Genus 2 Curves with Split Jacobians

Nils Bruin and Kevin Doerksen
Department of Mathematics
Simon Fraser University
kdoerkse@sfu.ca

1. Background of the Problem

Split Jacobians are special. A genus 2 curve C has a *split Jacobian* if its Jacobian, $J(C)$ is isogenous to the product of two elliptic curves. They can be recognized from the fact that C is a degree n cover of an elliptic curve for some integer n. If $\psi : C \longrightarrow E$ is a degree n cover then we say $J(C)$ is (n, n) split.

Problem. *Let n be a natural number.*

- *Classify all genus 2 curves C with (n, n)-split Jacobians.*
- *Classify the elliptic curves E_1 and E_2 which are subcovers of C and determine the isogeny $E_1 \times E_2 \longrightarrow J(C)$*

The isogeny is of particular interest in number theory as it can be used to visualize elements of the Tate-Shafarevich group of an elliptic curve (see Bruin and Flynn [2] for an example).
This problem has been considered by a number of people. Most notably, Frey and Kani [3] related the problem to maps between projective lines. The case for $n = 2$ is known; $n = 3$ was solved by Kuhn [4] and Shaska [5] over $\bar{\mathbb{Q}}$, and recently $n = 5$ has been solved in a preprint by Shaska, Magaard and Völklein). Arikushi [1] generalized the $n = 3$ result to arbitrary fields by providing the correct twist on the curves.

2. The construction

Let C be a genus two curve with a (n, n)-split Jacobian and let E_1 and E_2 be two elliptic curves whose direct product is isogenous to $J(C)$. Then there are degree n covers ψ_1 and ψ_2 from C to E_1 and E_2 respectively.
Let $\pi_C : C \longrightarrow \mathbb{P}^1$ and $\pi_i : E_i \longrightarrow \mathbb{P}^1$ be the natural degree 2 projections for $i \in \{1, 2\}$. Frey and Kani [3] and Kuhn [4] showed that exist covers ϕ_1 and ϕ_2 such that the following diagram commutes.

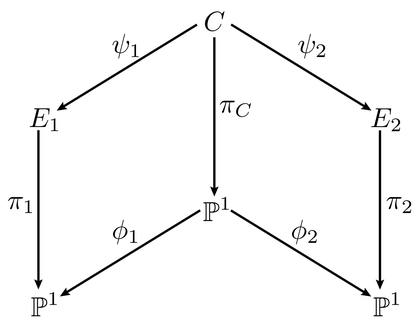

Figure 1: *Commutative diagram*

The genera of E_1, E_2, and C impose relations between the ramification of the maps in Figure 1. Let $i \in \{1, 2\}$:

- π_C is ramified at the Weierstrass points of C.
- π_i is ramified at the 2-torsion points of E_i.
- By using the Riemann–Hurwitz formula, we find there are 2 ramification points to distribute in the ψ_i cover and $2n - 2$ ramification points to distribute in the ϕ_i cover.

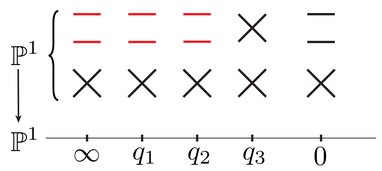

Figure 2: *One possible configuration of the ramification points of ϕ_1 for $n = 4$. The red lines correspond to the 6 Weierstrass points of C, and the X's are the 6 ramified points of ϕ_1. π_1 is ramified over q_1, q_2, q_3, and ∞.*

3. The case $n = 4$

In order to deal with the degree 4 case, we observe that every pair of elliptic curves which have isomorphic 4-torsion would also have isomorphic 2-torsion. So if E_1 and E_2 were two elliptic curves with isomorphic 4-torsion, then there exist genus two curves C_2 and C_4 such that $E_1 \times E_2$ is 2-isogenous to $J(C_2)$ and is 4-isogenous to $J(C_4)$ respectively. The obvious question is whether there is some sort of correspondence between C_2 and C_4.

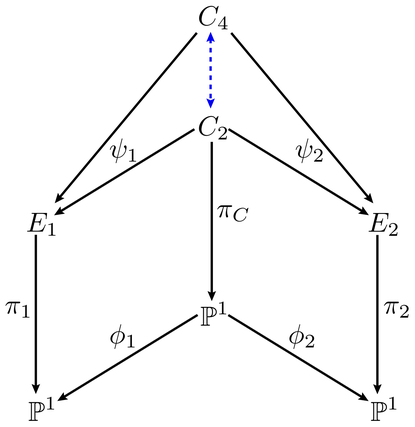

Figure 3: *Finding a connection between the two genus two curves*

By using the isogenies between $E_1 \times E_2$ and the two Jacobians of C_2 and C_4, we have:

$$E_1 \times E_2 \overset{4}{\longleftrightarrow} J(C_2)$$
$$E_1 \times E_2 \overset{16}{\longleftrightarrow} J(C_4)$$

If there were an isogeny between $J(C_2)$ and $J(C_4)$, by the above set up, it would have to have a kernel of order 4:

$$E_1 \times E_2 \overset{4}{\longleftrightarrow} J(C_2) \overset{4}{\longleftrightarrow} J(C_4)$$

Such an isogeny exists between $J(C_2)$ and $J(C_4)$; it is a *Richelot isogeny*. A Richelot isogeny splits multiplication by two on the Jacobian and can be described by a 2 by 2 correspondence between C_2 and C_4. The form of genus 2 curves which admit Richelot isogenies is known. By using the Richelot isogeny, we were able to characterize genus two curves C_4 which are degree 4 covers of an arbitrary elliptic curve.

Let E_1 be an elliptic curve over k with defining equation $E_1 : v^2 = u^3 + bu + c$ for arbitrary scalars $b, c \in k$. Then an appropriate elliptic curve E_2 with isogenous 4-torsion is given by:

$$E_2 : y^2 = x^3 + \frac{3a^2 + b}{d}x^2 + \frac{3a}{d}x + \frac{1}{d}$$

where

$$a = \frac{b^2s^4 + 8cs^3 + 2bs^2 - 1}{4s\left(cs^3 + bs^2 + 1\right)}$$
$$d = a^3 + ab + c$$

and s is a free parameter.
The genus 2 curve C_4 whose Jacobian is 4-isogenous to $E_1 \times E_2$ has similar defining equations in one free parameter s. Unfortunately, these equations are far too large to fit on this poster, so we present a worked example instead.

3.1 A worked example

For simplicity, we begin with an elliptic curve which is a degree 2 subcover of a genus 2 curve that has rational Weierstrass points.

$$\begin{aligned} E_1 : v^2 &= u^3 - \frac{1162084}{3}u - \frac{1044547504}{27} \\ &= \left(u - \frac{2002}{3}\right)\left(u + \frac{308}{3}\right)\left(u + \frac{1694}{3}\right) \end{aligned}$$

A genus 2 curve which is a degree 2 cover of E_1 is given by:

$$\begin{aligned} C_2 : z^2 &= w^6 - \frac{1400}{9}w^4 + \frac{490000}{81}w^2 - \frac{4000000}{81} \\ &= (w - 10)\left(w - \frac{20}{3}\right)\left(w - \frac{10}{3}\right)\left(w + \frac{10}{3}\right)\left(w + \frac{20}{3}\right)(w + 10) \end{aligned}$$

We can then obtain a genus 2 curve which is a degree 4 cover of E_1 is given by:

$$C_4 : y^2 = \left(x^2 + \frac{100}{3}x + \frac{1300}{9}\right)\left(x^2 - \frac{10}{3}x - \frac{350}{9}\right)\left(x^2 - \frac{60}{7}x + \frac{100}{21}\right)$$

The degree 4 covering map from $\mathbb{P}^1$ to $\mathbb{P}^1$ is given by:

$$u = \frac{1694}{75} \cdot \frac{3807x^4 - 32400x^3 + 77400x^2 - 3970000}{(3x - 26)^2\left(9x^2 + 300x + 1300\right)}$$

This cover map has the configuration of ramification points that is displayed in Figure 2, where $q_1 = \frac{2002}{3}$, $q_2 = -\frac{308}{3}$, $q_3 = -\frac{1694}{3}$.

4. References

[1] K. Arikushi, Elliptic Curves with isomorphic 3-torsion over $\mathbb{Q}$. *Report* (2005) see http://www.math.sfu.ca/numthry/report/2005oct16.pdf
[2] N. Bruin and E. V. Flynn, Exhibiting SHA[2] on hyperelliptic Jacobians. *J. Number Theory* **118** (2006), no. 2, 266–291.
[3] G. Frey and E. Kani, Curves of genus 2 covering elliptic curves and an arithmetic application. *Arithmetic algebraic geometry* (*Textel* 1989), 153–176, *Progr. Math.,* 89, Birkhäuser Boston, MA, 1991
[4] M. R. Kuhn, Curves of genus 2 with split Jacobian. *Trans. Amer. Math. Soc.* **307**, 41–49, 1988.
[5] T. Shaska, Genus 2 fields with degree 3 elliptic subfelds. *Forum Math.,* vol **16**, 2, 263–280, 2004.