TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 307, Number 1, May 1988

CURVES OF GENUS 2 WITH SPLIT JACOBIAN

ROBERT M. KUHN

ABSTRACT. We say that an algebraic curve has *split jacobian* if its jacobian is isogenous to a product of elliptic curves. If X is a curve of genus 2, and $f\colon X \to E$ a map from X to an elliptic curve, then X has split jacobian. It is not true that a complement to E in the jacobian of X is uniquely determined, but, under certain conditions, there is a canonical choice of elliptic curve E' and algebraic $f\colon X \to E'$, and we give an algorithm for finding that curve. The construction works in any characteristic other than two. Applications of the algorithm are given to give explicit examples in characteristics 0 and 3.

0. Introduction. We say that a curve has *split jacobian* if its jacobian is isogenous to a product of elliptic curves. In the later half of the nineteenth century a considerable body of work was done on the reduction of abelian integrals to elliptic. Krazer [**1**] gives a summary of the results obtained. Stated geometrically, the results are particular families of algebraic curves of genus 2 with maps of degree 2, 3 or 4 to elliptic curves. Such curves have split jacobian. The general question of split jacobian curves and particularly, those of genus 2, is of interest for several reasons. Split jacobian curves often have the maximal number of points over finite fields, e.g. the examples of Moret-Bailley [**2**] are one parameter families of curves of genus 2 over fields of order p^2 whose jacobians are isomorphic to the square of the supersingular elliptic curve, and which have maximal numbers of points over fields of order p^{2n}, $n \geq 2$. Split jacobian curves of genus 2 have also been used to exhibit nonisomorphic curves with the same jacobian; vide [**3, 4**]. The approach in these papers is through the algebraic geometry of abelian varieties, and the constructions are therefore far from explicit.

Consider the following: Let X be a curve of genus 2, and $f\colon X \to E$ a map from X to an elliptic curve. The jacobian of X is therefore isogenous to a product of E and another elliptic curve, E'. *Problem*: find E', e.g. what is its j-invariant?

It is not clear, nor even true (vide T. Shioda [**7**]), that E' is uniquely determined. However, under certain conditions there is a canonical choice of complement, and we give an algorithm for finding that curve. Our aim is to provide explicit equations for the curves and the maps between them.

We obtain a fairly complete combinatorial characterization of the splitting of the jacobians of curves of genus 2. The splitting is characterized by the degree of the map f above. Jacobi, generalizing an example of Legendre, gave the complete solution for degree 2. Given any involution of $\mathbf{P}^1$, and three points not fixed by the involution, the curve of genus 2 which has its 6 Weierstrass points above the three points and their images under the involution, maps to the two elliptic curves represented as double covers of the quotient of $\mathbf{P}^1$ by the involution, ramified at

Received by the editors July 20, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 14H40, 11G10.

the images of the three points and one of the two fixed points of the involution. Krazer attributes the results obtained for degree 3 to Hermite, Goursat, Burckhardt, Brioschi, and Bolza. They obtained the generic family of such curves, but did not obtain all the special cases. For higher degree, there is considerable effort involved in obtaining explicit results.

NOTATION. The symbol k is used throughout for a field of characteristic $p \neq 2$. If X is an algebraic curve, by $X(k)$ we mean the k-rational points of X. To indicate that any object, X, is defined over the field k, we write $X_{/k}$. If σ is an automorphism of X, then X^σ is the quotient of X under the action of the group generated by σ. The jacobian of X, $\mathrm{Jac}(X)$, is viewed as the linear equivalence classes of divisors of degree zero. If P_i are points of X, we represent a divisor D by $D = \sum n_i(P_i)$, $n_i \in \mathbf{Z}$. If D is a divisor of degree zero we write $[D]$ for the linear equivalence class of D which is therefore a point of $\mathrm{Jac}(X)$. We use g_X for the genus of X. Given a map $f\colon X \to E$, e_P is the ramification degree of f at $P \in X$ and we define the divisor R_f of f to be

$$R_f = \sum_{P \in X} (e_P - 1)(P).$$

When f is tamely ramified, this is the usual ramification divisor.

1. Coverings of curves of genus 1 by curves of genus 2.

LEMMA. *Let k be a field of characteristic $p \neq 2$. Let $X_{/k}$ be a hyperelliptic curve of genus $g \geq 2$ covering $E_{/k}$ a curve of genus 1 by a map $f_{/k}\colon X \to E$. Let ι be the unique hyperelliptic involution on X. Then ι induces a k-rational involution on E, with quotient of genus 0. The fixed points of X under ι lie over the fixed points of E under ι.*

PROOF. Let x_0 be a fixed point of $X(\bar{k})$ under ι and let $e_0 = f(x_0)$. Embed X and E in their respective jacobians via $x \mapsto [(x) - (x_0)]$ and $e \mapsto [(e) - (e_0)]$. Consider the following commutative diagram:

$$\begin{tikzcd}
X \arrow[r] \arrow[d, "f"] & \mathrm{Jac}(X) \arrow[d, "f_*"] \\
E \arrow[r, "\sim"] & \mathrm{Jac}(E)
\end{tikzcd}$$

Because of the choice of embeddings, the hyperelliptic involution, ι, on X induces the involution $-1 \in \mathrm{End}(\mathrm{Jac}(X))$ and hence induces the involution -1 on $\mathrm{Jac}(E) \simeq E$. Hence, there is an involution ι_E on E compatible with f and ι. Since ι_E is -1 on $\mathrm{Jac}(E)$, the genus of E^ι is 0. A simple argument shows that ι_E is defined over k. □

Let k be a field such that $\mathrm{char}(k) \neq 2$, and let $f_{/k}\colon X_{/k} \to E_{/k}$ be a function of degree d from a curve of genus 2 to a curve of genus 1. Also, let ι stand for both the hyperelliptic involution on X and the induced involution on E, and let X^ι and E^ι be the curves of genus 0 obtained from X and E respectively by taking the quotient by the involution. Consider the ramification of each map in the following commutative diagram:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi_X"] & E \arrow[d, "\pi_E"] \\ X^\iota \arrow[r, "f^\iota"] & E^\iota \end{tikzcd}$$

In this diagram we know that π_X ramifies at 6 points, $C_1, C_2, ..., C_6$, which lie over the 4 ramification points, D_1, D_2, D_3, D_4, of π_E. Suppose f is unramified over the 4 D_i, then $\pi_E \circ f$ has $4d$ double ramification points over them. $\pi_E \circ f = f^\iota \circ \pi_X$. Now, π_X is ramified at exactly 6 points, hence f^ι is doubly ramified at the $2d-3$ points over the D_i, other than the C_j. On the other hand, by Riemann-Hurwitz

$$2 - 2g_{X^\iota} = d(2 - 2g_{E^\iota}) - \deg(R_{f^\iota}) - W$$

(where W is the contribution for wild ramification), and hence

$$\deg(R_{f^\iota}) + W = 2d - 2.$$

We have therefore located nearly all of the ramification of f^ι, in the sense that, if f is unramified above the D_i, then f^ι has $2d-2$ double ramification points, $2d-3$ above the images, d_i, of the D_i, and one other. If f is ramified above the D_i, then all of the ramification of f^ι lies above the d_i.

LEMMA. *Let C_j, $j = 1,2,3,4,5,6$, be the Weierstrass ramification points of X, and D_i, $j = 1,2,3,4$, be the ramification points of E over E^ι. Let c_j and d_i be the images of these points in X^ι and E^ι, then $\{(f^\iota)^{-1}(d_i)\}$ contains c_j with odd multiplicity for each j and any other points of X^ι with even multiplicity. In terms of divisors,*

$$f^{\iota *}\left(\sum d_i\right) = \sum c_j \pmod 2.$$

PROOF. We prove this lemma by recourse to the function fields of the various curves over the algebraic closure, $\bar{k}$, of the field of definition. We view these function fields as subfields of $\bar{k}(X)$. If u is a parameter on X^ι, and s is a parameter on E^ι, then s is given by a rational function of u, $s = f^\iota(u) = \frac{A(u)}{B(u)}$. Without loss of generality, we may suppose $\bar{k}(X) = \bar{k}(u,v)/(v^2 = P(u))$, where P is a polynomial of degree 6, and $\bar{k}(E) = \bar{k}(s,t)/(t^2 = D(s))$, where D is a polynomial of degree 4.

Now the subfield of $\bar{k}(X)$ fixed by ι is $\bar{k}(u)$, and the subfield of $\bar{k}(E)$ fixed by ι is $\bar{k}(s)$. We also have $\iota(v) = -v$ and $\iota(t) = -t$, hence $\iota(\frac{t}{v}) = \frac{t}{v}$. Thus, $\frac{t}{v} \in \bar{k}(u)$ say, $\frac{t}{v} = \frac{E(u)}{F(u)}$.

Therefore,

$$t^2 = v^2 \, \frac{E(u)^2}{F(u)^2} = P(u)\frac{E(u)^2}{F(u)^2}$$

The zeros of the right-hand side are the points of X^ι over the d_i, and since $P(u)$ has multiplicity 1 at each c_j, the lemma is proved. □

The previous lemma severely restricts the ramification picture for X^ι over E^ι.

Suppose $d = \deg(f) = \deg(f^\iota)$ is odd, then there are an odd number of c_j above each d_i, hence there is a distinguished d_i, say d_1, such that $(f^\iota)^{-1}(d_1)$ contains three of the c_j, while the remaining d_i are such that there is a unique c_j above each.

If f has even degree, the situation is more complicated, since an even number of c_j then lie over each d_i. There are thus three ways the c_j can lie over the d_i, either

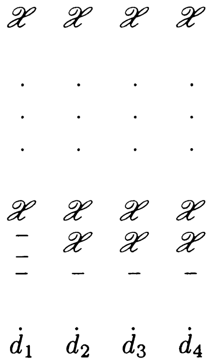
(1) $(f^\iota)^{-1}(d_2) \supset c_1, c_2, (f^\iota)^{-1}(d_3) \supset c_3, c_4$ and $(f^\iota)^{-1}(d_4) \supset c_5, c_6$.

(2) $(f^\iota)^{-1}(d_2) \supset c_1, c_2, c_3, c_4$ and $(f^\iota)^{-1}(d_1) \supset c_5, c_6$.

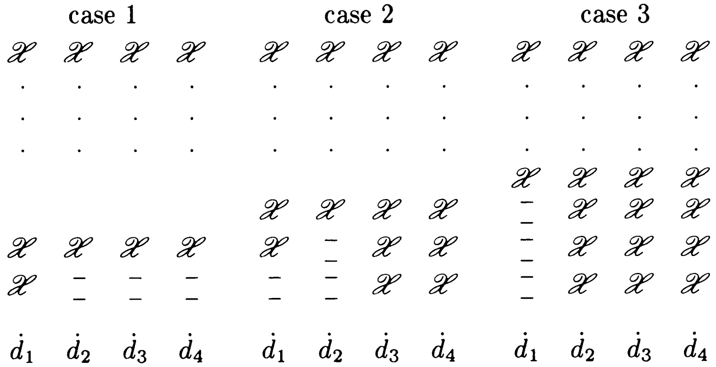
(3) $(f^\iota)^{-1}(d_1) \supset c_1, c_2, c_3, c_4, c_5, c_6$.

We can summarize the data above with the following ramification pictures for $f^\iota\colon X^\iota \to E^\iota$. In the diagrams, – represents an unramified point of X^ι over one of the d_i, which is therefore one of the c_j, and $\mathscr{X}$ represents a doubly ramified point.

odd degree



even degree



These diagrams show the ramification of f^ι over the d_i, assuming that f is unramified over the D_i; we might call this the "generic" picture. The ramification divisor of f^ι is of degree one greater than represented by the diagrams above. We now state the combinatorial characterization of f^ι in the following theorems.

THEOREM (GENERIC). *If f is unramified over the D_i, the ramification of f^ι over the d_i is one of the cases above. There is one more point of X^ι at which f^ι is doubly ramified.*

THEOREM (SPECIAL). *If f is ramified over some D_i, then the ramification of f^ι over the d_i is one of the cases except that either:*

(i) *One of the c_j has ramification degree* 3, *or*

(ii) *There is a unique point, not one of the c_j, with ramification degree* 4.

We note in passing that all three even degree cases occur. If $d = 2$ then the only possible case is case 1. If $f\colon X \to E$ is such a map, E can be given the structure of an elliptic curve by choosing the origin to be at d_1. Then the composition of f with the quotient by a subgroup of order 2 gives an example of case 2, and the composition of f with the quotient by the subgroup of all of the points of order 2 gives an example of case 3. An interesting question we answer later is whether there are any "primitive" examples of cases 2 and 3.

COROLLARY. *Let k be a number field, and let X be a curve of genus 2 defined over k. If there exists a map f from X to a curve E of genus 1, where f and E are both defined over k, then E has a k-rational point.*

PROOF. In each case above, the ramification picks out a distinguished d_1, hence d_1 is rational on E^ι and therefore D_1 is rational on E. □

REMARK. *Since the highest ramification degree possible is 4, wild ramification can only occur in characteristics 2 and 3. It is only in the characteristic 2 case that a nonzero Swann conductor is possible.*

Suppose we are given a map $f^\iota\colon P^1 \to P^1$ with one of the ramification pictures above, then f^ι clearly lifts to $f\colon X \to E$. Given X, the existence of f^ι from $X^\iota \to P^1$ lifting to a map from X to an elliptic curve is an algebraic condition in terms of the hyperelliptic points c_j of X^ι.

2. The complement to an elliptic curve in the Jacobian of a genus 2 curve.

DEFINITION. *Let k be a field with algebraic closure $\bar{k}$. We say that a k-rational map f from a curve X defined over k to an elliptic curve E defined over k is optimal if, whenever there exist an elliptic curve E' defined over $\bar{k}$ and maps g from X to E' and h from E' to E, both defined over $\bar{k}$ whose composition is f, then deg $(h) = 1$.*

LEMMA. *Let $X_{/k}$ be a nonsingular projective curve of genus 2 and $E_{/k}$ be an elliptic curve, both defined over k. If $f\colon X \to E$, of degree d, is optimal, then there exists a pair (E', f'), where E' is an elliptic curve and f' is an optimal map from X to E'. Moreover:*

(1) $\deg(f') = d$.

(2) $\mathrm{Jac}(X) = J$ *is isogenous to the direct sum $E \oplus E'$, ($J \simeq E \oplus E'$). Moreover the isogeny is given by the following:*

$$0 \to K \to E \oplus E' \to J \to 0$$

where $K = \ker(f^* + f'^*)$*, and*

(3) *K is isomorphic to the group of points of order d on E or E'.*

PROOF. Embed X in its jacobian J, by $x \mapsto [(x) - (x_0)]$, where x_0 is one of the 6 Weierstrass points of X. We could equally well embed X in its jacobian using any divisor D of degree 1 invariant under the hyperelliptic involution by $x \mapsto [(x) - D]$. Define E' and g by the following exact sequence of abelian varieties:

$$0 \to E' \xrightarrow{g} J \xrightarrow{f_*} E \to 0. \qquad (1)$$

REMARK. E' is connected because f is optimal. The dual sequence is also exact, i.e.

$$0 \to E \xrightarrow{f^*} J \xrightarrow{g'} E' \to 0. \tag{2}$$

Define $f'\colon X \to E'$ by composing the embedding of X in J with g', then $g = f'^*$ and $g' = f'_*$. The exactness of (2) requires the optimality of f'.

Now consider the map $f^*\colon E \to J$, and hence the map

$$f^* + g\colon E \oplus E' \to J.$$

This map is clearly onto, with some finite kernel K. Thus the following sequence is exact:

$$0 \to K \to E \oplus E' \to J \to 0.$$

Now

$$\begin{aligned} K &= E \cap E' = \operatorname{Im}(f^*) \cap \operatorname{Im}(f'^*) \\ &= \operatorname{Im}(f^*) \cap \ker(f_*) \\ &= \ker(f_* f^*) = \text{the points of order } d \text{ on } E. \quad \square \end{aligned}$$

Observe that if X, E, and f are all defined over a field k, E' will be canonical and therefore defined over k. On the other hand we have only established the existence of the canonical map f' over $k(x_0)$ where x_0 is one of the hyperelliptic ramification points of X, or more precisely, over any field in which an embedding of X in its jacobian is defined.

3. The Weil pairing. As the results of the previous two sections show, the odd and even degree cases of optimal maps from a curve of genus 2 to an elliptic curve are considerably different. Not only are the ramification pictures different but also, since the ramification points of the curve of genus 2 project to the points of order 2 on the elliptic curve, they fall into the kernel of the isogeny between the product of elliptic curves and the jacobian of the curve of genus 2, if and only if the degree is even. We therefore treat the two cases separately. Let $f\colon X \to E$ be an optimal (k-)rational map from a curve of genus 2 to a curve of genus 1. We have seen that E will therefore have a distinguished rational point D_1, and we identify E and $\operatorname{Jac}(E)$ via the rational isomorphism $e \mapsto [(e) - (D_1)]$. The hyperelliptic involution ι on X induces -1 on both X and E, and the (not necessarily rational) points of order 2 on E are D_2, D_3 and D_4. The (not necessarily rational) hyperelliptic ramification points of X are C_1, C_2, C_3, C_4, C_5, and C_6, and lie above the D_i.

The 15 distinct divisor classes

$$[(C_i) - (C_j)], \qquad 1 \le i < j \le 6,$$

are the 15 points of order 2 on $\operatorname{Jac}(X)$. Let us represent them by the unordered pair (i, j). For distinct i, j, k, l, m and n, the addition law is given by

$$(i,j) + (i,j) = 0, \quad (i,j) + (k,l) = (m,n), \quad (i,j) + (i,k) = (j,k).$$

The Weil pairing on the points of order 2 on $\operatorname{Jac}(X)$ is given by (see Mumford [**6**]):

$$\langle (i,j),(i,j) \rangle = +1, \quad \langle (i,j),(k,l) \rangle = +1, \quad \langle (i,j),(i,k) \rangle = -1.$$

4. Optimal maps of odd degree. We now restrict attention to $f: X \to E$ of odd degree. We observe that three of the C_i, without loss of generality C_1, C_2, and C_3, lie over D_1 and hence the divisor $C_1 + C_2 + C_3$ is effective, hence X^ι is rationally isomorphic to $\mathbf{P}^1$, and we can write $X: y^2 = P(x)$ with $P(x)$ a sextic rational polynomial. The rationality of D_1 then entails that $P(x)$ is the product of two cubics, $A(x)$ and $B(x)$, where the roots of $A(x)$ are c_1, c_2, and c_3 and lie over d_1. The canonical divisor $K = 2(C_i)$ is of course effective, so the divisor $(C_1) - (C_2) + (C_3)$ is effective, and moreover its divisor class is uniquely determined, since it is equal to the class of $(C_i) - (C_j) + (C_k)$, where $\{i, j, k\} = \{1, 2, 3\}$ or $\{4, 5, 6\}$. We can therefore conclude:

THEOREM. *Given $f: X \to E$ a rational optimal map of odd degree from a curve of genus 2 to a curve of genus 1, there is a rational embedding of X in its jacobian, canonically determined by f; namely,*

$$x \mapsto [(x) - (C_1) + (C_2) - (C_3)].$$

COROLLARY. *There is a uniquely determined rational, optimal map f' from X to the canonical complement E' of E in* Jac(X) *whose degree is the same as that of f.*

SYMMETRY PRINCIPLE. *If $f: X \to E$ is optimal of odd degree, then f' is obtained by exchanging the roles of the cubics $A(x)$ and $B(x)$.*

The image of C_i in Jac(X) is (j, k) where $\{i, j, k\} = \{1, 2, 3\}$ or $\{4, 5, 6\}$. Since we are considering f of odd degree, the isogeny between Jac(X) and $E \oplus E'$ is an isomorphism on points of order 2. We use the same names for the maps restricted to the points of order 2, thus

$$f_* + f'_*: J_2 \to E_2 \oplus E'_2 \quad \text{and}$$
$$f^* + f'^*: E_2 \oplus E'_2 \to J_2, \text{ are isomorphisms.}$$

Since $f^{-1}(D_1) = \{C_1, C_2, C_3\}$, we have that

$$f_*^{-1}(0) = \{(1,2), (2,3), (1,3)\}$$

and the statement that f' is obtained by exchanging the roles of the two cubics is equivalent to

$$f'^{-1}_*(0) = \{(4,5), (5,6), (4,6)\}.$$

Suppose $(i, j) \in f'^{-1}_*(0)$, we compare the Weil pairings on E'_2 and J_2.

$$\langle f'_*(i,j), D_2\rangle = \langle (i,j), f'^*(D_2)\rangle,$$

but $f'_*(i,j) = 0$, hence $\langle (i,j), f'_*(D_2)\rangle = 1$, and similarly for D_3 and D_4. But $\{f'_*(D_k)\}_{k=3,4,5}$ is $\{(1,2), (2,3), (1,3)\}$ and the result follows from the Weil pairing.

If $f: X \to E$ is of odd degree, then the determination of f, f', E, and E' is purely combinatorial and algorithmic.

5. Optimal maps of even degree. In the even degree case we cannot define the same canonical embedding of X in its jacobian. The optimality of f implies that E injects into Jac(X), and on the points of order 2, the image of f^* is the kernel of f_*. The kernel of f_* on points of order 2 therefore contains 0 and three of the divisor classes (i, j) forming a subgroup. Without loss of generality, $(1, 2) \in \ker(f_*)$.

If $(1,k) \in \ker(f_*)$, then $\ker(f_*) = \{0,(1,2),(1,k),(2,k)\}$, but then embedding X in its jacobian via $x \mapsto [(x)-(C_1)]$, we obtain $f^{-1}(0) = \{C_1, C_2, C_k\}$ which contradicts the ramification pictures for even degree. Hence, up to renumbering, $\ker(f_*) = \{0,(1,2),(3,4),(5,6)\}$. Since exactly two hyperelliptic ramification points of X lie over 0_E for each embedding of X in $\mathrm{Jac}(X)$ of the form $x \mapsto [(x)-(C_i)]$, we have shown that only the first ramification pattern for f of even degree can occur for an optimal map. Since the images of the points of order 2 on the elliptic curves E and E' are the same, the ramification picture for f'^{ι} is determined by that for f^{ι}, and again we get an algorithmic construction.

6. Example: Parametrizing splittings of degree 3. Using the results above, it is straightforward, (particularly with the aid of a computer symbolic manipulation program), to parametrize the curves of genus 2 which split with degree 3. Let X be a curve of genus 2 defined over a number field k, and suppose that $f\colon X \to E$ is not special in the sense of §1. The ramification point of f which is not over a point of order 2 on E is rational, as is the other point over its image. By a linear fractional transformation on X^{ι}, these points can be moved to 0, and ∞, i.e. we may suppose that $f^{\iota}\colon X^{\iota} \to E^{\iota}$ is given by

$$t = \frac{x^2}{x^3 + ax^2 + bx + c}.$$

The planar model for X is then

$$X\colon y^2 = (x^3 + ax^2 + bx + c)(4cx^3 + b^2x^2 + 2bcx + c^2).$$

The denominator of the other map is, therefore

$$4cx^3 + b^2x^2 + 2bcx + c^2,$$

and its numerator is

$$(x-d)^2(x-e)$$

where

$$d = \frac{-3c}{b} \quad \text{and,} \quad e = \frac{3ac^2 - b^2c}{9c^2 - 4abc + b^3}.$$

The j-invariants of the curves are

$$j(E) = \frac{16(972ac^3 - 405b^2c^2 - 216a^2bc^2 + 126ab^3c - 12b^5 - a^2b^4)^3}{(27c^2 - b^3)^3(27c^2 - 18abc + 4a^3c + 4b^3 - a^2b^2)^2},$$

$$j(E') = \frac{256(3b - a^2)^3}{27c^2 - 18abc + 4a^3c + 4b^3 - a^2b^2}.$$

There is a unique isomorphism class of curves of genus 2 with both functions special, namely,

$$y^2 = (3x^2 + 4)(x^3 + x).$$

Here the two maps are given by

$$t = \frac{x^3}{3x^2 + 4} \quad \text{and,} \quad t = \frac{1}{x^3 + x}.$$

The two elliptic curves then both have j-invariant 1728.

7. Example: The Moret-Bailley family of curves for $p = 3$. Moret-Bailley [**2**] gives a "construction" of a one parameter family X of curves of genus 2 over the prime fields $\mathbf{F}_p$ whose jacobians are isomorphic to the square of a supersingular elliptic curve E. Such supersingular curves of genus 2 are discussed in more generality by Ibukiyama, Katsura and Oort [**5**]. The optimal maps from X to E are of degree p. By means of the results above, and some computation, we give the explicit equations in the characteristic 3 case. Consequently, let

$$E\colon w^2 = z^3 - z$$

be the supersingular elliptic curve over $\mathbf{F}_3$. Then there is a $\mathbf{P}^1$-family of covers with parameter a given by

$$z = \frac{x^2(x-a)}{ax+a+1}, \quad w = y\frac{x(x-1)}{(ax+a+1)^2}$$

with obvious singularities at $a = 0, 1, -1, \infty$. The corresponding curve of genus 2 has model

$$X\colon y^2 = (x-a)(x-a-1)(ax+a+1)(x^3 - ax^2 + ax + a + 1).$$

There is then another map from X to another elliptic curve, E', given by

$$t = \frac{x^2 - (a^5+1)x + a^4(a+1)^2}{a^3(x-a)(x-a-1)(ax+a+1)},$$

$$s = a^5 y \frac{x^3 + (a^5 - a)x^2 + (a^5 - a^4 + a^3 + a^2 + 1)x + (a+1)^7}{(x-a)(x-a-1)(ax+a+1))^2}$$

yielding the elliptic curve

$$E'\colon s^2 = -a\left(t^3 + t - \frac{1}{a^9}\right).$$

Over $\mathbf{F}_9(a)$ this curve is isomorphic to E.

References

1. A. Krazer, *Lehrbuch der Thetafunctionen* Chelsea, New York, 1970.
2. L. Moret-Bailley, *Familles de courbes et de variétés abeliennes sur* $\mathbf{P}^1$, Asterisque **86** (1981), 109–124.
3. T. Hayashida and M. Nishi, *Existence of curves of genus two on a product of two elliptic curves*, J. Math. Soc. Japan **17** (1965), 1-16.
4. T. Hayashida, *A class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan **20** (1968), 26-43.
5. T. Ibukiyama, T. Katsura and F. Oort, *Supersingular curves of genus two and class numbers*, Compositio Math. **57** (1986), 127–152.
6. D. Mumford, *Tata lectures on theta*, Birkhäuser, Boston, Mass., 1984.
7. T. Shioda, *Some remarks on abelian varieties*, J. Fac. Sci. Univ. Tokyo **24** (1977), 11–21.

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138