SECOND YEAR REPORT

ELVIRA LUPOIAN

This report will present some of my recent work on the two-torsion subgroup of Jacobians of non-hyperelliptic curves. I will focus on curves of genus 5 and explain how the methods presented in my first year report generalise to this case.

The first section will be a brief overview some preliminary results which relate the two-torsion subgroup to the theta hyperplanes to the curve. The second, third and fourth sections will explain how these theta hyperplanes are calculated. In section 5 we calculate the two-torsion subgroup of the modular curve $X_0(42)$ using the methods of sections 2 to 4.

In the final section I will talk about how some of the previous calculations can be simplified by working over a field of characteristic 2.

1. Theta Characteristics and Two Torsion

This section will give a brief overview of [9][Chapter 5], establishing a correspondence between the two-torsion subgroup and the theta hyperplanes to a curve.

Definition. A symplectic space over a field k is a pair (V, b_V), where V is a finite dimensional k vector space and b_V is a nondegenerate alternating bilinear form on V.

Definition. A quadratic form q on (V, b_v) is a quadratic form on V, such that the corresponding alternating form $b_q(v, w) := q(v + w) - q(v) - q(w)$ coincides with b_V on V.

Remark. When the characteristic of k is not 2, given b_q we can recover the quadratic form q in a unique way, $2q(v) = b_q(v, v)$. However when k has characteristic 2, many quadratic forms correspond to the same bilinear form b_q.

Lemma 1. *Any symplectic space (V, b_V) is even dimensional and it admits a basis*

$$B = (e_1, \dots, e_n, f_1, \dots f_n)$$

with the following properties:

- $b_V(e_i, e_j) = b_V(f_i, f_j) = 0$ *for all* i, j
- $b_V(e_i, f_j) = \delta_{i,j}$ *for all* i, j

Note. A basis as above is called a symplectic basis.

Proof. See [16, Lemma1.2] □

Fix a symplectic space (V, b_V) over $\mathbb{F}_2$, with a symplectic basis $(e_1, \dots, e_n, f_1, \dots f_n)$. Let $Q(V)$ be the set of quadratic forms on (V, b_V). For any $q \in Q(V)$ and $v \in V$, a new quadratic form $q + v \in Q(V)$ can be defined by

$$(q + v)(x) = q(x) + b_V(v, x) \text{ for all } x \in V$$

Date: March 2022.

The addition of two quadratic forms $q, q^{'} \in Q(V)$ is also well defined by setting $q + q' = v \in V$ where v is a unique element of V with $q^{'} = q + v$. In this way, $\widetilde{V} = Q(V) \sqcup V$ is a $2g+1$ dimensional vector space over $\mathbb{F}_2$.

Definition. Let $q \in Q(V)$. The Arf invariant of q is

$$\operatorname{Arf}(q) = \sum_{i=1}^{n} q(e_i)\, q(f_i) \mod 2$$

Proposition 2. *The Arf invariant of any $q \in Q(V)$ is well defined and it's independent of the choice of symplectic basis.*

Proof. See [11, Page 36]. □

Definition. A quadratic form on (V, b_V) is called odd, resp. even, if $\operatorname{Arf}(q) = 1$, resp. 0.

Let $Q(V)_+$ be the set of even quadratic forms and $Q(V)_-$ the set of odd quadratic forms.

There is a natural action of the symplectic group $\operatorname{Sp}(V)$ on $Q(V)$. For any $T \in \operatorname{Sp}(V), q \in Q(V)$ define $T \cdot q \in Q(V)$ by

$$(T \cdot q)(x) = q\left(T^{-1}(x)\right) \text{ for all } x \in V$$

The two orbits of this action are $Q(V)_+$ and $Q(V)_-$.

Throughout this report, a curve over a field k will always be a 1-dimensional, projective, smooth and absolutely irreducible k-variety. The Jacobian of C will be it's Jacobian variety, and for computational purposes we identify the Jacobian with the zero Picard group of C.

Let C be a genus g curve over $\mathbb{Q}$. We'll denote its Jacobian variety by J_C and its function field by $k(C)$. Let $J_C[2] = J_C\left(\overline{\mathbb{Q}}\right)[2]$ be the two torsion subgroup of the Jacobian. Recall $J_C[2] \cong \mathbb{F}_2^{2g}$, so $J_C[2]$ can be regarded as a $2g$-dimensional vector space over $\mathbb{F}_2$. Moreover, it is a symplectic space with the Weil pairing which is defined as follows.

For any $f \in k(C) \setminus \{0\}$ and any divisor $D = \sum_{P \in C} n_P P$ on C with support disjoint from the support of $\operatorname{div}(f)$, define $f(D) = \prod_{P \in C} f(P)^{n_P}$.

Remark. Observe that $f(D_1 + D_2) = f(D_1) f(D_2)$ for any two divisors D_1, D_2 with support disjoint from $\operatorname{div}(f)$.

Theorem 3. *(Weil Reciprocity Law) For any $f, g \in k(C) \setminus \{0\}$ with disjoint support*

$$f(div(g)) = g(div(f))$$

Proof. See [12, Page 242]. □

Let $E_1, E_2 \in J_C[2]$, and take any representatives of these classes D_1, D_2 such that $2D_i = \operatorname{div}(f_i)$ for some $f_i \in k(C) \setminus \{0\}$ whose divisors have disjoint support.

Observe

$$\left(\frac{f_1(D_2)}{f_2(D_1)}\right)^2 = \frac{f_1(2D_2)}{f_2(2D_1)} = \frac{f_1(\operatorname{div}(f_2))}{f_2(\operatorname{div}(f_1))} = 1$$

Thus $\frac{f_1(D_2)}{f_2(D_1)} = \pm 1$, and define

$$e_2(E_1, E_2) = \begin{cases} 1 \text{ if } f_1(D_2)/f_2(D_1) = -1 \\ 0 \text{ otherwise} \end{cases}$$

This is known as the Weil pairing on $J_C[2]$.

Suppose $D_1' = D_1 + \operatorname{div}(h_1)$ and $D_2' = D_2 + \operatorname{div}(h_2)$ for two rational function h_1, h_2 on C. Applying the Weil Reciprocity Law twice shows

$$\frac{f_1\left(D_2'\right)}{f_2\left(D_1'\right)} = \frac{f_1(D_2) f_1(\operatorname{div}(h_2))}{f_2(D_1) f_2(\operatorname{div}(h_1))} = \frac{f_1(D_2) h_2(\operatorname{div}(f_1))}{f_2(D_1) f_1(\operatorname{div}(f_2))} = \frac{f_1(D_2)}{f_2(D_1)} \left(\frac{h_2(D_1)}{h_1(D_2)}\right)^2 = \frac{f_1(D_2)}{f_2(D_1)}$$

hence the Weil pairing is independent of the choice of representatives of E_1 and E_2, and thus it is well defined.

Elementary calculations show

- e_2 is bilinear
- e_2 is symplectic : $e_2(E, E) = 0$ for all $E \in J_C[2]$
- e_2 is alternating : $e_2(E_1, E_2) = -e_2(E_2, E_1)$ for all $E_i \in J_C[2]$

and therefore the Weil pairing defines a nondegenerate alternating bilinear form on $J_C[2]$ with values in $\mathbb{F}_2$, giving $J_C[2]$ the structure of a $2g$-dimensional symplectic space over $\mathbb{F}_2$.

Fix a curve C of genus g over a field $\mathbb{Q}$. Let J_C be its Jacobian with $J_C[2] := J_C\left(\overline{\mathbb{Q}}\right)[2]$ the two torsion subgroup.

Definition. A theta characteristic on C is a divisor class $\theta \in \operatorname{Pic}^{g-1}(C)$ with $2\theta = K_C$, where K_C is the canonical class of the curve C.

Let $\operatorname{TChar}(C)$ be the set of theta characteristics on C. For any $\theta_1, \theta_2 \in \operatorname{TChar}(C)$, $2\theta_1 - 2\theta_2 = K_C - K_C = 0$ and so $\theta_1 - \theta_2 \in J_C[2]$, and there are 2^{2g} theta characteristics.

Definition. The parity of a theta characteristic θ is the parity of the dimension of the Riemann-Roch space of θ.

Fact. A curve of genus g has $2^{g-1}(2^g + 1)$ even theta characteristics and $2^{g-1}(2^g - 1)$ odd theta characteristics.

For any $\theta \in \operatorname{TChar}(C)$ define

$$\begin{aligned} q_\theta : J_C[2] &\longrightarrow \mathbb{F}_2 \\ \alpha &\longmapsto l(\theta + \alpha) + l(\theta) \mod 2 \end{aligned}$$

where $l(D)$ is the dimension of the Riemann-Roch space of D.

Theorem 4. *(Riemann-Mumford Relation) The function q_θ defined by any theta characteristic θ is a quadratic form on $J_C[2]$. The associated bilinear form $b_\theta(E_1, E_2) = q_\theta(E_1 + E_2) - q_\theta(E_1) - q_\theta(E_2)$ coincides with the Weil pairing e_2 on $J_C[2]$. Moreover, the function*

$$\begin{aligned} TChar(C) &\longrightarrow Q(J_C[2], e_2) \\ \theta &\longmapsto q_\theta \end{aligned}$$

is a bijection.

Proof. See [14, Theorem 1.13] □

The notions of parity of quadratic forms and theta characteristics are consistent.

Theorem 5. *For any $\theta \in TChar(C)$, q_θ is an odd quadratic form if and only if θ is an odd theta characteristic.*

Proof. See [19, Page 186] □

From now on, we'll identify the set of odd quadratic forms on $(J_C[2], e_2)$ with the odd theta characteristics of C.

Let (V, b_V) be any symplectic space over $\mathbb{F}_2$ of dimension $2n$ and let $\mathbb{S}$ be the set of unordered pairs of elements in $Q(V)_-$. We previously defined addition on $Q(V)$, which can restricted to odd quadratic forms to give a map

$$s : \mathbb{S} \longmapsto V \setminus \{0\}$$

Definition. For any $v \in V \setminus \{0\}$. The Steiner complex of v is $\sum(v) = \bigcup_{\alpha \in s^{-1}(v)} \alpha$.

Theorem 6. *For an arbitrary symplectic space over $\mathbb{F}_2$ of dimension $2n$ there are $2^{2n}-1$ Steiner complexes. Each Steiner complex consists of $2^{n-1}\left(2^{n-1}-1\right)$ elements paired by translation $q \mapsto q+v$. An odd quadratic form q belongs to a Steiner complex $\sum(v)$ if and only if $q(v) = 0$.*

Proof. See [9, Page 227-228] □

Applying this theorem to $(J_C[2], e_2)$, since $|J_C[2] \setminus \{0\}| = 2^{2g} - 1$, Theorem 6 shows that the map defined by addition

$$Q(J_C[2], e_2)_- \times Q(J_C[2], e_2)_- \longrightarrow J_C[2]$$

is a surjection. Thus by the above, we conclude that all element of $J_C[2]$ can be expressed as the equivalence class of $\theta_1 - \theta_2$, where θ_1, θ_2 are two odd theta characteristics.

There is a geometrical interpretation of the odd theta hyperplanes.

Definition. Let $C \subset \mathbb{P}^{g-1}$ be a canonical curve of genus g, over a field $\mathbb{Q}$. A theta hyperplane to C is a hyperplane which is everywhere tangent to C.

Remark. In the genus 5 case, the theta hyperplanes are quadritangents to C.

Let $C \subseteq \mathbb{P}^4$ be a curve resulting from the intersection of 3 quadrics. This is a smooth, canonical, genus 5 curve [15, Page 346]. The intersection of a hyperplane with C is a divisor of degree 8 and rank 4, and it's in the canonical class of C. In particular, if H is tangent to C at 4 points, those points form a divisor D, such that $2D$ is in the equivalent class of K_C, so D is a theta characteristic of C.

Theorem 7. *Let C be a genus 5 curve obtained by intersecting 3 smooth quadric surfaces in $\mathbb{P}^4$. Then C has 496 quadritangent planes, in bijection with its odd theta characteristics.*

Proof. An almost identical argument to [13]. □

To find the two-torsion subgroup of the Mordell-Weil group of a genus 5, canonical, non-hyperelliptic curve we have the following strategy.

1. Find all 496 theta hyperplanes to the curve. These can be considered as non-zero rational functions on the curve.
2. All two torsion points on the Jacobian are of the form D, where $2D = \operatorname{div}(l_1) - \operatorname{div}(l_2)$, and l_1,l_2 are theta hyperplanes. These will determine generators of the 2-torsion subgroup $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^{10}$.
3. To determine the 2-torsion over any given number field K take Galois invariants.

2. Scheme of Quadritangents

This section will describe a general approach to defining a scheme of quadritangents for a given curve of genus 5. It should be noted that there is no general method for defining such a scheme, and all examples should be approached with caution. For an example of how such methods can be applied, please see section 5. The reader might find it useful to read through the explicit construction presented in section 5 before returning to this more abstract approach.

Let $C \subseteq \mathbb{P}^4$ be a genus 5, non-hyperelliptic, non-trigonal, canonical curve which has a model over $\mathbb{Q}$. As C has degree 8, by the Enriques-Babbge theorem [1, page 125], C is necessarily the intersection of 3 quadrics. That is, C is the solution set of

$$\begin{aligned} f_1(x_1, x_2, x_3, x_4, x_5) &= 0 \\ f_2(x_1, x_2, x_3, x_4, x_5) &= 0 \\ f_3(x_1, x_2, x_3, x_4, x_5) &= 0 \end{aligned}$$

for some $f_i \in \mathbb{Q}[x_1, x_2, x_3, x_4, x_5]$, homogenous of degree 2.

We work on an affine chart, say $\{x_5 = 1\}$ for notation purposes. The corresponding affine curve is the solution set of

$$F_i(x_1, x_2, x_3, x_4) = f_i(x_1, x_2, x_3, x_4, 1) = 0 \text{ for } i = 1, 2, 3$$

A general quadritangent to the affine curve is given by an equation of the form $b_1x_1+b_2x_2+b_3x_3+b_4x_4+b_5 = 0$, where at least one of the coefficients b_1, b_2, b_3, b_4 is non-zero. Assume that $b_4 \neq 0$, so the quadritangent is of the form

$$x_4 = a_1x_1 + a_2x_2 + a_3x_3 + a_4$$

for some $a_i \in \overline{\mathbb{Q}}$. The intersection of such a plane and the affine curve is given by

$$G_i(x_1, x_2, x_3) = F_i(x_1, x_2, x_3, a_1x_1 + a_2x_2 + a_3x_3 + a_4) \text{ for } i = 1, 2, 3$$

These equations can be rewritten as polynomials in x_3 with coefficients in $\mathbb{Q}[a_1, a_2, a_3, a_4][x_1, x_2]$ and degree at most 2

$$\begin{aligned} G_1 &= g_{1,2}x_3^2 + g_{1,1}x_3 + g_{1,0} \\ G_2 &= g_{2,2}x_3^2 + g_{2,1}x_3 + g_{2,0} \\ G_3 &= g_{3,2}x_3^2 + g_{3,1}x_3 + g_{3,0} \end{aligned}$$

where $g_{i,j} \in \mathbb{Q}[a_1, a_2, a_3, a_4][x_1, x_2]$.

If $g_{i,1} \neq 0$ for all i, using 2 of the above expression, say G_1 and G_2, we can obtain an expression for x_3 in terms of x_1 and x_2

$$x_3 = \varphi(x_1, x_2)$$

When calculating φ we often assume additional conditions on the $g_{i,j}$, or on their coefficients. All such conditions can be translated into equations, and additional variables if necessary, which we label as E_1. For instance, if we need to divide by a_1, we'll assume that $a_1 \neq 0$ and add the equation $v_1a_1 + 1 = 0$ to the list, where v_1 is a newly introduced variable.

If $g_{i,2} = 0$ and $g_{i,1} \neq 0$ for some i, then x_3 is simply

$$x_3 = \frac{-g_{i,0}}{g_{i,1}}$$

As before, denote by E_1 the equations introduced at this step.

Remark. For computational purposes, the resulting quadritangent schemes should be as simple as possible. Thus, at every step we should aim to have as few additional equations and variables as possible. It's

preferable in the above step that we are in the latter case, since only the condition $g_{i,1} \neq 0$ requires additional equations. Depending on the model of the curve, this can be made possible by an accommodating choice of affine coordinates and general quadritangent form. For instance, if the only monomials of f_1 divisible by x_1 and x_2 are x_1x_3 and x_2x_3, then f_1 is of the form

$$f_1 = x_1x_3 + x_2x_3 + g(x_3, x_4, x_5)$$

and we to choose to work on the affine patch $\{x_3 = 1\}$ and with planes of the form $x_1 = a_1x_2+a_2+a_3x_4+a_4x_5$. Then G_1 is

$$G_1(x_2, x_4, x_5) = (a_1 + 1)x_2 + G(x_4, x_5)$$

and for $a_1 \neq 1$

$$x_2 = \frac{-G(x_4, x_5)}{a_1 + 1}$$

with the only additional equation being $v_1(a_1 + 1) + 1 = 0$, and a single new variable v_1 is required.

Returning to the construction of the scheme, given a relation $x_3 = \varphi(x_1, x_2)$, we can substitute for x_3 in the G_i's. Clearing denominators, we obtain 2 independent polynomials in x_1 and x_2 with coefficients in $\mathbb{Q}[a_1, a_2, a_3, a_4]$. Denoted these by H_1 and H_2.

We now want to eliminate one of the variables x_1, x_2. Observe that by construction, the monomials in H_1, H_2 have degree at most 4. If for one of the variable, say x_2, the degree of x_2 is at most 2 in each monomial, then

$$H_1 = h_{1,2}x_2^2 + h_{1,1}x_2 + h_{1,0}$$
$$H_2 = h_{2,2}x_2^2 + h_{2,1}x_2 + h_{2,0}$$

for some $h_{i,j} \in \mathbb{Q}[a_1, a_2, a_3, a_4][x_1]$.

As before, we can use these expression to write x_2 as a function of x_1

$$x_2 = \phi(x_1)$$

and as before, we note any additional conditions required to derive such an expression, and convert them into a list of equations E_2, with any additional variables also noted.

Given such a ϕ, we can substitute for x_2 in H_1 (or H_2), and clear denominators to get a degree 8 polynomial

$$H_1(x_1, \phi(x_1)) = h(x_1) \in \mathbb{Q}[a_1, a_2, a_3, a_4][x_1]$$

In many case, excluding the one above, there is no clear method of eliminating x_1 or x_2, so we take the resultant with respect to one of the variables, say x_2,

$$H = \mathrm{Res}(H_1, H_2, x_2)$$

This is a polynomial in x_1, of degree at least 8 and with coefficients in $\mathbb{Q}[a_1, a_2, a_3, a_4]$. Factoring H, we expect this to be of the form

$$H(x_1) = r(x_1)h(x_1)$$

where h is irreducible of degree 8, and r is not necessarily irreducible.

The additional equations E_2 arise from any conditions required by the factor r, or its coefficients.

We define the scheme of quadritangents as follows. Given h as above, this polynomial should be a square when the stated plane is a quadritangent. That is,

$$h(x_1) = l\left(x_1^4 + a_5x_1^3 + a_6x_1^2 + a_7x_1 + a_8\right)^2$$

for some $a_5, a_6, a_7, a_8 \in \overline{\mathbb{Q}}$, and l is the leading coefficient of h.

Let E_3 be the 8 equations obtained from equating the coefficients in the above expression, and the additional equation

$$a_9\Delta + 1 = 0$$

where Δ is the discriminant of $x_1^4 + a_5x_1^3 + a_6x_1^2 + a_7x_1 + a_8$. This equation is required to ensure that the discriminant $\Delta \neq 0$ and to avoid singularities on our scheme.

The scheme of quadritangents is going to be the scheme defined by the equations in E_1, E_2 and E_3, in the variables $a_1, \ldots, a_9$ and any additional variables required by E_1 and E_2.

Warning. Taking the resultant in the derivation of h can result in points corresponding to non-quadritangent planes on our scheme. For example, if $(a_1, \ldots, a_9, \underline{a})$ is a point on our scheme, the corresponding plane $x_4 = a_1x_1 + a_2x_2 + a_3x_3 + a_4$ intersects the curve at points $(X_1, X_2, X_3, X_4, 1)$, where X_1 solves

$$f(X) = X^4 + a_5X^3 + a_6X^2 + a_7X + a_8 = 0$$

and X_2 solves

$$t(Y) = H_1(X_1, Y) = 0$$

For any root of f, the resulting equation $t(Y)$ is a polynomial of degree at least 3, which might not have repeated roots, and so the point $(X_1, X_2, X_3, X_4, 1)$, in the intersection of the plane and the curve, might have multiplicity 1 and thus the plane cannot be a quadritangent.

There is a theoretical solution to this issue. To our scheme S, add a variable x and the two equations

$$e_1 : x^4 + a_5x^3 + a_6x^2 + a_7x + a_8 = 0$$
$$e_2 : \delta = \text{Discriminant}(H_1(x, y)) = 0$$

where δ is the discriminant of $H_1(x, y)$, considered as a polynomial in y for a given x solving e_1.

This is theoretically a simple solution, but computationally it adds complications. Equation e_2 often has a high total degree (involving monomial in $a_1, \ldots, a_4$) and due to this, a start system for the homotopy describe in the next section cannot be computed in reasonable time. Also by adding x and e_1, the points of S will now be defined over the field of definition of some points on C. This can be quite different in structure to the field of definition of the quadritangents and as a result, we might not find points over a residue field and Hensel lift as in the example of Section 5.

The long (and uninteresting) solution to this problem is to acknowledge that the quadritangents will be a subscheme of S, find the points of S, define the corresponding planes and then test whether they are quadritangents.

Remark. Although this section repeatedly refers to "the" scheme of quadritangents, we should recognise the fact that we expect there to be multiple schemes of quadritangents. Clearly, not all quadritangents necessarily lie on the same affine chart and are not of the same form $x_4 = a_1x_1 + a_2x_2 + a_3x_3 + a_4$, so we should expect different schemes resulting from this. However, even for a fixed affine chart and a quadritangent form we expect multiple schemes. The equations of E_1 and E_2 result from conditions on certain polynomials being non-zero. This can be case analysed further, base on which coefficients are zero and which are non-zero. All such case will give different equations E_1 and E_2, and thus different schemes arise. Lastly, the defining equations should be irreducible (again, to avoid singularities) and so we should factorise, and consider any cases arising from this. For an explicit computation, please refer to Section 5.

3. Complex Approximations and Homotopy Continuation

Given a zero-dimensional scheme of quadritangents as constructed in the previous section, we want to find the $\overline{\mathbb{Q}}$- points lying on such as scheme. In the genus 3 and 4 case, it was possible to choose a small prime of good reduction p and a small $n \in \mathbb{N}$ such that the scheme had dimension 0 over $\mathbb{F}_p$ and all points have reductions defined over $\mathbb{F}_{p^n}$, satisfying the hypotheses of Hensel's lemma. Using Hensel's lemma, sufficiently precise p-adic approximates are obtained, which can then be used to obtained the algebraic expressions of these points using the LLL-algorithm (see First Year Report for details).

In the genus 5 case there are 496 planes and it is computationally challenging to attempt Hensel lifting. Even for primes of small norm, the increased number of equations and variables, make the previous computations very inefficient. Instead, the points on the scheme can be approximated as complex points to high precision using the Newton-Raphson method. As before, lattice based algorithms can then be used to obtain the algebraic expressions corresponding to the complex approximations.

The Newton-Raphson method requires accurate initial approximations, which can be obtained using homotopy continuation.

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, simpler system, whose solutions are easily determined. This subsection will be an overview of [10]. A more detailed approach to this theory can be found in [5] or [23].

Denote by $F(x) = 0$ a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0$$

in $x = (x_1, \ldots, x_n)$. The total degree of the system F is defined as

$$\deg(F) = \prod_{i=1}^{n} \deg(f_i)$$

Let $dF(x)$ be the Jacobian matrix of F.

Definition. A solution x^* of $F(x) = 0$ is singular if $\det(dF(x^*)) = 0$.

A homotopy is defined by

$$H : \mathbb{C}^n \times [0,1] \longrightarrow \mathbb{C}^n$$
$$H(x, \lambda) = (1 - \lambda) G(x) + \lambda \gamma F(x)$$

where $G(x)$ is a start system (details of which will be defined later) and $\gamma \in \mathbb{C}$ is a random constant.

Homotopy continuation deforms each solution of $G(x)$ into a solution of $F(x)$. Each solution of $G(x)$ is the starting point of a path in $\mathbb{C}^n \times [0,1]$ called a homotopy path.

The homogeneous part of F, denoted by F^0, is the system obtained from F by deleting the terms of lower degree in each equation. A solution at infinity of F is a solution of F^0, where the first non-zero entry if equal to 1.

Remark. If a system has a solution at infinity, the corresponding homotopy path diverges.

Any polynomial system can be transformed into an equivalent system, with no solution at infinity, for details of this construction see [10].

Given a system $F(x)$ of n equations in n variables, $x_1, \ldots, x_n$, let $\hat{F}(y)$ be the homogenization of F. This is a system of n equations in $n+1$ variables defined by

$$\hat{f}_i(y_1, \ldots y_{n+1}) = y_{n+1}^{d_i} f_i(y_1/y_{n+1}, \ldots, y_n/y_{n+1})$$

where $d_i = \deg(f_i)$.

Remark. Any solution $(x_1, \ldots, x_n)$ of F gives a solution $(x_1, \ldots, x_n, 1)$. of $\hat{F}$. Any solution $(y_1, \ldots, y_{n+1},)$ of $\hat{F}$ with $y_{n+1} \neq 0$ gives a solution of $(y_1/y_{n+1}, \ldots, y_n/y_{n+1})$ of F. The solutions of $\hat{F}$ with $y_{n+1} = 0$ correspond to solutions of F at infinity.

Define

$$L(x) = \sum_{i=1}^{n} b_i x_i + b_{n+1}$$

where the constants b_i are random complex numbers and $b_{n+1} \neq 0$.

The projective transformation of F, denoted by $\tilde{F}$, is the polynomial system in n variables

$$\tilde{f}_i(x_1, \ldots, x_n) = \hat{f}_i(x_1, \ldots, x_n, L(x))$$

Theorem 8. *Let $\tilde{F}$ and L be as above. If F has a finite number of solutions and solutions at infinity, then for almost all $b_i \in \mathbb{C}$, $\tilde{F}$ has no solutions at infinity.*

Proof. See [10] □

Remark. In practice, the condition on the b_i is satisfied by selecting random complex numbers $b_1, \ldots, b_{n+1} \in \mathbb{C}$.

Let F and L be as above. The standard start system $G(x)$ is defined by

$$g_i(x) = x_i^{d_i} - \alpha^{d_i} \;\; i = 1, \ldots, n$$

$$\alpha = L(x)$$

Then $G(x) = 0$ has $d = \deg(F)$ solutions,

$$x_i = k\eta_{d_i, j_i} \text{ with } i = 1, \ldots, n,\ j_i = 0, \ldots, d_i - 1$$

$$\alpha = k$$

where $\eta_{d_i i}, j_i$ are d_ith roots of unity and $k = \frac{b_{n+1}}{1 - \sum_{i=1}^{n} b_i \eta_{d_i, j_i}}$.

The standard homotopy can now be defined as

$$H(x, \lambda) = (1 - \lambda) G(x) + \lambda \gamma \tilde{F}(x)$$

This generates $\deg(F)$ paths in $\mathbb{C}^n \times [0, 1]$ starting at each of the solution of G.

Theorem 9. *For almost all choices of $b_1, \ldots, b_n$ and γ, the standard homotopy generates a collection of d, non-overlapping converging smooth paths.*

Proof. See [10]. □

Remark. The above theorem still holds if different start systems are used. Generally, a start system should be selected in such a way that:
- Its structure is similar to the structure of F
- Its roots are known or can be easily computed

With G the standard start system and H the standard homotopy, generate a path starting at each solution of G and proceed by computing points along the homotopy path, using the Newton-Raphson method, see the subsection which follows for a brief overview of a multivariate Newton-Raphson method.

Homotopy Continuation is implemented in the Julia package HomotopyContinuation.jl. For details see [3].

Newton-Raphson Method. Given a system of n equations $f_1, \ldots, f_n$ in n variables $x_1, \ldots, x_n$, we use homotopy continuation to obtain an approximate solutions $\mathbf{x_0}$. This is an approximate solution, known to 16 decimal places (this is the accuracy implemented in Julia). To increase the accuracy of this solution, we use a multivariate version of the Newton-Raphson method to construct an iterated sequence of approximate solutions to the given system, with increased precision. A detail explanation of this can be found in [4, page 298].

Let $f = (f_1, \ldots, f_n) : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ be a system as above, and let df denote the Jacobian matrix of f. Suppose $\mathbf{x_0}$ is an an approximate solution f with $df(\mathbf{x_0})$ invertible. Define

$$\mathbf{x_1} \;=\; \mathbf{x_0} - df(\mathbf{x_0})^{-1} f(\mathbf{x_0})$$

For $k \geq 1$, we can inductively define

$$\mathbf{x_k} \;=\; \mathbf{x_{k-1}} - df(\mathbf{x_{k-1}})^{-1} f(\mathbf{x_{k-1}})$$

The resulting sequence $\{\mathbf{x_k}\}_{k\geq 0}$ converges to a root of f, with each iterate having increased precision. This is easily implemented in Magma, and with approximately 600 steps, we obtained solutions which are accurate to 2000 decimal places. This was sufficient to calculate the minimal polynomials of these points in the next section.

4. Algebraic Quadritangents

Suppose $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$ is a complex approximation of a point on our scheme. This section will explain how the LLL-algorithm is used the determine the minimal polynomials of the a_i.

Lattices and the LLL-algorithm. This subsection of a summary of [22][Chapter 5].

Fix a positive integer n and let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$, that is, the set of all $\mathbb{Z}$-linear combinations of some linearly independent vectors $b_1, \ldots, b_n \in \mathbb{R}^n$. Let $B = (b_1, \ldots, b_n)$, the $n \times n$ real matrix, whose columns are the basis of $\mathcal{L}$. The determinant of the lattice is defined as

$$\Delta(\mathcal{L}) = |\det(B)|$$

and this is independent of a choice of basis for $\mathcal{L}$, and so it's well defined.

The norm of a vector $v = \sum_i x_i b_i \in \mathcal{L}$ is the square root of

$$||v||^2 \;=\; \langle v, v\rangle$$

where $<,>$ is the standard Euclidean inner product on $\mathbb{R}^n$.

Note. Any lattice is discrete, so there is a well defined notion of the shortest non-zero vector in a lattice.

Given any basis $B = \{b_i\}$ of a lattice $\mathcal{L}$, the Gram-Schmidt basis associated to B is $B^* = \{b_i^*\}$, where

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^* \text{ for all } 1 \leq i \leq n$$

$$\mu_{i,j} = \frac{b_i \cdot b_j^*}{b_j^* \cdot b_j^*} \text{ for all } 1 \leq j < i \leq n$$

Definition. A basis B of a lattice L is called LLL-reduced if the associated Gram-Schmidt basis B^* and the constants μ_{ij} satisfy

- $|\,\mu_{i,j}\,| \leq\; 1/2$ for all $1 \leq j < i \leq n$
- $\|\, b_i^* + \mu_{i,i-1} b_{i-1}^* \,\|^2 \geq\; 3/4 \,\|\, b_{i-1}^* \,\|^2$ for all $1 < i \leq n$.

Theorem 10. *Any lattice L has an LLL-reduced basis and it can be efficiently computed using the LLL algorithm.*

Proof. See [22, Chapter 5] or [6, Pages 85 -88] □

The following proposition allows us to compute the shortest vector in a lattice.

Theorem 11. *Let $b_1, \ldots, b_n$ be a reduced basis of a lattice L. Then for all non zero $x \in L$,*

$$\|b_1\| \leq c\|x\|$$

where $c = \max\{\|b_1\|^2/\|b_i^*\|^2\}$.

Proof. See [22, p69] or [6, Page 84] □

If B is an LLL-reduced basis, then the constant c is very close to 1, so b_1 is a good candidate for the shortest vector in the lattice.

Minimal Polynomials. Fix an algebraic number θ and suppose that $\alpha \in \mathbb{C}$ is an approximation, correct to m decimal places. As θ is algebraic, it satisfies an expression of the form

$$d_n\theta^n + d_{n-1}\theta^{n-1} + \ldots + d_1\theta + d_0 = 0$$

for some positive integer n and $d_n, \ldots, d_0 \in \mathbb{Z}$.

Suppose $\alpha \in \mathbb{R}$ and consider the lattice $\mathcal{L}_m$, generated by the columns of the $(n+1)\times(n+1)$ matrix

$$A_m = \begin{pmatrix} 1 & \ldots & 0 & 0 \\ 0 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \\ [C\alpha^n] & \ldots & [C\alpha] & [C] \end{pmatrix} = (v_n, \ldots, v_1, v_0)$$

for some constant $C \sim 10^m$.

As $d_0, \ldots, d_n \in \mathbb{Z}$, the following is an element in the lattice $\mathcal{L}_m$

$$d_n v_n + \ldots + d_0 v_0 = v = \begin{pmatrix} d_n \\ \vdots \\ d_1 \\ a \end{pmatrix}$$

where $a = d_n\,[C\alpha^n] + \ldots + d_1\,[C\alpha] + d_0\,[C]$. The coefficients $(d_n, \ldots, d_0)$ can be recovered from the vector v by

$$\begin{aligned} d(v) &= \left(d_n, \ldots, d_1, \frac{1}{[C]}\left(a - \left(d_n\,[C\alpha^n] + \ldots + d_1\,[C\alpha]\right)\right)\right) \\ &= (d_n, \ldots, d_1, d_0) \end{aligned}$$

In particular, for any m there exists a vector $v \in \mathcal{L}_m$ with $d(v) = (d_n, \ldots, d_1, d_0)$. This gives us a strategy for finding $d_0, \ldots, d_n$.

With d and v as above, observe

$$\begin{aligned} ||v||^2 &= \sqrt{d_n^2 + \ldots + d_1^2 + a^2} \\ &\leq \sqrt{d_n^2 + \ldots + d_1^2 + \left(d_n^2 + \ldots + d_1^2 + d_0^2\right)^2} \\ &\sim \ ||\ d(v)\ ||^2 \end{aligned}$$

As $||v||$ is approximately $||\ d(v)\ ||$, which is constant , and such a v can be found in any $\mathcal{L}_m$, for a large enough precision, v should be one of the shortest vectors in the lattice. We use of the following heuristic in our calculations.

Heuristic. For a full rank lattice $L \subset \mathbb{R}^n$, the length of the shortest vector in L is approximately $\Delta(L)^{1/n}$

As we increase precision, $||v||$ should be significantly smaller than the above bound and the resulting $d(v)$ should be constant.

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

$$A_m = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \\ 0 & \dots & 1 & 0 & 0 \\ [C\mathrm{Re}\,(\alpha^n)] & \dots & [C\mathrm{Re}\,(\alpha^2)] & [C\mathrm{Re}\,(\alpha)] & [C] \\ [C\mathrm{Im}\,(\alpha^n)] & \dots & [C\mathrm{Im}\,(\alpha^2)] & [C\mathrm{Im}\,(\alpha)] & [C] \end{pmatrix}$$

where $\mathrm{Re}\,(\alpha)$ and $\mathrm{Im}\,(\alpha)$ denote the real and imaginary parts of α.

A similar function d can be defined as above, which in the right context recovers the coefficients of the minimal polynomial.

Regarding the choice of degree n, this is a guess, but there are a few things we should consider when making this choice. Given an n, and we can start with fairly small values, if this the degree or slightly bigger than the degree the following conditions should hold

- the minimum vector in the lattice, the value $d\,(v)$, where $v \in \mathcal{L}_k$ should be stable as k increases
- the value $d\,(v)$, should be significantly smaller than $\Delta\,(\mathcal{L}_k)^{\frac{1}{n+1}}$, as k increases.
- the polynomial $f_{\min}$ whose coefficient are $d\,(v)$ should be irreducible or its factorization should contain an irreducible polynomial of degree close to the degree of $f_{\min}$
- the minimal polynomials should respect the Galois action on the quadritangents, so multiple points should have the same minimal polynomial

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

1. Guess the degree n.
2. Define lattices the lattices $\mathcal{L}_k$ and corresponding function d.
3. In $\mathcal{L}_k$ look for vectors which are shorter than $1/1000\Delta\,(\mathcal{L}_k)^{\frac{1}{n+1}}$. For a large enough k' we expect to see a common $d\,(v)$ for v the shortest vector in L_k for all $k \geq k^{'}$. If such a vector doesn't exists, guess a different degree and start again.
4. If such a vector exists, verify the conditions stated above, and if they are all satisfied, it's extremely likely that this vector represents the coefficients of the minimal polynomial. Otherwise, guess another degree and start again.

Algebraic Quadritangents. Given the minimal polynomials of the coefficients of a quadritangent $(\theta_1, \theta_2, \theta_3, \theta_4)$, we would like to determine the exact roots of these minimal polynomials which determine the quadritangent.

If the coefficients are defined over the same number field, we may express one coefficient as a rational combination of powers of the other.

Let f_i be the minimal polynomial of θ_i and S_i the splitting field of f_i for $i = 1, 2, 3, 4$.

Note. When the degree of f_i is large or S_i cannot be computed, similar computations can be carried out with the number fields defined by the f_i.

Suppose $S_2 \subseteq S_1$ so $\theta_1, \theta_2 \in S_1$, and we can express θ_2 as a rational combination of powers of θ_1, that is, we can find $q_0, \dots, q_{n-1} \in \mathbb{Q}$ such that

$$\theta_2 = q_{n-1}\theta_1^{n-1} + \dots + q_1\theta_1 + q_0$$

where n is the degree of f_1. Equivalently, there exist $z_{n-1}, \dots, z_0, z \in \mathbb{Z}$ such that

$$z_{n-1}\theta_1^{n-1} + \ldots + z_1\theta_1 + z_0 + z\theta_2 = 0$$

As before, we deduce $(z, z_0, \ldots, z_{n-1})$ by searching for the shortest vector in a lattice generated by the columns of

$$A_m = \begin{pmatrix} 1 & \ldots & 0 & 0 & 0 \\ 0 & \ldots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 \\ 0 & \ldots & 0 & 1 & 0 \\ \left[C\alpha_1^{n-1}\right] & \ldots & [C\alpha_1] & [C\alpha_2] & [C] \end{pmatrix}$$

when $\alpha_1, \alpha_2 \in \mathbb{R}$ and complex approximates of θ_1, θ_2 to a high precision, and C is a large constant determined by the precision of the approximations. If the imaginary part of θ_1 is not zero, we instead consider the lattice generated by the columns of

$$A_m = \begin{pmatrix} 1 & \ldots & 0 & 0 & 0 \\ 0 & \ldots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \\ 0 & \ldots & 1 & 0 & 0 \\ \left[C\mathrm{Re}\left(\alpha_1^{n-1}\right)\right] & \ldots & [C\mathrm{Re}\left(\alpha_1\right)] & [C\mathrm{Re}\left(\alpha_2\right)] & [C] \\ \left[C\mathrm{Im}\left(\alpha_1^{n-1}\right)\right] & \ldots & [C\mathrm{Im}\left(\alpha_1\right)] & [C\mathrm{Im}\left(\alpha_2\right)] & 0 \end{pmatrix}$$

and look for short vectors in this lattice.

5. Example $X_0(42)$

We'll calculate the two-torsion subgroup of the modular curve $X_0(42)$. This is a genus 5, non-hyperelliptic curve, embedded in $\mathbb{P}^4$ by the canonical embedding. The model we used is the intersection of the three quadrics f_1, f_2, f_3

$$\begin{aligned} f_1 &= x_1x_3 - x_2^2 + x_3x_4 \\ f_2 &= x_1x_5 - x_2x_5 - x_3^2 + x_4x_5 - x_5^2 \\ f_3 &= x_1x_4 - x_2x_3 + x_2x_4 - x_3^2 + x_3x_4 + x_3x_5 - x_4^2 \end{aligned}$$

For the scheme of quadritangents, with this model, it's convenient to work on the affine chart $\{x_5 = 1\}$ and with planes of the form

$$x_1 = a_1x_2 + a_2x_3 + a_3x_4 + a_4$$

for some $a_1, a_2, a_3, a_4 \in \overline{\mathbb{Q}}$.

The intersection of such a plane with the affine curve is given by

$$F_i(x_2, x_3, x_4) = f_i(a_1x_2 + a_2x_3 + a_3x_4 + a_4, x_2, x_3, x_4, 1) \text{ for } i = 1, 2, 3$$

Explicitly, these expressions are

$$\begin{aligned} F_1(x_2, x_3, x_4) &= -x_2^2 + a_1x_2x_3 + a_2x_3^2 + (a_3 + 1)x_3x_4 + a_4x_3 \\ F_2(x_2, x_3, x_4) &= (a_1 - 1)x_2 - x_3^2 + a_2x_3 + (a_3 + 1)x_4 + a_4 - 1 \\ F_3(x_2, x_3, x_4) &= -x_2x_3 + (a_1 + 1)x_2x_4 - x_3^2 + (a_2 + 1)x_3x_4 + x_3 + (a_3 - 1)x_4^2 + (a_4 - 2)x_4 \end{aligned}$$

For $a_1 \neq 1$, $F_2 = 0$ gives an expression for x_2 in terms of x_3 and x_4

$$x_2 = \frac{-1}{a_1 - 1}\left(-x_3^2 + a_2x_3 + (a_3 + 1)x_4 + a_4 - 1\right) = \phi(x_3, x_4) \tag{1}$$

Substituting for x_2 in F_1 and F_3, we get

$$\widetilde{G_1} = F_1\left(\phi\left(x_3, x_4\right), x_3, x_4\right) = \frac{G_1\left(x_3, x_4\right)}{\left(a_1 - 1\right)^2}$$
$$\widetilde{G_2} = F_3\left(\phi\left(x_3, x_4\right), x_3, x_4\right) = \frac{G_2\left(x_3, x_4\right)}{\left(a_1 - 1\right)}$$

Clearing denominators, the intersection is given by

$$G_1\left(x_3, x_4\right) = G_2\left(x_3, x_4\right) = 0$$

where

$$G_1 = -x_3^4 + \left(a_1^2 - a_1 + 2a_2\right) x_3^3 + \left(2a_3 + 2\right) x_3^2 x_4 + \left(-a_1 a_2 - a_2^2 + a_2 + 2a_4 - 2\right) x_3^2 + \left(-a_1 a_3 - a_1 - 2a_2 a_3 - 2a_2 + a_3 + 1\right) x_3 x_4 + \left(a_1^2 - a_1 a_4 - a_1 - 2a_2 a_4 + 2a_2 + a_4\right) x_3 + \left(-a_3^2 - 2a_3 - 1\right) x_4^2 + \left(-2a_3 a_4 + 2a_3 - 2a_4 + 2\right) x_4 - a_4^2 + 2a_4 - 1$$
$$G_2 = -x_3^3 + \left(a_1 + 1\right) x_3^2 x_4 + \left(-a_1 + a_2 + 1\right) x_3^2 + \left(a_1 - 2a_2 + a_3\right) x_3 x_4 + \left(a_1 + a_4 - 2\right) x_3 + \left(-2a_1 - 2a_3\right) x_4^2 + \left(-a_1 - 2a_4 + 3\right) x_4$$

These can be re-written as

$$G_1 = g_1\left(x_3\right) + h_1\left(x_3\right) x_4 + \alpha_1 x_4^2$$
$$G_2 = g_2\left(x_3\right) + h_2\left(x_3\right) x_4 + \alpha_2 x_4^2$$

with $g_1, g_2, h_1, h_2 \in \mathbb{Q}\left[a_1, a_2, a_3, a_4\right]\left[x_3\right]$ and $\alpha_1 = -\left(a_3 + 1\right)^2$, $\alpha_2 = -2\left(a_1 + a_2\right)$. If $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$

$$\alpha_2 G_2 - \alpha_1 G_2 = \left(\alpha_2 h_1\left(x_3\right) - \alpha_1 h_2\left(x_3\right)\right) x_4 + \alpha_2 g_1\left(x_3\right) - \alpha_1 g_2\left(x_3\right) = 0$$

and if $T_1 = \alpha_2 h_1\left(x_3\right) - \alpha_1 h_2\left(x_3\right) \neq 0$, as a polynomial in x_3, the above gives an expression for $x_4 = \frac{-T_2}{T_1}$ with $T_2 = \alpha_2 g_1\left(x_3\right) - \alpha_1 g_2\left(x_3\right)$.

Substituing for x_4 in G_1, we get

$$G\left(x_3\right) = G_1\left(x_3, \tfrac{-T_2}{T_1}\right) = \tfrac{h(x_3)}{g(x_3)}$$

where $h \in \mathbb{Q}\left[a_1, a_2, a_3, a_4\right]\left[x_3\right]$ has degree 8 and $g\left(x_3\right) = \left(\frac{T_1}{a_3+1}\right)^2$.

Clearing denominators in the expression above, we remark that if the given plane $x_1 = a_1 x_2 + a_2 x_3 + a_3 x_4 + a_4$ is a quadritangent, then h is necessarily a square. Equivalently, there exist $a_5, a_6, a_7, a_8 \in \overline{\mathbb{Q}}$ such that

$$h\left(x\right) = l\left(x^4 + a_5 x^3 + a_6 x^2 + a_7 x + a_8\right)^2$$

where l is the leading coefficient of h. Equating coefficients in the above expression, gives 8 equations $e_1, \ldots, e_8$ in $a_1, \ldots, a_8$.

We also add a 9th equation (and a 9th variable)

$$e_9 : a_9 \Delta\left(x^4 + a_5 x^3 + a_6 x^2 + a_7 x + a_8\right) + 1 = 0$$

to ensure that $x^4 + a_5 x^3 + a_6 x^2 + a_7 x + a_8$ has non-zero discriminant and avoid singularities on our scheme.

To derive $e_1, \ldots, e_8$, we assumed that $a_1 \neq 1$, $\alpha_1 \neq 0$ and $\alpha_2 \neq 0$, and equations are also required for these conditions.

$$e_{10} : a_{10}\left(a_1 - 1\right) + 1 = 0$$
$$e_{11} : a_{11}\left(a_3 + 1\right) + 1 = 0$$
$$e_{12} : a_{12}\left(a_1 + a_3\right) + 1 = 0$$

It can be checked that $e_2 \ldots e_{12}$ are irreducible, and $e_1 = s_1 s_2$,

$$s_1 = a_3a_4 - a_3a_8 - a_3 - 2a_4^2 + 5a_4 + a_8 - 3$$
$$s_2 = a_3a_4 + a_3a_8 - a_3 - 2a_4^2 + 5a_4 - a_8 - 3$$

It can be checked (using Julia), that the system

$$s_1 = s_2 = e_2 = \ldots = e_{12} = 0$$

has no solutions. We'll consider the cases $S_1 = 0$ and $S_2 = 0$ separately.

The condition $T_1 \neq 0$ will also require equations. As a polynomial, T_1 is non-zero, if its coefficients t_1, t_2 and t_3 are not all zero.

$$t_1 = a_1a_3 - 3a_1 - 3a_3 + 1$$
$$t_2 = k_1k_2 = (a_1 + 2a_2 + a_3)(2a_1 + a_3 - 1)$$
$$t_3 = a_1a_3 - 4a_1a_4 + 5a_1 - 2a_3a_4 + a_3 + 2a_4 - 3$$

Case 1. The first 12 equations are $s_1, e_2, \ldots e_{12}$ and we consider all possible combinations of zero and non-zero t_1, k_1, k_2 and t_3.

Case 1.1 : $t_1 \neq 0, k_1 \neq 0, k_2 \neq 0, t_3 \neq 0$

We add 4 equations and 4 variables

$$e_{13} : a_{13}t_1 + 1 = 0$$
$$e_{14} : a_{14}k_1 + 1 = 0$$
$$e_{15} : a_{15}k_2 + 1 = 0$$
$$e_{16} : a_{16}t_3 + 1 = 0$$

The system formed by the 16 equations in $a_1, \ldots, a_{16}$, has 96 solutions (via Julia) .

Case 1.2 : $t_1 \neq 0, k_1 \neq 0, k_2 = 0, t_3 \neq 0$

We add 4 equations and 3 variables

$$e_{13} : a_{13}t_1 + 1 = 0$$
$$e_{14} : a_{14}k_1 + 1 = 0$$
$$e_{15} : a_{15}t_3 + 1 = 0$$
$$e_{16} : k_2 = 0$$

The system formed by the 16 equations in $a_1, \ldots, a_{15}$, has 24 solutions (via Julia) .

Case 1.3 : $t_1 \neq 0, k_1 = 0, k_2 \neq 0, t_3 \neq 0$

We add 4 equations and 3 variables

$$e_{13} : a_{13}t_1 + 1 = 0$$
$$e_{14} : a_{14}k_2 + 1 = 0$$
$$e_{15} : a_{15}t_3 + 1 = 0$$
$$e_{16} : k_1 = 0$$

The system formed by the 16 equations in $a_1, \ldots, a_{15}$, has 14 solutions (via Julia) .

It can be checked that in all other cases, for all other possible combinations of zero an non-zero t_1, k_1, k_2, t_3, the corresponding systems have no solutions.

5.0.1. *Case 2.* The first 12 equations are $s_2, e_2, \ldots, e_{12}$.

Case 1.1 : $t_1 \neq 0, k_1 \neq 0, k_2 \neq 0, t_3 \neq 0$

We add 4 equations and 3 variables

$$\begin{aligned} e_{13} &: a_{13}t_1 + 1 = 0 \\ e_{14} &: a_{14}k_1 + 1 = 0 \\ e_{15} &: a_{15}k_2 + 1 = 0 \\ e_{16} &: a_{16}t_3 + 1 = 0 \end{aligned}$$

The system formed by the 16 equations in $a_1, \ldots, a_{16}$, has 256 solutions (via Julia) .

It can be checked that in all other cases, the resulting systems have no solutions.

Remark. We can also derive equations and schemes in all the extreme cases, $\alpha_1 = 0$,$\alpha_2 = 0$,$a_1 = 1$ etc. These cases, combined, had very few solutions, and in fact, these planes are not need in the calculation of the 2-torsion subgroup.

Aside: p-adic lifting on smaller patches. Although in general, p-adic lifting on the schemes of quadritangents of genus 5 curves is ineffective, this particular example is an exception. In this case, finding some non-singular points over $\mathbb{F}_{11}$ and lifting them was sufficient to find the 2-torsion subgroup over $\mathbb{Q}\left(\sqrt{-7}\right)$ and thus over $\mathbb{Q}$.

More precisely, consider the 12 base equations of case 1

$$s_1 = e_2 = \ldots = e_{12} = 0$$

These have 48 solutions over $\mathbb{F}_{11}$. For 12 of these points, the Jacobian matrix of $E = (s_1, e_2, \ldots, e_{12})$ has non-zero determinant modulo 11, and thus they have unique lifts by Hensel's lemma. As explained in the first year report, we can approximate these lifts modulo11^n for any $n \in \mathbb{N}$, and these lifts can be used to obtain the algebraic expressions of these points.

The 12 quadritangent planes, defined over $\mathbb{Q}\left(\sqrt{-7}\right)$, corresponding to the 12 points are the following

$$\begin{aligned}
l_1 &: -x_1 - x_3 + 2x_4 + 2x_5 = 0 \\
l_2 &: -x_1 - 3x_2 - x_3 + 5x_4 + 2x_5 = 0 \\
l_3 &: -2x_1 + \left(3 + \sqrt{-7}\right)x_2 + \left(3 - \sqrt{-7}\right)x_3 + \left(-9 + \sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_4 &: -2x_1 + \left(3 - \sqrt{-7}\right)x_2 + \left(3 + \sqrt{-7}\right)x_3 + \left(-9 - \sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_5 &: -2x_1 + \left(5 + \sqrt{-7}\right)x_2 - 2x_3 + \left(-1 - \sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_6 &: -2x_1 + \left(5 - \sqrt{-7}\right)x_2 - 2x_3 + \left(-1 + \sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_7 &: -32x_1 + 8\left(-1 - \sqrt{-7}\right)x_2 + \left(-1 - 3\sqrt{-7}\right)x_3 + 2\left(-5 - \sqrt{-7}\right)x_4 + 64x_5 = 0 \\
l_8 &: -32x_1 + 8\left(-1 + \sqrt{-7}\right)x_2 + \left(-1 + 3\sqrt{-7}\right)x_3 + 2\left(-5 + \sqrt{-7}\right)x_4 + 64x_5 = 0 \\
l_9 &: -2x_1 + 2\left(2 + \sqrt{-7}\right)x_2 + \left(-1 - 3\sqrt{-7}\right)x_3 + 2\left(-1 + 2\sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_{10} &: -2x_1 + 2\left(2 - \sqrt{-7}\right)x_2 + \left(-1 + 3\sqrt{-7}\right)x_3 + 2\left(-1 - 2\sqrt{-7}\right)x_4 + 4x_5 = 0 \\
l_{11} &: -8x_1 + 4\left(-3 + \sqrt{-7}\right)x_2 + \left(3 - \sqrt{-7}\right)x_3 + 2\left(3 - \sqrt{-7}\right)x_4 + 16x_5 = 0 \\
l_{12} &: -8x_1 + 4\left(-3 - \sqrt{-7}\right)x_2 + \left(3 + \sqrt{-7}\right)x_3 + 2\left(3 + \sqrt{-7}\right)x_4 + 16x_5 = 0
\end{aligned}$$

The rational cusps of the curve $X_0(42)$ are

$$C = \{(2:-1:1:-1:1), (2:2:1:2:1), (7:4:2:1:2), (1:-2:2:1:2), (3:0:0:-1:2), (1:0:0:0:0:1), (1:0:0:0:1:0), (1:0:0:0:0:0)\}$$

Let $J = J_0(42)$ be the Jacobian of $X_0(42)$ and define

$P_1 = 9(2:-1:1:-1:1) + 3(2:2:1:2:1) - 12(1:0:0:0:0:0)$

$P_2 = -108(2:-1:1:-1:1) - (2:2:1:2:1) - 13(7:4:2:1:2) + (1:0:0:1:0) + 121(1:0:0:0:0:0)$

$P_3 = -6(2:-1:1:-1:1) + 6(1:0:0:0:0:0)$

$P_4 = -7(2:-1:1:-1:1) - (2:2:1:2:1) - (3:0:0:-1:2) + (1:0:0:1:0) + 8(1:0:0:0:0:0)$

These are rational, 2-torsion points on $J \cong \mathrm{Pic}^0(X_0(42))$, which are also linearly independent. We will show that they are representatives of classes of generators of the $J(\mathbb{Q})[2]$.

Let $K = \mathbb{Q}(\sqrt{-7})$ and let O_K be its ring of integers. Then $\mathfrak{p} = < 11, 10 + 2\sqrt{-7} >$ is a prime ideal of O_K of norm 11, and thus it induces a reduction map

$$r_{\mathfrak{p}} : J(K) \longrightarrow J(\mathbb{F}_{11})$$

As 11 is a prime of good reduction for the curve and $e_{\mathfrak{p}}$, this map is injective on the torsion subgroup (see [17]) .

Define H to be the subgroup of $J(K)[2]$ generated by the equivalence classes of the divisors P_1, P_2, P_3, P_4 and the 11 divisors formed by taking the divisors of the quotients of the $l_2 \dots l_{12}$ by l_1 and multiplying by $\frac{1}{2}$

$$D_{i-1} = \tfrac{1}{2}\mathrm{div}\left(\tfrac{l_i}{l_1}\right) \text{ for } i = 2, \dots 12$$

The image of H, $r_{\mathfrak{p}}(H) \cong (\mathbb{Z}/2\mathbb{Z})^6$, so

$$r_{\mathfrak{p}}(H) \cong (\mathbb{Z}/2\mathbb{Z})^6 \subseteq J(\mathbb{F}_{11}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/96\mathbb{Z})$$

and since $r_{\mathfrak{p}}$ is injective, we conclude that $J(K)[2] = H$.

Taking Galois invariants of H, we find that $J(\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$, and so divisors P_1, P_2, P_3 and P_4 must be representatives of generators of this group. Thus, we have shown

Theorem 12. *The rational two-torsion subgroup of $J_0(42)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$.*

Due to [20], this has a powerful corollary.

Corollary 13. *$J_0(42)(\mathbb{Q}) = C \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/48\mathbb{Z})$, where C is the rational cuspidal subgroup.*

The Two-Torsion Subgroup $J_0(42)[2]$. As previously remarked, p-adic lifting, even on small patches usually doesn't work. Instead, we can use the complex approximations to obtain the rational-two torsion subgroup. In this example, the full two-torsion subgroup was determined.

Using the complex appromximates of solutions of the equations of the scheme arising in case 2.1, the following quadritangents were computed : $-x_1 + \theta_1 x_2 + \theta_2 x_3 + \theta_3 x_4 + \theta_4 x_5 = 0$

where θ_1 is a root of

$f_1(u) = 2713u^{16} + 9264u^{15} + 24252u^{14} - 1352u^{13} - 270446u^{12} - 739224u^{11} - 599968u^{10} + 1502208u^9 + 6136803u^8 + 10670696u^7 + 11231488u^6 + 7603968u^5 + 3052898u^4 + 591416u^3 + 141500u^2 + 210760u + 154057$

For a given root u of f_1

$$\begin{aligned}\theta_2 =& C_2(11909601366618833720625165746090293775993062 75u^{15}+\\ & 4640021056277737920428679468777354246900588561u^{14}+\\ & 1241609026569154513838836444529341314659007909 4u^{13}+\\ & 2293289970989296431493689410697144409535767739u^{12}-\\ & 1223229628823113231630536534839986865027959315 95u^{11}-\\ & 3878491303412250289964453985522975367002167442 42u^{10}-\\ & 3784724862783915415737367264728501049656335883 49u^{9}+\\ & 7085707129466057271075063561460257142715835922 59u^{8}+\\ & 3143244252588351682551036111998302606561987710 929u^{7}+\\ & 5666419328191937793276032459677283649005180999 062u^{6}+\\ & 5956195409217724011954458067223274155900647173 591u^{5}+\\ & 3643133243326958113346100359151784320855077856 135u^{4}+\\ & 1368271996204799351688040406930167500079155182 406u^{3}+\\ & 3123413275837462088068057377383479521352965922 89u^{2}+\\ & 9854799891832241098459027012103940804495221987 7u+\\ & 1929460948768327771861070316 79)\end{aligned}$$

where $C_2 = -1/135830738656783167174155021005116707238876304576$

$$\begin{aligned}\theta_3 =& C_3(64512977279539655114083692051542374278189756 0u^{15}+\\ & 2097116527425189955409642026865708591451413213u^{14}+\\ & 5065592383851869427188728033803517473520856627u^{13}-\\ & 1981787485175025986977273356629219005459957027u^{12}-\\ & 6600044519100380186641947771359667486681882460 7u^{11}-\\ & 1618240197827346279321475170337099020673555985 90u^{10}-\\ & 8227956734500724421394231001916179578048274517 0u^{9}+\\ & 4293074519148796902585486543604663173691127203 97u^{8}+\\ & 1376249717990430962068975165850372674116021424 981u^{7}+\\ & 2074565303331084985567583758393770840714838855 106u^{6}+\\ & 1782096698429499036631883598680861106604878140 422u^{5}+\\ & 9003756039357339565225657945273754575100397463 33u^{4}+\\ & 2485612183576961696526364063488132777415178757 13u^{3}+\\ & 3544420077426893742157227534076709691761748443 7u^{2}+\\ & 3858272128349501027077478110626853968171050153 5u+\\ & 5753632863853638358312105331096723499096477393 6)\end{aligned}$$

where $C_3 = 1/339576846641957917935387552512791768097190761 44$

$$\begin{aligned}\theta_4 =& C_4(266709184457275901868408940171826999593354092 7u^{15}+\\ & 81182936254314963697248899024939885958764263 61u^{14}+\\ & 21066018496715162443110369916722546543016381134u^{13}-\\ & 96814555402013123651762919891143727763236846 41u^{12}-\\ & 26230898796054124950870929228834781847011952 8803u^{11}-\\ & 63591187058078895769762974372361977667827466 2182u^{10}-\\ & 36222515315736964720272403792972614781906441 1989u^9+\\ & 16616878613974710025085039743160371791237007 83863u^8+\\ & 55012567159142435330544153063702804084993530 83644u^7+\\ & 84758812594968723332456274645066347554050537 67194u^6+\\ & 76876838340207448361559179639020169105074387 75239u^5+\\ & 40056680657644233359003390208115928542214871 40051u^4+\\ & 10303281954653752541396794465731287735328188 80954u^3+\\ & 46814857631089014471341024441023368649895917 437u^2+\\ & 49570498786897778677450003169715908133887036 573u+\\ & 45883518129164385873745345221144023800631762 8148)\end{aligned}$$

where $C_4 = 1/135830738656783167174155021005116707238876304576$.

Another 24 planes correspond to θ_1 being roots of

$$f_2(u) = u^8 + 11u^7 + 40u^6 + 57u^5 + 40u^4 + 13u^3 + 36u^2 + 15u + 43$$

$$f_3(u) = 121u^{16}+1276u^{15}+9088u^{14}+56024u^{13}+247700u^{12}+696592u^{11}+1008190u^{10}-422200u^9-4935704u^8-9046144u^7-5168416u^6+6791184u^5+15143145u^4+12793948u^3+6685384u^2+3243000u+1241788;$$

and there are expression for $\theta_2, \theta_3, \theta_4$ corresponding to these roots.

Another 8 planes can be computed from approximations to solutions of the equations of the scheme arising in case 1.1. The quadritangents are of the general form as above, with θ_1 being a root of

$$f_4(u) = 23u^8 + 78u^7 + 135u^6 + 146u^5 + 236u^4 + 322u^3 + 239u^2 + 94u + 23$$

Let K be the number field defined by f_1 and O_K its ring of integers. All of the 48 quadritangents above are defined over K. Clearing denominators and multiplying by a suitable scalar, we can assume that they are defined over O_K. Let L be the set of the 48 quadritangents defines over K. We can form the subgroup

$$H = <\tfrac{1}{2}\mathrm{div}\left(\tfrac{l}{l_0}\right) \mid l \in L> \subseteq J_0(42)[2]$$

Let $\mathfrak{p} = \langle 11, \theta\rangle$ where $\theta = 8\alpha_1 + 10\alpha_2 + 8\alpha_5 + 9\alpha_6 + 9\alpha_7 + 2\alpha_9 + \alpha_{10} + 3\alpha_{11}$ and $\alpha_1 = 1, \alpha_2, \ldots, \alpha_{16}$ are generators of O_K.

Remark. θ is a root of

$$u^{16} + 27111598u^{15} + 178341432684869u^{14} + 24526666390352186730u^{13} +$$
$$126552800884746499928337791 69u^{12} + 626040984350099526567865727 9875240u^{11} +$$
$$1417794389287870984139220556307862522212u^{10} +$$
$$191183792807683638441671507760709999811569196u^{9} +$$
$$169047799831091090074802336656371617141160888 50607u^{8} +$$
$$102623186523494690567536320871195441749888683 1289492886u^{7}$$
$$+ 443504469659308986334386359834968120400249877382396499702 89u^{6} +$$
$$146744592542111883082383551048454579255776101864701728749870 8082u^{5} +$$
$$441976738694722395473037977201090671643823797626692494097516018271 31u^{4}$$
$$+ 142117543745744098674643756976016884243608193617380161277628469984687 8484u^{3} +$$
$$419028419179210183953499471954068837950405518585073738190429675065428270 4342u^{2} +$$
$$838404735022841199712356660050859838834223563837960019006590091620897911074770200u +$$
$$807342640766757970778192648481409924558433305762817475901700100137058837772683603 1012$$

The ideal $\mathfrak{p}$ is a prime ideal of O_K, which has norm 121. Thus, reduction modulo $\mathfrak{p}$ defines a map

$$r_{\mathfrak{p}} : J(K) \longrightarrow J(\mathbb{F}_{121})$$

As 11 is a prime of good reduction for the curve, and $e_{\mathfrak{p}} = 1$, this map is injective on the torsion subgroup (see [17]) .

The image of H under $r_{\mathfrak{p}}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{10}$, so

$$r_{\mathfrak{p}}(H) \cong (\mathbb{Z}/2\mathbb{Z})^{10} \subseteq J(\mathbb{F}_{121})$$

where the Jacobian over $\mathbb{F}_{121}$ is isomorphic to

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/24\mathbb{Z}) \times (\mathbb{Z}/48\mathbb{Z}) \times (\mathbb{Z}/192\mathbb{Z}) \times (\mathbb{Z}/192\mathbb{Z})$$

Thus $r_{\mathfrak{p}}(H) = J(\mathbb{F}_{121})[2]$, and since r_p is injective on torsion points, $H = J(K)[2]$.

Remark. As $J(\overline{\mathbb{Q}}) \cong (\mathbb{Z}/2\mathbb{Z})^{10}$, H is the entire two-torsion subgroup of J.

The Galois group acts transitively on the quadritangents and as a result on the two-torsion. Studying this Galois action on the 48 quadritangents, we find that resulting classes of divisors are not fixed by any proper subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, and so $H = J[2]$ is defined over K.

6. Two Torsion Subgroup via Characteristic Two Calculations

For curves of lower genus, we could attempt to solve the equations of the scheme of theta hyperplanes over a finite field of odd characteristic and lift the solutions using Hensel's lemma. This is computationally challenging when the genus is 5, since the schemes considered have large degree. Computations could be simplified significantly by working in characteristic 2. In this section, I will present an example of computing the 2-torsion subgroup of a plane quartic by computing it's bitangents in characteristic 2 and lifting them. I hope to generalise this in the near future.

Let $C \subseteq \mathbb{P}^{g-1}$ be a general canonical curve of genus g over $\mathbb{Q}$. Denote by J_C the Jacobian of C. By the results presented in Section 1, $J_C[2]$ is generated by differences of odd theta characteristics. There are precisely $2^{g-1}(2^g - 1)$ odd theta characteristics, in bijection with the theta hyperplanes to the curve.

If we consider C over a field k of characteristic 2, provided C has good reduction at 2, there are significantly fewer theta hyperplanes over k .

Theorem 14. *Let $g \geq 3$ be an integer and let k be a field of characteristic 2. Let $C \subset \mathbb{P}_k^{g-1}$ be a general canonical curve. The scheme of theta-hyperplanes of C is finite of degree $2^{g-1}(2^g - 1)$ and the multiplicity of each point is 2^{g-1}.*

Proof. See [21, Theorem 3.11] □

Let $C \subset \mathbb{P}^2$ be a general canonical curve of genus 3 over $\mathbb{F}_2$, a plane quartic (see [15, 4.5]). In our example, C will be the reduction of a curve $\mathbb{Q}$ with good reduction at 2. Over a finite extension of $\mathbb{F}_2$, C has 7 bitangents. In our computations, using the above theorem, we can deduce that for each of these 7 bitangents, there are 4 bitangents to the rational curve reducing to it. It's almost trivial to compute the bitangents in characteristic 2, the difficulty occurs when attempting to lift them, since the scheme of bitangents does not have good reduction at 2. To overcome this issue we use the field of definition of the bitangents K, obtained by considering valuations, and then lift using Hensel's lemma.

We have the following strategy.

1. Define a scheme of bitangents S.
2. Using the defining equations of S deduce the extension over which the bitangents of C are defined.
3. Compute the points of S over $\mathbb{F}_{2^n} \cong O_K/\mathfrak{P}$, where $\mathfrak{P}$ is a prime of norm 2^n.
4. For each of the points above, compute the lifts modulo $\mathfrak{P}^k$, until we reach a point k where there are 4 distinct lifts and the hypothesis of Hensel's lemma is satisfied.
5. Lift the points found above using Hensel's lemma.
6. Compute the algebraic form of the above points using the LLL-algorithm.
7. Compute the 2-torsion subgroup.

We'll consider the genus 3 modular curve $X_0(45)$ throughout this section. This is the vanishing set of

$$f = x^3z - x^2y^2 + xyz^2 - y^3z - 5z^4$$

Scheme of Bitangents. We work on the affine chart $\{z = 1\}$ and with bitangents of the form $x = a_1y + a_2$. The intersection of the affine curve and the bitangent is given by

$$\begin{aligned} F(y) &= f(a_1y + a_2, y, 1) \\ &= -a_1^2y^4 + (a_1^3 - 2a_1a_2 - 1)y^3 + (3a_1^2a_2 + a_1 - a_2^2)y^2 \\ &+ (3a_1a_2^2 + a_2)y + a_2^3 - 5 \end{aligned}$$

If the above line is a bitangent, $F(y)$ is necessarily a square, so there exist $a_3, a_4 \in \overline{\mathbb{Q}}$ such that

$$F(y) = l(y^2 + a_3y + a_4)^2 \text{ where } l = -a_1^2$$

Equating coefficients in the above expression, gives 4 equations e_1, e_2, e_3, e_4 in a_1, a_2, a_3, a_4, which define the scheme of bitangents.

$$\begin{aligned} e1 &= a_1^3 + 2a_1^2a_3 - 2a_1a_2 - 1 \\ e2 &= 3a_1^2a_2 + a_1^2a_3^2 + 2a_1^2a_4 + a_1 - a_2^2 \\ e3 &= 2a_1^2a_3a_4 + 3a_1a_2^2 + a_2 \\ e4 &= a_1^2a_4^2 + a_3^2 - 5 \end{aligned}$$

Over $\mathbb{F}_4$, S has 6 points

$$(1,0,1,1),\ (1,1,1,0),\ (\theta,0,\theta,\theta^2),\ (\theta,\theta^2,\theta,0),\ (\theta^2,0,\theta^2,\theta),\ (\theta^2,\theta,\theta^2,0)$$

where $\mathbb{F}_4^* = \langle\theta\rangle$.

Note. The seventh bitangent can be found by working in a different affine chart.

Extensions. The aim of this subsection is to obtain the field of definition of bitangents to $X_0(45)$. This is work in progress, so this subsection is only a sketch of a few ideas. The main idea was inspired by calculations and lifts of bitangents to tropical quartics. See [18] and [8] for details.

Given a point $a = (a_1, a_2, a_3, a_4)$ defined over $\mathbb{F}_{2^n}$, we'll find its 4 lifts by writing a "2-adic" type expansion for each a_i. Using the 2-adic valuation and the defining equations of the scheme, we can find a finite extension K of $\mathbb{Q}_2$, over which there are 4 possibilities for the required 2-adic expansions reducing the staring point, and corresponding to the 4 expected lifts.

Remark. We expect the extension K to be ramified, to account for the 4 bitangents reducing to a single one over the residue field.

There is a valuation on K which extends the 2-adic valuation. The valuation will be determined by some prime ideal, and we will denote it by ν_2 to emphasise its reduction to the 2-adic valuation. In the discussion that follows, ν_2 is not normalised as a valuation of K, so $\nu_2(2) = 1$. In particular, we allow ν_2 to take rational values.

We begin with a simple example to illustrate this idea.

Suppose we want to compute the roots of $f(x) = x^2 - 3$. In over $\mathbb{F}_2$, this has a single root $x \equiv 1 \bmod 2$, with multiplicity 2. We'll find an extension K of $\mathbb{Q}$ over which we can separate the solutions and then apply Hensel's lemma.

As $x \equiv 1 \bmod 2$, $x = 1 + u$ where u has valuation greater than 0. Substitute $x = 1 + u$

$$f(1 + u) = -2 + 2u + u^2$$

Let $\nu_2(u) = n$ be the valuation of u. The above expression has valuation $\min\{1, 1+n, 2n\} = \min\{1, 2n\}$. As $f(1+u)$ should vanish modulo 2^m for some $m > 1$, this minimal valuation occurs at (at least) 2 terms. Thus, in the above case, $2n = 1$ and so $n = 1/2$. This suggests that for x to have a "$2 - adic$ "-type expansion, we should make a degree 2, ramified extension of $\mathbb{Q}_2$. There are only 6 non-isomorphic such extensions, all classified in [2]. Let K be the number field defined by $x^2 + 2x + 6$. Then $\mathfrak{P} = \langle 2, -1 + \sqrt{5} \rangle < O_K$ is a prime ideal of the ring of integers of K, and $8 + 3\sqrt{5}, 8 + 5\sqrt{5}$ are solutions of f modulo $\mathfrak{P}^8$, which are congruent to 1 modulo $\mathfrak{p}$. Furthermore, both solutions can be lifted using Hensel's lemma since $\nu_{\mathfrak{P}}(f(a)) = 3 > 2 = 2\nu_{\mathfrak{P}}(f'(a))$.

Returning to $X_0(45)$, denote by $\underline{a}$ any characteristic 0 solution (u_1, u_2, u_3, u_4) of e_1, e_2, e_3, e_4 which reduces to the $\mathbb{F}_2$ solution $(1, 0, 1, 1)$.

$$\begin{aligned} u_1 &\equiv 1 \bmod 2 \\ u_2 &\equiv 0 \bmod 2 \\ u_3 &\equiv 1 \bmod 2 \\ u_4 &\equiv 1 \bmod 2 \end{aligned}$$

The above suggest that there exists v_i, with

$$\begin{aligned} u_1 &= 1 + v_1 \\ u_2 &= v_2 \\ u_3 &= 1 + v_3 \\ u_4 &= 1 + v_4 \end{aligned}$$

with $\nu_2(v_i) = n_i$, where $n_1, n_2, n_3, n_4 > 0$.

Evaluating e_1 at $\underline{a}$ gives

$$e_1(\underline{a}) = v_1^3 + 2v_1^2v_3 + 5v_1^2 - 4v_1v_2 + 4v_1v_3 + 7v_1 - 4v_2 + 2v_3 + 2$$

with valuation $\nu_2(e_1(\underline{a})) = \min\{1, n_1\}$. As before, the valuation occurs at two minimal terms, so $n_1 = 1$ and this minimum is achieved at the two terms $7v_1$ and 2, so no extension is necessary.

Evaluating e_2 at $\underline{a}$ gives

$$\begin{aligned} e_2(\underline{a}) &= 3v_1^2v_2 + v_1^2v_3^2 + 2v_1^2v_3 + 2v_1^2v_4 + 3v_1^2 + 6v_1v_2 + 2v_1v_3^2 + \\ &\quad 4v_1v_3 + 4v_1v_4 + 7v_1 - v_2^2 + 3v_2 + v_3^2 + 2v_3 + 2v_4 + 4 \end{aligned}$$

with valuation $\nu_2(e_2(\underline{a})) = \min\{1, n_2, 2n_3\}$.

Evaluating e_3 at $\underline{a}$ gives

$$\begin{aligned} e_3(\underline{a}) &= 2v_1^2v_3v_4 + 2v_1^2v_3 + 2v_1^2v_4 + 2v_1^2 + 3v_1v_2^2 + 4v_1v_3v_4 + 4v_1v_3 + \\ &\quad 4v_1v_4 + 4v_1 + 3v_2^2 + v_2 + 2v_3v_4 + 2v_3 + 2v_4 + 2 \end{aligned}$$

with valuation $\nu_2(e_3(\underline{a})) = \min\{1, n_2\}$, so $n_2 = 1$. This valuation is achieved at v_2 and 2, so no extension is necessary.

Returning to the e_2 expression, substitute $n_2 = 1$ to conclude $n_3 = 1/2$. The valuation is achieved at the 3 terms $7v_1, 3v_2, v_3^2$, so a degree 2 extension is needed.

Evaluating e_4 at $\underline{a}$ gives

$$\begin{aligned} e_4(\underline{a}) &= v_1^2v_4^2 + 2v_1^2v_4 + v_1^2 + 2v_1v_4^2 + 4v_1v_4 + 2v_1 + v_2^3 \\ &\quad + v_4^2 - 2v_4 - 4 \end{aligned}$$

with valuation $\nu_2(e_4(\underline{a})) = \min\{2, n_4+1, 2n_4\}$, so $n_4 = 1$. The valuation occurs at the terms $v_1^2, 2v_1, v_4^2, 2v_4, 4$, so a degree 2 extension is necessary for a_4.

The required extension has degree 4. There are 59 degree 4 non-isomorphic extension of $\mathbb{Q}_2$, see [2] for a classification of these. Let K be the degree 4 number field $\mathbb{Q}\left(\sqrt{-3}, \sqrt{5}\right)$. This is the required extension for our problem (this is the known field of definition of the bitangents from [20]).

Separating Bitangents modulo $\mathfrak{p}^k$. Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$ be the extension found above and let $\mathfrak{p}$ be the prime ideal of norm 4 in K generated by 2 and θ, where θ is a root of $x^4 - x^2 + 4$.

The point $(1, 0, 1, 1) \in (O_K/\mathfrak{p})^4$ is a solution of $\mathbf{e} = (e_1, e_2, e_3, e_4)$ modulo $\mathfrak{p}$. There are 16 points of $\left(O_K/\mathfrak{p}^2\right)^4$ which are solutions of $\mathbf{e}$ modulo $\mathfrak{p}^2$ and reduce to $(1, 0, 1, 1)$ modulo $\mathfrak{p}$. Denote this set of points by S_2. At this point, we should note that for all $(a_1, a_2, a_3, a_4) \in S_2$, $(a_1, a_2) = (-1, 2)$.

Continuing this search, there are 64 points in $\left(O_K/\mathfrak{p}^3\right)^4$ which are solutions of $\mathbf{e}$ modulo $\mathfrak{p}^3$ and reduce to a point of S_2 modulo $\mathfrak{p}^2$. Let S_3 be the set of these points. At this level, for all $(a_1, a_2, a_3, a_4) \in S_3$, $(a_1, a_2) \in \{(-1, 4+\theta), (3, \theta), (-1, \theta), (3, 4+\theta)\}$, with each occurring for precisely 16 out of the 64 points.

This repeats modulo $\mathfrak{p}^4$, there are 64 points in $\left(O_K/\mathfrak{p}^4\right)^4$ which are solutions of $\mathbf{e}$ modulo $\mathfrak{p}^4$ and reduce to a point of S_3 modulo $\mathfrak{p}^3$. Let S_4 be the set of these points. As before, for all $(a_1, a_2, a_3, a_4) \in S_3$, (a_1, a_2) is one of 4 options $\{(7, 8+\theta), (-1+2\theta, 4+\theta), (7+2\theta, 4-\theta), (7, 8-\theta)\}$, with each occurring for precisely 16 out of the 64 points.

It's important to mention that these lifts don't occur in a one to one pattern. For 4 out of the 64 points in S_3, there 16 points in S_4 reducing to it, and for the remaining 60 points there are none.

In fact this pattern continues as far as $\mathfrak{p}^{12}$, and probably beyond. At each stage there are 64 points, lifting in this 1 to 16 or 1 to 0 pattern, and for all the points, the pairs of the first two coordinates have 4 possible values. Let S_i be the 4 possible values of (a_1, a_2) modulo $\mathfrak{p}^i$.

Recall that the first two coordinates are the coefficients of the bitangent, and we expect that for each bitangent over $\mathbb{F}_4$, there are 4 bitangents defined over $\overline{\mathbb{Q}}$ reducing to it. It's therefore a natural question to

ask whether the four bitangents over $O_K/\mathfrak{p}^k$ for $k \geq 3$ are reduction of the 4 algebraic bitangents. It turns out that this is indeed the case.

To explain this, we begin by eliminating the last 2 coordinates from our scheme. Let $\tilde{S}$ be the scheme defined by $f_1, \ldots, f_n$ where $f_i \in \mathbb{Q}[a_1, a_2]$ are obtained by eliminating a_3, a_4 from e_1, e_2, e_3, e_4. One way of doing this is by finding the elimination of ideal of the $I = \langle e_1, e_2, e_3, e_4 \rangle$ and taking a basis of it (the elimination ideal is the simply the ideal defined by all polynomials in I with monomials in a_1 and a_2 only). Thus, $\tilde{S}$ is a scheme of bitangents and it has dimension 0. Also, every point of $\tilde{S}$ over $\mathbb{F}_4$ has multiplicity 4.

It is probable , I have not proved this yet, that the scheme of bitangents is a local complete intersection. That is, if the variety $V(f_1, f_2)$ contains a point of our scheme as an irreducible component and the multiplicity of this point in $V(f_1, f_2)$ is 4, then f_1, f_2 is a regular sequence in the local ring of this point. Thus, we can describe the scheme fully at the point in terms of these 2 equations.

Remark. The scheme of bitangents can also be defined in an alternative way using invariants of binary quartics, and this is one of the reasons why it's probably a local complete intersection.

Returning to the point $(1, 0) \in \tilde{S}(\mathbb{F}_2)$, the four points in S_7 reducing to this are $A = \{(-33 - 12\theta, 8 + 7\theta), (55 - 10\theta, 20 + \theta), (-33 + 12\theta, 8 - 7\theta), (55 + 10\theta, 20 - \theta)\}$, and all these points occur with multiplicity 4 in the vanishing set of

$$\begin{aligned} f_1 =& 43290a_1^5a_2 - 134320a_1^4 + 104724, a_1^3a_2^2 + 2815a_1^2a_2^4 - 32950a_1^2a_2 + 376a_1a_2^6 + \\ & 60948a_1a_2^3 - 70500a_1 - 3238a_2^5 + 28855a_2^2 \\ f_2 =& 611a_1^6 + 6846a_1^4a_2 - 1676a_1^3a_2^3 - 14978a_1^3 + 5958a_1^2a_2^2 - 2766a_1a_2^4 + 6846a_1a_2 \\ & + 224a_2^6 - 1676a_2^3 + 611 \end{aligned}$$

Let $F = (f_1, f_2)$ and dF the Jacobian matrix of F. For every $a \in A$, the valuations of F and the determinant of J are $\nu_{\mathfrak{p}}(F(a)) = 9$ and $\nu_{\mathfrak{p}}(\det(dF(a))) = 4$. We use the following multivariate Hensel's lemma.

Theorem 15. *(Multivariate Hensel's Lemma) Let k be a number field and k_ν a non-Archimedean completion. Let O_ν denoted the ring of integers of k_ν. If $F \in O_\nu[x_1, \ldots, x_n]$ and $\mathbf{x_0} \in O_\nu^n$ is such that*

$$||lF(\mathbf{x_0})|| \ < \ (|\, dF(x_0)\,|_\nu)^2$$

Then there exists a unique $\mathbf{x} \in O_\nu^n$ satisfying:

$$\| \mathbf{x} - \mathbf{x_0} \| < |\det(J(x_0))|_\nu \text{ and } F(x) = 0$$

where dF is the Jacobian matrix.

Here $||\cdot||$ is the norm on k^n, defined as $||\mathbf{x}|| = \max_{1 \leq i \leq n} |x_i|_\nu$.

Proof. See [7, Theorem 2.1] □

Therefore each point of A has a unique lift to O_K. In the next subsection, we'll describe how to find these lifts.

Remark. The same method can be used to prove the existence of four unique lifts corresponding to each of the other five $\mathbb{F}_4$ points of the original scheme S. In each case, different equations f_1, f_2 are used.

Hensel Lifting. Take any point $\mathbf{a} = (a_1, a_2) \in A$. We explicitly describe how to calculate a lift of $\mathbf{a}$ modulo $\mathfrak{p}^k$ for any k.

Let $\nu_{\mathfrak{p}}(F(\mathbf{a})) = n$ and $\nu_{\mathfrak{p}}(\det(dF(\mathbf{a}))) = m$. As the Hensel hypothesis is satisfied, $n > 2m$ and $k = n - m > 0$. Define $\mathbf{z} = \mathbf{a} + 2^k\mathbf{y}$, this will a lift of $\mathbf{a}$ for a chosen $\mathbf{y}$. By Taylor expansion

$$\begin{aligned} F(\mathbf{z}) &= F\left(\mathbf{a} + 2^k\mathbf{y}\right) \\ &\equiv F(\mathbf{a}) + 2^k dF(\mathbf{a})\,\mathbf{y} \bmod \mathfrak{p}^{2k} \end{aligned}$$

If $F(\mathbf{z}) \equiv 0 \bmod \mathfrak{p}^{2k}$ then

$$2^k dF(\mathbf{a})\,\mathbf{y} \equiv -F(\mathbf{a}) \bmod \mathfrak{p}^{2k}$$

and since $\nu_{\mathfrak{p}}(F(\mathbf{a})) = n > k$, $(-F(\mathbf{a}))/2^k \equiv \delta \bmod \mathfrak{p}^{n-k}$ for some $\delta \in (O_K)^2$ by the Chinese Remainder theorem. Using this, we can reduce the above congruence to

$$dF(\mathbf{a})\,\mathbf{y} \equiv \delta \bmod \mathfrak{p}^k$$

Lemma 16. *Suppose $\mathbf{a} \in O_K^2$ is such that $\nu_{\mathfrak{p}}(F(\mathbf{a})) = n$, $\nu_{\mathfrak{p}}(\det(dF(\mathbf{a}))) = m$ and $2m < n$. Then there exist unimodular matrices $U, V \in M_{2\times 2}(O_K)$ and a diagonal matrix $M = diag(m_1, m_2)$ with $\nu_{\mathfrak{p}}(m_1) < \nu_{\mathfrak{p}}(m_2)$ such that $UdF(\mathbf{a})\,V = M \bmod \mathfrak{p}^k$.*

Proof. This is based on the algorithm for computing the Smith Normal form. The only key difference is that we pivot using an element of minimal valuation. □

Let U, V and M be as above, then

$$UdF(\mathbf{a})\,\mathbf{y} \equiv U\delta \bmod \mathfrak{p}^k$$

setting $\mathbf{y} = V\mathbf{x}$ and $\mathbf{u} = U\delta$ gives

$$UdF(\mathbf{a})\,V\mathbf{x} = M\mathbf{x} \equiv \mathbf{u} \bmod \mathfrak{p}^k$$

so $x_1 = u_1/m_1$ and $x_2 = u_2/m_2$. Note that these are congruent to elements of O_K, since $\nu_{\mathfrak{p}}(m_1 m_2) = m < k = n - m$. The required $\mathbf{y}$ is $\mathbf{y} = V\mathbf{x}$, and the resulting $\mathbf{z}$ is a root of F modulo $\mathfrak{p}^{2k}$ reducing to $\mathbf{a}$ modulo $\mathfrak{p}^k$.

By construction $\nu_{\mathfrak{p}}(\det(dF(\mathbf{z}))) = m$ and $\nu_{\mathfrak{p}}(F(\mathbf{a})) \geqslant 2k$, so we can repeat the procedure to obtain a root modulo $\mathfrak{p}^s$ where $s > 2k$. Continuing this, we find roots of F modulo increasing powers of $\mathfrak{p}$. For $X_0(45)$, lifts modulo $\mathfrak{p}^{120}$ were sufficient to calculate the minimal polynomials.

Algebraic Bitangents. Given the p-adic approximations, we use the LLL-algorithm to find their algebraic expressions. This is very similar to Section 3, with slight modifications accounting for the change to p-adic approximations.

Let $\theta = \tilde{a_1}$. This is an algebraic number and we'd like to find its minimal polynomial. As it's algebraic, it must satisfy an expression of the form

$$d_n\theta^n + d_{n-1}\theta^{n-1} + \cdots + d_1\theta + d_0 = 0$$

for some $n \geq 1$, $d_i \in \mathbb{Z}$ and $d_n \neq 0$.

For any $k \geq 1$, $\theta \equiv a_{1,k} \bmod \mathfrak{p}^k$ and these satisfy the same expression modulo $\mathfrak{p}^k$

$$d_n a_{1,k}^n + d_{n-1}a_{1,k}^{n-1} + \cdots + d_1 a_{1,k} + d_0 \equiv 0 \bmod \mathfrak{p}^k$$

Define a homomorphism

$$\phi_k : \mathbb{Z}^{n+1} \longrightarrow O_K/\mathfrak{p}^k$$
$$(u_0, \ldots u_n) \longmapsto u_n a_{1,k}^n + u_{n-1}a_{1,k}^{n-1} + \cdots + u_1 a_{1,k} + u_0 \bmod \mathfrak{p}^k$$

Define $L_k = \ker(\phi_k) \leqslant \mathbb{Z}^{n+1}$, a discrete subgroup of $\mathbb{Z}^{n+1}$. This contains all elements of the form $P\mathbf{e}_i$, where P is any integer in $\mathfrak{p}^k$ and $\mathbf{e}_i$ is the ith element in the standard orthonormal basis of $\mathbb{Z}^{n+1}$, so L_k has full rank.

With the standard quadratic form on $\mathbb{Z}^{n+1}$, $q(\mathbf{x}) = x_1^2 + \ldots + x_n^2$, the discrete subgroup L_k is a full rank lattice, for any $k \geq 1$.

Observe that $(d_0, \ldots, d_n) \in L_k$ for all $k \geq 1$. Given all lattices L_k we want to find this common vector. As k increases, general the length of vectors in L_k increases and so eventually $(d_0, \ldots, d_n) \in L_k$ should be the shortest vector in L_k, or close to the shortest vector, when k is large enough.

Remark. We measure the length of $v \in L_k$with respect to the norm defined by the quadratic form q, which in this case is the Euclidean norm

$$\| v \| = \sqrt{q(v)} = \sqrt{v_1^2 + \ldots + v_n^2}$$

It remains to decide when k is large enough for $(d_0, \ldots, d_n)$ to be the shortest vector in L_k. This can be decided using Hermites's theorem.

Theorem 17. *(Hermite) Let L be an n dimensional lattice and M the length of the shortest non-zero vector in L. There exist constant $\mu_n \in \mathbb{R}_{\geq 0}$ depending on only on n such that*

$$M^n \leq \mu_n d(L)^2$$

There are bounds on these μ_n given in [22, 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 [22, Page 66] □

Heuristic. For a full rank lattice $L \subset \mathbb{R}^n$, the length of the shortest vector in L is approximately $d(L)^{1/n}$

When k is large enough the length of the vector $(d_0, \ldots, d_n)$ should be smaller than the predicted bound, and this helps us identify it.

Regarding the choice of degree n, this is a guess, but there are a few things we should consider when making this choice. Given an n, and we can start with fairly small values, if this the degree or slightly bigger than the degree the following conditions should hold

- the minimum vector in the lattice, $v_{\min,k} \in L_k$ should be stable as k increases
- the length of $v_{\min,k}$ should decrease, and be significantly smaller than $d(L_k)^{\frac{1}{n+1}}$, as k increases.
- the polynomial $f_{\min}$ whose coefficient are $v_{\min,k}$ should be irreducible or its factorization should contain an irreducible polynomial of degree close to the degree of $f_{\min}$
- the minimal polynomials should respect the Galois action on the bitangents, so multiple points should have the same minimal polynomial

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

1. Guess the degree n.
2. Define the homomorphisms ϕ_k and the lattices L_k .
3. In L_k look for vectors which are shorter than $1/1000d(L_k)$. For a large enough k' we expect to see a common such short vector in all lattices L_k for all $k \geq k^{'}$. If such a vector doesn't exists, guess a different degree and start again.
4. If such a vector exists, verify the conditions stated above, and if they are all satisfied, it's extremely likely that this vector represents the coefficients of the minimal polynomial. Otherwise, guess another degree and start again.

As before, we look for linear relations between powers of the coefficients to identify which roots of the polynomials correspond to a bitangent.

If the coefficients are defined over the same number field, we may express one coefficient as a rational combination of powers of the other.

Let f_i be the minimal polynomial of θ_i and S_i the splitting field of f_i for $i = 1, 2, 3$.

Note. When the degree of f_i is large or S_i cannot be computed, similar computations can be carried out with the number fields defined by the f_i.

Suppose $S_2 \subseteq S_1$ so $\theta_1, \theta_2 \in S_1$, and we can express θ_2 as a rational combination of powers of θ_1, that is, we can find $q_0, \ldots, q_{n-1} \in \mathbb{Q}$ such that

$$\theta_2 = q_{n-1}\theta_1^{n-1} + \cdots + q_1\theta_1 + q_0$$

where n is the degree of f_1. Equivalently, there exist $z_{n-1}, \cdots, z_0, z \in \mathbb{Z}$ such that

$$z_{n-1}\theta_1^{n-1} + \ldots + z_1\theta_1 + z_0 + z\theta_2 = 0$$

As $\theta_i \equiv a_{i,k} \bmod \mathfrak{p}^k$ for all $k \geq 1$, substituting $a_{1,k}$ and $a_{2,k}$ in the above expression gives

$$z_{n-1}a_{1,k}^{n-1} + \cdots + z_1a_{1,k} + z_0 + za_{k,2} \equiv 0 \bmod \mathfrak{p}^k$$

For any $k \geq 1$, define a homomorphism,

$$r_k : \mathbb{Z}^{n+1} \longrightarrow O_K/\mathfrak{p}^k$$
$$(b, b_0, \ldots, b_{n-1}) \longmapsto ba_{2,k} + b_0 + b_1a_{1,k} + \cdots b_{n-1}a_{1,k}^{n-1} \bmod \mathfrak{p}^k$$

Let $R_k = \text{ Kernel}\,(r_k) < \mathbb{Z}^{n+1}$. As before, this is a full rank lattice in $\mathbb{Z}^{n+1}$ with the Euclidean quadratic form . For any $k \geq 1$ the vector of coefficients $(z, z_0, \ldots, z_{n-1})$ is an element of R_k for all $k \geq 1$, and when k is large enough, this will be the shortest vector R_k.

Following the same strategy as before, we search for vectors shorter than $1/1000d\,(R_k)^{1/n+1}$ and which are the shortest vectors in every R_k for $k \geq N$ for some large N.

The Torsion Subgroup of $X_0(45)$. To compute the two-torsion subgroup of $X_0\,(45)$, it was sufficient to find 14 bitangents. These are of the form $x = a_1y + a_2z$, where (a_1, a_2) are as follows

1. a_1 is a root of $x^4 - 7x^3 + 48x^2 - 7x + 1$ and $a_2 = 1/4(a_1^3 - 8a_1^2 + 48a_1 - 7)$
2. a_1 is a root of $x^4 - 3x^3 + 8x^2 - 3x + 1$ and $a_2 = 1/2(a_1^3 - 4a_1^2 + 8a_1 - 3)$
3. $a_1 = 1$ and a_2 is a root of $4x^2 + 13x + 19$
4. a_1 is a root of $x^4 + 3x^3 + 8x^2 + 3x + 1$ and $a_2 = 1/2(a_1^3 + 2a_1^2 + 8a_1 + 3)$

Remark. All of the above were found using the lifts of $(1, 0, 1, 1)$ and $(1, 1, 1, 0)$. At first, this might seem misleading as we expect to find 8 bitangent reducing to these 2 points. This is not contradictory since by using the 2-adic approximations with the LLL-algorithm, we actually found the required bitangent and all of it's Galois conjugates. It's not necessary for Galois conjugate bitangents to reduce to the same $\mathbb{F}_4$ bitangent.

Let K be the number field defined by $f = x^4 - 7x^3 + 48x^2 - 7x + 1$. All 14 bitangents above are defined over K, and clearing denominators, let $l_1, \ldots, l_{14}$ be the bitangents defined over the ring of integers of K, O_K. Consider these as function on the curve $X_0\,(45)\,/K$.

Let $\mathfrak{P} = \langle 19, 5 + \theta \rangle < O_K$, where θ is a root of f. This is a prime ideal of norm 19 and ramification index 1. By [17], reduction modulo $\mathfrak{P}$ induces an injective map

$$r_{\mathfrak{P}} : J_0\,(45)\,(K)_{\text{tors}} \longrightarrow J_0\,(45)\,(\mathbb{F}_{19})$$

Note. $J_0\,(45)\,(\mathbb{F}_{19}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})$

Let H be the subgroup of $J_0\,(45)\,(K)\,[2]$ generated by classes of divisors $\frac{1}{2}\text{div}\left(\frac{l_i}{l_1}\right)$ with $i = 2, \ldots, 14$, where the l_i the the equations of the bitangents, considered as functions on the curve. The image of H under $r_{\mathfrak{P}}$ is

$$r_{\mathfrak{P}}\,(H) \cong (\mathbb{Z}/2\mathbb{Z})^6$$

As $r_{\mathfrak{P}}$ is injective, $H \cong (\mathbb{Z}/2\mathbb{Z})^6$. Furthermore $X_0\,(45)$ has genus 3, so $J_0\,(45)\left(\overline{\mathbb{Q}}\right)[2] \cong (\mathbb{Z}/2\mathbb{Z})^6$, so $H = J_0\,(45)\left(\overline{\mathbb{Q}}\right)[2]$. Taking Galois invariants, we also deduce that K is the field of definition of the two torsion subgroup.

References

[1] Enrico Arbarello, Maurizio Cornalba, Phillip A Griffiths, and J Harris. Geometry of albebraic curves. volume i, 1985.

[2] Chad Awtrey, James R Beuerle, and Jade Schrader. Constructing galois 2-extensions of the 2-adic numbers. *The North Carolina Journal of Mathematics and Statistics*, 3:21–33, 2017.

[3] Paul Breiding and Sascha Timme. Homotopycontinuation. jl: A package for homotopy continuation in julia. In *International Congress on Mathematical Software*, pages 458–465. Springer, 2018.

[4] Roland Bulirsch, Josef Stoer, and J Stoer. *Introduction to numerical analysis*, volume 3. Springer, 2002.

[5] Roland Bulirsch, Josef Stoer, and J Stoer. *Introduction to numerical analysis*, volume 3. Springer, 2002.

[6] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[7] Keith Conrad. A multivariable hensel's lemma. *Lecture note available at http://kconrad. math. uconn. edu/blurbs*, 2020.

[8] Maria Angelica Cueto and Hannah Markwig. Combinatorics and real lifts of bitangents to tropical quartic curves. *arXiv preprint arXiv:2004.10891*, 2020.

[9] Igor V Dolgachev. *Classical algebraic geometry: a modern view*. Cambridge University Press, 2012.

[10] Cassiano Durand and Christoph M Hoffmann. Continuum: A homotopy-continuation solver for systems of algebraic equations. 1998.

[11] Roger H Dye. On the arf invariant. *Journal of Algebra*, 53(1):36–39, 1978.

[12] Phillip Griffiths and Joseph Harris. *Principles of algebraic geometry*. John Wiley & Sons, 2014.

[13] Corey Harris and Yoav Len. Tritangent planes to space sextics: the algebraic and tropical stories. In *Combinatorial Algebraic Geometry*, pages 47–63. Springer, 2017.

[14] Joe Harris. Theta-characteristics on algebraic curves. *Transactions of the American Mathematical Society*, 271(2):611–638, 1982.

[15] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[16] Gert Heckman. Symplectic geometry, 2013.

[17] Nicholas M Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1980.

[18] Yoav Len and Hannah Markwig. Lifting tropical bitangents. *Journal of Symbolic Computation*, 96: 122–152, 2020.

[19] David Mumford. Theta characteristics of an algebraic curve. In *Annales Scientifiques de l'École Normale Supérieure*, volume 4, pages 181–192, 1971.

[20] Ekin Ozman and Samir Siksek. Quadratic points on modular curves. *Mathematics of Computation*, 88 (319):2461–2484, 2019.

[21] Marco Pacini and Damiano Testa. Complex and tropical counts via positive characteristic. *arXiv preprint arXiv:2004.00955*, 2020.

[22] Nigel P Smart. *The algorithmic resolution of Diophantine equations: a computational cookbook*, volume 41. Cambridge University Press, 1998.

[23] JM Verschelde. Homotopy continuation methods for solving polynomial systems. 1998.