_1 \to C$ with twists D_d: $\begin{cases} du^2 = -x^2 - x + 1 \\ dv^2 = x^4 + x^3 + x^2 + x + 2 \end{cases}$
$\mathrm{Sel}^{\pi}(C) = \{d \in \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2 : D_d(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset\} = \emptyset$ $\quad (\subset \{1, 19, -1, -19\}$, use $3, \infty)$

- Mordell-Weil Sieve (see later in this talk)
  (Need r independent points in $J(\mathbb{Q})$, embedding $C \hookrightarrow J$)

Using the Jacobian

Knowing a point $P_0 \in C(\mathbb{Q})$, we obtain an embedding $\iota\colon C \hookrightarrow J$.
Then $C(\mathbb{Q}) = \iota^{-1}(J(\mathbb{Q}))$.

By (Mordell-)Weil, $J(\mathbb{Q})$ is a finitely generated abelian group,
so $J(\mathbb{Q}) \simeq J(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ with $r = \operatorname{rk} J(\mathbb{Q}) \in \mathbb{Z}_{\geq 0}$.

We need r independent points in $J(\mathbb{Q})$ (generating a finite-index subgroup).

- Upper bound for r: Selmer group or BSD.
  - Selmer group: curves with extra structure (e.g., hyperelliptic) needs class group/unit info for number fields (use GRH)
  - BSD: reasonably small conductor needs standard conjectures for L-series plus BSD
- Lower bound for r: search for points (and find them!)
  - Points can be large; high-dimensional search space for large g
  - Selmer bound may fail to be tight

Chabauty

We assume that $r < g$ and that $(J(\mathbb{Q}) : \langle G_1, \ldots, G_r \rangle) < \infty$.

Fix a (good) prime p. There is a pairing

$$J(\mathbb{Q}_p) \times \Omega^1(C_{\mathbb{Q}_p}) \longrightarrow \mathbb{Q}_p, \qquad \Bigl(\sum_i [P_i - P_0], \omega\Bigr) \longmapsto \sum_i \int_{P_0}^{P_i} \omega$$

Let $V \subset \Omega^1(C_{\mathbb{Q}_p})$ be the annihilator of $J(\mathbb{Q})$ under this pairing.
By assumption $\dim V \geq g - r > 0$. Let $0 \neq \omega \in V$. Then

$$\lambda(P) = \int_{P_0}^{P} \omega = 0 \qquad \text{for all } P \in C(\mathbb{Q}).$$

If $p \geq 3$ and $\bar{\omega}$ does not vanish on $C(\mathbb{F}_p)$, then $C(\mathbb{Q}) \hookrightarrow C(\mathbb{F}_p)$.

- Heuristically, there are many p satisfying this condition.
- Given $G_1, \ldots, G_r$, we can find all $\bar{\omega}$ such that ω kills $J(\mathbb{Q})$.

Example

$$C_1\colon x^2(x+1)y^3 - (5x^2+x+1)y^2 - x(x^2-2x-7)y + (x+1)(x-3) = 0$$

$$C_1(\mathbb{Q})_{\text{known}} = \{(\infty,-1),(\infty,0),(\infty,1),(-1,\infty),(-1,-\tfrac{4}{5}),\\ (-1,0),(0,\infty),(1,2),(2,1),(3,0)\}$$

$\operatorname{rk} J_1(\mathbb{Q}) = 3$ (using BSD),
$G_1 = [(\infty,0)-(-1,0)]$, $G_2 = [(3,0)-(-1,0)]$, $G_3 = [(2,1)-(-1,0)]$.
We take $p = 5$. Then $\bar{\omega}$ has divisor given by $x = 0$ or $y = \infty$.
Let $\rho\colon C_1(\mathbb{Q}) \to C_1(\mathbb{F}_5)$ be the reduction map; we have $\#C_1(\mathbb{F}_5) = 9$.
Away from $(0,\infty),(-1,\infty) \in C_1(\mathbb{F}_5)$, we get that $\#\rho^{-1}(P) \leq 1$.
A closer study shows that $\#\rho^{-1}((0,\infty)) = 1$ and $\#\rho^{-1}((-1,\infty)) = 2$.
This accounts for all points in $C_1(\mathbb{Q})_{\text{known}}$, so $C_1(\mathbb{Q}) = C_1(\mathbb{Q})_{\text{known}}$.

Mordell-Weil Sieve

If Chabauty was successful, then we have an injection $C(\mathbb{Q}) \hookrightarrow C(\mathbb{F}_p)$.
However, usually this will not be surjective.
So we need a way of proving that certain residue classes do not contain rational points.

Idea: Use information coming from other primes.

Let S ($\ni p$) be a finite set of good primes and $N \in \mathbb{Z}_{>1}$.

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow \rho \\ \prod_{q \in S} C(\mathbb{F}_q) & \xrightarrow{j} & \prod_{q \in S} J(\mathbb{F}_q)/NJ(\mathbb{F}_q) \end{array}$$

Let $P \in C(\mathbb{F}_p)$. If $j\left(\{P\} \times \prod_{q \in S \setminus \{p\}} C(\mathbb{F}_q)\right) \cap \mathrm{im}(\rho) = \emptyset$,

then no rational point reduces to P.

Mordell-Weil Sieve (continued)

- If N is coprime with the index $(J(\mathbb{Q}) : J(\mathbb{Q})_{\text{known}})$ (checkable), then $J(\mathbb{Q})/NJ(\mathbb{Q}) \simeq J(\mathbb{Q})_{\text{known}}/NJ(\mathbb{Q})_{\text{known}}$.
- We need $\#J(\mathbb{F}_p)$, N and the $\#J(\mathbb{F}_q)$ to have common factors.
- When r is not very small, we have to be careful to avoid combinatorial explosion.
- We can include information from bad primes and/or mod q^n information.

Example.

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

(with $r = g = 3$) has no rational points P
with $P \equiv (1:0:0)$ or $(1:1:1)$ mod 2 and $P \equiv (0:1:0)$ mod 3.
This uses MWS with $S = \{2, 3, 13, 23, 97\}$.

What Can Go Wrong?

There are several points where the approach sketched earlier may fail.

(1) We are unable to get an upper bound on the rank r.
Reasons: Selmer group computation infeasible and conductor too large.
Alternatives: Covering collections; Elliptic Curve Chabauty.

(2) We find too few independent points on J to match the upper bound.
Reasons: Upper bound not tight or points too large.
Alternatives: Improve upper bound; Selmer Group Chabauty; as for (1).

(3) $r \geq g$.
Reason: This is a fact of life.
Alternatives: Quadratic Chabauty (see next two talks); as for (1).

Covering Collections

Observation: if $\exists$ dominant morphism $f\colon C \to D$ over a number field K and we can determine a finite subset $S \subset D(K)$ with $f(C(\mathbb{Q})) \subset S$, then we can determine $C(\mathbb{Q})$.

A converse: if $\pi\colon D \to C$ over $\mathbb{Q}$ is étale and geometrically Galois, then $C(\mathbb{Q}) = \coprod_{\xi \in \mathrm{Sel}^{\pi}(C)} \pi_\xi(D_\xi(\mathbb{Q}))$, where $\pi_\xi\colon D_\xi \to C$ is a twist of π and the π-Selmer set $\mathrm{Sel}^{\pi}(C)$ is finite.

So we can "reduce" the determination of $C(\mathbb{Q})$
to the determination of $D_\xi(\mathbb{Q})$ for all $\xi \in \mathrm{Sel}^{\pi}(C)$.

The curves D_ξ are "more complicated" than C,
but they frequently allow maps to "simpler" curves (e.g., elliptic curves).

Elliptic Curve Chabauty

This applies in the following situation,
which often occurs in the context of covering curves.

$\exists$ dominant morphism $f\colon C \to E$ to an elliptic curve over a number field K
and $\exists$ morphism $h\colon E \to \mathbb{P}^1$ over K such that $h \circ f$ is defined over $\mathbb{Q}$.

Then $f(C(\mathbb{Q})) \subset \{P \in E(K) : h(P) \in \mathbb{P}^1(\mathbb{Q})\}$.

If $\operatorname{rk} E(K) < [K : \mathbb{Q}]$ (and f is not obtained by base-change from a smaller field),
then we can apply Chabauty to the image of C in $R_{K/\mathbb{Q}}E$.

Example.
Consider a hyperelliptic curve $C\colon y^2 = f(x)$ with $\deg f$ odd (even).
Assume that over K, $f(x) = h_1(x)h_2(x)$ with $\deg h_1 = 3$ $(= 4)$.
Then there is a computable finite set $S \subset K^\times$ such that
each $P \in C(\mathbb{Q})$ satisfies $\delta h_1(x(P)) = u^2$ for some $\delta \in S$ and some $u \in K$.

Selmer Group Chabauty

If we can compute a Selmer group of J resulting in a bound $r < g$, but we are unable to find enough independent points in $J(\mathbb{Q})$, then Selmer Group Chabauty might save us.

The idea is to use the Selmer group as a proxy for (a quotient of) $J(\mathbb{Q})$. We have to work p-adically, where p is the exponent of the Selmer group (usually a bad prime), and we need some luck.

Example.
Let p be an odd prime and consider $C_p \colon 5y^2 = 4x^p + 1$.
Then $C_p(\mathbb{Q}) = \{\infty, (1,1), (1,-1)\}$ for $7 \le p \le 53$ (under GRH for $p \ge 23$).
By work of Dahmen and Siksek, this implies that the Generalized Fermat Equation $x^5 + y^5 = z^p$ has no unexpected primitive integral solutions.

Thank You!