UNIVERSITÄT
BAYREUTH

Determining the rational points on a curve of genus 2 and Mordell-Weil rank 1

Michael Stoll
Universität Bayreuth

ChaBONNty Conference
Max-Planck-Institut für Mathematik, Bonn
June 29, 2026

The Task

Let C be a curve of genus 2 over $\mathbb{Q}$ with Jacobian variety J
and assume that $J(\mathbb{Q})$ has rank 1
and that we know a point $P \in J(\mathbb{Q})$ of infinite order.

The set $C(\mathbb{Q})$ of rational points on C is finite (Chabauty 1941).

Task.
Determine $C(\mathbb{Q})$!

Note: The input consists of

- a squarefree polynomial $f \in \mathbb{Q}[x]$ of degree 5 or 6 giving C
- a pair of polynomials $a, b \in \mathbb{Q}[x]$ specifying P

Outline of the Algorithm

❶ Check if C has points everywhere locally.
If not, return $\emptyset$.

❷ Check if C has rational divisors of odd degree.
If so, let D be an effective rational divisor of degree 1 or 3.
Otherwise, return $\emptyset$.

❸ Embed C into J using D
and run a Mordell-Weil sieve + Chabauty computation.
This will determine $C(\mathbb{Q})$ if it terminates.

The last step will terminate when some plausible conjectures hold for C.
In practice it always terminates and finishes within a few seconds.

What is New?

❶ An implementation of an efficient check
for points everywhere locally on hyperelliptic curves.
(Not the focus of this talk.)

❷ The check for rational divisors of odd degree.
(For time reasons, only sketched in this talk.)

❸ Dealing with the case that J is split
in the Mordell-Weil sieve + Chabauty computation.

Rational Divisors of Odd Degree (Sketch)

We assume that C has genus 2 and
that we know generators of a subgroup $G_0 \subset J(\mathbb{Q})$ of finite index.

❶ Let $G = \left\{ P \in J(\mathbb{Q}) \;\middle|\; \exists n \colon 2^n P \in G_0 \right\}$ be the 2-saturation of G_0.
Then $G/2G \to J(\mathbb{Q})/2J(\mathbb{Q})$ is an isomorphism.

❷ For each coset in $G/2G$:

- Let $P \in G$ be a representative.
- Check if $P \in \operatorname{im}\left(\operatorname{Pic}^1_C(\mathbb{Q}) \to J(\mathbb{Q})\right)$.
- If yes, check if a preimage of P is represented by a rational divisor.
  - If yes, return ‘true’ and such a divisor.
  - If no, return ‘false’.
- If no, continue with the next coset.

❸ Return ‘false’.

Mordell-Weil Sieve

Idea:

Pick a smooth number N and a finite set S of good primes.

Let $i\colon C \hookrightarrow J$ be an embedding defined over $\mathbb{Q}$

(This needs a rational divisor (class) of odd degree).

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{\quad i \quad} & J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \rho \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{i} & \prod_{p\in S} J(\mathbb{F}_p) & \longrightarrow & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p) \end{array}$$

$$\phi\big(C(\mathbb{Q})\big) \subset \rho^{-1}\big(\mathrm{im}(\psi)\big) \subset J(\mathbb{Q})/NJ(\mathbb{Q})$$

Mordell-Weil Sieve

$$\phi\big(C(\mathbb{Q})\big) \subset \rho^{-1}\big(\mathrm{im}(\psi)\big) \subset J(\mathbb{Q})/NJ(\mathbb{Q})$$

Conjecture.
For large enough N and S, we have equality.

- We can compute $\rho^{-1}\big(\mathrm{im}(\psi)\big)$.
- We can certify equality by finding a point in each fiber.
  If unsuccessful, increase N and S and repeat.
- If in addition ϕ is injective, this determines $C(\mathbb{Q})$!

So how can we make sure that ϕ is injective?

(Since $C(\mathbb{Q})$ is finite, ϕ must be injective for N large,
but we need an explicit condition that we can check.)

Chabauty

Since we assume that $J(\mathbb{Q})$ has rank 1,
for every good prime p there exists a regular differential $0 \neq \omega_p \in \Omega^1_{C/\mathbb{Q}_p}$ such that

$$\int_P^Q \omega_p = 0 \qquad \text{for all } P, Q \in C(\mathbb{Q}).$$

After scaling and reducing mod p, we obtain $0 \neq \bar{\omega}_p \in \Omega^1_{C/\mathbb{F}_p}$.

Fact.
Assume $p > 2$.
If $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$, then $C(\mathbb{Q}) \to C(\mathbb{F}_p)$ is injective.
This implies that $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective when $N \cdot J(\mathbb{F}_p) = 0$.

So we need to find at least one such prime!

Split Jacobians

Conjecture.
There are infinitely many primes p such that $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$,
unless J splits up to isogeny as a product of two elliptic curves
and the global "annihilating differential" $\omega \in \Omega^1_{C/\mathbb{Q}}$
vanishes at a rational point $Q = (\xi : \eta : \zeta)$.

Lemma.
In this exceptional case,
$C(\mathbb{Q}) \to C(\mathbb{F}_p)$ is injective for all good $p > 3$ if $\eta = 0$,
and for all good $p > 3$ such that $p \nmid \eta$ otherwise.

So we win again!

But: We need to verify the conditions:
J splits and ω vanishes at a rational point.

J Splits

Working with the analytic parametrization $J(\mathbb{C}) \cong \mathbb{C}^2/\Lambda$,
we can obtain a fairly reliable guess for the endomorphism ring $\mathrm{End}_{\mathbb{Q}}(J)$.
This allows us to detect if J splits
and also to obtain the degree d
of the associated coverings $C \to E$, $C \to E'$.

We still need to certify the splitting
and to determine the global annihilating differential ω
(so that we can check whether it vanishes at a rational point).

Certification

We verify that J splits
by explicitly exhibiting an elliptic curve E contained in J.

For practical reasons, we work on the Kummer surface $K \subset \mathbb{P}^3$.

The image of E on K is a (smooth) rational curve of degree d
passing through exactly four nodes.
One of the elliptic curves in J contains infinitely many rational points.

For a point $P \in J(\mathbb{Q})$ of infinite order
we try to interpolate the multiples of P.
If we find the right kind of curve for some P,
the splitting of J is certified and we can also determine ω.

Thank You!

Rational Divisors of Odd Degree

❶ Check if $P \in \mathrm{im}\big(\mathrm{Pic}^1_C(\mathbb{Q}) \to J(\mathbb{Q})\big)$:
- Check if the image of P on the Kummer surface of J is in the image of the twisted duplication map from the dual Kummer surface.
- Check for any preimage on the dual Kummer surface whether it lifts to $\mathrm{Pic}^1_C(\mathbb{Q})$.

❷ Check if a preimage of P is represented by a rational divisor:
- This reduces to solving a conic over $\mathbb{Q}$.

Note:
- The image of $\mathrm{Pic}^1_C(\mathbb{Q})$ under $[D] \mapsto 2[D] - K$ is empty or a coset of $2J(\mathbb{Q})$.
- If one point in $\mathrm{Pic}^1_C(\mathbb{Q})$ is represented by a rational divisor, then all points in $\mathrm{Pic}^1_C(\mathbb{Q})$ are.
- If $C(\mathbb{Q}) \neq \emptyset$, then C has an effective rational divisor of degree 1.