



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Journal of Number Theory 112 (2005) 369–385

JOURNAL OF
**Number
Theory**

www.elsevier.com/locate/jnt

Models of some genus one curves with applications to descent

Catherine O’Neil

Department of Mathematics, MIT, Room 2-267, 77 Massachusetts Ave, Cambridge, MA 02139, USA

Received 25 November 2003; revised 23 July 2004

Communicated by B. Poonen

Available online 1 February 2005

Abstract

Let p denote a prime, and K a field of characteristic prime to p and containing the p th roots of unity. For p equal to 3 and 5, the author finds a scheme T_p and a family of genus one curves over T_p such that any genus one curve defined over the field K of index p whose Jacobian elliptic curve E has $E[p](K) = E[p](\overline{K})$ is isomorphic to a curve lying over a K -point of T_p . The author then relates the explicit presentation of such families to the program of descent on elliptic curves.

© 2005 Published by Elsevier Inc.

Keywords: Elliptic curves; Descent; Index of genus one curves

1. Introduction

In [14], the author proved that the existence of models of certain genus one curves is equivalent to the triviality of a norm symbol. As a natural next step, one can start with a trivial norm symbol and find a corresponding explicit model. In this paper we in fact find families of genus one curves which live over the “generic trivial norm symbol;” as we will see, this is in some sense as close as we can come to finding a moduli space for genus one curves with fixed index and fixed Jacobian.

Such models can be used in performing n -descent for an elliptic curves E defined over a field K which has $E[n](K) = E[n](\overline{K})$. In particular, this paper gives families

E-mail address: coneil@math.mit.edu.

of genus one curves for special cases when $n = 3$ and 5 ; also included are explicit versions of another related map used in descent.

A few remarks are warranted. First, 2-descent over \mathbb{Q} is completely known and implemented for the computer even without assuming rationality of 2-torsion points; see John Cremona's "mwrank" program and [5], based on the methods explained in [2]. For complete 2-descent over a general number field see [19]. An algorithmic method for performing part of p -descent with no rationality assumption and which generalises to some higher genus cases can be found in [21] and is discussed further below. Even with the above references in mind, there is still work to be done; loosely speaking, when there is nontrivial 2-torsion in III , 2-descent is not effective, but 3-descent may be, if the 3-torsion of III is trivial. Therefore it is useful to have two primes completely understood, or maybe more if possible.

When descent was originally developed, it was intended that one would perform prime power descent for a fixed prime; thus the natural choice after 2-descent is 4-descent. In [3], it is explained how to see if a 2-covering can be lifted to a 4-covering, by showing how to compute the Cassels–Tate pairing. However, it is not easy to do in practice and when it shows that a lift is possible it does not deal with the practical questions concerning explicit models for the resulting 4-coverings and finding rational points on them. For an account of the state of 4-descent through 1996, see [12]. Currently, Womack and Cremona [6] are extending results from Womack's thesis [22] to work out a definitive theory of minimal models for locally soluble 4-coverings. Womack's thesis has been implemented in Magma 2.11, and, when combined with appropriate reduction techniques and Noam Elkies' LLL/ p -adic point search techniques [8], provides a feasible way to search for rational points on the locally soluble 4-coverings.

A genus one curve of order dividing a positive integer n always has a line bundle of degree n^2 , so an embedding (by a full linear series) in \mathbb{P}^{n^2-1} . The theorem in [14] explains when such a curve has in fact a line bundle of degree n , in other words an embedding (by a full linear series) in \mathbb{P}^{n-1} . When $n = 3$ this is the difference between cubic curves in \mathbb{P}^2 and intersections of quadrics in \mathbb{P}^8 , which is computationally significant. When $n = 5$ the difference is even more stark. Since all elements of Selmer groups of elliptic curves have these smaller degree line bundles, the curves we find are sufficient to perform n -descent.

Next, we know that no elliptic curve has full 3 or 5 torsion over \mathbb{Q} , by the Galois equivariance of the Weil pairing. Therefore the models we develop in this paper for performing 3-descent and 5-descent only apply over larger number fields. However it is still an interesting question to perform descent in this case in order to determine, on the one hand, the Mordell–Weil rank over a finite extension of \mathbb{Q} , thus bounding the \mathbb{Q} -rank, and on the other hand, the size of III over a finite extension of \mathbb{Q} , although this does not bound the size of $\text{III}[n]$ over \mathbb{Q} .

In [21], there is an algorithm which, given the Weierstrass equation for an elliptic curve, locates the p -torsion of its Selmer group (for a prime number p) as a subgroup of an arithmetic object over the basefield. There are many cases where just computing the size of the Selmer-group, together with a naive search for generators on the elliptic curve, suffices for finding a maximal independent set of points on elliptic curves. In

that situation, one usually still says that the Mordell–Weil rank has been successfully determined using a “descent”. In these situations, one does not need models of the homogeneous spaces. In fact, for higher-dimensional abelian varieties, this is the only technique that is applicable to any generality.

However, the algorithm in [21] does not give models for the corresponding curves, a key ingredient in descent when the naive approach outlined above fails. To some extent, this paper complements that approach: we do not attempt to locate the Selmer group per se (although the period–index obstruction is one that, as was mentioned above, is trivial for Selmer elements), but we do give models for all curves sitting inside an analogous arithmetic object. Collaborative work is currently in progress [7] to utilise the results of [21] and, to some extent, to generalise the techniques we use here, to explicitly perform 3-descent on E (in Weierstrass form) without any assumptions of rationality of the 3-torsion points of E .

Finally, just finding a model of the homogeneous space is probably not going to aid in finding rational points, unless one is able to “reduce” the model, i.e., find an isomorphic model with small coefficients. A relevant reduction theory is also being worked out in [7] at least for cubics.

2. Modeling genus one curves: sampling spaces

For elliptic curves, as well as for curves of higher genus, the usual moduli space constructions rely on the existence of a standard model of the curve in a fixed projective space. By contrast, not all curves of genus one over K have a smooth model in \mathbb{P}_K^2 , or, in fact, in projective space of any given dimension. The smallest integer n such that a genus one curve C has a line bundle of degree n (and so can be embedded normally in \mathbb{P}_K^{n-1} if $n \geq 3$) is called the *index* of C . If we fix a number field K and vary C , the index is unbounded [16].

2.1. Models

Let K be a field, and denote by G_K its absolute Galois group. Fix an elliptic curve E over K and an integer $n \geq 2$.

Definition 1. With respect to the data (E, n) as above, define the category $\mathcal{C}_{(E,n)}$ as follows. An *object* of $\mathcal{C}_{(E,n)}$ is a pair (C, \mathcal{L}) where C is a smooth genus one curve over K whose Jacobian elliptic curve $J(C)$ is isomorphic to E , and where \mathcal{L} is a degree n line bundle on C , i.e. an element in $\text{Pic}^n(C)(K)$. A *morphism* between two objects (C_1, \mathcal{L}_1) and (C_2, \mathcal{L}_2) of $\mathcal{C}_{(E,n)}$ is a K -isomorphism from C_1 to C_2 which pulls back \mathcal{L}_2 to \mathcal{L}_1 .

Remark. We distinguish between the *functor* $\text{Pic}^n(C)$ (taking a K -scheme S to the set of degree n line bundles over $C \times_K S$) with its corresponding *coarse moduli scheme* $\underline{\text{Pic}}^n(C)$: a K -point of $\underline{\text{Pic}}^n(C)$ corresponds not to an actual degree n line bundle over C but rather to a G_K -equivariant (degree n) divisor class. The difference between

these two notions is of essential importance and will be more thoroughly examined in Section 3.

Given a pair (C, \mathcal{L}) as above, fix a basis for $\Gamma(\mathcal{L}, C)$. With respect to this basis there exists a vector space V of equations F_i in \mathbb{P}^{n-1} and an injective map of K -group schemes $\chi : E[n] \rightarrow \mathrm{PGL}_n$ so that the equations F_i cut out the locus of the map $C \rightarrow \mathbb{P}(\Gamma(\mathcal{L}, C)) \cong \mathbb{P}^{n-1}$ and such that the for $T \in E[n](\overline{K})$, $\chi(T) \in \mathrm{PGL}_n(\overline{K})$ gives the automorphism “translation-by- T ” on C as a subvariety of \mathbb{P}^{n-1} . In particular, the image of $E[n]$ in PGL_n fixes the variety defined by the F_i .

Example. When $n = 3$, the vector space V is just 1-dimensional, generated by a cubic equation for the curve C , and in this case the “translation-by- T ” for a three-torsion point T is given by an element of $\mathrm{PGL}_n(K(T))$. For $n \geq 4$, V is $\frac{n(n-2)}{2}$ -dimensional and consists of quadrics (an easy generalisation of [10, Proposition IV.2.1]).

Definition 2. With notation as above, a *model* of the pair (C, \mathcal{L}) is the pair (V, χ) .

Remark 3. A model for (C, \mathcal{L}) depends on the choice of basis for $\Gamma(\mathcal{L}, C)$. Therefore the “space of models” for the pair (C, \mathcal{L}) is a GL_n -torsor over the category $\mathcal{C}_{(E,n)}$.

Now let \mathcal{C} be the category of schemes of finite type over K . For any scheme S of \mathcal{C} , we can define the category $\mathcal{C}_{(E,n)}(S)$ of pairs $(C \xrightarrow{\pi} S, \mathcal{L})$ where $C \xrightarrow{\pi} S$ is a projective flat morphism whose fibers are smooth genus one curves and \mathcal{L} is an invertible sheaf on C of degree n and whose morphisms are isomorphisms compatible with the line bundles. From [13, Remark A, p. 126], we see that we automatically get a closed immersion of C into $\mathbb{P}(\pi_*(\mathcal{L}))$ over S . Moreover, when S is a field or the spectrum of a local ring, $\mathbb{P}(\pi_*(\mathcal{L}))$ is isomorphic to \mathbb{P}_S^{n-1} once we have chosen a basis of the module of global sections of the sheaf \mathcal{L} .

The association $\mathcal{H} : S \mapsto \mathcal{C}_{(E,n)}(S)$ is a functor of groupoids. We will actually be working with a slightly coarser concept, arising from the period–index obstruction map. This map, denoted by Ob , will be studied in Section 3. In anticipation, we have the following definition:

Definition 4. Define H_{Ob} to be $\pi_0(\mathcal{H})$, which sends the scheme $S \in \mathcal{C}$ to *equivalence classes of objects* $(C \xrightarrow{\pi} S, \mathcal{L})$ of $\mathcal{C}_{(E,n)}(S)$, where two objects are in the same equivalence class when there is a morphism in $\mathcal{C}_{(E,n)}(S)$ between them.

Our goal is to find an efficient family of models living over the functor H_{Ob} . To this end we introduce the notion of sampling spaces.

2.2. Sampling spaces

Definition 5. An *arithmetic object* is a functor from \mathcal{C} to the category of sets.

For example, any scheme $X \in \mathcal{C}$ gives rise to its functor of points. This associated functor will also be denoted by X . A *natural transformation of functors* is the natural

analog to a morphism of schemes; indeed if we are given $X, Y \in \mathcal{C}$ and a morphism $f : X \rightarrow Y$, then their associated functors will have a natural transformation, also denoted by f .

Definition 6. A *sampling space* for an arithmetic object H is a pair (T, Φ) where $T \in \mathcal{C}$ and Φ is a natural transformation from the functor associated to T to H which is required to be surjective on L -points whenever L is a finite extension of K . In particular this implies that the map $T(\overline{K}) \rightarrow H(\overline{K})$ is surjective.

When an arithmetic object H is a representable functor, then its sampling space can be taken to be the corresponding fine moduli scheme. However, if H is not representable, sampling spaces are an alternative to coarse moduli schemes that trade efficiency for completeness. Sampling spaces live *above* our functor (i.e. map to H) and lose no arithmetic information. By contrast, coarse moduli schemes live *below* their functors and do lose arithmetic information. The difference between the dimension of a sampling space for H and the dimension of a coarse moduli scheme for H , if both exist, can be viewed as an arithmetic “bloating factor,” i.e. the number of extra parameters that one needs to, say, program a computer to completely list all arithmetic objects of a given type. A good example is given by the functor $\mathcal{E}ll$ which associates to $S \in \mathcal{C}$ the elliptic curves over S up to isomorphism. The coarse moduli scheme for $\mathcal{E}ll$ is the j -line, a curve. However, to actually list all elliptic curves over \mathbb{Q} (up to isomorphism), one needs both the j -invariant and a separate parameter to take into account all the quadratic twists of a fixed elliptic curve. It is not hard to see that this forces any sampling space for $\mathcal{E}ll$ to have dimension at least 2. For more on sampling spaces, see [15].

Remark 7. A sampling space for an arithmetic object H comes endowed with a “tautological object,” (e.g. if $H = H_{Ob}$, a genus one curve over T and a line bundle). To obtain this tautological object, we take the identity map on the sampling space T to $\Phi(Id_T)$, which will be an element in $H(T)$.

With the above discussion in mind, our goal is to explicitly find an efficient sampling space (and its tautological object) for H_{Ob} with respect to the data (E, n) over the base field K . The dimension of our sampling space T will roughly determine the efficiency of a computer package that would search through curves in the tautological object over T .

3. The period–index problem

Let K be a field, n an integer prime to the characteristic of K , and E an elliptic curve over K . Denote by G_K the absolute Galois group of K . We have a well-known exact sequence

$$1 \rightarrow E(K)/nE(K) \rightarrow H^1(K, E[n]) \rightarrow H^1(K, E)[n] \rightarrow 1.$$

By Theorem 3.6 of [18, p. 291], the group $H^1(K, E)$ in the above sequence parameterizes principal homogeneous spaces of the elliptic curve E . We typically denote a principal homogeneous space by C . The *period* of C is the exact order of C as an element of $H^1(K, E)$. Equivalently, the period of C is the smallest positive integer n so that there exists a K -rational point on $\text{Pic}_C^n(K)$. The *index* of C is the smallest integer d so there is a K -rational divisor of degree d on C . Equivalently, the index is the smallest degree of a field extension L over K so that $C(L) \neq \emptyset$. The classical period–index question is to determine when the period equals the index. This question can be generalised to abelian varieties (see [11]). In [14], this question was slightly refined. Instead of asking whether a given homogeneous space C has its period equal to its index, one lifts C to a diagram involving C (see below) and asks whether the diagram has period equal to index. A given C therefore may lift in different ways and give different answers. Finally, the classical period–index problem can be restated, is there a lift of C which has period equal to index?

By Proposition 2.2 of [14, p. 3], the middle group $H^1(K, E[n])$ parameterizes diagrams $C \rightarrow S$ where C is a period n principal homogeneous spaces of the elliptic curve E as above, and where S is a Brauer-Severi variety of dimension $n - 1$. These diagrams are twists of a fixed “base diagram” $E \rightarrow \mathbb{P}^{n-1}$, given by the divisor $n \cdot O_E$. In the above exact sequence, the map from the middle group to the right group is the forgetful map sending $C \rightarrow S$ to C . There is also another forgetful map, namely the map sending $C \rightarrow S$ to S , which is a quadratic map from $H^1(K, E[n])$ to $H^1(K, \text{PGL}_n) = H^2(K, \mathbb{G}_m)$ and is called the *period–index obstruction map*, or *Ob*. The obstruction is trivial exactly when S is isomorphic over K to \mathbb{P}^{n-1} , and in this case we say that the diagram $C \rightarrow S$ has its period equal to its index.

Assume now that there exists an G_K -equivariant isomorphism $E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which induces (via the Weil pairing) $H^1(K, E[n]) \cong K^*/K^{*n} \times K^*/K^{*n}$. The period–index obstruction for an element $(a, b) \in H^1(K, E[n])$ can be identified [14, Proposition 3.4, p. 6] as the “norm symbol” or the generalised Hilbert symbol $(a, b)_{\text{Hilb}, n}$. This symbol is trivial exactly when b is in the image of the norm map from the field $K(\alpha)$ to K , where α is chosen such that $\alpha^n = a$.

4. A sampling space for H_{Ob} for any odd n when $A = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Let K be a field whose characteristic is prime to n . Assume we have a fixed primitive n th root of unity $\zeta \in K$. Fix $A_n = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ with the pairing $e_n((a, b), (c, d)) = \zeta^{ad-bc}$. Note that an elliptic curve whose n -torsion is isomorphic to A_n corresponds to a point of the modular curve $X(n)$, so in some sense we are working over $X(n)$. However, it is enough to fix one elliptic curve E with $\alpha_n : A_n \cong E[n]$.

Define the K -algebra $K_a = K[x]/(x^n - a)$. Define as usual the trace and norm maps $Tr : K_a \rightarrow K$ and $\mathbb{N} : K_a^* \rightarrow K^*$. It is not hard to see that the norm symbol $(a, b)_{\text{Hilb}, n}$ is trivial exactly when b is in the image of the norm map from the algebra K_a to K . Define the scheme

$$T_n = \text{Proj}(K[a, a^{-1}, \beta_0, \beta_1, \dots, \beta_{n-1}, \mathbb{N}(\beta)^{-1}]).$$

Here $\mathbb{N}(\beta)$ denotes the norm of the element $\beta = \sum_{i=0}^{n-1} \beta_i x^i \in K_a$. This is a polynomial, homogeneous of degree n in the β_i , depending on a but not on a choice of n th root of a . Thus a K -point of $\text{Spec}(K[a, a^{-1}, \beta_0, \beta_1, \dots, \beta_{n-1}, \mathbb{N}(\beta)^{-1}])$ is a choice of an invertible element a and an invertible element $\beta \in K_a$. We can view this as a graded ring, where we endow each β_i with weight 1 and a with weight 0. A K -point of T_n will then be an invertible element a and an invertible element $\beta \in K_a$ modulo K^* . It is not hard to see that for any scheme S of finite type over K we have a functorial map $T(S) \rightarrow H_{\text{ét}}^1(S, \mu_n \times \mu_n)$ which is trivial after composing with the obstruction map to $H^2(S, \mathbb{G}_m)$. Thus we have proved the following theorem:

Theorem 8. *A sampling space for H_{Ob} with respect to the data $(E_\lambda, n, A_n, \alpha_n)$ over the base field K is given by T_n , a scheme of dimension n over K .*

The remainder of this paper will be devoted to explicitly computing the tautological genus one curve families lying over T_3 and T_5 .

5. The tautological family over T_3

Let K be a field of characteristic prime to 3. Assume there exists a primitive third root of unity $\zeta \in K^*$. Define the elliptic curve E_λ given by the cubic $X^3 + Y^3 + Z^3 + \lambda XYZ$ with origin $O_{E_\lambda} = (1; -1; 0)$. Here we fix $A_3 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ with the pairing $e((a, b), (c, d)) = \zeta^{ad-bc}$ and we fix α_3 to take $(1, 0)$ to the point $(1; -\zeta; 0)$ and to take $(0, 1)$ to the point $(0; 1; -1)$. The curve E_λ is the universal elliptic curve over $X(3)$. Now let E be any elliptic curve over the field K such that $E[3](K) = E[3](\overline{K})$. The curve E is then isomorphic to the elliptic curve E_λ for some $\lambda \in K$. We will choose such a λ and the cubic E_λ will serve as our “base diagram.”

We want to explicitly define the (tautological) genus one curve family lying over T_3 . We start with a pair $(a, \beta) \in K^* \times K_a^*$. Write $\beta = \beta_0 + \beta_1 x + \beta_2 x^2$, for $\beta_i \in K$. Define $b \in K^*$ to be the image of β under the norm map \mathbb{N} . Let $u = \beta/\sigma(\beta)$, where σ is a linear K -action of K_a taking x to $\zeta_3 x$. Note that u only depends on the class of β modulo the action of $\mathbb{G}_{m,K}$. Finally, define

$$M_{a,n} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a & 0 & 0 & \dots & 0 \end{pmatrix} \quad \text{and} \quad D_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \zeta_n & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ a & 0 & 0 & \dots & \zeta_n^{n-1} \end{pmatrix}.$$

Theorem 9. *The curve $C_{(a,\beta)}$ is given by*

$$(Tr(u) + \lambda)(a^2 X^3 + aY^3 + Z^3) + 3 Tr(xu)(aX^2 Z + aY^2 X + Z^2 Y) + 3 Tr(x^2 u)(aX^2 Y + Y^2 Z + Z^2 X) + 3(2a Tr(u) - \lambda a) XYZ = 0.$$

Proof. By results in [13], the “base diagram” $E \rightarrow \mathbb{P}^2$ induces an injective group scheme morphism $E[n] \rightarrow \text{PGL}_3$; that is, the action on E of translation by a 3-torsion point $T \in E[3](K)$ can be represented as an element of $\text{PGL}_3(K)$. Next, if C is represented in $H^1(G, E[3])$ by the pair (a, b) which depends on a chosen basis $\langle S, T \rangle$ then the determinants of the matrices representing “translation by S ” and “translation by T ” are a and b , respectively. Moreover the Weil pairing is given by the commutator of lifts to $\text{GL}_3(K)$. In fact the period–index obstruction for the pair (a, b) can be identified with the cyclic algebra $\langle x, y \mid x^3 = a, y^3 = b, xyx^{-1}y^{-1} = \zeta \rangle$. This algebra is trivial in the Brauer group exactly when it can be embedded in $\text{GL}_3(K)$. Such an embedding will give us the map χ from Definition 2.

With that in mind, define $\chi(S) = M_S$ to be the matrix $M_{a,3}$ and $\chi(T) = M_T$ to be the matrix $D_3[\beta_0 I + \beta_1 M_S + \beta_2 M_S^2]$, if $\beta = \beta_0 + \beta_1 \alpha + \beta_2 \alpha^2$. We will search for the model for $C \leftrightarrow (a, \beta)$ by finding cubics which are invariant under the image of χ . The determinant of M_S is a , the determinant of M_T is b , and the commutator $[M_S, M_T]$ is ζI . A cubic which is invariant under the action of M_S but with no fixed points must be of the form

$$F = A(a^2 X^3 + aY^3 + Z^3) + B(aX^2Z + aY^2X + Z^2Y) + C(aX^2Y + Y^2Z + Z^2X) + 3DXYZ = 0.$$

This is because M_S acts linearly on the 10-dimensional space of cubics. There are three eigenspaces of dimensions 3, 3, and 4, and the first two have zeroes at the fixed points of M_S , whereas the last eigenspace does not and is generated by the above four cubics.

On the other hand we also insist that F be invariant under the action of M_T . To ease computations we introduce the following notation: fix eigenvectors $v_i = (1, \alpha \zeta^i, \alpha^2 \zeta^{2i})$ of M_S , for some $\alpha \in K_a$ such that $\alpha^3 = a$. Then $M_S v_i = \alpha \zeta^i v_i$. The four coefficients A, B, C , and D are linear combinations of $F(v_0), F(v_1), F(v_2)$, and $\mathcal{T}(v_0, v_1, v_2)$, where \mathcal{T} is the trilinear form associated to F , as follows:

$$\begin{pmatrix} F(v_0) \\ F(v_1) \\ F(v_2) \\ \mathcal{T}(v_0, v_1, v_2) \end{pmatrix} = \begin{pmatrix} 3a^2 & 3a^{5/3} & 3a^{4/3} & 3a \\ 3a^2 & 3a^{5/3}\zeta^2 & 3a^{4/3}\zeta & 3a \\ 3a^2 & 3a^{5/3}\zeta & 3a^{4/3}\zeta^2 & 3a \\ 18a^2 & 0 & 0 & -9a \end{pmatrix} \begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix}.$$

Now it is easy to see how M_T acts on the $F(v_i)$:

$$\begin{aligned} F^{M_T}(v_i) &= F(M_T v_i) = F(D[\beta_0 I + \beta_1 M_S + \beta_2 M_S^2]v_i) \\ &= F(D(\beta_0 + \beta_1 \alpha \zeta^i + \beta_2 \alpha^2 \zeta^{2i})v_i) = F(\sigma^i(\beta) D v_i) = \sigma^i(\beta)^3 F(v_{i+1}). \end{aligned}$$

Similarly,

$$\mathcal{T}^{M_T}(v_0, v_1, v_2) = \mathcal{T}(\beta v_1, \sigma(\beta)v_2, \sigma^2(\beta)v_0) = b \mathcal{T}(v_0, v_1, v_2).$$

The fact that F is invariant under the action of M_T is equivalent to the projective point $P = (F(v_0); F(v_1); F(v_2); \mathcal{T}(v_0, v_1, v_2))$ being fixed by M_T . We have seen that $M_T(P) = (\beta^3 F(v_1); \sigma(\beta)^3 F(v_2); \sigma^2(\beta)^3 F(v_0); b \mathcal{T}(v_0, v_1, v_2))$. For some $\mu \neq 0$ we have $F(v_1) = \frac{\mu}{\beta^3} F(v_0)$ and $F(v_2) = \frac{\sigma^2(\beta)^3}{\mu} F(v_0)$. Moreover, the Jacobian of the above curve is (see [13]):

$$X^3 + Y^3 + \prod_{i=0}^2 F(v_i)Z^3 + \mathcal{T}(v_0, v_1, v_2)XYZ = 0,$$

in other words

$$X^3 + Y^3 + \frac{F(v_0)^3 \sigma^2(\beta)^3}{\beta^3} Z^3 + \mathcal{T}(v_0, v_1, v_2)XYZ = 0;$$

setting $F(v_0) = \frac{\beta}{\sigma^2(\beta)}$ (note that $F(v_0) \neq 0$ because F has no fixed points under the action of M_S) and renaming $\mathcal{T}(v_0, v_1, v_2) = \lambda$, the Jacobian is exactly E . Note that $\sigma(F(v_i)) = F(\sigma(v_i)) = F(v_{i+1})$, so $F(v_1) = \frac{\sigma(\beta)}{\beta}$ and $F(v_2) = \frac{\sigma^2(\beta)}{\sigma(\beta)}$. To finish the proof, we need to invert the above matrix to find the coefficients A, B, C , and D in terms of the $F(v_i)$'s and \mathcal{T} :

$$\begin{pmatrix} A \\ B \\ C \\ D \end{pmatrix} = \frac{1}{27a^2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 3\alpha & 3\alpha\zeta & 3\alpha\zeta^2 & 0 \\ 3\alpha^2 & 3\alpha^2\zeta^2 & 3\alpha^2\zeta & 0 \\ 2a & 2a & 2a & -a \end{pmatrix} \begin{pmatrix} F(v_0) \\ F(v_1) \\ F(v_2) \\ \mathcal{T}(v_0, v_1, v_2) \end{pmatrix}.$$

We can ignore the factor of $\frac{1}{27a^2}$, since we are working projectively. Then $A = F(v_0) + F(v_1) + F(v_2) + \mathcal{T}(v_0, v_1, v_2) = \frac{\beta}{\sigma^2(\beta)} + \frac{\sigma(\beta)}{\beta} + \frac{\sigma^2(\beta)}{\beta} + \lambda = Tr(u) + \lambda$, and similarly for the other coefficients. \square

6. The tautological family over T_5

Let K be a field. Assume $char(K) \neq 5$. Fix a primitive fifth root of unity $\zeta \in K^*$. Define E_λ to be the elliptic curve given by the equations $\lambda x_i^2 + \lambda^2 x_{i-2} x_{i+2} - x_{i-1} x_{i+1} = 0$ for i between 0 and 4 and whose origin is given by $\mathcal{O}_E = (\lambda; -1; 1; -\lambda; 0)$. Now we fix $A_5 = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ with the pairing $e((a, b), (c, d)) = \zeta^{ad-bc}$ and we fix α_5 to take $(1, 0)$ to the point $(\lambda; -\zeta; \zeta^2; -\lambda\zeta^3; 0)$ and to take $(0, 1)$ to the point $(0; \lambda; -1; 1; \lambda)$. The curve E_λ is the universal elliptic curve over $X(5)$. Now let E be any elliptic curve over the field K such that $E[5](K) = E[5](\overline{K})$. The curve E is then isomorphic to the elliptic curve E_λ for some $\lambda \in K$. We will choose such a λ and the above model for E_λ will serve as our “base diagram.”

We want to explicitly define the (tautological) genus one curve family lying over T_5 . We start with a pair $(a, \beta) \in K^* \times K_a^*$. Write $\beta = \sum_{i=0}^4 \beta_i x^i$, for $\beta_i \in K$. Define $b \in K^*$ to be the image of β under the norm map \mathbb{N} . Define u to be the point of $\beta/\sigma(\beta)$, where σ is a linear K -action of K_a taking x to ζx . Note that u only depends on the class of β modulo the action of $\mathbb{G}_{m,K}$.

Our first goal is to find a model for the curve $C_{(a,\beta)}$ (see Definition 2). As in the case $n = 3$ we will fix χ as follows: $\chi(S) = M_S = M_{a,5}$ and $\chi(T) = M_T = D_5 \cdot \left(\sum_{i=0}^4 \beta^i M_S^i\right)$. As before we will search for the model for $C \leftrightarrow (a, \beta)$ by finding the vector space $V_{a,\beta}$ of quadrics which is invariant under the image of χ . Note this vector space will give us our model (in other words, the model only depends on χ , not on V); modifying a diagram $C \rightarrow \mathbb{P}^{n-1}$ by an element of $\text{PGL}_n(K)$ has the effect of conjugating M_S and M_T . Since the group generated by M_S and M_T (a twist of the Heisenberg group) is its own centraliser, there is no non-trivial modification.

Our goal in this section is to determine $V_{a,\beta}$.

Definition 10. Define, for $i = 0, \dots, 4$, v_i to be points in \mathbb{A}_K^5 such that $M_S v_i = \alpha \zeta^i v_i$. In particular we see that $\sigma(v_i) = v_{i+1}$.

Definition 11. Define the action of a matrix M on a function f to be such that $f^M(x) = f(Mx)$. Then $f^{M_1 M_2} = (f^{M_1})^{M_2}$.

Lemma 12. *With notation as above, we can choose a quadric $Q \in V_{a,\beta}$ such that $Q(v_0) = Q(v_1)$ and such that $\{Q^{M_S^i}\}_{i=0..4}$ forms a basis of $V_{a,\beta}$. Moreover, such a Q is unique up to K -scaling. Therefore to determine $V_{a,\beta}$ it suffices to determine Q .*

Remark. We are actually taking a fixed quadric Q (not defined up to a scalar), since we need to make sense of the nonzero quantities $Q(v_0)$ and $Q(v_1)$.

Proof of Lemma 12. We can span $V_{a,\beta}$ by translates of any K -rational quadric Q by the action of powers of M_S since the eigenvalues of M_S acting on the space of quadrics are the fifth roots of a^2 , not defined over K . Note that $Q(v_i) \neq 0$ for all i since if so we would have $Q^{M_S^i}(v_i) = Q(M_S^i v_i) = 0$ as well, in other words we would have a point on C fixed by M_S , namely the projectivization of v_i . Next, note that $Q^{M_S^i}(v_0) = Q(M_S^i v_0) = Q(\alpha^i v_0) = \alpha^{2i} Q(v_0)$. Therefore if we replace Q by the quadric $Q' = \sum_{i=0}^4 a_i Q^{M_S^i}$, for $a_i \in K$, then $Q'(v_0) = \sum_{i=0}^4 a_i Q^{M_S^i}(v_0) = \left(\sum_{i=0}^4 a_i \alpha^{2i}\right) Q(v_0)$, and likewise $Q'(v_1) = \sum_{i=0}^4 a_i Q^{M_S^i}(v_1) = \left(\sum_{i=0}^4 a_i \alpha^{2i} \zeta^{2i}\right) Q(v_1)$. So in order to have $Q'(v_0) = Q'(v_1)$, we need to find $a = \sum_{i=0}^4 a_i \alpha^{2i}$ so that $Q(v_0)/Q(v_1) = \sigma(a)/a$. This is possible by Hilbert's Theorem 90, since $Q(v_0)/Q(v_1) = Q(v_0)/\sigma(Q(v_0))$ is in the kernel of the norm map. Next, Q' and its translates under M_S also generate $V_{a,\beta}$. The K -rational quadric Q' is nonzero since its value at v_0 is nonzero; by the above comment its translates by powers of M_S span $V_{a,\beta}$. Finally, such a Q' is unique up to an element of K , since if we had both Q and Q' such that $Q(v_0)/Q(v_1) = Q'(v_0)/Q'(v_1) = 1$,

we could write $Q' = \sum_{i=0}^4 a_i Q^{M_S^i}$ for $a_i \in K$ to get $Q'(v_0)/Q'(v_1) = a/\sigma(a) \cdot Q(v_0)/Q(v_1)$, i.e. we would have $a = \sigma(a)$, or in other words $a \in K$. \square

Our newly defined goal is to find Q as in Lemma 12. We will choose a matrix M by which to modify Q as in Lemma 12 so that the coefficients of Q^M are easy to manipulate. Define $M = (v_0 v_1 v_2 v_3 v_4)$, a 5×5 matrix defined over $K(\alpha)$. Then

$$Q^M(x) = Q(Mx) = Q\left(\sum_{i=0}^4 v_i x_i\right) = \sum_{i=0}^4 Q(v_i) x_i^2 + \sum_{0 \leq i < j \leq 4} B(v_i, v_j) x_i x_j,$$

where $B(w, v) = Q(w + v) - Q(w) - Q(v)$.

Define $M'_S = M^{-1} M_S M$ and $M'_T = M^{-1} M_T M$. Then we have $(Q^M)^{M'_S} = (Q^{M_S})^M$ and $(Q^M)^{M'_T} = (Q^{M_T})^M$. A calculation shows us $M'_S = \alpha D_5$ and $M'_T = M_{1,5}^{-1} \cdot \text{diag}(\beta, \sigma(\beta), \sigma^2(\beta), \sigma^3(\beta), \sigma^4(\beta))$.

Next, note that by assumption M_T fixes $V_{\alpha, \beta}$. Moreover, since M_T is defined over K , the image of Q under the action by M_T is again defined over K . Thus there exists $\gamma_i \in K$ such that $Q^{M_T} = \sum_{i=0}^4 \gamma_i Q^{M_S^i}$. Acting on that equation by M we get (here let $Q' = Q^M$):

$$Q'^{M'_T} = \sum_{i=0}^4 \gamma_i Q'^{(M'_S)^i}.$$

Since we know the M'_T and M'_S explicitly, we can compute the left and right sides of this equation and compare them.

$$Q'^{M'_T}(x) = \sum_{i=0}^4 Q(v_i) \sigma^{i-1}(\beta)^2 x_{i-1}^2 + \sum_{0 \leq i < j \leq 4} B(v_i, v_j) \sigma^{i-1}(\beta) \sigma^{j-1}(\beta) x_{i-1} x_{j-1}$$

and

$$Q'^{(M'_S)^i}(x) = \alpha^{2i} \left(\sum_{j=0}^4 Q(v_j) \zeta^{2ji} x_j^2 + \sum_{0 \leq j < k \leq 4} B(v_j, v_k) \zeta^{ji+ki} x_j x_k \right).$$

Proposition 13. For every $i = 0, \dots, 4$, $Q(v_i) = Q(v_0)$, $B(v_{i+1}, v_{i-1}) = B(v_1, v_4) \cdot \prod_{j=1}^i \sigma^{j-1} \left(\frac{\beta^2}{\sigma(\beta)\sigma^4(\beta)} \right)$, and $B(v_{i+2}, v_{i-2}) = B(v_2, v_3) \cdot \prod_{j=1}^i \sigma^{j-1} \left(\frac{\beta^2}{\sigma^2(\beta)\sigma^3(\beta)} \right)$.

Proof. We compare the coefficient of x_0^2 on both sides of the above equation. On the left, we get $Q(v_1)\beta^2$. On the right we get $\sum_{i=0}^4 \gamma_i \alpha^{2i} Q(v_0)$. Define $\gamma = \sum_{i=0}^4 \gamma_i \alpha^{2i}$, then we have $Q(v_1)\beta^2 = \gamma Q(v_0)$. On the other hand we have chosen Q as in Lemma

12 so that $Q(v_0) = Q(v_1) \neq 0$. Therefore $\gamma = \beta^2$. We can determine the rest of the $Q(v_i)$'s now since $1 = \sigma\left(\frac{Q(v_1)}{Q(v_0)}\right) = \frac{Q(v_2)}{Q(v_1)}$ etc. so all of the $Q(v_i)$'s are equal to $Q(v_0)$.

Next, compare the coefficients of x_1x_4 : on the left we get $B(v_2, v_0)\sigma(\beta)\sigma^4(\beta)$ and on the right we get $\sum_{i=0}^4 \gamma_i \alpha^{2i} B(v_1, v_4)$. In other words we have $\frac{B(v_2, v_0)}{B(v_1, v_4)} = \frac{\beta^2}{\sigma(\beta)\sigma^4(\beta)}$. Acting by σ on both sides gives $\frac{B(v_3, v_1)}{B(v_2, v_0)} = \sigma\left(\frac{\beta^2}{\sigma(\beta)\sigma^4(\beta)}\right)$, so $\frac{B(v_3, v_1)}{B(v_1, v_4)} = \frac{\beta^2}{\sigma(\beta)\sigma^4(\beta)} \cdot \sigma\left(\frac{\beta^2}{\sigma(\beta)\sigma^4(\beta)}\right)$. We continue in this way. Similarly, comparing coefficients of x_2x_3 on both sides we get $\frac{B(v_3, v_4)}{B(v_2, v_3)} = \frac{\beta^2}{\sigma^2(\beta)\sigma^3(\beta)}$ and we finish by acting on both sides by σ and solving for $\frac{B(v_{i+2}, v_{i-2})}{B(v_2, v_3)}$. \square

Now we have only to determine the three unknowns $Q(v_0)$, $B(v_1, v_4)$, and $B(v_2, v_3)$; moreover, since we are actually working projectively, we only need to know two of them, or more precisely it is adequate to know the ratios $\frac{Q(v_0)}{B(v_1, v_4)}$ and $\frac{Q(v_0)}{B(v_2, v_3)}$. Recall that E_λ is the elliptic curve given by the equations $\lambda x_i^2 + \lambda^2 x_{i-2}x_{i+2} - x_{i-1}x_{i+1}$ for i between 0 and 4 and whose origin is given by $\mathcal{O}_E = (\lambda; -1; 1; -\lambda; 0)$.

Theorem 14. *The Jacobian of $C_{a,\beta}$ is E_λ , where*

$$\lambda = -\frac{Q(v_0)}{B(v_2, v_3)} \frac{\sigma^3(\beta)\sigma^4(\beta)}{\beta\sigma(\beta)}.$$

Proof. By [13, Theorem 4.2, p. 37] the Jacobian of $C_{a,\beta}$ is given as E_A given by the quadratic equations $x_0^2 - x_2x_3 + x_1x_4 = 0$, $x_1^2 - x_0x_2 + Ax_3x_4 = 0$, $x_2^2 - x_1x_3 - Ax_0x_4 = 0$, $x_3^2 - x_0x_1 - x_2x_4 = 0$, and $Ax_4^2 + x_1x_2 - x_0x_3 = 0$ for a parameter

$$A = \prod_{i=0}^4 \frac{Q(v_i)}{B(v_i, v_{i+1})}.$$

Remark. This corrects a minus sign error in that paper, namely the coefficient of x_4^2 in the last equation above.

A calculation using Proposition 13 shows that the above A in this case is the fifth power of $\frac{Q(v_0)}{B(v_2, v_3)} \frac{\sigma^3(\beta)\sigma^4(\beta)}{\beta\sigma(\beta)}$. Finally, when A is a perfect fifth power, say of $-\lambda$, the K -rational map $\text{diag}(1, -\lambda, \lambda, -1, \lambda^{-2})$ maps E_A to E_λ . \square

Lemma 15.

$$\frac{Q(v_0)^2}{B(v_1, v_4)B(v_2, v_3)} = -\frac{\beta^2\sigma(\beta)}{\sigma^3(\beta)\sigma^4(\beta^2)}.$$

Proof. This follows from Lemma 4.3 of [13, p. 139] and using Proposition 13. Loosely speaking, this is a condition on the intersection of five quadrics to form a smooth genus one curve; note that five quadrics in general position do not intersect. \square

Corollary 16.

$$\frac{B(v_1, v_4)}{Q(v_0)} = \lambda \cdot \frac{\sigma^4(\beta)}{\beta}.$$

We now have all of the coefficients of Q' in terms of $Q(v_0)$. We can divide out by this non-zero term to get

Proposition 17. Let $u_1 = \frac{\sigma^4(\beta)}{\beta}$ and $u_2 = \frac{\sigma^3(\beta)\sigma^4(\beta)}{\beta\sigma(\beta)}$. Then Q' is given by

$$\sum_{i=0}^4 x_i^2 + \lambda \sum_{i=0}^4 x_i x_{i+2} \cdot \sigma^{i+1} u_1 - \lambda^{-1} \sum_{i=0}^4 x_i x_{i+1} \cdot \sigma^{i+3} u_2.$$

Finally, since $Q' = Q^M$, we can recover Q as $Q'^{M^{-1}}$. A calculation shows:

Theorem 18. Write

$$Q = \sum_{0 \leq i \leq j \leq 4} a_{ij} x_i x_j.$$

Then the a_{ij} are given as follows. For $i = j$ we have

$$a_{ii} = Tr \left(\frac{1}{\alpha^{2i}} \right) + \lambda Tr \left(\frac{u_1}{\alpha^{2i}} \right) - \lambda^{-1} Tr \left(\frac{u_2}{\alpha^{2i}} \right)$$

and for $i \neq j$ we have

$$a_{ij} = Tr \left(\frac{2}{\alpha^{i+j}} \right) + \lambda Tr \left((\zeta^{i-j} + \zeta^{j-i}) \frac{u_1}{\alpha^{i+j}} \right) - \lambda^{-1} Tr \left((\zeta^{2i-2j} + \zeta^{2j-2i}) \frac{u_2}{\alpha^{i+j}} \right).$$

Remark. The question of solving “norm equations,” that is, developing an algorithm to find β as in the above theorem, has been studied extensively by Simon [20], discussed in [4, Algorithm 7.5.15, p. 383], and implemented in Pari (website to be found at <http://pari.math.u-bordeaux.fr>).

7. Application: descent

Now let K be a number field. We will briefly introduce the theory of *descent*. For a basic explanation and some examples, see [18, Chapter 10]. For more advanced

approaches, see [5,21]. The basic exact sequence in elliptic curve descent theory is a modification of the above sequence (see [18, p. 297]):

$$1 \rightarrow E(K)/nE(K) \rightarrow Sel_n(E) \rightarrow \text{III}(E)[n] \rightarrow 1.$$

Here $\text{III}(E)[n]$ is the kernel of the natural map

$$H^1(G_K, E(\overline{K}))[n] \rightarrow \prod_v H^1(G_{K_v}, E(\overline{K}_v))[n],$$

where the v range over all primes (including infinite primes) of K .

A crucial fact that we will take advantage of is that the elements of $Sel_n(E)$, which a priori correspond to diagrams $C \rightarrow S$, always have $S \cong_K \mathbb{P}^{n-1}$; in other words elements of $\text{III}(E)$ always have trivial period-index obstruction (for a proof see the Remark [14, p. 3]).

The goal of descent is traditionally to measure the size of the left-most group of the above diagrams, namely $E(K)/nE(K)$. A direct attack using computers can often find points of this set but cannot prove that we have all of them. Thus we indirectly bound this set by bounding the middle set and by (hopefully) knowing the size of the right-most set. The program of descent can be split into two parts: first, to determine the image of elements of $E(K)/nE(K)$ in the middle group $Sel_n(E)$ via the left-hand map above, and second, given an element x of the middle group, i.e. a diagram $C \rightarrow \mathbb{P}^{n-1}$, to write down the equations of this open immersion. We have already performed the second part. The remainder of this section will be devoted to explicitly computing the first map for each of the cases $n = 3$ and 5 where $E[n](K) = E[n](\overline{K})$.

We will find a pair of rational functions $(f_{S,n}, f_{T,n})$ on E which when evaluated at a point of $E(K)$ gives its image in $H^1(G, E[n]) \cong K^*/K^{*n} \times K^*/K^{*n}$. By Corollary 1.1 in [18], the functions $f_{S,n}$ and $f_{T,n}$ satisfy $div(f_{S,n}) = n \cdot (S) - n \cdot (O_E)$ and $div(f_{T,n}) = n \cdot (T) - n \cdot (O_E)$ respectively; moreover, they can be chosen to satisfy $f_{S,n} \circ [n] = g_{S,n}^n$ and $f_{T,n} \circ [n] = g_{T,n}^n$ for some rational functions $g_{S,n}$ and $g_{T,n}$.

Lemma 19. *The expansions of $f_{S,n}$ and $f_{T,n}$ with respect to a local parameter at O_E can be chosen to have leading coefficients which are perfect n th powers, i.e. so $f_{S,n} = \frac{a}{t^n} + \dots$ and $f_{T,n} = \frac{b}{t^n} + \dots$ where both a and b are perfect n th powers and where $t \in \mathcal{O}_{E,O_E}$ is a parameter in the local ring at O_E . Here “ \dots ” refers to “higher order terms.”*

Proof. First we prove that locally the expansions look like:

$$f_{S,n} = \frac{a}{t^n} + \dots, \quad g_{S,n} = \frac{c}{t} + \dots, \quad \text{and} \quad t \circ [m] = d \cdot t + \dots .$$

The first is because we know $f_{S,n}$ has a pole of order n at O_E , the second because $g_{S,n}$ has a simple pole at O_E ; in fact $div(g_{S,n}) = \sum_{mP_i=S}(P_i) - \sum_{mQ_i=O}(Q_i)$, and

since the characteristic of K does not divide n , we get only one copy of \mathcal{O}_E on the right. Finally, $t \circ [m]$ has a simple zero at \mathcal{O}_E since $[m]\mathcal{O}_E = \mathcal{O}_E$ and $[m]$ is étale when $\text{char}(K) \nmid n$. We know that $f_{T,n} \circ [n] = g_{T,n}^n$, and a quick calculation shows this is equivalent to a being a perfect n th power. \square

We will use the above lemma in both cases $n = 3$ and $n = 5$.

Proposition 20. $f_{S,3} = (\lambda^3 + 27) \frac{3\zeta^2 X + 3\zeta Y - \lambda Z}{3X + 3Y - \lambda Z}$ and $f_{T,3} = (\lambda^2 - 3\lambda + 9) \frac{3X - \lambda Y + 3Z}{3X + 3Y - \lambda Z}$.

Proof. By Lemma 19, we want then to compute the expansion of $\frac{3\zeta^2 X + 3\zeta Y - \lambda Z}{3X + 3Y - \lambda Z}$ at the origin $\mathcal{O}_E = (1; -1; 0)$. Here we can work in affine coordinates by setting $X = 1$, since this is true locally. Then $F : 1 + Y^3 + Z^3 + \lambda YZ = 0$. Moreover, since \mathcal{O}_E takes on a non-zero value at the hyperplane at S , we can just evaluate there to get $(3\zeta^2 X + 3\zeta Y - \lambda Z)|_{\mathcal{O}_E} = 3\zeta^2 - 3\zeta$. Note that $\zeta^2 - \zeta = \sqrt{-3}$, so $3\zeta^2 - 3\zeta = (-\sqrt{-3})^3$ is a cube in K . So in fact we can completely ignore this term. We are left with $\frac{1}{3X + 3Y - \lambda Z}$ which has a triple zero at \mathcal{O}_E . In other words

$$3 + 3Y - \lambda Z \cong aZ^3 + \dots,$$

where \cong signifies that we are working in $\mathcal{O}_{E, \mathcal{O}_E}$. Multiply the above by the function Y , a nonzero function at \mathcal{O}_E , to get $3Y + 3Y^2 - \lambda YZ \cong aYZ^3 + \dots$; since $-\lambda YZ \cong 1 + Y^3 + Z^3$ (we are working modulo F) we substitute to get

$$1 + 3Y + 3Y^2 + Y^3 + Z^3 = (1 + Y)^3 + Z^3 \cong aYZ^3 + \dots$$

The function $1 + Y$ has a zero at \mathcal{O}_E , so it is an alternative parameter for the local ring $\mathcal{O}_{E, \mathcal{O}_E}$: $1 + Y \cong bZ + \dots$ but we already have the tangent line equation which tells us that $3(1 + Y) \cong \lambda Z + \dots$, i.e. $b = \lambda/3$. Replace $(1 + Y)^3$ above now by $(\lambda/3)Z^3$:

$$Z^3(1 + (\lambda/3)^3) \cong aYZ^3.$$

Evaluate at $Y = -1$ to get $a = -(1 + (\lambda/3)^3)$. Our original constant then is $1/a$, which modulo cubes is seen to be $\frac{1}{27 + \lambda^3}$. Finally, to normalize we want the function $f_{S,3}$ to have a leading coefficient which is 1. In other words, we need to multiply the ratio of the two hyperplanes by the constant $27 + \lambda^3$. For $f_{T,3}$, we are already almost done- the only difference is the value of the numerator at the origin: $(3X - \lambda Y + 3Z)|_{\mathcal{O}_E} = 3 + \lambda$. The leading coefficient then is $\frac{3 + \lambda}{27 + \lambda^3} = \frac{1}{\lambda^2 - 3\lambda + 9}$. \square

Similarly, we can take $f_{S,5}$ to be a scalar multiple of the quotient of the hypertangent plane at S by the hypertangent plane at \mathcal{O}_E , since both S and \mathcal{O}_E are hyperflex points (to see this, note that E is a degree 5 curve in \mathbb{P}_K^4 and that the hyperplane $x_0 = 0$ goes through the points $i \cdot S$ for i between 0 and 4, which means that the divisor giving the embedding $E \rightarrow \mathbb{P}^4$ is linearly equivalent to $(\mathcal{O}_E) + (S) + (2S) + (3S) + (4S) \equiv 5 \cdot (\mathcal{O}_E) \equiv 5 \cdot (S)$).

Proposition 21. *The hypertangent plane at the origin of E is given by*

$$H_{O_E} : \alpha x_0 + \beta(x_1 + x_4) + \gamma(x_2 + x_3),$$

where $\alpha = \lambda^{10} - 14\lambda^5 - 1$, $\beta = -5\lambda^2(1 + 2\lambda^5)$, and $\gamma = 5\lambda^3(\lambda^5 - 2)$.

Proof. An easy calculation (in Maple for example) verifies that the above hyperplane intersects E only at O_E . In order to find the above, we computed a local parameterization of the curve E in the local ring \mathcal{O}_{E,O_E} using the equations for E and Maple. \square

To finish finding the equations $f_{S,5}$ and $f_{T,5}$, we simply find the hypertangent planes at S and T (these are translates of H_{O_E} by the 5-torsion matrices D_5 and $M_{1,5}$) and evaluate them at O_E . We then scale H_S/H_{O_E} by the appropriate function of λ so that its leading coefficient in the expansion at O_E is a perfect fifth power:

Proposition 22. *The hypertangent planes at S and at T are given by*

$$H_S : \alpha x_0 + \beta(x_1\zeta^4 + x_4\zeta) + \gamma(x_2\zeta^3 + x_3\zeta^2)$$

and

$$H_T : \alpha x_4 + \beta(x_0 + x_3) + \gamma(x_1 + x_2).$$

The rational functions $f_{S,5}$ and $f_{T,5}$ are given by

$$f_{S,5} = \frac{[(\lambda^2 + \lambda - 1)(\lambda^4 - 3\lambda^3 + 4\lambda^2 - 2\lambda + 1)(\lambda^4 + 2\lambda^3 + 4\lambda^2 + 3\lambda + 1)]^2}{5 \lambda (\zeta - \zeta^4) (\lambda^5 - 2)} \frac{H_S}{H_{O_E}};$$

$$f_{T,5} = \frac{\lambda^2(\lambda^4 - 3\lambda^3 + 4\lambda^2 - 2\lambda + 1)^2(\lambda^4 + 2\lambda^3 + 4\lambda^2 + 3\lambda + 1)}{(\lambda^2 + \lambda - 1)} \frac{H_T}{H_{O_E}}.$$

References

[2] B. Birch, H. Swinnerton-Dyer, Notes on elliptic curves (I), J. Reine Angew. Math. 212 (1963) 7–25.
 [3] J.W.S. Cassels, Second descents for elliptic curves, J. Reine Angew. Math. 494 (1998) 101–127.
 [4] H. Cohen, Advanced Topics in Computational Number Theory, Graduate Texts in Mathematics, vol. 193, Springer, Berlin, 2000.
 [5] J. Cremona, Classical invariants and 2-descent on elliptic curves, J. Symbolic Comput. 31 (2001) 71–87.
 [6] J. Cremona, T. Womack, Explicit 4-descents on an elliptic curve II, in preparation.
 [7] J. Cremona, T. Fisher, C. O’Neil, M. Stoll, Descent on an Elliptic Curve, in preparation.

- [8] W. Bosma, Algorithmic Number Theory, Fourth International Symposium ANTS-IV, Leiden, The Netherlands, July 2–7, 2000, Proceedings Springer 2000.
- [10] K. Hulek, Projective Geometry of Elliptic Curves, Astérisque 137, Société Mathématique de France, 1986.
- [11] S. Lang, J. Tate, Principal homogeneous spaces over abelian varieties, *Amer. J. Math.* 80 (1958) 659–684.
- [12] J.R. Merriman, S. Siksek, N.P. Smart, Explicit 4-descents on an elliptic curve, *Acta Arith.* 77 (4) (1996) 385–404.
- [13] C. O'Neil, Jacobians of genus one curves, *Math. Res. Lett.* 8 (1–2) (2001) 125–140.
- [14] C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* 95 (2) (2002) 329–339.
- [15] C. O'Neil, Sampling spaces and arithmetic dimension, in preparation.
- [16] B. Poonen, Computational aspects of curves of genus at least 2, in: H. Cohen (Ed.), *Algorithmic Number Theory, Second International Symposium, ANTS-II*, Springer, Berlin, 1996, pp. 283–306.
- [18] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, New York, 1986.
- [19] D. Simon, Computing the rank of elliptic curves over number fields, *LMS JCM*, vol. 5, 2002, pp. 7–17.
- [20] D. Simon, Solving norm equations in relative number fields using S-units, *Math. Comp.* 71 (239) (2002) 1287–1305.
- [21] E.F. Schaefer, M. Stoll, How to do a p-descent on an elliptic curve, *Trans. Amer. Math. Soc.* 356 (3) (2004) 1209–1231.
- [22] T. Womack, Explicit descent on elliptic curves, Thesis, University of Nottingham, July 2003, located at <http://www.maths.nott.ac.uk/personal/jec/theses/>.