ABSTRACT

Title of dissertation: FAMILIES OF CYCLIC CUBIC FIELDS

Stephen M. Balady
Doctor of Philosophy, 2017

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

In [13], Shanks considered what he termed the "simplest cubic fields," defined as the splitting fields of the polynomials

$$S_n = X^3 + (n+3)X^2 + nX - 1. \tag{1}$$

In particular, he showed that if the square root of the polynomial discriminant is squarefree, then the roots of S_n form a system of fundamental units for its splitting field. The analysis of this family was extended by Lettl [9] and Washington [15]. Lecacheux [8], and later Washington [16], discovered a second one-parameter family with a similar property: if a certain specified chunk of the polynomial discriminant is squarefree, the roots of the polynomial form a system of fundamental units. Kishi [7] found a third such family. In the following, we show that there are many, many more families of cubics with this property. We generalize the model of Washington [16], explicitly exhibit new families of cyclic cubic fields, and interpret all known and new families as curves on the elliptic surface $X(3)$.

FAMILIES OF CYCLIC CUBIC FIELDS

by

Stephen M. Balady

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2017

Advisory Committee:
Professor Lawrence C. Washington, Chair
Professor Patrick Brosnan
Professor Daniel I. Chazan
Professor Amin Gholampour
Professor James A. Schafer

Dedication

This work would not have been possible without the warmth of the University of Maryland mathematics community. The author would like to express particular thanks to: Dr. Lawrence Washington, for infinite patience and support; Drs. Daniel Chazan and Jonathan Rosenberg, for guidance and perspective; the graduate students of MATH 4202, for their humanity; and the doers of mathematics, especially those in Spring 2017's Calculus I, who refused to work alone.

For Logan, Callie, and Koda

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction

In [13], Shanks considered what he termed the "simplest cubic fields," defined as the splitting fields of the polynomials

$$S_n = X^3 + (n+3)X^2 + nX - 1. \tag{1.1}$$

In particular, he showed that if the square root of the polynomial discriminant is squarefree, then the roots of S_n form a system of fundamental units for its splitting field. The analysis of this family was extended by Lettl [9] and Washington [15]. Lecacheux [8], and later Washington [16], discovered a second one-parameter family with a similar property: if a certain specified chunk of the polynomial discriminant is squarefree, the roots of the polynomial form a system of fundamental units. Kishi [7] found a third such family.

It is the goal of this work to show that there are many, many more families of cubics with this property. In the first part of the work, we generalize the model of Washington [16], show that all known families fit into our framework, and explicitly exhibit new families of cyclic cubic fields. In the second part, we interpret families both known and new as divisors on the elliptic surface $X(3)$ and compute their Néron-Severi classes.

Chapter 2: Families of Cyclic Cubic Fields

2.1 Introduction

Shanks [13] compares his “simplest cubic fields,” defined by

$$S_n = X^3 + (n+3)X^2 + nX - 1, \qquad n \in \mathbb{Z},$$

to the quadratic fields generated by

$$Q_n = X^2 - nX - 1.$$

The polynomial discriminant of Q_n is $D = n^2 + 4$; the larger root of Q_n is

$$\epsilon = \frac{\sqrt{D} + n}{2}.$$

By construction ϵ is a unit in $\mathbb{Q}[\sqrt{D}]$. If D is squarefree, ϵ in fact generates the group of units. Since ϵ is so concrete, explicit analysis of the regulator – and therefore of the class number – is feasible for these fields. The generalization of Q_n for real quadratic fields is given by Degert [5]: $\mathbb{Q}[\sqrt{D}]$ is said to be of Richaud-Degert type if

$$D = n^2 + r, -n < r \leq n, \text{ and } r|4n. \tag{2.1}$$

(That is, Q_n are the “simplest quadratic fields.”) The study of the class number 1 problem is complete for the quadratic fields of Richaud-Degert type assuming the

Generalized Riemann Hypothesis [11].

A reasonable generalization of Richaud-Degert type to cyclic cubic fields generated by

$$X^3 + aX^2 + \lambda X - 1$$

should involve some sort of relation between a and λ; imposing such a relation should allow us to conclude that two of the roots will generate the unit group. In the following, we present such a relation.

2.2 The Families

Let $f(n)$ and $g(n)$ be polynomials with integral coefficients, and assume that the following condition holds:

$$\lambda = \frac{f^3 + g^3 + 1}{fg} \text{ is a polynomial with integral coefficients.} \tag{2.2}$$

Examples will be given in Section 2.5. For now we remark only that this condition implies that $f|(g^3+1)$ and $g|(f^3+1)$; in particular, f and g have no common factors. If Condition 2.2 is satisfied, the pair (f, g) determines a one-parameter family of polynomials as follows:

$$P_{f,g}(X) = X^3 + a(n)X^2 + \lambda(n)X - 1, \text{ where}$$

$$a = 3(f^2 + g^2 - fg) - \lambda(f + g).$$

Note that $P_{f,g}$ is symmetric in f and g, so we'll assume that $\deg f \leq \deg g$. If this inequality is strict, then $\deg \lambda < \deg a$. Together with the rational root theorem, this implies that $P_{f,g}$ is irreducible for all but a small finite list of $n \in \mathbb{Z}$. For the rest of this chapter, we will make the standing assumptions that $\deg f < \deg g$ and then fix an integer n for which $P_{f,g}$ is irreducible. This is practical for theoretical purposes, though we note that the case where both f and g are constant is also of potential interest.

The discriminant of $P_{f,g}$ is

$$D_P = (f-g)^2(3a+\lambda^2)^2 \neq 0,$$

so $P_{f,g}$ determines a cyclic cubic field which we denote $K_{f,g}$ (or sometimes just K). Thus $P_{f,g}$ has three real roots which we denote $\theta_1, \theta_2, \theta_3$. Since the constant term of $P_{f,g}$ is a unit in $\mathbb{Z}$, these roots are units in the ring of integers $\mathcal{O}_{K_{f,g}}$.

Lemma 2.2.1. The $\mathbb{Z}_3$ action of the Galois group on the roots of $P_{f,g}$ is given by

$$G(\theta) = \frac{f\theta - 1}{(f^2+g^2-fg)\theta - g}.$$

Proof. Assume $P(\theta) = 0$. Since $1, \theta$, and θ^2 are linearly independent over $\mathbb{Q}$, we have $G(\theta) \neq \theta$. A messy but straightforward calculation shows that $P(G(\theta)) = 0$. □

Condition 2.2 and Lemma 2.2.1 might seem a bit miraculous (or at least deeply unmotivated). How could we have guessed that Condition 2.2 would lead to a cyclic cubic whose roots are units in $\mathcal{O}_K$ if we didn't already know that it did? It's possible in retrospect to intuit this from the work of Kishi [7], but we originally discovered it using the language of elliptic surfaces as follows.

If $X^3+aX^2+\lambda X-1$ generates a cyclic cubic field, its discriminant is a square: that is, there exists $b \in \mathbb{Q}$ such that

$$b^2 = 4a^3 + \lambda^2 a^2 - 18\lambda a - 4\lambda^3 - 27. \tag{2.3}$$

If we fix $\lambda \in \mathbb{Q}$, Equation 2.3 defines an elliptic curve on which (a, b) is a rational point. Treating λ as a parameter in $P^1(\mathbb{C})$ gives the equation of an elliptic surface W. In homogeneous coordinates, W is

$$b^2c = 4a^3 + \lambda^2 a^2 c - 18\lambda a c^2 - (4\lambda^3 + 27)c^3.$$

This surface is birationally equivalent to $X(3)$, which is described homogeneously as

$$x^3 + y^3 + z^3 = \lambda xyz.$$

Explicitly, the map[1] from the homogeneous form of W to $X(3)$ is given by

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} -\lambda & 1 & -9 \\ -\lambda & -1 & -9 \\ 6 & 0 & 2\lambda^2 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix}. \tag{2.4}$$

The inverse map from $X(3)$ to W is given by

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} -\lambda^2 & -\lambda^2 & -9 \\ \lambda^3 - 27 & -\lambda^3 + 27 & 0 \\ 3 & 3 & \lambda \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}. \tag{2.5}$$

The coordinates of Shanks's simplest cubics S_n (described by Equation 1.1) on W are $[a : b : c;\ \lambda] = [n+3 : n^2+3n+9 : 1;\ n]$. This is sent by the above map to the constant section $[x : y : z;\ \lambda] = [0 : -1 : 1;\ n]$ on $X(3)$. We can do the same with the family of Lecacheux [8] (presented here in the form given by Washington [16]):

$$L_n = X^3 - (n^3 - 2n^2 + 3n - 3)X^2 - n^2 X - 1.$$

[1] The observation that W is a model for $X(3)$ is contained in unpublished notes of Washington.

The W coordinates of L_n are

$$[a:b:c;\ \lambda] = [-n^3+2n^2-3n+3 : (n-1)(n^2+3)(n^2-3n+3) : 1;\ -n^2],$$

which are considerably simpler on $X(3)$:

$$[x:y:z;\ \lambda] = [-1 : -n : 1;\ -n^2].$$

Kishi's [7] family K_n also takes a simple form on $X(3)$:

$$[x:y:z;\ \lambda] = [-n : -n^2-n-1 : 1;\ -n^3-2n^2-3n-3].$$

The key observation here is that on $X(3)$, each of S_n, L_n, and K_n are of the form $[x:y:z;\ \lambda] = [f(n) : g(n) : 1;\ \lambda]$ for some polynomials f and g. Further, on $X(3)$ we can solve explicitly for λ:

$$\lambda = \frac{f^3+g^3+1}{fg}.$$

Condition 2.2 is exactly what we need to reverse this process. In this language, when f, g, and λ are polynomials with integral coefficients, $[f(t) : g(t) : 1;\ \lambda]$ determines an algebraic curve on $X(3)$. Translating back to Weierstrass form gives a family of integral points $[a : b : 1;\ \lambda]$: that is, it gives a family of polynomials $P_{f,g} = X^3 + aX^2 + \lambda X - 1$ with integral coefficients and square discriminants.

For a general $X^3 + aX^2 + \lambda X - 1$ generating a cyclic cubic field, the Galois group is generated by the fractional linear transformation

$$G = \begin{bmatrix} f & -h \\ (f^2+g^2-fg)/h & -g \end{bmatrix}$$

for some integers f, g, h, since these represent all elements $G \in \mathrm{PGL}_2(\mathbb{Q})$ for which $G^3 = I$. Conversely, if we fix f, g, h with $fgh \neq 0$, we can reconstruct

$$P_{f/h,g/h} = X^3 + \frac{3(f^2 + g^2 - fg) - \lambda h(f+g)}{h^2} X^2 + \frac{f^3 + g^3 + h^3}{fgh} X - 1;$$

that is,

$$f^3 + g^3 + h^3 = \lambda fgh.$$

This shows that the equivalence of W with $X(3)$ is actually a consequence of the structure of the Galois action. This also shows that, unless $h = 1$ and Condition 2.2 is satisfied, there's no guarantee that the roots of the associated polynomial will be algebraic integers.

2.3 The Discriminant

In this section we analyze the discriminant of $K_{f,g}$. A prime number $p \neq 3$ contributes a factor of exactly p^2 to the discriminant if and only if p ramifies (and therefore ramifies tamely) in $K_{f,g}$. If 3 ramifies, it contributes a factor of exactly 3^4. The only primes that can ramify are those that divide the polynomial discriminant of $P_{f,g}$: that is, those dividing

$$\sqrt{D_P} = (f-g)(3a + \lambda^2).$$

In fact, the discriminant factors further:

$$\sqrt{D_P} = (f-g)ABCf^{-2}g^{-2}, \text{ where}$$

$$A = f^2 + g^2 - f - g + 1,$$

$$B = (f+1)^2 + g^2 - (f+1)g, \text{ and}$$

$$C = (g+1)^2 + f^2 - (g+1)f.$$

It's mostly possible to analyze the contributions of each of these factors separately, following Washington [16] or Kishi [7]. Unfortunately this approach runs into problems in the general setting, especially for primes that divide both fg and $\sqrt{D_P}$. The core issue is that while Condition 2.2 implies that $f^2g^2|ABC$, we have very little control over in which of A, B, C this divisibility happens.

Instead of the direct approach we do the following. Let ω be a primitive cube root of unity. Then $P_{f,g}$ determines a Kummer extension of $\mathbb{Q}(\omega)$: that is, an extension of the form $\mathbb{Q}(\omega, \sqrt[3]{\alpha})$ for some $\alpha \in \mathbb{Q}(\omega)$. From there we will descend to $K_{f,g}$.

$$\begin{tikzcd}
 & \mathbb{Q}(\omega, \sqrt[3]{\alpha}) \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\omega) \arrow[d, dash] & K_{f,g} \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

A Kummer generator α_0 is constructed as follows: let θ be a root of $P_{f,g}$, so the other two roots are $G(\theta)$ and $G^2(\theta)$. Then

$$\alpha_0 = (\theta + \omega G(\theta) + \omega^2 G^2(\theta))^3.$$

This gives a massive rational function in θ, f, and g that we can reduce using the fact that θ satisfies $P_{f,g}(\theta) = 0$. When we reduce the numerator and denominator to degree 2 functions of θ, the vast majority of the terms cancel and leave an expression in f and g. We have that

$$3a + \lambda^2 = \beta\overline{\beta}, \text{ where } \beta = \lambda - 3f - 3\omega(f-g),$$

and a long and painful calculation (made possible by PARI/GP [14]) shows that

$$\alpha_0 = (f+\omega g)^3(3a+\lambda^2)\beta = (f+\omega g)^3\beta^2\overline{\beta}.$$

Since $(f+\omega g)^3$ is a perfect cube in $\mathbb{Q}(\omega)$, we choose the Kummer generator

$$\alpha = \alpha_0(f+\omega g)^{-3} = \beta^2\overline{\beta}.$$

If $\mathfrak{p} \nmid 3$ is any prime in $\mathbb{Q}(\omega)$, $\mathfrak{p}$ ramifies in $\mathbb{Q}(\omega, \sqrt[3]{\alpha})$ if and only if $v_{\mathfrak{p}}(\alpha)$ is not a multiple of 3: that is, if and only if $\mathfrak{p}$ divides α to a non-cube power. Thus we need to consider only those $\mathfrak{p}$ dividing β or $\overline{\beta}$. Together with the knowledge of the decomposition of rational primes in $\mathbb{Q}(\omega)$, we can compute $D(K_{f,g})$. We begin with the following special case.

Theorem 2.3.1. Let $K_{f,g}$ be as in Section 2.2. If $3a+\lambda^2$ is squarefree, then

$$D(K_{f,g}) = (3a+\lambda^2)^2.$$

Proof. The prime 3 is special, so we deal with it first. If $3|(3a+\lambda^2)$, then $3|\lambda$. The definition of a shows that $v_3(a) \geq 1$, so $v_3(3a+\lambda^2) \geq 2$ and $3a+\lambda^2$ is not squarefree. If $3 \nmid 3a+\lambda^2$ and 3 ramifies in $K_{f,g}$, then $f \equiv g \mod 3$ since $D(K_{f,g})$ divides D_P. If $f \equiv 0$, then (f,g) does not satisfy Condition 2.2. If $f \equiv 1$, then $3|(3a+\lambda^2)$ which we already assumed it did not. If $f \equiv 2$, then

$$P_{f,g} \equiv X^3 + X^2 - X - 1 \equiv (X-1)(X+1)^2 \mod 3,$$

so the roots are not all congruent mod the prime above 3 and therefore cannot possibly be fixed by the Galois action. So 3 is unramified and contributes nothing to $D(K_{f,g})$.

Since $|\beta|^2 = 3a+\lambda^2$, a rational prime $p \neq 3$ ramifies in $K_{f,g}$ only if $p|(3a+\lambda^2)$. In this case, there is a $\mathfrak{p}$ above p for which $\mathfrak{p}|\beta$. Since $\mathfrak{p}$ is unramified in $\mathbb{Q}(\omega)$ and $3a+\lambda^2$ is squarefree, $v_{\mathfrak{p}}(\beta) = 1, v_{\mathfrak{p}}(\overline{\beta}) = 0$, and $v_{\mathfrak{p}}(\alpha) = 2$. Therefore p ramifies in $K_{f,g}$. □

Because α is so explicit, we can do much better. The prime $p = 3$ is badly behaved, but it can be dealt with directly (as in [16] or [7]) when we're actually given a fixed family (f, g). If a prime $p \neq 3$ ramifies in $K_{f,g}$, it divides $3a+\lambda^2$. If $p \equiv 2 \mod 3$, p is inert in $\mathbb{Q}(\omega)$. Let $p^m||\beta$; then $p^m||\overline{\beta}$, so p^{3m} is a removable cube in α. If $p \equiv 1 \mod 3$, p splits as $\mathfrak{p}\overline{\mathfrak{p}}$ in $\mathbb{Q}(\omega)$; we choose $\mathfrak{p}$ so that $\mathfrak{p}|\beta$. From here we have two cases: either $\overline{\mathfrak{p}}|\beta$ or it does not. If $\overline{\mathfrak{p}} \nmid \beta$ and m is the exact power of p dividing $3a+\lambda^2$, then the p-part of α equals $\mathfrak{p}^{2m}\overline{\mathfrak{p}}^m$, which is a removable cube if and only if $3|m$. This leaves us to deal with the case where $p \equiv 1 \mod 3$ and $\overline{\mathfrak{p}}|\beta$. But in this case the rational prime $p = \mathfrak{p}\overline{\mathfrak{p}}$ divides $\beta = \lambda - 3f - 3\omega(f-g)$. Since $\{1, \omega\}$ is a $\mathbb{Z}$-basis for $\mathbb{Z}[\omega]$, we must have $p|(f-g)$. Since f and g have no common factors, $p \nmid f$. Substituting $f \equiv g$ in $3a+\lambda^2$ implies

$$\frac{(f^3-1)^2}{f^4} \equiv 0 \mod p,$$

so we conclude that $p|(f^3-1)$ and $p|(g^3-1)$, so $p|\gcd(f^3-1, g^3-1)$. If the polynomial resultant of f^3-1 and g^3-1 is nonzero (which seems always to be the case in examples), this last condition is satisfied only for the finite collection of

$p|\mathrm{res}(f^3-1, g^3-1)$. Therefore, for a family given by polynomials f, g, there are only finitely many rational primes p with $p|\beta$, and these must be treated individually. The remaining primes ramify if and only if they divide $3a+\lambda^2$ to a non-cube power. An example using this discussion to compute $D(K_{f,g})$ exactly for a specific family will be given in Section 2.5.

2.4 The Regulator and Fundamental Units

In this section, we temporarily drop the standing assumption that we have fixed an integer n and once again treat f and g as polynomials for which $\deg f < \deg g$. This implies

$$\begin{aligned} \deg \lambda &= 2\deg g - \deg f \text{ and} \\ \deg a &= 3\deg g - \deg f, \text{ so} \\ \deg(3a+\lambda^2) &= 4\deg g - 2\deg f. \end{aligned}$$

Since $\deg a > \deg \lambda$, we have

$$\begin{aligned} P_{f,g}(-a-1) &= -a^2 + o(a^2) \text{ and} \\ P_{f,g}(-a+1) &= a^2 + o(a^2). \end{aligned}$$

If n is sufficiently large we can choose θ_1 to be a root of $P_{f,g}$ for which $-a-1 < \theta_1 < -a+1$. Since we know the Galois action, we get bounds on all the roots:

$$\begin{aligned}
\log|\theta_1| &\approx \log a(n) \approx \deg a \log n = (3\deg g - \deg f)\log n,\\
\log|\theta_2| &= \log \frac{f\theta_1 - 1}{(f^2+g^2-fg)\theta_1 - g} \approx (\deg f - 2\deg g)\log n,\\
\log|\theta_3| &= -\log|\theta_1||\theta_2| \approx -\deg g \log n.
\end{aligned}$$

(These approximations are accurate to $o(\log n)$.) The polynomial regulator R_P is

$$R_P = \left\| \begin{matrix} \log|\theta_1| & \log|\theta_2| \\ \log|\theta_2| & \log|\theta_3| \end{matrix} \right\| \approx (7\deg^2 g - 5\deg g \deg f + \log^2 f)\log^2 n.$$

Using a result of Cusick [4], we can bound R_K, the regulator of $\mathcal{O}_{K_{f,g}}$, in terms of the discriminant $D(K_{f,g})$. If $3a+\lambda^2$ is squarefree, we can apply Theorem 2.3.1:

$$R_K \geq \frac{1}{16}\log^2\left(D(K_{f,g})/4\right) \approx (4\deg^2 g - 4\deg g\deg f + \deg^2 f)\log^2 n. \tag{2.6}$$

Take E_K to be the group of units of $K_{f,g}$ and E_P to be the subgroup of E_K generated by $\{\pm 1, \theta_1, \theta_2\}$ (and $\theta_3 = (\theta_1\theta_2)^{-1}$). For $\epsilon > 0$ and sufficiently large n,

$$[E_K : E_P] = \frac{R_P}{R_K} < \frac{7\deg^2 g - 5\deg g\deg f + \deg^2 f}{4\deg^2 g - 4\deg g \deg f + \deg^2 f} + \epsilon.$$

Set $\deg f = \rho \deg g$ for $0 \leq \rho < 1$; then for sufficiently small ϵ,

$$[E_K : E_P] < \frac{7 - 5\rho + \rho^2}{4 - 4\rho + \rho^2} + \epsilon < 3,$$

so $[E_K : E_P] = 1$ or 2. But the index must be a norm from $\mathbb{Z}[\omega]$ by [16, p. 412], so it can't be 2. We have proved:

Theorem 2.4.1. Let $K_{f,g}$ be as in Section 2.2. Assume that $\deg f < \deg g$, that $3a + \lambda^2$ is squarefree, and that n is sufficiently large. Then $\{\theta_1, \theta_2\}$ forms a system of fundamental units for $K_{f,g}$.

2.5 Examples

The machinery of the previous sections applies to all published families of cubic polynomials whose roots form systems of fundamental units. The data of these families are summarized in the following table.

Table 2.1: Previously-known one-parameter families.

	f	g	λ	$3a+\lambda^2$	Ref.
S_n	0	-1	n	n^2+3n+9	[13], [15]
L_n	-1	$-n$	$-n^2$	$(n^2+3)(n^2-3n+3)$	[8], [16]
K_n	$-n$	$-n^2-n-1$	$-n^3-2n^2-3n-3$	$n^6+o(n^6)$	[7]
K'_n	$-n$	n^3-1	$-n^5+2n^2$	$n^{10}+o(n^{10})$	[7]

Shanks's simplest cubic fields S_n are degenerate in multiple ways. Condition 2.2 gives $0/0$, but if we define λ to be any polynomial, the machinery works. We choose $\lambda = n$ since any other choice is a subparametrization of this one. The previous section's bound for the index $[E_K : E_P]$ also gives $0/0$, but (excellent) bounds for the regulator of S_n are given in [13].

The above table suggests that there might be a family with $f = -n^2$, and in fact there is. Take $(f, g) = (-n^2, n^3 - 1)$. Then $\lambda = n^3 - 4n$ and $P_{f,g}$ is

$$B_n = X^3 + (n^7 + 2n^6 + 3n^5 - n^4 - 3n^3 - 3n^2 + 3n + 3)X^2 + (-n^4 + 3n)X - 1.$$

Since $\deg f$ and $\deg g$ are coprime, B_n is not simply a subparametrization of S_n, L_n, or K_n. The discriminant is the square of

$$\sqrt{D_P} = (n^3 + n^2 - 1)(n^4 - 3n + 3)(n^4 + 3n^3 + 6n^2 + 6n + 3).$$

The first factor is $g - f$, and the product of the last two is $3a + \lambda^2$. By Theorem 2.3.1, whenever $3a + \lambda^2$ is squarefree,

$$D(B_n) = (n^4 - 3n + 3)^2(n^4 + 3n^3 + 6n^2 + 6n + 3)^2.$$

For $0 < n < 10^4$, it turns out that $3a + \lambda^2$ is squarefree 14.8% of the time. This is perfectly fine, but we can do better. Following the discussion after Theorem 2.3.1, we have an algorithm that completely determines $D(B_n)$. Write $3a + \lambda^2 = bc^3$ with b cubefree and take $p|(3a + \lambda^2)$. If $p = 3k + 2$, then p is unramified. For primes of the form $p = 3k+1$, we need to take special care only if $p|\text{res}(f^3 - 1, g^3 - 1) = -5^3$, which never happens. Therefore $p = 3k + 1$ ramifies iff $p|b$.

We can also deal with $p = 3$ (though admittedly in a more *ad hoc* manner). Straightforward calculations show that

$$3|D_P \iff v_3(3a + \lambda^2) > 0 \iff 3|n \iff v_3(3a + \lambda^2) = 2 \iff 3|b.$$

Thus 3 ramifies only if $3|b$. Conversely, writing out $B_{3k}(X+1)$ shows that it satisfies Eisenstein's criterion, so 3 ramifies if $3|b$. We have shown the following.

Theorem 2.5.1. Write $(n^4 - 3n + 3)(n^4 + 3n^3 + 6n^2 + 6n + 3) = bc^3$ with b cubefree. Then

$$D(B_n) = 81^\delta \prod_{p|b, p=3k+1} p^2,$$

where $\delta = 1$ if $3|b$ and $\delta = 0$ otherwise.

To bound the regulator, we have roots of order approximately n^7, n^{-4}, and n^{-3}. Numerical calculation shows that we get an index of less than 3 whenever $|n| > 4$, and computing the regulators of $K(B_n)$ for $|n| \leq 4$ individually by computer shows that we need only restrict to $n \neq -1$. (The roots of $B_{-1} = X^3 - 3X^2 - 4X - 1$ generate an index 3 subgroup of the full unit group. Since $3a + \lambda^2 = 7$ is squarefree, the restriction is in fact necessary.) We have shown the following.

Theorem 2.5.2. Let $n \in \mathbb{Z}$ with $n \neq -1$, and suppose $3a + \lambda^2$ is squarefree. Then $\{\pm 1, \theta_1, \theta_2\}$ generate the unit group of the ring of integers of $K(B_n)$.

For this theorem to be useful, we'd like to know that it gives units other than those produced by S_n, L_n, or K_n. Consider $B_2 = X^3 + 309X^2 - 10X - 1$. The regulator of $K(B_2)$ is approximately 24.733. Equation 2.6 tells us that we only need to check the regulators of $K(L_n)$ and $K(K_n)$ for $|n| < 10$. Shanks [13] computes that the regulator of $K(S_n)$ is $\log^2 |n| + o(1)$, which is greater than $K(B_2)$ for $|n| > 150$. Checking the regulators for small n in PARI/GP shows that the regulator of the units produced by B_2 is not a regulator produced by S_n, L_n, or K_n. Therefore, these units are new. (We are not claiming that the field $K(B_2)$ is necessarily distinct from $K(S_n), K(L_n)$, and $K(K_n)$ for all n, just that the units are new. It is possible that $K(B_2)$ is somehow isomorphic to one of these fields, but that the units produced there are not fundamental.)

At this point one might suspect that these families are abundant and go hunting for (f, g) with $f = -n^3$. As we've said before, Condition 2.2 implies that $g|(f^3 + 1)$. This limits the search considerably: a given f determines a finite list of possible g. For $f = -n^3$, the only potential candidates for g are $\pm(n-1), \pm(n^2 + n + 1)$, and $\pm(n^6 + n^3 + 1)$. Of these, the only pair satisfying Condition 2.2 is $(-n^3, -n^6 - n^3 - 1) = K_{n^3}$. Actually, an argument using the fac-

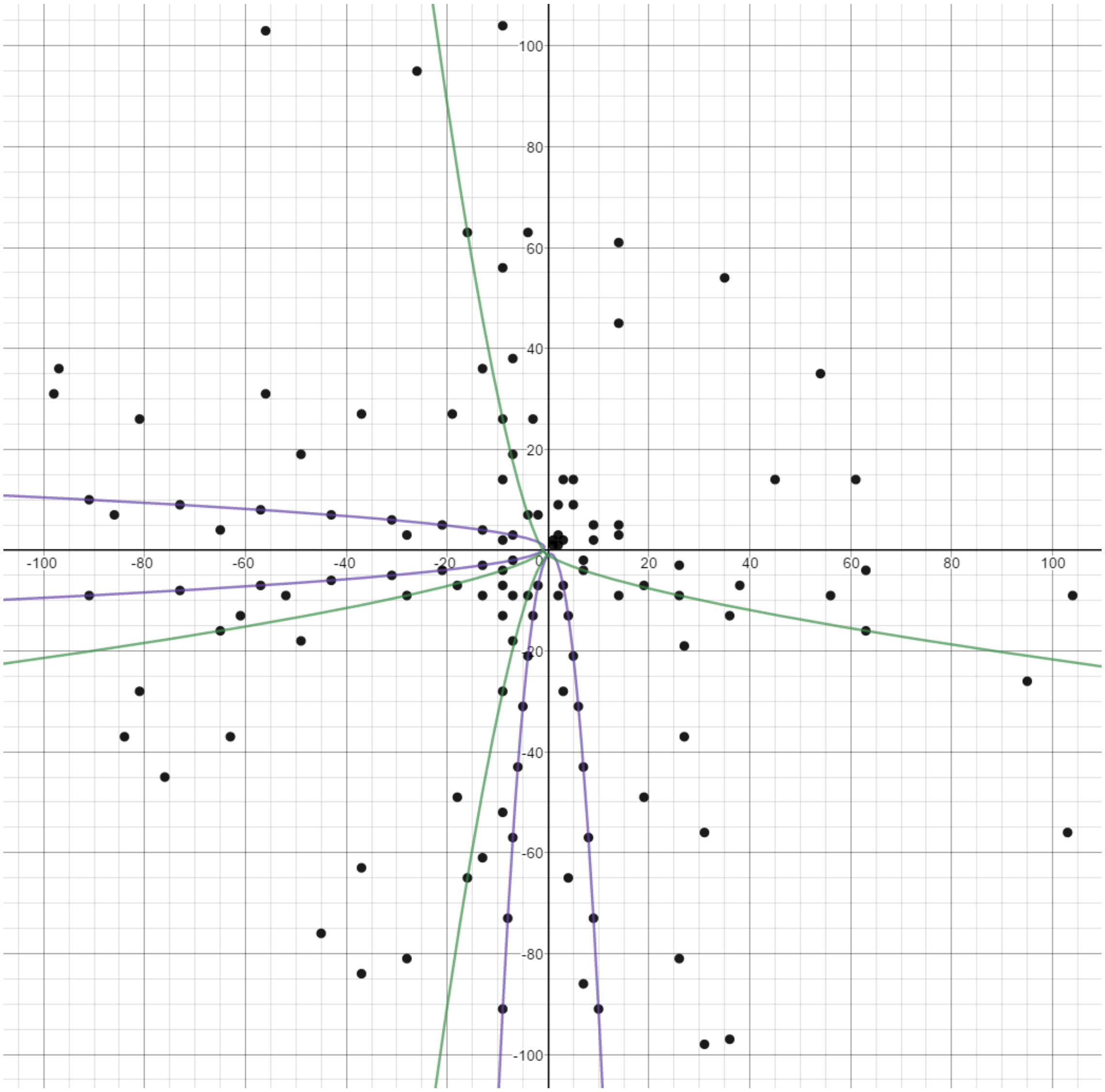

Figure 2.1: Integral points (x, y) on $X(3)$ satisfying Condition 2.2. Note the symmetry about $y = x$. Points on Lecacheux's family L_n are suppressed. The purple parabolas are Kishi's family K_n; the green twisted cubics are the family B_n.

torization of $n^{3k} \pm 1$ shows that this is always the case: if $k > 2$, any family of the form $(\pm n^k, g)$ is a subparametrization of the families K_n or $K'_n = (-n, n^3 - 1)$.

This raises the question of whether all families might be subparametrizations of some finite list. This isn't right either:

Theorem 2.5.3. Assume (f, g) satisfy Condition 2.2 and $f \neq 0$. Then (g, k), where $k = (g^3 + 1)/f$, also satisfy Condition 2.2. If $\deg f$ and $\deg g$ are coprime, then $\deg g$ and $\deg k$ are coprime.

Proof. A calculation shows that

$$\frac{g^3 + k^3 + 1}{gk} = \frac{f^3 + (g^3 + 1)^2}{f^2 g}.$$

Since $f | (g^3 + 1), g | (f^3 + 1)$, and f is coprime to g, we have $f^2 g | (f^3 + (g^3 + 1)^2)$. The second part of the theorem follows from the fact that $\deg k = 3 \deg g - \deg f$. □

We can apply Theorem 2.5.3 to L_n, K_n, or B_n repeatedly to produce any number of new families. Since the construction is asymmetric in f and g, we can also run it backwards by applying it to (g, f). For example, applying the construction forwards iteratively to B_n (more precisely, to $(f, g) = (-n^2, n^3 - 1)$) produces

$$(g, k_1) = (n^3 - 1, -n^7 + 3n^4 - 3n),$$

$$(k_1, k_2) = (-n^7 + 3n^4 - 3n, -n^{18} + o(n^{18})),$$

$$(k_2, k_3) = (-n^{18} + o(n^{18}), n^{47} + o(n^{47}), ...$$

(Incidentally the ratio $\deg g / \deg f$ approaches $\frac{3+\sqrt{5}}{2} = \phi + 1 = \phi^2$ as we iterate; this is true in general and a consequence of the degree calculation.) Running B_n

backwards gives B_{-n}. Running L_n backwards gives S_n (which has $f = 0$, so we stop there), while running it forwards gives K'_n and then new families. Running K_n backwards gives the family corresponding to $(-n, n-1)$ and then K_n again, while running it forwards gives new families. The families K'_n and $K_{-n,n-1}$ are discussed briefly in Kishi [7]; the rest, as far as I know, are all completely new. $K_{-n,n-1}$ is badly behaved; it has $\lambda = 3$ and always produces units of index 3 in the full unit group. (This does not contradict Theorem 2.4.1 since $\deg f = \deg g$.) Note that we claim only that the families themselves are new. I do not know whether these new families all produce new units, or even whether they all generate distinct fields.

We might ask if all families of cyclic cubic fields are of the form $P_{f,g}$ for the right choice of (f, g). Here the answer is also negative. For instance, plotting the pairs of (a, λ) for which the discriminant of $X^3 + aX^2 + \lambda X - 1$ is a square reveals (among other things) a parabola in the second quadrant. Computation shows that this is the family $X^3 + (-n^2 + 2n - 6)X^2 + (n^2 + 5)X - 1$. The Galois group is generated by the fractional linear transformation

$$\begin{bmatrix} n^2 - n + 1 & -(n^2 + n + 1) \\ n^2 - 3n + 3 & -2 \end{bmatrix},$$

which cannot possibly come from $f, g \in \mathbb{Z}[n]$. In the language of elliptic surfaces, this is the family $[n^2 - n + 1 : 2 : n^2 + n + 1;\ n^2 + 5]$ on the homogeneous coordinates for $X(3)$. As it happens, we know this family already. Begin with S_n, Shanks' simplest cubic fields. If we square the roots (which are units) we get another family S_n^2, and that family is the one above.

2.6 The Order $\mathbb{Z}[\theta_1, \theta_2]$

The referee of the paper [2] asked if Theorem 2.4.1 could be strengthened to the statement that $\{\theta_1, \theta_2\}$ generate the unit group of the order $\mathbb{Z}[\theta_1, \theta_2] \supset \mathbb{Z}[\theta_1]$. In fact, this is true:

Theorem 2.6.1. Assume (f, g) satisfy Condition 2.2, that $\deg f < \deg g$, and that n is sufficiently large. Then $\{\theta_1, \theta_2\}$ forms a system of fundamental units for the order $\mathbb{Z}[\theta_1, \theta_2]$.

Note that, unlike Theorem 2.4.1, this theorem does not make any assumptions on the discriminant of $\mathbb{Z}[\theta_1, \theta_2]$. The core difference is that knowing the discriminant of $K_{f,g}$ requires knowing which primes ramify, whereas the discriminant of $\mathbb{Z}[\theta_1, \theta_2]$ can be computed directly from the polynomial $P_{f,g}$.

The most technical part of the proof of Theorem 2.6.1 is the following:

Lemma 2.6.2. Assume (f, g) satisfy Condition 2.2. Then $[\mathbb{Z}[\theta_1, \theta_2] : \mathbb{Z}[\theta_1]] = |f(n) - g(n)|$.

The proof of the lemma is at the end of this section. Assuming it for the moment, we have

Corollary 2.6.3. The discriminant of $\mathbb{Z}[\theta_1, \theta_2]$ is $(3a + \lambda^2)^2$.

Proof. The discriminant of $\mathbb{Z}[\theta_1]$ is the polynomial discriminant $D_P = (f - g)^2(3a + \lambda^2)^2$. Since the ratio of order discriminants is the square of the index of the orders,

Lemma 2.6.2 implies that

$$D(\mathbb{Z}[\theta_1,\theta_2]) = \frac{D(\mathbb{Z}[\theta_1])}{[\mathbb{Z}[\theta_1,\theta_2]:\mathbb{Z}[\theta_1]]^2} = \frac{(f-g)^2(3a+\lambda^2)^2}{(f-g)^2} = (3a+\lambda^2)^2.$$

□

The regulator-discriminant bounds of Cusick [4] apply to any order (maximal or not). Therefore, by replacing Theorem 2.3.1 with Corollary 2.6.3 in Section 3, Theorem 2.6.1 is proved.

If $3a+\lambda^2$ happens to be squarefree, then $D(K_{f,g}) = D(\mathbb{Z}[\theta_1,\theta_2])$, so $\mathbb{Z}[\theta_1,\theta_2] = \mathcal{O}_K$. Thus Theorem 2.6.1 is a generalization of Theorem 2.4.1 – it shows that $\{\theta_1,\theta_2\}$ generates the group of units of some order, which may or may not be maximal.

Proof of Lemma 2.6.2. Denote by T_1 the matrix that represents θ_1 by its action on the basis $\{1,\theta_1,\theta_1^2\}$ – that is, the companion matrix for $P_{f,g}$ in this basis:

$$T_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & -\lambda \\ 0 & 1 & -a \end{bmatrix}.$$

Since we know the Galois action G, we can apply G to T_1 to obtain

$$T_2 = G(T_1) = (fT_1 - I_3)((f^2+g^2-fg)T_1 - gI_3)^{-1}.$$

The coefficients of the matrix T_2 are predictably messy, but they explicitly represent the action of θ_2 in terms of the basis $\{1,\theta_1,\theta_1^2\}$. In particular, the first column of T_2 gives the coefficients of θ_2 as a linear combination of $\{1,\theta_1,\theta_1^2\}$. Repeated use of

Condition 2.2 eventually tells us that

$$(f-g)\theta_2 = A + B\theta_1 + C\theta_1^2, \text{ where} \tag{2.7}$$

$$A = -af - 2,$$

$$B = \lambda - fg\lambda^2 + 3f^4 - 6gf^3 + 9g^2f^2 - 6g^3f + 3g^4 + g,$$

$$C = f^2 + g^2 - fg.$$

The explicit coefficients A, B, C are unenlightening, but all that matters for now is their integrality. If $p|(f-g)$, then $C \equiv g^2 \mod p$. But we already know that $f-g$ is coprime to g, so $f-g$ is coprime to C. Therefore, if M is the lattice

$$M = \mathbb{Z} + \mathbb{Z}\theta_1 + \mathbb{Z}\theta_1^2 + \mathbb{Z}\theta_2,$$

then $[M : \mathbb{Z}[\theta_1]] = |f-g|$ as lattices. To conclude the lemma, we need to show that $M = \mathbb{Z}[\theta_1, \theta_2]$. That is, we need to show that $\{\theta_2^2, \theta_1\theta_2, \theta_1^2\theta_2, \theta_1\theta_2^2, \theta_1^2\theta_2^2\} \subset M$.

Here's the argument for θ_2^2. When we write out (using PARI) the matrix T_2^2, we see once again that the first column (which represents the action of θ_2^2) becomes integral after clearing a denominator of $f-g$, so $(f-g)\theta_2^2 \in M$. Unfortunately, this only immediately tells us that $(f-g)^2|[M + \mathbb{Z}\theta_2^2 : \mathbb{Z}[\theta_1]]$, so we need to be more careful. Write

$$\theta_2^2 = \frac{1}{f-g}[A'(f,g) + B'(f,g)\theta_1 + C'(f,g)\theta_1^2],$$

where $A', B', C' \in \mathbb{Z}[f,g]$. Since $A'(f,g) \equiv A'(g,g) \mod (f-g)$, we can write

$$\theta_2^2 = m + \frac{1}{f-g}[A'(g,g) + B'(g,g)\theta_1 + C'(g,g)\theta_1^2]$$

for some $m \in M$. Evaluating A', B', and C' at $f = g$ and simplifying yields

$$\theta_2^2 - m = \frac{g^3+1}{f-g} \cdot [g^2 - (g^3+1)\theta_1 + g\theta_1^2].$$

A similar calculation, starting with (2.7), tells us that

$$\theta_2 - m_1 = \frac{g}{f-g} \cdot [g^2 - (g^3+1)\theta_1 + g\theta_1^2]$$

for some $m_1 \in M$. Combining the previous two equations,

$$g(\theta_2^2 - m) = (g^3+1)(\theta_2 - m_1),$$

so $g\theta_2^2 \in M$. Since $(f-g)\theta_2^2 \in M$ and g is coprime to $f-g$, we conclude that $\theta_2^2 \in M$. A similar argument works for each of the remaining generators of $\mathbb{Z}[\theta_1, \theta_2]$. □

Chapter 3: Calculations on $X(3)$

The goal of this chapter is to compute intersection data for families of curves on the elliptic surface $X(3)$. Each family described in Section 2.5 is a divisor on the surface, and therefore an element of the Néron-Severi group of divisors modulo algebraic equivalence. As such, understanding the various Néron-Severi classes gives an understanding how the families relate on $X(3)$. This chapter is intended to be read somewhat independently of the previous one, so some objects and arrows will be redefined as needed for readability.

3.1 The Néron-Severi Group

Our model is

$$\mu(x^3 + y^3 + z^3) = \lambda xyz, \tag{3.1}$$

where $[x : y : z; \lambda : \mu] \in P^2(\mathbb{C}) \times P^1(\mathbb{C})$ gives explicit coordinates for the fibration. We immediately drop the μ and write our coordinates as $[x : y : z; \lambda]$ on the surface

$$x^3 + y^3 + z^3 = \lambda xyz$$

with the understanding that $\lambda = \infty$ means that $[\mu : \lambda] = [0 : 1]$. The standard name for this projective surface is the Hesse pencil, and an elliptic curve in the form $x^3 + y^3 + 1 = \lambda xy$ is said to be in Hessian form. Schütt and Shioda [12] survey general results on elliptic surfaces, Beauville [3] first classified semi-stable elliptic surfaces with four singular fibers (including $X(3)$), and Artebani [1] surveys the geometry of the Hesse pencil. In the following theorems, we summarize the particular geometrical properties of $X(3)$ needed to compute intersection data. As a reminder, we fix a primitive cube root of unity $\omega = e^{2\pi i/3}$.

Theorem 3.1.1. The Hesse pencil (3.1) is a rational model for $X(3)$, the compactified modular curve of level 3. Said differently, the nonsingular fibers of the Hesse pencil parametrize elliptic curves with a chosen basis for their 3-torsion.

Proof. This is classical; see, for example, Miranda and Persson [10]. □

We fix the following notation:

$$\mathcal{O} = [-1 : 1 : 0; \lambda],$$

$$\mathcal{S} = [0 : -1 : 1; \lambda],$$

$$\mathcal{N} = [0 : -\omega : 1; \lambda].$$

Each of $\mathcal{O}$, $\mathcal{S}$, and $\mathcal{N}$ is a global section on $X(3)$. In the language of intersection theory, these are known as the horizontal divisors. We take $\mathcal{O}$ to be the origin of the group law on $X(3)$; explicit computations show that $\langle \mathcal{S} \rangle \oplus \langle \mathcal{N} \rangle \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$. In fact (see Artebani [1]) it turns out that this is the full Mordell-Weil group for $X(3)$, so we have the following 9 horizontal divisors:

$$\begin{array}{c|ccc} + & \mathcal{O} & \mathcal{S} & 2\mathcal{S} \\ \hline \mathcal{O} & [-1:1:0] & [0:-1:1] & [-1:0:1] \\ \mathcal{N} & [-1:\omega:0] & [0:-1:\omega] & [-1:0:\omega] \\ 2\mathcal{N} & [-1:\omega^2:0] & [0:-1:\omega^2] & [-1:0:\omega^2] \end{array} \tag{3.2}$$

Although we do not need it, the following gives another characterization of the global sections. (This would be useful for computing self-intersections.)

Theorem 3.1.2. The Hesse pencil has 9 base points given by the 9 global sections.

Proof. This follows the discussion in Example 3.2 of [12]: our model for $X(3)$ is exactly the cubic pencil formed from the homogeneous cubics $x^3 + y^3 + z^3$ and xyz. Explicitly, define a map $P^2 \to P^1$ by $[x : y : z] \mapsto [x^3 + y^3 + z^3 : xyz]$. This map is well-defined everywhere except when $x^3 + y^3 + z^3 = xyz = 0$. Setting $z = 0$ gives $x^3 = -y^3$; since $[x : y : z] \in P^2$, $x \neq 0$. When we deprojectivize by choosing $x = 1$ we get the singular points $[1 : -1 : 0], [1 : -\omega : 0]$, and $[1 : -\omega^2 : 0]$. The cases $x = 0$ and $y = 0$ follow by symmetry to give a total of 9 singular points. The Hesse pencil is therefore the blowup of P^2 in these nine points. □

Next, we analyze the vertical divisors – that is, the components of the singular fibers on $X(3)$.

Theorem 3.1.3. $X(3)$ has exactly four singular fibers: $\lambda = 3, 3\omega, 3\omega^2, \infty$. Each fiber has type I_3 in Kodaira's classification [12].

Proof. When $\lambda = \infty$, the Hesse pencil reduces to

$$0 = xyz.$$

This is a fiber of type I_3 – that is, a triangle of pairwise transverse lines intersecting at the sections $\mathcal{O}, \mathcal{S}$, and $2\mathcal{S}$.

Now assume $\lambda \in \mathbb{C}$ and the fiber $x^3 + y^3 + z^3 = \lambda xyz$ is singular. Consider the affine patch $[x : y : 1]$, on which the singular fibers will be given by the simultaneous vanishing of the partials. That is, we have

$$x^3 + y^3 + 1 = \lambda xy,$$

$$3x^2 = \lambda y,$$

$$3y^2 = \lambda x.$$

Solving for λ gives $\lambda^3 = 27$. Further, for each of these three values, the equation defining the curve factors:

$$0 = x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z),$$

$$0 = x^3 + y^3 + z^3 - 3\omega xyz = (x + y + \omega z)(x + \omega y + z)(x + \omega^2 y + \omega^2 z),$$

$$0 = x^3 + y^3 + z^3 - 3\omega^2 xyz = (x + y + \omega^2 z)(x + \omega y + \omega z)(x + \omega^2 y + z).$$

As with $\lambda = \infty$, each of these varieties is a triangle whose vertices are base points.

□

Again, for bookkeeping purposes, we give names to the twelve components of the singular fibers:

$$\begin{array}{r|l}
A_3 & \lambda = 3, \quad x + y + z = 0 \\
B_3 & \lambda = 3, \quad x + \omega y + \omega^2 z = 0 \\
C_3 & \lambda = 3, \quad x + \omega^2 y + \omega z = 0 \\
\hline
A_{3\omega} & \lambda = 3\omega, \quad x + y + \omega z = 0 \\
B_{3\omega} & \lambda = 3\omega, \quad x + \omega y + z = 0 \\
C_{3\omega} & \lambda = 3\omega, \quad x + \omega^2 y + \omega^2 z = 0 \\
\hline
A_{3\omega^2} & \lambda = 3\omega^2, \quad x + y + \omega^2 z = 0 \\
B_{3\omega^2} & \lambda = 3\omega^2, \quad x + \omega y + \omega z = 0 \\
C_{3\omega^2} & \lambda = 3\omega^2, \quad x + \omega^2 y + z = 0 \\
\hline
A_\infty & \lambda = \infty, \quad x = 0 \\
B_\infty & \lambda = \infty, \quad y = 0 \\
C_\infty & \lambda = \infty, \quad z = 0
\end{array} \tag{3.3}$$

We're almost ready to compute intersections. The following theorem tells us the work we need to do:

Theorem 3.1.4. The Néron-Severi lattice of $X(3)$ has rank 10. It is generated as a $\mathbb{Z}$-module by the divisor classes of $\mathcal{F}$, $\mathcal{O}$, and any pair of lines in each of the four singular fibers.

Proof. By Theorem 3.1.1, $X(3)$ is a rational elliptic surface. Section 8 of Schütt and Shioda [12] surveys results on the intersection theory of rational elliptic surfaces, from which this theorem follows. The sum of divisors given by adding the three lines of a singular triangle is clearly algebraically equivalent to $\mathcal{F}$, which explains why the third line is redundant. □

Corollary 3.1.5. Let D be a divisor on $X(3)$. Then the Néron-Severi class of D, written $NS(D)$, is determined by the following table of intersections:

	A_3	B_3	C_3	$A_{3\omega}$	$B_{3\omega}$	$C_{3\omega}$	$A_{3\omega^2}$	$B_{3\omega^2}$	$C_{3\omega^2}$	A_∞	B_∞	C_∞	$\mathcal{O}$	$\mathcal{F}$
D	–	–	–	–	–	–	–	–	–	–	–	–	–	–

where each empty space is the intersection of D with the fiber component in its column.

As written, $NS(D)$ is a vector in $\mathbb{Z}^{14}$, but Theorem 2.4 tells us that there are four redundancies:

$$\begin{aligned} D.\mathcal{F} &= D.A_3 + D.B_3 + D.C_3 \\ &= D.A_{3\omega} + D.B_{3\omega} + D.C_{3\omega} \\ &= D.A_{3\omega^2} + D.B_{3\omega^2} + D.C_{3\omega^2} \\ &= D.A_\infty + D.B_\infty + D.C_\infty. \end{aligned}$$

This is useful for checking for errors. Rather than making arbitrary choices, we'll give the full vector and understand that the Néron-Severi lattice is a 10-dimensional subspace of $\mathbb{Z}^{14}$.

Finally, each family of cyclic cubic fields defined in the previous chapter determines and is determined by a divisor on $X(3)$. First, we have the following named families, each of which have roots that give the full unit group under mild conditions.

$$S = [0 : -1 : 1;\ n]$$

$$L = [-1 : -n : 1;\ -n^2]$$

$$K = [-n : -n^2 - n - 1 : 1;\ -n^3 - 2n^2 - 3n - 3]$$

$$B = [-n^2 : n^3 - 1 : 1;\ -n^4 + 3n]$$

Given a family on F whose associated cubic polynomial is $(x-\theta_1)(x-\theta_2)(x-\theta_3)$, we can generate infinitely many curves on $X(3)$ by setting F^k to be the family associated with $(x-\theta_1^k)(x-\theta_2^k)(x-\theta_3^k)$. The roots of F multiply to 1, so this process does in fact generate a family. By construction these are new curves that generate finite-index subgroups of the unit group of F. Unlike F, they're not guaranteed to be cut out by polynomials on the affine patch $z = 1$. Here are some of these, explicitly:

$$S^2 = [n^2 + 3n + 3 : 2 : n^2 + n + 1; n^2 + 2n + 6]$$

$$S^3 = [9 : -n^4 - 6n^3 - 18n^2 - 27n - 18 : n^4 + 3n^3 + 9n^2 + 9n + 9; n^3 + 3n^2 + 9n + 3]$$

$$L^2 = [n^2 - n + 3 : n^4 - n^3 + 3n^2 - 2n + 2 : n^2 + n + 1; n^4 - 2n^3 + 4n^2 - 6n + 6].$$

(Not surprisingly, the coefficients grow quickly and are pretty unenlightening.)

We also have the trick that given a family $[f : g : 1]$ on $X(3)$, we get another family $[g : (g^3 + 1)/f : 1]$. This gives rise to the following families:

$$L' = [-n : n^3 - 1 : 1; -n^5 + 2n^2]$$

$$K' = [-n^2 - n - 1 : n^5 + 3n^4 + 6n^3 + 7n^2 + 6n + 3 : 1; -n^8 + ...]$$

With all this in place, we're ready to compute intersections. We illustrate the process with the following extended calculation:

Theorem 3.1.6. $NS(K)$ is determined by the following data:

	A_3	B_3	C_3	$A_{3\omega}$	$B_{3\omega}$	$C_{3\omega}$	$A_{3\omega^2}$	$B_{3\omega^2}$	$C_{3\omega^2}$	A_∞	B_∞	C_∞	$\mathcal{O}$	$\mathcal{F}$
K	1	1	1	1	2	0	1	0	2	2	0	1	0	3

Proof. In homogeneous coordinates on $X(3)$,

$$K = [x : y : z; \lambda] = [-n : -n^2 - n - 1 : 1;\ -n^3 - 2n^2 - 3n - 3].$$

Because $\deg \lambda = 3$, a fiber in general position intersects K transversely at 3 different points, so $K.\mathcal{F} = 3$. Also, K can only possibly intersect $\mathcal{O}$ when $n = \infty$, and evaluating at infinity (more on this in a bit) gives $[0 : -1 : 0] \neq [-1 : 1 : 0]$, so $K.\mathcal{O} = 0$.

Near $\lambda = 3$, $X(3)$ is a surface inside $\mathbb{C}^3$ with local coordinates $(x/z, y/z, \lambda)$. The λ-coordinate for K is $-n^3 - 2n^2 - 3n - 3$; $\lambda - 3 = (n+2)(n+\sqrt{-3})(n-\sqrt{-3})$. At $n = -2$, $K = [2 : -3 : 1;\ 3]$. This point is on the fiber component $x + y + z = 0$ and is not on the other two, so the contribution made by the intersection of K with the fiber $\lambda = 3$ at $n = -2$ is $[k, 0, 0]$ where $k \geq 1$ is yet to be determined. Evaluating at $n = \pm\sqrt{-3}$ gives intersections with the other two fibers, so $K.\mathcal{F} = 3$ implies that we must have intersection data $[1, 1, 1]$ at $\lambda = 3$.

This last step illustrates a general phenomenon: if $\lambda - 3$ has no repeated roots, K is not parallel to the surface $\lambda = 3$ (here thought of as living in affine complex

3-space) at any of its intersections with the fiber. Since each of the fiber components certainly is parallel to this surface, we must have that each point of intersection is transverse and thus contributes exactly 1 to the total intersection number. This seems to be a common phenomenon in practice and is quickly checked with the resultant of $\lambda - 3$ and its derivative (that is, the discriminant of $\lambda - 3$). The same is true of $\lambda - 3\omega$ and $\lambda - 3\omega^2$, neither of which have repeated roots.

We still have to check $\lambda = \infty$. Setting $n = 1/t$ and homogenizing λ to $[\lambda : \mu]$ gives local parameter $\mu = 1/\lambda = t^3/(-3t^3 - 3t^2 - 2t - 1)$, which vanishes to order 3 at $t = 0$. This means that we'll actually need to worry about higher tangencies. Near infinity, $K = [-t : -t^2 - t - 1 : t^2;\ t^3/(-3t^3 - 3t^2 - 2t - 1)]$. At $t = 0$ this is $[0 : 1 : 0;\ 0]$, so K intersects both the x- and z-axes. This means that we don't have a choice of coordinates for affine space: we must use $(x/y, z/y, \mu) = (-t/(-t^2 - t - 1), t^2/(-t^2 - t - 1), \mu)$. In this system, the tangent vector to K at $t = 0$ is $(1, 0, 0)$. Since this is parallel to the x-axis and transverse to the z-axis, we must have intersection data $[k, 0, 1]$ for $k > 1$. Again, the total intersection must be 3, so we conclude that $k = 2$. If we didn't have this piece of data, we could compute k directly by expanding the parameters in a Taylor series: $K = (t - t^2 + O(t^3), -t^2 + O(t^3), -t^3 + O(t^4))$. □

Similar calculations yield the following intersection data:

Table 3.1: Intersection data for known families.

	A_3	B_3	C_3	$A_{3\omega}$	$B_{3\omega}$	$C_{3\omega}$	$A_{3\omega^2}$	$B_{3\omega^2}$	$C_{3\omega^2}$	A_∞	B_∞	C_∞	$\mathcal{O}$	$\mathcal{F}$
S	1	0	0	0	0	1	0	1	0	1	0	0	0	1
L	0	1	1	1	0	1	1	1	0	1	0	1	0	2
K	1	1	1	1	2	0	1	0	2	2	0	1	0	3
B	0	2	2	2	2	0	2	0	2	3	0	1	0	4
L'	1	2	2	2	2	1	2	1	2	2	0	3	0	5

Some obvious symmetries appear in the table. This is a consequence of the fact that none of our families involve complex coefficients:

Theorem 3.1.7. Let F be a divisor on $X(3)$ defined over $\mathbb{R}$. Then

$$F.A_{3\omega} = F.A_{3\omega^2}$$

$$F.B_{3\omega} = F.C_{3\omega^2}$$

$$F.C_{3\omega} = F.B_{3\omega^2}$$

Proof. Each pair of fibers is permuted by complex conjugation. □

Theorem 3.1.8. The families S^n generate a subgroup of rank at least 6 in the Néron-Severi group of $X(3)$.

Proof. The following table of $NS(S^n)$ shows explicitly that the rank of their span is at least 6.

□

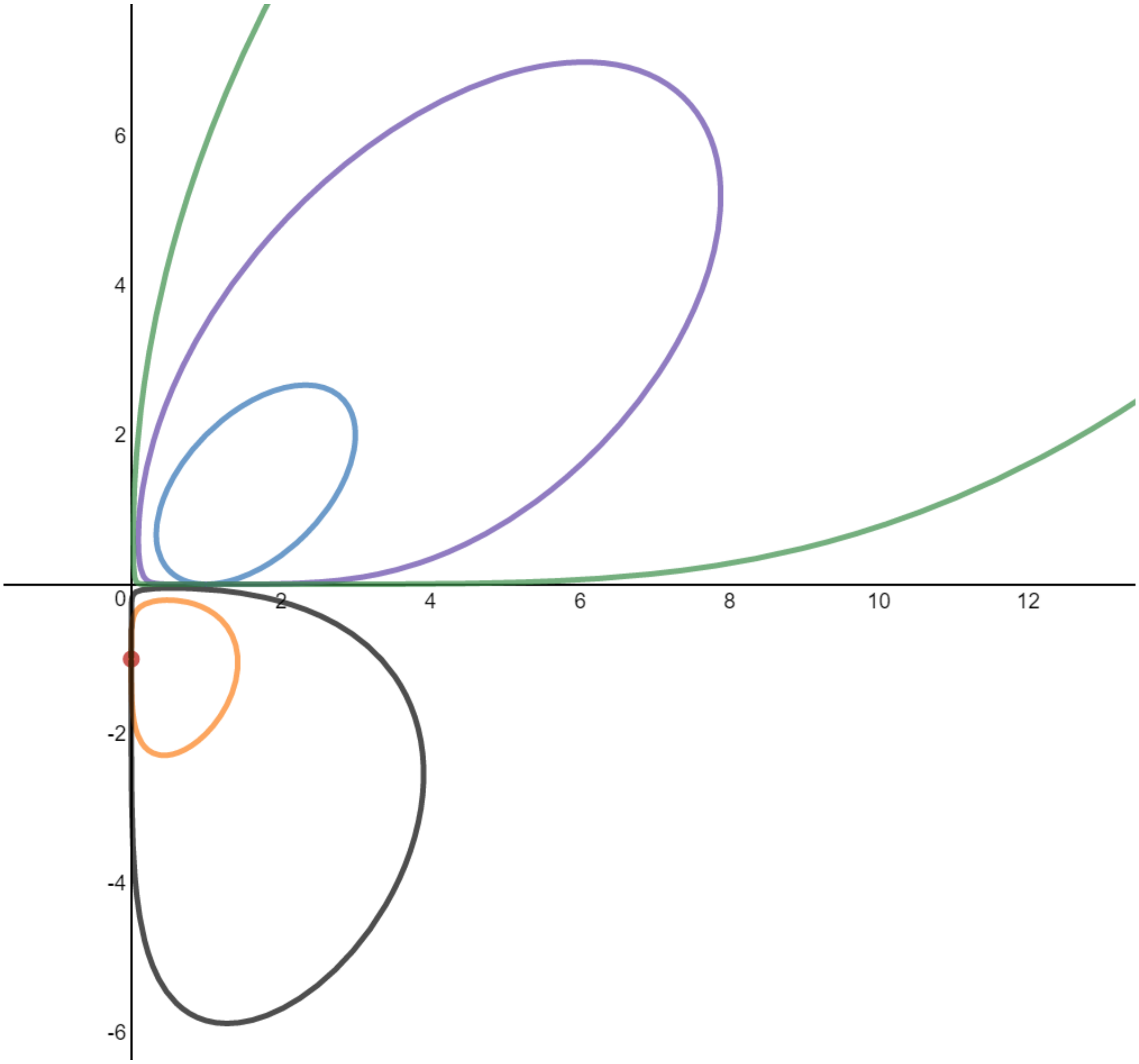

Figure 3.1: Successive powers of Shanks on the affine patch $z = 1$, graphed in red, blue, orange, purple, black, and green. Note that $(1, 0)$ is not a point on $X(3)$ on this affine patch: S^{2n} meets the y-axis at $\lambda = \infty$.

Table 3.2: Intersection data for powers of Shanks's family.

	A_3	B_3	C_3	$A_{3\omega}$	$B_{3\omega}$	$C_{3\omega}$	$A_{3\omega^2}$	$B_{3\omega^2}$	$C_{3\omega^2}$	A_∞	B_∞	C_∞	$\mathcal{O}$	$\mathcal{F}$
S	1	0	0	0	0	1	0	1	0	1	0	0	0	1
S^2	2	0	0	1	0	1	1	1	0	0	2	0	0	2
S^3	1	1	1	3	0	0	3	0	0	3	0	0	0	3
S^4	4	0	0	3	1	0	3	0	1	0	4	0	0	4
S^5	5	0	0	4	1	0	4	0	1	5	0	0	0	5
S^6	4	1	1	6	0	0	6	0	0	0	6	0	0	6

Conjecture. Based on our calculations for powers of Shanks's family, we conjecture the following general formula. This is only conjectural and the explicit algebraic equivalencies implied by this formula is a topic of future research. If the conjecture is true, one consequence will be that the powers of Shanks generate a subgroup of the Néron-Severi group of rank exactly 6.

	A_3	B_3	C_3	$A_{3\omega}$	$B_{3\omega}$	$C_{3\omega}$	$A_{3\omega^2}$	$B_{3\omega^2}$	$C_{3\omega^2}$	$\mathcal{O}$	$\mathcal{F}$
S^{3n}	$3n-2$	1	1	$3n$	0	0	$3n$	0	0	0	$3n$
S^{3n+1}	$3n+1$	0	0	$3n$	1	0	$3n$	0	1	0	$3n+1$
S^{3n+2}	$3n+2$	0	0	$3n+1$	0	1	$3n+1$	1	0	0	$3n+2$

	A_∞	B_∞	C_∞
S^{2n}	0	$2n$	0
S^{2n+1}	$2n+1$	0	0

3.2 Tripling on the Hesse pencil

In this section we prove an unpublished remark of Washington which was noticed during computations: "The map from cyclic cubic polynomials to the points on the elliptic surface W has an inverse that can be described as follows. Let $P_W = (x, y, \lambda)$ be a rational point on W. Consider the field generated over $\mathbb{Q}$ by $\sqrt{-3}$ and the coordinates of $\frac{1}{3}P_W$. Often, this will contain a unique cyclic extension of $\mathbb{Q}$. This will correspond to the original polynomial. More precisely, let $x_1, ..., x_9$ be the x-coordinates of the various choices of $P_W/3$. Then $(x_1+x_2+x_3)/(-9)$, under a suitable numbering (corresponding to $P_W/3$ and its translates by plus/minus the nonrational 3-torsion point above) seems to satisfy the original cubic polynomial." (Notation has been changed from the original remark to match this work's conventions.)

Rather than computing $\frac{1}{3}P_W$ on the Weierstrass form, we exploit the group structure of $X(3)$ to vastly simplify calculations.

Theorem 3.2.1. Let $[f, g] = [f : g : 1; \lambda]$ on $X(3)$. Then

$$\begin{aligned} 3[f, g] = [&-f^3g^6 + (3f^3 - 1)g^3 - f^6 : \\ &- g^6 + (-f^6 + 3f^3)g^3 - f^3 : \\ &fg(-g^6 - f^6 + f^3g^3 + g^3 + f^3 - 1)], \end{aligned}$$

where $3[f, g]$ represents tripling via the group law on $X(3)$.

Proof. A calculation with the usual chord-and-tangent formula for addition of points on $X(3)$ tells us that

$$2[f : g : 1] = [g(f^3 - 1) : f(g^3 - 1) : g^3 - f^3].$$

Adding this to $[f : g : 1]$ gives the conclusion. Expressions for the full group law on $X(3)$ are worked out in [6] using slightly different methods. □

Corollary 3.2.2. Let $[f, g] \in X(3)$. Then

$$P_{3[f,g]} = (x - fg)(x - f/g^2)(x - g/f^2).$$

Proof. This is a direct computation using the previous theorem and the birational transformation. □

This is enough to prove Washington's remark. We need the following table:

$+$	$\mathcal{O}$	$\mathcal{S}$	$2\mathcal{S}$
$\mathcal{O}$	$[f : g : 1]$	$[g/f : 1/f : 1]$	$[1/g : f/g : 1]$
$\mathcal{N}$	$[\omega f : \omega^2 g : 1]$	$[\omega g/f : \omega^2/f : 1]$	$[\omega/g : \omega^2 f/g : 1]$
$2\mathcal{N}$	$[\omega^2 f : \omega g : 1]$	$[\omega^2 g/f : \omega/f : 1]$	$[\omega^2/g : \omega f/g : 1]$

(3.4)

An element in the following table is $[f : g : 1]$ plus the section in its row plus the section in its column – for example, $[f : g : 1] + \mathcal{O} + \mathcal{N} = [\omega f : \omega^2 g : 1]$.

We begin with a polynomial factored over $\mathbb{C}$:

$$h(x) = (x - r)(x - s)(x - t).$$

Assume that $h(x)$ defines a point on the elliptic surface W – that is, $rst = 1$ and $h(x)$ generates a cyclic cubic field. Then $h(x)$ determines a point P on $X(3)$. Now we define f and g implicitly by the equations

$$fg = r$$

$$f/g^2 = s.$$

By construction, $3[f, g] = P$. The ambiguity in our choice of f and g is annihilated by the 3-torsion on $X(3)$. That is, the nine points on $X(3)$ which triple to the point P on $X(3)$ are exactly those in the previous table, so we have found all nine values of $\frac{1}{3}P$ explicitly. Each of these nine points then determines a point (x_{ij}, y_{ij}) on the Weierstrass model W via the birational transformation. A calculation in PARI/GP shows that adding x_{ij} down each column in the table gives $-9r, -9s, -9t$. This proves the conjecture.

We illustrate this process with a worked example. Consider

$$B_2(x) = x^3 + 309x^2 - 10x - 1,$$

which corresponds to the point $(309, 11297)$ on the Weierstrass form of the elliptic surface and the point $P = (-4, 7)$ on $X(3)$. (Note that $\lambda = -10$ on both surfaces, though we do not need this.) The roots of B_2 are -309.0324, 0.0753, and 0.0430. Solving for f and g gives $(-16.0094, 19.3031)$ (and its eight conjugates in the table above); this is $\frac{1}{3}P$. The x-coordinates of those nine points in Weierstrass form and their sums follow:

$2846.7739 + 0.000i$	$-8.5348 + 0.000i$	$-5.5751 + 0.000i$
$-32.7414 - 3.6350i$	$3.9285 - 13.6680i$	$2.9809 + 9.4113i$
$-32.7414 + 3.6350i$	$3.9285 + 13.6680i$	$2.9809 - 9.4113i$
2781.2911	-0.6778	0.3867

Dividing the last line by -9 gives the three roots of B_2.

Appendix A: PARI/GP Script

Many of the calculations in this dissertation would have been impossible (at least for the author) without the following PARI/GP script. The functions have been checked thoroughly for accuracy and I strongly recommend that any computations confirming or extending the results of this work begin with this .gp file.

```
/*␣Steve␣Balady␣*/
/*␣May␣2017␣*/
/*␣PARI/GP␣script␣for␣calculations␣on␣X(3)␣*/

/*␣definitions␣of␣the␣Hesse␣pencil␣X(3)␣*/
/*␣and␣the␣coordinates␣of␣the␣Weierstrass␣form␣W␣*/
w␣=␣exp(2*Pi*I/3);

XH␣=␣x^3+y^3+z^3-L*x*y*z;
X␣=␣subst(XH,z,1);
XW␣=␣-y^2␣+␣4*x^3␣+␣L^2*x^2␣-␣18*L*x␣+␣(-4*L^3␣-␣27);

Aw␣=␣-(a^4+b^4+(a-b)^4+2*a+2*b)/2/a/b;
Bw␣=␣(-b^7␣+␣4*a*b^6␣-␣9*a^2*b^5␣+␣(13*a^3␣-␣2)*b^4
+␣(-13*a^4␣+␣5*a)*b^3␣+␣9*a^5*b^2
+␣(-4*a^6␣-␣5*a^3␣-␣1)*b␣+␣(a^7␣+␣2*a^4␣+␣a))/(a^2*b^2);
/*␣Note:␣Bw␣factors␣completely␣into␣linear␣*/
/*␣and␣quadratic␣terms␣of␣multiplicity␣1␣*/
Lw␣=␣(a^3+b^3+1)/a/b;

/*␣the␣birational␣map:␣toFamily:␣X(3)␣\to␣W,␣toX:␣W␣\to␣X(3)␣*/
ToW␣=␣[-L^2,-L^2,-9;L^3-27,-(L^3-27),0;3,3,L];␣/*␣L␣=␣\lambda␣*/
ToX␣=␣[-L,1,-9;-L,-1,-9;6,0,2*L^2];

toFamily(V)␣=␣{
local(A,L);
A␣=␣subst(subst(Aw,a,V[1]),b,V[2]);L=subst(subst(Lw,a,V[1]),b,V[2]);
return(x^3+A*x^2+L*x-1);
}

toX(f)␣=␣{
local(aa,bb,ll,XX,yy);
aa␣=␣polcoeff(f,2);
ll␣=␣polcoeff(f,1);
XX␣=␣subst(ToX,L,ll);
bb␣=␣truncate(sqrt(poldisc(f)));
yy␣=␣ToX*[aa;bb;1];
yy␣=␣subst(yy,L,ll);
yy␣=␣yy/yy[3,1];
yy␣=␣yy*denominator(yy[1,1]);
return([yy[1,1],yy[2,1],yy[3,1]]);
}

/*␣doubling␣on␣the␣affine␣patch␣z=1␣*/
a2=b*(a^3-1)/(b^3-a^3);
b2=-a*(b^3-1)/(b^3-a^3);

/*␣tripling␣on␣z=1␣*/
a3␣=␣-a^3*b^6+(3*a^3-1)*b^3-a^6;
b3␣=␣-b^6+(-a^6+3*a^3)*b^3-a^3;
c3␣=␣a*b*(-b^6-a^6+a^3*b^3+b^3+a^3-1);

/*␣known␣families␣*/
S␣=␣[0,-1];
LL␣=␣[-1,-n];
K␣=␣[-n,-n^2-n-1];
B␣=␣[-n^2,n^3-1];
B56␣=␣[-n^5-n^4-3*n^3-2*n^2-2*n,␣-n^6-n^5-4*n^4-2*n^3-4*n^2-1];
Sfam␣=␣x^3␣+(n+3)*x^2+n*x-1;␣/*␣toFamily␣degenerates␣on␣S␣*/

/*␣generating␣new␣families␣*/
fgtrick(V)␣=␣{[V[2],(V[2]^3+1)/V[1]]};
unitpow(f,n)␣=␣minpoly(matcompanion(f)^n);
fampow(V,n)␣=␣toX(unitpow(toFamily(V),n));

/*components␣of␣the␣singular␣fibers␣on␣X(3)␣*/
t1␣=␣[1,1,1];
t2␣=␣[1,w,w^2];
t3␣=␣[1,w^2,w];
tw1␣=␣[1,1,w];
tw2␣=␣[1,w,1];
```

```
tw3␣=␣[1,w^2,w^2];
tww1␣=␣[1,1,w^2];
tww2␣=␣[1,w,w];
tww3␣=␣[1,w^2,1];
inf1␣=␣[0,-1,1];
inf2␣=␣[-1,0,1];
inf3␣=␣[-1,1,0];
```

Bibliography

[1] Michela Artebani and Igor Dolgachev. The Hesse pencil of plane cubic curves. *Enseign. Math. (2)*, 55(3-4):235–273, 2009.

[2] Steve Balady. Families of cyclic cubic fields. *J. Number Theory*, 167:394–406, 2016.

[3] Arnaud Beauville. Les familles stables de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(19):657–660, 1982.

[4] T. W. Cusick. Lower bounds for regulators. In *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, volume 1068 of *Lecture Notes in Math.*, pages 63–73. Springer, Berlin, 1984.

[5] Günter Degert. über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper. *Abh. Math. Sem. Univ. Hamburg*, 22:92–97, 1958.

[6] Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In *Cryptographic hardware and embedded systems—CHES 2001 (Paris)*, volume 2162 of *Lecture Notes in Comput. Sci.*, pages 402–410. Springer, Berlin, 2001.

[7] Yasuhiro Kishi. A family of cyclic cubic polynomials whose roots are systems of fundamental units. *J. Number Theory*, 102(1):90–106, 2003.

[8] Odile Lecacheux. Units in number fields and elliptic curves. In *Advances in number theory (Kingston, ON, 1991)*, Oxford Sci. Publ., pages 293–301. Oxford Univ. Press, New York, 1993.

[9] Günter Lettl. A lower bound for the class number of certain cubic number fields. *Math. Comp.*, 46(174):659–666, 1986.

[10] Rick Miranda and Ulf Persson. On extremal rational elliptic surfaces. *Math. Z.*, 193(4):537–558, 1986.

[11] R. A. Mollin and H. C. Williams. Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception). In *Number theory (Banff, AB, 1988)*, pages 417–425. de Gruyter, Berlin, 1990.

[12] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[13] Daniel Shanks. The simplest cubic fields. *Math. Comp.*, 28:1137–1152, 1974.

[14] The PARI Group, Bordeaux. *PARI/GP version* `2.7.3`, 2015. http://pari.math.u-bordeaux.fr/.

[15] Lawrence C. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48(177):371–384, 1987.

[16] Lawrence C. Washington. A family of cubic fields and zeros of 3-adic L-functions. *J. Number Theory*, 63(2):408–417, 1997.