# EXPLICIT ON GENUS-3 CURVES, II

NILS BRUIN (WITH FLYNN, POONEN, STOLL)

Let $C$ be $\sum x_i y^j z^{4-i-j} - y^2z^2 - 2z^4 = 0$. This has points

$$\begin{aligned}
p_0 &: (-1 : 1 : 1) \\
p_1 &: (1 : -1 : 1) \\
p_2 &: (1 : 1 : -1) \\
p_3 &: (25 : -17 : 31) \\
p_4 &: \{x^2 + 2z^2, y + z = 0\} \\
p_5 &: \{3x^2 + 2y^2 - 3yz - 2z^2 = 0 \\
&\quad 3xy + 2y^2 + 3yz + z^2 = 0 \\
&\quad 3xz - 5y^2 + 3yz - z^2 = 0 \\
&\quad 5y^3 - y^2z + 4yz^2 + z^3 = 0\}
\end{aligned}$$

Define

$$\begin{aligned}
g_1 &:= [p_2 - p_0] \\
g_2 &:= [p_4 - 2p_0] \\
g_3 &:= [p_5 - 3p_0].
\end{aligned}$$

In terms of these, we have

$$\begin{aligned}
[p_1 - p_0] &:= 3g_1 + 2g_2 - 2g_3 \\
[p_2 - p_0] &:= g_1 \\
[p_3 - p_0] &:= 2g_2.
\end{aligned}$$

**Theorem 0.1.** *Subject to GRH, $\langle g_1, g_2, g_3 \rangle$ has finite odd index in $J_C(\mathbb{Q}) \simeq \mathbb{Z}^3$.*

Strategy:

$$\begin{array}{ccccc}
\text{almost } 2J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) & \longrightarrow & \dfrac{L^\times}{L^{\times 2}\mathbb{Q}^\times} \\
 & & \downarrow & & \downarrow \\
\text{almost } 2J(\mathbb{Q}_p) & \longrightarrow & J(\mathbb{Q}_p) & \longrightarrow & \dfrac{L_p^\times}{L_p^{\times 2}\mathbb{Q}_p^\times}
\end{array}$$

where $L_p := L \otimes \mathbb{Q}_p$.

*Date*: July 23, 2007.

Here the group $\frac{L^\times}{L^{\times 2}\mathbb{Q}^\times}$ is a substitute for $H^1(\mathbb{Q}, J[2])$. We may impose the conditions that cohomology classes are unramified outside a finite set $S$ to replace $\frac{L^\times}{L^{\times 2}}$ by a finite subgroup $L(2,S)$ essentially generated by $S$-units:

$$\begin{array}{ccccc} \text{almost } 2J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}) & \longrightarrow & \dfrac{L(2,S)}{\mathbb{Q}^\times} \\ & & \downarrow & & \downarrow \\ \text{almost } 2J(\mathbb{Q}_p) & \longrightarrow & J(\mathbb{Q}_p) & \longrightarrow & \dfrac{L_p^\times}{L_p^{\times 2}\mathbb{Q}_p^\times} \end{array}$$

We compute the image of $J(\mathbb{Q}_p) \to \frac{L_p^\times}{L_p^{\times 2}\mathbb{Q}_p^\times}$ for each $p \in S$.

In the example, $S = \{\infty, 2, 5, 402613\}$.

## 1. Description of $L$

The genus-3 curve is in $\mathbb{P}^2$ with coordinates $x, y, z$. In the dual projective space $\check{\mathbb{P}}^2$ with coordinates $u, v, w$, the set of bitangents corresponds to a reduced 0-dimensional subscheme of degree 28. Project this to a line, to get $\operatorname{Spec} L$, where $L = \mathbb{Q}[t]/(g(t))$ where $g(t)$ is a polynomial of degree 28.

The general bitangent is given by

$$\lambda_\theta \colon u_\theta x + v_\theta y + w_\theta z = 0.$$

The map

$$\begin{aligned} J(\mathbb{Q}) &\to \frac{L^\times}{L^{\times 2}\mathbb{Q}^\times} \\ \sum n_P P &\mapsto \prod_P (u_\theta x(P) + v_\theta y(P) + w_\theta z(P))^{n_P}. \end{aligned}$$

## 2. Identification of the image of Galois

Identify $\operatorname{Gal}(g(t))$ as a subgroup of $\operatorname{Sp}_6(\mathbb{F}_2) \subset \mathfrak{S}_{28}$ up to conjugacy. GAP or Magma can list the conjugacy classes of subgroups of $\operatorname{Sp}_6(\mathbb{F}_2)$, and the orbit lengths of the elements.

For the example at hand, we find $\operatorname{Gal}(g(t)) = \operatorname{Sp}_6(\mathbb{F}_2)$; this is as hard as it gets.

## 3. Cassels kernel

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & J[2](\mathbb{Q}) & \longrightarrow & R_{27}^\vee(\mathbb{Q}) & \longrightarrow & R_{21}^\vee(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, J[2]) & \longrightarrow & H^1(\mathbb{Q}, R_{27}^\vee) \\ & & & & & & \uparrow & & \uparrow & & \\ & & & & & & \dfrac{J(\mathbb{Q})}{2J(\mathbb{Q})} & \longrightarrow & \dfrac{L^\times}{L^{\times 2}\mathbb{Q}^\times} & & \end{array}$$

The construction of $R_{28} = (\mathbb{Z}/2\mathbb{Z})^S$ is straightforward. There is a unique $R_{27}$ in $R_{28}$, and a unique $R_{21}$ in $R_{28}$. View $J[2]$ as $R_{27}/R_{21}$. Magma shows that $J[2](\mathbb{Q})$, $R_{27}^\vee(\mathbb{Q})$, $R_{21}^\vee(\mathbb{Q})$ are all 0. Therefore

$$\frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \to \frac{L^\times}{L^{\times 2}\mathbb{Q}^\times}$$

is injective.

When we projected, we were working over $\mathbb{Q}$, but to get the ring of integers of $L$, we should use possibly more than one projection over $\mathbb{Z}$.

## 4. Computing $L(2, S)$

This requires $\mathrm{Cl}(\mathcal{O}_L)$, and GRH is required to verify this computation. In our example, $\mathrm{Cl}(\mathcal{O}_L)$ is trivial (assuming GRH).

## 5. Local computation

We have

$$\frac{\#J(\mathbb{Q}_p)}{2J(\mathbb{Q}_p)} = \frac{\#J[2](\mathbb{Q}_p)}{|2|_p^3}.$$

For $p = 2$, we have

$$L \otimes \mathbb{Q}_2 = \mathbb{Q}_2 \oplus \mathbb{Q}_2 \oplus (\deg 2) \oplus (\deg 8) \oplus (\deg 16).$$

One finds

$$\begin{aligned} \dim J[2](\mathbb{Q}_2) &= 1 \\ \dim R_{27}^\vee(\mathbb{Q}_2) &= 4 \\ \dim R_{21}^\vee(\mathbb{Q}_2) &= 3. \end{aligned}$$

Thus there is no Cassels kernel. Also, by the formula above,

$$\dim \frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)} = 1 - (-3) = 4.$$

To find enough generators of $\frac{J(\mathbb{Q}_2)}{2J(\mathbb{Q}_2)}$, we intersect $C$ with random lines $\ell$ and hope that $C.\ell$ decomposes over $\mathbb{Q}_2$.

For $p = 5$, we find

$$\begin{aligned} \dim J[2](\mathbb{Q}_5) &= 1 \\ \dim R_{27}^\vee(\mathbb{Q}_5) &= 5 \\ \dim R_{21}^\vee(\mathbb{Q}_5) &= 4. \end{aligned}$$

We find

$$\dim \frac{J(\mathbb{Q})}{2J(\mathbb{Q})} \leq 3.$$

This completes the proof that $J(\mathbb{Q})$ has rank 3.

*Remark* 5.1. We did not need the information from the prime 402613, which is lucky since

$$\dim J[2](\mathbb{Q}_{402613}) = 2$$
$$\dim R_{27}^{\vee}(\mathbb{Q}_{402613}) = 7$$
$$\dim R_{21}^{\vee}(\mathbb{Q}_{402613}) = 6,$$

leaving the possibility of a nontrivial Cassels kernel.