International
University
Bremen

Deciding Existence of Rational Points on Genus 2 Curves: A Computational Experiment

Michael Stoll
International University Bremen
joint work with Nils Bruin (SFU)

Göttingen, July 21, 2006

Motivation

Question.
Given a smooth projective curve $C/\mathbb{Q}$,
can we algorithmically decide whether $C(\mathbb{Q}) = \emptyset$ or not?

General Remarks.

- If $g(C) = 0$, the Hasse Principle holds $\implies$ OK.
- If $g(C) = 1$, then problem is related to determining $\operatorname{rank} E(\mathbb{Q})$ for elliptic curves E (another open problem).
- First interesting case is $g(C) = 2$:
  $C : y^2 = f(x)$ with $\deg f = (5 \text{ or}) \ 6$, f squarefree.

Practical Remarks.

- If $C(\mathbb{Q}) \neq \emptyset$, we can find a point $\implies$ OK.
- If $C(\mathbb{Q}_v) = \emptyset$ for some place v, then $C(\mathbb{Q}) = \emptyset$ $\implies$ OK.
- If $\forall v : C(\mathbb{Q}_v) \neq \emptyset$, but apparently $C(\mathbb{Q}) = \emptyset$, we can try *descent*.

Descent 1

Let $\pi : D \to C$ be a finite étale, geometrically Galois covering (more precisely: a C-torsor under a finite $\mathbb{Q}$-group scheme G).

This covering has *twists* $\pi_\xi : D_\xi \to C$ for $\xi \in H^1(\mathbb{Q}, G)$.

More concretely, a twist $\pi_\xi : D_\xi \to C$ of $\pi : D \to C$ is another covering of C that over $\bar{\mathbb{Q}}$ is isomorphic to $\pi : D \to C$.

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 a C-torsor under $\mathbb{Z}/2\mathbb{Z}$,
and the twists are $D_d : u^2 = d\,g(x),\ v^2 = d\,h(x)$, $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

Every rational point on C lifts to one of the twists,
and there are only finitely many twists such that $D_d(\mathbb{Q}_v) \neq \emptyset$ for all v.

Descent 2

More generally, we have the following result.

Theorem.

- $C(\mathbb{Q}) = \bigcup_{\xi \in H^1(\mathbb{Q},G)} \pi_\xi(D_\xi(\mathbb{Q}))$.
- $\mathrm{Sel}^\pi(\mathbb{Q}, C) := \{\xi \in H^1(\mathbb{Q}, G) : D_\xi(\mathbb{A}_\mathbb{Q}) \neq \emptyset\}$ is finite (and computable).

(Fermat, Chevalley-Weil, . . .)

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

More specifically, we can consider n-coverings of C:
Coverings obtained through pull-back of n-coverings
of the principal homogeneous space Pic^1_C under the Jacobian of C.
Let $\mathrm{Sel}^{(n)}(\mathbb{Q}, C)$ denote the corresponding Selmer set.

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

The Experiment

Question. How far can we get in practice?

Consider all "small" genus 2 curves $C : y^2 = f(x)$
where f has coefficients in $\{-3, -2, -1, 0, 1, 2, 3\}$.

There are 196 171 isomorphism classes.
Try to decide for each of them whether there are rational points or not!

Outline of Procedure.

Step 1. Look for rational points.
Step 2. Check for local points.
Step 3. Do a 2-descent.
Step 4. Apply the Mordell-Weil sieve.

Rational Points

Step 1. Look for rational points.

Points are found on 137 490 of the curves.
There remain 56 681 curves which we suspect have no rational points.

Remark. The largest points found were $(\frac{1519}{601}, \frac{4816728814}{601^3})$ on

$$C : y^2 = 3\,x^6 - 2\,x^5 - 2\,x^4 - x^2 + 3\,x - 3$$

and $(\frac{193}{436}, \frac{165847285}{436^3})$ on

$$C : y^2 = 3\,x^6 - 3\,x^5 - x^4 - x^3 - 3\,x^2 + x - 3\,.$$

All other smallest points have height < 80.

It remains to show $\boxed{C(\mathbb{Q}) = \emptyset}$ for the 56 681 remaining curves!

A Simple Way To Show a Set is Empty

Step 2. Check for local points (over $\mathbb{R} = \mathbb{Q}_\infty$ and $\mathbb{Q}_p$).

Lemma. If $f : A \to B$ is a map and $B = \emptyset$, then $A = \emptyset$.

We use the obvious maps $C(\mathbb{Q}) \hookrightarrow C(\mathbb{Q}_v)$.

Among the 56 681 curves without apparent rational point,
we find 29 278 curves that do have points everywhere locally.

(Hence they will provide counterexamples to the Hasse Principle,
once we have proved they have no rational points!)

A Sophisticated Way To Show a Set is Empty

Lemma. Consider the following diagram:

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \beta \\ C & \xrightarrow{\gamma} & D \end{array}$$

If the diagram commutes and the images of β and γ are disjoint, then $A = \emptyset$.

We will apply this in two instances with $A = C(\mathbb{Q})$, where the upper horizontal map is a "global" map and the lower horizontal map is a "local" map.

2-Descent

Step 3. Do a 2-descent.

Let $C : y^2 = f(x)$, let $L = \mathbb{Q}[T]/(f(T))$, let $\theta \in L$ be the image of T.
Define $F : C(\mathbb{Q}) \to \frac{L^\times}{\mathbb{Q}^\times (L^\times)^2}$, $(x, y) \mapsto (x - \theta)\mathbb{Q}^\times (L^\times)^2$.

With $L_v = L \otimes_{\mathbb{Q}} \mathbb{Q}_v$, we have similar "local" maps $F_v : C(\mathbb{Q}_v) \to \frac{L_v^\times}{\mathbb{Q}_v^\times (L_v^\times)^2}$.
Consider

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{F} & \frac{L^\times}{\mathbb{Q}^\times (L^\times)^2} \\ \downarrow & & \downarrow \\ \prod_v C(\mathbb{Q}_v) & \xrightarrow{\prod F_v} & \prod_v \frac{L_v^\times}{\mathbb{Q}_v^\times (L_v^\times)^2} \end{array}$$

Remark. This implicitly computes $\mathrm{Sel}^{(2)}(\mathbb{Q}, C)$.

Result. Among the 29 278 curves that remained after Step 2, there are 1 492 that have $\mathrm{Sel}^{(2)}(\mathbb{Q}, C) \neq \emptyset$.

Mordell-Weil Sieve

Step 4. Apply the Mordell-Weil sieve.

Let J be the Jacobian of C. Assume:

- We know generators of $J(\mathbb{Q})$.
- We know a rational divisor (class) D of degree 1 on C.

Then we have a $\mathbb{Q}$-defined embedding $\iota : C \to J$, $P \mapsto [P - D]$.

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

$$\begin{array}{ccc} C(\mathbb{Q}) & \xrightarrow{\iota} & J(\mathbb{Q}) \\ \downarrow & & \downarrow \rho \\ \prod_{p \in S} C(\mathbb{F}_p) & \xrightarrow{\iota} & \prod_{p \in S} J(\mathbb{F}_p) \end{array}$$

(Scharaschkin, Flynn)

Remark. If $\text{Ш}(\mathbb{Q}, J)$ is finite, then the MW sieve is equivalent to descent with respect to all n-coverings of C.

Satisfying the Assumptions

By a 2-descent on J, we obtain upper bounds on $\operatorname{rank} J(\mathbb{Q})$.
To get lower bounds, we have to find points in $J(\mathbb{Q})$.

These generators can be very large, so a “naïve” search is not sufficient.

We also need to find a rational point on Pic^1_C
($=$ a rational divisor class of degree 1).

To do this, we work on the dual Kummer surface $\mathrm{Pic}^1_C/(\text{hyp. invol.})$.

Note: $D \in \mathrm{Pic}^1_C(\mathbb{Q})$ gives $P = 2D - K \in J(\mathbb{Q})$ $\quad$ ($K =$ canonical class).

If unsuccessful, we can do a 2-descent on Pic^1_C, using the $x - T$ map again.

The largest generator found has (logarithmic) canonical height > 95.

Examples of Large Generators

For

$$C : y^2 = -3\,x^6 + x^5 - 2\,x^4 - 2\,x^2 + 2\,x + 3$$

$J(\mathbb{Q})$ is infinite cyclic generated by $P_1 + P_2 - W$, where the x-coordinates of P_1 and P_2 are the roots of

$$x^2 + \frac{37482925498065820078878366248457300623}{34011049811816647384141492487717524243}\,x + \frac{58145262828082430669892656161839396703 3}{54417679698906635814626387980348038788 8}.$$

The canonical logarithmic height of this generator is 95.26287.

The second largest example is

$$C : y^2 = -2\,x^6 - 3\,x^5 + x^4 + 3\,x^3 + 3\,x^2 + 3\,x - 3$$

with $J(\mathbb{Q})$ generated by a point coming from

$$x^2 + \frac{836283543413625628607991530 63}{267798119543522958491436140 59}\,x + \frac{85297254727650728651326915768 9}{32135774345222755018972336870 8}.$$

The canonical height of this generator is 77.33265.

Some Statistics

For all but 47 curves, we can determine $J(\mathbb{Q})$ in this way.

For the remaining 47 curves, we suspect 2- or even 4-torsion in $Ш(\mathbb{Q}, J)$:

conj. $Ш(\mathbb{Q}, J)$	0	$(\mathbb{Z}/2\mathbb{Z})^2$	$(\mathbb{Z}/4\mathbb{Z})^2$	total
rank $J(\mathbb{Q}) = 0$	3		36	39
rank $J(\mathbb{Q}) = 1$	516	5	5	526
rank $J(\mathbb{Q}) = 2$	772		1	773
rank $J(\mathbb{Q}) = 3$	152			152
rank $J(\mathbb{Q}) = 4$	2			2
all ranks	1445	5	42	1492

The cases with $Ш(\mathbb{Q}, J) = (\mathbb{Z}/2\mathbb{Z})^2$ can be dealt with by *visualization*.

For the remaining 42 cases, assuming the BSD Conjecture,

we find $\mathrm{Pic}^1_C(\mathbb{Q}) = \emptyset$, hence $C(\mathbb{Q}) = \emptyset$ as well.

Mordell-Weil Sieve: Practice

The main problem here is to keep the combinatorics in check.

First pick a promising set S of (good) primes
(primes p below a given bound such that $\#J(\mathbb{F}_p)$ is smooth).

For the computation, work with groups $J(\mathbb{Q})/BJ(\mathbb{Q})$, $J(\mathbb{F}_p)/BJ(\mathbb{F}_p)$,
with a sequence $1 = B_0, B_1, \ldots, B_n$ of values for B
such that $B_{i+1} = q_{i+1}B_i$ with suitable primes q_i.

A preliminary heuristic computation produces a suitable sequence (B_i).
We then successively compute the subsets of $J(\mathbb{Q})/B_iJ(\mathbb{Q})$, $i = 0, 1, \ldots$,
that map into the image of $C(\mathbb{F}_p)$ in $J(\mathbb{F}_p)/B_iJ(\mathbb{F}_p)$ for all $p \in S$.
We stop when we reach the empty set.

This worked for all the curves (as predicted by Bjorn Poonen's heuristics).
(Maximal computing time for a single curve was $\sim$ 16 hours.)

Conclusions

- We were able to decide existence of rational points for *all* our curves (assuming BSD in 42 cases).
- If $C(\mathbb{Q}) \neq \emptyset$ for one of our curves, then C has a rational point of x-coordinate height ≤ 1519.
- There are 29 278 counterexamples to the Hasse Principle among our curves.
- The Brauer-Manin obstruction is the only one against rational points for our curves (assuming finiteness of $Ш(\mathbb{Q}, J)$ in 1492 cases and BSD in 42 cases).
- Our result provides support for the conjecture that existence of rational points on smooth projective curves should be decidable.