THREE-TORSION SUBGROUPS AND CONDUCTORS OF GENUS 3 HYPERELLIPTIC CURVES

ELVIRA LUPOIAN

ABSTRACT. We give a practical method for computing the 3-torsion subgroup of the Jacobian of a genus 3 hyperelliptic curve. We define a scheme for the 3-torsion points of the Jacobian and use complex approximations, homotopy continuation and lattice reduction to find precise expression for the 3-torsion. In the latter stages of the paper, we explain how the 3-torsion subgroup can be used to compute the wild part of the local exponent of the conductor at 2.

1. INTRODUCTION

Let C be a smooth, projective, hyperelliptic curve of genus 3 defined over $\mathbb{Q}$ and let J be its Jacobian variety. Recall that J is a 3-dimensional abelian variety whose points can be identified with elements of the zero Picard group of C, $\operatorname{Pic}^0(C)$. An affine model of such a curve is

$$C : y^2 = f(x)$$

where $f(x) \in \mathbb{Q}[x]$ has degree 7 or 8, and no repeated roots. The Mordell-Weil theorem states that $J(L)$ is a finitely generated group for any number field L; that is, $J(L) \cong J(L)_{\text{tors}} \oplus \mathbb{Z}^r$ where $J(L)_{\text{tors}}$ is the finite torsion subgroup and r is the rank. For a hyperelliptic curve we can compute a large part of the 2-torsion subgroup of J, $J[2] = \{P \in J : 2P = 0\}$. For any two roots of f, x_1 and x_2, the class of the divisor $(x_1, 0) - (x_2, 0) - \infty_1 - \infty_2$ is a non-zero element of $J[2]$, where ∞_1, ∞_2 are two marked points on the projective curve. The two marked points are distinct when f had degree 8 nd $\infty_1 = \infty_2$ when f has degree 7. Moreover, all points of order 2 are of this from when f has degree 7, see [13] or [7].

The problem of finding a point of order 3 is not as straightforward. In Section 2, we will show that all 3-torsion elements correspond to ways of expressing f, or a scalar multiple of f, as

$$f(x)(x+\alpha_1)^2 + \alpha_7\left(x^3+\alpha_8x^2+\alpha_9x+\alpha_{10}\right)^3 = \left(\alpha_2x^4+\alpha_3x^3+\alpha_4x^2+\alpha_5x+\alpha_6\right)^2$$

when f has degree 7, and

$$\left(-x^6 - \frac{a_7}{2}x^5 - \left(-\frac{a_6}{2}+\frac{a_7^2}{8}\right)x^4 + \alpha_1\left(-x^5-\frac{a_7}{2}x^4\right) - \alpha_2x^4+\alpha_3x^3+\alpha_4x^2+\alpha_5x+\alpha_6\right)^2$$
$$= \alpha_7\left(x^3+\alpha_8x^2\alpha_9x+\alpha_{10}\right)^3 + \left(x^2+\alpha_1x+\alpha_2\right)^2 f(x)$$

when f has degree 8, for some $\alpha_1, \dots, \alpha_{10} \in \overline{\mathbb{Q}}$, where a_6 and a_7 are coefficients of f. The above correspondence can be used to define schemes parametrising the

Date: August 16, 2023.
2010 *Mathematics Subject Classification.* 11G30, 11G20.
Key words and phrases. Jacobians, Conductor, Hyperelliptic Curve .
The author is supported by the EPSRC studentship.

3-torsion points of J. In Sections 3 we give a method of approximating the points of such schemes as complex numbers using homotopy continuation and the Newton-Raphson method. These numerical analysis techniques are used to efficiently compute approximations with a large precision, around 5000 decimal places, and in Section 4 we explain how such approximations are used to find algebraic expressions for the 3-torsion points of J, using lattice reduction. In Section 5, we compute the 3-torsion subgroups of the modular Jacobians $J_0(30)$ and $J_0(40)$. A similar method of complex approximations and lattice reduction was used in [8] to compute the 2-torsion subgroup of some non-hyperelliptic modular Jacobians.

The second half of this paper will explain how the 3-torsion subgroup $J[3]$ can be used to determine the local conductor exponent of C at 2. Recall that the conductor of a curve $C/\mathbb{Q}$ is a representation theoretic constant, defined as a product $N = \prod_p p^{n_p}$ over the primes p where C has bad reduction. Thus the problem of computing the conductor of C reduces to computing the local exponents n_p for all primes of bad reduction p. When C is an elliptic curve, the n_p can be computed using Tate's algorithm (see [9, Chapter 4]). For hyperelliptic curves of arbitrary genus, there are formulae for n_p for all $p \neq 2$, see [5]. For curves of genus 2, Dokchitser and Doris [6] give an algorithm for n_2. In [6], the authors take C to be a non-singular projective curve of genus 2, defined over a finite extension K of $\mathbb{Q}_2$. Then, n_2 is the sum of the tame and wild parts,

$$n_2 = n_{\text{tame}} + n_{\text{wild}}$$

where n_{tame} can be deduced from a regular model of the curve and n_{wild} is the Swan conductor of the 3-adic Tate module of the Jacobian of C/K, and it can be computed from the action of $\text{Gal}(K(J[3])/K)$ on $J[3]$.

In the final two sections, we will assume C to be a smooth, projective and hyperelliptic curve of genus 3, defined over $\mathbb{Q}_2$, and following [6] we use the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $J[3]$ to compute n_{wild} when C is hyperelliptic of genus 3. In Section 6, we give a brief theoretic overview of how the local conductor exponent at 2 is calculated using a regular model of the curve and the 3-torsion subgroup of its Jacobian. In Section 7, we compute the wild part of n_2 for the modular curve $X_0(40)$ using the 3-torsion subgroups computed in Section 5.

Acknowledgements. I would like to thank my supervisors Samir Siksek and Damiano Testa for their continued support, the many helpful conversations and their invaluable suggestions throughout this project. I would also like to thank Tim Dokchitser for the helpful conversation regarding the tame part of the conductor.

2. Scheme of 3-torsion points

Let C be a smooth, projective, hyperelliptic curve of genus 3, defined over a number field K. By possible passing to a quadratic extension of K, C has an affine model of the form

$$y^2 = f(x)$$

where $f(x) \in K[x]$ is monic, has degree 7 or 8 and has no repeated roots.

The projective closure of C in $\mathbb{P}^2$ is defined by

$$Y^2 Z^{d-2} = Z^d f(X/Z)$$

where d is the degree of f.

Remark 2.1. We refer to the points of C not appearing on the affine model as the points at infinity. These correspond to $Z = 0$, and we observe that there is a single such point, namely $(0:1:0)$ when the degree of f is 7; and 2 points: $(1:1:0)$ and $(1:-1:0)$ when the degree of f is 8.

Let J be the Jacobian variety of C. Recall that J is a 3-dimensional, abelian variety over K, whose points can be identified with points of $\mathbf{Pic}^0(C)$, the zero Picard group of C. From now on we simply regard points on J as classes of divisors of degree 0 on C. See [13] or [7] for details on the arithmetic of hyperelliptic curves.

The 3-torsion subgroup of J consists of all elements $[D] \in \mathbf{Pic}^0(C)$ such that $3D = \operatorname{div}(h)$, where h is a rational function on C. To parametrise all such points, we treat the two degree cases separately. We begin with the following straightforward result, which is required throughout the remainder of the section.

Lemma 1. *Let C be a smooth, projective and hyperelliptic curve of genus g over a number field K and let $K(C)$ be its function field. Let $y^2 = f(x)$ be an affine model of the curve with $f \in K[x]$. Suppose $g(x)$ is any polynomial in x, which is also an element of $K(C)$ and its divisor of zeros is of the form $3D$, where D is an effective divisor. Then $g(x)$ is a cube as an element of $\overline{K}[x]$.*

Proof. We can write g as

$$g(x) = \alpha(x-\beta_1)^{r_1}\dots(x-\beta_s)^{r_s}(x-\gamma_1)^{t_1}\dots(x-\gamma_n)^{t_n}$$

where $f(\beta_i) = 0$ for all $i = 1\dots s$, $f(\gamma_j) \neq 0$ for all $j = 1\dots n$ and $\alpha \in K^\times$.The divisor of zero of g is

$$\sum_{i=1}^{s} 2r_i(\beta_i, 0) + \sum_{j=1}^{n} t_j\left(\left(\gamma_j, \sqrt{f(\gamma_j)}\right) + \left(\gamma_j, -\sqrt{f(\gamma_j)}\right)\right)$$

By assumption, this must equal $3D$, and hence 3 divides $2r_i$ and t_j for all $i = 1\dots s$ and $j = 1\dots n$, and the result follows. □

Proposition 1. *Let C be an odd degree hyperelliptic curve of genus 3, over a number field K, with an affine model*

$$y^2 = f(x) = x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

where $a_i \in K$ and f has no repeated roots. Let J be the Jacobian of C. Then any non-zero 3-torsion point of J is the form $\left[\frac{1}{3}div(h)\right]$ where

$$h = y(x+\alpha_1) + \alpha_2x^4 + \alpha_3x^3 + \alpha_4x^2 + \alpha_5x + \alpha_6$$

with $\alpha_1, \dots, \alpha_6 \in \overline{K}$ satisfying

$$f(x)(x+\alpha_1)^2 + \alpha_7\left(x^3 + \alpha_8x^2 + \alpha_9x + \alpha_{10}\right)^3 = \left(\alpha_2x^4 + \alpha_3x^3 + \alpha_4x^2 + \alpha_5x + \alpha_6\right)^2$$

for some $\alpha_7, \alpha_8, \alpha_9, \alpha_{10} \in \bar{K}$. Furthermore this correspondence preserves the action of $G_K = \operatorname{Gal}\left(\overline{K}/K\right)$.

Proof. Let ∞ be the unique point at infinity on this model and $[D] \in J[3] \setminus 0$. By Riemann-Roch there exists a unique, effective divisor $D_0 = P_1 + P_2 + P_3$ such that

$$D \sim D_0 - 3\infty$$

As $3D$ is principal, $3D_0 - 9\infty = \operatorname{div}(h)$, where h is a rational function on C. Thus h is in the Riemann-Roch space $L(9\infty)$ which has basis

$$1, x, x^2, x^3, x^4, xy, y$$

Then, replacing h by a scalar multiple if necessary, h is either a polynomial in x of degree at most 4, or $h = y + k(x)$ with $k(x) \in K[x]$, $\deg(x) \leq 4$, or $h = y(x+\alpha_1) + k(x)$ with $\alpha_1 \in K$, $k(x) \in K[x]$ and $\deg(x) \leq 4$.

Case 1. Suppose $h \in K[x]$ and $d = \deg(h) \leq 4$. Let $\theta_1, \ldots, \theta_d$ be the roots of h. The divisor of zeros of h is $3D_0 = 3P_1 + 3P_2 + 3P_3$ since $\operatorname{div}(h) = 3D_0 - 9\infty$. We can also compute the divisor of zeros directly, and find it to be

$$\sum_{i=1}^{d} \left(\left(\theta_i, \sqrt{f(\theta_i)} \right) + \left(\theta_i, -\sqrt{f(\theta_i)} \right) \right)$$

The above divisor has degree at most 8, whilst $\deg(3D_0) = 9$, and hence they cannot be equal. Thus h cannot be a polynomial in x of degree at most 4.

Case 2. Suppose $h = y + g(x)$ where $g \in K[x]$ and $\deg(g) \leq 4$, and let $\tilde{h} = -y + g(x)$. As before, the divisor of zeros of h is $3D_0$, and the divisor of zeros of $\tilde{h}$ is

$$3\iota(D_0) = 3\iota(P_1) + 3\iota(P_2) + 3\iota(P_3)$$

where $\iota : C \longrightarrow C$ denotes the hyperelliptic involution on C. The divisor of zeros of $h\tilde{h}$ is $3D_0 + 3\iota(D_0)$, and hence $h\tilde{h} = -f(x) + g(x)^2$ is necessarily a cube as an element of $\overline{K}[x]$ by Lemma 1. However, this is a contradiction since $-f(x) + g(x)^2$ has degree 7 or 8.

Case 3. This is the only remaining case. Suppose $h = y(x+\alpha_1) + g(x)$ where $\alpha_1 \in K$, $g(x) \in K[x]$ and g has degree at most 4, and let $\tilde{h} = -y(x+\alpha_1) + g(x)$. Arguing as before, the divisor of zeros of $h\tilde{h}$ is $3D_0 + 3\iota(D_0)$ and hence by Lemma 1, $h\tilde{h} \in K[x]$ is necessarily a cube. Hence

$$\begin{aligned} h\tilde{h} &= (y(x+\alpha_1) + g(x))(-y(x+\alpha_1) + g(x)) \\ &= -f(x)(x+\alpha_1)^2 + g(x)^2 \\ &= \alpha_7 \left(x^3 + \alpha_8 x^2 + \alpha_9 x + \alpha_{10} \right)^3 \end{aligned}$$

for some $\alpha_7, \ldots, \alpha_{10} \in \overline{K}$, where $g(x) = \alpha_2 x^4 + \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6$ for some $\alpha_2, \ldots, \alpha_6 \in \overline{K}$.

□

Equating coefficients in this expression

$$f(x)(x+\alpha_1)^2 + \alpha_7 \left(x^3 + \alpha_8 x^2 + \alpha_9 x + \alpha_{10} \right)^3 = \left(\alpha_2 x^4 + \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6 \right)^2$$

gives 10 equations in $\alpha_1, \ldots, \alpha_{10}$, where $(\alpha_1, \ldots, \alpha_6)$ define a 3-torsion point. We will refer to the scheme defined by these 10 equations as the scheme of 3-torsion points.

Proposition 2. *Let C be an even degree hyperelliptic curve of genus* 3*, over a number field K, with an affine model*

$$y^2 = f(x) = x^8 + a_7 x^7 + a_6 x^6 + a_5 x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

where $a_i \in K$ and f has no repeated roots. Let J be the Jacobian of C. Then any non-zero 3-torsion point of J is the form $\left[\frac{1}{3}div(h)\right]$ where

$$h = x^2y - x^6 - \frac{a_7}{2}x^5 + \left(-\frac{a_6}{2} + \frac{a_7^2}{8}\right)x^4 + \alpha_1\left(xy - x^5 - \frac{a_7}{2}x^4\right) + \alpha_2\left(y - x^4\right)$$
$$+ \alpha_3x^3 + \alpha_4x^2 + \alpha_5x + \alpha_6$$

for some $\alpha_1, \dots, \alpha_6 \in \overline{K}$ satisfying

$$-f(x)\,l(x)^2 + g(x)^2 = \alpha_7\left(x^3 + \alpha_8x^2 + \alpha_9x + \alpha_{10}\right)^3$$

for some $\alpha_7, \dots, \alpha_{10} \in \overline{K}$ where

$$l(x) = x^2 + \alpha_1x + \alpha_2$$
$$g(x) = -x^6 + \left(-\frac{a_7}{2} - \alpha_1\right)x^5 + \left(-\frac{a_6}{2} + \frac{a_7^2}{8} - \frac{\alpha_1a_7}{2} - \alpha_2\right)x^4 + \alpha_3x^3 + \alpha_4x^2 + \alpha_5x + \alpha_6$$

Furthermore this correspondence preserves the action of $G_K = \mathrm{Gal}\left(\overline{K}/K\right)$.

Proof. Let ∞_+ and ∞_- be the two points at infinity on this model and $[D] \in J[3]\smallsetminus 0$. By Riemann-Roch there exists a unique, effective divisor $D_0 = P_1 + P_2 + P_3$ such that

$$D \sim D_0 - \infty_+ - 2\infty_-$$

As $3D$ is principal, $3D_0 - 3\infty_+ - 6\infty_- = \mathrm{div}(h)$, where h is a rational function on C. Thus h is in the Riemann-Roch space $L(3\infty_+ + 6\infty_-)$ which has basis

$$1, x, x^2, x^3,\ y - x^4,\ xy - x^5 - \tfrac{a_7}{2}x^4,\ x^2y - x^6 - \tfrac{a_7}{2}x^5 + \left(-\tfrac{a_6}{2} + \tfrac{a_7^2}{8}\right)x^4$$

By possibly replacing h by a scalar multiple, h will necessarily fall in one of the following four cases.

Case 1. Suppose h is a polynomial in x of degree $d \leq 3$. Let $\theta_1, \dots, \theta_d$ be the roots of h. The divisor of zeros of h is $3D_0$ since $\mathrm{div}(h) = 3D_0 - 9\infty$. We can also compute the divisor of zeros directly, and find it to be

$$\sum_{i=1}^{d}\left(\left(\theta_i, \sqrt{f(\theta_i)}\right) + \left(\theta_i, -\sqrt{f(\theta_i)}\right)\right)$$

The above divisor has degree at most 6, whilst $\deg(3D_0) = 9$, and hence they cannot be equal. Thus h cannot be a polynomial in x of degree at most 3.

Case 2. Suppose h is of the form

$$h = y - x^4 + \alpha_1x^3 + \alpha_2x^2 + \alpha_3x + \alpha_4$$
$$= y + g(x)$$

for some $\alpha_1, \dots, \alpha_4 \in \overline{K}$, where $g(x) = -x^4+\alpha_1x^3+\alpha_2x^2+\alpha_3x+\alpha_4$. Let $\tilde{h} = -y+g(x)$. Arguing as in the proof of the previous proposition, the divisor of zeros of h is $3D_0$; and the divisor of zeros of $\tilde{h}$ is $3\iota(D_0)$. The divisor of zeros of $h\tilde{h} \in K[x]$ is $3D_0+3\iota(D_0)$, and thus by Lemma 1, $h\tilde{h} \in K[x]$ is necessarily a cube. We find that

$$h\tilde{h} = (y + g(x))(-y + g(x))$$
$$= -f(x) + g(x)^2$$

has degree at most 7, and hence it has degree 6 or 3 if it is indeed a cube. Suppose $h\tilde{h}$ has degree 6, so $h\tilde{h} = q^3$ where $q \in K[x]$ is a quadratic polynomial. Let θ_1, θ_2 be the roots of q. Then the divisor of zeros of $h\tilde{h}$ is

$$3\sum_{i=1}^{2}\left(\left(\theta_i, \sqrt{f(\theta_i)}\right) + \left(\theta_i, -\sqrt{f(\theta_i)}\right)\right)$$

and by considering the degree of this divisor, it cannot equal $3D_0$. A very similar argument shows that the $\deg\left(h\tilde{h}\right) = 3$ also leads to a contradiction. Thus h cannot be of the stated form.

Case 3. Suppose h is of the form

$$\begin{aligned} h &= xy - x^5 - \frac{a_7}{2}x^4 + \alpha_1\left(y - x^4\right) + \alpha_2 x^3 + \alpha_3 x^2 + \alpha_4 x + \alpha_5 \\ &= l(x)y + g(x) \end{aligned}$$

for some $\alpha_1, \ldots, \alpha_5 \in \overline{K}$, where $l(x) = x + \alpha_1$, $g(x) = -x^5 - \frac{a_7}{2}x^4 - \alpha_1 x^4 + \alpha_2 x^3 + \alpha_3 x^2 + \alpha_4 x + \alpha_5$. Let $\tilde{h} = -l(x)y + g(x)$. Arguing as before, $h\tilde{h} \in K[x]$ is a cube. We find that

$$\begin{aligned} h\tilde{h} &= (l(x)y + g(x))(-l(x)y + g(x)) \\ &= -l(x)^2 f(x) + g(x)^2 \end{aligned}$$

has degree at most 8, and hence it must have degree 3 or 6 if it is a cube. As in case 2, both possible degrees lead to a contradiction. Hence h cannot be of the stated form.

Case 4. Suppose h is of the form

$$\begin{aligned} h = {} & x^2 y - x^6 - \frac{a_7}{2}x^5 + \left(-\frac{a_6}{2} + \frac{a_7^2}{8}\right)x^4 + \alpha_1\left(xy - x^5 - \frac{a_7}{2}x^4\right) + \alpha_2\left(y - x^4\right) \\ & + \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6 \\ = {} & l(x)y + g(x) \end{aligned}$$

for some $\alpha_1, \ldots, \alpha_6 \in \overline{K}$, where $l(x) = x^2 + \alpha_1 x + \alpha_2$, $g(x) = -x^6 - \frac{a_7}{2}x^5 - \left(-\frac{a_6}{2} + \frac{a_7^2}{8}\right)x^4 + \alpha_1\left(-x^5 - \frac{a_7}{2}x^4\right) - \alpha_2 x^4 + \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6$. Following previous arguments, set $\tilde{h} = -l(x)y + g(x)$, then by considering the divisor of zeros of $h\tilde{h}$ we find that $h\tilde{h} \in K[x]$ must be a cube. In general,

$$\begin{aligned} h\tilde{h} &= (l(x)y + g(x))(-l(x)y + g(x)) \\ &= -l(x)^2 f(x) + g(x)^2 \end{aligned}$$

has degree 9, and so it must be the cube of a degree 3 polynomial; and so there exist $\alpha_7, \ldots, \alpha_{10} \in \overline{K}$ such that

$$-l(x)^2 f(x) + g(x)^2 = \alpha_7\left(x^3 + \alpha_8 x^2 \alpha_9 x + \alpha_{10}\right)^3$$

Thus such h define 3-torsion points on J.

□

Equating coefficients in the expression

$$\left(-x^6 - \frac{a_7}{2}x^5 - \left(-\frac{a_6}{2} + \frac{a_7^2}{8}\right)x^4 + \alpha_1\left(-x^5 - \frac{a_7}{2}x^4\right) - \alpha_2 x^4 + \alpha_3 x^3 + \alpha_4 x^2 + \alpha_5 x + \alpha_6\right)^2$$
$$= \alpha_7\left(x^3 + \alpha_8 x^2 + \alpha_9 x + \alpha_{10}\right)^3 + \left(x^2 + \alpha_1 x + \alpha_2\right)^2 f(x)$$

gives 10 equations in $\alpha_1, \dots, \alpha_{10}$, where $(\alpha_1, \dots, \alpha_6)$ define a 3-torsion point. We will refer to the scheme defined by these 10 equations as the scheme of 3-torsion points.

3. Complex Approximations and Homotopy Continuation

Let $e_1, \dots, e_{10}$ be the equations in $\alpha_1, \dots, \alpha_{10}$ defining a scheme of 3-torsion points as in the previous section. We want to determine the solution set of this system of equations. In theory, this can be done using Gröbner basis techniques, the following two `Magma` commands do precisely this: `PointsOverSplittingField` and `Points`. The input for the former is a set of equations defining a zero-dimensional scheme and its output is the solution set of the system of equations. Due to the large degree of our scheme, we found that this command was inefficient in our examples. The latter command is less ambitious. It is designed to give the set of K-rational points of a zero- dimension scheme S, where K is the field of definition of S. In this case, determing the field of definition of the 3-torsion subgroup is as difficult as determining the 3-torsion subgroup itself. Thus, we were unable to use this latter command in our computations.

Instead, we will take a two step approach to determine the points of our scheme. First, the solutions of $e_1, \dots, e_{10}$ can be approximated as complex points using the Newton-Raphson method. We give a brief overview of this, a detailed explanation can be found in [12, Page 298]. In the section which follows, we explain how these approximations can be used to find precise expressions for these points.

Complex Approximations. Let $E = (e_1, \dots, e_{10})$ be as above, and view this 10-tuple of equations as a function $\mathbb{C}^{10} \longrightarrow \mathbb{C}^{10}$. Let dE be the Jacobian matrix of E. Suppose $\mathbf{x}_0$ is an approximate solution to E with $dE(\mathbf{x}_0)$ invertible. For $k \geq 1$, define

$$\mathbf{x}_k = \mathbf{x}_{k-1} - dE(\mathbf{x}_{k-1})^{-1} E(\mathbf{x}_{k-1})$$

Provided the initial approximation $\mathbf{x}_0$ is a good enough approximation, the resulting sequence $\{\mathbf{x}_k\}_{k\geq 0}$ converges to a root of E, with each iterate having increased precision. In fact, at each step the number of decimal places to which the approximation is accurate roughly doubles [12, Section 5.8]

This method requires initial complex approximations to the solutions of E. These can be obtained using homotopy continuation and its implementation in `Julia` (see [3]).

Homotopy Continuation. Homotopy continuation is a method for numerically approximating the solutions of a system of polynomial equations by deforming the solutions of a similar system whose solutions are known. We give a brief sketch of the idea, but a more detailed explanation if this theory can be found in [3] or [15] .

The total degree of E is defined as $\deg(E) = \prod_i \deg(e_i)$, where $\deg(e_i)$ is the maximum of the total degrees of the monomials of e_i.

Let F be a system of 10 polynomials in $\alpha_1, \ldots, \alpha_n$, which has exactly $\deg(E)$ solutions and these solutions are known. The system F will be known as a start system. The standard homotopy of F and E is a function

$$\begin{aligned} H : \mathbb{C}^{10} \times [0,1] &\longrightarrow \mathbb{C}^{10} \\ H(\mathbf{x}, t) &= (1-t) F(\mathbf{x}) + tE(\mathbf{x}) \end{aligned}$$

Fix $N \in \mathbb{N}$, and for any $s \in [0, N] \cap \mathbb{N}$ define $H_s(\mathbf{x}) = H(\mathbf{x}, s/N)$, this is a system of 10 polynomials in $\alpha_1, \ldots, \alpha_n$.

For N large enough, the solutions of $H_s(\mathbf{x})$ are good approximations of the solutions of $H_{s+1}(\mathbf{x})$, and using the Newton-Raphson method we can increase their precision. The solutions of $H_0(\mathbf{x}) = F(\mathbf{x})$ are known, and they can be used to define solution paths to approximate solutions of $H_N(\mathbf{x}) = E(\mathbf{x})$.

There are two important things to highlight.

1. Given any E, a start system (and its solutions) can always be computed.
2. A start system can be modified to ensure solutions paths are non-overlapping and converging to approximate solutions of E.

Homotopy Continuation is implemented in the `Julia` package HomotopyContinuation.jl (see [3]).

Remark 3.1. The implementation of homotopy continuation in `Julia` gives approximates to solutions of E which are accurate to 16 decimal places. For our computations we used the approximate solutions and 1000 iterations of Newton-Raphson to obtain an accuracy of 5000 decimal places.

4. Algebraic Expressions

Suppose $(\alpha_1, \ldots, \alpha_{10})$ is a point on a scheme of 3-torsion points defined by $E = (e_1, \ldots, e_{10})$, which has a complex approximation $(a_1, \ldots, a_{10})$, accurate to k decimal places. We use the short vector algorithm to find the minimal polynomials of the α_i and define the corresponding 3-torsion point.

4.1. **Minimal Polynomials.** Fix i, $1 \le i \le 10$ and let $\alpha = a_i$, $\theta = \alpha_i$. As α is an algebraic number, there exists $d \in \mathbb{N}$ and $c_0, \ldots, c_d \in \mathbb{Z}$ such that

$$c_d \alpha^d + \ldots + c_1 \alpha + c_0 = 0$$

Suppose $\theta \in \mathbb{R}$, that is the imaginary part of θ is small, so we'll assume that θ is approximating a real algebraic number and take $\theta = \mathrm{Re}(\theta) \in \mathbb{R}$. Fix a constant $C = 10^{k'}$, with $k' < k$ such that

$$|\left[C \cdot \theta^i\right] - C \cdot \alpha^i| \le 1 \text{ for all } 0 \le i \le d$$

where $[x]$ denotes the integer part of $x \in \mathbb{R}$. Let $\mathcal{L}_k$ be the lattice generated by the columns $v_d, \ldots, v_0$ of the $(d+1) \times (d+1)$ matrix

$$A_k = \begin{pmatrix} 1 & \ldots & 0 & 0 \\ 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \\ \left[C\theta^d\right] & \ldots & [C\theta] & [C] \end{pmatrix} = (v_d, \ldots, v_1, v_0)$$

As $c_0, \ldots, c_d \in \mathbb{Z}$

$$\mathbf{c}_k = \begin{pmatrix} c_d \\ \vdots \\ c_1 \\ a \end{pmatrix} = c_d v_n + \ldots + c_0 v_0 \in \mathcal{L}_k$$

where $a = c_d \left[C\theta^d\right] + \ldots + c_1 \left[C\theta\right] + c_0 \left[C\right]$. We can recover $\mathbf{c}_\infty = (c_d, \ldots, c_0)$ from $\mathbf{c}_k$ by setting

$$c_0 = a - \left(c_d \left[C\theta^d\right] + \ldots + c_1 \left[C\theta\right]\right)$$

For any $k \geq 1$:

$$\begin{aligned}
\|\mathbf{c}_k\| &= \sqrt{c_{d_\theta}^2 + \ldots + c_1^2 + \gamma^2} \\
&\leq \sqrt{c_{d_\theta}^2 + \ldots + c_1^2 + (\gamma - Cc_{d_\theta}\theta^{d_\theta} - \ldots - Cc_1\theta - Cc_0)^2} \\
&\leq \sqrt{c_{d_\theta}^2 + \ldots + c_1^2 + (c_{d_\theta}([Ca^{d_\theta}] - C\theta^{d_\theta}) + \ldots + c_1([Ca] - C\theta) + c_0([C] - C))^2} \\
&\leq \sqrt{c_{d_\theta}^2 + \ldots + c_1^2 + (c_{d_\theta} + \ldots + c_1 + c_0)^2} \\
&\leq \sqrt{c_{d_\theta}^2 + \ldots + c_1^2 + \left(c_{d_\theta}^2 + \ldots + c_1^2 + c_0^2\right)^2} \\
&\leq \sqrt{2\left(c_{d_\theta}^2 + \ldots + c_1^2 + c_0^2\right)^2} = \sqrt{2} \parallel \mathbf{c}_\infty\|^2
\end{aligned}$$

and this shows that although the length $\|\mathbf{c}\|$ depends on the precision of the approximation k, $\|\mathbf{c}\|$ is bounded by the fixed constant $\sqrt{2}\| \mathbf{c}_\infty\|^2$. As k increases, we expect the general size of a vector in $\mathcal{L}$ to increase, but our vector $_k$ is of bounded lenght, and thus when k is sufficiently large, this vector will be the shortest vector in the lattice.

We use Hermite's theorem to determine when the shortest vector in our lattice is a good candidate for the vector $_k$.

Theorem 1. *(Hermite) Let $\mathcal{L}$ be an n dimensional lattice and M the length of the shortest non-zero vector in $\mathcal{L}$. There exist constant $\mu_n \in \mathbb{R}_{\geq 0}$ depending only on n such that*

$$M^n \leq \mu_n d\left(\mathcal{L}\right)^2$$

where $d\left(\mathcal{L}\right)$ is the discriminant of $\mathcal{L}$.

There are bounds on these μ_n given in [10, Page 66]. For a general lattice of full rank, we expect this bound to be close to the actual size of the shortest non-zero vector in the lattice.

Proof. See [10, Page 66] □

Hermite's theorem suggests that the length of the shortest vector in $\mathcal{L}_k$ is approximately $d\left(\mathcal{L}_k\right)^{\frac{1}{d+1}}$. In our case, $d\left(\mathcal{L}\right) = \det\left(A\right) = C = 10^{k'}$; and so if our minimal polynomial has coefficients of order 10^n, k, k' are such that:

$$\left(d_\theta + 1\right) 10^{2n} \leq 10^{k'/(d_\theta+1)}.$$

and if the shortest vector in $\mathcal{L}$ is shorter than $d\left(\mathcal{L}\right)^{\frac{1}{d_\theta+1}}$, then it is a suitable candidate for the vector we are looking for. As before, we search for the shortest vector in the lattice using the `Magma` command `ShortestVectors` (see [2]).

Remark 4.1. When the imaginary part of θ is not 0, the same method can be used but with $\mathcal{L}_k$ being generated by the columns of

$$A_k = \begin{pmatrix} 1 & \dots & 0 & 0 \\ 0 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \\ \left[C\mathrm{Re}\left(\theta^d\right)\right] & \dots & \left[C\mathrm{Re}\left(\theta\right)\right] & [C] \\ \left[C\mathrm{Im}\left(\theta^d\right)\right] & \dots & \left[C\mathrm{Im}\left(\theta\right)\right] & 0 \end{pmatrix}$$

where $\mathrm{Re}(\theta)$ and $\mathrm{Im}(\theta)$ denote the real and imaginary parts of θ.

To summarise, the strategy for finding the coefficients of the minimal polynomial of α is as follows.

1. Choose d.
2. Define the lattice $\mathcal{L}_k$.
3. In $\mathcal{L}_k$ look for vectors which are shorter than, say $1/1000d\left(\mathcal{L}_k\right)^{\frac{1}{d+1}}$. If such a vector doesn't exists, either increase the precision k and start again, or choose a different degree and start again.
4. If such a vector exists, verify that θ is an approximate solution of the corresponding polynomial. If this is not the case, choose a different degree and start again.

Note that regarding the choice of degree, we start with $d = 1$ and run through the natural number until we find a suitable vector.

4.2. **Coefficient Relations.** Suppose $(\alpha_1, \dots, \alpha_6)$ define a rational function h on C, which corresponds to a 3-torsion point as in Section 2. Let f_i be the minimal polynomial of α_i and set $d_i = \deg(f_i)$. For a fixed root $\alpha = \alpha_1$ of f_1, we want to determine the roots of $f_2, \dots, f_6$ defining h, and thus the corresponding 3-torsion point. Simplest way theoretically of doing this is to compute all possible six tuples of roots, and simply test whether each possibility defines a 3-torsion points. However, this is incredibly impractical, especially when the degrees of the minimal polynomials are large. Instead, we explain an alternative method to compute relations amongst the coefficients using lattice reduction.

Firstly, we can try to express $\alpha_2, \dots, \alpha_6$ in terms of powers of α. Let $K_1 = \mathbb{Q}(\alpha)$ be the number field defined by α. If f_2 has a root over K_1, we can write it as

$$b_{d_1}\alpha_2 = b_{d_1-1}\alpha^{d_1-1} + \dots + b_1\alpha + b_0$$

for some $b_0, \dots, b_{d_1} \in \mathbb{Z}$. Let a_1, a_2 be complex approximations of α, α_2 correct to k decimal places. If $a_1, a_2 \in \mathbb{R}$, that is the imaginary part of both a_1 and a_2 is small, we search for $b_0, \dots, b_{d_1}$ by looking for short vectors in the lattice generated by the columns of

$$A_k = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ \left[Ca_1^{d_1-1}\right] & \dots & [Ca_1] & [Ca_2] & [C] \end{pmatrix}$$

where C is a constant of order 10^k, chosen as before. If $a_1, a_2 \notin \mathbb{R}$, we instead search for short vectors in the lattice generated by the columns of

$$A_k = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ \left[C\mathrm{Re}\left(a_1^{d_1-1}\right)\right] & \dots & \left[C\mathrm{Re}\left(a_1\right)\right] & \left[C\mathrm{Re}\left(a_2\right)\right] & [C] \\ \left[C\mathrm{Im}\left(a_1^{d_1-1}\right)\right] & \dots & \left[C\mathrm{Im}\left(a_1\right)\right] & \left[C\mathrm{Im}\left(a_2\right)\right] & 0 \end{pmatrix}$$

Remark 4.2. If no relations as above exist, we can use a similar lattice method to look for higher order relations, that could help to identify the corresponding the root of f_2. In practice, we were able to compute relations as above in our examples.

When the degrees d_i are small, factorising our polynomials can often be quicker than searching for coefficient relations. Suppose a_i is a complex approximation of α_i, and f_i is the minimal polynomial of α_i. Over $\mathbb{C}$, f_i can be factorised into linear factors.

$$f_i = s_1 \dots s_{d_i}$$

For k large enough, there is an n such that $s_n\left(a_i\right)$ is almost zero. Thus s_n corresponds to the required root of f_i.

Checking the correctness of our minimal polynomials and coefficient is straightforward. We simply define the points determined by our candidate polynomials and check that they are solutions of our defining set of equations.

5. Examples

Using the method described in Sections 2-4, we computed the 3-torsion subgroup of the modular Jacobians $J_0(30)$ and $J_0(40)$.

The `MAGMA` code in the computations presented in this section can be found at

https://github.com/ElviraLupoian/3TorsionOfGenus3HypCurves

5.1. $J_0(30)[3]$. We work with the model of the modular curve $X_0(30)$ given by `Magma`

$$y^2 + \left(-x^4 - x^3 - x^2\right)y = 3x^7 + 19x^6 + 60x^5 + 110x^4 + 121x^3 + 79x^2 + 28x + 4$$

Completing the square gives a model of the form required by section 2,

$$y^2 = x^8 + 14x^7 + 79x^6 + 242x^5 + 441x^4 + 484x^3 + 316x^2 + 112x + 16$$

The scheme of 3-torsion points is defined by 10 equations

$$-\alpha_2^2 + \alpha_6^2 - \alpha_7\alpha_{10}^3,$$

$$-2\alpha_1\alpha_2 - 14\alpha_2^2 + 2\alpha_5\alpha_6 - 3\alpha_7\alpha_9\alpha_{10}^2,$$

$$-\alpha_1^2 - 28\alpha_1\alpha_2 - 79\alpha_2^2 - 2\alpha_2 + 2\alpha_4\alpha_6 + \alpha_5^2 - 3\alpha_7\alpha_8\alpha_{10}^2 - 3\alpha_7\alpha_9^2\alpha_{10},$$

$$-14\alpha_1^2 - 158\alpha_1\alpha_2 - 2\alpha_1 - 242\alpha_2^2 - 28\alpha_2 + 2\alpha_3\alpha_6 + 2\alpha_4\alpha_5 - 6\alpha_7\alpha_8\alpha_9\alpha_{10} - \alpha_7\alpha_9^3 - 3\alpha_7\alpha_{10}^2,$$

$$-79\alpha_1^2 - 484\alpha_1\alpha_2 - 112\alpha_1\alpha_6 - 28\alpha_1 - 441\alpha_2^2 - 2\alpha_2\alpha_6 - 158\alpha_2 + 2\alpha_3\alpha_5 + \alpha_4^2 + 2820\alpha_6 - 3\alpha_7\alpha_8^2\alpha_{10}$$
$$- 3\alpha_7\alpha_8\alpha_9^2 - 6\alpha_7\alpha_9\alpha_{10} - 1,$$

$$-242\alpha_1^2 - 882\alpha_1\alpha_2 - 112\alpha_1\alpha_5 - 2\alpha_1\alpha_6 - 158\alpha_1 - 484\alpha_2^2 - 2\alpha_2\alpha_5 - 484\alpha_2 + 2\alpha_3\alpha_4 + 2820\alpha_5$$
$$- 112\alpha_6 - 3\alpha_7\alpha_8^2\alpha_9 - 6\alpha_7\alpha_8\alpha_{10} - 3\alpha_7\alpha_9^2 - 14,$$

$$-441\alpha_1^2 - 968\alpha_1\alpha_2 - 112\alpha_1\alpha_4 - 2\alpha_1\alpha_5 - 484\alpha_1 - 316\alpha_2^2 - 2\alpha_2\alpha_4 - 882\alpha_2 + \alpha_3^2 + 2820\alpha_4 - 112\alpha_5$$
$$2\alpha_6 - \alpha_7\alpha_8^3 - 6\alpha_7\alpha_8\alpha_9 - 3\alpha_7\alpha_{10} - 79,$$

$$
\begin{aligned}
&-484\alpha_1^2 - 632\alpha_1\alpha_2 - 112\alpha_1\alpha_3 - 2\alpha_1\alpha_4 - 882\alpha_1 - 112\alpha_2^2 - 2\alpha_2\alpha_3 - 968\alpha_2 + 2820\alpha_3 - 112\alpha_4 - 2\alpha_5\\
&\qquad - 3\alpha_7\alpha_8^2 - 3\alpha_7\alpha_9 - 242,\\
&2820\alpha_1^2 - 112\alpha_1\alpha_2 - 2\alpha_1\alpha_3 - 158888\alpha_1 - 3452\alpha_2 - 112\alpha_3 - 2\alpha_4 - 3\alpha_7\alpha_8 + 1987659,\\
&2820\alpha_1 - 112\alpha_2 - 2\alpha_3 - \alpha_7 - 158404,
\end{aligned}
$$

where the 3-torsion points are classes of divisors of the form $\frac{1}{3}\mathrm{div}\,(h)$

$$
\begin{aligned}
h = {} & x^2y - x^6 - 7x^5 - 15x^4 + \alpha_1\left(xy - x^5 - 7x^4\right) + \alpha_2\left(y - x^4\right) + \alpha_3x^3\\
& + \alpha_4x^2 + \alpha_5x + \alpha_6
\end{aligned}
$$

By approximating the solutions of the above system and then finding precise algebraic expressions for the 3-torsion points, we find that $J_0(30)[3] \cong (\mathbb{Z}/3\mathbb{Z})^6$ can be generated using 3 Galois orbits, 2 consisting of 8 points each, and 1 consisting of 6 points.

For each orbit, we give the minimal polynomial of α_1 and expressions for $\alpha_2, \ldots, \alpha_6$ in terms of α_1.

$u^6 - 21u^5 + 184u^4 - 861u^3 + 2296u^2 - 3381u + 2439$
$\alpha_1 = u$
$\alpha_2 = u - 2$
$\alpha_3 = (1/639)\left(4u^5 - 70u^4 + 704u^3 - 3962u^2 - 3192u - 10638\right)$
$\alpha_4 = (1/213)\left(4u^5 - 70u^4 + 704u^3 - 3962u^2 + 5541u - 7230\right)$
$\alpha_5 = (1/213)\left(4u^5 - 70u^4 + 704u^3 - 3962u^2 + 8310u - 8934)\right)$
$\alpha_6 = (1/639)\left(4u^5 - 70u^4 + 704u^3 - 3962u^2 + 9588u - 10638\right)$

$u^8 - 28u^7 + 343u^6 - 2401u^5 + 10414u^4 - 28147u^3 + 45290u^2 - 39200u + 13925$
$\alpha_1 = u$
$\alpha_2 = 2u - 2$
$\alpha_3 = (1/2169)\left(16u^7 - 392u^6 + 4116u^5 - 24010u^4 + 83312u^3 - 168882u^2 + 113309u - 54568\right)$
$\alpha_4 = (1/723)\left(32u^7 - 784u^6 + 8232u^5 - 48020u^4 + 166624u^3 - 337764u^2 + 326392u - 119258\right)$
$\alpha_5 = (1/723)\left(64u^7 - 1568u^6 + 16464u^5 - 96040u^4 + 333248u^3 - 675528u^2 + 699056u - 279004\right)$
$\alpha_6 = (1/2169)\left(128u^7 - 3136u^6 + 32928u^5 - 192080u^4 + 666496u^3 - 1351056u^2 + 1427032u - 592712\right)$

$u^8 - 86u^7 + 2449u^6 - 33383u^5 + 252436u^4 - 1109723u^3 + 2786294u^2 - 3689116u + 2224811$
$\alpha_1 = u$
$\alpha_2 = (1/1214905376480298255)(29876018790328u^7 - 2417413903833052u^6 + 60684703080638118u^5$
$- 674976608990629628u^4 + 3832952879194486442u^3 - 11087064205570838970u^2$
$+ 16027124735004738752u - 11008190935547438114)$
$\alpha_3 = (-1/1214905376480298255)(226884728945872u^7 - 18363364083540328u^6 + 460287793516793082u^5$
$- 5069981080078429502u^4 + 28138121917331765018u^3 - 77651266046887373580u^2$

$+ 119961145357139022083u - 45446963859192685796)$

$\alpha_4 = (-1/404968458826766085)(221239419854296u^7 - 17945665351388284u^6 + 451320054316335906u^5$
$- 4984082896579474376u^4 + 27907810187789236094u^3 - 78911274653216131110u^2$
$+ 111314232875845983914u - 60056349012914418458)$

$\alpha_5 = (-1/1214905376480298255)(593735119981072u^7 - 48868278713945128u^6 + 1258524218508960012u^5$
$- 14170047695264405192u^4 + 81156089944126098548u^3 - 237313632893922545220u^2$
$+ 339196464518479391108u - 198602211969557067116)$

$\alpha_6 = (-1/242981075296059651)(35094171383296u^7 - 3004896812056480u^6 + 81787675076005272u^5$
$- 944075033879118080u^4 + 5498949927080657672u^3 - 16418946803186159928u^2$
$+ 23935267946866848320u - 14729053581484018328)$

The field of definition of definition of all 3-torsion points defined by the above expressions is the degree 144 number field L defined as follows. Let K be the degree 48 number field defined by

$$x^{48} - 9x^{47} + 36x^{46} - 75x^{45} + 57x^{44} + 45x^{43} + 114x^{42} - 1134x^{41} + 2649x^{40} - 2694x^{39} - 9x^{38} + 3708x^{37} - 4208x^{36} - 549x^{35} - 477x^{34} + 24297x^{33} - 35388x^{32} - 15957x^{31} - 58908x^{30} + 587655x^{29} - 1095192x^{28} + 147498x^{27} + 2477835x^{26} - 4287114x^{25} + 2891076x^{24} + 570960x^{23} - 2932713x^{22} + 2692353x^{21} - 803187x^{20} - 889560x^{19} + 1287588x^{18} - 729954x^{17} + 58869x^{16} + 358671x^{15} - 388314x^{14} + 194094x^{13} - 21821x^{12} - 50094x^{11} + 63396x^{10} - 45024x^9 + 22035x^8 - 8640x^7 + 2955x^6 - 684x^5 + 111x^4 - 24x^3 + 1$$

then, L is the degree 6 extension of K defined by

$$x^6 - 21x^5 + 184x^4 - 861x^3 + 2296x^2 - 3381x + 2439$$

We verify that the above generate the entire 3-torsion subgroup as follows. We form the subgroup H of 3-torsion points generated by the above, as a subgroup of $J_0(30)(L)_{\text{tors}}$, and reduce modulo an ideal of $\mathcal{O}_L$ of norm 529. As 23 is prime of good reduction for the curve, the induced reduction map on the Jacobian is injective on torsion. We verify that the image of the H under the reduction map is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^6$. Since the genus is 3 and the reduction map is injective, $H \cong (\mathbb{Z}/3\mathbb{Z})^6$ is the entire 3-torsion subgroup $J_0(30)[3]$.

5.2. $J_0(40)[3]$**.** We work with the model of the modular curve $X_0(30)$ given by `Magma`

$$y^2 + (-x^4 - 1)y = 2x^6 - x^4 + 2x^2$$

Completing the square gives a model of the form required by section 2,

$$y^2 = x^8 + 8x^6 - 2x^4 + 8x^2 + 1$$

The scheme of 3-torsion points is defined by 10 equations

$\alpha_2^2 - \alpha_6^2 - \alpha_9^3\alpha_{10}$,

$2\alpha_1\alpha_2 - 2\alpha_5\alpha_6 - 3\alpha_8\alpha_9^2\alpha_{10}$,

$\alpha_1^2 + 8\alpha_2^2 + 2\alpha_2 - 2\alpha_4\alpha_6 - \alpha_5^2 - 3\alpha_7\alpha_9^2\alpha_{10} - 3\alpha_8^2\alpha_9\alpha_{10}$,

$16\alpha_1\alpha_2 + 2\alpha_1 - 2\alpha_3\alpha_6 - 2\alpha_4\alpha_5 - 6\alpha_7\alpha_8\alpha_9\alpha_{10} - \alpha_8^3\alpha_{10} - 3\alpha_9^2\alpha_{10}$,

$8\alpha_1^2 - 2\alpha_2^2 + 2\alpha_2\alpha_6 + 16\alpha_2 - 2\alpha_3\alpha_5 - \alpha_4^2 + 8\alpha_6 - 3\alpha_7^2\alpha_9\alpha_{10} - 3\alpha_7\alpha_8^2\alpha_{10} - 6\alpha_8\alpha_9\alpha_{10} + 1$,

$$-4\alpha_1\alpha_2 + 2\alpha_1\alpha_6 + 16\alpha_1 + 2\alpha_2\alpha_5 - 2\alpha_3\alpha_4 + 8\alpha_5 - 3\alpha_7^2\alpha_8\alpha_{10} - 6\alpha_7\alpha_9\alpha_{10} - 3\alpha_8^2\alpha_{10},$$
$$-2\alpha_1^2 + 2\alpha_1\alpha_5 + 8\alpha_2^2 + 2\alpha_2\alpha_4 - 4\alpha_2 - \alpha_3^2 + 8\alpha_4 + 2\alpha_6 - \alpha_7^3\alpha_{10} - 6\alpha_7\alpha_8\alpha_{10} - 3\alpha_9\alpha_{10} + 8,$$
$$16\alpha_1\alpha_2 + 2\alpha_1\alpha_4 - 4\alpha_1 + 2\alpha_2\alpha_3 + 8\alpha_3 + 2\alpha_5 - 3\alpha_7^2\alpha_{10} - 3\alpha_8\alpha_{10},$$
$$8\alpha_1^2 + 2\alpha_1\alpha_3 + 8\alpha_2 + 2\alpha_4 - 3\alpha_7\alpha_{10} - 18,$$
$$8\alpha_1 + 2\alpha_3 - \alpha_{10},$$

where the 3-torsion points are classes of divisors of the form $\frac{1}{3}\mathrm{div}\,(h)$,

$$h = x^2y - x^6 - 4x^4 + \alpha_1\left(xy - x^5\right) + \alpha_2\left(y - x^4\right) + \alpha_3x^3 + \alpha_4x^2 + \alpha_5x + \alpha_6$$

By approximating the solutions of the above system and then finding precise algebraic expressions for the 3-torsion points, we find that $J_0(40)[3] \cong (\mathbb{Z}/3\mathbb{Z})^6$ can be generated using 3 Galois orbits, 2 consisting of 6 points each, and 1 consisting of 8 points.

For each orbit, we give the minimal polynomial of α_1 and expressions for $\alpha_2, \ldots, \alpha_6$ in terms of α_1.

$u^6 + 4u^4 - 8u^2 + 12$
$\alpha_1 = u$
$\alpha_2 = u + 1$
$\alpha_3 = (-1/9)(u^5 + u^3 + 16u + 18)$
$\alpha_4 = (-1/3)(u^5 + u^3 + 4u + 3)$
$\alpha_5 = (-1/3)(u^5 + u^3 + u - 6)$
$\alpha_6 = (-1/9)(u^5 + u^3 + 7u + 9)$

$u^6 - 6u^5 + 4u^4 + 24u^3 + 256u^2 - 576u + 324$
$\alpha_1 = u$
$\alpha_2 = (1/198)(-u^4 + 4u^3 + 58u^2 - 124u + 126)$
$\alpha_3 = (-1/99)(u^4 - 4u^3 - 58u^2 + 322u + 468)$
$\alpha_4 = (-1/99)(u^4 - 4u^3 - 58 * u^2 - 74u + 765)$
$\alpha_5 = (-1/99)(u^4 - 4u^3 - 58u^2 - 173u + 468)$
$\alpha_6 = (1/198)(u^4 - 4u^3 - 58u^2 + 520u - 522)$

$u^8 - 126u^4 - 648u^2 - 1323$
$\alpha_1 = u$
$\alpha_2 = -1$
$\alpha_3 = (1/189)(u^7 - 63u^3 - 648u)$
$\alpha_4 = 3$
$\alpha_5 = -u$
$\alpha_6 = 1$

The field of definition of the 3-torsion subgroup is the degree 48 number field defined by

$$x^{48} - 22x^{47} + 220x^{46} - 1298x^{45} + 4840x^{44} - 10758x^{43} + 7848x^{42} + 30564x^{41} - 90644x^{40} - 54378x^{39} + 983934x^{38} - 3228430x^{37} + 6037118x^{36} - 6706868x^{35} + 3859158x^{34} - 6290682x^{33} + 41469355x^{32} - 151827480x^{31} + 375328308x^{30} - 727099012x^{29} + 1204881284x^{28} - 1812362612x^{27} + 2558319144x^{26} - 3402905364x^{25} + 4192192588x^{24} - 4669768140x^{23} + 4602283152x^{22} - 3939374364x^{21} + 2873125672x^{20} - 1738390504x^{19} + 830314684x^{18} - 275496188x^{17} + 30094447x^{16} + 31178478x^{15} - 22364652x^{14} + 5362086x^{13} + 2307708x^{12} - 2995626x^{11} + 1676724x^{10} - 615660x^{9} + 121728x^{8} + 25686x^{7} - 31194x^{6} + 9162x^{5} + 1458x^{4} - 2088x^{3} + 738x^{2} - 126x + 9$$

Checking that the above orbits generate the entire 3-torsion subgroup of $J_0(40)$ can be done as in the previous example.

6. Local Conductor Exponent at 2

Throughout this section, C/K will denote a smooth, projective, hyperelliptic curve defined over K, a finite extension of $\mathbb{Q}_2$. Let J be the Jacobian variety associated to C, $T = T_l J$ the l-adic Tate module and $V = V_l J = T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ the associated l-adic representation, where l is any prime different from 2. The conductor exponent of such a representations, as defined in [6] and [14] , is

$$n = \int_{-1}^{\infty} \mathrm{codim} V^{G_K^u}\ du$$

where $G_K = \mathrm{Gal}\left(\overline{K}/K\right)$ is the absolute Galois group of K and $\{G_K^u\}_{u\geq -1}$ denote the ramification groups of G_K in upper numbering. The tame and wild parts are defined as

$$n_{\text{tame}} = \int_{-1}^{0} \mathrm{codim} V^{G_K^u}\ du$$

$$n_{\text{wild}} = \int_{0}^{\infty} \mathrm{codim} V^{G_K^u}\ du$$

Remark 6.1. The definition is independent of the choice of prime l, see [14].

Our approach is to take $l = 3$ and use the 3-torsion subgroup, computed as in Section 2 to 4.

6.1. **Tame Conductor.** From the above, the tame part of the conductor can be computed as

$$n_{\text{tame}} = 6 - \dim V_3 J^I$$

where $I \leqslant G_K$ is the inertia subgroup.

Alternatively, we can also also deduce the tame part of the conductor from the regular model of C. From a regular model of C over $\mathbb{Z}_2$ we can calculate

- the abelian part a, equal to the sum of the genera of all components of the model
- the toric part t, equal to the number of loops in the dual graph of C

Then, the tame part of the exponent is equal to $6 - 2a - t$, see [1, Chapter 9] for details. Regular models can often be computed using the method described in [4], however, this is often a challenging problem.

6.2. **Wild Conductor.** Recall that we wish to compute

$$n_{\text{wild}} = \int_0^\infty \text{codim} V^{G_K^u} \, du$$

For $u \geq 0$, G_K^u is pro-p and $\text{codim} V^{G_K^u} = \text{codim} \bar{V}^{G_K^u} = \text{codim} J[3]^{G_K^u}$, see [14]. We may replace G_K by $G = \text{Gal}(K(J[3])/K)$, and thus

$$n_{\text{wild}} = \int_0^\infty \text{codim} J[3]^{G^u} \, du$$

Alternatively, using the definition of G^u and G_u, the ramification groups in upper numbering and lower numbering respectively, we find

$$n_{\text{wild}} = \int_0^\infty \frac{\text{codim} J[3]^{G_u}}{[G_0 : G_u]} \, du = \sum_{k=0}^{\infty} \frac{\text{codim} J[3]^{G_k}}{[G_0 : G_k]}$$

Remark 6.2. Using our presentation of $J[3]$, the ramification groups G_u and their action on $J[3]$ are completely explicit; and as a result n_{wild} is a straightforward computation.

7. Example

Recall that the 3-torsion subgroup $J_0(40)[3]$ is defined over a degree 48 number field defined by the polynomial f, stated in Section 5.2. This polynomial remains irreducible over $\mathbb{Q}_2$, and defines a degree 48 Galois extension of $\mathbb{Q}_2$, which we denote by L. Let $G = \text{Gal}(L/\mathbb{Q}_2)$. We find that G can be generated by τ_1,τ_2,β, σ_1, σ_2, where τ_i have order 2, β has order 3 and σ_j have order 4. Then,

$$\begin{aligned}
&G_0 = \langle \tau_1, \beta, \sigma_1, \sigma_2 \rangle \text{ and } |G_0| = 24 \\
&G_1 = \langle \tau_1, \sigma_1, \sigma_2 \rangle \text{ and } |G_1| = 8 \\
&G_2 = G_3 = \langle \tau_1 \rangle \text{ and } |G_2| = |G_3| = 2 \\
&G_n = 1 \text{ for all } \ n \geq 4
\end{aligned}$$

Using the explicit generators stated in section 5.2, we can compute the Galois invariants

$$\begin{aligned}
J_0(40)^{G_0} &\cong (\mathbb{Z}/3\mathbb{Z})^2 \\
J_0(40)^{G_1} &\cong (\mathbb{Z}/3\mathbb{Z})^4 \\
J_0(40)^{G_2} &\cong (\mathbb{Z}/3\mathbb{Z})^4
\end{aligned}$$

and thus

$$n_{\text{wild}} = 4/1 + 2/3 + 2/12 + 2/12 = 5$$

As $X_0(40)$ is a modular curves, we may compute its conductor from the isogenous decomposition of its Jacobian into a product of abelian varieties of smaller dimension. The modular Jacobian $X_0(N)$ is isogenous to $\oplus_f A_f$ where A_f is the abelian variety associated to a newform $f \in S_2(M_f)$ of some level M_f, and the direct sum is over equivalence classes of newforms in $S_2(N)$. These can be computed using Stein's modular symbols algorithms and its implementation in `Magma`, see [11]. The conductor of $J_0(N)$ is equal to product, over equivalence classes of newforms in $S_2(N)$, of the conductors of A_f. This is clear from the definition of the conductor, as given in Section 6, if we take $l \neq p$ and not dividing the degree of the isogeny.

In this example using Magma, we find

$$J_0(40) \simeq E_1 \oplus E_2 \oplus E_3$$

where E_i are abelian varieties of dimension 1, and conductors $2^3 \cdot 5$, $2^2 \cdot 5$ and $2^2 \cdot 5$, respectively. This suggests that $n_2 = 7$.

Remark 7.1. The above suggest that $n_{\text{tame}} = 2$, but the author is yet to verify this directly.

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21. Springer Science & Business Media, 2012. 6.1

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 4.1

[3] P. Breiding and S. Timme. Homotopycontinuation.jl: A package for homotopy continuation in julia, 2018. 3, 3

[4] T. Dokchitser. Models of curves over dvrs. *arXiv preprint arXiv:1807.00025*, 2018. 6.1

[5] T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan. Arithmetic of hyperelliptic curves over local fields. *arXiv preprint arXiv:1808.02936*, 2018. 1

[6] T. Dokchitser and C. Doris. 3-torsion and conductor of genus 2 curves. *Mathematics of Computation*, 88(318):1913–1927, 2019. 1, 6

[7] E. Flynn. The arithmetic of hyperelliptic curves. In *Algorithms in Algebraic Geometry and Applications*, pages 165–175. Springer, 1996. 1, 2

[8] E. Lupoian. Two-torsion subgroup of some modular jacobians. *arXiv preprint arXiv:2205.13017*, 2022. 1

[9] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 1994. 1

[10] N. P. Smart. *The algorithmic resolution of Diophantine equations: a computational cookbook*, volume 41. Cambridge university press, 1998. 4.1

[11] W. A. Stein. *Modular forms, a computational approach*, volume 79. American Mathematical Soc., 2007. 7

[12] J. Stoer, R. Bulirsch, R. Bartels, W. Gautschi, and C. Witzgall. *Introduction to numerical analysis*, volume 1993. Springer, 1980. 3, 3

[13] M. Stoll. Arithmetic of hyperelliptic curves. *Summer Semester*, 2014. 1, 2

[14] D. Ulmer. Conductors of l-adic representations. *Proceedings of the American Mathematical Society*, 144:2291–2299, 2016. 6, 6.1, 6.2

[15] J. Verschelde. Homotopy continuation methods for solving polynomial systems. 1998. 3

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom
Email address: e.lupoian@warwick.ac.uk