How to Find the Rational Points on a Rank 1 Genus 2 Curve

Michael Stoll
Jacobs University Bremen

Lorentz Center, Leiden, May 14, 2007
The Goal

Let $C/\mathbb{Q}$ be a smooth projective curve of genus 2, given by

$$y^2 = f(x) = f_6 x^6 + f_5 x^5 + f_4 x^4 + f_3 x^3 + f_2 x^2 + f_1 x + f_0.$$ 

Goal: Determine $C(\mathbb{Q})$!

Assumptions: Let $J$ be the Jacobian of $C$.

- $\text{rank } J(\mathbb{Q}) = 1$, and a generator $G$ of $J(\mathbb{Q})$ (mod torsion) is known;
- We know a point $P_0 \in C(\mathbb{Q})$.

For simplicity, we will assume that $J(\mathbb{Q}) = \mathbb{Z} \cdot G$.

Remark.
If $C(\mathbb{Q})$ is non-empty, then $P_0$ is usually easy to find.
If $C(\mathbb{Q})$ is empty, there are ways to prove this fact.
The Idea

Let \( \iota : C \longrightarrow J, \quad P \longmapsto [P - P_0] \)
be the embedding determined by the basepoint \( P_0 \).

We have to determine the set

\[
R = \{ n \in \mathbb{Z} : nG \in \iota(C) \} = \phi(C(\mathbb{Q})) \subset \mathbb{Z},
\]

where \( \phi : C(\mathbb{Q}) \xrightarrow{\iota} J(\mathbb{Q}) \xrightarrow{\cong} \mathbb{Z} \).

Outline of Procedure:

1. Find \( N \) such that \( R \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z} \) is injective;
2. For each coset \( k + N\mathbb{Z} \),
   either exhibit a point \( P \in C(\mathbb{Q}) \) with \( \phi(P) \in k + N\mathbb{Z} \),
   or show that \( R \cap (k + N\mathbb{Z}) \) is empty.
Step 1

We don’t know how to do Step 1 in general.

However, we can hope to find a suitable $N$ in our case, or more generally, when $\text{rank } J(\mathbb{Q}) < g(C)$.

The idea here is to use Chabauty’s Method:

Let $p$ be a prime. There is a pairing

$$\Omega^1_J(\mathbb{Q}_p) \times J(\mathbb{Q}_p) \rightarrow \mathbb{Q}_p, \quad (\omega, R) \mapsto \int_0^R \omega.$$ 

Since $\text{rank } J(\mathbb{Q}) = 1$ and $\text{dim}_{\mathbb{Q}_p} \Omega^1_J(\mathbb{Q}_p) = 2$, there is a differential

$$0 \neq \omega_p \in \Omega_C(\mathbb{Q}_p) \cong \Omega^1_J(\mathbb{Q}_p)$$

that kills $J(\mathbb{Q}) \subset J(\mathbb{Q}_p)$. 
How to Find $N$

Theorem.
If the reduction $\bar{\omega}_p$ does not vanish on $C(\mathbb{F}_p)$ and $p > 2$, then each residue class contains at most one rational point.

This implies that $C(\mathbb{Q}) \to J(\mathbb{Q})/NJ(\mathbb{Q})$ is injective, where $N = (J(\mathbb{Q}) : J(\mathbb{Q}) \cap J(\mathbb{Q}_p)^1)$.

Heuristically, the set of primes $p$ satisfying this condition should have positive density (at least when $J$ is simple):

Note that for a random $\bar{\omega} = \frac{(a + bx) \, dx}{y}$, there is a $\approx 50\%$ chance.

Heuristic/Conjecture 1.
If $J$ is simple, then there are primes $p > 2$ such that $\bar{\omega}_p \neq 0$ on $C(\mathbb{F}_p)$.

In practice, this works very well.
How to Compute $\bar{\omega}_p$

Given a prime $p$ of good reduction, we find $\bar{\omega}_p$ as follows.

Let $K \subset \mathbb{P}^3$ be the Kummer Surface of $J$: $J \xrightarrow{\pi} K = J/\{\pm1\}$.

Compute the image of $NG$ on $K$; it will have the form $\pi(NG) = (p^2a : p^2b : p^2c : d)$ with $p \nmid d$.

We have $ax^2 - bx + c \equiv \lambda(\alpha x + \beta)^2 \mod p$; and

$$\bar{\omega}_p = \frac{(\bar{\alpha}x + \bar{\beta})dx}{y}.$$  

Remarks.
1. We can compute $\pi(NG)$ from $\pi(G)$.
2. We can do the computation $\mod p^3$ (i.e., efficiently even for large $N$).
Step 2

Given a coset \( k + N\mathbb{Z} \), we let \( k_0 \) be the absolutely smallest representative and check whether \( k_0G \in \iota(C) \).

(Before embarking on a potentially costly exact computation of \( k_0G \), we check for several primes \( p \) whether its image mod \( p \) is in \( \iota(C(F_p)) \).)

If so, we have found \( P_k = \iota^{-1}(k_0G) \in C(\mathbb{Q}) \); this is then the only rational point in this residue class.

Otherwise, we try to prove that \( R \cap (k + N\mathbb{Z}) = \emptyset \) by a Mordell-Weil Sieve computation.
Mordell-Weil Sieve

Let $S$ be a finite set of primes of good reduction.
Let $B$ be a multiple of $N$. Consider the following diagram.

\[
\begin{array}{ccc}
C(\mathbb{Q}) & \xrightarrow{\cong} & R \\
\downarrow & & \downarrow \rho \\
\prod_{p \in S} C(\mathbb{F}_p) & \xrightarrow{\imath} & \prod_{p \in S} J(\mathbb{F}_p) \\
& & \xrightarrow{\prod_{p \in S} J(\mathbb{F}_p)/BJ(\mathbb{F}_p)} \\
& & \beta \downarrow \\
& & \mathbb{Z}/B\mathbb{Z}
\end{array}
\]

If the images of $\beta \circ \rho$ and of $\alpha$ do not intersect, then $R \cap (k + N\mathbb{Z}) = \emptyset$.

**Heuristic/Conjecture 2:**
If $R \cap (k + N\mathbb{Z}) = \emptyset$, then this will be the case when $B$ and $S$ are sufficiently large.
Practical Remarks

- To avoid combinatorial explosion, we compute $\beta^{-1}\left(\text{im}(\alpha)\right)$ successively for a sequence $1 = B_0, B_1, \ldots, B_n = B$, where $B_m = q_mB_{m-1}$ with $q_m$ a prime.

- When $B_m$ is a multiple of $N$, we check the smallest point in the class if it comes from $C$; if so, we can discard everything in the same coset mod $N$.

- We can work with several values of $N$ at the same time.
Conclusion

• Given a curve $C$ of genus 2, a point in $C(\mathbb{Q})$ and a generator of $J(\mathbb{Q})$, there is an algorithm that computes $C(\mathbb{Q})$.

• Termination of the algorithm is conditional on two conjectures; these conjectures are supported by heuristics and experimental evidence.

• In practice, the procedure works and is quite efficient. For example, for the “Flynn-Poonen-Schaefer Curve”

$$C : y^2 = x^6 + 8x^5 + 22x^4 + 22x^3 + 6x^2 + 5x + 1,$$

it takes about 1.5 seconds to find $\#C(\mathbb{Q}) = 6$.

• Step 2 does not require the “Chabauty Condition” $r < g$. So if we can do Step 1 for a given curve $C$, we are in good shape to find $C(\mathbb{Q})$. 