Elliptic Curves with isomorphic 3-torsion over $\mathbb{Q}$

Karin Arikushi

October 16, 2005

Abstract

Let C be a genus 2 curve over $\mathbb{Q}$, and let E_1 and E_2 be non-isomorphic elliptic curves over $\mathbb{Q}$, such that C is a degree 3 cover of E_1 and E_2. Then, in a certain case E_1 and E_2 have isomorphic 3-torision structure over $\mathbb{Q}$. We will study such elliptic curves and find explicit equations describing C, E_1, E_2 and the covers. We will also find expressions for C, E_2 and the covers, in terms of the coefficients of the equation defining the elliptic curve E_1.

1 Introduction

During the summer semester of 2005, I was given the opportunity to do an undergraduate research term with Dr. Nils Bruin at Simon Fraser University. I will provide a summary of the work done, which mainly involved studying elliptic curves with isomorphic 3-torsion subscheme over the field of rational numbers. These arise when considering certain degree 3 coverings of an elliptic curve by a genus 2 curve. These coverings have been studied in the degree n case extensively by Gerhard Frey, Ernst Kani, Robert Kuhn, and Tony Shaska.

$$\begin{tikzcd}
& C \arrow[dl, "\psi_1"'] \arrow[dr, "\psi_2"] \arrow[dd, "\pi_C"] & \\
E_1 \arrow[dd, "\pi_1"] & & E_2 \arrow[dd, "\pi_2"] \\
& \mathbb{P}^1 \arrow[dl, "\phi_1"] \arrow[dr, "\phi_2"'] & \\
\mathbb{P}^1 & & \mathbb{P}^1
\end{tikzcd}$$

Let C be a genus 2 curve and E_1 an elliptic curve such that $\phi_1 : C \to E_1$ is a degree 3 covering. If π_1 and π_C are specific coverings of the projective line (which we define later), then there exists an induced covering ϕ_1 such that the left half of the diagram above commutes. We call this induced covering the Frey-Kani cover. When ψ_1 is "non-degenerate", C covers another elliptic curve E_2 with degree 3, and induces another Frey-Kani cover so that the whole diagram commutes. When this occurs, E_1 and E_2 have isomorphic 3-torsion structure over $\mathbb{Q}$, (Frey and Kani, [2]).

We begin by providing some basic definitions and results involving elliptic curves, genus 2 curves, and coverings. Then we give a summary of work done by the mentioned authors, but we will only consider the case when the covering is degree 3. For the most part, we are concerned with which genus 2 curves can form covers of elliptic curves in this way, and what the expressions for the Frey-Kani coverings and elliptic curves are. Finally, we finish with the results of our investigations.

In their study of coverings of elliptic curves, the authors we mentioned worked mostly over an algebraically closed field, such as $\mathbb{C}$. We were able to find explicit equations for the elliptic curves E_1 and E_2 over $\mathbb{Q}$. Also, given an elliptic curve E_1 over $\mathbb{Q}$, we found explicit relations defining $\phi_1 : C \to E_1$ in terms of the coefficients of E_1, and found that the parameters for our genus 2 curve C are given by a genus zero curve, which has a rational point.

2 Preliminaries

We begin with a discussion of elliptic curves and describe some of their basic properties.

Definition 1. An elliptic curve E over a field K is a nonsingular cubic curve in two variables, $f(x, y) = 0$, together with a K-rational point. When $\text{char}(K) \neq 2, 3$ we can write E in short Weierstrass form as

$$E : y^2 = x^3 + ax + b \text{ where } a, b \in K.$$

The set of points $(x_0, y_0) \in K \times K$ that satisfy $f(x_0, y_0) = 0$ are the points on E over K, and is denoted $E(K)$.

Although we will not go into the details here, it is possible to define an "addition" operation on the points of an elliptic curve. Under this addition operation, the set of points forms a group, where the identity $\mathcal{O}$, is usually taken to be the point at infinity. We are interested in the set of 3-torsion points; the points P such that $P + P + P = \mathcal{O}$.

Definition 2. The set

$$E(K)[n] = \{P \in E(K) : nP = \mathcal{O}\}$$

is the n-torsion group of E over K.

Lemma 1. *For any elliptic curve E over an algebraically closed field K,*

$$E(K)[n] \cong \mathbb{Z}/n \times \mathbb{Z}/n.$$

Lemma 2. *For any elliptic curve E over $\mathbb{Q}$,*

$$E(\mathbb{Q})[3] \ncong \mathbb{Z}/3 \times \mathbb{Z}/3.$$

Definition 3. Two elliptic curves, E_1 and E_2 are *isomorphic* if there exists a birational regular map between E_1 and E_2.

Definition 4. Let E_1 and E_2 be elliptic curves defined over $\mathbb{Q}$. If there exists a birational map

$$\Phi : E_1[3](\overline{\mathbb{Q}}) \to E_2[3](\overline{\mathbb{Q}}),$$

defined over $\mathbb{Q}$ that is a group homomorphism, we say that E_1 and E_2 have isomorphic 3-torsion structure over $\mathbb{Q}$.

Over an algebraically closed field, we can find an isomorphism between the 3-torsion groups of any pair of elliptic curves because we know what the group must be. However, over $\mathbb{Q}$ it is not generally true that two nonisomorphic elliptic curves will have isormorphic 3-torsion groups.

Keeping in mind how the group law works, it is easy to characterize the 2- and 3-torsion points. For any elliptic curve $E : f(x, y) = 0$, $E(\overline{K})[2]$ is the set of points such that $f(x_0, 0) = 0$ and the identity. These are the points that are inverses of themselves under the group law.

$E(\overline{K})[3]$ is the set of inflection points, which occur in pairs above and below the x-axis, and the identity. This observation allows us to find a degree four polynomial, whose roots are the x-coordinates of the non-zero 3-torsion points. If $E : y^2 = x^3 + ax + b$ then,

$$\frac{d^2y}{dx^2} = \frac{3x^4 + 6ax^2 + 12bx - a^2}{4y^3}.$$

Therefore, the eight inflection points on E are $(x_1, \pm y_1), \ldots, (x_4, \pm y_4)$, where the x_i are roots of the numerator above, and the y_i satisfy $f(x_i, y_i) = 0$. As a subvariety of E, $E(\overline{K})[3]$ is given by $E \cap \text{Hessian}(E)$. Note that E is a cubic, so we will not see all 8 inflection points unless we are in an algebraically closed field such as $\mathbb{C}$ or $\overline{\mathbb{Q}}$.

Now that we know a little bit about elliptic curves, we should describe what genus 2 curves are like and what coverings are. For the purposes of this discussion, we can think of a genus 2 curve as given by a sextic in two variables, since any genus 2 curve can be written in the form

$$C : y^2 = a_6x^6 + \cdots + a_1x + a_0.$$

Definition 5. Let $f : R \to S$ be a non-constant rational map between curves. Then, f is a *covering* of S by R.

Definition 6. Given a covering $f : R \to S$, the *fibre* of a point $p \in S$ is

$$\{f^{-1}(p)\},$$

and the *degree* of f, $\deg(f)$, is the maximum cardinality of all fibres over an algebraically closed field.

Definition 7. *Ramification points* of a covering $f : R \to S$ are the finite set of points $p \in S$ such that

$$|\{f^{-1}(p)\}| < \deg(f),$$

over an algebraically closed field. If $p \in S$ and $P \in \{f^{-1}(p)\}$, then the number of branches going through P is the *ramificaton index* of P, denoted $e_f(p)$.

We'll give an example of a ramified covering of degree 2.

Example 1. Let $C : y^2 = w(x - w_1)(x - w_2) \cdots (x - w_6)$ be a genus 2 curve over an algebraically closed field. Then,

$$\begin{array}{rcl} \pi\colon C & \to & \mathbb{P}^1 \\ (x, y) & \mapsto & x \end{array}$$

is a degree 2 covering, with ramification points $w_1, \ldots, w_6$. Each $P_i = (w_i, 0)$ lying above w_i has ramification index 2.

The following result gives us a nice way to determine what the configuration of ramification points for a cover might look like. We will use it extensively to determine expressions for the induced Frey-Kani coverings given in the next section.

Theorem 3. *Riemann-Hurwitz*

Let $f : R \to S$ be a covering. Then

$$2(g(R) - 1) = 2\deg(f)(g(S) - 1) + \sum_{p \in R}(e_f(p) - 1)$$

where $g(S)$ and $g(T)$ denote the genus of S and T respectively.

We've defined all the necessary objects to begin our discussion of how to construct elliptic curves with isomorphic 3-torsion structure of $\mathbb{Q}$.

3 The construction

In this section, we summarize the work pertaining to degree 3 coverings of elliptic curves done by the authors mentioned in the introduction. The intention is to outline how the genus 2 curves that form degree 3 covers are characterized, how expressions for the Frey-Kani covers are determined, and when we have a second elliptic curve covered by the same genus 2 curve.

$$\begin{tikzcd}
 & C \arrow[dl, "\psi_1"'] \arrow[dr, "\pi_C"] & \\
E_1 \arrow[dr, "\pi_1"'] & & \mathbb{P}^1 \arrow[dl, "\phi_1"] \\
 & \mathbb{P}^1 &
\end{tikzcd}$$

Let us start by defining the maps we want to study above.

Definition 8. Let $\psi_1 : C \to E_1$ be a covering where,

$$\begin{aligned}
C : y^2 &= w(x - w_1)(x - w_2)\cdots(x - w_6), \text{ where } w_i \in \overline{\mathbb{Q}} \\
E_1 : v_1^2 &= f_1(u_1)
\end{aligned}$$

such that all coefficients are in $\mathbb{Q}$. The maps $\pi_C : C \to \mathbb{P}^1, \pi_1 : E_1 \to \mathbb{P}^1$ to the projective lines are

$$\pi_C(x, y) = x, \pi_1(u_1, v_1) = u_1.$$

These covers are all degree 2 so we know by applying the Riemann-Hurwitz formula that π_C has six ramification points, $W = \{w_1, \ldots, w_6\}$ above $\mathbb{P}^1$, and π_1 has four, $\{q_1, \ldots, q_4\}$, which are precisely the points in

$E_1(\overline{\mathbb{Q}})[2]$. All these points have ramification index 2, but more importantly there exists an induced covering ϕ_1 (the Frey-Kani cover), such that the diagram above commutes. (See [2]). We are interested in ϕ_1 because a map between two projective lines is easier to work with than a map between two curves, ψ_1.

If $\psi_1 : C \to E_1$ is a degree 3 cover, then Riemann-Hurwitz dictates that

$$\sum_{P \in C} (e_{\psi_1}(P) - 1) = 2,$$

so that ψ_1 is ramified above two points, each with ramification index 2 (the non-degenerate case), or ψ_1 is ramified above only one place, with ramification index 3 (the degenerate case). We are interested in the first case, so we will assume that ψ_1 is non-degenerate.

Ramification of the Frey-Kani covering occurs in a similar way (see [4], Theorem 3.1), so that if ψ_1 is non-degenerate, then ϕ_1 has four points of ramification index 2. When ψ_2 is degenerate, ϕ_2 has two points of ramification index 2, and one point of ramification index 3.

$$\begin{tikzcd}
 & C \arrow[dl, "\psi_1"'] \arrow[dr, "\psi_2"] \arrow[dd, "\pi_C"] & \\
E_1 \arrow[dd, "\pi_1"] & & E_2 \arrow[dd, "\pi_2"] \\
 & \mathbb{P}^1 \arrow[dl, "\phi_1"] \arrow[dr, "\phi_2"'] & \\
\mathbb{P}^1 & & \mathbb{P}^1
\end{tikzcd}$$

In the degree 3 case, ψ_1 is called a maximal covering (since it does not factor over a nontrivial isogeny). When ψ_1 is maximal, there exists a second covering $\psi_2 : C \to E_2$ of an elliptic curve such that $\deg(\psi_2) = \deg(\psi_1)$ (Shaska, [4]). A nice fact is that once ψ_1 is fixed, ψ_2 is unique up to isomorphism of elliptic curves (Kuhn, [3]), and it has a corresponding Frey-Kani cover ϕ_2. To determine explicit equations for ϕ_1 and ϕ_2, we look at the relation between the configuration of ramification points.

Recall that π_1 is ramified in four places $q_1, \ldots, q_4$. In the non-degenerate case, ϕ_1 is also ramified at four places, three of which are the same as π_1 (see [4]). Let these places be q_1, q_2 and q_3, and let $u_1 = 0$ be the fourth ramification point of ϕ_1 (the one not ramified in π_1), such that $x = 0$ above

$u_1 = 0$ has ramification index 2, and $x = \infty$ has ramification index 1. We can do this because the fourth ramification point is rational [3]. These conditions, with the fact that $\deg(\phi_1) = 3$ dictate that

$$\phi_1(x) = \frac{x^2}{x^3 + ax^2 + bx + c}$$

where $c \neq 0$ and the denominator has no repeated roots.

Then, C is given by an equation of the form

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

Moreover, since the two coverings ψ_1 and ψ_2 behave in a symmetric manner, the denominator of ϕ_2 is $4cx^3 + b^2x^2 + 2bcx + c^2$ (see Kuhn, [3]). The roots of this cubic are unramified points of ϕ_2 above $u_2 = \infty$. ϕ_2 is ramified above $u_2 = 0$, so let $x = d$ be the point above $u_2 = 0$ with ramification index 2, and $x = e$ the point with ramification index 1 so that

$$\phi_2 = \frac{(x-d)^2(x-e)}{4cx^3 + b^2x^2 + 2bcx + c^2}.$$

This determines the scaling of ϕ_2, and Kuhn in [3] gives possible values for d and e,

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

We will verify that the expressions given for d and e are correct, once we determine explicit equations defining our elliptic curves E_1 and E_2.

4 Expressions for E_1 and E_2

If a genus 2 curve C covers two nonisomorphic elliptic curves, E_1 and E_2, with isomorphic 3-torsion structure over $\mathbb{Q}$, then C must be given by an equation of the form

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

Also, the maps from the x-line to the u_1-line, respectively u_2-line are defined to be

$$\begin{aligned} \phi_1 : \mathbb{P}^1 &\rightarrow \mathbb{P}^1 \\ x &\mapsto \frac{x^2}{x^3 + ax^2 + bx + c} \\ \phi_2 : \mathbb{P}^1 &\rightarrow \mathbb{P}^1 \\ x &\mapsto \frac{(x-d)^2(x-e)}{4cx^3 + b^2x^2 + 2bcx + c^2} \end{aligned}$$

where

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

Given this information, we would like to find explicit equations for both E_1 and E_2, and find expressions for their coordinates u_1, v_1, u_2, v_2 in terms of x and y.

An expression for E_1 is given by taking the discriminant of an expression involving $\phi_1(x)$.

$$\begin{aligned} E_1 : v_1^2 &= \frac{\Delta_x(x^2 - u_1(x^3 + ax^2 + bx + c))}{u_1} \\ &= (a^2b^2 - 27c^2 + 18abc - 4a^3c - 4b^3)u_1^3 \\ &\quad +(12a^2c - 18bc - 2ab^2)u_1^2 + (b^2 - 12ac)u_1 + 4c. \end{aligned}$$

We already have $u_1 = \phi_1(x)$ and we obtain an expression for v_1 by substituting $\phi_1(x)$ into the right-hand side above. After some basic manipulation we obtain

$$v_1 = \frac{y(x^3 - bx - 2c)}{(x^3 + ax^2 + bx + c)^2}$$

Obtaining an expression for E_2 is done in a similar manner, but we must take the correct twist of the curve. Again, we have $u_2 = \phi_2(x)$ and

$$\begin{aligned} \tilde{E}_2 : \tilde{v}_2^2 &= \frac{\Delta_x((x - d)^2(x - e) - u_2(4cx^3 + b^2x^2 + 2bcx + c^2))}{u_2} \\ &= -16b^8c^4(27c^2 - b^3)(9c^2 - 4abc + b^3)^4u_2^3 \\ &\quad -16b^6c^4(27c^2 - b^3)(9c^2 - 4abc + b^3)^3(54ac^2 + ab^3 - 27b^2c)u_2^2 \\ &\quad -16b^4c^4(27c^2 - b^3)(9c^2 - 4abc + b^3)^2 \\ &\quad (729a^2c^4 + 54a^xb^3c^2 - 972ab^2c^3 - 18ab^5c + 729bc^4 + 189b^4c^2 + b^7)u_2 \\ &\quad +16b^2c^5(27c^2 - b^3)(9c^2 - 4abc + b^3)(27c^2 - 9abc + 2b^3)^3. \end{aligned}$$

Substituting $\phi_2(x)$ into the right-hand side, we obtain

$$\frac{\tilde{v}_2}{\sqrt{s}} = \frac{y(b^3 - 27c^4)^2((4abc - 8c^2 - b^3)x^3 + (4ac^2 - b^2c)x^2 + bc^2x + c)}{(4cx^3 + b^2x^2 + 2bcx + c^2)^2}$$

where

$$s = 16b^2c^4(9c^2 - 4abc + b^3).$$

The correct twist of $\tilde{E}_2$ is obtained when $v_2 = \tilde{v}_2/\sqrt{s}$, so that

$$E_2 : v_2^2 = \frac{\Delta_x((x - d)^2(x - e) - u_2(4cx^3 + b^2x^2 + 2bcx + c^2))}{u_2}.$$

Thus, we have obtained the correct expressions for E_1 and E_2 over $\mathbb{Q}$. As mentioned, the authors we cite worked over $\mathbb{C}$, so they did provide expressions for E_1 and E_2 over $\mathbb{C}$, but did not provide them over $\mathbb{Q}$.

5 Verifying expressions for ϕ_2

In [3], Kuhn gives an expression for $\phi_2 : \mathbb{P}^1 \to \mathbb{P}^1$,

$$\phi_2(x) = \frac{(x-d)^2(x-e)}{4cx^3 + b^2x^2 + 2bcx + c^2},$$

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

The configuration of ramification points dictates that ϕ_2 must be in the above form, but we nevertheless spent some deriving the expressions for d and e correctly.

To do this, we found

$$\frac{\Delta_x((x-d)^2(x-e) - u_2(4cx^3 + b^2x^2 + 2bcx + c^2))}{u_2},$$

and made the substitution $u_2 = \phi_2(x)$. The resulting expression should factor so that there is a cubic denominator, and a numerator that is the product of a constant in a, b, c, the factor $x^3 + ax^2 + bx + c$, and a square factor. We obtained a system of four equations from which we could derive the same expressions for d and e. There were other choices, but they would require an algebraic extension of $\mathbb{Q}$.

6 Finding covers of a given elliptic curve

Given an elliptic curve E_1, we were able to find a genus 2 curve C, such that C is a non-degenerate degree 3 cover of E_1. If E_1 is given by the equation

$$\tilde{v}_1^2 = \tilde{u}_1^3 + g_1\tilde{u}_1 + g_0,$$

then the goal is to find the parameters a, b, c in the map

$$\begin{aligned} \phi_1 \colon \mathbb{P}^1 &\to \mathbb{P}^1 \\ x &\mapsto \frac{x^2}{x^3 + ax^2 + bx + c} \end{aligned}$$

in terms of g_1 and g_0, since C must be defined by an equation in the form

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

In the non-degenerate case ϕ_1 is ramified in 4 places, above $0, q_1, q_2$ and q_3, which depend on a, b and c. If C is to cover E_1, then the map

$$\begin{array}{rcl} \pi_1\colon E_1 & \rightarrow & \mathbb{P}^1 \\ (u_1, v_1) & \mapsto & u_1 \end{array}$$

should be ramified above q_1, q_2, q_3 and ∞. Note that the ramification points here are the 2-torsion points of E_1. To accommodate this we shift and scale E_1 so that its 2-torsion points lie at q_1, q_2, q_3 and ∞ by performing a change of variables,

$$\tilde{u_1} = Au_1 + B.$$

In terms of the map ϕ_1, E_1 should be defined by

$$v_1^2 = \frac{\Delta_x(x^2 - u_1(x^3 + ax^2 + bx + c))}{u_1}.$$

Equating the right-hand side of the equation above to $\tilde{u}_1 + g_1\tilde{u}_1 + g_0$, and matching up the coefficients, we obtain a system of equations that a, b and c must satisfy. Solving the system using Maple, we see that a, b, c satisfy

$$\begin{array}{rcl} 0 & = & 1147912560b^3c^8g_1^3 + 5184b^{14}a^2g_1^3 + 11664a^2b^{14}g_0^2 + 972a^4b^{13}g_0^2 \\ & & -288a^4b^{13}g_1^3 + 4a^6b^{12}g_1^3 + 27a^6b^{12}g_0^2 + 17496a^6b^9c^2g_0^2 \\ & & -15058224a^3b^9c^3g_1^3 - 117074484a^3b^9c^3g_0^2 + 223205220b^6c^6g_1^3 \\ & & -20995200ab^10c^3g_1^3 - 4320a^6b^9c^2g_1^3 - 110539728ab^{10}c^3g_0^2 \\ & & -2439314190ab^7c^5g_0^2 - 259343208ab^7g_1^3c^5 + 3779136a^6b^6c^4g_0^2 \\ & & +942244893a^2b^8c^4g_0^2 + 357128352a^4b^7c^4g_0^2 + 46924272a^4b^7c^4g_1^3 \\ & & -944784a^5b^8c^3g_1^3 - 4487724a^5b^8c^3g_0^2 + 156597948a^2b^8c^4g_1^3 \\ & & +2379456a^2b^{11}c^2g_1^3 + 354780a^4b^{10}c^2g_1^3 + 1738665a^4b^{10}c^2g_0^2 \\ & & +136048896a^6c^8g_1^3 - 65664a^3b^{12}cg_1^3 + 1119744a^6b^6c^4g_1^3 \\ & & -3507510600a^3b^6c^5g_0^2 - 576318240a^3b^6c^5g_1^3 - 68024448a^5b^5c^5g_1^3 \\ & & -510183360a^5b^5c^5g_0^2 + 1428513408a^2b^5c^6g_1^3 + 11823499368a^2b^5c^6g_0^2 \\ & & +1017532368a^4b^4c^6g_1^3 + 5892617808a^4b^4c^6g_0^2 - 155520ab^{13}cg_1^3 \\ & & -244944a^3b^{12}cg_0^2 - 10206a^5b^{11}cg_0^2 + 1944a^5b^{11}cg_1^3 \\ & & +18738216a^2b^{11}c^2g_0^2 + 1793613375b^6c^6g_0^2 - 1836660096a^3c^9g_1^3 \end{array}$$

$$
\begin{aligned}
&-24794911296a^3c^9g_0^2 + 6198727824c^{10}g_1^3 + 4723920b^{12}c^2g_0^2 \\
&-1469664ab^{13}cg_0^2 + 1166400b^{12}c^2g_1^3 + 1594323300b^9c^4g_0^2 \\
&+15746400b^9c^4g_1^3 + 46656b^15g_0^2 - 2219297616ab^4c^7g_1^3 \\
&+272097792a^6b^3c^6g_0^2 + 25194240a^6b^3c^6g_1^3 - 3095112384a^3b^3c^7g_1^3 \\
&-23417416224a^3b^3c^7g_0^2 - 3673320192a^5b^2c^7g_0^2 - 612220032a^5b^2c^7g_1^3 \\
&+30993639120a^2b^2c^8g_0^2 + 6887475360a^2b^2c^8g_1^3 + 1224440064a^4bc^8g_1^3 \\
&+16529940864a^4bc^8g_0^2 - 8264970432abc^9g_1^3 - 12914016300ab^4c^7g_0^2.
\end{aligned}
$$

The monster above is a weighted homogeneous equation in a, b and c, where the weights are $1, 2$ and 3 respectively, so we may assume that $a = 1$. If we can find (b_0, c_0) such that $b_0, c_0 \in \mathbb{Q}$, satisfying the equation then we have found a degree 3 cover of E_1.

Let $h(b, c)$ equal the right-hand side above, with $a = 1$. Then $H\colon h = 0$ is a genus 0 curve with singular points

$$
(0, 0)\,, \left(\frac{1}{3}, \frac{1}{27}\right), \infty.
$$

To find a nonsingular point on H, fit a line though the first two singular points to obtain a third point on H,

$$
P = \left(-\frac{4g_1^3}{81g_0^2}, -\frac{4g_1^3}{729g_0^2}\right).
$$

P is nonsingular for almost all values of g_1 and g_0, except when

$$
(g_1, g_0) = (0, \lambda), (2\lambda^2, -3\lambda^2),
$$

where λ is a rational parameter. For these values of g_1 and g_0, h becomes reducible.

Notice that we have considerable choice in choosing a curve C that covers a given elliptic curve, E_1. However, once the covering is fixed E_2 is uniquely determined, and we can find an expression for it using the method outlined.

References

[1] Gerhard Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2.*

[2] Gerhard Frey and Ernst Kani, *Curves of genus 2 covering elliptic curves and an arithmetical application*, Prog. Math. **89** (1989), 153–177 (English).

[3] Robert M. Kuhn, *Curves of genus 2 with split Jacobian*, Transactions of the American Mathematical Society **307** (1988), no. 1, 41–49 (English).

[4] Tony Shaska, *Curves of genus 2 with* (n, n) *decomposable Jacobians*, J. Symbolic Computation **31** (2001), no. 5, 603–617 (English).

[5] ———, *Genus 2 curves with (3,3)-split Jacobian and large automorphism group*, Lecture Notes in Computer Science, 2369, Springer, 2002, pp. 205–218.

[6] ———, *Genus 2 fields with degree 3 elliptic subfields*, Forum Mathematicum **16** (2004), no. 2, 263–280 (English).

[7] Tony Shaska and Helmut Völkein, *Elliptic subfields and automorphisms of genus 2 function fields*, Algebra, Arithmetic and Geometry with Applications, Springer, 2004, pp. 703–723 (English).