Searching for Rational Points on Genus 2 Jacobians

Michael Stoll
Universität Bayreuth

BIRS
December 5, 2008

Motivation

Let $C : y^2 = f(x)$ be a curve of genus 2 over $\mathbb{Q}$, with Jacobian J.

We will assume that $C(\mathbb{A}_\mathbb{Q}) \neq \emptyset$.

Task: Find generators of $J(\mathbb{Q})$!

1. 2-Descent on J gives upper bound on rank
2. Search for points on $J(\mathbb{Q})$ gives lower bound on rank
3. Hope that bounds agree
4. Use heights to saturate the known subgroup

We focus on step 2 in this talk,
but we will also have to review step 1.

Example

In general, let $\pi : J \to K \subset \mathbb{P}^3$ denote the map to the Kummer Surface.

Consider

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

Then $J(\mathbb{Q}) = \langle P \rangle \cong \mathbb{Z}$, with

$$\begin{aligned}\pi(P) = (\ \ & 1\ 9590364691\ 6063888932\ 6549967292\ 5293963968 : \\ & -2\ 1590165086\ 8859123654\ 3393895911\ 1405158848 : \\ & 2\ 0932294618\ 1096750411\ 6135621826\ 2182813188 : \\ & 9\ 1247794946\ 8811884895\ 4941275692\ 2959999369)\end{aligned}$$

Naive height	$h(P) = 94.31440-$
Canonical height	$\hat{h}(P) = 95.26287-$

General Point Search

How can we search for rational points of height $\leq H$ on a d-dimensional variety $X \subset \mathbb{P}^{N-1}$?

The obvious way: Project to some $\mathbb{P}^d$, check which $P \in \mathbb{P}^d(\mathbb{Q})$ lift to $X(\mathbb{Q})$.
Complexity: H^{d+1}.

This can be combined with sieving using information mod p.

Example: $J \to K \to \mathbb{P}^2$. Find points in $K(\mathbb{Q})$ lifting to $J(\mathbb{Q})$.
This is implemented (`j-points`), small constant in front of H^3.
Takes about 1 hour for $H = 10^4$ (degree 6; faster for degree 5).

Good for finding small points quickly.

Using Lattices

Pick a good prime p.
For each $P \in X(\mathbb{F}_p)$, construct a lattice $L_P \subset \mathbb{Z}^N$
that contains coordinate vectors of all rational points reducing to P
and look for small vectors in L_P.

Let $t_1, \ldots, t_d$ be local coordinates near a lift $P_0 \in X(\mathbb{Q}_p)$ of P.
There is a vector-valued power series $\mathbf{u} \in \mathbb{Z}_p[\![t_1, \ldots, t_d]\!]^N$
such that the residue class of P is $\{\mathbf{u}(pt_1, \ldots, pt_s) : t_1, \ldots, t_d \in \mathbb{Z}_p\}$.

Write $\mathbf{u} = \sum_{i_1,\ldots,i_d \geq 0} \mathbf{u}_{i_1,\ldots,i_d} t_1^{i_1} \cdots t_d^{i_d}$ and set

$$L_P = \mathbb{Z}^N \cap \sum_{i_1,\ldots,i_d \geq 0} \mathbb{Z}_p \cdot p^{i_1+\cdots+i_d} \mathbf{u}_{i_1,\ldots,i_d} .$$

Generically, $(\mathbb{Z}^N : L_P) = p^{\rho(d,N)}$; $\rho(d,N) = \sum_{j=0}^{N-1} \max\{k : \binom{k+d-1}{d} \leq j\}$.

Complexity

$$(\mathbb{Z}^N : L_P) = p^{\rho(d,N)} \text{ with } \rho(d,N) = \sum_{j=0}^{N-1} \max\{k : \binom{k+d-1}{d} \leq j\}.$$

Can expect small vectors to be of height about $p^{\rho(d,N)/N}$.

Hence: Take $p \gg H^{N/\rho(d,N)}$.

Since $\#X(\mathbb{F}_p) \approx p^d$, the complexity is $\approx H^{dN/\rho(d,N)}$.

Surface in $\mathbb{P}^3$ gives H^2.
Surface in $\mathbb{P}^{15}$ gives $H^{32/45}$.

For $J \subset \mathbb{P}^{15}$, note that height gets squared,
so we get $H^{64/45}$ in terms of the Kummer Surface height.

But: Constant too large to be faster than the simple method!

Covering Spaces

To make progress, we need some means of making the points smaller.

This can be achieved using covering spaces of J.

There is a finite set of (for example) 2-coverings $X_j \to J$
such that every point in $J(\mathbb{Q})$ lifts to some $X_j(\mathbb{Q})$.
Also, the height goes down from H to $H^{1/4}$.

The 2-descent computation (that we did for the upper rank bound)
gives us a set that classifies the X_j.

But: It is not easy to use this to construct explicit models (in $\mathbb{P}^{15}$).

2-Descent

Recall: $C : y^2 = f(x)$.

Define $A = \mathbb{Q}[\theta] = \mathbb{Q}[T]/(f(T))$.

There is a group homomorphism

$$\mu : \mathrm{Div}_C(\mathbb{Q}) \to \mathrm{Pic}_C(\mathbb{Q}) \to \frac{A^\times}{\mathbb{Q}^\times (A^\times)^2}, \quad \sum_P n_P P \longmapsto \prod_P \Big(x(P) - \theta\Big)^{n_P}$$

We can compute a finite subgroup S of $A^\times/\mathbb{Q}^\times(A^\times)^2$ that contains $\mu\Big(J(\mathbb{Q})\Big)$.

Each element $\delta \cdot \mathbb{Q}^\times(A^\times)^2 \in S$ gives rise to one or two 2-covering spaces X_δ of J.

Application to Point Search

Given δ, construct a K3 Surface Y_δ:

Write $\mathbf{z} = z_0 + z_1\theta + \cdots + z_5\theta^5 \in A$. Then

$$\delta\mathbf{z}^2 = Q_{\delta,0}(\mathbf{z}) + Q_{\delta,1}(\mathbf{z})\theta + \cdots + Q_{\delta,5}(\mathbf{z})\theta^5 .$$

with quadratic forms $Q_{\delta,j} \in \mathbb{Q}[z_0, \ldots, z_5]$.

Define $\quad Y_\delta \subset \mathbb{P}(A) = \mathbb{P}^5 : \quad Q_{\delta,3} = Q_{\delta,4} = Q_{\delta,5} = 0 .$

$$\begin{tikzcd}
X_\delta \arrow[r] \arrow[d, "\pi_\delta"'] & K_\delta \arrow[d] & Y_\delta \arrow[l] \arrow[dl] \arrow[d, "\delta\mathbf{z}^2"] \\
J \arrow[r] & K \arrow[r, dashed] & \mathbb{P}^2
\end{tikzcd}$$

Complexity for points of height $\leq H$ in $\mathbb{P}^2$ is $H^{3/4}$.

Algorithm

Input: C, $\delta \in A^\times$ and H.

1. Select a good $\mathbb{Q}$-basis for δ of A.
2. Compute the quadratic forms $Q_{\delta,j}$ w.r.t. this basis.
3. Let $Y_\delta \subset \mathbb{P}(A)$ be the K3 Surface $Q_{\delta,3} = Q_{\delta,4} = Q_{\delta,5} = 0$.
4. For good primes $p_1, \ldots, p_k$ with $p_1 \cdots p_k \gg H^{3/8}$,
   compute $P_j = \{P \in Y_\delta(\mathbb{F}_{p_j}) : P$ gives point in $J(\mathbb{F}_{p_j})\}$.
5. Compute the sets $\Lambda_j = \{L_P : P \in P_j\}$.
6. For each lattice $L = L_1 \cap \cdots \cap L_k$ with $L_j \in \Lambda_j$,
   find small vectors in L and check if they give a point in $J(\mathbb{Q})$.
   Return this point when one is found, and stop.
7. Return "No point found."

Example

Consider $y^2 = x^5 - 41$.

The rank of $J(\mathbb{Q})$ should be 1, but there are no small points.

The nontrivial element of S is represented by

$$\delta = 38903213\theta^4 + 81019029\theta^3 + 248047293\theta^2 + 260114981\theta + 1085600973$$

We find equations for Y_δ (in 'good' coordinates):

$$\begin{aligned} -2z_1z_4 + 2z_2z_5 + z_3^2 &= 0 \\ z_1^2 - 2z_1z_5 + 2z_2z_3 + 4z_2z_4 - 2z_3z_4 - 4z_3z_5 + 2z_4z_5 - 3z_5^2 &= 0 \\ -z_0^2 - 4z_1z_2 - 4z_1z_4 - 2z_1z_5 + z_2^2 - 2z_2z_4 & \\ - 4z_3^2 - 6z_3z_4 - 8z_3z_5 + 5z_4^2 - 8z_4z_5 + 6z_5^2 &= 0 \end{aligned}$$

The point $(-2197 : -142 : 656 : 566 : -703 : -92) \in Y_\delta(\mathbb{Q})$
gives a generator of $J(\mathbb{Q})$;
the image on K is $(77228944 : 39966176 : 39032976 : 7200361913)$.

Beyond 2-Coverings

In many cases, Pic^1_C is a nontrivial 2-covering of J.

We can use 2-descent on Pic^1_C to construct some 4-coverings of J.

Recall the map

$$\begin{aligned} \mu: \qquad C^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^1_C(\mathbb{Q}) &\to \frac{A^\times}{\mathbb{Q}^\times (A^\times)^2} \\ P_1 + P_2 + P_3 &\longmapsto (x(P_1) - \theta)(x(P_2) - \theta)(x(P_3) - \theta)\,. \end{aligned}$$

We can compute a finite subset S of $A^\times / \mathbb{Q}^\times (A^\times)^2$
that contains $\mu\big(\mathrm{Pic}^1_C(\mathbb{Q})\big)$.

Each element $\delta \cdot \mathbb{Q}^\times (A^\times)^2 \in S$ gives rise to a 2-covering space X_δ of Pic^1_C.

A Diagram

We define $Z_\delta \subset \mathbb{P}(A) : Q_{\delta_4} = Q_{\delta,5} = 0$.

Then X_δ is the variety of lines in Z_δ.
Let W_δ be the universal family over X_δ.

$$
\begin{tikzcd}
 & W_\delta \arrow[dl, "\mathbb{P}^1"'] \arrow[dr, "4:1"] \arrow[dd] & \\
X_\delta \arrow[dd, "\pi_\delta"'] & & Z_\delta \arrow[dd, "\delta\mathbf{z}^2"] \\
 & C^{(3)} \arrow[dl, "\mathbb{P}^1"'] \arrow[dr, "8:1"] & \\
\mathrm{Pic}^1_C \arrow[d] & & \mathbb{P}^3 \\
J & &
\end{tikzcd}
$$

If height on $\mathbb{P}^3$ is comparable with height on $X_\delta \subset \mathbb{P}^{15}$, then we gain a factor of 16 in the exponent of H.

Threefold in $\mathbb{P}^5$: $H^{3 \cdot 6/7}$
Gives complexity $H^{9/56}$.

Algorithm

Input: C, $\delta \in A^\times$ and H.

1. Select a good $\mathbb{Q}$-basis for δ of A.
2. Compute the quadratic forms $Q_{\delta,j}$ w.r.t. this basis.
3. Let $Z_\delta \subset \mathbb{P}(A)$ be given by $Q_{\delta,4} = Q_{\delta,5} = 0$.
4. For good primes $p_1, \dots, p_k$ with $p_1 \cdots p_k \gg H^{3/56\,?}$,
   compute $P_j = \{P \in Z_\delta(\mathbb{F}_{p_j}) : P \text{ lifts to } W_\delta(\mathbb{F}_{p_j})\}$.
5. Compute the sets $\Lambda_j = \{L_P : P \in P_j\}$.
6. For each lattice $L = L_1 \cap \cdots \cap L_k$ with $L_j \in \Lambda_j$,
   find small vectors in L and check if they give a point in $C^{(3)}(\mathbb{Q})$.
   Return this point when one is found, and stop.
7. Return "No point found."

Example

Consider the example from the beginning:

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

There is one nontrivial element of S:

$$\delta = -768\theta^5 - 113\theta^4 + 295\theta^3 + 825\theta^2 + 30\theta - 337\,.$$

Equations for Z_δ are

$$\begin{aligned} z_0^2 - 2z_0z_1 + 2z_0z_3 + 4z_0z_4 + z_1^2 - 6z_1z_2 - 2z_1z_5 + z_2^2 + 2z_2z_5 - z_3^2 + 2z_3z_4 + 2z_5^2 &= 0 \\ z_0^2 - 2z_0z_2 + 2z_0z_4 - 2z_1z_2 + 2z_1z_4 - 2z_2z_4 + 2z_2z_5 - 2z_3z_5 - z_4^2 - 2z_4z_5 + 4z_5^2 &= 0 \end{aligned}$$

Find point $(181 : 7 : 22 : 138 : -61 : 6)$ on Z_δ.

Image in $\mathbb{P}^3$ is $35028\,x^3 + 59577\,x^2 + 49066\,x + 13929$.

What Next?

Idea from Wednesday:

Try to write X_δ explicitly as $X_\delta \subset G(\mathbb{P}^1, \mathbb{P}^5) \subset \mathbb{P}^{14}$.

If the height there is comparable to the "4Θ height" on X_δ,
then searching for points on $X_\delta \subset \mathbb{P}^{14}$ leads to:

Surface in $\mathbb{P}^{14}$: $H^{2\cdot 15/40} = H^{3/4}$
Gain in exponent of height: 8

So the complexity would be $H^{3/32}$.

This might extend the range of "findable" points.

Application

The information we obtain can be used to verify that $C(\mathbb{Q}) = \emptyset$.

Given:

- An explicit embedding $\iota : C \to J$ ($\in \mathrm{Pic}^1_C(\mathbb{Q})$),
- Explicit generators of $J(\mathbb{Q})$,

we can run a Mordell-Weil Sieve computation.

It uses local information to put conditions on the image of $C(\mathbb{Q})$ in $J(\mathbb{Q})$; when these conditions are contradictory, this gives a proof of $C(\mathbb{Q}) = \emptyset$.

Conjecturally, this should always work.