Resolution of Singularities on Elkies' Models of Towers of Modular Curves

David Marcil

Summer 2017

Contents

Introduction

This document serves as an introduction to modular curves. Its main goal is to study some explicit modular curves of the form $X_0(N)$. One may skip some of the definitions and focus on the specific examples, coming back to the theory later if needed. Although, a proper introduction to algebraic geometry is probably necessary to understand some concepts not introduced here.

In 2001, Elkies published a paper (see [E]) giving many explicit models of modular curves, and we aim to understanding their stucture as much as possible.

In Chapter 1, we first introduce the notion of elliptic curves as algebraic varieties. They are central objects of modern algebra and we discuss their importance by looking at their behavior over $\mathbb{Q}$. Their classification naturally leads to new algebraic varieties, called modular curves. The main examples we will consider are modular curves $X_0(N)$, for integers $N \geq 1$. This section can easily be omitted for more advanced readers.

In Chapter 2, we take a look at Elkies' paper in greater detail. Some specific notions on the theory of modular curve are first introduced to better understand Elkies' proposition. Then, the construction of the first two models given in [E] are presented. We discuss a few of their notable properties.

In Chapter 3, the notion of resolution of singularities of an algebraic curve is introduced. Since Elkies' models reveal themselves to be singular, we familiarize ourselves with the idea of finding the smooth model of a curve. We consider a few examples to learn various techniques and build up our intuition.

In Chapter 4, we finally attack our main problem. We look exclusively at the modular tower $X_0(3^n)$ given by Elkies. We resolve the singularities of the curves in Elkies' model for this tower. This leads to a surprising link between modular curves and Fermat curves. Then, we end this document by looking at maps between curves in this tower to find a general formula for the genus of $X_0(3^n)$.

Acknowledgments
I would like to thank Dr. Jan Vonk and Prof. Eyal Goren, my supervisors in this project, for the time they devoted to help me both in my research and in the redaction of this paper, and to answer all of my unceasing questions. Furthermore, as a recipient of a SURA scholarship, I also want to thank Prof. Goren and McGill University for their financial support.

Chapter 1

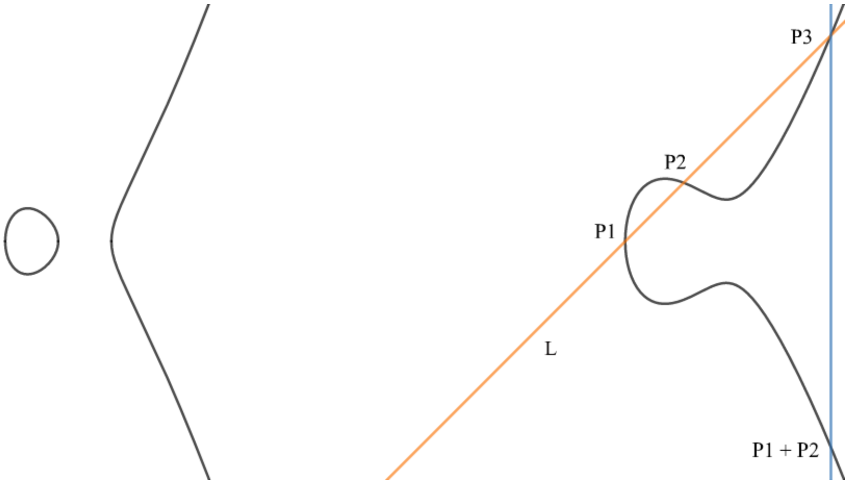
Construction of Modular Curves

1.1 Complex Elliptic Curves

In algebraic geometry, an *elliptic curve* is a projective plane curve $E : y^2 = 4x^3 + ax + b$ in $\mathbb{P}^2(\mathbb{C})$, some $a, b \in \mathbb{C}$, for which $4a^3 + 27b^2 \neq 0$. This is simply the condition for this curve to be nonsingular. Let's first study the case when $a, b \in \mathbb{Q}$, in which case we say that E is defined over $\mathbb{Q}$. In general, if $a, b \in K$, some field K, we say that E is defined over K, and write $E(K)$ for the set of all its points defined over K.

Before explaining their relation with complex tori, let us simply show a bit of their behavior over the rational numbers, to see the interest they generate in algebra. Firstly, observe that by homogenizing the polynomial for E, one obtains $y^2z = 4x^3 + axz^2 + bz^3$. Then, we see that these curves have only one point at infinity, i.e. $\mathcal{O} = [0 : 1 : 0] \in E(\mathbb{Q})$. Furthermore, elliptic curves are given by a polynomial of degree 3, hence they have genus 1. In fact, one can show that any curve of genus one over $\mathbb{C}$ can be described by such a polynomial equation. Thus, one can equivalently define elliptic curves as any genus one curves over $\mathbb{C}$.

The solution space $E(\mathbb{R})$ of an elliptic curve E over $\mathbb{R}$ always looks like one of these two curves. The important fact here is that one can define a group structure on E.



Remark 1.1.1. The colored lines here demonstrate how to add two points on E.

Let $L : Ax + By = D$ be a line passing through two distinct rational points $P_i = (x_i, y_i) \in E(\mathbb{Q})$. We can assume that $A, B, D \in \mathbb{Q}$. Using Bézout theorem, we know L and E both intersect at three points, counting multiplicities.

If P_1 and P_2 are vertically aligned, we know this third intersection point is $P_3 = \mathcal{O}$. In this case, we define $P_1 \oplus P_2 = \mathcal{O}$. Otherwise, we can rewrite $L : y = mx + c$, with $m, c \in \mathbb{Q}$. Then, we have

$$4x^3 + ax + b - (mx + c)^2 = 4(x - x_1)(x - x_2)(x - x_3) \text{ , some } x_3 \in \mathbb{C}$$

Since E is defined over $\mathbb{Q}$ and the coefficient of x^2 is $-4(x_1 + x_2 + x_3)$, we must have $x_3 \in \mathbb{Q}$. Hence, our third intersection is $P_3 = (x_3, y_3)$, for $y_3 = mx_3 + c$, again a rational point. In this case we define $P_1 \oplus P_2 = (x_3, -y_3)$. In both scenario, we can see $P_1 \oplus P_2$ as the reflection of P_3 w.r.t. the x-axis (which sends $\mathcal{O}$ back to itself). Above we assume that P_1 and P_2 were distinct, but if $P_1 = P_2$, one simply picks L to be the tangent of E at P_1.

Then, one readily sees that the identity element is $\mathcal{O}$. For any $P = (x, y) \in E(\mathbb{Q})$, the line passing through P that intersect E at infinity must be vertical. Thus, the third intersection point is $(x, -y)$, and so $P \oplus \mathcal{O} = \mathcal{O} \oplus P = (x, y) = P$. This also shows that the inverse of $P = (x, y)$ is $-P = (x, -y)$. As we have just seen, this operation is closed in $E(\mathbb{Q})$, and the fact that this operation is abelian is trivial. Its associativity is much more challenging; nonetheless provable.

In the 1920s, Mordell's Theorem showed that for any elliptic curve E, $E(\mathbb{Q})$ is finitely generated. This implies that $E(\mathbb{Q})$ is always of the form

$$E(\mathbb{Q}) = T \times \mathbb{Z}^r$$

where T is a finite group, called the *torsion group* of E, and r is the *rank* of E. The torsion group is very well understood, thanks to Mazur's theorem. The rank however still has many secrets. The BSD conjecture attempts to predict the behavior of the rank of E by looking at the L-function attached to E. Despite remarkable progress towards proving the BSD however, the rank remains very mysterious. It is actually still considered as one of the most difficult unsolved mathematical problem.

To unravel these mysteries, mathematicians tried to classify these elliptic curves to learn their global behavior; e.g. When is $E(\mathbb{Q})$ finite? When does $E(\mathbb{Q})$ contain a subgroup of order N? This is where the link between elliptic curves $E \subset \mathbb{P}^2$ and complex tori comes in. These two mathematical objects, as we'll soon see, are completely equivalent to one another. Their relation lies in terms of their function fields. Firstly, one needs to know what a complex torus is and see what are the function defined on it.

Definition 1.1.2. The *upper half complex plane* is a subset of $\mathbb{C}$ defined as

$$\mathcal{H} = \{ \ z \in \mathbb{C} \ : \ \Im(z) > 0 \ \}$$

Definition 1.1.3. A *lattice* in $\mathbb{C}$ is defined by two complex numbers $\omega_1, \omega_2 \in \mathbb{C}$ such that $\omega_1/\omega_2 \in \mathcal{H}$ as

$$\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z} = \{ \ m\omega_1 + n\omega_2 \ : \ m, n \in \mathbb{Z}^2 \ \}$$

Definition 1.1.4. Given a lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, we define a *complex torus* $\mathbb{C}/\Lambda$ as the quotient of $\mathbb{C}$ by Λ, denoted as

$$\mathbb{C}/\Lambda = \{ \ z + \Lambda \ : \ z \in \mathbb{C} \ \}$$

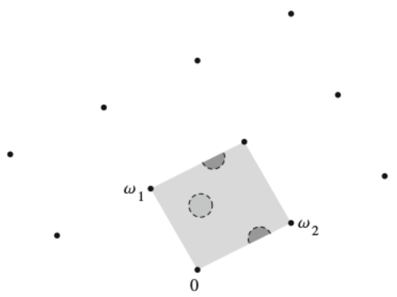


Figure 1.1: Image from [DS]

As the figure above suggests, the points in the rectangle form an appropriate set of representatives for $\mathbb{C}/\Lambda$. Then, opposite sides are equivalent (demonstrated by the circle cut in half), hence one can glue two of them together to obtain a tube, and do the same with the remaining two to obtain a torus.

Analytic functions on a complex torus $\mathbb{C}/\Lambda$ are simply Λ-periodic meromorphic functions, i.e. $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$, with $f(z + \Lambda) = f(z)$ for all $z \in \mathbb{C}$. The *Weierstrass $\wp$-function*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \tag{1.1}$$

and its derivative

$$\wp'_\Lambda(z) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3} \tag{1.2}$$

are two such functions, and their poles are exactly at $z \in \Lambda$. The study of these two functions alone is sufficient since one can prove that the field of meromorphic functions on $\mathbb{C}/\Lambda$ is exactly $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$. The notation $\wp_\Lambda$ serves to emphasize the dependence of the function on the choice of lattice.

Furthermore, for all $k > 2$ even, define the function $G_k : \{$ Lattices on $\mathbb{C}$ $\} \to \mathbb{C}$ as

$$G_k(\Lambda) = \sum_{w \in \Lambda \setminus \{0\}} \frac{1}{w^k} \ , \tag{1.3}$$

and show that this sum is always absolutely convergent.

Remark 1.1.5. If we restrict our choices to lattices of the form $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$, where $\Im(\tau) > 0$, this becomes

$$G_k : \mathcal{H} \to \mathbb{C} \text{ as } G_k(\tau) = \sum_{\substack{(c,d) \in \mathbb{Z}^2 \\ (c,d) \neq (0,0)}} \frac{1}{(c\tau + d)^k} \tag{1.4}$$

in which case this is called an *Eisenstein series.* As more advanced readers certainly know, such functions are exemples of *modular form of weight k and level 1.* For more on this subject, see [DS], chapter 1.

Proposition 1.1.6. *Let Λ be some lattice, and write $\wp$ and $\wp'$ for $\wp_\Lambda$ and $\wp'_\Lambda$. Then, these two functions on $\mathbb{C}$ satisfy the relation*

$$(\wp')^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda)$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$ are constants.

This shows that for the elliptic curve $E : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ (this variety is indeed nonsingular), we have a well-defined map

$$(\wp_\Lambda, \wp'_\Lambda) : \mathbb{C}/\Lambda \to E \text{ as } z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z)) \tag{1.5}$$

As both $\wp_\Lambda$, $\wp'_\Lambda$ have a unique pole at the origin, one takes its image as $(\wp_\Lambda(0), \wp'_\Lambda(0)) = \mathcal{O}$. Most importantly, we may show that $(\wp_\Lambda, \wp'_\Lambda)$ is a bijection between the points of $\mathbb{C}/\Lambda$ and the points of E. Furthermore, there is a converse to this statement.

Proposition 1.1.7. *Given an elliptic curve $E : y^2 = 4x^3 + ax + b$ defined over $\mathbb{C}$, then there exists a lattice Λ on $\mathbb{C}$ such that $a = -g_2(\Lambda)$ and $b = -g_3(\Lambda)$.*

All these results are proved in [DS], chapter 1. Therefore, one can completely interchange complex tori and algebraic elliptic curves. Then, to study the general structure of these special curves in $\mathbb{P}^2$, it is natural to classify them as complex tori, accordingly called *complex elliptic curves*, and construct *modular curves*, as we'll see in the following sections.

1.2 Modular Curve $X(1)$

Consider the set $S(1)$ of all isomorphism classes of complex elliptic curves. In this section, we see how the points of $S(1)$ are in canonical bijection with the complex points of a projective curve over $\mathbb{C}$, which we call $X(1)$. The points at infinity of $X(1)$, called *cusps*, will not correspond to points of $S(1)$ but are necessary to properly define $X(1)$ as an algebraic curve.

Let us first study the structure of $S(1)$, that is, describe what makes two complex tori isomorphic. Firstly, note that for a lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$, different choices of ω_i can generate the same lattice, hence the same complex torus. For instance, picking $\omega'_1 = \omega_2$ and $\omega'_2 = -\omega_1$ obviously generates the same lattice. Similarly, Λ can also be formed by $\omega'_1 = \omega_1 + \omega_2$ and $\omega'_2 = \omega_2$. One readily notices that these two change of basis correspond respectively to the following linear transformations

$$\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \text{ and } \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \tag{1.6}$$

These two matrices $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are generators of the set $\mathrm{SL}_2(\mathbb{Z})$ of 2×2 matrices over $\mathbb{Z}$ with determinant 1. Thus, this next result shows that the two change of basis above are, in some sense, the only ones.

Lemma 1.2.1. *Consider two lattices $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ and $\Lambda' = \omega'_1\mathbb{Z} \oplus \omega'_2\mathbb{Z}$, with both ω_1/ω_2, $\omega'_1/\omega'_2 \in \mathcal{H}$. Then, $\Lambda' = \Lambda$ if and only if*

$$\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \text{ , \textit{for some} } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

Proof. Two lattices are the same if and only if $\{\omega'_1, \omega'_2\} \in \Lambda$ and $\{\omega_1, \omega_2\} \in \Lambda'$. This is condition is satisfied exactly when there exists some $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

and that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible over $\mathbb{Z}$. Therefore, it has determinant ±1. But one can easily show that

$$\Im(\omega_1'/\omega_2') = \frac{(ad-bc)\cdot\Im(\omega_1/\omega_2)}{|c\omega_1+d\omega_2|^2}$$

It follows immediately that $\omega_1'/\omega_2' \in \mathcal{H}$ exactly when this determinant is 1, i.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. □

This characterizes the equality between two complex tori. Furthermore, skipping through quite a few definitions (see [DS], Corollary 1.3.3), one can show that two complex tori $\mathbb{C}/\mathit{\Lambda}$ and $\mathbb{C}/\mathit{\Lambda}'$ are isomorphic if and only if $\mathit{\Lambda}' = \alpha\mathit{\Lambda}$, for some $\alpha \in \mathbb{C}$.

Considering this, given any $\mathit{\Lambda} = \omega_1\mathbb{Z}\oplus\omega_2\mathbb{Z}$, one can take $\tau = \omega_1/\omega_2$ and $\alpha = \omega_2$, to obtain $\alpha(\tau\mathbb{Z}\oplus\mathbb{Z}) = \mathit{\Lambda}$. This means that, for $\mathit{\Lambda}_\tau := \tau\mathbb{Z}\oplus\mathbb{Z}$, every complex tori $\mathbb{C}/\mathit{\Lambda}$ is isomorphic to some $\mathbb{C}/\mathit{\Lambda}_\tau$. Therefore, to represent isomorphism classes, one can focus only on lattices generated by some $\tau \in \mathcal{H}$ and 1. However, it is still possible to choose two different $\tau, \tau' \in \mathcal{H}$ and obtain $\mathbb{C}/\mathit{\Lambda}_\tau \cong \mathbb{C}/\mathit{\Lambda}_{\tau'}$. Using Lemma 1.2.1, this is possible exactly when

$$\alpha\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \tau \\ 1 \end{pmatrix}\ ,\ \text{for some} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{1.7}$$

Clearly, it follows that $\alpha = c\tau + d$, hence the following equality holds

$$\tau' = \frac{a\tau+b}{c\tau+d} \tag{1.8}$$

Consequently, let us define the left action of the *modular group* $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ on $\mathcal{H}$ as

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau+b}{c\tau+d}\ ,\ \text{where} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \tag{1.9}$$

Remark 1.2.2. Since both matrices $\gamma, -\gamma \in \mathrm{SL}_2(\mathbb{Z})$ send τ to the same complex number, it is most natural to define this as an action of $\Gamma(1)$ instead of $\mathrm{SL}_2(\mathbb{Z})$.

Therefore, (1.8) shows that two complex tori $\mathbb{C}/\mathit{\Lambda}_\tau$ and $\mathbb{C}/\mathit{\Lambda}_{\tau'}$ are isomorphic if and only if τ and τ' are on the same $\Gamma(1)$-orbit. Understanding isomorphism classes of complex elliptic curves is therefore equivalent to describing the set of orbits

$$Y(1) = \Gamma(1)\backslash\mathcal{H} = \{\Gamma(1)\tau\ :\ \tau \in \mathcal{H}\}. \tag{1.10}$$

This becomes an easy task when one recalls that the two matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{1.11}$$

from (1.6), respectively sending $\tau \in \mathcal{H}$ to $-1/\tau$ and $\tau + 1$, generate $\Gamma(1)$. Thus, for any $\tau \in \mathcal{H}$, one can find τ' in the same orbit with norm ≥ 1, using S, and with $\Re(\tau') \in (-1/2, 1/2]$, using T. This τ' is clearly unique, except if $|\tau'| = 1$. There, one restricts $\Re(\tau') \in [0, 1/2]$ to obtain uniqueness. Then, this region, called the *Fundamental Domain of* $\Gamma(1)$, appropriately represents $Y(1)$ as

$$Y(1) = \{\ \tau \in \mathcal{H}\ :\ |\tau| \geq 1, \Re(\tau) \in (-1/2, 1/2] \text{ and if } |\tau| = 1,\ \text{then } \Re(\tau) \in [0, 1/2]\ \} \tag{1.12}$$

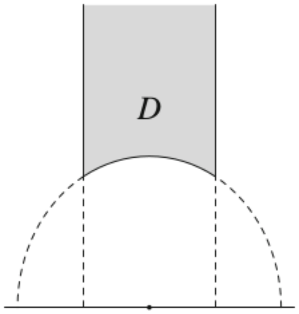


Figure 1.2: Fundamental Domain of $\Gamma(1)$. Image from [DS]

This action on $\mathcal{H}$ gives a canonical bijection between $S(1)$ and $Y(1)$, thus identifies $Y(1)$ as the complete classification of isomorphism classes of elliptic curves. But one can do more by extending this action to $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, it is understood that

$$\gamma(\infty) = a/c \text{ and } \gamma(-d/c) = \infty \tag{1.13}$$

except if $c = 0$, in which case ∞ is mapped back to itself. The set of orbits is now denoted by $X(1)$.

Given any fraction $a/c \in \mathbb{Q}$ with $\gcd(a, c) = 1$, there exists $b, d \in \mathbb{Z}$ such that $ad - bc = 1$, hence $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ sends ∞ to a/c. Therefore, the $\Gamma(1)$-orbit of ∞ is exactly $\mathbb{P}^1(\mathbb{Q})$. Thus, we simply have $X(1) = Y(1) \cup \{\infty\}$, where this single point at infinity (which one can see as on top of this grey area) doesn't represent an isomorphism class of elliptic curves. It is called a *cusp* of $X(1)$.

The motivation behind this extension is because it makes $X(1)$ into a compact Riemann surface, see [S]. It is then a known result from complex analysis that any compact Riemann surfaces can be described as the solution set of polynomial equations. Hence, $X(1)$ is an algebraic variety, and it is actually a curve. We call $X(1)$ a *modular curve*. In this case, using the proper tools, it is actually not too difficult to prove that $X(1)$ is isomorphic to $\mathbb{P}^1(\mathbb{C})$ (again see [S]). This means that the isomorphism classes of elliptic curves are actually well-structured enough to again form an algebraic curve.

1.3 Modular Curve $X_0(N)$

We will now construct a different type of modular curves, which classify elliptic curves, together with extra data, up to isomorphism. Let $E = \mathbb{C}/\Lambda$ be an elliptic curve, for some lattice $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Then, for any integers $N \geq 1$, observe that the kernel of the *multiplication by* N map $[N] : E \to E$, defined by

$$z + \Lambda \mapsto Nz + \Lambda \tag{1.14}$$

is a subgroup of E isomorphic to $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, and generated by ω_1/N and ω_2/N. It is the set of *N-torsion* points of E. The subgroups isomorphic to $\mathbb{Z}/N\mathbb{Z}$ in this kernel are the *cyclic subgroup of order* N of E. It is trivial to see that there are exactly $N + 1$ of them, all of the $\langle \frac{a\omega_1 + b\omega_2}{N} + \Lambda \rangle$, where $\gcd(a, b, N) = 1$.

One can then classify complex elliptic curves, while still holding cyclic subgroup data. The modular group $\Gamma(1)$ is no longer appropriate. One needs to find a restriction of $\Gamma(1)$ that knows when isomorphisms of complex tori send cyclic sugroups of order N to one another.

Definition 1.3.1. Given an integer $N \geq 1$, consider the *congruence subgroup* $\Gamma_0(N)$ of $\Gamma(1)$, defined as

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\} \tag{1.15}$$

This set $\Gamma_0(N)$ is easily seen to be a subgroup of $\Gamma(1)$. By describing explicit orbits of the action defined in (1.9) with respect to this subgroup, we can likewise find a fundamental domain for $\Gamma_0(N)$, to obtain $Y_0(N)$ (see [DS] - Chapter 3 for images).

$$Y_0(N) = \{ \ \Gamma_0(N)\tau \ : \ \tau \in \mathcal{H} \ \} \tag{1.16}$$

Definition 1.3.2. An *enhanced elliptic curve for* $\Gamma_0(N)$ is a pair (E, C) where E is an elliptic curve and C is a cyclic subgroup of order N of E. One refers to such pairs (E, C) and (E', C') as equivalent if some isomorphism $E \to E'$ maps C to C'. The set of equivalence classes is a *moduli space* for $\Gamma_0(N)$, and one refers to it as

$$S_0(N) = \{\text{Enhanced elliptic curves for } \Gamma_0(N)\}/\sim \tag{1.17}$$

Theorem 1.3.3. *Let $N \geq 1$ be an integer. The moduli space $S_0(N)$ is given by*

$$S_0(N) = \{(E_\tau, \langle 1/N + \Lambda_\tau \rangle) \ : \ \tau \in \mathcal{H}\}$$

where $E_\tau = \mathbb{C}/\Lambda_\tau$. Moreover, two pairs $(E_\tau, \langle 1/N + \Lambda_\tau \rangle)$ and $(E_{\tau'}, \langle 1/N + \Lambda_{\tau'} \rangle)$ in $S_0(N)$ are equivalent if and only if τ and τ' are in the same $\Gamma_0(N)$-orbit. Hence, the map $S_0(N) \to Y_0(N)$ defined as follows is a bijection

$$(E_\tau, \langle 1/N + \Lambda_\tau \rangle) \mapsto \Gamma_0(N)\tau \tag{1.18}$$

Proof. Let $(E, C) \in S_0(N)$ be any enhanced elliptic curve for $\Gamma_0(N)$. We can assume $E = E_\tau$, in which case we have $C = \langle \frac{c\tau+d}{N} + \Lambda_\tau \rangle$, where $\gcd(c, d, N) = 1$. We know $\exists\ a, b, k \in \mathbb{Z}$ such that $ad - bc + kN = 1$, namely $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. One can show that the natural homomorphism from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective, hence we may assume $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ by adjusting its entries by multiples of N. Since for all $m_1, m_2 \in \mathbb{Z}$,

$$\left\langle \frac{(c + m_1N)\tau + (d + m_2N)}{N} + \Lambda_\tau \right\rangle = \left\langle \frac{c\tau + d}{N} + m_1\tau + m_2 + \Lambda_\tau \right\rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = C \ ,$$

this slight modification of c, d doesn't affect C. Then, for $\tau' = \gamma(\tau)$ and $\alpha = c\tau + d$, we have $\alpha\Lambda'_\tau = \Lambda_\tau$, as well as

$$\alpha\langle 1/N + \Lambda_{\tau'} \rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = C$$

Thus, $(E, C) \equiv (E'_\tau, 1/N + \Lambda'_\tau)$, proving the first part of the statement.

Now, take $(E_\tau, 1/N + \Lambda_\tau) \in S_0(N)$. If $\tau' = \gamma(\tau)$, for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, then again, for $\alpha = c\tau + d$, we have $\alpha\Lambda_{\tau'} = \Lambda_\tau$, and

$$\alpha\langle 1/N + \Lambda_{\tau'} \rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = \langle d/N + \Lambda_\tau \rangle = \langle 1/N + \Lambda_\tau \rangle \ ,$$

where this last equation holds because $1 = \gcd(c, d, N) = \gcd(d, N)$, i.e. d has order N so it is a generator as well.

Conversely, assume $(E_\tau, 1/N + \Lambda_\tau) \equiv (E_{\tau'}, 1/N + \Lambda_{\tau'})$ in $S_0(N)$. Then, using the same argument as above, we know $\tau' = \gamma(\tau)$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and for $\alpha = c\tau + d$,

$$\alpha\langle 1/N + \Lambda_{\tau'}\rangle = \left\langle \frac{c\tau + d}{N} + \Lambda_\tau \right\rangle = \langle 1/N + \Lambda_\tau\rangle$$

It follows that $c \equiv 0 \mod (N)$, that is, $\gamma \in \Gamma_0(N)$. □

In [DS], section 1.5, a proof of a very similar statement is provided, and this is an adapted version. This result shows that for every enhanced elliptic curves (E, C) for $\Gamma_0(N)$, one can always consider $E = E_\tau$ for some $\tau \in \mathcal{H}$, and its cyclic subgroup to be $C = \langle 1/N + \Lambda_\tau\rangle$. Moreover, it shows that $\Gamma_0(N)$ brings the same relation between $S_0(N)$ and $Y_0(N)$ as $\Gamma(1)$ does for $S(1)$ and $Y(1)$.

Furthermore, as in the previous section, it is possible to compactify $Y_0(N)$, by again considering this action of $\Gamma_0(N)$ on $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}(\mathbb{Q})$. The new set of orbits is denoted $X_0(N)$. Here however, it is not true that all points in $\mathbb{Q}$ are in the same $\Gamma_0(N)$-orbit as ∞. Hence, distinct *cusps* will form in $X_0(N)$, but there are still only finitely many. Again, the cusps do not represent isomorphisms classes. The points of $X_0(N)$ that do represent isomorphisms classes of enhanced elliptic curves, i.e. the points in $Y_0(N) \subset X_0(N)$, will now be refered to as the *complex point* of $X_0(N)$.

Doing all of this again makes $X_0(N)$ into a compact Riemann surfaces, thus it is still described by polynomial equations. One can even show that these polynomials are defined over $\mathbb{Q}$ (see [DS], chapter 7).

Chapter 2

Explicit Modular Curves

2.1 The curves $X_0(l^n)$

Take $l \geq 2$ prime. As we concluded in the previous chapter, the complex points of the modular curve $X_0(l^n)$ over $\mathbb{C}$ are in canonical bijection with isomorphism classes of elliptic curves over $\mathbb{C}$ together with a cyclic subgroup of order l^n. Recall that this interpretation of the complex points does not extend to the cusps of $X_0(l^n)$, and they will require careful manipulation later on.

Note that in [E], Elkies phrases the moduli interpretation of the complex points of $X_0(l^n)$ in terms of the associated isogenies, as follows :

Given a point $(\mathbb{C}/\Lambda_\tau, \langle 1/l^n + \Lambda_\tau \rangle) \in Y_0(l^n) \subset X_0(l^n)$, take $\rho = 1/l^n$. The lattice $\Lambda_{\tau,\rho} = \tau\mathbb{Z} + \rho\mathbb{Z}$ can be seen as a superlattice of Λ_τ, and therefore gives rise to the *cyclic quotient map* from $\mathbb{C}/\Lambda_\tau$ onto $\mathbb{C}/\Lambda_{\tau,\rho}$, defined by $z + \Lambda_\tau \mapsto z + \Lambda_{\tau,\rho}$.

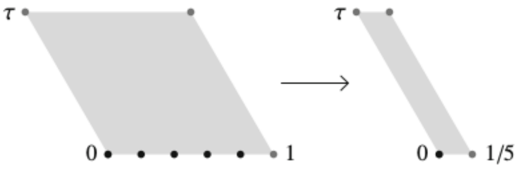


Figure 2.1: Image from [DS].

The kernel of this map is obviously $C = \langle 1/l^n + \Lambda_\tau \rangle$. It follows that from a pair $(\mathbb{C}/\Lambda_\tau, C)$, one can always construct this cyclic l^n-isogeny on E_τ. Conversely, from any cyclic l^n-isogeny φ on E_τ, one may take the enhanced elliptic curve $(\mathbb{C}/\Lambda_\tau, \ker(\varphi))$.

Then, to fully identify the points of $Y_0(l^n)$ as l^n-isogeny, we need to define an equivalence relation on such maps that ensures that two pairs of enhanced elliptic curves $(E_1, C_1), (E_2, C_2) \in Y_0(l^n)$ are equivalent if and only if their corresponding isogenies are equivalent.

Simply say that two l^n-isogenies of elliptic curves $\varphi_i : E_i \to E_i'$ are equivalent if it is possible to form a commutative diagram

$$\begin{tikzcd}
E_1 \arrow[r, "\varphi_1"] \arrow[d, leftrightarrow, "\gamma"] & E_1' \arrow[d, leftrightarrow, "\gamma'"] \\
E_2 \arrow[r, "\varphi_2"] & E_2'
\end{tikzcd}$$

where both $\gamma : E_1 \to E_2$ and $\gamma' : E_1' \to E_2'$ are isomorphisms. Since E_i' is isomorphic to $E_i / \ker(\varphi_i)$, where we use the same notation for the subgroup $\ker(\varphi_i)$ and the superlattice it forms, we know this diagram exists exactly when $(E_1, \ker(\varphi_1)) \cong (E_2, \ker(\varphi_2))$. Thus, one can identify the complex points of $X_0(l^n)$ as isomorphisms classes of elliptic curves with a cyclic l^n-isogeny. As isogenies are simply group homomorphisms on elliptic curves, one can avoid all this work by simply noting that identifying a cyclic subgroup of E_1 is equivalent as giving a group homomorphism on E with a cyclic subgroup, but our description above simply aims to give details to the general picture.

Observe that any cyclic l^n-isogeny can be decomposed into a sequence of l-isogenies

$$E_0 \to E_1 \to \ldots \to E_n \tag{2.1}$$

by taking the l-cyclic quotient map n times, where all the composite isogenies $E_{j-1} \to E_{j+1}$ are cyclic l^2-isogenies.

Remark 2.1.1. Since $\ker(E_{j-1} \to E_j) = \langle 1/l + \Lambda_\tau \rangle$, we know the lattice of E_j is $\Lambda_{\tau,\rho} = \tau\mathbb{Z} \oplus \rho\mathbb{Z}$, where $\rho = 1/l$. Only if we take the quotient of E_j by one of the l cyclic subgroups $\langle (a\tau + \rho)/l + \Lambda_{\tau,\rho} \rangle$, for $a = 0, \ldots, l-1$, do we obtain $\ker(E_{j-1} \to E_{j+1}) \cong \mathbb{Z}/l^2\mathbb{Z}$. For any other one, i.e. $\langle \tau/l + \Lambda_{\tau,\rho} \rangle$, one easily sees that we would get $\ker(E_{j-1} \to E_{j+1}) \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. Thus, the extra condition that all $E_{j-1} \to E_{j+1}$ are cyclic is there to ensure that all sequences such as (2.1) do represent a cyclic l^n-isogeny.

Then, as one might have realized, for any $0 < m \leq n$, the maps $E_j \to E_{j+m}$ are cyclic l^m-isogenies, where $j = 0, \ldots, n-m$. Thus, we have $n-m+1$ natural maps $\pi_j : X_0(l^n) \to X_0(l^m)$ extracting the "subisogenies" $E_j \to E_{j+m}$. These maps have degree l^{n-m}, and in particular, they give us the sequence of degree l maps

$$X_0(l^n) \xrightarrow{\pi_0} X_0(l^{n-1}) \xrightarrow{\pi_0} \cdots \xrightarrow{\pi_0} X_0(l^2) \xrightarrow{\pi_0} X_0(l) \tag{2.2}$$

2.2 Construction of Modular Curves - Elkies' Proposition

To understand Elkies proposition, one needs the Atkin-Lehner involution $w_l^{(n)} : X_0(l^n) \to X_0(l^n)$. It maps a cyclic l^n-isogeny $E_0 \to E_n$ to its dual isogeny $E_n \to E_0$.

In our case, given any cyclic l^n-isogeny $\varphi : E_0 \to E_n$, let $C_0 = \langle 1/l^n + \Lambda_\tau \rangle$ be its kernel, where $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$ is the lattice of E_0. Then, the lattice of E_n is $\Lambda_{\tau,\rho} = \tau\mathbb{Z} \oplus \rho\mathbb{Z}$, where $\rho = 1/l^n$. Now, take $C_n = \langle \tau/l^n + \Lambda_{\tau,\rho} \rangle$, a cyclic subgroup of E_n. Then, let $\varphi_n : E_n \to E_n'$ be the cyclic quotient map of E_n by C_n. Since the lattice of E_n' is given by $\Lambda_{\rho\tau,\rho} = \rho\tau\mathbb{Z} \oplus \rho\mathbb{Z}$, we can simply rescale it back to E_0 with $\varphi_n' : E_n' \to E_0$ as $z + \Lambda_{\rho\tau,\rho} \mapsto l^n z + l^n \Lambda_{\rho\tau,\rho} = l^n z + \Lambda_\tau$. The composition $\varphi_{dual} = \varphi_n' \circ \varphi_n : E_n \to E_0$ is called the *dual isogeny* of φ.

Remark 2.2.1. On $\mathcal{H}$, we can also see the Atkin-Lehner involution as the automorphism $w_l^{(n)}(\tau) = -1/l^n\tau$.

Therefore, we can take the Atkin-Lehner involution $w_l^{(1)}$ of every l-isogeny in (2.1) to obtain the dual sequence

$$E_n \to E_{n-1} \to \ldots \to E_0 \tag{2.3}$$

Then one readily sees that extracting an l^m-isogeny and applying $w_l^{(m)}$ to it is identical as taking the Atkin-Lehner involution $w_l^{(n)}$ of the original l^n-isogeny and extracting the appropriate l^m-isogeny. That is,

$$w_l^{(m)} \circ \pi_j = \pi_{n-m-j} \circ w_l^{(n)} \tag{2.4}$$

Proposition 2.2.2 (Elkies)**.** *For $n > 2$, the map*

$$\pi = \pi_0 \times \pi_1 \times \cdots \times \pi_{n-2} : X_0(l^n) \to (X_0(l^2))^{n-1} \tag{2.5}$$

gives a one-to-one correspondence between l^n-isogenies and the points $\pi(X_0(l^n))$. The image $\pi(X_0(l^n))$ is the set of points $(P_1, \ldots, P_{n-1}) \in (X_0(l^2))^{n-1}$ such that

$$\pi_0 \circ w_l^{(2)}(P_j) = w_l^{(1)} \circ \pi_0(P_{j+1}), \textit{ for all } j = 1, \ldots, n-2 \tag{2.6}$$

Using this proposition, one can construct the whole tower $X_0(l^n)$ by only knowing explicit expressions for π_0 and the Atkin-Lehner involutions involved. This proposition is really a statement about the complex points of $X_0(l^n)$. The cusps are also represented by solutions of (2.6), but the correspondence might no longer be one-to-one. In general, this shows that $X_0(l^n)$ is birationally equivalent to the locus of points $(P_1, \ldots, P_{n-1})$ in $(X_0(l^2))^{n-1}$ satisfying the $n-2$ equations described in (2.6).

Remark 2.2.3. The following proof will not discuss the behavior of the cusps under this map π. We will write $Y_0(l^n)$ instead of $X_0(l^n)$ to stress furthermore the fact that we are only working with complex points. As mentioned above, this correspondence does extends to cusps, but is simply no longer necessarily one-to-one. A more advanced reader may therefore see $X_0(l^n)$ where we write $Y_0(l^n)$ and still see the statements as true, as Elkies does in his paper.

Proof. For any $j = 0, \ldots, n-2$, we have $\pi_j : Y_0(l^n) \to Y_0(l^2)$ taking a sequence

$$s := E_0 \to E_1 \to \ldots \to E_n \in Y_0(l^n)$$

to its image $P_{j+1} := \pi_j(s) = E_j \to E_{j+1} \to E_{j+2}$. Since the sequence s is completely determined by its l^2-subisogenies $E_j \to E_{j+2}$, it follows that s is uniquely determined by $(P_1, \ldots, P_{n-1})$. This shows that π is injective. Thus, the points of $Y_0(l^n)$ are in one-to-one correspondance with the points of $\pi(Y_0(l^n))$.

To describe explicitely this image, take $P_j = E_0^j \to E_1^j \to E_2^j \in Y_0(l^2)$, for $j = 1, \ldots, n-2$. For $(P_1, \ldots, P_{n-1})$ to be in $\pi_0(Y_0(l^n))$, all that is required is that we can glue the isogenies that each of these P_i represent consecutively together, i.e.

$$E_1^j \to E_2^j \text{ is the same as } E_0^{j+1} \to E_2^{j+1}$$

But these two l-isogenies are simply points in $Y_0(l)$, thus using $\pi_0, \pi_1 : Y_0(l^2) \to Y_0(l)$, this statement translates into

$$\pi_1(P_j) = \pi_0(P_{j+1})$$

and taking the Atkin-Lehner involution $w_l^{(1)}$ on both sides and using (2.4) gives us

$$\pi_0(w_l^{(2)}(P_j)) = w_l^{(1)}(\pi_0(P_{j+1})) \ ,\forall \ j = 1, \dots , n-2 \ ,$$

which is exactly what we wanted. Thus, the map π is an isomorphism between $Y_0(l^n)$ and the solution space of the $n-2$ equation from (2.6) in $(Y_0(l^2))^{n-1}$. Since this maps extends to cusp, it follows that that $X_0(l^n)$ is birationally equivalent to the curve defined by this solution space in $(X_0(l^n))^{n-1}$. □

Remark 2.2.4. Using this new description, it follows that these $\pi_j : X_0(l^n) \to X_0(l^m)$ are simply

$$(P_1, \dots , P_{n-1}) \mapsto (P_{j+1}, \dots , P_{j+m-1}) \tag{2.7}$$

The complex points of $X_0(l^n)$, i.e. sequences as in (2.1), are now described by the $n-1$ consecutive l^2-isogenies that composes them. Then, exctracting the l^m-isogeny $E_j \to E_{j+m}$, is exactly the same as extracting the $m-1$ consecutive l^2-isogenies $E_j \to E_{j+1} \to E_{j-1}, \dots , E_{j+m-2} \to E_{j+m-1} \to E_{j+m}$, as (2.7) points out. This new description given by Elkies simply makes this diagram commute

$$\begin{tikzcd}
X_0(l^n) \arrow[r, "\pi"] \arrow[d, "\pi_j \text{ (old)}"] & (X_0(l^2))^{n-1} \arrow[d, "\pi_j \text{ (new)}"] \\
X_0(l^m) \arrow[r, "\pi"] & (X_0(l^2))^{m-1}
\end{tikzcd}$$

2.3 Model for $X_0(2^n)$

Using Elkies' proposition, the first requirement is to find equations for $X_0(2)$ and $X_0(4)$. Then, understanding $\pi_0 : X_0(4) \to X_0(2)$, and the Atkin-Lehner involution's $w_2^{(1)}$, $w_2^{(2)}$ reveals the algebraic conditions necessary to identify $(P_1, \dots , P_{n-1}) \subset (X_0(4))^{n-1}$ as a point in $X_0(2^n)$.

Since both $X_0(2)$ and $X_0(4)$ have genus 0, they are isomorphic to $\mathbb{P}^1$. Thus, one can parametrize them by giving appropriate coordinates on $\mathbb{P}^1 := \mathbb{P}^1(\mathbb{C})$. For $X_0(4)$, Elkies uses the identification $\tau \leftrightarrow \xi(\tau)$, where

$$\xi(\tau) = 1 + \frac{1}{8}\left(\frac{\eta(\tau)}{\eta(4\tau)}\right)^8 = \frac{1}{8}(q^{-1} + 20q - 62q^3 + 216q^5 - \dots) \tag{2.8}$$

Here, $q = e^{2\pi i\tau}$ as usual, with $q = 0$ for $\tau = \infty$. On the other hand, η is a function on $\mathcal{H}^*$ defined as

$$\eta(\tau) = \prod_{r=1}^{\infty}(1 - q^r) \tag{2.9}$$

Both of these functions have very strong connection to modular curve theory. For more information, see [DS], section 1.1 and 1.2. This map ξ provides an isomorphism between $X_0(4)$ and $\mathbb{P}^1$, thus one can parametrize $X_0(4)$ by looking at $\xi(\tau)$ as a coordinate for $\mathbb{P}^1$, now appropriately refered to as $\mathbb{P}^1_\xi$.

To use proposition 2.2.2, one also need to know the effect on $w_2^{(2)}$ on $\mathbb{P}^1_\xi$. Using the following identity (proof in [DS]),

$$\eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau) \ , \tag{2.10}$$

it follows that

$$w_2^{(2)}(\xi(\tau)) = \xi(-1/4\tau) = 1 + 32\left(\frac{\eta(4\tau)}{\eta(\tau)}\right)^8 = 1 + \frac{4}{\xi(\tau) - 1} = \frac{\xi(\tau) + 3}{\xi(\tau) - 1} \tag{2.11}$$

Thus, $w_2^{(2)} : \mathbb{P}^1_\xi \to \mathbb{P}^1_\xi$ is $w_2^{(2)}(\xi) = \dfrac{\xi+3}{\xi-1}$. Now, the same procedure needs to be applied for $w_2^{(1)}$ on coordinates of $X_0(2)$. Elkies chooses the Hauptmodul h_2 to parametrize $X_0(2)$, defined as

$$h_2(\tau) = \left(\frac{\eta(\tau)}{\eta(2\tau)}\right)^{24} = q^{-1} - 24 + 276q - 2048q^2 + \dots \tag{2.12}$$

Again, using (2.10), one can show that $w_2^{(1)} : \mathbb{P}^1_{h_2} \to \mathbb{P}^1_{h_2}$ is $w_2^{(1)}(h_2) = 2^{12}/h_2$. The last requirement now is to describe $\pi_0 : \mathbb{P}^1_\xi \to \mathbb{P}^1_{h_2}$, i.e. write h_2 as a rational function in ξ. By inspecting the q-expension of h_2 and ξ, we see that $h_2 - 8\xi + 24$ is a rational function, of degree 1 in ξ, and has a simple zero at $\xi = \infty$.

Remark 2.3.1. Note that π_0 lets us see h_2 as a function in ξ. Since $\deg_\xi(h_2) = \deg_\xi(\pi_0) = 2$, we need to clarify why $z = h_2 - 8\xi + 24$ has degree 1 in ξ. It suffices to demonstrate that z has a unique simple pole. Clearly, $z = \infty$ implies either $h_2 = \infty$ or $\xi = \infty$. One easily sees from the q-expension of z that $\xi = \infty$ (i.e. $q = 0$) is not a pole, it is a simple zero.

Then, showing that only one of the two elements in the fiber of $h_2 = \infty$ leads to a pole of z suffices. From the q-expensions of ξ and h_2, we know $\xi(\tau) = \infty \Rightarrow \tau = \infty \Rightarrow h_2(\tau) = \infty$. This doesn't lead to a pole, hence $h_2(\tau) = \infty$ must have another solution. This one must be a pole since z must have one (because z has at least one zero), which proves our claim.

Moving on, since $h_2 - 8\xi + 24$ has degree 1, it can be written has $(a\xi + b)/(c\xi + d)$, some coefficients $a, b, c, d \in \mathbb{C}$. Moreover, one easily sees that $a = 0$, as $\xi = \infty$ is a zero. Therefore, $1/(h_2 - 8\xi + 24)$ is a polynomial of degree 1 in ξ. Thus, Elkies simply solves the system

$$\begin{array}{rcl} \alpha(\xi+\beta) & = & 2^{-3}\alpha(q^{-1} + 8\beta + 20q - 62q^3 + \dots) \\ \times \quad h_2 - 8\xi + 24 & = & 256q - 2048q^2 + 11264q^3 + \dots \\ \hline 1 & = & 32\alpha + 256(\beta-1)\alpha q + 2048(1-\beta)\alpha q^2 + \dots \end{array}$$

to obtain $\alpha = 2^{-5}$ and $\beta = 1$. Then, by solving the following equation for h_2, one obtains

$$\frac{1}{h_2 - 8\xi + 24} = \frac{\xi+1}{32} \iff h_2 = 8\frac{(\xi-1)^2}{\xi+1} \tag{2.13}$$

Remark 2.3.2. There is a small typo in Elkies paper here, the $+/-$ signs were flipped in this last equation.

This shows that

$$h_2(\tau) = \pi_0(\xi(\tau)) = 8\frac{(\xi(\tau)-1)^2}{\xi(\tau)+1}\ , \tag{2.14}$$

which means that all the pieces of the puzzle are now available : $w_2^{(1)}$, $w_2^{(2)}$ and π_0 as explicit rational maps. One can then use (2.6) for $j = 1$. That is, pick $P_1 \in X_0(4)$, and find $P_2 \in X_0(4)$ satisfying

$$\pi_0 \circ w_2^{(2)}(P_1) = w_2^{(1)} \circ \pi_0(P_2) \iff \pi_0(P_2) = w_2^{(1)} \circ \pi_0 \circ w_2^{(2)}(P_1) \tag{2.15}$$

By taking $P_1 = \xi(\tau)$, we can use the definition of each of these maps to obtain

$$\pi_0(P_2) = w_2^{(1)} \circ \pi_0(\xi(-1/4\tau)) = w_2^{(1)}(h_2(-1/4\tau)) = h_2(2\tau) \tag{2.16}$$

Hence, to describe $X_0(8)$ as an algebraic curve in $(X_0(4))^2$, Elkies simply writes down the algebraic relation between $\xi(\tau)$ and $\xi(2\tau)$.

Firstly, he writes $h_2(2\tau)$ explicitely from (2.16) as

$$h_2(2\tau) = w_2^{(1)} \circ \pi_0(\xi(-1/4\tau)) = w_2^{(1)} \circ \pi_0 \left(\frac{\xi(\tau)+3}{\xi(\tau)-1} \right) = 64(\xi(\tau)^2 - 1) \tag{2.17}$$

Secondly, he simply rewrites $h_2(\tau)$ by using (2.11) to obtain

$$h_2(\tau) = \frac{8(\xi(\tau)-1)^2}{\xi(\tau)+1} = \frac{8\left(\frac{4}{\xi(-1/4\tau)-1}\right)^2}{\frac{4}{\xi(-1/4\tau)-1}+2} = \frac{64}{w_2^{(2)}(\xi(\tau))^2 - 1} \tag{2.18}$$

Therefore, by replacing τ by 2τ in this last equation, he can equate these last two expressions and obtain the relation

$$(\xi(\tau)^2 - 1)(w_2^{(2)}(\xi(2\tau))^2 - 1) = 1 \tag{2.19}$$

Conclusion : By taking $x_1 = \xi(\tau)$ and $x_2 = \xi(2\tau)$, one can consider the points of $X_0(8)$ as the pairs $(x_1, x_2) \in (X_0(4))^2 = \mathbb{P}^1 \times \mathbb{P}^1$ satisfying

$$(x_1^2 - 1)(z_2^2 - 1) = 1 \text{ , where } z_2 = w_2^{(2)}(x_2) = \frac{x_2+3}{x_2-1}. \tag{2.20}$$

Similarly, for all $n \geq 2$, one can write down explicitely $X_0(2^n)$ by iterating this procedure $n-2$ times. But then, we consecutively obtain the same relation as in (2.20), but with the pairs $(x_2, x_3) = (\xi(2\tau), \xi(4\tau))$ as well, and then again with $(x_3, x_4) = (\xi(4\tau), \xi(8\tau))$, etc. Therefore, for $x_i = \xi(2^{i-1}\tau)$, Elkies has shown that $X_0(2^n)$ is birationally equivalent to the locus of points $(x_1, \ldots, x_{n-1}) \in (\mathbb{P}^1)^{n-1}$ satisfying the $n-2$ equations

$$(x_i^2 - 1)(z_{i+1}^2 - 1) = 1 \text{ , } \forall\, i = 1, \ldots, n-2 \text{ ,} \tag{2.21}$$

where

$$z_i := \frac{x_i + 3}{x_i - 1} \tag{2.22}$$

2.4 Model for $X_0(3^n)$

For the tower of modular curves $X_0(3^n)$, we again have to choose coordinates on $X_0(3)$ and $X_0(9)$, which is still easy since they are both isomorphic to $\mathbb{P}^1$, and adapt the computations accordingly. Elkies suggests to parametrize $X_0(9)$ using $\xi(\tau)$, now defined as

$$\xi(\tau) = 1 + \frac{1}{3}\left(\frac{n(\tau)}{n(9\tau)}\right) = \frac{1}{3}(q^{-1} + 5q - 7q^5 + 3q^8 + 15q^{11} - 32q^{14} + \ldots) \text{ ,} \tag{2.23}$$

and then the Atkin-Lehner involution $w_3^{(2)}$ acts on $\mathbb{P}^1_\xi$ as

$$w_3^{(2)}(\xi(\tau)) = \xi(-1/9\tau) = 1 + \frac{3}{\xi(\tau)-1} = \frac{\xi(\tau)+2}{\xi(\tau)-1} \tag{2.24}$$

For $X_0(3)$, he similarly uses the Hauptmodul h_3 defined as

$$h_3(\tau) = \left(\frac{\eta(\tau)}{\eta(3\tau)}\right) = q^{-1} - 12 + 54q - 76q^2 - 243q^3 + 1188q^4 + \ldots \text{ ,} \tag{2.25}$$

which satisfies

$$w_3^{(1)}(h_3(\tau)) = h_3(-1/3\tau) = 3^6/h_3(\tau) \tag{2.26}$$

Then, all there is left to describe is $\pi_0 : X_0(9) \to X_0(3)$, i.e. write h_3 as a rational function in ξ. Elkies does not show this step. He arrives directly to (2.28). However, for our purposes, this explicit map does show some relevant properties (more comments below). After going through the calculations, similar to our derivation of (2.18), one obtains

$$h_3(\tau) = \pi_0(\xi(\tau)) = 9\frac{(\xi(\tau)-1)^3}{\xi(\tau)^2+\xi(\tau)+1} \tag{2.27}$$

Using the same argument as in (2.16), we see that a point $(P_1, P_2) \in (X_0(9))^2$ will correspond to a complex point of $X_0(27)$ if $P_1 = \xi(\tau)$, and $P_2 \in X_0(9)$ verifies the equality $\pi_0(P_2) = h_3(3\tau)$. Using the same logic as previously, Elkies writes down $h_3(3\tau)$ in two different ways as

$$h_3(3\tau) = 27(\xi(\tau)^3 - 1) = \frac{27}{w_3^{(2)}(\xi(3\tau))^3 - 1}\ , \tag{2.28}$$

Conclusion : With the coordinates $x_i = \xi(3^{i-1}\tau) \in X_0(9)$, $i = 1, \dots, n-1$, the modular curve $X_0(3^n)$ is birationally equivalent to the locus of $(x_1, \dots, x_{n-1}) \in (\mathbb{P}^1)^{n-1}$ satisfying the algebraic conditions

$$(x_i^3 - 1)(z_{i+1}^3 - 1) = 1 \tag{2.29}$$

where $i = 1, \dots, n-2$ and $z_i := \dfrac{x_i + 2}{x_i - 1}$.

In the last chapter of this paper, we will thoroughly study this model of the modular tower $X_0(3^n)$. For instance, this model turns out to be singular, particularly at infinity. We will later try to unravel the structure of these multiples points on each of these curves and see how they are fundamentally linked to the ramifications of the maps $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$.

The reason why they are so important is that they represent the images in $(\mathbb{P}^1)^{n-1}$ of cuspidal points of the actual modular curves $X_0(3^n)$. They are exactly the points where the proposition of Elkies becomes subtle, but in this sense, where everything interesting is most likely to happen.

To see that these singularities correspond to cusps, consider the formula of π_0 from (2.27). It is known that for such a polynomial maps, cusps are sent to cusps. Moreover, the cusps of $X_0(3)$ are parametrized by $h_3 = 0$ or $h_3 = \infty$. Then, (2.27) gives us that the cusps of $X_0(3^n)$ are given by points where at least one coordinates $x_j = \xi(3^{j-1}\tau)$ is $x_j = \infty$ or $x_j = \zeta_3^k$, $k = 0, 1, 2$ (any cube root of unity). We'll see that these values keep appearing in our future computations of singularities and ramifications.

Remark 2.4.1. These two models are only the first ones given in Elkies' paper. Refer to [E] to see quite a few other examples. However, some of them require more involved arguments and computations. Also, some types of modular curves considered in [E] were not introduced here. However, know that it represents a tremendous accomplishment to explicitely write down the polynomials over $\mathbb{Q}$ of all these modular curves. For instance, according to a paper published in 2017 by Hasegawa, see [H], the models given by Elkies of two different towers of Shimura modular curves are the only ones ever constructed.

Chapter 3

Resolution of Singularities

As mentionned in the previous chapter, the models of tower of modular curves given by Elkies in [E] turn out to be singular. In this chapter, we discuss the procedure of *resolving singularities* and consider various examples. In our next chapter, this will lead to a fabulous result relating the modular curves $X_0(8)$, $X_0(27)$ and $X_0(64)$ with Fermat curves! Moreover, it will play a key role to understand the ramifications of $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$.

Remark 3.0.1. This chapter is the result of shared effort with my collegue Kevin Watmough.

Let X be an variety over an algebraically closed field k, with $\text{char}(k) = 0$. If X is singular, then we wish to resolve these singularities by finding a nonsingular variety $\tilde{X}$, and a proper birational map $\varphi : \tilde{X} \to X$.

Definition 3.0.2. A *modification* is a morphism of algebraic varieties which is birational and proper.

Theorem 3.0.3 (Hirokana's Theorem). *Let X be an variety over an algebraically closed field k, with char$(k) = 0$. Then, there exists a modification $\varphi : \tilde{X} \to X$ such that $\tilde{X}$ is a nonsingular variety.*

Remark 3.0.4. Published in 1964, this theorem was a huge accomplishment, as it answered many open questions and enable at least as many applications. Moreover, by pushing Hironaka's proof even further, mathematicians were able to prove that it is always possible to choose φ to be an isomorphism exactly on the smooth locus of X. However, even though Hironaka showed this theorem by giving an explicit construction of $\tilde{X}$ and φ, it is still consider as an highly advanced and difficult proof. Therefore, even for some singular curves, it is highly nontrivial to find their respective nonsingular models. When this theorem doesn't apply, i.e. we're are not in characteristic 0 (or is too difficult to apply), the concept of *alterations* gives us another alternative.

Remark 3.0.5. Note that the concept of *proper* birational maps is fundamental for this theorem, since removing it makes the statement trivial. For any singular variety X, we know the set of singularities S is a subvariety of X, then $X' = X \setminus S$ is an open subvariety of X, hence a variety itself. Simply taking φ to be the inclusion map then would be sufficient. However, this is clearly not what we mean by a *resolution* of singularities. This solution is not valid because such a morphism φ is not proper. In general, the properness of a morphism forces it to have no "holes" in its fibers.

One of the main tools in algebraic geometry to desingularise a variety X is to compute a *blow-up*. In some sense, this takes a singularity P of X and streches the space at this point to separate the different tangents of

X at P. The proof of Hironaka produces the modification φ as a sequence of such blow-ups, which simplify the nature of the singular locus of X at every step. Furthermore, using notation from Hironaka's theorem, one can even prove that $\tilde{X}$ is unique, up to isomorphism, using the following result.

Proposition 3.0.6. *Let X, Y be two projective smooth curves. If X and Y are birationally equivalent, they are in fact isomorphic.*

Thus, if $\psi : \tilde{X}' \to X$ is any other proper birational map, with $\tilde{X}'$ smooth, then we must have an isomorphism $f : \tilde{X}' \to \tilde{X}$ making the following diagram commute

$$\begin{tikzcd}
\tilde{X}' \arrow[r, "f"] \arrow[dr, "\psi"'] & \tilde{X} \arrow[d, "\varphi"] \\
 & X
\end{tikzcd}$$

Therefore, we say that $\tilde{X}$ is the *nonsingular model* of X.

3.1 Normalization of Singular Curves

In this section, we will show how to resolve the singularities of curves. We will use a process called *normalization*. In this case, it turns out that the normalization of a curve can be seen as a sequence of consecutive blow-ups.

Definition 3.1.1. Let C be an affine algebraic curve, with coordinate ring $\Gamma(C)$. The *normalization* of $\Gamma(C)$ is its integral closure in its quotient field $k(C)$. We denote it by $\tilde{\Gamma}(C)$. If $\tilde{\Gamma}(C) = \Gamma(C)$, we say that C is a normal curve.

Note that the affiness condition is important here. Otherwise, for projective curves, this is not adapted. For instance, if we consider the projective singular curve $C : y^2 = x^3 + x^2 \subset \mathbb{P}^2$, we obtain $\Gamma(C) = k$ since the only regular functions on a projective curve over a algebraically closed field are constant. Thus, we would have both C normal and singular, which would contradict the following proposition 3.1.3. To adapt the concept of *normality*, we need the following definition.

Definition 3.1.2. Let $X = \mathbb{P}^{n_1} \times \ldots \times \mathbb{P}^{n_r} \times \mathbb{A}^m$ be a mixed space, and $C \subset X$ a curve. Then, C is *normal* if, for all affine patch $U \subset X$, the affine curve $C \cap U$ is normal.

Similarly, we say that $P \in C$ is a *normal point of* X if $\mathcal{O}_P(C)$ is integrally closed in $k(C)$. Then, it is equivalent to define C as normal when all its points are normal. Note that the normality of $P \in C$ only depends on the local ring $\mathcal{O}_P(C)$. Similarly, from [F], we know that a point P is simple if and only if $\mathcal{O}_P(C)$ is a DVR. Thus, both of these property are completely based on the behavior of $\mathcal{O}_P(C)$. Then, it is only natural to ask if it is possible to related this two properties, and we obtain the following.

Proposition 3.1.3. *Let C be any algebraic curve. Then, C is smooth if and only if C is normal.*

Proof. (Sketch)

The first part of this proves is easy. Let C be any curve, and $P \in C$ a smooth point. By contradiction, assume there is a rational function $z \in k(C) \setminus \mathcal{O}_P(C)$ that is integral over $\mathcal{O}_P(C)$. Since $\mathcal{O}_P(C)$ is DVR, it induces an order function on its quotient ring, ord : $k(C) \to \mathbb{Z}$.

Since $z \notin \mathcal{O}_P(C)$, we know $\mathrm{ord}(z) < 0$. Moreover, the fact that z is integral over $\mathcal{O}_P(C)$ implies that for some monic polynomial $f \in \mathcal{O}_P(C)[t]$

$$f(z) = z^m + a_{m-1}z^{m-1} + \ldots + a_1 z + a_0 = 0, \text{ with } a_i \in \mathcal{O}_P(C) \text{ and } m > 1$$

Since the a_i's are in $\mathcal{O}_P(C)$, they all have $\mathrm{ord}(a_i) \geq 0$. Moreover, recall that multiply two elements sums their order, thus z^m has a strictly lower order than all the other terms in this expression. Therefore, $\mathrm{ord}(f(z)) = m \cdot \mathrm{ord}(z)$, as for any $a, b \in k(C)$, with ord(a) $< \mathrm{ord}(b)$, we know $\mathrm{ord}(a + b) = \mathrm{ord}(a)$. However, this implies that 0 has a finite order, contradiction. It follows that for a smooth curve C, all its points are normal, thus C is normal.

For the converse, broadly speaking, Kollar takes some singular point $P \in C$ so that

$$\dim_k(\mathfrak{m}_P(C)/\mathfrak{m}_P(C)^2) \geq 2$$

Then, by using two linearly independent elements $x, y \in \mathfrak{m}_P(C)$, he explicitely constructs an integral element of the form

$$z = \frac{y}{x + ay}u \ ,$$

for some $a \in k$ and units $u \in \mathcal{O}_P(C)$. In terms of commutative algebra, this shows how integral elements and singularities are related. For instance, in our later examples, notice how all the integral elements we will find give a case $\frac{0}{0}$ if we were to evaluate them at the singular point. This is what we observe in the integral element z above. (Since x and y are two rational functions in $\mathfrak{m}_P(F)$, we know they are zero at P) □

Note that this is a result very specific to curves. In general, for algebraic varieties of dimension greater than 1, a normal variety might very well be singular. For instance look at the cone $X \subset \mathbb{A}^3$ define by $x^2 + y^2 = z^2$. Clearly, this variety is singular at the origin, however one can still show that it is normal. But even if this correspondence fails in higher dimension, this is of great use to resolve the singularities of curves.

We will now consider the curve C to be affine and demonstrate the process of normalization. If C was projective, we can simply restrict it in an affine patch, apply the technique and take back its projective closure. For an affine curve C, one can show that $\tilde{\Gamma}(C)$ is finite over $\Gamma(C)$. Therefore, to compute the normalization of C, we have to find finitely many $z_1, \ldots, z_r \in k(C)$, integral over $\Gamma(C)$, such that $\tilde{\Gamma}(C) = \Gamma(C)[z_1, \ldots, z_r]$.

Generally, this is a very difficult task. Firstly, you need to *find* integral elements, and moreover, you need to show that you have all of them. There is no way around finding integral elements. We can only hope that the polynomials defining C are not too horrific, or stare at them long enough. To see an algorithm which finds such an integral element, the one vaguely described in our proof above, see Theorem 1.30 of [K].

On the other hand, to show we have all of them, the previous theorem helps us greatly. Showing that the curve $\tilde{C}$ satisfying $\Gamma(\tilde{C}) = \Gamma(C)[z_1, \ldots, z_r]$ is smooth will show that it is normal, hence that we have found all integral elements.

Moreover, the inclusion map

$$\varphi^* : \Gamma(C) \hookrightarrow \tilde{\Gamma}(C) = \Gamma(\tilde{C})$$

gives a natural birational map $\varphi : \tilde{C} \to C$. Since one can show that this is a proper morphism, Hirokana's Theorem tells us that $\tilde{C}$ is the nonsingular model of C. This gives us a way to find a suitable $\tilde{C}$. To summarize, here is a general idea of the method. Consider an affine singular curve C, with $\Gamma(C) = k[x_1, \ldots, x_n]$, then

1. Find an integal element $z \in k(C)$ over $\Gamma(C)$, and take $\Gamma' = \Gamma(C)[z]$.

2. If $z = \frac{h(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ satisfies the monic (in z) polynomial $f(x_1, ..., x_n, z) = 0$, then take

$$\Gamma' = k[x_1, ..., x_n, z]/(I, f, gz - h) \ .$$

3. Simplify the ideal $(I, f, gz - h)$ and Γ' as much as possible by removing redundant equations and variables, to find $\Gamma' = k[x'_1, ..., x'_m]/J'$. Then, take $\tilde{C} = V(J')$, so that $\Gamma(\tilde{C}) = \Gamma'$.

4. If $\tilde{C}$ is nonsingular, then $\Gamma(\tilde{C}) = \tilde{\Gamma}(C)$, and the inclusion map

$$\tilde{\varphi} : \Gamma(C) \to \tilde{\Gamma}(C) = \Gamma(\tilde{C}) \text{ as } x_i \mapsto x_i, \ \forall \ i = 1, ..., n$$

   gives us naturally the birational morphism $\varphi : \tilde{C} \to C$, and we have now the smooth model of C.

5. If $\tilde{C}$ is singular, $\Gamma(\tilde{C})$ is missing some integral elements, and repeating (1)-(4) a finite number of times will be sufficient to find all integral elements.

We now illustrate this method with some examples.

3.2 Example 1 : Nodal Curve

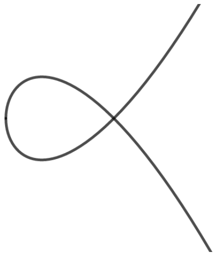
Let $C : y^2 - x^2(x + 1) = 0$. This curve C has a singular point, a node, at $P = (0, 0)$. We will use the method above to resolve the singularity at P. We first find the integral closure $\widetilde{\Gamma}(C)$ of $\Gamma(C)$. Note that $z = y/x \in k(C)$ is integral over $\Gamma(C)$, and it satisfies the relation $z^2 = x + 1$, since $y^2 = x^2(x + 1)$ in $\Gamma(C)$. Then

$$\Gamma(C)[z] = k[x, y, z]/(y^2 - x^2(x + 1), y - xz, z^2 - x - 1).$$

Since $y^2 - x^2(x + 1) = (y - xz)(y + xz) + x^2(z^2 - x - 1)$, we can remove this polynomial from the generators of the ideal. Then, we obtain

$$\Gamma(C)[z] = k[x, y, z]/(y - xz, z^2 - x - 1) \simeq k[z] \ ,$$

where the second equality holds as $y = xz$ and $x = z^2 - 1$.



$C : y^2 - x^2(x + 1) = 0$

Remark 3.2.1. Our claim that $k[x, y, z]/(y - xz, z^2 - x - 1) = k[z]$ needs a bit of justification. What we actually mean is that the map $k[x, y, z] \to k[z]$ as

$$x \mapsto z^2 - 1 \ ; \ y \mapsto z(z^2 - 1) \ ; \ z \mapsto z$$

is surjective with kernel $(y - xz, z^2 - x - 1)$. Surjectivity is easy to check. Now, observe that we can always write

$$f(x, y, z) = f(z^2 - 1, z(z^2 - 1), z) + (y - xz)A(x, y, z) + (z^2 - x - 1)B(x, y, z)$$

using the following procedure :

To replace y with xz, write

$$\begin{aligned} f &= f_0(x, z) + yf_1(x, y, z) \\ &= f_0(x, z) + xzf_1(x, y, z) + (y - xz)f_1(x, y, z). \end{aligned}$$

Then, the degree of f_1 in y will be lower than that of f, so repeating this a finite number of times (on f_1) will get f in the form $f(x, xz, z) + (y - xz)A(x, y, z)$. A similar process replaces x with $z^2 - 1$.
Hence, $f(z^2 - 1, z(z^2 - 1), z) = 0$ if and only if $f \in (y - xz, z^2 - x - 1)$.

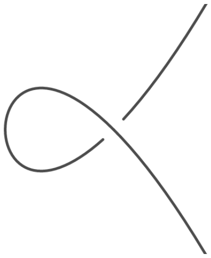
Returning to the problem at hand, we have the map $\varphi^* : \Gamma(C) \to k[z]$ as

$$x \mapsto z^2 - 1\ ;\ y \mapsto z(z^2 - 1) \tag{3.1}$$

Since $k[z] = \Gamma(\mathbb{P}^1)$, φ^* gives us the map $\varphi : \mathbb{P}^1 \to C$ as

$$z \mapsto (z^2 - 1, z(z^2 - 1)) \tag{3.2}$$

Since $\mathbb{P}^1$ is smooth, we are done, and so C is birationally equivalent to $\mathbb{P}^1$ via the map φ. This shows that the nonsingular model of C is simply a line. Moreover, note that the map φ is one-to-one everywhere except at the points $\pm 1 \in \mathbb{P}^1$, which both map to $(0, 0) \in C$, our singular point. So, intuitively, we have pulled apart the two tangent lines at $(0, 0)$ to get two simple points.



Remark 3.2.2. Recall that in Remark 3.0.5, we had found a birational morphism over a smooth curve, but it wasn't proper, hence not a valid resolution. But the reader might be relief to know that normalization always yields proper morphisms such as φ above. Thus, normalizing a curve always explicitely constructs its nonsingular model.

3.3 Example 2 : Quadrifolium

We now examine the quadrifolium

$$C : (x^2 + y^2)^3 - 4x^2y^2 = 0, \tag{3.3}$$

which has exactly one singular point, at $(0, 0)$ – see figure below.

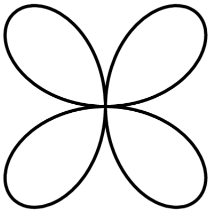


Figure 3.1: $C : (x^2+y^2)^3 - 4x^2y^2 = 0$

We will show that C is birationally equivalent to $\mathbb{P}^1$ over $\mathbb{Q}$, by resolving the singularity at $(0,0)$. This will give us the rational parametrization of the curve, i.e. we will then be able to find all the rational point of this curve which are far from obvious to find!

We proceed by the same method of finding the integral closure of $\Gamma(C)$. We first find, by inspection, that the integral element

$$z = \frac{2xy}{x^2+y^2} \tag{3.4}$$

satisfies $z^2 = x^2 + y^2$. We obtain the subring $\Gamma' = \Gamma(C)[z] \subseteq \widetilde{\Gamma}(C)$ defined by the quotient of $k[x,y,z]$ by the ideal defined by the equations

$$\begin{cases} f_1 = (x^2+y^2)^3 - 4x^2y^2 \\ f_2 = x^2 + y^2 - z^2 \\ f_3 = z(x^2+y^2) - 2xy \end{cases}$$

The first equation is redundant, since $f_1 = (z(x^2+y^2)+2xy)f_2 + (x^2+y^2)^2 f_3$, and we can substitute $z^2 = x^2+y^2$ into the f_3 to get

$$\Gamma' = k[x,y,z]/(x^2+y^2-z^2, z^3-2xy),$$

and a map $\varphi_1^* : \Gamma(C) \to \Gamma'$, simply given by by $x \mapsto x$ and $y \mapsto y$.

Let $C_1 = V(x^2+y^2-z^2, z^3-2xy) \subset \mathbb{A}^3$. Then, we have the polynomial map $\varphi_1 : C_1 \to C$ as

$$(x,y,z) \mapsto (x,y) \tag{3.5}$$

However, the Jacobian of C_1 is

$$J = \begin{pmatrix} 2x & 2y & -2z \\ -2y & -2x & 3z^2 \end{pmatrix},$$

which is 0 at $(0,0,0)$, hence C_1 still has a singular point at $(0,0,0)$. This means we need more integral elements. Let's rewrite the ideal $(x^2+y^2-z^2, z^3-2xy)$ slightly. Substracting these two generators, we have

$$(x^2+y^2-z^2, z^3-2xy) = (x^2+y^2-z^2, z^2(z+1)-(x+y)^2)$$

Then, dividing the second equation by z^2 gives us the integral element

$$w = \frac{x+y}{z} \tag{3.6}$$

verifying $w^2 = z + 1$. Thus, we have $\Gamma'' = \Gamma(C')[w] \subseteq \tilde{\Gamma}(C)$ is equal to the quotient of $k[x, y, z, w]$ by the ideal generated by

$$\begin{cases} f_1 = x^2 + y^2 - z^2 \\ f_2 = z^3 - 2xy \\ f_3 = zw - x - y \\ f_4 = w^2 - z - 1 \end{cases}$$

First, note $f_2 = (zw + x + y)f_3 - z^2 f_4 + f_1$, so we can remove it. Moreover, in Γ'', we have $z = w^2 - 1$ and $y = zw - x = w(w^2 - 1) - x$, so we get

$$\Gamma'' = k[x, w]/((w(w^2 - 1) - x)^2 + x^2 - (w^2 - 1)^2)$$

Renaming w as y, and taking $C_2 = V((y(y^2 - 1) - x)^2 + x^2 - (y^2 - 1)^2) \subset \mathbb{A}^2$, we now have a map $\varphi_2 : C_2 \to C_1$ as

$$(x, y) \mapsto (x, y(y^2 - 1) - x, y^2 - 1)$$

Again, C_2 is singular, since it has singular points at $(0, \pm 1)$.

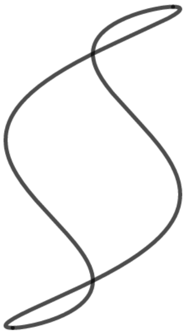


Figure 3.2: $C_2 : (y(y^2 - 1) - x)^2 + x^2 - (y^2 - 1)^2 = 0$

Rewriting our equation for C_2 gives $C_2 : (y^2 - 1)(2xy - (y^2 - 1)^2) - 2x^2 = 0$. Then, from dividing by $-(y^2 - 1)^2$, we obtain

$$2\left(\frac{x}{y^2 - 1}\right)^2 - 2y\left(\frac{x}{y^2 - 1}\right) + y^2 - 1 = 0$$

Therefore, we get the integral element $a = \dfrac{x}{(y^2 - 1)}$ satisfying the relation $2a^2 - 2ya + y^2 - 1 = 0$. We then get Γ''' as the quotient of $k[x, y, a]$ by the ideal generated by

$$\begin{cases} 2x(y(y^2 - 1) - x) - (y^2 - 1)^3 \\ x - a(y^2 - 1) \\ 2a^2 - 2ay + (y^2 - 1) \end{cases}$$

Again, in this ring, we have $x = a(y^2 - 1)$, and substituting this into the first equation gives 0. So we obtain

$$\Gamma''' = k[y, a]/(2a^2 - 2ay + (y^2 - 1)) \tag{3.7}$$

Finally, rewrite (y, a) as (x, y), and since $2y^2 - 2xy + x^2 - 1 = (x - y)^2 + y^2 - 1$, take the curve $C_3 : (x - y)^2 + y^2 = 1 \subset \mathbb{A}^2$, we have the map $\varphi_3 : C_3 \to C_2$ as

$$(x, y) \mapsto (y(x^2 - 1), x) \tag{3.8}$$

One readily sees that C_3 is a smooth ellipse and there is an obvious isomorphism between it and the circle $C_4 : x^2 + y^2 = 1 \subset \mathbb{A}^2$, namely $\varphi_4 : C_4 \to C_3$ as $(x, y) \mapsto (x - y, x)$. Since a circle is isomorphic to $\mathbb{P}^1$, all of this finally shows that the the nonsingular model of the quadrifolium is $\mathbb{P}^1$.

Moreover, recall that the rational parametrization of the circle is given by

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right) \tag{3.9}$$

Then we by finally composing this with the map $\varphi_1 \circ \varphi_2 \circ \varphi_3 \circ \varphi_4$, we obtain the rational parametrization of the quadrifolium $(x^2 + y^2)^3 = 4x^2y^2$ as

$$\left(\frac{8t^2(1 - t^2)}{(1 + t^2)^3}, \frac{-4t(1 - t^2)^2}{(1 + t^2)^3}\right) \tag{3.10}$$

This therefore gives us all the rational point of the quadrifolium. Moreover, using Desmos (or any other plotting software), one can visualize this parametrization, and see how soothing it is to watch!

3.4 Standard Quadratic Transformations

Let $U = \mathbb{P}^2 \setminus V(xyz)$, $P_1 = [1 : 0 : 0]$, $P_2 = [0 : 1 : 0],$, $P_3 = [0 : 0 : 1]$. Consider the map

$$Q : \mathbb{P}^2 \setminus \{P_1, P_2, P_3\} \to \mathbb{P}^2$$
$$Q([x : y : z]) = [yz : xz : xy]$$

Note that for $[x : y : z] \in U$, $Q^2([x : y : z]) = [x^2yz : xy^2z : xyz^2] = [x : y : z]$. So $Q = Q^{-1}$ on U, and $Q|_U : U \to U$ is an isomorphism. Hence Q is a birational map $\mathbb{P}^2 \to \mathbb{P}^2$. We call Q the *standard quadratic transformation*, and for a curve C, we denote by C^Q the curve resulting from this transformation.

In the next section, we give an example where it is helpful to apply a quadratic transformation to a curve to put it in a form with more easily spotted integral elements.

Remark 3.4.1. This is not the intended use of quadratic transformations. Quadratic transformations give us a way to transform singular plane curves into plane curves with "better" (i.e. ordinary) singular points. We have the following theorem, see [F].

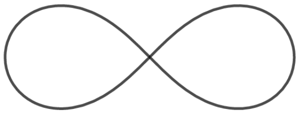
Theorem 3.4.2. *Let C be an irreducible projective plane curve. With a finite number of quadratic transformations, we can transform C into a plane curve with only ordinary multiple points.*

The important thing here is that the final curve is a plane curve. Normalization already gives us a way to remove singularities, but there is no guarantee that the resulting curve is a plane curve. Quadratic transformations are useful in instances where we want a plane curve at the end, and "improving" the singularities is enough.

3.5 Example 3 : Lemniscate of Bernoulli

We will use this new tool to help resolve the singularities of the Lemniscate of Bernoulli, defined as

$$C : (x^2 + y^2)^2 = 2(x^2 - y^2) \subset \mathbb{A}^2 \tag{3.11}$$



We see that C has a singularity at $(0, 0)$, thus we would like to use the same method to resolve this singularity. However, there is no obvious integral element. So we'll try applying a quadratic transformation, and hope that C comes out nicer.

Firstly, projectivising C gives

$$C^* = (x^2 + y^2)^2 - 2z^2(x^2 - y^2) \tag{3.12}$$

Then, applying the standard quadratic transformation gives

$$\begin{aligned} C' := (C^*)^Q &= ((yz)^2 + (xz)^2)^2 - 2(xy)^2((yz)^2 - (xz)^2) \\ &= z^2(z^2(x^2 + y^2)^2 + 2x^2y^2(x^2 - y^2)) \\ &= z^2(x^2 + y^2)^2 + 2x^2y^2(x^2 - y^2) \end{aligned} \tag{3.13}$$

Note we can drop the z^2 since we only consider C' on $U = \mathbb{P}^2 \setminus V(xyz)$. We now deprojectivize C' to resolve its singularities. The reader can check that there is a singularity at $[0 : 1 : 0]$, so we deprojectivize with respect to y to get

$$C'_* = z^2(x^2 + 1)^2 + 2x^2(x^2 - 1) \tag{3.14}$$

to obtain an affine curve singular at the origin. Then, $\Gamma(C'_*)$ has the integral element

$$w = \frac{z(x^2 + 1)}{\sqrt{2}x}, \tag{3.15}$$

satisfying the relation $w^2 = 1 - x^2$. This element w makes a $\sqrt{(2)}$ appear, which makes our map no longer defined over $\mathbb{Q}$. Although, this not a problem, since we will clear out this square root in a moment and come back to $\mathbb{Q}$. One may do this resolution without the need to extend $\mathbb{Q}$ to $\mathbb{Q}[\sqrt{(2)}]$, the end result is the same.

Then, we obtain the coordinate ring

$$\Gamma(C'_*)[w] = k[x, z, w]/(z^2(x^2 + 1)^2 + 2x^2(x^2 - 1), \sqrt{2}xw - z(x^2 + 1), w^2 + x^2 - 1) \tag{3.16}$$

and using similar computations as in our previous example, one can reduce it to

$$k[x, z, w]/(\sqrt{2}xw - z(x^2 + 1), w^2 + x^2 - 1) \tag{3.17}$$

Hence C is birationally equivalent to $C'' = V(\sqrt{2}xw - z(x^2+1), w^2+x^2-1) \subset \mathbb{A}^3$. Furthermore, note that there is no point on C'' such that $x^2+1=0$ (otherwise $w^2=2$, and then $\pm 2i = 0$). Hence, in the coordinate ring, we have

$$z = \frac{\sqrt{2}xw}{x^2+1}, \tag{3.18}$$

All of this gives us the map from $V(x^2+y^2-1)$ to C'' defined by

$$(x,y) \mapsto \left(x, \frac{\sqrt{2}xy}{x^2+1}, y\right) \tag{3.19}$$

Again, recall that we know the rational parametrization of the circle $V(x^2+y^2-1)$ is given by

$$t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \tag{3.20}$$

A straightforward calculation composing all these operations gives a parametrization for the Lemniscate of Bernoulli:

$$\left(\frac{\sqrt{2}t(1+t^2)}{1+t^4}, \frac{\sqrt{2}t(1-t^2)}{1+t^4}\right) \tag{3.21}$$

Because of the $\sqrt{2}$ this is not a rational map, but sending $t \mapsto \sqrt{2}t$ gives

$$\left(\frac{2t(1+2t^2)}{1+4t^4}, \frac{2t(1-2t^2)}{1+4t^4}\right) \tag{3.22}$$

Since a birational equivalence only requires an isomorphism on an open subset of C and $\mathbb{P}^1$, we don't need to worry about what happened to the points at infinity. Namely, there is no issue with projectivising and then deprojectivising C. All of this proves that the nonsingular model of C is $\mathbb{P}^1$, and this parametrization gives all the rational solutions of Bernoulli's Lemniscate.

Chapter 4

Tower of Modular Curves $X_0(3^n)$

Let's consider the model given in [E] of the tower of modular curves $X_0(3^n)$, described in chapter 2. For $n \geq 2$, we have $X_0(3^n)$ birationally equivalent to the curve in $(\mathbb{P}^1)^{n-1}$ defined by the $n-2$ equations

$$(x_i^3 - 1)(z_{i+1}^3 - 1) = 1, \text{ where } z_i = \frac{x_i + 2}{x_i - 1}$$

for $i = 1, \ldots, n-2$.

This model is singular, hence it is not completely isomorphic to $X_0(3^n)$. To avoid confusion, we will refer to the model above by E_{3^n} and denote these $n-2$ equations as $F^{(i)}(x_i, x_{i+1}) = (x_i^3 - 1)(z_{i+1}^3 - 1) - 1$.

Remark 4.0.1. Clearly, each of the rational expressions $F^{(i)}$ lies in $\mathbb{C}(x_1, \ldots, x_{n-1})$. However, since they only depend on x_i and x_{i+1}, we write $F^{(i)}(x_i, x_{i+1})$ instead of $F^{(i)}(x_1, \ldots, x_{n-1})$. Moreover, the z_{i+1} can be seen as just a change of variable from x_{i+1} to $\frac{x_{i+1}+2}{x_{i+1}-1}$.

We will first find these singularites and try to understand as much as possible how they affect the structure of both E_{3^n} and $X_0(3^n)$. However, before starting, we need to specify one important feature of the model E_{3^n}.

Remark 4.0.2. This is the first instance where we see how the image of the cusps of $X_0(3^n)$ affects the behavior of E_{3^n}. In the previous chapter, we pointed out how the values $1, \zeta_3, \zeta_3^2$ and ∞ are important for the coordinates x_i. Doing some simple computations, one can see that if a point $P \in E_{3^n}$ has one coordinate $x_i = \zeta_3^k$, for some $i = 1, \ldots, n-1$ and $k = 1, 2$, then $x_j = \infty$ for all $j < i$, and $x_j = 1$ for all $j > i$. We will denote these special points as

$$P_{i,k} = (\infty, \ldots, \infty, \zeta_3^k, 1, \ldots, 1) ,$$

where ζ_3^k is at the i-th position. By abusing notation modulo 3, we may say, when considering $P_{i,k}$, that the other one is $P_{i,2k}$.

Moreover, these are almost the only points involving coordinates equal to ∞ and 1. The only others are the 2 points

$$P_0 = (1, 1, \ldots, 1) \ ; \ P_\infty = (\infty, \ldots, \infty)$$

In the spirit of P_0, lets rename $P_{1,1}$ and $P_{1,2}$ as P_1 and P_2 respectively, so that in general we have

$$P_e = (\zeta_3^e, 1, \ldots, 1) \ , \text{ for } e = 0, 1, 2$$

4.1 Singularities of Elkies Models

Recall that to find singular points of a curve, we need to look at the rank of its Jacobian. For E_{3^n}, differentiate each F_i by x_i and z_{i+1}, to obtain

$$J_n = \begin{pmatrix} F^{(1)}_{x_1} & F^{(1)}_{z_2} & 0 & \cdots & \cdots & 0 \\ 0 & F^{(2)}_{x_2} & F^{(2)}_{z_3} & \cdots & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \cdots & 0 \\ 0 & 0 & \cdots & F^{(n-3)}_{x_{n-3}} & F^{(n-3)}_{z_{n-2}} & 0 \\ 0 & 0 & \cdots & 0 & F^{(n-2)}_{x_{n-2}} & F^{(n-2)}_{z_{n-1}} \end{pmatrix}, \tag{4.1}$$

where all the partial derivatives are of the forms

$$F^{(i)}_{x_i}(x_i, z_{i+1}) = 3x_i^2(z_{i+1}^3 - 1)$$

$$F^{(i)}_{z_{i+1}}(x_i, z_{i+1}) = 3z_{i+1}^2(x_i^3 - 1)$$

Given $P \in E_{3^n}$, since J_n is an $n-2 \times n-1$ matrix, we know $\operatorname{rank}(J_n(P)) < n-2$ if and only if all its $n-2 \times n-2$ submatrices (i.e. when we remove any one row) have determinant 0 at P. It turns out that only looking at the one where we removed the last row, say M, will be sufficient. Since M is diagonal, we know it has determinant 0 exactly when $F^{(i)}_{x_i} = 0$ for some $i = 1, \ldots, n-2$. Thus, we must have $x_i = 0$ or $z_{i+1}^3 = 1$, i.e. x_{i+1} is equal to ζ_3, ζ_3^2 or ∞.

Case $x_i = 0$ **:** We obtain that $x_{i+1} = -2$, which gives both $F^{(i)}_{x_i}(0, -2) = F^{(i)}_{x_{i+1}}(0, -2) = 0$. This means that the i-th line of the J_n is zero, hence it's a singular point. In the next section, they will be studied in depth.

Case $x_{i+1} = \zeta_3$**,** ζ_3^2**,** ∞ **:** We are dealing with $P = P_{i,k}$ from Remark 4.0.2 for some $i = 1, \ldots, n-2$ and $k = 1, 2$. To see which of these are actually singular, we need to evaluate the partial derivatives at every significant pairs, i.e, $(\infty, \infty), (\infty, \zeta_3^k), (\zeta_3^k, 1)$ and $(1, 1)$.

Evaluating these requires precaution as they can lead to indefinite forms like $0 \times \infty$ or simply a derivative equal to ∞, which doesn't mean anything. Again, considering the polynomial $F^{(i)}$ as depending on (x_i, z_{i+1}) instead of (x_i, x_{i+1}) simplifies the computations significantly. By changing affine patch appropriately, one obtains

(x_i, x_{i+1})	(x_i, z_{i+1})	$F^{(i)}_{x_i}(x_i, z_{i+1})$	$F^{(i)}_{z_{i+1}}(x_i, z_{i+1})$
(∞, ∞)	$(\infty, 1)$	0	-3
(∞, ζ_3^k)	(∞, ζ_3^{2k})	0	$-3\zeta_3^k$
$(\zeta_3^k, 1)$	(ζ_3^k, ∞)	$-3\zeta_3^{2k}$	0
$(1, 1)$	(∞, ∞)	-3	0

Therefore, in general, we have the Jacobian

$$J_n(P_{i,k}) = \begin{pmatrix} 0 & -3 & 0 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & -3 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & & 0 & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & -3 & 0 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & -3\zeta_3^k & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & -3\zeta_3^{2k} & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 & -3 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 0 & 0 & 0 & & & -3 & 0 \end{pmatrix} \tag{4.2}$$

where the entries $-3\zeta_3^k$ and $-3\zeta_3^{2k}$ are both on the i-th column, and respectively on the $(i-1)$-th and i-th row. Moreover, this gives us that the Jacobian of P_e, for $e = 0, 1, 2$, and P_∞ are

$$J_n(P_e) = \begin{pmatrix} -3\zeta_3^{2e} & 0 & 0 & \dots & 0 \\ 0 & -3 & 0 & \dots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \dots & & -3 & 0 \end{pmatrix} \text{ and } J_n(P_\infty) = \begin{pmatrix} 0 & -3 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & -3 \end{pmatrix} \tag{4.3}$$

It follows readily that the only singular points of this type are the points $P_{i,k} \in E_{3^n}$, where $i = 2, \dots, n-2$ and $k = 1, 2$. The behavior of these curves E_{3^n} around those points, as we'll see in section 4.3, fundamentally dictates the ramification of $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$.

4.2 Resolution of Singularities on Elkies Models

Let us study the singularities of the form $P = (\dots, 0, -2, \dots) \in E_{3^n}$, found in the previous section. Understanding the geometry of E_{3^n} near them will help us later on. Moreover, resolving such singularity is fairly straightforward in general, and yields surprising relations between modular curves with Fermat curves.

Let $P = (x_1, \dots, x_{n-1}) \in E_{3^n}$ such that $(x_i, x_{i+1}) = (0, -2)$, for some $i = 1, \dots, n-2$. In this case, the i-th row of $J_n(P)$ is null. One easily sees that the other rows of this Jacobian are linearly independent, thus the surface defined by $F^{(1)}, \dots, F^{(i-1)}, F^{(i+1)}, \dots, F^{(n-2)}$ has a well-defined tangent plane T at P. It is given by the kernel of $J(P)$, after removing the row full of 0's. Then, the local geometry of E_{3^n} at this point is given by the intersection of this plane with the tangent branches, at P, of the singular variety defined by $F^{(i)}(x_i, x_{i+1}) = 0$.

To find these branches, we use a theory developped in [F]. Let $C \subset \mathbb{P}^2$ be plane curve, defined by some polynomial $F \in k[x, y]$, where k is some algebraically closed field. Say C is singular at some point $P \in C$. By doing a change of variable, we can always assume $P = (0, 0)$. Then, the form F_m of lowest degree in F has degree $m > 1$. Since k is algebraically closed, we can factorize $F_m = \epsilon \prod_{i=1}^{m} L_i$ into irreducible linear components $L_i = a_i x + b_i y$, with $a_i, b_i \in k$. The branches of C, the lines $L_i = 0$, are not necessarily all distincts.

In our case, $F^{(i)}$ only depends on two variables, hence it does define a plane curve. Working in terms of variables (x_i, z_{i+1}) is again more conveniant. Then, the singularity of $F^{(i)}$ passes from $(0, -2)$ to $(0, 0)$ and looking at the form of lowest degree gives us

$$z_{i+1}^3 - x_i^3 = (z_{i+1} - x_i)(z_{i+1} - \zeta_3 x_i)(z_{i+1} - \zeta_3^2 x_i) \ . \tag{4.4}$$

Then, one embeds these lines of $\mathbb{P}^1 \times \mathbb{P}^1$ in $(\mathbb{P}^1)^{n-1}$ to obtain three hyperplanes. Trivially, their intersection with our tangent plane T gives three simple lines, hence E_{3^n} has three distinct tangent lines at P. It follows that these singularities are ordinary triple points, which implies that when resolving any one of them, the point will separate into exactly three distinct smooth points. Locally, the resolution of singularity will look similar to the example of the Nodal Curve from section 3.2, and the three branches will simply be pulled apart. To see this, one may refer section 7.2 and 7.3 of [F] to see exactly how one can algebraically separate distinct tangents of ordinary multiple points.

Let us try to resolve such singularities for $n = 3$, i.e. E_{27}. This is certainly an interesting case as it is given by a single equation and $P = (0, -2)$ is its only singular point. Thus, resolving the singularity at P will give a nonsingular model C_{27} of E_{27}. But recall that by definition, $X_0(27)$ is a smooth model of E_{27}. Since this model is unique up to isomorphism, this resolution process will let us conclude $X_0(27) \cong C_{27}$

Remark 4.2.1. This type of singularities $(\dots, 0, -2, \dots)$ are easy to resolve in general, and one can apply the same argument as we will now present on any of them. The other coordinates do not affect anything, the algebra is almost identical, with the only exception that we have some other polynomials to carry.

As in the previous chapter, one could try to resolve the singulary at P by normalization, and that is how I originally obtained the following result. However, by inspection, one can actually directly find the smooth model. Recall that E_{27} is given by $(x^3 - 1)(y^3 - 1) = 1 \subset \mathbb{P}^1 \times \mathbb{P}^1$, where here we renamed x_1 and z_2 to x and y respectively. Rearranging the equation gives $E_{27} : x^3 y^3 = x^3 + y^3$. Then, consider $F_3 : z^3 = x^3 + y^3$, the Fermat cubic curve. We have a rational map $\varphi : F_3 \to E_3$ as

$$[x : y : z] \mapsto \left(\frac{z}{x}, \frac{z}{y} \right) \tag{4.5}$$

Firstly, observe that this map does send points of F_3 to E_3. Let $P = [x : y : z] \in F_3$. If $x = 0$ (resp. $y = 0$), then $\varphi_3(P) = (\infty, 1)$ (resp. $(1, \infty)$), which is a point of E_3. For every other point with $x, y \neq 0$, hence

$$z^3 = x^3 + y^3 \Rightarrow (z \cdot z)^3 = (z \cdot y)^3 + (z \cdot x)^3 \Rightarrow \left(\frac{z \cdot z}{x \cdot y} \right)^3 = \left(\frac{z}{x} \right)^3 + \left(\frac{z}{y} \right)^3 \tag{4.6}$$

namely, $\varphi_3(P) \in E_3$. Moreover, when $x, y, z \neq 0$, this map is invertible with $\psi : E_3 \to F_3$ as

$$(x, y) \mapsto [y : x : xy] \tag{4.7}$$

It follows that φ is invertible, except at finitely many points of F_3, i.e. is a birational map from $F_3 \to E_3$. But one readily sees that F_3 is smooth everywhere. Therefore, we found an explicit nonsingular model of E_3 which, as explained above, proves

$$X_0(27) \cong x^3 + y^3 = z^3 \tag{4.8}$$

Remark 4.2.2. This link between modular curve and Fermat curve is in no way trivial. The sudden appearance of Fermat curves is actually quite surprising. Moreover, the model Elkies gives for $X_0(8)$ and $X_0(64)$ are almost identical, and one can apply the same argument to obtain

$$X_0(8) \cong x^2 + y^2 = z^2 \cong \mathbb{P}^1 \ ; \ X_0(64) \cong x^4 + y^4 = z^4 \tag{4.9}$$

But for $n = 5$, $X_0(125) \ncong x^5 + y^5 = z^5$. For instance, their respective geni are not equal. However here, this marvelous relation enables us to draw the following results.

Theorem 4.2.3. *There exists infinitely many elliptic curves with a rational subgroup of order 8.*

Proof. Since $F_2 : x^2 + y^2 = z^2$ is a smooth curve of degree 2 (hence of genus 0) with a rational point, it must be isomorphic to $\mathbb{P}^1$, hence $X_0(8) \cong F_2 \cong \mathbb{P}^1$ over $\mathbb{Q}$. Since $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$ has infinitely many rational points (i.e. $\mathbb{Q} \subset \mathbb{P}^1$), using the moduli interpretation yields our results. □

Remark 4.2.4. Looking closer at the isomorphism $\mathbb{P}^1 \to F_2$, the birational morphism $F_2 \to E_2$, and the birational morphism $\pi : X_0(8) \to E_2$ that Elkies constructs, one could compose all these maps and find our isomorphism $\mathbb{P}^1 \to X_0(8)$. This would give an explicit parametrization of all these elliptic curves! However, elliptic curves with rational subgroups of order 27 suffer a different fate.

Theorem 4.2.5. *There exists a unique elliptic curve with a rational subgroup of order 27.*

Proof. Using the moduli interpretation, it suffices to show that all rational solutions of F_3, but one, represent cusps of $X_0(27)$. Since both $X_0(27)$ and F_3 are smooth moduls for E_3, we know there exists an isomorphism $f : X_0(27) \to F_3$ such that the following diagram commutes :

$$\begin{tikzcd}
X_0(27) \arrow[r, "f"] \arrow[rd, "\pi"] & F_3 \arrow[d, "\varphi_3"] \\
 & E_3
\end{tikzcd}$$

Therefore, a point $P \in F_3$ represents a cusp if and only if $\varphi_3(P) = \pi(Q)$, some cusp Q of $X_0(27)$. However as seen at the end of Chapter 2 when discussing the construction of the Elkies' model for $X_0(3^n)$, we know $Q \in X_0(27)$ is a cusps if and only if $\pi(Q)$ is a point at infinity of E_3. Thus, we simply have to answer the following question : If $P \in F_3$ is defined over $\mathbb{Q}$, is $\varphi_3(P)$ a point at infinity of E_3?

But this part is rather easy to answer. Fermat's Last Theorem tells us that F_3 only has trivial rational solutions, i.e.

$$P_1 = [1 : 0 : 1], \; P_2 = [0 : 1 : 1] \text{ and } P_3 = [1 : -1 : 0] \tag{4.10}$$

Then, evaluating φ at these points gives

$$\varphi_3(P_1) = (1, \infty), \; \varphi_3(P_2) = (\infty, 1) \text{ and } \varphi_3(P_3) = (0, 0) \tag{4.11}$$

which is exactly what we wanted. □

This shows that there exists a unique elliptic curve having a rational subgroup of order 27, but it even tells us which one! It is the unique point $P \in X_0(27)$ such that $f(P) = P_3$. Finding this point would require us to further investigate the behavior of $\pi : X_0(27) \to E_3$. We won't continue in that direction but it is rather interesting that mathematicians, using different tools, actually found it. The unique elliptic curve having a rational subgroup of order 27 is

$$y^2 + y = x^3 - 270x - 1708 \tag{4.12}$$

4.3 Ramification of π_0

Let us now solely focus on the map $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$. From Remark 2.7, we can see this map in terms of the models E_{3^n}, in which case it is given by $\pi_0 : E_{3^n} \to E_{3^{n-1}}$ as

$$(x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-2}) \tag{4.13}$$

As we have seen, this map is of degree 3. We will try to find the ramification points of π_0 and compute their ramification index. We will study $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$, using the map $\pi_0 : E_{3^n} \to E_{3^{n-1}}$. This will be achieved by finding all the points of $E_{3^{n-1}}$ whose preimage has cardinality less than 3, and then deciding which of these corresponds to ramification points on the desingularisation $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$. As easy as this first matter will be, the second will certainly reveal itself to be more difficult as it will require some deep understanding of the local geometry around singularities of E_{3^n}.

Remark 4.3.1. To clarify what is meant here, consider the projective nodal curve $C : y^2 = x^2(x+1) \subset \mathbb{P}^2$ and the polynomial map $\alpha' : C \to \mathbb{P}^1$ as $(x, y) \mapsto x$. The curve C is easily seen to have a single point at infinity, say R, which is mapped to $\infty \in \mathbb{P}^1$. We see that this map as degree 2, and the only ramified point are clearly $P = (0, 0)$ and $Q = (-1, 0)$ and our point R.

However, as we have seen in section 3.2, the resolution of singularity at P gives that its smooth model is $\mathbb{P}^1$. It gives the modification $\varphi : \mathbb{P}^1 \to C$ found in (3.2). The resolution pulled appart its two distinct tangent to give 2 distinct points in its smooth model, i.e. "resolved the ramification" as well. However, one might have realized that Q and R are still ramified, with ramification index 2, in the nonsingular model. Therefore, by studying α', we were able to find the ramification of the map $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$

$$\begin{tikzcd}
\mathbb{P}^1 \arrow[r, "\varphi"] \arrow[dr, "\alpha"'] & C \arrow[d, "\alpha'"] \\
& \mathbb{P}^1
\end{tikzcd}$$

Given α directly, this problem would have been completely trivial. However, we will perform a similar inspection to $\pi_0 : E_{3^n} \to E_{3^{n-1}}$ to study $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$, respectively in the role of α' and α.

Our main goal is to be able to use the Riemann-Hurwitz formula. It states that for any finite morphism $\varphi : C_1 \to C_2$, where both C_1, C_2 are smooth projective curves, then

$$(2g(C_1) - 2) = \deg(\varphi) \cdot (2g(C_2) - 2) + \sum_{P \in C_1} (e_P - 1) \tag{4.14}$$

The quantity $g(C_i)$ is the genus of C_i and e_P is the ramification index of $P \in C_1$. However, this formula requires smooth varieties, such as $X_0(3^n)$ and $X_0(3^{n-1})$.

We will see in a moment that the ramification points always can only have index 1 or 3 in π_0. Then, using the fact that $X_0(9) \cong \mathbb{P}^1$, i.e. $g(X_0(9)) = 0$, we will be able to write the genus for the curves for the whole tower $X_0(3^n)$ recursively as

$$g(X_0(3^n)) = 3g(X_0(3^{n-1})) + m - 2 \tag{4.15}$$

where m is the number of ramification points of $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$.

4.3.1 Structure of fibers of π_0 using Galois theory

Note that in our next section, we will explicitely find the ramification index of all our points on these modular curves. However, it is satisfying to see that we can compute it by only using group theory. To show that the ramification index of the map $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$ can only be equal to 1 or 3, it suffices to prove that π_0 provides a Galois cover of $X_0(3^{n-1})$ by $X_0(3^n)$.

Namely, one has to show that for any points $P \in X_0(3^{n-1})$, there exists a transitive action on the fiber of P. Using Galois theory, this follows if $\Gamma_0(3^n)$ is normal in $\Gamma_0(3^{n-1})$. To show that the latter holds true, one can use principal congruence subgroups. Since the principal congruence subgroup $\Gamma(3^{n-1})$ is normal in $\Gamma_0(3^{n-1})$, it suffices to show that the principal congruence subgroup $\Gamma(3^n)$ is normal in $\Gamma(3^{n-1})$. Since they are both finite groups and $[\Gamma(3^{n-1}) : \Gamma(3^n)] = 3$ is the smallest prime dividing the order of $\Gamma(3^{n-1})$, the following proposition proves our claim.

Proposition 4.3.2. *Let G be a finite group and $H < G$, a subgroup. If $[G : H] = p$, where p is the smallest prime dividing $|G|$, then H is a normal subgroup.*

Proof. Let G act on G/H via the coset representation. Then, we obtain an homomorphism

$$\tau : G \to \sum_{G/H} \text{ as } g \mapsto \tau_g \tag{4.16}$$

where $\tau_g(g'H) = (gg')H$, for all cosets $g'H \in G/H$. Then, clearly, if $g \in \ker(\tau) =: K$, we have

$$gH = \tau_g(H) = H \Rightarrow g \in H \Rightarrow K \subset H \tag{4.17}$$

Since $K \lhd G$, we can prove our claim by showing that in fact $K = H$. To achieve this, it suffices to show that K has the same index as H in G, as we already know $K \subset H$, and we are dealing with finite groups.

Observe that from the First Isomorphism Theorem, we may identify $G/K \cong \operatorname{Im}(\tau)$ as a subset of $\sum_{G/H} \cong S_p$, where we recall $p = [G : H]$. Therefore, $[G : K]$ divides $p!$. But since $[G : K]$ also divides $|G|$, it follows that $[G : K]$ divides $\gcd(p!, |G|) = p$. This last equation holds true because every other divisor of $p!$ is divisible by some integer $1 < n < p$, hence can't divide $|G|$ by hypothesis. Therefore, $[G : K] = 1$ or p. But it can't be equal to 1, as otherwise $K = G \Rightarrow H \supset K = G \Rightarrow H = G \Rightarrow [G : H] = 1$, contradiction. Thus, $[G : K] = p = [G : H]$, which proves our claim. □

4.3.2 Genus of $X_0(3^n)$

Given any point $P = (x_1, \ldots, x_{n-2}) \in E_{3^{n-1}}$, its fiber $\pi_0^{-1}(P)$ contains exactly the elements of the form $Q_i = (x_1, \ldots, x_{n-2}, x_{n-1})$, where the x_{n-1} is one of the three solutions of

$$(x_{n-2}^3 - 1)(z_{n-1}^3 - 1) = 1 \iff z_{n-1}^3 = \frac{x_{n-2}^3}{x_{n-2}^3 - 1} \tag{4.18}$$

It follows readily that z_{n-1} has less than 3 distinct solutions if and only if the RHS evaluates to 0 or ∞, in which case it has only one solution. Since the correspondence $x_{n-1} \leftrightarrow z_{n-1}$ is one-to-one, this shows that ramification happens exactly when $x_{n-2} = 0$ or $x_{n-2} = \zeta_3^e$, $e = 0, 1, 2$. These are our "special values of ramification".

If $x_{n-2} = 0$, then P lies below the singular point $Q = (x_1, \ldots, x_{n-3}, 0, -2)$. As we have seen in the previous section, Q has three distinct simple tangents. Namely, if one resolves the singularities at each of these points, the same thing will happen as in the example of the nodal curve in section 3.2, and the three tangents will simply be pulled appart. This will outburst three distinct points in the smooth model, no longer ramified.

This case is of no interest in the actual ramification of $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$. We will soon draw a modelisation of the ramification behavior in this tower, and these points won't make an appearance, as there is nothing more to say about them in this regard.

The cases $x_{n-2} = 1$, ζ_3, ζ_3^2, on the other hand, will create "towers of ramification". Observe that these cases involve our points $P_{i,k}$, P_e and P_∞. Just to make the notation slightly more precise (but heavier), let's now denote them as $P_{i,k}^{(n)}$, $P_e^{(n)}$ and $P_\infty^{(n)}$, all in E_{3^n}, to specify in which of these curves they are.

If $x_{n-2} = 1$, we must have $P = P_{i,k}^{(n-1)}$, for some $i < n-2$, and its fiber is therefore $P_{i,k}^{(n)}$, for the same value of i. Similarly, if $x_{n-2} = \zeta_3^k$, $k = 1, 2$, then we are dealing with $P = P_{n-2,k}^{(n-1)}$, and its fiber is $P_{n-2,k}^{(n)}$.

What is interesting is how this interacts with the rest of tower. For instance, no matter which cube root of unity x_{n-2} is, it always leads to $x_{n-1} = 1$. Since this is again a "special value of ramification", the ramification is then carried over in $\pi_0 : E_{3^{n+1}} \to E_{3^n}$. By induction, this is carried over in all $\pi_0 : E_{3^m} \to E_{3^{m-1}}$ for all $m \geq n$, and this is what what is by a "tower of ramification".

Pictorially, we represent this situation by only writing the last coordinate of every point. Its other coordinates are obvious by looking at the points below it.

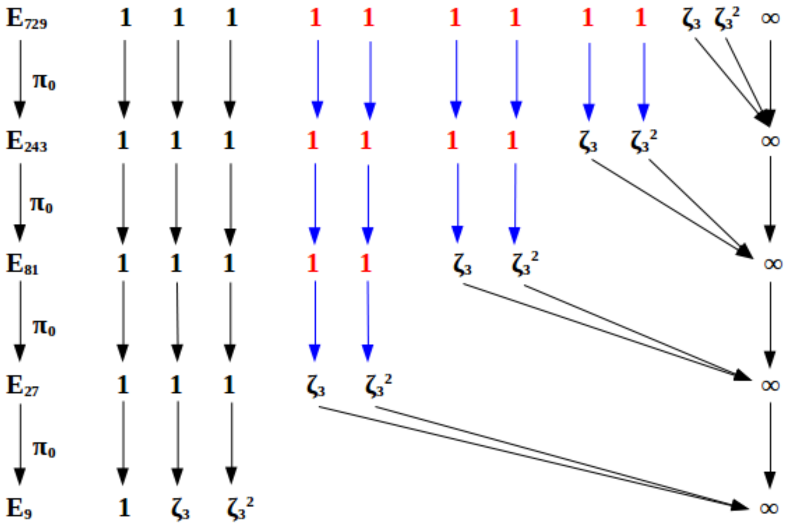


Figure 4.1: Ramifications behavior in the tower E_{3^n}

As indicated by the different colors, the red points are singular points found in the previous sections. Thus, we now need to study the behavior of these blue fibers : Do they act like the nodal curve example or differently? To figure it out, one can always try to resolve these singularities directly but it turns out to be much more complicated than our previous examples. Instead, let us study the local geometry of $P_{i,k}^{(n)} = (\infty, \ldots, \infty, \zeta_3^k, 1, \ldots, 1) \in E_{3^n}$, for some $i = 2, \ldots, n-2$.

To do so, one usually computes the *formal completion* of the local ring $\mathcal{O}_{P_i}(E_{3^n})$. This simply means that we allow ourselves the use of infinite power series, without having to worry about if it converges or not. Algebraically, this let us focus solely on our point and zoom in on the curve to forget about everything else.

To see that, let us first consider a toy example. We will show that around the origin, the curve $C : y^2 = x^2(x+1)$ looks like $V : xy = 0$. To see this, solve y as a function of x, i.e. $y = x\sqrt{x+1}$. Previously, we couldn't make sense of this square root, but now with the usage of power serie, one may check that

$$x\sqrt{1+x} = \sum_{n=0}^{\infty} \frac{(-1)^n(2n)!}{(1-2n)(n!)^2(4^n)} x^{n+1} \tag{4.19}$$

By denoting this power serie as $u(x)$, we have that the formal completion of the coordinate ring of C is

$$\mathbb{C}[[x,y]]/((y-u(x))(y+u(x))) \ , \tag{4.20}$$

where the double brackets [[ ]] mean that we allow infinite power series. This ring looks exactly the same as $\mathbb{C}[[x,y]]/(xy)$, exposing their similarty at the origin.

Let us now compute the formal completion of our curve E_{3^n} around our point

$$P_{i,k}^{(n)} = (\infty, \ldots, \infty, \zeta_3^k, 1, \ldots, 1)$$

where the ζ_3^k is at the i-th coordinate and $k = 1, 2$. To do so, one needs to apply a change of coordinates to send the point of interest at the origin. Thus, take $y_j = 1/x_j$ for $j < i$, $y_i = x_i - \zeta_3^k$ and $y_j = 1/z_j$ for $j > i$. Note that in the example above with the nodal curve, one writes y in terms of x to describe the local geometry around the origin. However, we can't always pick arbitrarily one coordinate and write all the others in terms of it.

For instance, in the previous example, we wrote y as a power serie of degree 1 (i.e. its lowest term has degree 1) in x. However, if it had degree $n > 1$, then it wouldn't be possible to write x as a power serie in y. This will be particularly important in our case.

Indeed, using Elkies equations $F^{(j)} = 0$, which relates y_j and y_{j+1}, we may write both of these coordinates as an expression with respect to the other, and obtain

$j < i-1$	$y_{j+1} = \dfrac{1-(1-y_j^3)^{1/3}}{1+2(1-y_j^3)^{1/3}}$	$y_j = \left(1 - \left(\dfrac{1-y_{j+1}^3}{1+2y_{j+1}^3}\right)^3\right)^{1/3}$
$j = i-1$	$y_i = \dfrac{1+2\zeta_3^k(1-y_{i-1}^3)^{1/3}}{1-\zeta_3^k(1-y_{i-1}^3)^{1/3}} - \zeta_3^k$	$y_{i-1} = \left(1 - \left(\dfrac{y_i+\zeta_3^k-1}{y_i+\zeta_3^k+2}\right)^3\right)^{1/3}$
$j = i$	$y_{i+1} = \left(1-(y_i+\zeta_3^k)^{-3}\right)^{1/3}$	$y_i = \zeta_3^k \left(\dfrac{1}{1-y_{i+1}^3}\right)^{1/3} - \zeta_3^k$
$j > i$	$y_{j+1} = \left(1 - \left(\dfrac{1-y_j}{1+2y_j}\right)^3\right)^{1/3}$	$y_j = \dfrac{1-(1-y_{j+1}^3)^{1/3}}{1-(1+2y_{j+1}^3)^{1/3}}$

(4.21)

Remark 4.3.3. Note that expressions such as $(1-y)^{1/3}$ will now become infinite power series. We may multiply all its coefficient by a cube root of unity to get a similar infinite power series. However, after such rescaling, the expressions above containing $(1-y)^{1/3}$ might no longer be satisfied by $(y_j, y_{j+1}) = (0,0)$. We need to worry about this issue in the cases for $j < i$ when writing y_{j+1} in terms of y_j (the 2 cases in the top left corner), and $j \geq i$ when writing y_j in terms of y_{j+1} (the 2 cases on the bottom right). Then only one of the three possible power series will be valid. However, for the other four cases, all three power series are valid.

Writting these power series explicitely, one easily sees that y_j has degree 3 w.r.t. to y_{j-1}, for all $j \leq i$, and y_j has degree 3 w.r.t. y_{j+1}, for all $j \geq i$. Thus, one can always write y_j in terms of y_{j-1} for $j \leq i$, but this is no longer possible when $j > i$. However, by induction, $\deg_{y_1}(y_i) = 3^{i-1}$, hence $\deg_{y_1}(y_{i+1}) = 3^{i-2}$. Thus, one may write y_{i+1} as a power serie in y_1. In fact, we have the following chart

coordinates	y_1	y_2	$\dots$	y_{i-1}	y_i	y_{i+1}	$\dots$	y_{n-1}
$\deg_{y_1}$	1	3	$\dots$	3^{i-2}	3^{i-1}	3^{i-2}	$\dots$	3^{2i-n}

which shows that one can write all coordinates $y_1, \dots, y_{n-1}$ in terms of y_1, provided $n \leq 2i$. Namely, in the values of the coordinates of $P_{i,k}^{(n)}$, we require at most as many ending 1's as the number of leading ∞'s. Conversely, if there are more 1's than ∞'s, then one simply needs to write everything in terms of y_{n-1} since the following chart is also valid

coordinates	y_{n-1}	y_{n-2}	$\dots$	y_{i+1}	y_i	y_{i-1}	$\dots$	y_1
$\deg_{y_{n-1}}$	1	3	$\dots$	3^{n-i-1}	3^{n-i}	3^{n-i-1}	$\dots$	3^{n-2i}

We will soon consider these two cases distinctively but first, let us look at a specific example. Consider $P_{4,1}^{(6)} = (\infty, \infty, \infty, \zeta_3, 1) \in E_{729}$, and rewrite all y_j in terms of y_1, using (4.21) for $i = 4$. But recall that from Remark 4.3.3, we know y_5 can be written in three different ways in terms of y_4 (depending on which cube root is taken). Hence, one obtains

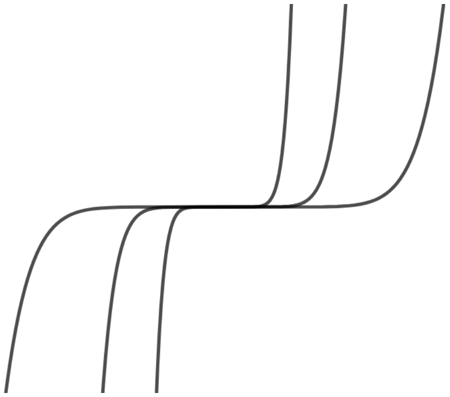
$$\begin{aligned}
y_2 &= \frac{1}{9}y_1^3 + \frac{5}{81}y_1^6 + \frac{31}{729}y_1^9 + \frac{212}{6561}y_1^{12} + \dots \\
y_3 &= \frac{1}{6561}y_1^9 + \frac{5}{19683}y_1^{12} + \frac{56}{177147}y_1^{15} + \dots \\
y_4 &= \frac{1}{847288609443}y_1^{27} + \frac{5}{847288609443}y_1^{30} + \frac{131}{7625597484987}y_1^{33} + \dots \\
y_5 &= -\zeta_3^e \cdot \zeta_9^2(1+\zeta_3) \cdot \left(\frac{1}{6561}y_1^9 + \frac{5}{19683}y_1^{12} + \frac{56}{177147}y_1^{15} + \dots \right) \text{ , for } e = 0, 1, 2.
\end{aligned}$$

Note that we may forget the higher order term since they do not affect the local geometry. It is for the exact same reason that we were able to find the tangents of a plane curve at the origin by looking at the form of the lowest degree in the polynomial defining the curve. Moreover, omitting them doesn't change anything to the following result, it is just longer and messier to write if one keeps them.

We may now conclude that the formal completion of the coordinate ring at this point is

$$\begin{aligned}
&\mathbb{C}[[y_1, \dots, y_5]] / \left(y_2 - \frac{1}{9}y_1^3, y_3 - \frac{1}{6561}y_1^9, y_4 - \frac{1}{847288609443}y_1^{27}, \prod_{e=0}^{2} \left(y_5 + \zeta_3^e \cdot \frac{\zeta_9^2(1+\zeta_3)}{6561}y_1^9 \right) \right) \\
&\cong \mathbb{C}[[x, y]] / \left(\prod_{e=0}^{2} \left(y + \zeta_3^e \cdot \frac{\zeta_9^2(1+\zeta_3)}{6561}x^9 \right) \right)
\end{aligned}$$

This means that locally, the curve looks like



where these are 3 curves of degree 9. The nonsingular model here is trivial : it is simply 3 lines. They each send $t \mapsto (t, -\zeta_3^e \cdot \frac{\zeta_9^2(1+\zeta_3)}{6561} t^9)$ for some $e = 0, 1, 2$. Thus, when resolving the singularity $P_{4,1}^{(6)}$ on E_{729}, one obtains 3 distinct simple points. Clearly, the same holds for $P_{4,2}^{(6)}$

Claim : For any $P_{i,k}^{(n)} \in E_{3^n}$ where $n \leq 2i$, when resolving the singularity, it separates into 3^{n-i-1} distinct points. However, for any $n \geq 2i$, it constantly gives 3^{i-1} distinct simple points.

If $n \leq 2i$, we may write everything in terms of y_1. As above, every y_j for $j \leq i$, one simply obtains $y_j = c_j \cdot y_1^{3^{j-1}}$, for some constants $c_j \in \mathbb{C}$. On the other hand, for the $j > i$, use (4.21) and Remark 4.3.3, to find first

$$y_{i+1} = \zeta_3^e c_{i+1} \cdot y_i^3 = \zeta_3^e c_{i+1} \cdot \left(c_i y_1^{3^{i-1}}\right)^3 = \zeta_3^e c'_{i+1} \cdot y_1^{3^i} \tag{4.22}$$

for $e = 0, 1, 2$. Similarly, for y_{i+2}, one obtains

$$y_{i+2} = \zeta_3^{e'} c_{i+2} \cdot y_{i+1}^3 = \zeta_3^{e'} c_{i+2} \cdot \left(\zeta_3^e c'_{i+1} y_1^{3^i}\right)^3 = \zeta_3^{e'} c'_{i+2} \cdot y_1^{3^{i+1}} \tag{4.23}$$

for $e, e' = 0, 1, 2$. By induction, one obtains

$$y_j = \zeta_3^e c'_j \cdot y_1^{3^{j-1}} \tag{4.24}$$

for all $j > i$, where $e = 0, 1, 2$. Thus, the formal completion of the coordinate ring is

$$\mathbb{C}[[y_1, \ldots, y_{n-1}]] / \left(y_2 - c_2 y_1^3, \ldots, y_i - c_i y_1^{3^{i-1}}, \prod_{e=0}^{2} \left(y_{i+1} - \zeta_3^e c'_{i+1} \cdot y_1^{3^i}\right), \ldots, \prod_{e=0}^{2} \left(y_{n-1} - \zeta_3^e c'_{n-1} \cdot y_1^{3^{n-2}}\right) \right)$$

$$\cong \mathbb{C}[[y_1, y_{i+1}, \ldots, y_{n-1}]] / \left(\prod_{e=0}^{2} \left(y_{i+1} - \zeta_3^e c'_{i+1} \cdot y_1^{3^i}\right), \ldots, \prod_{e=0}^{2} \left(y_{n-1} - \zeta_3^e c'_{n-1} \cdot y_1^{3^{n-2}}\right) \right)$$

Again, the resolution of the singularity here is trivial : it is 3^{n-i-1} lines. They each send

$$t \mapsto (t \ , \ \zeta_3^{e_1} c'_{i+1} \cdot t^{3^i} \ , \ \zeta_3^{e_2} c'_{i+2} \cdot t^{3^{i+1}} \ , \ \ldots \ , \ \zeta_3^{e_{n-i-1}} c'_{n-1} \cdot t^{3^{n-2}}) \tag{4.25}$$

for all possible combinations $(e_1, \ldots, e_{n-i-1}) \in \{0, 1, 2\}^{n-i-1}$. This proves the first part of our claim.

For the second part, one simply has to apply the same procedure, but by writting everything in terms of y_{n-1} instead. One may verify that the situation is perfectly anti-symmetrical. Namely, it is the first few equations, i.e. $F^{(j)}$ for $j < i$, that factor into products of 3 distinct terms, when all the last ones, i.e. $F^{(j)}$ for $j \geq i$, only factor into a unique irreducible term. Namely, one may check that for $P_{i,k}^{(n)} \in E_{3^n}$, where $n > 2i$, the formal completion of the coordinate ring is

$$\mathbb{C}[[y_1,\dots,y_{n-1}]]/\left(\prod_{e=0}^{2}(y_1-\zeta_3^e d_1\cdot y_{n-1}),\dots,\prod_{e=0}^{2}\left(y_{i-1}-\zeta_3^e d_{i-1}\cdot y_{n-1}^{3^{i-2}}\right), y_i-c_i y_{n-1}^{3^{i-1}},\dots,y_{n-2}-c_{n-2}y_{i-1}^{3}\right)$$

$$\cong \mathbb{C}[[y_1,\dots,y_{i-1},y_{n-1}]]/\left(\prod_{e=0}^{2}(y_1-\zeta_3^e d_1\cdot y_{n-1}),\dots,\prod_{e=0}^{2}\left(y_{i-1}-\zeta_3^e d_{i-1}\cdot y_{n-1}^{3^{i-2}}\right)\right)$$

for some constants $d_j \in \mathbb{C}$. Therefore, no matter the value of $n > 2i$, the nonsingular model here is always exactly 3^{i-1} lines. They each map

$$t \mapsto (\zeta_3^{e_1}d_1\cdot t,\dots,\zeta_3^{e_{i-1}}d_{i-1}\cdot t^{3^{i-2}},t) \tag{4.26}$$

for all possible combinations $(e_1,\dots,e_{i-1}) \in \{0,1,2\}^{i-1}$. This shows the second part of our claim.

This finally tells us exactly what happens to the blue arrows from Figure 4.1, i.e. how many points are ramified in $\pi_0 : X_0(3^n) \mapsto X_0(3^{n-1})$. For any fixed i,k, the points $P_{i,k}^{(n)}$ is no longer ramified when $n \leq 2i$. The first singularity $P_{i,k}^{(i+2)}$ separates into 3 points, $P_{i,k}^{(i+3)}$ separates into 9 points, and so on until $P_{i,k}^{(2i)}$ which separates into 3^{i-1} points. However, all the points above this, i.e. $P_{i,k}^{(n)}$, for $n > 2i$, will also separate into exactly 3^{i-1} points. Thus, this leads to a tower of ramification involving 3^{i-1} ramified points, all of ramification index 3. In the following picture, we change color to better identify the different towers of ramification. Also, one may see that the fibers in the top right corner are not fully written, due to the lack of space. Finally, for the simple points of E_{3^n} (the black points in Figure 4.1), the same notation is used to denote the point the represent in $X_0(3^n)$.

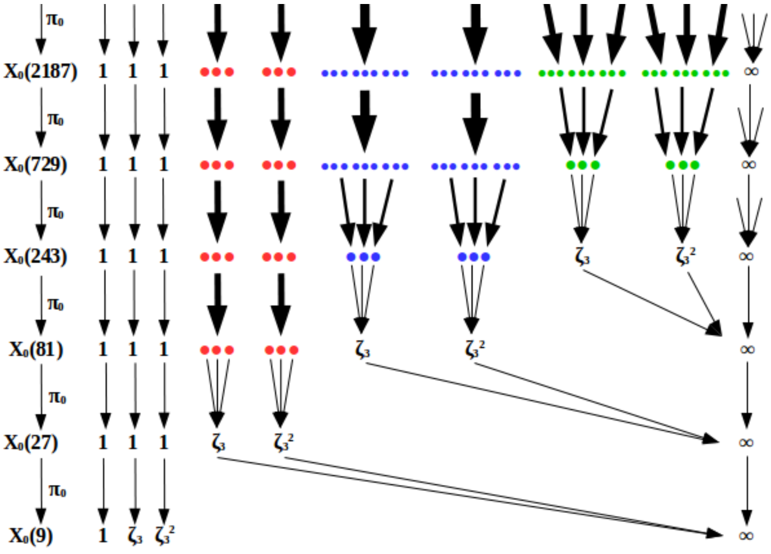


Figure 4.2: Ramifications behavior in the tower $X_0(3^n)$

Therefore, we now have that $\pi_0 : X_0(3^n) \to X_0(3^{n-1})$ has exactly

$$3 + (2 \cdot 3) + (2 \cdot 9) + \ldots + (2 \cdot 3^{\lfloor (n-2)/2 \rfloor}) = 3^{\lfloor (n-1)/2 \rfloor} \tag{4.27}$$

ramification points, where $\lfloor x \rfloor$ is the floor value of x.

Conclusion : We can finally substitute this into (4.15) and working out the recursion, we obtain that, for $n \geq 3$, the genus of $X_0(3^n)$ is

$$g(X_0(3^n)) = 1 + \sum_{i=1}^{n-3} 3^{\lfloor (n+i-2)/2 \rfloor} = \begin{cases} 3^{n-2} - 2 \cdot 3^{\frac{n-2}{2}} + 1 \ , & \text{if } n \text{ is even.} \\ 3^{n-2} - 3^{\frac{n-1}{2}} + 1 \ , & \text{if } n \text{ is odd.} \end{cases} \tag{4.28}$$

Bibliography

[DS] DIAMOND, Fred. SHURMAN, Jerry. *A First Course in Modular Forms.* Springer, 2005.

[E] ELKIES, Noam D. Explicit modular towers. Harvard University, 2001.

[F] FULTON, William. Algebraic curves. Université de Versailles, 2005.

[H] HASEGAWA, Takehiro. An Explicit Shimura Tower of Function Fields over a Number Field: An Application of Takeuchi's List. Shiga University, Otsu, Japan, 2017.

[K] KOLLÁR, János. Resolution of Singularities. Princeton University, 2005.

[S] SILVERMAN, Joseph H., Advanced Topics in the Arithmetic of Elliptic Curves. Brown University, 1994.