A Chabauty computation on a curve of genus 2

Nils Bruin

In these notes, we redo part of a Chabauty argument that explicitly determines all rational points on a curve of genus 2. The curve in question comes from Flynn, Poonen, Schaefer, Cycles of Quadratic Polynomials, Duke 90, 1997.

The argument we give here is slightly different from the computation done in the original article. The advantage of the present approach is that it more easily generalises to non-hyperelliptic curves.

1. Picard group of a curve

For a projective curve $C$, the group variety we can use is quite a bit more complicated than for an affine curve. First we describe the group. Here, we’ll concentrate on one particular curve of genus 2. Much of the methods we describe apply in general.

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

Again, this is just an affine model. What we really mean, is the complete curve in weighted projective space:

$C : Y^2 = X^6 + 8X^5Z + 22X^4Z^2 + 22X^3Z^3 + 5X^2Z^4 + 6XZ^5 + Z^6$

and well, write $\infty^+ = (1 : 1 : 0)$ and $\infty^- = (1 : -1 : 0)$. There are 6 rational points on this curve:

$\infty^\pm, (0 : \pm1 : 1), (-3 : \pm1 : 1)$

Definition: A divisor on a curve is a formal linear combination of points in $C(\mathbb{Q})$

$$\sum P \cdot n_P.$$

A divisor is defined over $\mathbb{Q}$ if the sum is galois-stable, i.e., $n_{P^\sigma} = n_P$. The degree of a divisor is $\sum n_P$.

Definition: A divisor is called principal if the multiplicities describe the pole and zero orders of a function on $C$:

$$(x) = (0, 1) + (0, -1) - \infty^+ - \infty^-$$

The principal divisors form a subgroup of the divisor group. Note that on a projective curve, functions have the same number of poles as they have zeros, so principal divisors are of degree 0.

Definition: The Picard group of a curve is the group of divisors modded out by principal divisors. An element of the picard group is called a divisor class.

Theorem: If a curve has points everywhere locally then every galois-stable divisor class can be represented by a galois-stable divisor.

Definition/Theorem: The Jacobian of a curve is a $g$-dimensional projective group variety of which the rational points represent the galois-stable divisor classes of degree 0. More specific for genus 2 curves, every (rational) divisor class can be represented in the form

$$[P + Q - 2\infty^-]$$

where $P, Q$ are either rational points or quadratic conjugate points.
Abel-Jacobi map: \[ C \to J \]
\[ P \mapsto [P - \infty] \]

Complicated computation:
\[ \text{Pic}^0(C/\mathbb{Q}) = \langle G = [\infty^+ - \infty^-] \rangle \simeq \mathbb{Z} \]

Some elements of \( \text{Pic}^0(C/\mathbb{Q}) \):

\[
\begin{array}{l|l}
-6G & [2(0,1) - 2\infty^-] \\
-5G & [(-3,-1) - \infty^-] \\
-4G & [(-3,-1) + \infty^+ - 2\infty^-] \\
-3G & [(0,1) - \infty^-] \\
-2G & [(0,1) + \infty^+ - 2\infty^-] \\
-G & [(0,-1) + (-3,-1) - 2\infty^-] \\
0 & [\infty^- - \infty^-] \\
G & [\infty^+ - \infty^-] \\
2G & [2\infty^+ - 2\infty^-] \\
3G & [(0,1) + (-3,1) - 2\infty^-] \\
4G & [(0,-1) - \infty^-] \\
5G & [(0,-1) + \infty^+ - 2\infty^-] \\
6G & [(-3,1) - \infty^-] \\
7G & [(-3,1) + \infty^+ - 2\infty^-] \\
8G & [2(0,-1) - 2\infty^-] \\
9G & [P + \overline{P} - 2\infty^-] \\
\end{array}
\]

where \( \alpha = \sqrt{33} \) and
\[ P = (1 : 101\alpha - 580 : \alpha - 6) \text{ and } \overline{P} = (1 : -101\alpha - 580 : -\alpha - 6) \]

Note that if we reduce 9G modulo 3 then we get 9G \( \equiv 0 \mod 3 \). Furthermore, we have \( C(\mathbb{F}_3) = \{(1 : \pm 1 : 0), (0 : \pm 1 : 1)\} \), so we see that under the Abel-Jacobi-map, \( C(\mathbb{Q}) \) maps into
\[ \{0, G, 4G, 6G\} + \langle 9G \rangle \]

2. Logarithms for \( \mathbb{G}_m \)

Recall from last time that we used
\[
\text{Log}(1 + z) = z - z^2/2 + z^3/3 - z^4/4 + \cdots
\]

to convert an equation in \( \mathbb{G}_m \) around 1 into an equation around 0 in \( \mathbb{A}^1 \). The observation to be made here is that this log has a better interpretation as
\[
\text{Log}(1 + z) = \int_0^z \frac{1}{1 + t} \, dt.
\]

The important bit here is that the differential \( \omega = \frac{1}{z} \, dz \) is regular on \( \mathbb{G}_m \) (it has a pole in \( z = 0, \infty \), but those are not on \( \mathbb{G}_m \)). The nice thing is that (formally),
\[
\int_0^{z_1} \frac{1}{1 + t} \, dt + \int_0^{z_2} \frac{1}{1 + t} \, dt = \int_0^{(1+z_1)(1+z_2)-1} \frac{1}{1 + t} \, dt
\]
which gives the fundamental property of Log. If the corresponding power series converge (say, \( z_i \in p\mathbb{Z}_p \) and \( p > 2 \)) then these identities really hold.

**Coleman integration:** These integrals can be made to work along larger paths as well, but this requires deeper results. We will make sure we only need to integrate along paths that fit inside small \( p \)-adic neighbourhoods, so that we stay inside the radius of convergence. Then integration really just corresponds to the formal power series operation.

3. **Regular differentials on \( C \)**

On hyperbolic curves, one can find multiple regular differentials. For instance, on \( C \), we have

\[
\omega_1 = \frac{dx}{y}, \omega_2 = \frac{xdx}{y}
\]

We use integration to define functions on \( \text{Pic}^0(C) \) by insisting that for \( \sum [P_i - Q_i] \) we have \( \sum \int_{Q_i}^{P_i} \omega_j \). This yields a group homomorphism:

\[
\begin{align*}
J & \rightarrow \mathbb{A}^2 \\
\sum [P_i - Q_i] & \mapsto (\sum \int_{Q_i}^{P_i} \omega_1, \sum \int_{Q_i}^{P_i} \omega_2)
\end{align*}
\]

In a way, this is actually how \( J \) is really defined.

4. **Computing differential that vanishes along the Mordell-Weil group**

Note that the points \( P \) and \( P \) are 3-adically close to \( \infty^- \). To be precise,

\[
(1 : -1 + y_1 : t)
\]

is equal to \( P \) for \((t, y_1) = 141\alpha - 810, 101\alpha - 580\). We know that

\[
(-1 + y_1)^2 = 1 + 8t + 22t^2 + 22t^3 + 5t^4 + 6t^5 + t^6
\]

so

\[
y_1 = -4t - 3t^2 + t^3 - 2t^4 + 2t^5 - 2t^6 + O(t^7)
\]

Then

\[
\omega_1 = \frac{t^3}{-1 + y_1} d(1/t) = t - 4t^2 + 13t^3 - 39t^4 + 111t^5 + O(t^6)
\]

\[
\omega_2 = \frac{t^2}{-1 + y_1} d(1/t) = 1 - 4t + 13t^2 - 39t^3 + 111t^4 - 304* t^5 + O(t^6)
\]

\[
\int_{0}^{[P+P]} \omega_1 \equiv 12 \mod 3^4
\]

\[
\int_{0}^{[P+P]} \omega_2 \equiv 63 \mod 3^4
\]

so \( \omega = (21 + O(3^3))\omega_1 - (4 + O(3^3))\omega_2 \) has the property that \( \int_{0}^{D} \omega = 0 \) if \( D \) in the Mordell-Weil group.
5. Determining the number of points in a fiber of reduction

Let’s see how many points in $C(\mathbb{Q})$ reduce to $(0 : 1 : 1)$ modulo 3. For this, we make once again a power series expansion:

$$P_t = (3t : y_2 : 1)$$

where

$$y_2 = 1 + 9t - 18t^2 + 459t^3 - 3402t^4 + O(3^5, t^5)$$

If $P_t \in C(\mathbb{Q})$ for some $t \in \mathbb{Z}_3$ then $[P_t - P_0] \in J(\mathbb{Q})$, so

$$\int_0^t \omega = 0$$

In fact,

$$\int_0^t \omega \equiv 9t + 9t^2 \mod (3^3)$$

So indeed, by Strassman’s Theorem we see that this power series should have at most 2 zeros for $t \in \mathbb{Z}_3$. In fact, we know that $t = 0, -1$ are such zeroes, so we see that the points $(0 : 1 : 1)$ and $(-3 : 1 : 1)$ are the only two rational points on $C(\mathbb{Q})$ that reduce to that point $\mod 3$.

6. Exercise

Do the Chabauty argument for the fiber around $\infty^+$. 