On binary quartics and the Cassels-Tate pairing

Tom Fisher

University of Cambridge

Algorithmic Number Theory Symposium, ANTS-XV,
Bristol 9th August 2022

A brief review of 2-descent

$$E/K: \quad y^2 = x^3 - 27Ix - 27J, \quad \text{elliptic curve/number field}$$
$$L = K[\varphi] = K[x]/(x^3 - 3Ix + J), \quad \text{cubic étale algebra}$$

$$E(K)/2E(K) \stackrel{\delta}{\hookrightarrow} \ker\left(L^\times/(L^\times)^2 \xrightarrow{N_{L/K}} K^\times/(K^\times)^2 \right)$$
$$(x,y) \mapsto x + 3\varphi \mod (L^\times)^2$$

Definition. $S^{(2)}(E/K) =$ the subgroup of the RHS consisting of elements that are everywhere locally in the image of δ.

Given $\xi \in S^{(2)}(E/K)$ we consider the equation

$$x + 3\varphi = \xi(u_0 + u_1\varphi + u_2\varphi^2)^2$$

Comparing coefficients of φ and φ^2 and homogenising gives

$$\begin{aligned} 3y^2 &= Q_1(u_0, u_1, u_2), \\ 0 &= Q_2(u_0, u_1, u_2). \end{aligned}$$

Binary quartics and their invariants

Parametrising the conic $Q_2 = 0$ and substituting into Q_1 gives $y^2 = g(x,z)$ where g is a binary quartic. The binary quartic

$$g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

has invariants

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned}$$

Lemma.

$$S^{(2)}(E/K) = \left\{ \begin{array}{c} \text{ELS binary quartics} \\ \text{with the same} \\ \text{invariants as } E \end{array} \right\} / (\text{proper } K\text{-equivalence}).$$

Def$^{\mathbf{n}}$. Binary quartics g_1 and g_2 are *properly K-equivalent* if

$$g_2(x,z) = \lambda^2 g_1(\alpha x + \gamma z, \beta x + \delta z)$$

for some $\lambda, \alpha, \beta, \gamma, \delta \in K$ with $\lambda(\alpha\delta - \beta\gamma) = \pm 1$.

Converting back to an element of $L^\times/(L^\times)^2$

The binary quartic

$$g(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

has Hessian

$$h(x,z) = (3b^2 - 8ac)x^4 + 4(bc - 6ad)x^3z \\ + 2(2c^2 - 24ae - 3bd)x^2z^2 + 4(cd - 6be)xz^3 + (3d^2 - 8ce)z^4.$$

The pencil spanned by $g(x,z)$ and $h(x,z)$ has 3 "singular fibres". More precisely, with $L = K[\varphi]$ as above,

$$\frac{4\varphi g(x,z) + h(x,z)}{3} = \text{constant} \cdot (\text{binary quadratic form})^2$$

The "constant" represents the class in $L^\times/(L^\times)^2$ corresponding to g.

Remark. The procedure for adding two binary quartics in the Selmer group involves solving a conic.

The Cassels-Tate pairing

From the commutative diagram with exact rows

$$\begin{tikzcd} E(K) \arrow[r, "\times 4"] \arrow[d, "\times 2"] & E(K) \arrow[r] \arrow[d, equal] & S^{(4)}(E/K) \arrow[d, "\alpha"] \\ E(K) \arrow[r, "\times 2"] & E(K) \arrow[r] & S^{(2)}(E/K) \end{tikzcd}$$

we see that

$$E(K)/2E(K) \subset \mathrm{Im}(\alpha) \subset S^{(2)}(E/K)$$

The *Cassels-Tate pairing* is an alternating bilinear pairing of $\mathbb{F}_2$-vector spaces

$$\langle\ ,\ \rangle : S^{(2)}(E/K) \times S^{(2)}(E/K) \to \mathbb{F}_2$$

whose kernel is $\mathrm{Im}(\alpha)$.

Methods for computing $\langle\ ,\ \rangle$

- **Cassels, Second descents for elliptic curves, (Crelle 1998)** – has to solve a conic over the field of definition of each 2-torsion point of E.
- **Donnelly, Algorithms for the Cassels-Tate pairing, (preprint 2015)** – only has to solve a conic over K.

Observation. The conic appearing in Donnelly's method for computing $\langle [g_1], [g_2] \rangle$ is the same as that needed to add $[g_1]$ and $[g_2]$.

Idea. Give a simplified formula for the pairing, taking as input binary quartics g_1, g_2, g_3 with $[g_1] + [g_2] + [g_3] = 0$.

N.B. We expect a "simplified formula" since there are no longer any conics to solve.

Recent developments.

- Jiali Yan wrote her PhD thesis (2021) extending some of these ideas to Jacobians of genus 2 curves.
- Bill Allombert has implemented our method for computing the pairing in `pari/gp`.

Method in outline. Let $C_i = \{y^2 = g_i(x,z)\}$ for $i = 1, 2, 3$, represent elements of $S^{(2)}(E/K)$ with $[C_1] + [C_2] + [C_3] = 0$. If $g_2(x,z) = ax^4 + \ldots$ then $[C_2]$ determines an element

$$\mathcal{A} = (K(\sqrt{a})/K, \gamma) \in \mathrm{Br}(C_1)$$

and the pairing is given by

$$\langle [C_1], [C_2] \rangle = \sum_v \mathrm{inv}_v\, \mathcal{A}(P_v) = \sum_v (a, \gamma(P_v))_v$$

where for each place v of K we pick $P_v \in C_1(K_v)$ avoiding the zeros and poles of γ.

Question. How to compute $\gamma \in K(C_1)$?

The $(2,2,2)$-forms

Untwisted version.

$$\begin{tikzcd} E \times E \times E \arrow[r, "\mu"] \arrow[d, "\pi"] & E \\ \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \end{tikzcd}$$

$S = \pi(\mu^{-1}(0_E)) \subset \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ is defined by a $(2,2,2)$-form.

Twisted version. Let $C_i = \{y^2 = g_i(x,z)\}$ for $i = 1,2,3$, represent elements of $S^{(2)}(E/K)$ with $[C_1] + [C_2] + [C_3] = 0$.

$$\begin{tikzcd} C_1 \times C_2 \times C_3 \arrow[r, "\mu"] \arrow[d, "\pi"] & E \\ \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 \end{tikzcd}$$

$S = \pi(\mu^{-1}(0_E)) \subset \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ is defined by a $(2,2,2)$-form.

Twisted version. Let $C_i = \{y^2 = g_i(x,z)\}$ for $i = 1,2,3$, represent elements of $S^{(2)}(E/K)$ with $[C_1] + [C_2] + [C_3] = 0$.

$$\begin{tikzcd} C_1 \times C_2 \times C_3 \arrow[r, "\mu"] \arrow[d, "\pi"] & E \\ \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1 & \end{tikzcd}$$

$S = \pi(\mu^{-1}(0_E)) \subset \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1$ is defined by a $(2,2,2)$-form F_2.

We can compute F_2 using

$$\sqrt{\prod_{i=1}^{3} \left(\frac{4\varphi g_i(x_i,z_i) + h_i(x_i,z_i)}{3} \right)} = F_0 + F_1\varphi + F_2\varphi^2$$

We can compute $\langle \ , \ \rangle$ by taking

$$\gamma(x,z) = F_2(x,z;1,0;1,0)/z^2.$$

THE END